A Probabilistic Logic for Concrete Security

David Baelde *, Caroline Fontaine ‡, Adrien Koutsos †, Guillaume Scerri ‡, Théo Vignon ‡
* Univ Rennes, CNRS, IRISA, France
† Inria Paris, France
‡ Université Paris-Saclay, CNRS, ENS Paris-Saclay, LMF, Gif-sur-Yvette, France

***Index Terms*—Logic, Concrete Security, Crypto Protocols**

***Abstract*—The Squirrel Prover is a proof assistant designed for the computational verification of cryptographic protocols. It implements a probabilistic logic that captures cryptographic and probabilistic arguments used in security proofs. This logic operates in the asymptotic security setting, which limits the expressiveness of formulas and proofs. As a consequence, it can only prove security for finite interactions with a protocol, falling outside of the polynomial-level of security usually expected by cryptographers. We lift all these limitations by moving to a concrete security setting. We extend the logic with concrete security predicates, and design a corresponding proof system. We show the usefulness of these extensions on a case study, and through a novel proof-transformation result which shows that a large class of asymptotic logic security proofs can be automatically rewritten into concrete logic security proofs, improving security bounds exponentially.**

I. Introduction

Cryptographic protocols are crucial to get secure communications, e.g. for online payment or messaging. Strong guarantees on their security can be provided through cryptographic proofs, *via* formal mathematical analyses of the protocols and the targetted security properties. Unfortunately, properly designing a protocol remains challenging [1], [2], as cryptographic proofs can be involved and error-prone [3], [4], because of the complexity of the protocol and the intricacies of the cryptographic arguments needed. Theses issues have lead to the development of verification tools allowing for the *mechanization* of cryptographic proofs (see [5] for a survey).

In more details, the principle of a cryptographic proof is to show that no adversary — assumed to be an arbitrary probabilistic polynomial Turing machine (PPTM) — can break the protocol security. Pen-and-paper proofs usually proceed as follows. First, the security of the protocol is expressed as a *game* between the adversary and a *challenger*, modeling the security of the protocol. Then, this game is iteratively modified by a sequence of game hops [6], where each hop is justified by a cryptographic reduction or some other probabilistic argument. Finally, the proof concludes when the prover manages to obtain a game in which security trivially holds.

Example 1. *The Private Authentication (PA) protocol [7] is a two-message protocol in which agents* A *and* B *attempt to authenticate each other and establish a shared session key. It aims to ensure privacy in the sense that an outside observer cannot tell whether* B *accepts to communicate with* A*. To do so,* A *sends to* B *the message* $\mathsf{enc}(\langle \mathsf{pk_A}, \mathsf{n_A}\rangle, \mathsf{pk_B}, \mathsf{r_A})$*, i.e. a randomized asymmetric encryption of* A*'s identity (represented by its public key) and of a fresh random nonce* $\mathsf{n_A}$ *of length* η*, under the public key of* B *—* $\mathsf{r_A}$ *is the randomness needed by the randomized asymmetric encryption* enc*. When he receives this message,* B *decrypts it and replies with* $\mathsf{enc}(\langle \mathsf{n_B}, \mathsf{n_A}\rangle, \mathsf{pk_A}, \mathsf{r_B})$*. If the received message is not valid,* B *replies with* $\mathsf{enc}(\langle \mathsf{n_B}, 0^\eta\rangle, \mathsf{pk_A}, \mathsf{r_B})$*. Notice that* B*'s two possible answers are encryptions of same-length plaintexts, and will thus be indistinguishable for an outside observer. In this example, we want to prove that the adversary cannot know if B wanted to talk to A or not. This property holds thanks to B's second possible answer, which is a decoy message sent when B doesn't accept the communication with A. Note that this is independent from proving that A is able to know whether B has accepted her message or not (which is actually the case here, up to negligible probability).*

Several techniques have been developed to mechanize the analysis of such cryptographic arguments. The CryptoVerif [8] tool proceeds by the automatic application of game transformations. While this tool is highly automated on simple examples, more complex protocols often require heavy user guidance. It must also be noted that CryptoVerif does not support generic mathematical reasoning: when such arguments are needed, they must be assumed in the tool through axioms, and externally proven. Probabilistic Relational Hoare Logics [9] (pRHL), upon which several tools are based (e.g. EasyCrypt [10], CryptHOL [11], and SSProve [12]), encodes games as imperative programs, and allows to express cryptographic reductions as relational properties of these programs. This is a very expressive logic, but this comes at a cost: reasoning is done at a relatively low level, which can lead to long and tedious proof developments.

In this paper, we are interested in another approach for cryptographic protocol verification called the Computationally Complete Symbolic Attacker (CCSA) model. This approach, initially introduced in [13], is based on a logic with a probabilistic semantics that can be used to encode a protocol security as an indistinguishability formula $\vec{u} \sim \vec{v}$ where, essentially, $\vec{u}$ and $\vec{v}$ model messages exchanged over the network (typically, $\vec{u}$ corresponds to an execution of the protocol studied, while $\vec{v}$ is for an idealized version of this protocol). Then, the formula $\vec{u} \sim \vec{v}$ can be shown valid using reasoning rules, therefore proving that the protocol is secure. The CCSA logic — modified to internalize the notion of

This work received funding from the France 2030 program managed by the French National Research Agency under grant agreement No. ANR-22-PECY-0006.

protocol execution and of inductive reasoning — has been implemented into a proof assistant called Squirrel [14]. Since then, Squirrel and its logic have been extended and used several times, to support and analyze stateful protocols [15], to be adapted to a post-quantum cryptography setting [16], and to support higher-order reasoning [17]. As the logic of [17] is the most expressive one, we will rely on it in this paper.

Example 2. *We consider a simple scenario with two agents* A *and* B *willing to talk to each other, where each agent plays an arbitrary number of sessions. Our encoding uses some mutually recursive functions:* output (X,N) *is the output of agent* X $\in \{$A, B$\}$ *for the* N*-th interaction with the adversary;* choose N *lets the adversary decide whether the* N*-th interaction is with* A *or* B*;* input N *is the* N*-th input sent by the adversary; and* frame N *is the sequence of the first* N *outputs of the protocol, extended with the public values* $\mathsf{pk_A}$ *and* $\mathsf{pk_B}$.

The N*-th input* input N *is any value that can be computed by the adversary using its current knowledge,* i.e. *the sequence* frame (N–1) *of the first* N–1 *outputs of the protocol. We model the adversary's computation using the adversarial function* $\mathsf{att_i}$*, and define* choose (N–1) *using the adversarial function* $\mathsf{att_c}$*:*

$$\mathsf{input}\ \mathsf{N} \stackrel{\text{def}}{=} \mathsf{att_i}(\mathsf{frame}\ (\mathsf{N}-1)) \quad \mathsf{choose}\ \mathsf{N} \stackrel{\text{def}}{=} \mathsf{att_c}(\mathsf{frame}\ (\mathsf{N}-1))$$

The sequence of outputs frame N *is easily defined as:*

$$\mathsf{frame}\ \mathsf{N} \stackrel{\text{def}}{=} \begin{cases} \langle\, \mathsf{frame}\ (\mathsf{N}-1), \mathsf{output}\ (\mathsf{choose}\ \mathsf{N}, \mathsf{N})\rangle & \textit{if}\ \mathsf{N} \geq 0 \\ \mathsf{pk_A}, \mathsf{pk_B} & \textit{if}\ \mathsf{N} = 0 \end{cases}$$

To model the freshness of the random nonce $\mathsf{n_A}$ *and encryption randomness* $\mathsf{r_A}$ *in* A*'s message, we index these values by the interaction number* N*. We do the same for* B*.*

$$\begin{aligned}
\mathsf{output}\ (\mathsf{A},\mathsf{N}) &\stackrel{\text{def}}{=} \mathsf{enc}(\langle\, \mathsf{pk_A}, \mathsf{n_A}\ \mathsf{N}\rangle, \mathsf{pk_B}, \mathsf{r_A}\ \mathsf{N})\\
\mathsf{output}\ (\mathsf{B},\mathsf{N}) &\stackrel{\text{def}}{=} \\
&\quad \textbf{if}\ \mathsf{fst}\ (\mathsf{dec}(\mathsf{input}\ \mathsf{N}, \mathsf{sk_B})) = \mathsf{pk_A}\ \&\& \\
&\qquad \mathsf{len}\ (\mathsf{snd}\ (\mathsf{dec}(\mathsf{input}\ \mathsf{N}, \mathsf{sk_B}))) = \eta\\
&\quad \textbf{then}\ \mathsf{enc}(\langle\, \mathsf{n_B}\ \mathsf{N}, \mathsf{snd}\ (\mathsf{dec}(\mathsf{input}\ \mathsf{N}, \mathsf{sk_B}))\rangle, \mathsf{pk_A}, \mathsf{r_B}\ \mathsf{N})\\
&\quad \textbf{else}\ \mathsf{enc}(\langle\, \mathsf{n_B}\ \mathsf{N}, 0^{\eta}\rangle, \qquad \mathsf{pk_A}, \mathsf{r_B}\ \mathsf{N})
\end{aligned}$$

Here, fst *and* snd *denote the first and second projections w.r.t.* $\langle\cdot,\cdot\rangle$*, and* len *denotes the length function.*

The CCSA approach operates in the *asymptotic security* model, which considers that a protocol is secure if the probability that an adversary breaks it is a negligible function of the *security parameter* η — where η can be, e.g., the length of the keys, and a function is negligible if it is asymptotically smaller than the inverse of any polynomial. In particular, predicate $\vec{u} \sim \vec{v}$ states that the advantage of any PTIME adversary in distinguishing $\vec{u}$ from $\vec{v}$ is negligible in η.

Example 3. *Following our running example of the PA protocol, we can express the fact that it preserves user* A*'s privacy with the* unlinkability *property [18]* frame N $\sim$ $\mathsf{frame_{id}}$ N *which states that no adversary can distinguish an execution of the protocol from an idealization of the protocol where, each time* A *sends a new message, we change its identity by using a different public key* $\mathsf{pk'_A}$ N *in each output. This idealized protocol is defined as the normal protocol, except for* A*'s output which is replaced by:* $\mathsf{output_{id}}\ (\mathsf{A},\mathsf{N}) \stackrel{\text{def}}{=} \mathsf{enc}(\langle\, \mathsf{pk'_A}\ \mathsf{N}, \mathsf{n_A}\ \mathsf{N}\rangle, \mathsf{pk_B}, \mathsf{r_A}\ \mathsf{N})$*. The identity verification in* B *remains the same, but it may not pass anymore even when an output of* A *is forwarded to* B*:* $\mathsf{pk_A}$ *may or may not be equal to* $\mathsf{pk'_A}$ N *depending on* N*.*

If the encryption function is IND-CCA1, it can be shown that the PA protocol is unlinkable for any constant number of sessions. More precisely, we can prove by induction over N*:*

$$\tilde{\forall}\, \mathsf{N}.\ \mathsf{const}(\mathsf{N}) \,\tilde{\Rightarrow}\, \mathsf{frame}\ \mathsf{N} \sim \mathsf{frame_{id}}\ \mathsf{N} \tag{1}$$

a) Limitations: The asymptotic model allows for simple, high-level CCSA logic that completely hides probabilities and security parameter from the user. However, this limits the logic in several ways:

1) *Expressivity:* precise security bounds cannot be expressed by the logic, limiting the practical applicability of the logic [19]. E.g., the logic cannot be used to determine what should be the size the keys in a concrete application.
2) *Reasoning:* some cryptographic arguments cannot be captured in their full generality by the logic. For example, the most general version of the hybrid argument [20], [21] states that $t_0 \sim t_{P(\eta)}$ (where P is a polynomial) if it can be proved that, for every $i < P(\eta)$, we have $t_i \sim t_{i+1}$ *with a uniform advantage w.r.t. the security parameter*. Since the asymptotic CCSA logic cannot express precise security bounds, the uniformity conditions cannot be checked, putting such arguments out-of-reach.
3) *Security guarantees:* as a consequence of 2), the adversary must usually be restricted to a constant (i.e. independent from η) number of interactions with the protocol. For example, this is the case for the formula in Eq. (1) of Example 3, as it is proved by induction over N — induction is essentially an hybrid argument. Said otherwise, asymptotic CCSA logic can usually only be used to prove that a protocol provides a *parametric* level of security, instead of the stronger *polynomial* level of security expected by cryptographers.

b) Contributions: We lift all these limitations by moving to the concrete security setting. As a first contribution, we extend the asymptotic CCSA logic of [17] with concrete security variants of the security predicates: e.g., the new predicate $u \sim_{\varepsilon} v$ states that the distinguishing advantage of any adversary against $u \sim v$ is at most ε. Then, we design a new proof system for these new concrete security predicates, and show its usefulness through a case study.

Unfortunately, translating idiomatic asymptotic CCSA proofs in the concrete logic yields advantage upper-bounds which are exponential in the number of interactions with the adversary. Because of this, it could be feared that the idiomatic CCSA proof strategy — and all existing proofs relying on it — should be abandoned. We argue that this is not the case through our second contribution, a novel theoretical result which shows that a large class of (asymptotic) CCSA proofs can be automatically rewritten into concrete security proofs with an optimized advantage which reaches the sought-after polynomial level of security. Crucially, this result is not a simple rule-by-rule translation, but involves a whole-proof transformation through non-trivial rule commutations. Finally, we show a representative practical example proof which falls in our class of proofs, and can thus be transformed to obtain polynomial security.

c) Outline: We describe our CCSA logic for concrete security in Section II, and its proof system in Section III. We illustrate this system on the Private Authentication protocol in Section IV. We then present in Section V our proof-transformation result, allowing to derive polynomial security from any proof in a significant fragment of our system.

II. Logic

We now present our extension of the probabilistic logic for cryptographic reasoning of [17] to a concrete security setting.

Terms of the logic, which are the same as in [17] (extended with let in constructor), are simply-typed higher-order terms with special symbols (called *names*) used to denote random samplings. A key feature of the logic is that all terms are interpreted using the same set of random bits, from which they retrieve exactly the randomness they need. This allows to track probabilistic dependencies between terms.

Formulas of [17] are first-order formulas built on top of a set of predicates capturing probabilistic and computational properties of terms. Mainly, our new logic extends the formulas of [17] with two new concrete security predicates: $[\phi]_\varepsilon$ states that the probability that ϕ does not hold is at most ε, and $t_0 \sim_\varepsilon t_1$ states that the probability that an adversary distinguishes t_0 from t_1 is at most ε.

A. Terms

We first recall the types and terms of our logic.

a) Types: We consider simple types, noted τ, generated from base types $\tau_\mathsf{b} \in \mathbb{T}$ using the arrow construct $\cdot \to \cdot$. The set of *base types* $\mathbb{T}$ must contain at least the types $\mathsf{bool}, \mathsf{message}, \mathsf{int}, \overline{\mathsf{int}}$ (modeling the set $\mathbb{N} \cup \{+\infty\}$), bint (modeling the set of integers $[0, N_\eta]$ where N_η is an arbitrary integer fixed by the model), and $\overline{\mathsf{real}}$ (modeling the set $\mathbb{R} \cup \{-\infty, +\infty\}$).

We identify a subset $\mathbb{B} \subseteq \mathbb{T}$ of *bit-string encodable* base types, that contains at least bool, $\mathsf{message}$, bint, int, and $\overline{\mathsf{int}}$. We say that a type has *order* 0 when it belongs to $\mathbb{B}$, and that it has order $n+1$ when it is of the form $\tau \to \tau'$ where τ has order at most n and τ' has order at most $n+1$. For example, $\mathsf{int}^k \to \mathsf{message} = \mathsf{int} \to \ldots \to \mathsf{int} \to \mathsf{message}$ has order 1.

The semantics of types is described by a *type structure* $\mathbb{M}$ which assigns to each base type $\tau_\mathsf{b} \in \mathbb{T}$ and each value of the security parameter $\eta \in \mathbb{N}$ an interpretation domain $[\![\tau_\mathsf{b}]\!]^\eta_\mathbb{M}$. The interpretation of a type in $\mathbb{B}$ must be a subset of $\{0,1\}^*$. We force the interpretation of standard types to be the expected one, e.g. $[\![\mathsf{int}]\!]^\eta_\mathbb{M}$ is the set of (bit-string encodings of) integers $\mathbb{N}$ and $[\![\mathsf{message}]\!]^\eta_\mathbb{M} = \{0,1\}^*$ (for every η). Arbitrary types are then interpreted by defining $[\![\tau_0 \to \tau_1]\!]^\eta_\mathbb{M} = [\![\tau_0]\!]^\eta_\mathbb{M} \to [\![\tau_1]\!]^\eta_\mathbb{M}$. We say that a type is *finite* if its interpretation is finite for every η. For example, the type bint is finite since for every $\eta \in \mathbb{N}$, it contains $N_\eta + 1$ elements for some arbitrary integer N_η fixed by the model.

b) Terms: Our *terms* are simply-typed λ-terms built upon a set of variables $\mathcal{X}$:

$$t ::= x \mid t\ t \mid \lambda(x:\tau).\,t \mid \forall(x:\tau).\,t \mid \mathsf{let}\ (x:\tau) = t\ \mathsf{in}\ t$$

where $x \in \mathcal{X}$. Terms are considered modulo α-renaming, and we let $\mathsf{fv}(t)$ be the free variables of t. A variable x in $\mathcal{X}$ can be used to denote a function argument coming from a λ binder, a logical variable quantified by a $\forall$, but also a function symbol (e.g. integer addition $+$). We write $\lambda x_1, \ldots, x_n.\,t$ for $\lambda x_1. \ldots . \lambda x_n.\,t$, and $t\ \vec{u}$ stands for $((t\ u_1)\ \ldots\ u_n)$ when $\vec{u} = u_1, \ldots, u_n$.

An *environment* $\mathbb{E}$ is a finite sequence of variable *declarations* $(x:\tau)$ and *definitions* $(x:\tau = t)$. A declared or defined variable is said to be bound in $\mathbb{E}$, and we require that no environment declares a variable twice. We consider the same standard type system as [17], and we write $\mathbb{E} \vdash t : \tau$ (resp. $\vdash \mathbb{E}$) if t has type τ in $\mathbb{E}$ (resp. if $\mathbb{E}$ is well-typed). As usual, we require that terms and environments are well-typed.

We only consider environments containing at least the declarations of a number of standard functions such as Boolean connectives (e.g. $\wedge, \vee, \to$), integer operations ($+, \times, \ldots$), etc.

Environments support (mutually) recursive definitions. In our examples, this is used when defining $\mathsf{frame}\ \mathsf{N}$. We refer the reader to [17] for a presentation of the well-foundedness conditions guarding recursive definitions.

A *term structure* $\mathbb{M}$ for $\mathbb{E}$ is a type structure extended with:

- a set $\mathbb{T}_{\mathbb{M},\eta} = \mathbb{T}^\mathsf{a}_{\mathbb{M},\eta} \times \mathbb{T}^\mathsf{h}_{\mathbb{M},\eta}$ where $\mathbb{T}^\mathsf{a}_{\mathbb{M},\eta}$ (resp. $\mathbb{T}^\mathsf{h}_{\mathbb{M},\eta}$) is the finite set of all random tapes of a given length. For example, $\mathbb{T}^\mathsf{a}_{\mathbb{M},\eta}$ can be the set $\{0,1\}^{P(\eta)}$ of all random tapes of length $P(\eta)$ for some polynomial P. Tapes in $\mathbb{T}^\mathsf{a}_{\mathbb{M},\eta}$ are used for the *adversarial* randomness, while tapes in $\mathbb{T}^\mathsf{h}_{\mathbb{M},\eta}$ are used for *honest* randomness (e.g. for names).
- for any defined or declared variable x in $\mathbb{E}$ of type τ, $\mathbb{M}$ defines its interpretation $\mathbb{M}(x) \in \mathbb{RV}_\mathbb{M}(\tau)$ where $\mathbb{RV}_\mathbb{M}(\tau)$ is the set of η-indexed random variables from $\mathbb{T}_{\mathbb{M},\eta}$ to the sampling space $[\![\tau]\!]^\eta_\mathbb{M}$.

Variables interpretation is lifted to term interpretation $[\![\cdot]\!]^{\eta,\rho}_\mathbb{M}$:

$$[\![x]\!]^{\eta,\rho}_\mathbb{M} \stackrel{\mathsf{def}}{=} \mathbb{M}(x)(\eta)(\rho) \qquad [\![t\ t']\!]^{\eta,\rho}_\mathbb{M} \stackrel{\mathsf{def}}{=} [\![t]\!]^{\eta,\rho}_\mathbb{M}\,([\![t']\!]^{\eta,\rho}_\mathbb{M})$$

$$[\![\lambda(x:\tau_0).\,t]\!]^{\eta,\rho}_\mathbb{M} \stackrel{\mathsf{def}}{=} \begin{cases} [\![\tau_0]\!]^\eta_\mathbb{M} & \to\ [\![\tau]\!]^\eta_\mathbb{M} \\ \quad a & \mapsto\ [\![t]\!]^{\eta,\rho}_{\mathbb{M}[x\mapsto \mathbb{1}^\eta_a]} \end{cases}$$

where, in the last case, t is of type τ and $\mathbb{1}^\eta_a \in \mathbb{RV}_\mathbb{M}(\tau)$ is a random variable such that $\mathbb{1}^\eta_a(\eta)(\rho) = a$ for every ρ.

A *model* $\mathbb{M}$ for $\mathbb{E}$ is a term structure such that, for any definition $(x:\tau = t) \in \mathbb{E}$, $[\![x]\!]^{\eta,\rho}_\mathbb{M} = [\![t]\!]^{\eta,\rho}_\mathbb{M}$. The existence of models is non-trivial due to recursive definitions, but [17, Theorem 1] guarantees it, thanks to well-foundedness conditions.

c) Names: We assume a subset $\mathcal{N} \subseteq \mathcal{X}$ of symbols called *names*, used to denote random samplings. A name $\mathsf{n} \in \mathcal{N}$ can only be declared in $\mathbb{E}$, and must be of type $\tau_0 \to \tau_1$. The semantics $[\![\mathsf{n}]\!]_\mathbb{M}$ of [17] interprets a name n as a sequence (indexed by values in τ_0) of *independent identically distributed random samplings* over τ_1. For example, $[\![\mathsf{n}\ 0]\!]_\mathbb{M}$ and $[\![\mathsf{n}\ 1]\!]_\mathbb{M}$

are independent random variables. This is also true for distinct name symbols: $[\![\mathsf{n}\ i]\!]_{\mathbb{M}}$ and $[\![\mathsf{n}'\ j]\!]_{\mathbb{M}}$ are always independent.

To guarantee that all instances of a name can be sampled with finite randomness, we require that τ_0 is a finite type.

When indices are not needed, we allow names of base types, corresponding to a single random sampling (independent of other names, as before). For instance, Example 2 uses indexed names $\mathsf{r_A} : \mathsf{bint} \to \mathsf{message}$ but also name $\mathsf{sk_A} : \mathsf{message}$ to model the secret key from which $\mathsf{pk_A} = \mathsf{pk}\ \mathsf{sk_A}$ is derived.

B. Execution and Cost Model

Many rules of our logic will be proven by reductions and will thus have a time overhead, *i.e.* the additional time taken by the adversary involved in the reduction. In a concrete security setting, this time overhead needs to be tracked, leading to two difficulties: first, accumulated time overheads can clutter the proof, making it hard to analyze; second, bounding the time overhead in a reduction step may require proving additional cost-related sub-goals, which can be tedious. We alleviate these issues by fine-tuning our execution and cost model. The model described below is a key ingredient to obtain a simple proof system: it allows to reduce (and sometimes entirely remove) time overheads in proof rules.

We now describe PPTM, our set of machines. A machine $\mathcal{A} \in \mathsf{PPTM}$ with l bit-string inputs and k oracles is a Turing machine over the binary alphabet with a special read-only input tape used to receive the security parameter in unary, at least l working tapes, a special *oracle input* tape, and a read-only randomness tape. The working tapes of the machine also serve as input and output tapes, as well as output tapes for the oracles. If $\vec{w}$ is a vector of l bit-strings and $\vec{f}$ is a vector of k bit-string oracles, i.e. functions from bit-strings to bit-strings:

$$\vec{w} = (w_1, \dots, w_l) \text{ where } \forall i.\, w_i \in \{0,1\}^*$$
$$\vec{f} = (f_1, \dots, f_k) \text{ where } \forall i.\, f_i \in \{0,1\}^* \to \{0,1\}^*$$

then the result $\mathcal{A}^{\vec{f}}(1^\eta, \vec{w}, \rho_{\mathsf{a}})$ of the execution of $\mathcal{A}$ on inputs $\vec{w}, \vec{f}$ with security parameter η and randomness ρ_{a} is the bit-string obtained as follows:

- $\mathcal{A}$'s security parameter tape is initialized to 1^η, its randomness tape to ρ_{a}, its first l working tapes to $\vec{w}$. The rest of the tapes are all initially empty.
- Then, $\mathcal{A}$ starts its execution, modifying the content of its tapes according to its transition table.
- At any point, $\mathcal{A}$ can make a special transition to call oracle f_i, as follows. $\mathcal{A}$ selects a *working tape* T (T cannot be the oracle input tape). Then, in one step $f_i(x)$ is written on tape T, where x is the content of the oracle input tape and the oracle input tape is reset to the empty tape.
- When it ends, $\mathcal{A}$ returns the content of its output tape.

We allow $\mathcal{A}$ to have several heads, also allowing multiple heads on the same tape, we require that all heads start at the begining of the tape when the execution of $\mathcal{A}$ start. The layout of the machine $\mathcal{A}$ is static: in particular, no new tape (or head) can be spawned during the execution, and $\mathcal{A}$'s output tape is always the same. We require that $\mathcal{A}$'s transitions are deterministic — any source of randomness must come from the random tape ρ_{a}.

The *time cost* $\mathsf{time}_{\mathcal{A}}(1^\eta, \vec{w}, \vec{f}, \rho_{\mathsf{a}})$ is the number of computation steps of $\mathcal{A}^{\vec{f}}(1^\eta, \vec{w}, \rho_{\mathsf{a}})$.

One of the consequences of our model choice, which helps to simplify overhead expressions in several rules, is that a machine $\mathcal{A}$ running in time t cannot call an oracle on an input of size larger than t. Indeed, such an input would have to be written on the oracle input tape. This relies on the fact that the oracle input tape is not a working tape, and therefore cannot be selected by $\mathcal{A}$ to hold the result of an oracle call. However, we do not make any assumption on oracles, which can return arbitrarily large bit-strings in one step.

C. Global Formulas

We now present the formulas of our logic and their semantics. We use a standard first-order logic over our higher-order terms, with predicates that are specific to concrete security reasoning. We consider, in particular, a predicate $\sim$ for computational indistinguishability and a predicate $[\cdot]$ for almost-always truth. The syntax is as follows, where $u, \vec{u}, \vec{v}, \phi, \varepsilon, l$ and t are (sequences of) terms (see below for constraints on their types):

$$F ::= F \mathrel{\tilde{\Rightarrow}} F \mid \tilde{\neg} F \mid \tilde{\forall}(x : \tau).\, F \mid \mathsf{const}(u) \mid \mathsf{adv}_{t,\vec{\sigma}}(u) \mid [\phi]_\varepsilon \mid \vec{u} \sim_\varepsilon \vec{v} \mid \mathsf{blen}_l(u)$$

We write $\mathbb{M} \models F$ when F holds in $\mathbb{M}$. This is defined as usual in first-order logic for Boolean connectives and quantifiers, and we give below the semantics of our specific predicates. As usual, we obtain $\tilde{\wedge}, \tilde{\vee}, \tilde{\exists}$ from $\tilde{\Rightarrow}, \tilde{\neg}$ and $\tilde{\forall}$. Remark that we use a special notation to distinguish global Boolean connectives and quantifiers $\tilde{\Rightarrow}, \tilde{\forall}, \dots$ from their local counter-parts $\Rightarrow, \forall, \dots$.

We now describe and give the semantics of our predicates.

a) Almost-always truth: The predicate $[\phi]_\varepsilon$ states that ϕ (a term of type bool) is true with a probability of error that is bounded by ε (a term of type $\overline{\mathsf{real}}$). In order to ease equational reasoning in our proof system, we will more specifically use the *expectation* of the random variable $\rho \mapsto [\![\varepsilon]\!]^{\eta,\rho}_{\mathbb{M}}$. Formally,

$$\mathbb{M} \models [\phi]_\varepsilon \quad \text{iff} \quad \Pr_\rho\left([\![\phi]\!]^{\eta,\rho}_{\mathbb{M}}\right) \geq 1 - \mathsf{E}_\rho([\![\varepsilon]\!]^{\eta,\rho}_{\mathbb{M}}) \quad \text{for all } \eta$$

For example if $\mathsf{n}_0, \mathsf{n}_1$ are names drawn uniformly at random from $\{0,1\}^\eta$, both $[\mathsf{n}_0 = \mathsf{n}_0]_0$ and $[\mathsf{n}_0 \neq \mathsf{n}_1]_{\frac{1}{2^\eta}}$ hold (where 0 and $\frac{1}{2^\eta}$ are terms interpreted as their real counterpart).

b) Indistinguishability: The indistinguishability predicate only makes sense when the terms on both sides of the equivalence can be passed to a distinguisher $\mathcal{A} \in \mathsf{PPTM}$, either as inputs or as oracles. The former case corresponds to order 0 terms (i.e. terms with order 0 types) and the latter to order 1 terms. We thus only consider instances $\vec{u}_l, \vec{f}_l \sim_\varepsilon \vec{u}_r, \vec{f}_r$ where:

- $\vec{u}_l$ and $\vec{u}_r$ are two same-length sequences of order 0 terms, where the k^{th} terms of each sequence have the same type;
- $\vec{f}_l, \vec{f}_r$ are two sequences of order 1 terms, of length m, with similarly matching types for k^{th} elements;
- ε has type $\overline{\mathsf{int}} \to \overline{\mathsf{int}}^k \to \overline{\mathsf{real}}$: intuitively, the bound ε is a function of (a) the execution time of the distinguisher

$\mathcal{A}$ and (b) the number of calls to each of the k oracles in the execution of $\mathcal{A}$.

The predicate $\vec{u}_l, \vec{f}_l \sim_\varepsilon \vec{u}_r, \vec{f}_r$ states that ε upper-bounds the probability that an adversary distinguishes two scenarios: in the left scenario, the adversary receives the bit-strings $\vec{u}_l$ and has access to the oracles $\vec{f}_l$; while in the right scenario, it receives $\vec{u}_r$ and has access to oracles $\vec{f}_r$. We require that the probability that any adversary $\mathcal{A}$ distinguishes these two scenarios is bounded by the expectation of $\varepsilon(t, \vec{\sigma})$, where t is an upper-bound on $\mathcal{A}$'s running time and $\vec{\sigma}$ is a vector of integers representing the maximal numbers of calls that $\mathcal{A}$ can make for each oracle. Formally, for an adversary $\mathcal{A}$ with no inputs, we let $\mathsf{time}^\eta_\mathcal{A} \in \mathbb{N} \cup \{+\infty\}$ be the maximal run-time of $\mathcal{A}$ for a fixed η:

$$\mathsf{time}^\eta_\mathcal{A} \stackrel{\mathsf{def}}{=} \sup_{\vec{u}, \vec{f}, \rho_\mathsf{a}} \mathsf{time}_\mathcal{A}(1^\eta, \vec{u}, \vec{f}, \rho_\mathsf{a})$$

Similarly, we let $\mathsf{calls}^\eta_\mathcal{A} \in (\mathbb{N} \cup \{+\infty\})^m$ be the vector of the maximal numbers of oracle calls of $\mathcal{A}$ for security parameter η on any oracles and random tape. All these upper bounds may be infinite for some adversaries $\mathcal{A}$: in that case, the bound on the advantage of $\mathcal{A}$ will typically be uninformative, but this is an expected feature of concrete security. Then, $\mathbb{M} \models \vec{u}_l, \vec{f}_l \sim_\varepsilon \vec{u}_r, \vec{f}_r$ iff for any $\mathcal{A}$ with $|\vec{u}_l|$ inputs and m oracles,

$$\left| \begin{array}{l} \Pr\big(\mathcal{A}^{[\![\vec{f}_l]\!]^{\eta,\rho}_\mathbb{M}}(1^\eta, [\![\vec{u}_l]\!]^{\eta,\rho}_\mathbb{M}, \rho_\mathsf{a})\big) \\ - \Pr\big(\mathcal{A}^{[\![\vec{f}_r]\!]^{\eta,\rho}_\mathbb{M}}(1^\eta, [\![\vec{u}_r]\!]^{\eta,\rho}_\mathbb{M}, \rho_\mathsf{a})\big) \end{array} \right| \le \mathsf{E}_\rho\big([\![\varepsilon]\!]^{\eta,\rho}_\mathbb{M}(\mathsf{time}^\eta_\mathcal{A}, \mathsf{calls}^\eta_\mathcal{A})\big)$$

where the probabilities are taken over $\rho = (\rho_\mathsf{a}, \rho_\mathsf{h})$ in $\mathbb{T}_{\mathbb{M},\eta}$.

Example 4. *Let us assume that* enc *is interpreted as an IND-CPA encryption with associated public key derivation* pk*, over a type of plaintexts that is finite. Assuming that* $0_\mathsf{len} : \mathsf{message} \to \mathsf{message}$ *is interpreted as the function* $x \mapsto 0^{|x|}$*, we have*

$$\lambda i.\mathsf{enc}(i, \mathsf{pk}\ \mathsf{k}, \mathsf{r}\ i) \sim_\varepsilon \lambda i.\mathsf{enc}(0_\mathsf{len}\ i, \mathsf{pk}\ \mathsf{k}, \mathsf{r}\ i)$$

provided that $\varepsilon : \mathsf{int} \to \mathsf{int} \to \mathsf{real}$ *is such that* $\varepsilon\ t\ n$ *upper-bounds the concrete advantage of an IND-CPA adversary against* enc*, running in time at most* t *and making at most* n *calls to the CPA oracle.*

c) Constancy: The predicate $\mathsf{const}(u)$ states that the semantics of an arbitrary term u does not depend on the security parameter η or the random tape ρ. Formally, $\mathbb{M} \models \mathsf{const}(u)$ iff. there exists c such that $[\![u]\!]^{\eta,\rho}_\mathbb{M} = c$ for all η and $\rho \in \mathbb{T}_{\mathbb{M},\eta}$.

d) Deterministic values: For any term u of any type and order, the predicate $\mathsf{det}(u)$ states that u is a deterministic value that, as opposed to $\mathsf{const}(u)$, can depend on the security parameter η. More precisely, for any model $\mathbb{M}$, we have $\mathbb{M} \models \mathsf{det}(u)$ iff. there exists a sequence of values $(c_\eta)_{\eta \in \mathbb{N}}$ such that $[\![u]\!]^{\eta,\rho}_\mathbb{M} = c_\eta$ for any η and ρ.

e) Bounded length: The predicate $\mathsf{blen}_l(u)$ states that the interpretation of u is of length at most l. Its precise meaning depends on the order of u, which must be at most 1.

When u is of order 0, l must have type $\overline{\mathsf{int}}$, and we have $\mathbb{M} \models \mathsf{blen}_l(u)$ if for all η and ρ, $[\![\mathsf{len}(u)]\!]^{\eta,\rho}_\mathbb{M} \le \inf_\rho [\![l]\!]^{\eta,\rho}_\mathbb{M}$. Note that we handle the possible dependency of $[\![l]\!]$ on ρ by taking the infimum of $[\![l]\!]^{\eta,\rho}_\mathbb{M}$ over all tapes (for a given η). In practice, proofs only need constant length values.

When u has order 1, l must also be a function: intuitively, it provides a bound on the length of $u\ \vec{v}$, for all $\vec{v}$, as a function of the lengths of $\vec{v}$. For example, we have $\mathbb{M} \models \mathsf{blen}_{\lambda n,m.n+m}(\lambda x, y.\langle x, y\rangle)$ in models where tupling is interpreted as concatenation.

f) Adversarial computability: Predicate $\mathsf{adv}_{t,\vec{\sigma}}(u)$ roughly expresses that u is computable by an adversary in time at most t, with at most $\vec{\sigma}$ oracle calls. Again, its meaning depends on the order of u, which must be at most 2; $\vec{\sigma}$ must be empty when u is of order at most 1.

When u has order 0, term t must have type $\overline{\mathsf{int}}$, and $\mathbb{M} \models \mathsf{adv}_t(u)$ means that there exists a machine $\mathcal{A} \in \mathsf{PPTM}$ such that $[\![u]\!]^{\eta,\rho}_\mathbb{M} = \mathcal{A}(1^\eta, \rho_a)$ for all η and ρ, such that $\mathsf{time}_\mathcal{A}(1^\eta) \le \inf_\rho([\![t]\!]^{\eta,\rho}_\mathbb{M})$. Importantly, the adversary cannot access the honest tape ρ_h here.

This is then generalized to order 1 by asking that a machine can compute the output of the function for each input, in time that depends on the size of order 0 inputs (Meaning that the bound on time t become of type $\overline{\mathsf{int}} \to \overline{\mathsf{int}}$). We further extend adversarial computability to order-2 terms by making use of oracles: for example, $\lambda f, x.\ f\ x$ where x has order 0 and f has order 1 is computable by an adversary taking a function f as oracle and an input x, and returns the output of f on x. The term t in that case imposes a bound on the execution time, as a function of the length of order-0 inputs and of length-bounding functions (of type $\overline{\mathsf{int}} \to \overline{\mathsf{int}}$) for each of the order-1 inputs. Terms $\vec{\sigma}$ bound the number of calls to each order-1 input. See Appendix A for more details.

III. Proof System

We now adapt the proof system given for asymptotic computational security in [17] to a concrete security setting. Our logic supports reasoning at two different levels, local and global, according to the kind of formulas being manipulated. This is reflected by the judgement of our logic. A *global* judgement $\mathbb{E}; \Theta \vdash F$ is composed of an environment $\mathbb{E}$, a set of global formulas Θ (the hypotheses), and a global formula F (the conclusion). A *local* judgement $\mathbb{E}; \Theta; \Gamma \vdash_\varepsilon \phi$ is composed of an environment $\mathbb{E}$, a set of global formulas Θ (the global hypotheses), a set of local formulas Γ (the local hypotheses), a local formula (i.e. a term of type bool) ϕ (the conclusion), and a term ε of type $\overline{\mathsf{real}}$ (the advantage upper-bound). All formulas (local and global) occurring in a judgement (local and global) must be well-typed in the judgement environment. The validity of global and local judgements is defined by:

$$\begin{array}{lll} \models \mathbb{E}; \Theta \vdash F & \text{iff.} & \models (\tilde{\wedge}\Theta) \tilde{\Rightarrow} F \\ \models \mathbb{E}; \Theta; \Gamma \vdash_\varepsilon \phi & \text{iff.} & \models (\tilde{\wedge}\Theta) \tilde{\Rightarrow} [(\wedge\Gamma) \Rightarrow \phi]_\varepsilon \end{array}$$

Our global judgements are the same as in [17] since the global logic remains unchanged (we only added new predicates). However, local judgements have been extended with an explicit advantage upper-bound, reflecting the move from $[\phi]$ to $[\phi]_\varepsilon$.

Example 5. *Recall that* $\mathsf{choose}\ \mathsf{N}$ *represents the agent the adversary decides to interact with at step* N *of the protocol* *execution. We can model the fact that there are only two agents in our protocol by adding the following global formula as an axiom:*

$$[\forall N.(\mathsf{choose}\ \mathsf{N} = \mathsf{A}) \vee (\mathsf{choose}\ \mathsf{N} = \mathsf{B})]_0 .$$

The validity of this formula amounts to that of the local judgement:

$$\vdash_0 (\mathsf{choose}\ \mathsf{N} = \mathsf{A}) \vee (\mathsf{choose}\ \mathsf{N} = \mathsf{B}).$$

This formula means that choose N *is always either equal to* A *or* B*. Remark that this is not equivalent to the following global formula:*

$$\tilde{\forall} N.\ [\mathsf{choose}\ \mathsf{N} = \mathsf{A}]_0\ \tilde{\vee}\ [\mathsf{choose}\ \mathsf{N} = \mathsf{B}]_0 ,$$

which states that choose N *is either always equal to* A *or always equal to* B*, and is an unrealistic assumption, as it prevents the adversary from choosing* A *or* B *in a randomized fashion.*

A. Local Proof System

Our *local proof system* provides a set of generic reasoning rules allowing to deal with Boolean connectives and higher-order quantification, and is essentially an extension of the rules of [17] with an explicit advantage upper-bound. Most local rules of our concrete security proof system are straightforward adaptations of the corresponding asymptotic rules, simply propagating probabilities in the expected way. As an example, we show two typical rules below:

$$\text{L}_\varepsilon.\text{R-}\wedge\ \frac{\mathbb{E};\Theta;\Gamma \vdash_{\varepsilon_0} \phi \qquad \mathbb{E};\Theta;\Gamma \vdash_{\varepsilon_1} \psi}{\mathbb{E};\Theta;\Gamma \vdash_{\varepsilon_0+\varepsilon_1} \phi \wedge \psi} \qquad \text{L}_\varepsilon.\text{R1-}\vee\ \frac{\mathbb{E};\Theta;\Gamma \vdash_{\varepsilon} \phi}{\mathbb{E};\Theta;\Gamma \vdash_{\varepsilon} \phi \vee \psi}$$

The $\text{L}_\varepsilon.\text{R-}\wedge$ rule states that the probability that two formulas do not jointly hold is bounded by the sum of the probabilities that each formula does not hold; while $\text{L}_\varepsilon.\text{R1-}\vee$ states that the probability that a disjunction $\phi \vee \psi$ does not hold is bounded by the probability that the left disjunct ϕ does not hold (the corresponding right rule is not shown here).

The probability that a formula does not hold lies in the real interval $[0;1]$. Nonetheless, we choose to bound such probabilities using the type $\overline{\mathsf{real}}$ corresponding to $\mathbb{R} \cup \{-\infty, +\infty\}$, as having a set that is stable by the standard arithmetic operations ($+$, $-$, and countable sums) usually allows for simpler and more elegant rules. E.g., if we use $[0;1]$, then the probability upper-bound $\varepsilon + \varepsilon'$ in the $\text{L}_\varepsilon.\text{R-}\wedge$ rule should be replaced by $\min(\varepsilon + \varepsilon', 1)$. Still, there are a few cases where this requires additional checks on the probability bounds, as in the right weakening rule shown below:

$$\text{L}_\varepsilon.\text{WEAK}_0\ \frac{\mathbb{E};\Theta;\Gamma \vdash_{\varepsilon} \psi \quad \mathbb{E};\Theta;\emptyset \vdash_0 \varepsilon \leq \varepsilon'}{\mathbb{E};\Theta;\Gamma \vdash_{\varepsilon'} \psi} \qquad \text{L}_\varepsilon.\text{WEAK}^{\mathsf{s}}_\varepsilon\ \frac{\mathbb{E};\Theta;\Gamma \vdash_{\varepsilon} \psi \quad \mathbb{E};\Theta;\emptyset \vdash_{\varepsilon_0} \varepsilon \leq \varepsilon' \qquad \mathbb{E};\Theta;\emptyset \vdash_0 \varepsilon \leq 1}{\mathbb{E};\Theta;\Gamma \vdash_{\varepsilon'+\varepsilon_0} \psi}$$

The $\text{L}_\varepsilon.\text{WEAK}_0$ rule allows to replace a probability upper-bound ε by ε' as long as ε' is *always* greater or equal to ε. The $\text{L}_\varepsilon.\text{WEAK}^{\mathsf{s}}_\varepsilon$ rule can be used if the inequality $\varepsilon \leq \varepsilon'$ does not hold unconditionally, simply by adding to ε the bound ε_0 on the probability that $\varepsilon \leq \varepsilon'$ does not hold. Moreover, because of the usage of probabilistic expectation in the logic semantics (recall that $[\phi]_\varepsilon$ holds if $\Pr(\neg[\![\phi]\!])$ is bounded by $\mathsf{E}([\![\varepsilon]\!])$), we also need to check that the bound in the premises is smaller than one. We show that such a check is necessary below.

Example 6. *Let* n *be a name (without argument) of type* message*, and assume that names over* message *are uniform random samplings among bit-strings of length η. Considering the term $\varepsilon \stackrel{\mathsf{def}}{=} 2^\eta \cdot \mathbb{1}_{\mathsf{n}=0}$, where $\mathbb{1}_\phi$ is syntactic sugar for* (if ϕ then 1 else 0)*, we have*

$$\mathsf{E}([\![\varepsilon]\!]^{\eta,\rho}_{\mathbb{M}}) = 2^\eta \cdot \Pr([\![\mathsf{n}]\!]^{\eta,\rho}_{\mathbb{M}} = 0) = 2^\eta \cdot \tfrac{1}{2^\eta} = 1$$

and $\mathbb{E};\emptyset;\emptyset \vdash_\varepsilon \bot$ holds. Moreover, $\mathbb{E};\emptyset;\emptyset \vdash_{\frac{1}{2^\eta}} \varepsilon \leq \frac{1}{2^\eta}$ holds. If the $\text{L}_\varepsilon.\text{WEAK}^{\mathsf{s}}_\varepsilon$ rule did not require that the probability bound in the premises is smaller that 1, we would obtain that $\mathbb{E};\emptyset;\emptyset \vdash_{2\cdot\frac{1}{2^\eta}} \bot$ is valid, stating that $\bot$ is true with non-zero probability. This is absurd.

For the full set of local rules, see Fig. 9 and Fig. 7 in appendix.

B. Global Proof System

Our *global proof system* comprises the usual generic reasoning rules (for Boolean connectives and quantifiers), as well as rules dedicated to the predicates of our logic (such as computational indistinguishability). Our global formulas and the semantics of their connectives are the same as in [17] — we only added new predicates. Thus, the generic logical global rules of [17] remain valid in our extension. We recall them in Appendix B for the sake of completeness, but do not describe them any further. The situation is different for rules related to specific predicates, which must be adapted.

a) Notation: Recall that in an indistinguishability formula $\vec{u} \sim_\varepsilon \vec{w}$, the advantage bound ε is a function of the adversary time t and of the number of oracle calls $\vec{o}$, where $\vec{o}$ contains as many entries as there are terms of order 1 in $\vec{u}$. For the sake of clarity, we lift the usual mathematical operations to this kind of function terms: e.g., if ε and ε' are two such bounding terms, then $\varepsilon + \varepsilon'$ denotes the term $\lambda t, \vec{o}.\, \varepsilon\ t\ \vec{o} + \varepsilon'\ t\ \vec{o}$.

b) Rewriting: Any equality, possibly with some error probability, can be used to rewrite terms occurring in a predicate of the logic, by adding the error probability of the equality to the bound in the predicate. For instance, we can rewrite the terms involved in an indistinguishability formula:

$$\frac{\mathbb{E};\Theta \vdash \vec{u}\{v_0\} \sim_\varepsilon \vec{w} \qquad \mathbb{E};\Theta \vdash [v_0 = v_1]_{\varepsilon_0}}{\mathbb{E};\Theta \vdash \vec{u}\{v_1\} \sim_{\varepsilon+\varepsilon_0} \vec{w}}$$

This rule only allows to rewrite terms on one side, as rewriting on both sides requires to pay the error probability twice.

Remark 1. *Let us show that, when rewriting terms in an equivalence formula, we cannot simultaneously rewrite on the left and right side of the equivalence without paying the equality error twice. Said otherwise, the following rule is* unsound*:*

$$\frac{\mathbb{E};\Theta \vdash \vec{u}\{v_0\} \sim_\varepsilon \vec{w}\{v_0\} \qquad \mathbb{E};\Theta \vdash [v_0 = v_1]_{\varepsilon_0}}{\mathbb{E};\Theta \vdash \vec{u}\{v_1\} \sim_{\varepsilon+\varepsilon_0} \vec{w}\{v_1\}} \qquad (2)$$

To fix this rule, it is necessary to pay ε_0 twice, i.e. to replace the bound in the conclusion by $\varepsilon + 2\,\varepsilon_0$. Now, considering three names $\mathsf{n}_0, \mathsf{n}_1, \mathsf{n}_2$ of type message *and* 0 : message *the zero bitstring, Assuming that names are uniform random samplings among bitstrings of length η, we get that:*

$$\big((\mathsf{n}_0 \neq 0) \vee \big((\mathsf{n}_1 = 0) \wedge (\mathsf{n}_2 = 0)\big)\big) \sim_\alpha \neg(\mathsf{n}_1 = 0 \wedge \mathsf{n}_2 = 0) \tag{3}$$

with $\alpha \overset{\text{def}}{=} \frac{1}{2^\eta} - \frac{1}{2^{3*\eta}} - \frac{1}{2^{2*\eta}}$ *as the exact optimal upper-bound. Indeed since any adversary cannot be better than the statistical difference between the two underlining distribution. (And the adversary that accept when the boolean it gets is true and reject otherwise as this exact advantage). Therefore, for any $\eta \in \mathbb{N}^*$,*

$$\alpha = \left| \begin{array}{c} \Pr_{\rho \in \mathbb{T}_{\mathbb{M},\eta}}\left([\![\mathsf{n}_0 \neq 0]\!]_{\mathbb{M}}^{\eta,\rho} \vee ([\![\mathsf{n}_1 = 0]\!]_{\mathbb{M}}^{\eta,\rho} \wedge [\![\mathsf{n}_2 = 0]\!]_{\mathbb{M}}^{\eta,\rho})\right) \\ -\Pr_{\rho \in \mathbb{T}_{\mathbb{M},\eta}}\left([\![\mathsf{n}_1 \neq 0]\!]_{\mathbb{M}}^{\eta,\rho} \vee [\![\mathsf{n}_2 \neq 0]\!]_{\mathbb{M}}^{\eta,\rho}\right) \end{array} \right|$$

$$= \left| \begin{array}{c} \Pr_{\rho \in \mathbb{T}_{\mathbb{M},\eta}}\left([\![\mathsf{n}_0 \neq 0]\!]_{\mathbb{M}}^{\eta,\rho}\right) \Pr_{\rho \in \mathbb{T}_{\mathbb{M},\eta}}\left(\mathsf{n}_1 \neq 0 \vee \mathsf{n}_2 \neq 0\right) \\ -\Pr_{\rho \in \mathbb{T}_{\mathbb{M},\eta}}\left([\![\mathsf{n}_1 = 0 \vee [\![\mathsf{n}_2 = 0]\!]_{\mathbb{M}}^{\eta,\rho}]\!]_{\mathbb{M}}^{\eta,\rho}\right) \end{array} \right|$$

$$= \frac{1}{2^\eta} - \frac{1}{2^{3*\eta}} - \frac{1}{2^{2*\eta}}$$

and

$$((\mathsf{n}_0 \neq 0)) \sim_{\frac{1}{2^\eta}} \top \tag{4}$$

and this bound is tight. We know that the probabilty that both n_1 and n_2 are equal to 0 at the same time is exactly $\frac{1}{2^{2\eta}}$, so $[(\mathsf{n}_1 = 0) \wedge (\mathsf{n}_2 = 0)]_{\frac{1}{2^{2\eta}}}$ holds. Rewriting this equality with help of the rule given in Eq. (2) on both the left and right side of Eq. (3), we get $((\mathsf{n}_0 \neq 0) \vee \bot) \sim_{\alpha + \frac{1}{2^{2\eta}}} \neg\bot$, which is equivalent to $((\mathsf{n}_0 \neq 0)) \sim_{\alpha + \frac{1}{2^{2\eta}}} \top$ which is exactly the formula of Eq. (4), but with a tighter bound since $\alpha + \frac{1}{2^{2\eta}} = \frac{1}{2^\eta} - \frac{1}{2^{(k+1)\eta}} < \frac{2}{2^\eta}$. This contradicts the tightness of the bound of Eq. (4), showing that the rule in Eq. (2) is unsound.

Moreover, this rule does not allow to rewrite in the advantage upper-bound ε. Allowing such rewritings can be done, but it requires an additional check to ensure that the initial bound is no greater than 1 (for the same reason than the one given in Example 6):

$$\frac{\mathbb{E}; \Theta \vdash \vec{u} \sim_{\varepsilon_0} \vec{v} \qquad \mathbb{E}; \Theta \vdash [\varepsilon_0 = \varepsilon_1]_{\varepsilon_e} \qquad [\varepsilon_0 \leq 1]_0}{\mathbb{E}; \Theta \vdash \vec{u} \sim_{\varepsilon_1 + \varepsilon_e} \vec{w}}$$

We present our generalized global rewriting rules at the bottom of Fig. 10, which includes rewriting rules in several concrete security predicates of the logic. Rewriting rules for other predicates of the logic are similar, and are thus omitted. Remark that there is no approximated version of the rule that allows to rewrite in a length predicate, as this predicate does not allow for an error probability.

c) Indistinguishability Rules: We designed concrete security versions of the rules provided for asymptotic computational indistinguishability in [17]. We show a selected set of our rules in Fig. 1 (the full set is in Fig. 11 in appendix).

G$_\varepsilon$.E:TRANS

$$\frac{\mathbb{E}; \Theta \vdash \vec{u} \sim_{\varepsilon_0} \vec{w} \qquad \mathbb{E}; \Theta \vdash \vec{w} \sim_{\varepsilon_1} \vec{v}}{\mathbb{E}; \Theta \vdash \vec{u} \sim_{\varepsilon_0 + \varepsilon_1} \vec{v}}$$

G$_\varepsilon$.E:FA-BASE

$$\frac{\mathbb{E}; \Theta \vdash \vec{u}_l \sim_\varepsilon \vec{u}_r \qquad \mathbb{E}; \Theta \vdash \mathsf{adv}_{t_v}(v)}{\mathbb{E}; \Theta \vdash \vec{u}_l, v \sim_{\varepsilon'} \vec{u}_r, v}$$

where $\varepsilon' \overset{\text{def}}{=} \lambda t, \vec{o}.\, \varepsilon\ (t + t_v)\ \vec{o}$

$$\frac{\mathbb{E}; \Theta \vdash \vec{u}_l, f_l \sim_\varepsilon \vec{u}_r, f_r}{\mathbb{E}; \Theta \vdash \vec{u}_l, f_l, f_l \sim_{\varepsilon'} \vec{u}_r, f_r, f_r} \text{ G}_\varepsilon\text{.E:DUP-FUN}$$

where $\varepsilon' \overset{\text{def}}{=} \lambda t, \vec{o}, o_1, o_2.\, \varepsilon\ t\ \vec{o}\ (o_1 + o_2)$

$$\frac{\mathbb{E}; \Theta \vdash \vec{u}_l \sim_\varepsilon \vec{u}_r}{\mathbb{E}; \Theta \vdash \vec{u}_l, \mathsf{n_f} \sim_{\varepsilon'} \vec{u}_r, \mathsf{n_f}} \text{ G}_\varepsilon\text{.E:FA-NAMES}$$

where $\varepsilon' \overset{\text{def}}{=} \lambda t, \vec{o}, o_n.\, \varepsilon\ (t + o_n \cdot t_n)\ \vec{o}$

G$_\varepsilon$.E:CS

$$\frac{\mathbb{E}; \Theta \vdash \vec{u}_l, b_l, v_l \sim_{\varepsilon_1} \vec{u}_r, b_r, v_r \qquad \mathbb{E}; \Theta \vdash \vec{u}_l, b_l, w_l \sim_{\varepsilon_2} \vec{u}_r, b_r, w_r}{\mathbb{E}; \Theta \vdash \vec{u}_l, \text{if } b_l \text{ then } v_l \text{ else } w_l \sim_{\varepsilon_1 + \varepsilon_2} \vec{u}_r, \text{if } b_r \text{ then } v_r \text{ else } w_r}$$

In the rules above, v is an order-0 and f_l, f_r are order-1.
In G$_\varepsilon$.E:FA-NAMES, $\mathsf{n_f}$ only occurs in its declaration in $\mathbb{E}$, and t_n is an upper-bound on the time needed by $\mathsf{n_f}$ for a single sampling.

Figure 1. Selected concrete security rules for indistinguishability.

The G$_\varepsilon$.E:TRANS states that advantage bounds must be added in a transitive step, and G$_\varepsilon$.E:CS allows to perform a case study over the branching test of a conditional term, summing the advantage bounds of both branches. Remaining rules of Fig. 1 capture reduction-based arguments, and are more interesting as they require to carefully track bounds on running time, number of oracle calls, and error probabilities.

G$_\varepsilon$.E:FA-BASE allows to remove a term v (of order zero) appearing on both sides of an equivalence as long as v can be computed by the adversary. To understand this rule's advantage bound, let us consider an adversary $\mathcal{A}$ against the conclusion, running in time at most t and calling its oracles at most $\vec{o}$ times. By hypothesis, there exists a machine $\mathcal{M}$ computing v in time at most t_v. We can thus build an adversary $\mathcal{B}$ against the premise $\vec{u}_l \sim_\varepsilon \vec{u}_r$ by composing $\mathcal{M}$ with $\mathcal{A}$. This adversary runs in time $t + t_v$, and calls its oracle $\vec{o}$ times (as did $\mathcal{A}$). We conclude that $\mathcal{B}$'s advantage must be at most $\varepsilon\ (t + t_v)\ \vec{o}$.

The other reduction-based rules have similar features. The rule G$_\varepsilon$.E:DUP-FUN allows to get rid of a duplicated oracle, by having the total number of calls to this oracle be the sum of the number of calls to each of its copies. The rule G$_\varepsilon$.E:FA-NAMES removes a name $\mathsf{n_f}$ from an equivalence by letting the adversary sample it itself, at the cost of a time overhead $o_n \cdot t_n$ in the advantage bound, where o_n is the maximal number of adversary calls to the name oracle $\mathsf{n_f}$.

Example 7. *The bound on the case-study rule is tight, and cannot be improved. To see why this is the case, let us consider two Booleans b and b' representing two independent coin-flips (i.e. both have 50/50 chance to be true or false). Let us show* that:

$$\begin{aligned}&\textsf{if } b \textsf{ then } (\textsf{if } b \wedge b' \textsf{ then } \bot \textsf{ else } \top) \textsf{ else } \top\\ \sim\ &\textsf{if } b \textsf{ then } \top \textsf{ else } (\textsf{if } \neg b \wedge b' \textsf{ then } \bot \textsf{ else } \top)\end{aligned}$$

is valid using the case-study rule. After the application of the rule, we are left to prove:

$$\begin{aligned}&b, \textsf{if } \ b \wedge b' \textsf{ then } \bot \textsf{ else } \top \ \sim\ b, \top\\ \textit{and}\quad &b, \textsf{if } \neg b \wedge b' \textsf{ then } \bot \textsf{ else } \top \ \sim\ b, \top\end{aligned}$$

It is easy to check that both premises hold with an upper-bound of $\frac{1}{4}$, since the adversary with the best advantage is the one returning its second input unchanged. Summing both advantages yields a probability upper-bound of $\frac{1}{2}$, as does our rule.

d) Bi-deduction: To ease the proof transformations that we will presented in Section V, it is desirable to reduce the number of different rules while keeping the same expressive power. To that end, we designed a single rule, called G$_\varepsilon$.E:BI-DEDUCE, that captures many rules relying on reduction-based arguments of our proof-system. As the full bi-deduction rule is very technical, we only present a simplified version of the rule which is sufficient to show most of its key aspects. The full rule is described in Appendix B-B.

Let $\vec{u} \stackrel{\text{def}}{=} u_1, \dots, u_m$, $\vec{v} \stackrel{\text{def}}{=} v_1, \dots, v_m$ and $\vec{l} \stackrel{\text{def}}{=} l_1, \dots, l_m$ be three sequences of terms of the same length. Let $\mathbb{E}$ be an environment such that any declared symbol x in $\mathbb{E}$ is only used in eta-long form and is such that $\mathbb{E}; \Theta \vdash \mathsf{adv}_{+\infty}(x)$ is valid. Then the following rule is valid:

$$\text{G}_\varepsilon\text{.E:BI-DEDUCE}^s\ \frac{\mathbb{E};\Theta \vdash \vec{u} \sim_\varepsilon \vec{v} \qquad \mathbb{E};\Theta \vdash \mathsf{adv}_{t_c,\vec{o}_c}(C) \qquad \mathbb{E};\Theta \vdash \tilde{\bigwedge}_{i\leq n} \mathsf{blen}_{l_i}(u_i) \mathbin{\tilde{\wedge}} \mathsf{blen}_{l_i}(v_i)}{\mathbb{E};\Theta \vdash C\ \vec{u} \sim_{\varepsilon'} C\ \vec{v}}$$

where ε' must precisely account for the simulation times:

$$\varepsilon' \stackrel{\text{def}}{=} \begin{cases} \lambda t.\quad \varepsilon\left(t + \quad t_c\ \vec{l}\right)\left(\quad \vec{o}_c\right) & ((C\ \vec{u}) \text{ of order } 0)\\ \lambda t, o.\, \varepsilon\left(t + o \cdot t_c\ \vec{l}\right)\left(o \cdot \vec{o}_c\right) & ((C\ \vec{u}) \text{ of order } 1)\end{cases}$$

Recall that $C\ \ \vec{u}$ stand for $((t\ \ u_1) \dots u_n)$ when $\vec{u} = u_1, \dots, u_n$.

This rule subsumes the G$_\varepsilon$.E:FA-BASE rule, and has a similar structure. It allows to remove a computable (by the adversary) context C from both side of an equivalence. Here, since C can be of order at most two ($\vec{u}$ and $\vec{v}$ contains terms of order 0 or 1), the predicate $\mathsf{adv}(C)$ take two subscripts arguments t and $\vec{o}_C$. The first argument is the computation time of C and in particular take the length of the terms in $\vec{u}$ and $\vec{v}$ as argument. Those length are bounded by the vector $\vec{l}$ and the premise on $\mathsf{blen}(\cdot)$. The second one takes into account the number of calls to the first-order terms in $\vec{u}$ and $\vec{v}$.

Example 8. *Consider name symbols* $\mathsf{k}, \mathsf{k}', \mathsf{r}, \mathsf{n}, \mathsf{n}'$ *of type* message, *representing independent samplings of length η. We show the following toy formula:*

$$\mathsf{enc}(0_{\mathsf{len}}\ \mathsf{n}, \mathsf{r}, \mathsf{pk}\ \mathsf{k}) \sim_{\varepsilon'} \mathsf{enc}(0_{\mathsf{len}}\ \mathsf{n}', \mathsf{r}, \mathsf{pk}\ \mathsf{k}').$$

First, the formula above can be rewritten without error into:

$$\begin{aligned}&(\lambda x, y, z.\ \mathsf{enc}(0_{\mathsf{len}}\ x, y, \mathsf{pk}\ z))\ \mathsf{n}\ \mathsf{r}\ \mathsf{k}\\ \sim_{\varepsilon'}\ &(\lambda x, y, z.\ \mathsf{enc}(0_{\mathsf{len}}\ x, y, \mathsf{pk}\ z))\ \mathsf{n}'\ \mathsf{r}\ \mathsf{k}'\end{aligned}$$

Let C be the context defined by:

$$C \stackrel{\text{def}}{=} \lambda x, y, z.\ \mathsf{enc}(0_{\mathsf{len}}\ x, y, \mathsf{pk}\ z)$$

Applying G$_\varepsilon$.E:BI-DEDUCE^s *leaves us with the main premise*

$$\mathsf{n}, \mathsf{r}, \mathsf{k} \sim_\varepsilon \mathsf{n}', \mathsf{r}, \mathsf{k}'.$$

and additional premises $\mathsf{adv}_{t_C}(C)$ (for some t_C to be determined), and $\mathsf{blen}_\eta(m)$ for m any of the previous names. The $\mathsf{blen}_\eta(m)$ premise can be easily proven under our assumptions on the size of names. For the $\mathsf{adv}_{t_C}(C)$ premise, assume that t_{enc}, t_0 and t_{pk} are upper-bounds on the computation times of the underlying functions, and also that l_0 and l_{pk} represent the lengths of the outputs of the functions. We can prove $\mathsf{adv}_{t_C}(C)$ with:

$$t_C \stackrel{\text{def}}{=} \lambda l_x, l_y, l_z.\ t_{\mathsf{enc}}(l_0\ l_x)\ l_y\ l_{\mathsf{pk}}\ l_z + t_0\ l_x + t_{\mathsf{pk}}\ l_z$$

(Here, since all of input terms of C are of order 0, $\vec{o}_C$ does not appear.) Finally, we obtain:

$$\varepsilon' \stackrel{\text{def}}{=} \lambda t.\ \varepsilon(t + t_C\ \eta\ \eta\ \eta).$$

The full bi-deduction rule (in Appendix B-B) generalizes the rule above in several ways: i) we provide additional fresh names to the contexts; ii) we allow for an arbitrary number of contexts instead of a single one. These two extensions make our bi-deduction rule general enough to subsume many reduction-based CCSA rules: e.g. adding names captures the G$_\varepsilon$.E:FA-NAMES rule capabilities, while having many contexts captures the duplication rules (such as G$_\varepsilon$.E:DUP-FUN).

C. Global Induction

The asymptotic logic of [17] only supports induction for a constant number of steps, which can be expressed using the following *asymptotic logic* induction rule:

$$\frac{\begin{array}{c}\mathbb{E};\Theta \vdash \mathsf{well\text{-}founded}_\tau(<) \wedge \mathsf{det}(<)\\ \mathbb{E};\Theta \vdash \tilde{\forall}(x:\tau).\,\mathsf{const}(x) \tilde{\Rightarrow}\\ (\tilde{\forall}(x_1:\tau).\,\mathsf{const}(x_1) \tilde{\Rightarrow} [x_1 < x]_{\mathsf{negl}} \tilde{\Rightarrow} F\{x \mapsto x_1\}) \tilde{\Rightarrow} F\end{array}}{\mathbb{E};\Theta \vdash \tilde{\forall}(x:\tau).\mathsf{const}(x) \tilde{\Rightarrow} F}$$

where $[\phi]_{\mathsf{negl}}$ holds iff the probability that ϕ does not hold is negligible, *i.e.* $\Pr_\rho([\![\neg\phi]\!]^{\eta;\rho}_{\mathbb{M}}) \in \mathsf{negl}(\eta)$, and $\mathsf{well\text{-}founded}_\tau(<)$ is a global formula stating that $([\![\tau]\!]^\eta_{\mathbb{M}}, [\![<]\!]^\eta_{\mathbb{M}})$ is well-founded for every η (see Appendix A for details).

Remark 2. *Actually, the asymptotic logic induction rule of [17] is not restricted to values x such that $\mathsf{const}(x)$ holds. This is a mistake, as the rule is unsound without this, as shown in the example below.*

Example 9. *Consider a model $\mathbb{M}$ such that type* nat *is interpreted as the set of natural numbers, and $<$ as the standard* *order over $\mathbb{N}$. For all $i \in \mathbb{N}$, we let $(X^i(\eta))_{\eta\in\mathbb{N}}$ be the η-indexed sequence of random variables over $\mathbb{N}$ defined by:*

$$X^i(\eta)(\rho) \stackrel{\text{def}}{=} \max(\eta - i, 0). \qquad \text{(for any } \rho \in \mathbb{T}_{\mathbb{M},\eta})$$

For every $i < j$, there exists a rank η_0 such that for every $\eta \geq \eta_0$, we have $X^i(\eta) > X^j(\eta)$ (e.g. $\eta_0 = j$). Thus:

$$\Pr_\rho\left(X^i(\eta)(\rho) > X^j(\eta)(\rho)\right) = 1. \qquad \text{(for } \eta \text{ large enough)}$$

Hence, the set of η-indexed sequence of random variables $\mathbb{RV}_{\mathbb{M}}(\mathsf{nat})$ ordered by: "X is smaller than Y" iff.:

$$\Pr_\rho\left(\llbracket\neg(x < y)\rrbracket^{\eta,\rho}_{\mathbb{M}[x\mapsto X, y\mapsto Y]}\right) \in \mathsf{negl}(\eta)$$

is not well-founded, even though $<$ is well-founded over $\mathbb{N}$.

a) Hybrid arguments: Actually, the issue shown above is a well-known pitfall of hybrid arguments, which are the way inductions are usually used in cryptographic proofs. Essentially, an hybrid argument is the specialization of the induction principle to the case where the property to be shown is of the form $\vec{u}(n) \sim \vec{u}(n+1)$. Informally, it says that:

$$\vec{u}(1) \sim \vec{u}(2) \sim \cdots \sim \vec{u}(n) \quad \text{implies} \quad \vec{u}(1) \sim \vec{u}(n).$$

In its asymptotic formulation, the above argument is sound if n is constant, or more generally if the bound $\varepsilon(\eta, i)$ on the advantage of any adversary against $\vec{u}(i) \sim \vec{u}(i+1)$ is *uniformly* bounded by a negligible function $\varepsilon'(\eta)$ — here, uniformly means independently from i. The counter-example shown in Example 9 shows a typical case of the issues arising when uniformity does not hold. (We refer the reader to [20] for a detailed discussion of uniformity and hybrid arguments.)

Since *asymptotic* CCSA logics do not provide explicit advantage bounds, they cannot capture the more expressive variant of the hybrid argument, and must restrict themselves to the constant case where the number of induction steps does not depend on the security parameter η. This limits the logics applicability: e.g., they can only be used to prove the security of a protocol for a constant number of sessions, instead of the stronger polynomial-level of security (this is exactly what happens in Example 3).

b) Concrete security induction: Our concrete logic does not suffer from such a restriction, as the advantages can be explicitly established during an induction proof. More precisely, our logic allows for the following global induction principle:

G_ε.INDUCTION

$$\frac{\mathbb{E};\Theta \vdash \mathsf{well\text{-}founded}_\tau(<) \qquad \mathbb{E};\Theta \vdash \tilde{\forall}(x:\tau).\,(\tilde{\forall}(x_1:\tau).\,[x_1 < x]_0 \tilde{\Rightarrow} F\{x \mapsto x_1\}) \tilde{\Rightarrow} F}{\mathbb{E};\Theta \vdash \tilde{\forall}(x:\tau).\,F}$$

Note that we require $[x_1 < x]_0$, avoiding the pitfall described in Example 9.

D. Freshness and Cryptographic Rules

A fourth class of rules deals with cryptographic assumptions and reasoning about probabilistic independence. We present here two examples of such rules.

A crucial tool for such rules are freshness conditions, as defined in [17]. Intuitively, the formula $\phi^{n,v}_{\mathsf{fresh}}(\vec{u})$ is an approximation of the conditions under which the name $\mathsf{n}\ v$ can appear in the *generalized* subterms of $\vec{u}$, *i.e.* subterms considering the expansion of (recursive) definitions. If $\llbracket\phi^{\mathsf{n},v}_{\mathsf{fresh}}(\vec{u})\rrbracket^{\eta,\rho}_{\mathbb{M}}$ holds, then the term u can be computed without sampling the name n at index $\llbracket v\rrbracket^{\eta,\rho}_{\mathbb{M}}$. A full definition can be found in Appendix B-D.

The general idea of the fresh rule is that a name that is not used anywhere can be replaced by another one. In addition to adding explicit advantages, we generalize the rule from [17] to work under a context (to ease proof transformations):

G_ε.E:FRESH

$$\frac{\mathbb{E};\Theta \vdash \left[\phi^{\mathsf{n},i}_{\mathsf{fresh}}(\vec{u}, C\ (\mathsf{n_{fresh}}\ ())) \tilde{\vee}\ \phi^{\mathsf{n_{fresh}},i}_{\mathsf{fresh}}(\vec{u}, C\ (\mathsf{n_{fresh}}\ ()))\right]_{\varepsilon'} \qquad \mathbb{E};\Theta \vdash \vec{u}, C\ (\mathsf{n_{fresh}}\ ()) \sim_\varepsilon \vec{v}}{\mathbb{E};\Theta \vdash \vec{u}, C\ (\mathsf{n}\ i) \sim_{\varepsilon+\varepsilon'} \vec{v}}$$

The freshness premise ensures that $\mathsf{n}\ i$ and $\mathsf{n_{fresh}}\ ()$ are not sampled at the same time in any evaluation of C (with an error at most ε'). E.g., we can rewrite ($\mathsf{if}\ b\ \mathsf{then}\ \mathsf{n}\ i\ \mathsf{else}\ \mathsf{n}\ t$) into ($\mathsf{if}\ b\ \mathsf{then}\ \mathsf{n}\ i\ \mathsf{else}\ \mathsf{n_{fresh}}\ ()$) as, in this context, $\mathsf{n_{fresh}}$ is only sampled under condition $\neg b$, and $\mathsf{n}\ i$ is only sampled under condition b.

We present in Fig. 2 a simplified version of the rule for indistinguishability against chosen-ciphertext attack (CCA1), that states that an attacker cannot learn anything about the content of a ciphertext except its length. We model it by replacing the plaintext inside the ciphertext with the same length of zeros. The full version can be found in Fig. 12 with other cryptographic rules.

A key ingredient for this rule is the ability to simulate all relevant terms during the reduction for the soundness proof. This is done through the predicate $\vdash^{\mathsf{c}}_t$, which has a lot of similarity with the adv_t predicate since they both represent the ability of the adversary to compute something. However, in the $\vdash^{\mathsf{c}}_t$ predicate, the adversary can simulate the randomness of the protocol, while it cannot in the adv_t function. This predicate is an adaptation of the $\vdash_{\mathrm{pptm}}$ of [17] to the explicit advantage settings. Details can be found in Appendix B-C.

We also need some condition on key and randomness usage in the context. We reuse the conditions from [17]: intuitively, ϕ_{key} means that all needed terms can be computed without using the secret key except for decryption, while ϕ_{rand} ensures that the randomness used in the ciphertext is fresh, and ϕ_{dec} ensures that the context does not decrypt with the secret key. Formal definitions can be found in Appendix B-D.

This rule is a generalization of the rule in [17] since it allows to apply the CCA1 hypothesis under a context. Again, this will be important in our proof transformation result.

IV. Application to Private Authentication

In this section, we prove the unlinkability of the PA protocol with our proof system. We first describe an idiomatic CCSA proof, without specifying upper-bounds on advantages. Then we analyze these bounds and explain why the usage of case studies in proofs by induction yields advantage upper-bounds which are exponential in the number of inductive steps, failing

G_ε.CCA1^s

$$\frac{\mathbb{E};\Theta;\emptyset\vdash^{\mathsf{c}}_{\vec{t_0}} \vec{u},b,m,i_r,i_k \qquad \mathbb{E};\Theta;\emptyset\vdash^{\mathsf{c}}_{t_C} C \qquad \mathbb{E};\Theta\vdash \mathsf{det}(i_r)\,\tilde{\wedge}\,\mathsf{det}(i_k) \\ \mathbb{E};\Theta\vdash \mathsf{blen}_{l_e}\,(\mathsf{enc}\ m\ (\mathsf{r}\ i_r)\ (\mathsf{pk}(\mathsf{k}\ i_k)))\ \tilde{\wedge}\ \mathsf{blen}_{l_e}\,(\mathsf{enc}\ (0_{\mathsf{len}}(m))\ (\mathsf{r}\ i_r)\ (\mathsf{pk}(\mathsf{k}\ i_k))) \\ \mathbb{E};\Theta;\emptyset\vdash_{\varepsilon_\phi} \phi^{\mathsf{k},i_k}_{\mathsf{key}}(\vec{w},C)\wedge\phi^{\mathsf{r},i_r}_{\mathsf{rand}}(\vec{w},C)\wedge\phi^{\mathsf{k},i_k}_{\mathsf{dec}}(C) \qquad \mathbb{E};\Theta\vdash\vec{u},\mathsf{if}\ b\ \mathsf{then}\ C\ (\mathsf{enc}\ (0_{\mathsf{len}}(m))\ (\mathsf{r}\ i_r)\ (\mathsf{pk}(\mathsf{k}\ i_k)))\ \mathsf{else}\ u_e\sim_\varepsilon\vec{v}}{\mathbb{E};\Theta\vdash\vec{u},\mathsf{if}\ b\ \mathsf{then}\ C\ (\mathsf{enc}\ m\ (\mathsf{r}\ i_r)\ (\mathsf{pk}(\mathsf{k}\ i_k)))\ \mathsf{else}\ u_e\sim_{\varepsilon_f}\vec{v}}$$

where $\vec{v}$ is of order 0 and $\vec{w}\stackrel{\mathsf{def}}{=}\vec{u},b,m,i_r,i_k$ (note that u_e is *not* in $\vec{w}$) and $\varepsilon_f\stackrel{\mathsf{def}}{=}\lambda t,\vec{o}.\,\varepsilon\ t\ \vec{o}+\varepsilon_\phi+\varepsilon_{\mathsf{CCA}}(t+t_C\ l_{\mathsf{e}}+\vec{1}\cdot\vec{t_0}),\vec{1}\cdot\vec{w}=\sum_i w_i$ is the scalar product of $\vec{w}$ with the sequence $1,\ldots,1$ of the same length.

Figure 2. Simplified rule for the CCA1 cryptographic game.

to provide a polynomial level of security. Finally, we describe how our proof can be modified to fix this issue, hinting at the general result of the next section.

A. Idiomatic Proof by Case Study

Following up on Example 2, we are going to prove, in our concrete security logic, that PA is unlinkable for any deterministic number of sessions N that can be computed by the adversary in time $(t\ \mathsf{N})$. More precisely, we must derive

$$\mathbb{E};\Theta\vdash\tilde{\forall}t,\mathsf{N}.\,\mathsf{det}(\mathsf{N})\,\tilde{\Rightarrow}\,\mathsf{adv}_{t\ \mathsf{N}}(\mathsf{N})\,\tilde{\Rightarrow}\,F_{\mathsf{N}}$$

where $F_{\mathsf{N}}\stackrel{\mathsf{def}}{=}\mathsf{frame}\ \mathsf{N}\sim_{\varepsilon\ \mathsf{N}}\mathsf{frame}_{\mathsf{id}}\ \mathsf{N}$ and where $\mathsf{det}(t)$ is a new predicate of the logic that states that t is a deterministic value *that can depend on the security parameter* η (see Appendix A). The bound $\varepsilon\ \mathsf{N}$ will be described in the next subsection. In fact, all bounds are omitted for now.

Using an induction principle specialized on integers that only applies to deterministic variables N, it suffices to prove, after some minor book-keeping, that

$$\mathbb{E};\Theta,\mathsf{det}(0),\mathsf{adv}_{t\ 0}(0)\vdash F_0 \qquad\text{and}\qquad \mathbb{E}_0;\Theta_0\vdash F_{\mathsf{N}+1}$$

where $\mathbb{E}_0$ declares $\mathsf{N}:\mathsf{bint}$ and $\Theta_0\stackrel{\mathsf{def}}{=}\Theta,\mathsf{det}(\mathsf{N}),\mathsf{adv}_{t\ \mathsf{N}}(\mathsf{N}),F_{\mathsf{N}}$.

We focus on the proof of $F_{\mathsf{N}+1}$, which is the interesting case. From definition of frame and $\mathsf{frame}_{\mathsf{id}}$, and using bi-deduction (*i.e.* the G_ε.E:BI-DEDUCE^s rule) to remove the tupling function $\langle\cdot,\cdot\rangle$, we must show that:

$$\mathbb{E}_0;\Theta_0\vdash \begin{array}{l}\mathsf{frame}\ \ \mathsf{N},\mathsf{output}\ \ (\mathsf{choose}\ \ (\mathsf{N}+1),\mathsf{N}+1)\\ \sim\ \mathsf{frame}_{\mathsf{id}}\ \mathsf{N},\mathsf{output}_{\mathsf{id}}\ (\mathsf{choose}_{\mathsf{id}}\ (\mathsf{N}+1),\mathsf{N}+1)\end{array} \quad (5)$$

From now on, we omit $\mathbb{E}_0$ and Θ_0, as they remain unchanged throughout the rest of the proof. We assume that the adversary can only choose to interact with A or B, i.e. we use the modeling axiom:

$$\tilde{\forall}\mathsf{N}_0.\ [\mathsf{choose}\ \mathsf{N}_0=\mathsf{A}\vee\mathsf{choose}\ \mathsf{N}_0=\mathsf{B}]_0\,.$$

Using this axiom for $\mathsf{N}_0=\mathsf{N}+1$, and by rewriting (with no error) in the terms on the left of the equivalence in Eq. (5), we obtain the (left) terms:

$$\begin{array}{l}\mathsf{frame}\ \mathsf{N},\ \mathbf{if}\ \mathsf{choose}\ (\mathsf{N}+1)=\mathsf{A}\ \ \mathbf{then}\ \mathsf{output}\ (\mathsf{A},\mathsf{N}+1)\\ \qquad\qquad\qquad\qquad\qquad\qquad\quad\ \mathbf{else}\ \ \mathsf{output}\ (\mathsf{B},\mathsf{N}+1)\end{array}$$

We do the same on the terms on the right of $\sim$, which yields the same conditional term, except that it uses the idealized versions of frame, output, and choose.

Then, doing a case study with G_ε.E:CS on $\mathsf{b}\stackrel{\mathsf{def}}{=}(\mathsf{choose}\ (\mathsf{N}+1)=\mathsf{A})$ on the left and $\mathsf{b}_{\mathsf{id}}\stackrel{\mathsf{def}}{=}(\mathsf{choose}_{\mathsf{id}}\ (\mathsf{N}+1)=\mathsf{A})$ on the right, we get the two equivalences:

$$\begin{array}{l}\mathsf{frame}\ \ \ \mathsf{N},\mathsf{b},\ \ \mathsf{output}\ \ \ (\mathsf{A},\mathsf{N}+1)\\ \sim\ \mathsf{frame}_{\mathsf{id}}\ \mathsf{N},\mathsf{b}_{\mathsf{id}},\mathsf{output}_{\mathsf{id}}\ (\mathsf{A},\mathsf{N}+1)\end{array} \quad (\dagger\text{-A})$$

$$\begin{array}{l}\mathsf{frame}\ \ \ \mathsf{N},\mathsf{b},\ \ \mathsf{output}\ \ \ (\mathsf{B},\mathsf{N}+1)\\ \sim\ \mathsf{frame}_{\mathsf{id}}\ \mathsf{N},\mathsf{b}_{\mathsf{id}},\mathsf{output}_{\mathsf{id}}\ (\mathsf{B},\mathsf{N}+1)\end{array} \quad (\dagger\text{-B})$$

We focus on case ($\dagger$-A) (case ($\dagger$-B) is similar). By definition, choose $(\mathsf{N}+1)$ and $\mathsf{choose}_{\mathsf{id}}\ (\mathsf{N}+1)$ are equal to, resp.,

$$\mathsf{att}_{\mathsf{c}}(\mathsf{frame}\ \mathsf{N}) \qquad\text{and}\qquad \mathsf{att}_{\mathsf{c}}(\mathsf{frame}_{\mathsf{id}}\ \mathsf{N}).$$

Using bi-deduction to remove the computation $\lambda x,y.\,(x=\mathsf{att}_{\mathsf{c}}(y))$, and replacing the outputs by their definitions, we get:

$$\begin{array}{l}\mathsf{frame}\ \ \ \mathsf{N},\mathsf{enc}(\langle\,\mathsf{pk}_{\mathsf{A}},\qquad\qquad\ \mathsf{n}_{\mathsf{A}}\ (\mathsf{N}{+}1)\rangle,\mathsf{pk}_{\mathsf{B}},\mathsf{r}_{\mathsf{A}}\ (\mathsf{N}{+}1))\\ \sim\ \mathsf{frame}_{\mathsf{id}}\ \mathsf{N},\mathsf{enc}(\langle\,\mathsf{pk'}_{\mathsf{A}}\ (\mathsf{N}{+}1),\mathsf{n}_{\mathsf{A}}\ (\mathsf{N}{+}1)\rangle,\mathsf{pk}_{\mathsf{B}},\mathsf{r}_{\mathsf{A}}\ (\mathsf{N}{+}1))\end{array}$$

We apply the CCA1 rule twice, once per side, to zero-out the content of both encryptions using $0_{\mathsf{len}}(\cdot)$ — the verification of the premises that are not an indistinguishability predicate of this rule is not central, and we omit it. To prove the calculability premise, before applying the CCA1 rule, we apply rewriting without error, to change the definition of frame and frame_{id} to another one that use let in to be able to compute it in polynomial time. (and we reverse it after.) Thanks to some basic modeling assumptions on lengths, we then get that both plaintexts are of the same length u_{len}, which we assume to be a publicly known quantity (*i.e.* such that $\mathsf{adv}_{t_u}(u_{\mathsf{len}})$ holds for some efficient time t_u). Then, using bi-deduction and rewriting without error to remove the encryption computation, the zeroing function $0_{\mathsf{len}}(\cdot)$ and the publicly known length u_{len}, we get:

$$\mathsf{frame}\ \mathsf{N},\ \mathsf{pk}_{\mathsf{B}},\mathsf{r}_{\mathsf{A}}\ (\mathsf{N}{+}1)\sim\mathsf{frame}_{\mathsf{id}}\ \mathsf{N},\ \mathsf{pk}_{\mathsf{B}},\mathsf{r}_{\mathsf{A}}\ (\mathsf{N}{+}1).$$

The name $\mathsf{r}_{\mathsf{A}}\ (\mathsf{N}{+}1)$ is fresh in this context, as it is never sampled in frame N and $\mathsf{frame}_{\mathsf{id}}$ N, and thus can be sampled by the adversary itself. This reasoning can be captured using the freshness rules G_ε.E:FRESH and G_ε.E:FA-NAMES, which yields, after discharging some minor proof obligations:

$$\mathsf{frame}\ \mathsf{N},\ \mathsf{pk}_{\mathsf{B}}\sim\mathsf{frame}_{\mathsf{id}}\ \mathsf{N},\ \mathsf{pk}_{\mathsf{B}}$$

Observe that pk_{B} can be obtained by computation from the frame on both sides, as it is included in frame 0 and $\mathsf{frame}_{\mathsf{id}}$ 0.

Thus, by bi-deduction, it remains to prove that frame N $\sim$ frame_{id} N, which follows from the induction hypothesis F_{N}.

The proof of the branch (†-B) follows very similar steps, and also uses the CCA1 cryptographic rule exactly once.

B. Analysis of the Advantage Upper-Bound

We now analyze the advantage bound obtained from the previous proof. We are not interested in its precise expression, but seek to analyze how it grows with the number of sessions.

As this is a proof by induction, we need to find the recurrence relation between the advantages ε N and ε (N + 1) (the initial value ε 0 is of little interest here). Our proof of the inductive step is of the form described in the figure on the right, where $F^{\mathsf{A}}_{\mathsf{N}+1}$ and $F^{\mathsf{B}}_{\mathsf{N}+1}$ are, resp., the formulas in Eq. (†-A) and Eq. (†-B), and the branching comes from the case study on whether choose $=$ A or choose $=$ B.

$$\dfrac{\dfrac{\dfrac{F_{\mathsf{N}}}{F^{\mathsf{A}}_{\mathsf{N}+1}}\,\Pi_{\mathsf{A}} \qquad \dfrac{F_{\mathsf{N}}}{F^{\mathsf{B}}_{\mathsf{N}+1}}\,\Pi_{\mathsf{B}}}{F_{\mathsf{N}+1}}\,\Pi}{}$$

Figure 3. Shape of the proof of the inductive step for the PA protocol.

The advantage bounds are modified by the proof as follows, when *descending* from the induction hypothesis F_{N} to the conclusion $F_{\mathsf{N}+1}$:

- Both leaves start at advantage ε N.
- *Simple reduction-based* steps (e.g. bi-deductions) add a time overhead to the current advantage: roughly, the advantage $\lambda t.\, \varepsilon_0\ t$ in premise is changed into $\lambda t.\, \varepsilon_0\ (t{+}t_0)$, where t_0 is the time needed to evaluate the added computations.
- *Cryptographic* steps increase the advantage by the advantage in breaking the cryptographic assumption under consideration: e.g, here, the advantage is increased by $\varepsilon_{\mathsf{CCA}}(t{+}t_{\mathsf{CCA}})$, where t_{CCA} is a bound on the time needed to simulate the particular context used in our proof.
- *Logical* steps, such as rewriting without error or the logical reasoning rules, leave the advantage (mostly) unchanged.
- Last but not least, the case study rule $\mathrm{G}_{\varepsilon}.\mathrm{E{:}CS}$ *adds* the advantages of both premises.

Putting everything together, we get the relation:

$$\begin{aligned}\varepsilon(\mathsf{N}+1) = \lambda t. \quad & (\varepsilon\ \mathsf{N}\ (t+t_{\mathsf{A}}) + 2\ \varepsilon_{\mathsf{CCA}}\ (t+t^{\mathsf{A}}_{\mathsf{CCA}})) \\ +\ & (\varepsilon\ \mathsf{N}\ (t+t_{\mathsf{B}}) + 2\ \varepsilon_{\mathsf{CCA}}\ (t+t^{\mathsf{B}}_{\mathsf{CCA}}))\end{aligned} \tag{6}$$

where, very roughly, t_{A} is the sum of the time overheads in Π_{A} and Π, $t^{\mathsf{A}}_{\mathsf{CCA}}$ is the time needed to simulate the context when the CCA1 rule is applied (plus any time overhead added later); t_{B} and $t^{\mathsf{B}}_{\mathsf{CCA}}$ are similar, but for the right branch corresponding to the case choose $=$ B. The top quantity of Eq. (6) comes from the left branch of the proof in Fig. 3, while the bottom quantity comes from the right branch. Any advantage ε N satisfying the recurrence relation in Eq. (6) is exponential in N (as it must contain 2^{N} CCA1 advantages upper-bounds $\varepsilon_{\mathsf{CCA}}$).

To summarize, our idiomatic proof yields the parametric level of security that is today's standard with Squirrel: the advantage is negligible in η for any N that does not depend on η. However, it is not satisfying when N is polynomial in η, *i.e.* when the attacker can dynamically choose for how long it interacts with the protocol: in that case, the CCA1 advantage is multiplied by 2^{η}, canceling out assumption that this cryptographic advantage is negligible. To obtain a polynomial level of security, we need a proof with (in particular) an at-most polynomial factor for the CCA1 advantage.

C. Fixing the PA Proof

The crucial problem in our previous proof is the fact that the induction hypothesis is used twice. This stems from the fact that we use a case study to split the (†-A) and (†-B) cases. In order to fix this problem, we do away with the case study and apply the $\mathrm{G}_{\varepsilon}.\mathrm{CCA1}$ rule under the context.

Starting from the equivalence goal we have in the naive proof, between the terms

$$\begin{aligned}\text{frame N},\ \textbf{if}\ \text{choose (N + 1) = A}\ \ \textbf{then}\ \text{output (A, N + 1)}\\ \textbf{else}\ \text{output (B, N + 1)}\end{aligned}$$

and their idealized versions, we need to define contexts under which we can apply the $\mathrm{G}_{\varepsilon}.\mathrm{CCA1}$ rule.

Replacing the output by its definition, the $\mathrm{G}_{\varepsilon}.\mathrm{CCA1}$ rule is applied for the A side with the trivial context $C = (\lambda x.x)$, condition (b $=$ choose (N + 1) = A), ignored term (u_e $=$ output (B, N + 1)), and vector of outside terms frame N. We obtain the left side of the equivalence goal where the encryption in the A branch is zeroed out. We do the same transformation in the B branch, and on the right side of the equivalence. Finally, using some lengths reasoning and bi-deduction, we get the goal:

$$\begin{aligned}&\text{frame N},\ \ \text{choose (N + 1)}, \mathsf{pk_B}, \mathsf{pk_A}, \mathsf{r_A}\ (\text{N+1}), \mathsf{r_B}\ (\text{N+1})\\ \sim\ &\text{frame}_{\text{id}}\ \text{N}, \text{choose (N + 1)}, \mathsf{pk_B}, \mathsf{pk_A}, \mathsf{r_A}\ (\text{N+1}), \mathsf{r_B}\ (\text{N+1}).\end{aligned}$$

We conclude by remarking that choose (N + 1), $\mathsf{pk_B}$, $\mathsf{pk_A}$ can be computed from frame N and the fact that $\mathsf{r_A}$ (N+1), $\mathsf{r_B}$ (N+1) are not used in frame N and therefore are fresh sampling. We can now directly use the induction hypothesis exactly once.

Summing up the advantages of the proof, and taking t_{CCA} as an upper-bound of all time overheads in the different uses of the CCA rule, we get the relation:

$$\varepsilon(\mathsf{N}+1) = \lambda t.\ (\varepsilon\ \mathsf{N}\ (t+t'_{\mathsf{AB}}) + 4 \cdot \varepsilon_{\mathsf{CCA}}\ (t+t_{\mathsf{CCA}}))\,.$$

This relation is satisfied by an ε that uses a linear number (in N) of $\varepsilon_{\mathsf{CCA}}$ and with some polynomial time overheads in both N and η, and is thus negligible for N polynomial in η.

More generally, the technique we used in this proof, applying cryptographic rules under context rather than using case studies (*i.e.* commuting case studies and cryptographic rules) can be generalized to a general proof rewriting strategy applicable to most existing idiomatic proofs, as shown in the next section.

V. Proof Rewriting Strategy

We now present our proof transformation result, which can be used to improve the advantage bound of a large class of proofs, allowing to reach a polynomial level of security. Our result proceeds by rewriting the proof to be improved: i) we design a set of local proof transformations; ii) we design a proof transformation strategy that terminates on *admissible* proofs — a syntactic proof fragment defined below — and guarantees that normalized proofs only use their induction hypothesis once; and iii), we prove that if Π is an admissible proof that only features terms that can be computed in polynomial-time, and if Π only relies on cryptographic assumptions that hold with a negligible advantage, then a normalization of Π by our proof transformation strategy provides polynomial security.

Our proof transformation strategy operates on the proof of the inductive step of a proof of security of a protocol, and is based on two key ideas, exposed below.

i) Proof commutations: we move the applications of the case study rule G_ε.E:CS upward across the proof-tree using proof commutations. There are some rules that do not commute with G_ε.E:CS, most notably the bi-deduction rule G_ε.E:BI-DEDUCE: such rules also need to be moved upward, pushed by rising case study rules. This naturally separates our rules in two disjoint sets, ascending rules and descending rules, For each pair of ascending rule A and descending rule D, there must exists a proof commutation $\blacktriangleright_{\mathsf{AD}}$. An ideal commutation would look like the figure on the right. Of course, our commutations are almost never that simple, as the rules to commute can have several premises, and the proof transformation may need to introduce new rules when modifying the proof.

$$\dfrac{\dfrac{F_3}{F_2}\,\mathrm{D}}{F_1}\,\mathrm{A} \quad \blacktriangleright_{\mathsf{AD}} \quad \dfrac{\dfrac{F_3}{F_2'}\,\mathrm{A}}{F_1}\,\mathrm{D}$$

ii) Collapsing case-studies: once all ascending rules, and thus application of the case-study rule, are at the top of the proof-tree, we start a second round of proof transformations $\blacktriangleright_{\mathsf{col}}$, this time with the goal of *collapsing* applications of the case study rule. For example, a case study CS followed by an application of the bi-deduction B and induction I rules in both branches is an unnecessary detour, that can be replaced by a single application of a bi-deduction and induction hypothesis. We schematize this in the figure on the right, where $F_1 = F_1'$ up-to some errorless rewriting.

$$\dfrac{\dfrac{\dfrac{}{F}\,\mathrm{I}}{F_2}\,\mathrm{B} \qquad \dfrac{\dfrac{}{F}\,\mathrm{I}}{F_3}\,\mathrm{B}}{F_1}\,\mathrm{CS} \quad \blacktriangleright_{\mathsf{col}} \quad \dfrac{\dfrac{}{F}\,\mathrm{I}}{F_1'}\,\mathrm{B}$$

Figure 4. A case-study collapse.

A. The Proof Fragment of Admissible Proofs

We now define the proof fragment our result applies to. To that end, we first partition rules according to their behavior during the proof transformations. Then, we describe the restrictions defining the proof fragment of admissible proofs.

a) Rule partitioning: We partition our set of rules in three: *leaf rules* are the leaves of our proofs, *ascending rules* are the rules that will be pushed upwards by our proof transformations, while *descending rules* will be moved downwards.

We have four *leaf rules*: the reflexivity of equivalence G_ε.E:REFL, the application of an axiom G.AXIOM, and the trivial rules G.L-$\tilde{\bot}$ and G_ε.L-LOC:$\bot$. We have three *ascending rules*: the case study rule G_ε.E:CS, the bi-deduction rule G_ε.E:BI-DEDUCE and the hypothesis weakening rule G.WEAK. Finally, *descending rules* are any other rule of the logic that can have an equivalence in conclusion, at the exception of: induction G_ε.INDUCTION, transitivity G_ε.E:TRANS, rewriting with errors G_ε.E:REWRITE, the upper-bound weakening rules, the left disjunction rules for $\tilde{\vee}$ and $\vee$, and the G.ABSURD rule.

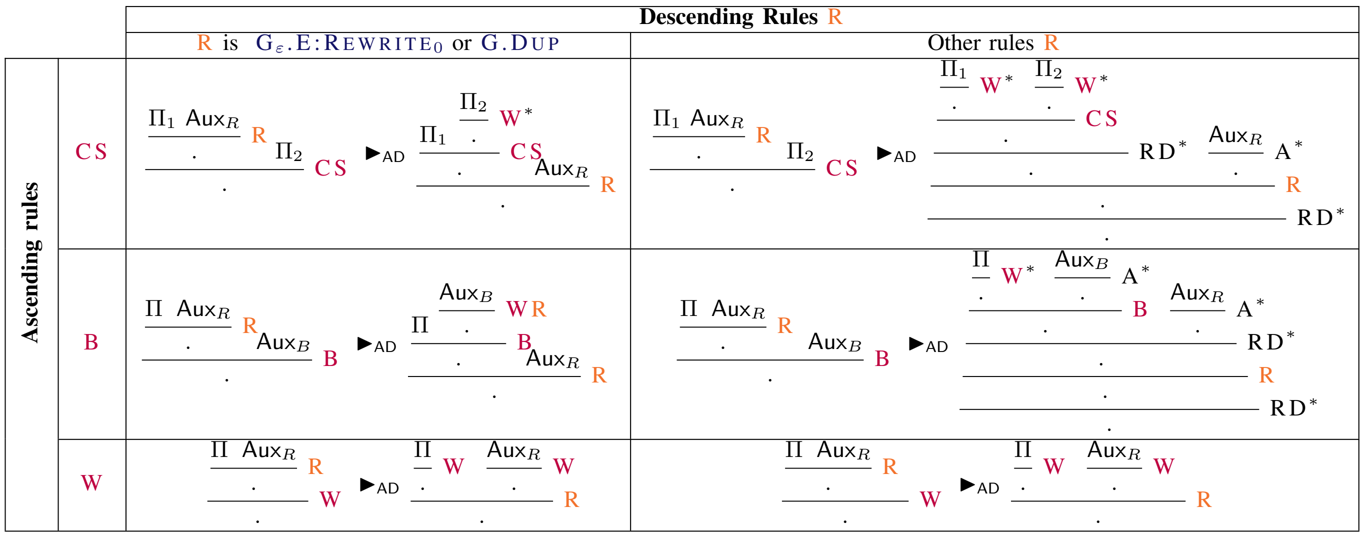
Moreover, all rules subsumed by the bi-deduction rule are excluded from consideration here, without loss of generality. We quickly discuss why we do not support some rules in our proof-transformation result, and the impact that removing these rules has, in Appendix C-B.

All ascending or descending rule (except G_ε.E:CS, G.CUT and G.L-$\tilde{\Rightarrow}$) have at most one indistinguishability premise, which we call the *principal premise* of the rule. The rest of the premises are the *auxiliary premises* of the rule. For the G.CUT and G.L-$\tilde{\Rightarrow}$ rules, the premise with the larger context is the principal one, the other premise is auxiliary. Finally, G_ε.E:CS is the only rule with two principal premises.

b) Admissible proofs: We present and justify the class of proofs to which our result applies using our running example. We can identify in our example proof in Section IV-A a proof structure which is standard in CCSA proofs (e.g. [15], [22], [23]). Looking at the proof of the induction step from the top to the bottom, we see that we start with the induction hypothesis $\mathsf{frame}\ \mathsf{N} \sim \mathsf{frame}_{\mathsf{id}}\ \mathsf{N}$ which is then iteratively augmented with additional elements (say, $\vec{u}_0$ on the left and $\vec{v}_0$ on the right) and surrounded by a computing context (say C), which yields intermediate equivalences of the form $C\ (\mathsf{frame}\ \mathsf{N})\ \vec{u}_0 \sim C\ (\mathsf{frame}_{\mathsf{id}}\ \mathsf{N})\ \vec{v}_0$. Then, the proof modifies the context C or the elements in $\vec{u}_0$ and $\vec{v}_0$, e.g. by rewriting, bi-deduction, application of cryptographic rules, and by merging distinct branches using the case study rule. The proofs ends when it reaches the target equivalence $\mathsf{frame}\ (\mathsf{N{+}1}) \sim \mathsf{frame}_{\mathsf{id}}\ (\mathsf{N{+}1})$.

Interestingly, We add the induction hypothesis $\mathsf{frame}\ \mathsf{N} \sim \mathsf{frame}_{\mathsf{id}}\ \mathsf{N}$ to ours hypothesis at the beginning of our proof and only use it at the end to close our induction. Further, we can observe that the case study over $\mathsf{choose} = \mathsf{A}$ in Section IV-A deals with a condition that can be computed by the adversary from the induction hypothesis terms $\mathsf{frame}\ \mathsf{N}$ and $\mathsf{frame}_{\mathsf{id}}\ \mathsf{N}$. Essentially, our proof fragment is the subset of proofs of this form. Roughly, we say that a proof is $(\vec{u};\vec{v})$-admissible if:

- it is only a single leaf rule with $\vec{u} \sim_\varepsilon \vec{v}$ (for some arbitrary term ε) or its root is a ascending or descending rule, and the principal premise of this rule is proven by an $(\vec{u};\vec{v})$-admissible proof.
- The application of the case study rule must only be done on a branching condition that can be computed (i.e. bi-deduced) from $\vec{u}$ in the left side of $\sim$, (respectively $\vec{v}$ in right side)
- All intermediate equivalences along the *main trunk* (i.e. the part of the proof-tree which only considers principal premises of rules, starting from the root) of the proof



Legend:

CS : G$_\varepsilon$.E:CS B : G$_\varepsilon$.E:BI-DEDUCE W : G.WEAK RD : G$_\varepsilon$.E:REWRITE$_0$ and G.DUP A : any rule

Convention: Ascending rules in purple. Auxiliary sub-proofs are denoted by Aux.

Figure 5. Shapes of the proof transformations commuting descending and ascending rules on the trunk of an admissible proof.

are of the form $\vec{u}, \vec{u}_0 \sim_\varepsilon \vec{v}, \vec{v}_0$ where $\vec{u}_0, \vec{v}_0$ and ε are arbitrary terms. Said otherwise, $\vec{u}$ and $\vec{v}$ are not modified in the main trunk.

The full definition of $(\vec{u}; \vec{v})$-admissibility is in Appendix C-A. A proof is said to be admissible if it is $(\vec{u}; \vec{v})$-admissible for some terms $(\vec{u}; \vec{v})$. Finally, an auxiliary sub-proof of an admissible proof Π is any proof anchored in auxiliary premises of the trunk of Π.

B. *Commuting Ascending and Descending Rules*

We design a set of proof transformations $\blacktriangleright_{\mathsf{AD}}$ which can be used to commute any pair of descending and ascending rules occurring in the main trunk of an admissible proof: if Π_1 is an admissible proof then $\Pi_1 \blacktriangleright_{\mathsf{AD}} \Pi_2$ if Π_2 can be obtained from Π_1 using one of our proof commutations applied on a rule on the trunk of Π_1. We can notice that in this case Π_2 is also an admissible proof since $\blacktriangleright_{\mathsf{AD}}$ preserve admissible proofs. The shapes of our transformation steps $\blacktriangleright_{\mathsf{AD}}$, omitting the formulas to improve readability, are shown in Fig. 5 (detailed transformations are given in Appendix E).

Lemma 1. *The relation $\blacktriangleright_{\mathsf{AD}}$ terminates on any admissible proof Π. Moreover, if Π is an admissible proof irreducible w.r.t. $\blacktriangleright_{\mathsf{AD}}$ then no ascending rule appears below a descending rule on the trunk of Π.*

We prove this by showing that admissibility is preserved by $\blacktriangleright_{\mathsf{AD}}$, and that some well-chosen numerical quantity $\mathsf{Value}_{\blacktriangleright_{\mathsf{AD}}}(\Pi)$ (see Fig. 13) strictly decreases after each proof transformation of the shape described in Fig. 5. See Appendix C-C for a proof sketch .

C. *Collapsing Proofs*

We consider a proof of the main inductive step of a larger proof with induction hypothesis $\vec{u} \sim \vec{v}$. W.l.o.g., we assume that $\vec{u} \neq \vec{v}$ (otherwise, the hypothesis is a triviality). Our goal is to reduce the number of applications of the induction hypothesis until there remains only one, through a sequence of proof transformation collapsing applications of the case-study rule.

A proof is $(\vec{u}, \vec{v})$-collapsible if it is $(\vec{u}; \vec{v})$-admissible and if G$_\varepsilon$.E:REWRITE$_0$ is the only descending rule appearing in its trunk. This represents the top of a normalized proof w.r.t. $\blacktriangleright_{\mathsf{AD}}$, where all descending rules have been moved down the proof-tree. We allow the (descending) rule G$_\varepsilon$.E:REWRITE$_0$ to appear in collapsible proofs as new occurrences of this rule may be added by collapse proof transformations.

We design a set of collapsing proof transformations $\blacktriangleright_{\mathsf{col}}$ that applies on the trunk of a collapsible proof, transforming it into another collapsible proof. For example, we show the shape of a key transformation for the case study rule in Fig. 4, which allows to merge two occurrences of the axiom rule above a case study into a single axiom rule. We refer the reader to Fig. 14 for an overview of the shapes of the $\blacktriangleright_{\mathsf{col}}$ transformations, and Appendix E for more details.

Lemma 2. *Let $\vec{u} \sim_\varepsilon \vec{v}$ be an equivalence predicate such that $\vec{u} \neq \vec{v}$. Let Π be an $(\vec{u}, \vec{v})$-collapsible proof where all occurrences of G.AXIOM in the trunk are on $\vec{u} \sim_\varepsilon \vec{v}$. Then, the rewrite relation $\blacktriangleright_{\mathsf{col}}$ terminates on Π and yields proofs with at most one application of this axiom rule in the trunk.*

See Appendix C-D for a proof sketch.

D. Polynomial security

We now seek to find conditions on proof by induction over natural numbers that make it possible to derive polynomial security from it. In essence, we will adapt the proof in order to obtain better advantage upper-bounds. This is done in the key lemma presented below, which relies on a specialized version of induction that we introduce first.

Consider the following induction rule specialized to integers:

$$\frac{\begin{array}{c}\mathbb{E}';\Theta, u\ n \sim_{\mathsf{x}_\varepsilon} v\ n \vdash \\ u\ n, u'\ (n+1) \sim_{\varepsilon_{ih}} v\ n, v'\ (n+1) \\ \mathbb{E};\Theta \vdash u_0 \sim_{\varepsilon_0} v_0\end{array}}{\mathbb{E};\Theta \vdash \tilde{\forall}(n:\mathsf{bint}).\, \mathsf{det}(n) \tilde{\Rightarrow} u\ n \sim_{\varepsilon\ n} v\ n}\ \mathbb{N}\text{-IND}$$

where $\mathbb{E}'$ declares x_ε and $n : \mathsf{bint}$. As for u, v and ε, they are defined by recurrence:

$$u\ 0 \stackrel{\mathsf{def}}{=} u_0 \quad v\ 0 \stackrel{\mathsf{def}}{=} v_0 \quad \varepsilon\ 0 \stackrel{\mathsf{def}}{=} \varepsilon_0$$

$$u\ (n+1) \stackrel{\mathsf{def}}{=} \langle u\ n, u'(n+1)\rangle \quad v\ (n+1) \stackrel{\mathsf{def}}{=} \langle v\ n, v'\ (n+1)\rangle$$

$$\varepsilon\ (n+1) \stackrel{\mathsf{def}}{=} \lambda t.\,(\varepsilon_{ih}\{\mathsf{x}_\varepsilon \mapsto \varepsilon\ n\})\ (t + t_{\langle\rangle}) \qquad (7)$$

and where the main inductive premise has already been simplified by removing the top-level pair in $u\ (n+1)$ and $v\ (n+1)$ (remark that we account for the time of simulating the pair computation in the advantage $\varepsilon\ n$, where $t_{\langle\rangle}$ must bound the time needed to compute each application of $\langle\rangle$).

Lemma 3. *Let Π be an $(u\ n; v\ n)$-admissible proof proving the inductive premise of the rule above where: the only occurrence of G.AXIOM in the trunk is on the induction hypothesis $u\ n \sim_{\varepsilon\ n} v\ n$; and where the induction hypothesis and x_ε are only used in the trunk.*

Then there exists Π_{poly} proving the inductive case of $\mathbb{N}$-IND with an improved upper-bound $\varepsilon^{\mathsf{negl}}_{ih}$, i.e. Π_{poly} proves:

$$\mathbb{E}';\Theta, u\ n \sim_{\mathsf{x}_\varepsilon} v\ n \vdash u\ n, u'\ (n+1) \sim_{\varepsilon^{\mathsf{negl}}_{ih}} v\ n, v'\ (n+1)$$

where $\varepsilon^{\mathsf{negl}}_{ih}$ is such that the final advantage $\varepsilon^{\mathsf{negl}}$, defined from $\varepsilon^{\mathsf{negl}}_{ih}$ as described in Eq. (7), is such that for any $\mathbb{M}$ where:

- *Π is in $\varepsilon/\mathsf{poly}^{\mathsf{x}_\varepsilon,n}_{\mathbb{M}}$, i.e. (roughly) the advantage terms (resp. time and length terms) appearing in all auxiliary sub-proofs of Π are negligible (resp. polynomial) in $\mathbb{M}$, for any number of session n and adversarial time t which are polynomial in η. See Appendix C-E for a formal definition of $\varepsilon/\mathsf{poly}^{\mathsf{x}_\varepsilon,n}_{\mathbb{M}}$.*
- *The initial advantage bound ε_0 and the cryptographic advantages $\varepsilon_{\mathit{CCA1}}$ and $\varepsilon_{\mathit{PRF}}$ must be negligible for adversaries running in time polynomial in η.*

Then the term $\varepsilon^{\mathsf{negl}}$ is a negligible term w.r.t. n and $\mathbb{M}$, i.e. for any polynomials $P_n, P_t \in \mathbb{N}[\eta]$ bounding, resp., the number of sessions and the execution time of the adversary:

$$\mathsf{E}_\rho(\llbracket \varepsilon^{\mathsf{negl}}\ n \rrbracket^{\eta,\rho}_{\mathbb{M}[n\mapsto P_n(\eta)]})(P_t(\eta)) \in \mathsf{negl}(\eta).$$

A proof sketch is given in Appendix C-F.

We can check that this result applies to the proof of Section IV-A establishing the main inductive step of the security of PA. This shows that PA provides a polynomial-level of security, though the initial proof did not.

VI. Conclusion

The CCSA approach has already been studied and extended in many directions, but always for asymptotic analyses and estimations. In this paper, we propose the first concrete logic for this approach, providing precise advantages bounds inside the proofs reasoning steps. Also, whereas it is of major interest in many papers to improve the tightness of the estimation of the adversary advantages, it is usually done in ad-hoc ways, and mainly for pen-and-paper proofs. To our knowledge, it is the first time that such precise advantages are managed in an automatic and generic way for the derivation of security proofs. As a future work, we plan to tackle the sizeable task of implementing our concrete security logic in Squirrel. Another line of future work could be to extend the class of admissible proofs, one possible extension is the proof with mutual inductions, that are out of scope for now.

References

[1] K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Pironti, and P. Strub, "Triple handshakes and cookie cutters: Breaking and fixing authentication over TLS," in *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2014, pp. 98–113.

[2] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. A. Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B. VanderSloot, E. Wustrow, S. Z. Béguelin, and P. Zimmermann, "Imperfect forward secrecy: how diffie-hellman fails in practice," *Commun. ACM*, vol. 62, no. 1, pp. 106–114, 2019.

[3] V. Shoup, "OAEP reconsidered," *J. Cryptol.*, vol. 15, no. 4, pp. 223–249, 2002.

[4] M. Barbosa, G. Barthe, C. Doczkal, J. Don, S. Fehr, B. Grégoire, Y. Huang, A. Hülsing, Y. Lee, and X. Wu, "Fixing and mechanizing the security proof of fiat-shamir with aborts and dilithium," in *CRYPTO (5)*, ser. Lecture Notes in Computer Science, vol. 14085. Springer, 2023, pp. 358–389.

[5] M. Barbosa, G. Barthe, K. Bhargavan, B. Blanchet, C. Cremers, K. Liao, and B. Parno, "Sok: Computer-aided cryptography," in *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 777–795.

[6] V. Shoup, "Sequences of games: a tool for taming complexity in security proofs," Cryptology ePrint Archive, Paper 2004/332, 2004, https://eprint.iacr.org/2004/332. [Online]. Available: https://eprint.iacr.org/2004/332

[7] M. Abadi and C. Fournet, "Private authentication," *Theor. Comput. Sci.*, vol. 322, no. 3, pp. 427–476, 2004.

[8] B. Blanchet, "A computationally sound mechanized prover for security protocols," in *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2006, pp. 140–154.

[9] G. Barthe, B. Grégoire, and S. Z. Béguelin, "Formal certification of code-based cryptographic proofs," in *POPL*. ACM, 2009, pp. 90–101.

[10] G. Barthe, B. Grégoire, S. Heraud, and S. Z. Béguelin, "Computer-aided security proofs for the working cryptographer," in *CRYPTO*, ser. Lecture Notes in Computer Science, vol. 6841. Springer, 2011, pp. 71–90.

[11] D. A. Basin, A. Lochbihler, and S. R. Sefidgar, "Crypthol: Game-based proofs in higher-order logic," *J. Cryptol.*, vol. 33, no. 2, pp. 494–566, 2020.

[12] C. Abate, P. G. Haselwarter, E. Rivas, A. V. Muylder, T. Winterhalter, C. Hritcu, K. Maillard, and B. Spitters, "Ssprove: A foundational framework for modular cryptographic proofs in coq," in *CSF*. IEEE, 2021, pp. 1–15.

[13] G. Bana and H. Comon-Lundh, "A computationally complete symbolic attacker for equivalence properties," in *CCS*. ACM, 2014, pp. 609–620.

[14] D. Baelde, S. Delaune, C. Jacomme, A. Koutsos, and S. Moreau, "An interactive prover for protocol verification in the computational model," in *SP*. IEEE, 2021, pp. 537–554.

[15] D. Baelde, S. Delaune, A. Koutsos, and S. Moreau, "Cracking the stateful nut: Computational proofs of stateful security protocols using the squirrel proof assistant," in *CSF*. IEEE, 2022, pp. 289–304.

[16] C. Cremers, C. Fontaine, and C. Jacomme, "A logic and an interactive prover for the computational post-quantum security of protocols," in *SP*. IEEE, 2022, pp. 125–141.

[17] D. Baelde, A. Koutsos, and J. Lallemand, "A higher-order indistinguishability logic for cryptographic reasoning," in *LICS*, 2023, pp. 1–13.
[18] M. Arapinis, L. I. Mancini, E. Ritter, and M. D. Ryan, "Analysis of privacy in mobile telephony systems," *Int. J. Inf. Sec.*, vol. 16, no. 5, pp. 491–523, 2017.
[19] M. Bellare, "Practice-oriented provable security," in *Lectures on Data Security*, ser. Lecture Notes in Computer Science, vol. 1561. Springer, 1998, pp. 1–15.
[20] M. Fischlin and A. Mittelbach, "An overview of the hybrid argument," *IACR Cryptol. ePrint Arch.*, p. 88, 2021.
[21] M. Bellare, A. Boldyreva, and S. Micali, "Public-key encryption in a multi-user setting: Security proofs and improvements," in *EUROCRYPT*, ser. Lecture Notes in Computer Science, vol. 1807. Springer, 2000, pp. 259–274.
[22] H. Comon and A. Koutsos, "Formal computational unlinkability proofs of RFID protocols," in *CSF*. IEEE Computer Society, 2017, pp. 100–114.
[23] A. Koutsos, "The 5G-AKA authentication protocol privacy," in *EuroS&P*. IEEE, 2019, pp. 464–479.

Appendix A
Semantics of Predicates

We give here the full definitions of the predicates decribed in Section II and in rules of Section III.

a) Bounded length: For u an order-1 term of type $\tau_0 \to \tau_1$, l a term of type $\overline{\mathsf{int}} \to \overline{\mathsf{int}}$, the predicate $\mathsf{blen}_l(u)$ holds if, for any η and $a \in [\![\tau_0]\!]^\eta_{\mathbb{M}}$ of length $n_a \in \mathbb{N}$, and for every $\rho \in \mathbb{T}_{\mathbb{M},\eta}$, we have $|\,[\![u]\!]^{\eta,\rho}_{\mathbb{M}}\,(a)| \leq \inf_\rho [\![l]\!]^{\eta,\rho}_{\mathbb{M}}\,(n_a)$. The definition extends naturally to order-1 terms with more than one argument.

b) Adversarial computability: Let u be a term of type $\vec{\tau}_1 \to \vec{\tau}_0 \to \tau$ with $\vec{\tau}_1$ are types of order 1, $\vec{\tau}_0$ and τ have order 1. Let t be a term of type $(\overline{\mathsf{int}} \to \overline{\mathsf{int}})^n \to \overline{\mathsf{int}}^m \to \overline{\mathsf{int}}$, and $\vec{o}$ of type $\overline{\mathsf{int}}^n$, with $n = |\vec{\tau}_1|$ and $m = |\vec{\tau}_0|$. The predicate $\mathsf{adv}_{t,\vec{o}}(u)$ holds if there exists a Turing machine $\mathcal{A}$ with n oracles and m inputs such that, for all

- $\eta \in \mathbb{N}$ and $\rho \in \mathbb{T}_{\mathbb{M},\eta}$,
- $\vec{f} \in [\![\vec{\tau}_1]\!]^{\eta,\rho}_{\mathbb{M}}$ and $\vec{l}$ such that $|f_i(x)| \leq l_i(|x|)$ for all i and x,
- $\vec{w} \in [\![\vec{\tau}_0]\!]^{\eta,\rho}_{\mathbb{M}}$ and $\vec{s}$ such that $w_i = |s_i|$ for all i,

we have:

$$\begin{aligned} [\![u]\!]^{\eta,\rho}_{\mathbb{M}}\,(\vec{f},\vec{w}) &= \mathcal{A}^{\vec{f}}(1^\eta,\vec{w},\rho_a) \\ \mathsf{time}_{\mathcal{A}}(1^\eta,\vec{w},\vec{f}) &\leq \inf_\rho \left[\!\!\left[t\,\vec{l}\,\vec{s}\right]\!\!\right]^{\eta,\rho}_{\mathbb{M}} \\ \mathsf{calls}^\eta_{\mathcal{A}} &\leq \inf_\rho [\![\vec{o}]\!]^{\eta,\rho}_{\mathbb{M}} \end{aligned}$$

c) Well-foundedness: Let τ be a type and $<_\tau$ be a symbol of type $\tau \to \tau \to \mathsf{bool}$. We let $\mathsf{well\text{-}founded}_\tau(<_\tau)$ be the following global formula, which checks if type τ, ordered by $<_\tau$, is well-founded :

$$\mathsf{well\text{-}founded}_\tau(<_\tau) \stackrel{\mathsf{def}}{=} [\forall(l : \mathsf{nat} \to \tau).\,\neg(\forall i, j.\, i < j \to l\ j <_\tau l\ i)]_0$$

where nat and $<: \mathsf{nat} \to \mathsf{nat} \to \mathsf{bool}$ are always interpreted as, resp., the set of natural numbers and the standard order over natural numbers.

Appendix B
Proof System

A. Permutation Rule

Let $u_l^1,\dots,u_l^n$ and $u_r^1,\dots,u_r^n$ be two sequences of terms of the same length, whose types are compatible. Let π be a permutation of $\{1,\dots,n\}$. Then we can permute terms in an equivalence formula with the permutation rule:

$$\textsc{G}_\varepsilon.\textsc{E:Perm}\ \frac{\mathbb{E};\Theta \vdash u_l^{\pi(1)},\dots,u_l^{\pi(n)} \sim_{\pi(\varepsilon)} u_r^{\pi(1)},\dots,u_r^{\pi(n)}}{\mathbb{E};\Theta \vdash u_l^1,\dots,u_l^n \sim_\varepsilon u_r^1,\dots,u_r^n},$$

where $\pi(\varepsilon)$ permutes oracle calls in ε according to π, and is defined by:

$$\pi(\varepsilon) \stackrel{\mathsf{def}}{=} \lambda t, o_1,\dots,o_r.\,\varepsilon\ t\ o_{\pi'(1)}\ \dots\ o_{\pi'(r)}$$

where, if we let r be the number of terms of order 1 in $u_l^1,\dots,u_l^n$, then π' is the permutation of $\{1,\dots,r\}$ defined by:

$$\pi'(i) \stackrel{\mathsf{def}}{=} \left|\left\{j \mid \pi(j) \leq \pi(i) \text{ and } \pi(u_l^j) \text{ is of order } 1\right\}\right|.$$

B. Bi-Deduction

The bi-deduction rule shown in Section III-B is a generalization of several reductionistic rules of our proof system. More precisely, this rule captures the Function Applications rules $\textsc{G}_\varepsilon$.E:FA-App, $\textsc{G}_\varepsilon$.E:FA-Fun and $\textsc{G}_\varepsilon$.E:FA-Base, as well as the weakening rule $\textsc{G}_\varepsilon$.E:Weak.

We now present our full bi-deduction rule, which generalizes the rule presented in the body of this paper in several ways:

- we provide additional fresh names to the contexts;
- we allow for an arbitrary number of contexts instead of a single context.

These two extensions make our bi-deduction rule general enough to subsume more standard CCSA rules: adding names captures the $\textsc{G}_\varepsilon$.E:FA-Names rule capabilities, while having many contexts captures the duplication rules $\textsc{G}_\varepsilon$.E:Dup-Base and Ge.Equiv:Dup-Fun , as well as $\textsc{G}_\varepsilon$.E:Perm. The rules subsumed by the generalized bi-deduction rule are clearly marked in Fig. 11.

a) Generalized bi-deduction: We now describe our first generalization of the bi-deduction rule. Let $\mathbb{E}$ be an environment such that any declared symbols x in $\mathbb{E}$ is only used in eta-long form and is such that $\mathbb{E};\Theta \vdash \mathsf{adv}_{+\infty}(x)$ is valid, and let Θ be a set of global hypotheses.

Let $\vec{u} \stackrel{\mathsf{def}}{=} u_1,\dots,u_m$ and $\vec{v} \stackrel{\mathsf{def}}{=} v_1,\dots,v_m$ be two sequences of terms of the same length such that, for every i, terms u_i and v_i have the same types. Let $\vec{l} \stackrel{\mathsf{def}}{=} l_1,\dots,l_m$ be a sequence of length terms for $\vec{u}$ and $\vec{v}$:

- we assume that the types of $\vec{l}$ are compatible with $\vec{u}$ and $\vec{v}$, *i.e.* l_i has type $\overline{\mathsf{int}}$ if u_i and v_i are of order 0, and has type $\overline{\mathsf{int}} \to \overline{\mathsf{int}}$ if u_i and v_i are of order 1;
- we will require $\mathsf{blen}_{l_i}(u_i) \,\tilde{\wedge}\, \mathsf{blen}_{l_i}(v_i)$ for every i.

Similarly, let $\vec{w}_0$ and $\vec{w}_1$ be two sequences of terms of the same length with compatible types, and let $\vec{l^{\mathsf{w}}}$ be a sequence of length terms for $\vec{w}_0$ and $\vec{w}_1$.

Let $C_1,\dots,C_n$ be sequences of terms representing the contexts that are to be simulated by the adversary. To account for the cost aspects of the rule, we consider, for every $i \leq n$:

- a term t_i representing the execution time of C_i;

- a sequence of terms $\vec{\sigma}_i$ representing the number of calls that C_i makes to its arguments of order 1.

We will require that $\mathsf{adv}_{t_i,\vec{\sigma}_i}(C_i)$ holds for every $i \leq n$, and that the terms $C_1, \ldots, C_n$ are *without names*.

Let $\vec{\mathsf{n}} \stackrel{\text{def}}{=} \mathsf{n}_1, \ldots, \mathsf{n}_p$ a sequence of names that are to be provided to $C_1, \ldots, C_n$. We require that:

- names in $\vec{\mathsf{n}}$ are fresh, i.e. we require that no name in $\vec{\mathsf{n}}$ appears in $\vec{w}_0, \vec{w}_1, \vec{u}, \vec{v}, C_1, \ldots, C_n$, and Θ;
- names in $\vec{\mathsf{n}}$ do not appear in $\mathbb{E}$, except in their declarations;
- we are provided, for every $i \leq p$, with a term t_j^{n} upper-bounding the time needed by n_j to do a single sampling in any model;
- we are given a sequence of length terms $\vec{l^{\mathsf{n}}} = l_1^{\mathsf{n}}, \ldots, l_p^{\mathsf{n}}$ for $\vec{\mathsf{n}}$, where we will require that $\mathsf{blen}_{l_i^{\mathsf{n}}}(\mathsf{n}_i)$ holds for every $i \leq p$.

We let $j_i, \ldots, j_q$ be such that

$$(C_{j_1}\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}}), \ldots, (C_{j_q}\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}})$$

is the sub-sequence, in the same order, of terms of order 1 in $(C_1\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}}), \ldots, (C_n\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}})$. Furthermore, for every context C_i, we decompose $\vec{\sigma}_i$ into $\vec{\sigma}_i^{\mathsf{a}}, \vec{\sigma}_i^{\mathsf{n}}$ where: $\vec{\sigma}_i^{\mathsf{a}}$ bounds the number of calls from C_i to each order-1 argument in $\vec{w}_0, \vec{u}$ (or $\vec{w}_1, \vec{v}$); $\vec{\sigma}_i^{\mathsf{n}}$ is of length p and bounds the number of calls from C_i to each name symbol in $\vec{n}$.

Then, we have the rule:

G$_\varepsilon$.E:BI-DEDUCE

$$\frac{\begin{array}{c}\mathbb{E};\Theta \vdash \vec{w}_0, \vec{u} \sim_\varepsilon \vec{w}_1, \vec{v} \qquad \mathbb{E};\Theta \vdash \tilde{\bigwedge}_{i \leq n} \mathsf{adv}_{t_i,\vec{\sigma}_i}(C_i) \\ \mathbb{E};\Theta \vdash \mathsf{blen}_{\vec{l^{\mathsf{w}}}}(\vec{w}_0)\ \tilde{\wedge}\ \mathsf{blen}_{\vec{l^{\mathsf{w}}}}(\vec{w}_1) \\ \mathbb{E};\Theta \vdash \mathsf{blen}_{\vec{l}}(\vec{u})\ \tilde{\wedge}\ \mathsf{blen}_{\vec{l}}(\vec{v}) \qquad \mathbb{E};\Theta \vdash \mathsf{blen}_{\vec{l^{\mathsf{n}}}}(\vec{\mathsf{n}})\end{array}}{\mathbb{E};\Theta \vdash \vec{w}_0, (C_1, \ldots, C_n)\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}} \sim_{\varepsilon'} \vec{w}_1, (C_1, \ldots, C_n)\ \vec{w}_1\ \vec{v}\ \vec{\mathsf{n}}}$$

where $(C_1, \ldots, C_n)\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}}$ denotes the sequence terms

$$C_1\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}}, \ldots, C_n\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}},$$

and ε' is the advantage bound term:

$$\lambda t, a_1, \ldots, a_q. \\ \varepsilon\left(t + t_{\mathsf{oracle}} + \sum_{i \leq n} \mathsf{cpt}_i \cdot t_i\ \vec{l^{\mathsf{w}}}\ \vec{l}\ \vec{l^{\mathsf{n}}}\right)\left(\sum_{i \leq n} \mathsf{cpt}_i \cdot \vec{\sigma}_i^{\mathsf{a}}\right) \quad (8)$$

where t_{oracle} is the time needed to compute all random samplings for names $\vec{n}$ defined by:

$$t_{\mathsf{oracle}} \stackrel{\text{def}}{=} \sum_{i \leq n, j \leq p} t_j^{\mathsf{n}} \cdot \vec{\sigma}_i^{\mathsf{n}}[j]$$

and where, for every $i \leq n$, the term cpt_i represents the number of times we need to simulate C_i, and is defined as:

$$\mathsf{cpt}_i \stackrel{\text{def}}{=} \begin{cases} 1 & \text{if } (C_i\ \vec{u}\ \vec{\mathsf{n}}) \text{ is of order } 0 \\ a_r & \text{if } (C_i\ \vec{u}\ \vec{\mathsf{n}}) \text{ is of order } 1, \text{ where } r \text{ is s.t. } j_r = i. \end{cases}$$

C. The Computability Predicate $\mathbb{E};\Theta;\vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t,\vec{\sigma}} u$

For u a term of order at most 2, the computability predicate $\mathbb{E};\Theta;\vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t,\vec{\sigma}} u$ represents the fact that $[\![u]\!]^{\eta,\rho}_{\mathbb{M}}$ can be simulated from $\vec{\mathsf{a}}$, in time t and calling its first order arguments at most $\vec{\sigma}$ times (where t and $\vec{\sigma}$ are well-type in $\mathbb{E}$). It is an extension of the $\vdash_{pptm}$ predicate from [17]. Practically this predicate is similar to $\mathsf{adv}_{t,\vec{\sigma}}(u)$ with two major differences:

- we allow for simulation of names, that is the distribution of the simulation should be equal to the distribution of $[\![u]\!]^{\eta,\rho}_{\mathbb{M}}$, as opposed to $\mathsf{adv}()$ where we require equality for every ρ;
- we fix the evaluation strategy for the simulation, i.e. the simulation evaluates u in a standard way, as opposed to $\mathsf{adv}()$ where we only require that a simulator exists.

In order to be able to provide a proof system that allows for simulating quantifiers, we need a new predicates. For any type τ of order 0, we consider an additional global predicate $\mathsf{enum}_\tau(t_{\mathsf{e}})$, which is satisfied in a model $\mathbb{M}$ iff. there exists a machine $\mathcal{M} \in \mathsf{PPTM}$ such that, for any η, $\mathcal{M}$ enumerates all elements of type τ in time at most $\inf_\rho([\![t_{\mathsf{e}}]\!]^{\eta,\rho}_{\mathbb{M}})$. By enumerating, we mean that there exists a particular working tape T of $\mathcal{M}$ such that, during an execution of $\mathcal{M}$, the tape T will successively contains all values of type τ, where $\mathcal{M}$ enters a special state each time it emits a value of type τ on tape T (and $\mathcal{M}$ enter this state only when it emits such a value).

We provide a proof system for $\mathbb{E};\Theta;\vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t,\vec{\sigma}} u$ in 6.

D. Generalized Subterms and Freshness Conditions

To recall the definition of the $\phi^{\mathsf{n}\ i}_{\mathsf{fresh}}(u)$ (This condition can be any formula that imply the freshness of $\mathsf{n}\ i$ in u, meaning that the sampling of $\mathsf{n}\ i$ isn't necessary to compute u), we first recall the notion of generalize subterms $\mathcal{ST}_{\mathbb{E}}(u)$ in Fig. 8, that represent all subterm v necessary to compute a given term u in a given environment $\mathbb{E}$ with the conditions ψ require to have to compute v and the variables $\vec{\alpha}$ bound in u that can be found in v. The formal definition of $\phi^{n,v}_{\mathsf{fresh}}(C(n\ v))$ is any well-typed formula in $\mathbb{E}$ such as for all model $\mathcal{M}$ of Θ, and for all $\eta \in \mathbb{N}, \rho \in \mathbb{T}_{\mathbb{M},\eta}$:

$$[\![\phi^{n,v}_{\mathsf{fresh}}(\vec{u})]\!]^{\eta,\rho}_{\mathbb{M}} = 1 \text{ implies} \\ [\![\forall\vec{\alpha}.\psi \implies v \neq v_0]\!]^{\eta,\rho}_{\mathbb{M}} = 1 \\ \text{for every } (\vec{\alpha}, \psi, n\ v_0) \in \mathcal{ST}_{\mathbb{E}}(\vec{u})$$

We recall the definition given for $\phi_{\mathsf{key}}()$ and $\phi_{\mathsf{rand}}()$ in [17], starting by some extra cases to add to the generalized subterms:

$$\mathcal{ST}^{\mathsf{cca}}_{\mathbb{E},k,i_k}(\mathsf{pk}(k\ i_0)) \stackrel{\text{def}}{=} \{(\varepsilon, \top, \mathsf{pk}(k\ i_0))\} \\ \cup \mathcal{ST}^{\mathsf{cca}}_{\mathbb{E},k,i_k}(i_0) \cup [i_0 \neq i_k]\mathcal{ST}^{\mathsf{cca}}_{\mathbb{E},k,i_k}(k\ i_0)$$

and

$$\mathcal{ST}^{\mathsf{cca}}_{\mathbb{E},k,i_k}(\mathsf{adec}\ u\ (k\ i_k)) \\ \stackrel{\text{def}}{=} \{(\varepsilon, \top, \mathsf{adec}\ u\ (k\ i_k)), (\varepsilon, \top, \mathsf{adec})\} \\ \cup \mathcal{ST}^{\mathsf{cca}}_{\mathbb{E},k,i_k}(u) \cup \mathcal{ST}^{\mathsf{cca}}_{\mathbb{E},k,i_k}(i_0) \cup [i_0 \neq i_k]\mathcal{ST}^{\mathsf{cca}}_{\mathbb{E},k,i_k}(k\ i_0)$$

Those represent the added capacity of the adversary given the oracles of the CCA1 game. And then, we can define $\phi_{\mathsf{key}}()$ and

In C.NAME, *and* t_n *and* l_n *are upper-bounds on, resp., the time needed by* n *for a single sampling, and the length of a single sampling.*

C.INPUT$_0$
$$\frac{\tau \text{ of order } 0}{\mathbb{E}; \Theta; \vec{\mathsf{a}}, (x : \tau :\!- l) \vdash^{\mathsf{c}}_{l} x :\!- l}$$

C.INPUT$_1$
$$\frac{\tau \text{ of order } 1}{\mathbb{E}; \Theta; \vec{\mathsf{a}}, (f : \tau :\!- l, 0) \vdash^{\mathsf{c}}_{0} f :\!- l}$$

C.LET
$$\frac{\Theta; \mathbb{E}, l_v : \overline{\mathsf{int}}; \vec{\mathsf{a}}, (x : \tau :\!- l_v) \vdash^{\mathsf{c}}_{t_u,\vec{o}_u} u :\!- l_u \qquad \mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t_v,\vec{o}_v} v :\!- l_v \qquad \tau \text{ of order } 0}{\mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t_u+t_v,\vec{o}_u+\vec{o}_v} \mathsf{let}\ (x : \tau) = v \ \mathsf{in}\ u :\!- l_u}$$

C.APP$_0$
$$\frac{\mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t_u,\vec{o}} u :\!- l_u \qquad \mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t_v} v :\!- l_v \qquad \mathbb{E}, \vec{\mathsf{a}} \vdash v : \tau \qquad \tau \text{ of order } 0 \qquad u \notin \vec{\mathsf{a}}}{\mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t_u\ l_v + t_v,\vec{o}} u\ v :\!- l_u\ l_v}$$

C.APP$_{1n}$
$$\frac{\mathbb{E}; \Theta; \vec{\mathsf{a}}, (u :\!- l_u, j) \vdash^{\mathsf{c}}_{t_v} v :\!- l_v \qquad \mathbb{E}, \vec{\mathsf{a}} \vdash v : \tau \qquad \tau \text{ of order } 0}{\mathbb{E}; \Theta; \vec{\mathsf{a}}, (u :\!- l_u, j+1) \vdash^{\mathsf{c}}_{t_u\ l_v + t_v} u\ v :\!- l_u\ l_v}$$

C.APP$_{21i}$
$$\frac{\mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t_u,(o_1,\dots,o_n)} u :\!- l_u \qquad \mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t_v} v :\!- l_v \qquad v \notin \vec{\mathsf{a}} \qquad \mathbb{E}, \vec{\mathsf{a}} \vdash v : \tau \qquad \tau \text{ of order } 1}{\mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t_u\ l_v + t_v,(o_2,\dots,o_n)} u\ v :\!- l_u\ l_v}$$

C.APP$_{21n}$
$$\frac{\mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t_u,(o_1,\dots,o_n)} u :\!- l_u \qquad \tau \text{ of order } 1}{\mathbb{E}; \Theta; \vec{\mathsf{a}}, (v : \tau :\!- l_v, o_1) \vdash^{\mathsf{c}}_{t_u\ l_v + t_v,(o_2,\dots,o_n)} u\ v :\!- l_u\ l_v}$$

C.NAME
$$\frac{\mathsf{n} \in \mathcal{N} \qquad \mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t} i :\!- l}{\mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t+t_n} \mathsf{n}\ i :\!- l_n}$$

C.ADV
$$\frac{\mathbb{E}; \Theta \vdash \mathsf{adv}_{t,\vec{o}}(u) \qquad \mathbb{E}; \Theta \vdash \mathsf{blen}_l(u)}{\mathbb{E}; \Theta; \emptyset \vdash^{\mathsf{c}}_{t,\vec{o}} u :\!- l}$$

C.QUANT$_0$
$$\frac{\mathcal{Q} \in \{\exists; \forall\} \qquad \tau \text{ of order } 0 \qquad \mathbb{E}; \Theta \vdash \mathsf{enum}_\tau(t_{\mathsf{e}}) \qquad \mathbb{E}; \Theta \vdash \tilde{\forall}(x : \tau).\, \mathsf{blen}_{l_\tau}(x) \qquad \mathbb{E}; \Theta; \vec{\mathsf{a}}, (x : \tau :\!- l_\tau) \vdash^{\mathsf{c}}_{t} \phi :\!- 1}{\mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t_{\mathsf{e}} + \sum_{x:\tau}(t + l_\tau)} \mathcal{Q}(x : \tau).\, \phi :\!- 1}$$

C.DEF:DELTA
$$\frac{(x : \tau = u) \in \mathbb{E} \qquad \mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t} u :\!- l}{\mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t} x :\!- l}$$

C.LAMBDA$_0$
$$\frac{\mathbb{E}, l_x : \overline{\mathsf{int}}; \Theta; \vec{\mathsf{a}}, (x : \tau :\!- l_x) \vdash^{\mathsf{c}}_{t,\vec{o}} u :\!- l \qquad \tau \text{ of order } 0}{\mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{\lambda l_x.\, t,\vec{o}} \lambda x.\, u :\!- \lambda l_x.\, l}$$

C.LAMBDA$_1$
$$\frac{\mathbb{E}, l_x : \overline{\mathsf{int}} \to \overline{\mathsf{int}}; \Theta; \vec{\mathsf{a}}, (x : \tau :\!- l_x, i) \vdash^{\mathsf{c}}_{t,\vec{o}} u :\!- l \qquad \tau \text{ of order } 1}{\mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{\lambda l_x.\, t,(i,\vec{o})} \lambda x.\, u :\!- \lambda l_x.\, l}$$

C.HYPSWEAK
$$\frac{\mathbb{E}_0 \text{ well-typed} \qquad \mathbb{E}_0 \vdash \Theta_0 \qquad \mathbb{E}_0 \vdash u : \tau \qquad \mathbb{E}_0; \Theta_0; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t,\vec{o}} u}{\mathbb{E}_0, \mathbb{E}_1; \Theta_0, \Theta_1; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t,\vec{o}} u}$$

C.INDUCTION
$$\frac{\mathbb{E} = \mathbb{E}_0, (f : \mathsf{bint} \to \tau = \lambda y.b) \qquad \tau \text{ of order } 0 \qquad \mathbb{E}_0, l_y : \overline{\mathsf{int}}; \Theta; \vec{\mathsf{a}}, (y :\!- l), (g :\!- l_f) \vdash^{\mathsf{c}}_{t} b\{f \mapsto g\} :\!- l_f\ l_y \qquad l_y \notin \mathsf{fv}(t) \qquad \mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t_u} u :\!- l_u \qquad \mathbb{E}; \Theta \vdash \mathsf{det}(u)}{\mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t_u + u \cdot t} f\ u :\!- l_f\ l_u}$$

Figure 6. Rules for the computability predicate $\mathbb{E}; \Theta; \vec{\mathsf{a}} \vdash^{\mathsf{c}}_{t} u$.

$\phi_{\mathsf{rand}}()$. For all model $\mathcal{M}$ of Θ, for all $\eta \in \mathbb{N}$ and $\rho \in \mathbb{T}_{\mathbb{M},\eta}$, we have that:

$$\text{if } \left[\!\left[\phi^{k,i}_{\mathsf{key}}(u)\right]\!\right]^{\eta,\rho}_{\mathbb{M}} = 1 \text{ then } \llbracket \forall \vec{\alpha}.\psi \implies i \neq i_0 \rrbracket^{\eta,\rho}_{\mathbb{M}} = 1 \text{ for all } (\vec{\alpha}, \psi, k\ i_0) \in \mathcal{ST}^{\mathsf{cca}}_{\mathbb{E},k,i}(u)$$

and

$$\text{if } \left[\!\left[\phi^{k,i}_{\mathsf{rand}}(u)\right]\!\right]^{\eta,\rho}_{\mathbb{M}} = 1 \text{ then } \llbracket \forall \vec{\alpha}.\psi \implies i \neq i_0 \rrbracket^{\eta,\rho}_{\mathbb{M}} = 1 \text{ for all } (\vec{\alpha}, \psi, r\ i_0) \in \mathcal{ST}^{\mathsf{cca}}_{\mathbb{E},k,i}(u).$$

Finally, the formula $\phi_{\mathsf{dec}}()$ is defined as follows:

$$\text{if } \left[\!\left[\phi^{k,i}_{\mathsf{dec}}(u)\right]\!\right]^{\eta,\rho}_{\mathbb{M}} = 1 \text{ then } \llbracket \forall \vec{\alpha}.\psi \implies i \neq i_0 \rrbracket^{\eta,\rho}_{\mathbb{M}} = 1 \text{ for all } (\vec{\alpha}, \psi, \mathsf{adec}\ u\ (k\ i_0)) \in \mathcal{ST}^{\mathsf{cca}}_{\mathbb{E},k,i}(u).$$

APPENDIX C
PROOF TRANSFORMATIONS

A. Admissible Proofs

a) Notation: For any b, $\vec{u} = u_1, \dots, u_n$ and $\vec{v} = v_1, \dots, v_n$, we let $\mathsf{if}\ b\ \mathsf{then}\ \vec{u}\ \mathsf{else}\ \vec{v}$ be the sequence of terms:

$$\mathsf{if}\ b\ \mathsf{then}\ u_1\ \mathsf{else}\ v_1, \dots, \mathsf{if}\ b\ \mathsf{then}\ u_n\ \mathsf{else}\ v_n$$

b) Restricting the case-study rule: We use a restricted version of the G$_\varepsilon$.E:CS rule that can only be used if the

Mixed judgements rules.

$$\textsc{L}_\varepsilon.\textsc{ByGlob}\ \frac{\mathbb{E};\Theta \vdash [\psi]_\varepsilon}{\mathbb{E};\Theta;\emptyset \vdash_\varepsilon \psi} \qquad \textsc{G}_\varepsilon.\textsc{ByLoc}\ \frac{\mathbb{E};\Theta;\emptyset \vdash_\varepsilon \psi}{\mathbb{E};\Theta \vdash [\psi]_\varepsilon} \qquad \textsc{L}_\varepsilon.\textsc{Localise}\ \frac{\mathbb{E};\Theta;\Gamma,\phi \vdash_{\varepsilon_0} \psi}{\mathbb{E};\Theta,[\phi]_{\varepsilon_1};\Gamma \vdash_{\varepsilon_0+\varepsilon_1} \psi}$$

$$\textsc{L}_\varepsilon.\textsc{Rewrite-Equiv}\ \frac{\mathbb{E};\Theta;\Gamma_1 \vdash_{\varepsilon_1} \psi_1 \qquad \mathbb{E};\Theta \vdash (\Gamma_0 \Rightarrow \psi_0) \sim_{\varepsilon_0} (\Gamma_1 \Rightarrow \psi_1)}{\mathbb{E};\Theta;\Gamma_0 \vdash_{\varepsilon_1+\varepsilon_0(1)} \psi_0}$$

Figure 7. Mixed judgements rules.

$$\begin{aligned}
\mathcal{ST}_{\mathbb{E}}(x) &\stackrel{\text{def}}{=} \{(\varepsilon,\top,x)\} && \text{(when } (x:\tau)\in\mathbb{E} \text{ or } x\notin\mathbb{E})\\
\mathcal{ST}_{\mathbb{E}}(x) &\stackrel{\text{def}}{=} \mathcal{ST}_{\mathbb{E}}(u) && \text{(when } (x:\tau=u)\in\mathbb{E})\\
\mathcal{ST}_{\mathbb{E}}(u\ u') &\stackrel{\text{def}}{=} \begin{cases}\mathcal{ST}_{\mathbb{E}}(u_0\{y\mapsto u'\}) & \text{(when } u\equiv x \text{ and } (x:\tau=\lambda y.u_0)\in\mathbb{E})\\ \{(\varepsilon,\top,(u\ u'))\}\cup\mathcal{ST}_{\mathbb{E}}(u)\cup\mathcal{ST}_{\mathbb{E}}(u') & \text{(otherwise)}\end{cases}\\
\mathcal{ST}_{\mathbb{E}}(\lambda(x:\tau).u) &\stackrel{\text{def}}{=} \{(\varepsilon,\top,\lambda(x:\tau).u)\}\cup(x:\tau).\mathcal{ST}_{\mathbb{E}}(u) && \text{(where } x \text{ is fresh)}\\
\mathcal{ST}_{\mathbb{E}}(\mathsf{if}\ \phi\ \mathsf{then}\ u_1\ \mathsf{else}\ u_0) &\stackrel{\text{def}}{=} \{(\varepsilon,\top,\mathsf{if}\ \phi\ \mathsf{then}\ u_1\ \mathsf{else}\ u_0)\}\cup\mathcal{ST}_{\mathbb{E}}(\phi)\cup[\phi]\mathcal{ST}_{\mathbb{E}}(u_1)\cup[\neg\phi]\mathcal{ST}_{\mathbb{E}}(u_0)\\
\mathcal{ST}_{\mathbb{E}}(\mathsf{let}\ (x:\tau)=u_0\ \mathsf{in}\ u_1) &\stackrel{\text{def}}{=} \{(\varepsilon,\top,\mathsf{let}\ (x:\tau)=u_0\ \mathsf{in}\ u_1)\}\cup\mathcal{ST}_{\mathbb{E}}(u_0)\cup(x:\tau).[x=u_0]\mathcal{ST}_{\mathbb{E}}(u_1)
\end{aligned}$$

Where $[\phi]S \stackrel{\text{def}}{=} \{(\vec{\alpha},\psi\wedge\phi,u) \mid (\vec{\alpha},\psi,u)\in S\}$ and $(x:\tau).S \stackrel{\text{def}}{=} \{(\vec{\alpha},x:\tau),\psi,u \mid (\vec{\alpha},\psi,u)\in S\}$

Figure 8. Generalised subterms.

branching condition is bi-deducible from the unmodified part of the equivalence:

$$\textsc{G}_\varepsilon.\textsc{E:CS}_{\textsf{R}}\ \frac{\mathbb{E};\Theta\vdash\vec{u}_l,\vec{v}_l\sim_{\varepsilon_1}\vec{u}_r,\vec{v}_r \qquad \mathbb{E};\Theta\vdash\vec{u}_l,\vec{w}_l\sim_{\varepsilon_2}\vec{u}_r,\vec{w}_r \qquad \mathbb{E};\Theta\vdash\mathsf{adv}_{t,\vec{\sigma}}(C) \qquad \mathbb{E};\Theta\vdash\mathsf{blen}_{\vec{l}}(\vec{u}_l)\,\tilde{\wedge}\,\mathsf{blen}_{\vec{l}}(\vec{u}_r)}{\mathbb{E};\Theta\vdash \vec{u}_l,\mathsf{if}\ C\ \vec{u}_l\ \mathsf{then}\ \vec{v}_l\ \mathsf{else}\ \vec{w}_l \sim_{\varepsilon'} \vec{u}_r,\mathsf{if}\ C\ \vec{u}_r\ \mathsf{then}\ \vec{v}_r\ \mathsf{else}\ \vec{w}_r}$$

where C is a context without names and the bound ε' is:

$\varepsilon' \stackrel{\text{def}}{=} \lambda t,\vec{a}.\,\varepsilon_1\ (t+t_C\ \vec{l})\ (\vec{a}+\vec{\sigma})+\varepsilon_2\ (t+t_C\ \vec{l})\ (\vec{a}+\vec{\sigma})+1$

c) $(\vec{u};\vec{v})$-admissible proofs: Let $\vec{u}$ and $\vec{v}$ be two same-length sequence of terms with compatible types. We define the set of proofs that are $(\vec{u};\vec{v})$-admissible by induction:

- If
$$\frac{\Pi}{\mathbb{E};\Theta\vdash\vec{u},\vec{u}_0,\vec{u}_1\sim_\varepsilon\vec{v},\vec{v}_0,\vec{v}_1}$$
is $(\vec{u},\vec{u}_0;\vec{v},\vec{v}_0)$-admissible then it is also $(\vec{u};\vec{v})$-admissible.
- If L is a leaf rule then $\dfrac{}{\mathbb{E};\Theta\vdash\vec{u}\sim_\varepsilon\vec{v}}\,\textsf{L}$ is $(\vec{u};\vec{v})$-admissible.
- If $\dfrac{\Pi}{\mathbb{E};\Theta\vdash\vec{u},\vec{u}_0\sim_\varepsilon\vec{v},\vec{v}_0}$ is $(\vec{u};\vec{v})$-admissible then
$$\frac{\dfrac{\Pi}{\mathbb{E};\Theta\vdash\vec{u},\vec{u}_0\sim_\varepsilon\vec{v},\vec{v}_0} \qquad \dots}{\mathbb{E};\Theta\vdash \vec{u},(C_1,\dots,C_n)\ \vec{u}\ \vec{u}_0\ \vec{\mathsf{n}} \sim_{\varepsilon'} \vec{v},(C_1,\dots,C_n)\ \vec{v}\ \vec{v}_0\ \vec{\mathsf{n}}}\ \textsc{G}_\varepsilon.\textsc{E:Bi-Deduce}$$
is $(\vec{u};\vec{v})$-admissible. Note that the immutable components of the proof $\vec{u}$ and $\vec{v}$ must be exactly the part of the conclusion that is not touched by the bi-deduction rule.
- If $\dfrac{\Pi_0}{\mathbb{E};\Theta\vdash\vec{u},\vec{u}_0\sim_\varepsilon\vec{v},\vec{v}_0}$ and $\dfrac{\Pi_1}{\mathbb{E};\Theta\vdash\vec{u},\vec{u}_1\sim_\varepsilon\vec{v},\vec{v}_1}$ are $(\vec{u};\vec{v})$-admissible then the following application of the $\textsc{G}_\varepsilon.\textsc{E:CS}_{\textsf{R}}$ rule:
$$\frac{\dfrac{\Pi_0}{\mathbb{E};\Theta\vdash\vec{u},\vec{u}_0\sim_{\varepsilon_0}\vec{v},\vec{v}_0} \qquad \dfrac{\Pi_1}{\mathbb{E};\Theta\vdash\vec{u},\vec{u}_1\sim_{\varepsilon_1}\vec{v},\vec{v}_1} \qquad \dots}{\mathbb{E};\Theta\vdash \vec{u},\mathsf{if}\ C\ \vec{u}\ \mathsf{then}\ \vec{u}_0\ \mathsf{else}\ \vec{u}_1 \sim_{\varepsilon'} \vec{u},\mathsf{if}\ C\ \vec{v}\ \mathsf{then}\ \vec{v}_0\ \mathsf{else}\ \vec{v}_1}$$
is $(\vec{u};\vec{v})$-admissible, where C is a context without names. Note that the case-study branching conditions $C\ \vec{u}$ and $C\ \vec{v}$ must be fully computable from the immutable components $\vec{u}$ and $\vec{v}$.
- If $\dfrac{\Pi}{\mathbb{E};\Theta\vdash\vec{u},\vec{u}_0\sim_\varepsilon\vec{v},\vec{v}_0}$ is $(\vec{u};\vec{v})$-admissible then
$$\frac{\dfrac{\Pi}{\mathbb{E};\Theta\vdash\vec{u},\vec{u}_0\sim_\varepsilon\vec{v},\vec{v}_0} \qquad \vec{\Pi}_{\mathsf{Aux}}}{\mathbb{E};\Theta\vdash\vec{u},\vec{u}_1\sim_{\varepsilon'}\vec{v},\vec{v}_1}\ \textsf{R}$$
is $(\vec{u};\vec{v})$-admissible, where the auxiliary premises $\vec{\Pi}_{\mathsf{Aux}}$ of rule R (if there are any) are arbitrary proofs, and $\vec{u}_1$ and $\vec{v}_1$ are arbitrary terms (such that the derivation above is valid).

d) Positions, paths: We define the path to a position in a proof as the set of all prefix positions of this position. Given an admissible proof Π, we denote $\mathsf{Trunk}(\Pi)$ its trunk, $\mathsf{Aux}_{\mathsf{Proof}}(\Pi)$ the multi-set of the auxiliary proof of Π. Also, given a position $p\in\mathsf{Trunk}(\Pi)$, we let $\mathsf{Path}_\Pi(p)$ the path from the root of Π to position p, and $R_\Pi(p)$ the rule at position p.

B. Discussion: Rule Restrictions

We quickly discuss why we do not support some rules in our proof-transformation result, and the impact that removing these rules has.

We do not support the transitivity rule because of the completely new terms that appear in the premises, which cannot be linked to the terms in the conclusion. This prevent us from commuting this rule, notably with the bi-deduction rule, as we do not know how to establish the new auxiliary proof obligations appearing after commutation. Removing transitivity has a limited impact on expressivity, as rules that need it already incorporate a (single, controlled) transitivity step. For example, this is the case for cryptographic rules, and explains some differences in presentation between our $\mathrm{G}_{\varepsilon}.\mathrm{CCA1}$ rule and the CCA1 rule of [17].

We believe our result could have been extended to support the upper-bound weakening rules and the left disjunction rules could have been, but at the cost of a more complicated presentation.

C. Termination of $\blacktriangleright_{\mathsf{AD}}$

We now sketch the proof of Lemma 1.

Lemma 1. *The relation $\blacktriangleright_{\mathsf{AD}}$ terminates on any admissible proof Π. Moreover, if Π is an admissible proof irreducible w.r.t. $\blacktriangleright_{\mathsf{AD}}$ then no ascending rule appears below a descending rule on the trunk of Π.*

Proof sketch. Let Π be a transformable proof.

Given a position p in the trunk of Π, we define $\mathsf{HW}(p)$, $\mathsf{CB}(p)$, then $\mathsf{Value}_{\blacktriangleright_{\mathsf{AD}}}(\Pi)$ in Fig. 13. We can show that this value strictly decreases (for the lexicographic ordering) for any proof transformation in $\blacktriangleright_{\mathsf{AD}}$. Thus the proof-transformation relation $\blacktriangleright_{\mathsf{AD}}$ terminate.

Let Π_T a proof in normal form for $\blacktriangleright_{\mathsf{AD}}$. Assume by contradiction that there exists a position $p \in \mathsf{Trunk}(\Pi)$ at which a descending rule is applied, and such as there exists $q \in \mathsf{Path}_{\Pi}(p)$ such that the rule applied at q is ascending.

We can assume without lost of generality that q is the greatest strict prefix of p. To conclude, we observe that if q is the greatest strict prefix of p, then the proof transformation $\triangleright^{R_{\Pi}(q)}_{R_{\Pi}(p)}$ applies. Thus, Π is not in normal form. Contradiction. ☐

D. Termination of the Collapse Proof Transformations

We now sketch the proof of Lemma 2 which we omitted from the body.

Lemma 2. *Let $\vec{u} \sim_{\varepsilon} \vec{v}$ be an equivalence predicate such that $\vec{u} \neq \vec{v}$. Let Π be an $(\vec{u}, \vec{v})$-collapsible proof where all occurrences of $\mathrm{G.Axiom}$ in the trunk are on $\vec{u} \sim_{\varepsilon} \vec{v}$. Then, the rewrite relation $\blacktriangleright_{\mathsf{col}}$ terminates on Π and yields proofs with at most one application of this axiom rule in the trunk.*

Proof sketch. First, we can show that Π doesn't contain any $\mathrm{G}_{\varepsilon}.\mathrm{E{:}Refl}$ leaf in it trunk: indeed, if that happens, we can show that $\vec{u} = \vec{v}$ just by looking at all the cases of the rule before it.

We reuse the new numerical quantity $\mathsf{Count\text{-}CB}_{\Pi}(p)$ defined in Fig. 13. Then, we let:

$$A_{R_0}(\Pi) = \sum_{p \in \mathsf{Trunk}(\Pi)} \mathsf{Count\text{-}CB}_{\Pi}(p).$$

Notice that:

$$A_{R_0}(\Pi) = \sum_{p \in \mathsf{Trunk}(\Pi) \wedge R_{\Pi}(p) = \mathrm{G}_{\varepsilon}.\mathrm{E{:}Rewrite}_0} \mathsf{Count\text{-}CB}_{\Pi}(p)$$

since $\mathrm{G}_{\varepsilon}.\mathrm{E{:}Rewrite}_0$ is the only ascending rule allowed in a collaspable proof.

We define a new quantity $\mathsf{Count\text{-}HW}^{\mathsf{col}}_{\Pi}(p)$ similarly to $\mathsf{Count\text{-}HW}_{\Pi}(p)$ but for all rules that are not $\mathrm{G.Weak}$ instead of just the ascending rules.

Now, We can define the decreasing quantity for the $\blacktriangleright_{\mathsf{col}}$ w.r.t the lexicographic order, as such :

$$\left(\begin{array}{c} \left| \left\{ p \in \mathsf{Trunk}(\Pi) \mid R_{\Pi}(p) = \begin{array}{c} \mathrm{G}_{\varepsilon}.\mathrm{E{:}CS}_{\mathsf{R}} \\ \text{or} \\ \mathrm{G}_{\varepsilon}.\mathrm{E{:}Bi\text{-}Deduce} \end{array} \right\} \right| \\ , A_{R_0}(\Pi), \sum_{p \in \mathsf{Trunk}(\Pi)} \mathsf{Count\text{-}HW}^{\mathsf{col}}_{\Pi}(p), \\ \left| \{ p \in \mathsf{Trunk}(\Pi) \mid R_{\Pi}(p) = \mathrm{G.Weak} \} \right| \end{array} \right)$$

Finally, we analyze what are the possible shapes of proofs in normal form w.r.t $\blacktriangleright_{\mathsf{col}}$ by case study.

Indeed, we can notice that it cannot have any $\mathrm{G.Weak}$ since it has a transformation with every rule, and all the $\mathrm{G}_{\varepsilon}.\mathrm{E{:}Rewrite}_0$ are at the bottom since it have a commutation with every ascending rule. Therefore, it there is a $\mathrm{G}_{\varepsilon}.\mathrm{E{:}CS}$ Consider the higher such rule (meaning that it doesn't have any $\mathrm{G}_{\varepsilon}.\mathrm{E{:}CS}$ above it), then it cannot have $\mathrm{G.Axiom}$ above it since a proof obligation of $\mathrm{G}_{\varepsilon}.\mathrm{E{:}CS}$ cannot be $\vec{u} \sim \vec{v}$ directly. And it cannot have any other leaf as one of it proofs since it can be transformed. Therefore, both rule directly above the $\mathrm{G}_{\varepsilon}.\mathrm{E{:}CS}$ is a $\mathrm{G}_{\varepsilon}.\mathrm{E{:}Bi\text{-}Deduce}$, which at it turn cannot have anything above it except a $\mathrm{G.Axiom}$ and therefore collapse. So, there is not any $\mathrm{G}_{\varepsilon}.\mathrm{E{:}CS}$ rule. As this is the only rule with two principal premises, there cannot remain more than one application of the axiom rule. ☐

E. Proof Fragment $\varepsilon/\mathsf{poly}^{\mathsf{x}_{\varepsilon},n}_{\mathbb{M}}$

a) Definition of negligibility for ε and of polynomial for t and l: We define a semantical notion of polynomial-time for the time, oracles calls and length annotations, and a notion of of negligibility for the upper-bound annotations. Note that it is given relatively to a formal variable N of type bint, used to interpret the number of inductive steps of the proof.

We say that a term ε is a *negligible term w.r.t. N in a model* $\mathbb{M}$, which we write $\mathsf{negl}^{N}_{\mathbb{M}}(\varepsilon)$, if one of the following case holds:

- ε is of type $\overline{\mathsf{real}}$ and for any $P \in \mathbb{N}[\eta]$,

$$\mathsf{E}_{\rho}(\llbracket \varepsilon \rrbracket^{\eta,\rho}_{\mathbb{M}[N \mapsto P(\eta)]}) \in \mathsf{negl}(\eta).$$

- ε is of type $\overline{\mathsf{int}}^l \rightarrow \overline{\mathsf{real}}$ and for any, $P \in \mathbb{N}[\eta], P_1, \ldots, P_l \in \mathbb{Z}[\eta]$

$$\mathsf{E}_\rho(\llbracket \varepsilon \rrbracket^{\eta,\rho}_{\mathbb{M}[N \mapsto P(\eta)]} (P_1(\eta), \ldots, P_l(\eta))) \in \mathsf{negl}(\eta).$$

We say that a term u is a *polynomial term w.r.t. N in a model* $\mathbb{M}$, which we write $\mathsf{poly}^N_{\mathbb{M}}(u)$, if one of the following case holds:

- u is of type $\overline{\mathsf{int}}$ and for any $P \in \mathbb{N}[\eta]$,

$$\sup_\rho (\llbracket u \rrbracket^{\eta,\rho}_{\mathbb{M}[N \mapsto P(\eta)]}) \in \mathbb{Z}[\eta].$$

- u is of type $\overline{\mathsf{int}}^l \rightarrow \overline{\mathsf{int}}$ and for any $P \in \mathbb{N}[\eta], P_1, \ldots, P_l \in \mathbb{Z}[\eta]$,

$$\sup_\rho \left(\llbracket u \rrbracket^{\eta,\rho}_{\mathbb{M}[N \mapsto P(\eta)]} (P_1(\eta), \ldots, P_l(\eta)) \right) \in \mathbb{Z}[\eta].$$

  Such a term is called an order one polynomial, and the set of such functions is noted $\mathbb{Z}_1[\eta]$.
- u is of type

$$(\overline{\mathsf{int}}^{k_i} \rightarrow \overline{\mathsf{int}})^m \rightarrow \overline{\mathsf{int}}^l \rightarrow \overline{\mathsf{int}}$$

  and for any

$$P \in \mathbb{N}[\eta] \qquad f_1, \ldots, f_m \in \mathbb{Z}_1[\eta]$$

$$P_{1,1}, \ldots, P_{1,k_1}, \ldots, P_{m,1}, \ldots, P_{m,k_m} \in \mathbb{Z}[\eta]$$

$$P_1 \ldots, P_l \in \mathbb{Z}[\eta],$$

  the following quantity is a polynomial in $\mathbb{Z}[\eta]$:

$$\sup_\rho \left(\llbracket u \rrbracket^{\eta,\rho}_{\mathbb{M}[N \mapsto P(\eta)]} \begin{pmatrix} f_1(P_{1,1}(\eta), \ldots, P_{1,k_1}), \\ \ldots, f_m(P_{m,1}(\eta), \ldots, P_{m,k_m}(\eta)), \\ P_1(\eta), \ldots, P_l(\eta) \end{pmatrix} \right)$$

b) Definition of $\varepsilon/\mathsf{poly}$ :: Let n be a variable of type bint. We say that a global formula F is *poly-secure compatible* w.r.t. n and a model $\mathbb{M}$ when all the advantages, time and length terms appearing in its predicates are polynomial or negligible (according to their type) w.r.t n and $\mathbb{M}$.

Similarly, a judgement is poly-secure compatible (w.r.t. n and $\mathbb{M}$) if its conclusion is poly-secure compatible. If we consider a local or a time judgement, we also require that the advantage or time term labeling the judgement are poly-secure compatible.

Let ε_{x} be variable of a type compatible with $\vec{u}; \vec{v}$, in the sense that $\vec{u} \sim_{\mathsf{x}_\varepsilon} \vec{v}$ is a well-typed predicate. We say that a proof Π which is $(\vec{u}; \vec{v})$-admissible proof is *ε-linear with polynomial overhead* w.r.t. x_ε, n and $\mathbb{M}$, which we write $\varepsilon/\mathsf{poly}^{\mathsf{x}_\varepsilon,n}_{\mathbb{M}}$, if all its auxiliary judgements are poly-secure compatible w.r.t. n and $\mathbb{M}$, and if the advantage at the conclusion of Π is of the form:

$$\lambda t, \vec{o}.\, \varepsilon_0 + \sum_i \mathsf{x}_\varepsilon \; (t + t_i) \; (\vec{o} + \vec{o}_i)$$

where t and $\vec{o}$ do not occur in t_i and $\vec{o}_i$ (for any i), and where x_ε does not occur in ε_0. The crucial point, here, is that the time over-heads t_i and the oracle calls overheads $\vec{o}_i$ *do not depend on the execution time of the adversary*, tough they can of course depends on the protocol. Without this, it would not be possible to bound the time in the full inductive proof by a polynomial.

Remark 3. *If Π is $\varepsilon/\mathsf{poly}^{\mathsf{x}_\varepsilon,n}_{\mathbb{M}}$, then any transformation of Π by the transformation relations $\blacktriangleright_{\mathsf{AD}}$ and $\blacktriangleright_{\mathsf{col}}$ is also $\varepsilon/\mathsf{poly}^{\mathsf{x}_\varepsilon,n}_{\mathbb{M}}$. This can be checked by a simple case analysis of all proof transformations.*

Proposition 1. *Let Π be a $(\vec{u}; \vec{v})$-admissible proof that only use* G.AXIOM *as its leafs in it trunk and only on one particular conclusion $u \sim_{\mathsf{x}_\varepsilon} v$, where x_ε is a variable.*

The advantage of its conclusion $\varepsilon_{\mathsf{final}}$ is of the form:

$$\varepsilon_{\mathsf{final}} = \lambda t, \vec{o}.\, \varepsilon_0 + \sum_{i=1}^{k} (\mathsf{x}_\varepsilon \; (t + t_i) \; (\vec{o} + \vec{o}_i)$$

where k is the number of G.AXIOM *in the trunk of Π.*

Furthermore, if $\mathbb{M}$ is such that Π is $\varepsilon/\mathsf{poly}^{\mathsf{x}_\varepsilon,n}_{\mathbb{M}}$ (for some n), then:

$$\forall i, \mathsf{poly}^n_{\mathbb{M}}(t_i) \wedge \mathsf{poly}^n_{\mathbb{M}}(\vec{o}_i)$$

where a vector is polynomial if each of its component is.

Finally, if $\mathbb{M}$ is a model such that $\mathsf{negl}^n_{\mathbb{M}}(\varepsilon_{\mathit{CCA1}})$ and $\mathsf{negl}^n_{\mathbb{M}}(\varepsilon_{\mathit{PRF}})$ holds, then $\mathsf{negl}^n_{\mathbb{M}}(\varepsilon_0)$ holds as well.

This can be proven by induction on the inductive definition of admissible proof, by case analysis over all possible rules involved

F. Obtaining a Polynomial Level of Security

We now recall and prove Lemma 3.

Lemma 3. *Let Π be an $(u\ n; v\ n)$-admissible proof proving the inductive premise of the rule above where: the only occurrence of* G.AXIOM *in the trunk is on the induction hypothesis $u\ n \sim_{\varepsilon\ n} v\ n$; and where the induction hypothesis and x_ε are only used in the trunk.*

Then there exists Π_{poly} proving the inductive case of $\mathbb{N}$-IND *with an improved upper-bound $\varepsilon^{\mathsf{negl}}_{ih}$, i.e. Π_{poly} proves:*

$$\mathbb{E}'; \Theta, u\ n \sim_{\mathsf{x}_\varepsilon} v\ n \vdash u\ n, u'\ (n+1) \sim_{\varepsilon^{\mathsf{negl}}_{ih}} v\ n, v'\ (n+1)$$

where $\varepsilon^{\mathsf{negl}}_{ih}$ is such that the final advantage $\varepsilon^{\mathsf{negl}}$, defined from $\varepsilon^{\mathsf{negl}}_{ih}$ as described in Eq. (7), is such that for any $\mathbb{M}$ where:

- *Π is in $\varepsilon/\mathsf{poly}^{\mathsf{x}_\varepsilon,n}_{\mathbb{M}}$, i.e. (roughly) the advantage terms (resp. time and length terms) appearing in all auxiliary sub-proofs of Π are negligible (resp. polynomial) in $\mathbb{M}$, for any number of session n and adversarial time t which are polynomial in η. See Appendix C-E for a formal definition of $\varepsilon/\mathsf{poly}^{\mathsf{x}_\varepsilon,n}_{\mathbb{M}}$.*
- *The initial advantage bound ε_0 and the cryptographic advantages $\varepsilon_{\mathit{CCA1}}$ and $\varepsilon_{\mathit{PRF}}$ must be negligible for adversaries running in time polynomial in η.*

Then the term $\varepsilon^{\mathsf{negl}}$ is a negligible term w.r.t. n and $\mathbb{M}$, i.e. for any polynomials $P_n, P_t \in \mathbb{N}[\eta]$ bounding, resp., the number of sessions and the execution time of the adversary:

$$\mathsf{E}_\rho(\llbracket \varepsilon^{\mathsf{negl}}\ n \rrbracket^{\eta,\rho}_{\mathbb{M}[n \mapsto P_n(\eta)]})(P_t(\eta)) \in \mathsf{negl}(\eta).$$

Proof sketch. Since Π is a $(u\ n; v\ n)$-admissible proof, we can rewrite it into another $(u\ n; v\ n)$-admissible proof that use the induction hypothesis only once in it trunk (we apply the transformation $\blacktriangleright_{\mathsf{AD}}$ until we have a normal form then we apply $\blacktriangleright_{\mathsf{col}}$ on the only $(u\ n, v\ n)$-collapse proof at the top of the tree (there is only one since all the descending rules have only one principal premise)).

Therefore, we now have a proof Π' such that:

- Π' is a $(u\ n; v\ n)$-admissible proof
- Π' is a $\varepsilon/\mathsf{poly}_{\mathbb{M}}^{\mathsf{x}_\varepsilon, n}$ (since it a transformation of a $\varepsilon/\mathsf{poly}_{\mathbb{M}}^{\mathsf{x}_\varepsilon, n}$ proof)
- G.AXIOM is the only leaf in the trunk of Π' and it only appear once.

By Proposition 1, we get that the upper-bound derived by Π' is of the form $\lambda t\vec{o}.\mathsf{x}_\varepsilon(t + t_n)(\vec{o} + \vec{o}_n) + \varepsilon_n$.

Finally, we take $\varepsilon_{\mathsf{poly}}$ to be

$$\lambda n.\,\mathsf{if}\ n = 0\ \mathsf{then}\ \varepsilon\ 0\ \mathsf{else}\ \lambda t\vec{o}.\varepsilon_{\mathsf{poly}}(t + t_n)(\vec{o} + \vec{o}_n) + \varepsilon_n$$

which is well-defined since all the terms in it are well-defined in Π' and it is well-founded. And it is negligable w.r.t n and $\mathbb{M}$ since Π' is $\varepsilon/\mathsf{poly}_{\mathbb{M}}^{\mathsf{x}_\varepsilon, n}$.

Therefore, we take the proof Π_{poly} to be Π' and ε by $\varepsilon_{\mathsf{poly}}$ to conclude the proof.

□

Local judgement: left local rules.

$$\frac{\mathbb{E};\Theta;\Gamma,\psi\{x\mapsto t\}\vdash_\varepsilon \phi \qquad \mathbb{E}\vdash t:\tau}{\mathbb{E};\Theta;\Gamma,\forall(x:\tau).\psi\vdash_\varepsilon \phi}\ \text{L}_\varepsilon.\text{L-}\forall
\qquad
\frac{\mathbb{E},x:\tau;\Theta;\Gamma,\psi\vdash_\varepsilon \phi}{\mathbb{E};\Theta;\Gamma,\exists(x:\tau).\psi\vdash_\varepsilon \phi}\ \text{L}_\varepsilon.\text{L-}\exists
\qquad
\frac{\mathbb{E};\Theta;\Gamma\vdash_{\varepsilon_0}\phi_0 \qquad \mathbb{E};\Theta;\Gamma,\phi_1\vdash_{\varepsilon_1}\psi}{\mathbb{E};\Theta;\Gamma,\phi_0\Rightarrow\phi_1\vdash_{\varepsilon_0+\varepsilon_1}\psi}\ \text{L}_\varepsilon.\text{L-}\Rightarrow$$

$$\frac{\mathbb{E};\Theta;\Gamma,\phi_0,\phi_1\vdash_\varepsilon\psi}{\mathbb{E};\Theta;\Gamma,\phi_0\wedge\phi_1\vdash_\varepsilon\psi}\ \text{L}_\varepsilon.\text{L-}\wedge
\qquad
\frac{\mathbb{E};\Theta;\Gamma,\phi_0\vdash_{\varepsilon_0}\psi \qquad \mathbb{E};\Theta;\Gamma,\phi_1\vdash_{\varepsilon_1}\psi}{\mathbb{E};\Theta;\Gamma,\phi_0\vee\phi_1\vdash_{\varepsilon_0+\varepsilon_1}\psi}\ \text{L}_\varepsilon.\text{L-}\vee
\qquad
\frac{}{\mathbb{E};\Theta;\Gamma,\bot\vdash_0\phi}\ \text{L}_\varepsilon.\text{L-}\bot$$

Local judgement: left global rules.

$$\frac{\mathbb{E};\Theta,F\{x\mapsto t\};\Gamma\vdash_\varepsilon\phi \qquad \mathbb{E}\vdash t:\tau}{\mathbb{E};\Theta,\tilde\forall(x:\tau).F;\Gamma\vdash_\varepsilon\phi}\ \text{L}_\varepsilon.\text{L-}\tilde\forall
\qquad
\frac{\mathbb{E},x:\tau;\Theta,F;\Gamma\vdash_\varepsilon\phi}{\mathbb{E};\Theta,\tilde\exists(x:\tau).F;\Gamma\vdash_\varepsilon\phi}\ \text{L}_\varepsilon.\text{L-}\tilde\exists
\qquad
\frac{\mathbb{E};\Theta\vdash F_0 \qquad \mathbb{E};\Theta,F_1;\Gamma\vdash_\varepsilon\psi}{\mathbb{E};\Theta,F_0\tilde\Rightarrow F_1;\Gamma\vdash_\varepsilon\psi}\ \text{L}_\varepsilon.\text{L-}\tilde\Rightarrow$$

$$\frac{\mathbb{E};\Theta,F_0,F_1;\Gamma\vdash_\varepsilon\psi}{\mathbb{E};\Theta,F_0\tilde\wedge F_1;\Gamma\vdash_\varepsilon\psi}\ \text{L}_\varepsilon.\text{L-}\tilde\wedge
\qquad
\frac{\mathbb{E};\Theta,F_0;\Gamma\vdash_{\varepsilon_0}\psi \qquad \mathbb{E};\Theta,F_1;\Gamma\vdash_{\varepsilon_1}\psi}{\mathbb{E};\Theta,F_0\tilde\vee F_1;\Gamma\vdash_{\varepsilon_0+\varepsilon_1}\psi}\ \text{L}_\varepsilon.\text{L-}\tilde\vee
\qquad
\frac{}{\mathbb{E};\Theta,\tilde\bot;\Gamma\vdash_0\phi}\ \text{L}_\varepsilon.\text{L-}\tilde\bot$$

Local judgement: right rules.

$$\frac{\mathbb{E},x:\tau;\Theta;\Gamma\vdash_\varepsilon\phi}{\mathbb{E};\Theta;\Gamma\vdash_\varepsilon\forall(x:\tau).\phi}\ \text{L}_\varepsilon.\text{R-}\forall
\qquad
\frac{\mathbb{E};\Theta;\Gamma\vdash_\varepsilon\phi\{x\mapsto t\} \qquad \mathbb{E}\vdash t:\tau}{\mathbb{E};\Theta;\Gamma\vdash_\varepsilon\exists(x:\tau).\phi}\ \text{L}_\varepsilon.\text{R-}\exists
\qquad
\frac{\mathbb{E};\Theta;\Gamma,\phi\vdash_\varepsilon\psi}{\mathbb{E};\Theta;\Gamma\vdash_\varepsilon\phi\Rightarrow\psi}\ \text{L}_\varepsilon.\text{R-}\Rightarrow
\qquad
\frac{\mathbb{E};\Theta;\Gamma\vdash_{\varepsilon_0}\phi \qquad \mathbb{E};\Theta;\Gamma\vdash_{\varepsilon_1}\psi}{\mathbb{E};\Theta;\Gamma\vdash_{\varepsilon_0+\varepsilon_1}\phi\wedge\psi}\ \text{L}_\varepsilon.\text{R-}\wedge$$

$$\frac{\mathbb{E};\Theta;\Gamma\vdash_\varepsilon\phi}{\mathbb{E};\Theta;\Gamma\vdash_\varepsilon\phi\vee\psi}\ \text{L}_\varepsilon.\text{R}_0\text{-}\vee
\qquad
\frac{\mathbb{E};\Theta;\Gamma\vdash_\varepsilon\psi}{\mathbb{E};\Theta;\Gamma\vdash_\varepsilon\phi\vee\psi}\ \text{L}_\varepsilon.\text{R1-}\vee
\qquad
\frac{}{\mathbb{E};\Theta;\Gamma\vdash_0\top}\ \text{L}_\varepsilon.\text{R-TRUE}$$

Local judgement: other rules.

$$\frac{\mathbb{E};\Theta;\Gamma\vdash_{\varepsilon_0}\phi\{s\} \qquad \mathbb{E};\Theta;\Gamma\vdash_{\varepsilon_1}s=t}{\mathbb{E};\Theta;\Gamma\vdash_{\varepsilon_0+\varepsilon_1}\phi\{t\}}\ \text{L}_\varepsilon.\text{REWRITE}
\qquad
\frac{}{\mathbb{E};\Theta;\Gamma,\phi\vdash_0\phi}\ \text{L}_\varepsilon.\text{AXIOM}
\qquad
\frac{\mathbb{E};\Theta;\Gamma,\psi\Rightarrow\bot\vdash_\varepsilon\bot}{\mathbb{E};\Theta;\Gamma\vdash_\varepsilon\psi}\ \text{L}_\varepsilon.\text{ABSURD}$$

$$\frac{\mathbb{E};\Theta;\Gamma\vdash_{\varepsilon_0}\phi \qquad \mathbb{E};\Theta;\Gamma,\phi\vdash_{\varepsilon_1}\psi}{\mathbb{E};\Theta;\Gamma\vdash_{\varepsilon_0+\varepsilon_1}\psi}\ \text{L}_\varepsilon.\text{CUT-LOC}
\qquad
\frac{\mathbb{E};\Theta\vdash F \qquad \mathbb{E};\Theta,F;\Gamma\vdash_\varepsilon\psi}{\mathbb{E};\Theta;\Gamma\vdash_\varepsilon\psi}\ \text{L}_\varepsilon.\text{CUT-GLOB}
\qquad
\frac{\mathbb{E};\Theta_0;\Gamma_0\vdash_\varepsilon\psi}{\mathbb{E};\Theta_0,\Theta_1;\Gamma_0,\Gamma_1\vdash_\varepsilon\psi}\ \text{L}_\varepsilon.\text{WEAK}$$

Local judgement: ε weakening rules.

$$\frac{\mathbb{E};\Theta;\Gamma\vdash_\varepsilon\psi \qquad \mathbb{E};\Theta;\emptyset\vdash_0\varepsilon\le\varepsilon'}{\mathbb{E};\Theta;\Gamma\vdash_{\varepsilon'}\psi}\ \text{L}_\varepsilon.\text{WEAK}_0
\qquad
\frac{\mathbb{E};\Theta;\Gamma\vdash_{\varepsilon+\varepsilon_0}\psi \qquad \mathbb{E};\Theta;\emptyset\vdash_{\varepsilon_l}\varepsilon_0\le\varepsilon_0' \qquad \mathbb{E};\Theta;\emptyset\vdash_0\varepsilon_0\le 1}{\mathbb{E};\Theta;\Gamma\vdash_{\varepsilon+\varepsilon_0'+\varepsilon_l}\psi}\ \text{L}_\varepsilon.\text{WEAK}_\varepsilon$$

Figure 9. Local judgement rules.

Global judgements: left rules.

$$\textsf{G.L-}\tilde{\forall}\quad \frac{\mathbb{E}; \Theta, F_0\{x \mapsto t\} \vdash F_1 \qquad \mathbb{E} \vdash t : \tau}{\mathbb{E}; \Theta, \tilde{\forall}(x : \tau).F_0 \vdash F_1}$$

$$\textsf{G.L-}\tilde{\exists}\quad \frac{\mathbb{E}, x : \tau; \Theta, F_0 \vdash F_1}{\mathbb{E}; \Theta, \tilde{\exists}(x : \tau).F_0 \vdash F_1}$$

$$\textsf{G.L-}\tilde{\Rightarrow}\quad \frac{\mathbb{E}; \Theta \vdash F_0 \qquad \mathbb{E}; \Theta, F_1 \vdash F}{\mathbb{E}; \Theta, F_0 \mathrel{\tilde{\Rightarrow}} F_1 \vdash F}$$

$$\textsf{G.L-}\tilde{\wedge}\quad \frac{\mathbb{E}; \Theta, F_0, F_1 \vdash F}{\mathbb{E}; \Theta, F_0 \mathrel{\tilde{\wedge}} F_1 \vdash F}$$

$$\textsf{G.L-}\tilde{\vee}\quad \frac{\mathbb{E}; \Theta, F_0 \vdash F \qquad \mathbb{E}; \Theta, F_1 \vdash F}{\mathbb{E}; \Theta, F_0 \mathrel{\tilde{\vee}} F_1 \vdash F}$$

$$\textsf{G.L-}\tilde{\bot}\quad \frac{}{\mathbb{E}; \Theta, \tilde{\bot} \vdash F}$$

Global judgements: right rules.

$$\textsf{G.R-}\tilde{\forall}\quad \frac{\mathbb{E}, x : \tau; \Theta \vdash F}{\mathbb{E}; \Theta \vdash \tilde{\forall}(x : \tau).F}$$

$$\textsf{G.R-}\tilde{\exists}\quad \frac{\mathbb{E}; \Theta \vdash F\{x \mapsto u\} \qquad \mathbb{E} \vdash u : \tau}{\mathbb{E}; \Theta \vdash \tilde{\exists}(x : \tau).F}$$

$$\textsf{G.R-}\tilde{\Rightarrow}\quad \frac{\mathbb{E}; \Theta, F_0 \vdash F_1}{\mathbb{E}; \Theta \vdash F_0 \mathrel{\tilde{\Rightarrow}} F_1}$$

$$\textsf{G.R-}\tilde{\wedge}\quad \frac{\mathbb{E}; \Theta \vdash F_0 \qquad \mathbb{E}; \Theta \vdash F_1}{\mathbb{E}; \Theta \vdash F_0 \mathrel{\tilde{\wedge}} F_1}$$

$$\textsf{G.R}_0\textsf{-}\tilde{\vee}\quad \frac{\mathbb{E}; \Theta \vdash F_0}{\mathbb{E}; \Theta \vdash F_0 \mathrel{\tilde{\vee}} F_1}$$

$$\textsf{G.R}_1\textsf{-}\tilde{\vee}\quad \frac{\mathbb{E}; \Theta \vdash F_1}{\mathbb{E}; \Theta \vdash F_0 \mathrel{\tilde{\vee}} F_1}$$

$$\textsf{G.R-}\tilde{\top}\quad \frac{}{\mathbb{E}; \Theta \vdash \tilde{\top}}$$

Global judgement: other rules.

$$\textsf{G.Axiom}\quad \frac{}{\mathbb{E}; \Theta, F \vdash F}$$

$$\textsf{G.Absurd}\quad \frac{\mathbb{E}; \Theta, F \mathrel{\tilde{\Rightarrow}} \tilde{\bot} \vdash \tilde{\bot}}{\mathbb{E}; \Theta \vdash F}$$

$$\textsf{G.Cut}\quad \frac{\mathbb{E}; \Theta \vdash F_1 \qquad \mathbb{E}; \Theta, F_1 \vdash F_0}{\mathbb{E}; \Theta \vdash F_0}$$

$$\textsf{G.Weak}\quad \frac{\mathbb{E}; \Theta_0 \vdash F}{\mathbb{E}; \Theta_0, \Theta_1 \vdash F}$$

$$\textsf{G.Dup}\quad \frac{\mathbb{E}; \Theta, F_0, F_0 \vdash F_1}{\mathbb{E}; \Theta, F_0 \vdash F_1}$$

Global judgement: local and global relations.

$$\textsf{G}_\varepsilon\textsf{.L-Loc:}\Rightarrow\quad \frac{\mathbb{E}; \Theta, [\phi]_0 \mathrel{\tilde{\Rightarrow}} [\psi]_\varepsilon \vdash F \qquad \mathbb{E}; \Theta \vdash \mathsf{const}(\phi)}{\mathbb{E}; \Theta, [\phi \Rightarrow \psi]_\varepsilon \vdash F}$$

$$\textsf{G}_\varepsilon\textsf{.L-Loc:}\vee\quad \frac{\mathbb{E}; \Theta, [\phi]_\varepsilon \vdash F \qquad \mathbb{E}; \Theta, [\psi]_\varepsilon \vdash F \qquad \mathbb{E}; \Theta \vdash \mathsf{const}(\phi) \mathrel{\tilde{\vee}} \mathsf{const}(\psi)}{\mathbb{E}; \Theta, [\phi \vee \psi]_\varepsilon \vdash F}$$

$$\textsf{G}_\varepsilon\textsf{.L-}\tilde{\forall}\textsf{-}\forall\quad \frac{\mathbb{E}; \Theta, \tilde{\forall}(x : \tau).\, [\psi]_\varepsilon \vdash F}{\mathbb{E}; \Theta, [\forall(x : \tau).\psi]_\varepsilon \vdash F}$$

$$\textsf{G}_\varepsilon\textsf{.L-}\forall\textsf{-}\tilde{\forall}\quad \frac{\mathbb{E}; \Theta, [\forall(x : \tau).\psi]_\varepsilon \vdash F}{\mathbb{E}; \Theta, \tilde{\forall}(x : \tau).\, [\psi]_\varepsilon \vdash F}$$

$$\textsf{G}_\varepsilon\textsf{.L-Loc:}\forall\quad \frac{\mathbb{E}; \Theta, [\psi\{x \mapsto u\}]_\varepsilon \vdash F \qquad \mathbb{E} \vdash u : \tau}{\mathbb{E}; \Theta, [\forall(x : \tau).\psi]_\varepsilon \vdash F}$$

$$\textsf{G}_\varepsilon\textsf{.L-Loc:}\wedge\quad \frac{\mathbb{E}; \Theta, [\psi]_\varepsilon, [\phi]_\varepsilon \vdash F}{\mathbb{E}; \Theta, [\psi \wedge \phi]_\varepsilon \vdash F}$$

$$\textsf{G}_\varepsilon\textsf{.L-Loc:}\bot\quad \frac{}{\mathbb{E}; \Theta, [\bot]_0 \vdash F}$$

Global judgement: ε weakening rules.
Weakening rules for other predicates of the logic are similar. We omit them here.

$$\textsf{G}_\varepsilon\textsf{.Reach:}\varepsilon\textsf{-Weak}_0\quad \frac{\mathbb{E}; \Theta \vdash [\psi]_\varepsilon \qquad \mathbb{E}; \Theta \vdash [\varepsilon \leq \varepsilon']_0}{\mathbb{E}; \Theta \vdash [\psi]_{\varepsilon'}}$$

$$\textsf{G}_\varepsilon\textsf{.Reach:}\varepsilon\textsf{-Weak}\quad \frac{\mathbb{E}; \Theta \vdash [\psi]_{\varepsilon+\varepsilon_0} \qquad \mathbb{E}; \Theta \vdash [\varepsilon_0 \leq \varepsilon'_0]_{\varepsilon_l} \qquad \mathbb{E}; \Theta \vdash [\varepsilon_0 \leq 1]_0}{\mathbb{E}; \Theta \vdash [\psi]_{\varepsilon+\varepsilon'_0+\varepsilon_l}}$$

$$\textsf{G}_\varepsilon\textsf{.E:}\varepsilon\textsf{-Weak}_0\quad \frac{\mathbb{E}; \Theta \vdash \vec{u} \sim_\varepsilon \vec{v} \qquad \mathbb{E}; \Theta \vdash [\varepsilon \leq \varepsilon']_0}{\mathbb{E}; \Theta \vdash \vec{u} \sim_{\varepsilon'} \vec{v}}$$

$$\textsf{G}_\varepsilon\textsf{.E:}\varepsilon\textsf{-Weak}\quad \frac{\mathbb{E}; \Theta \vdash \vec{u} \sim_{\varepsilon+\varepsilon_0} \vec{v} \qquad \mathbb{E}; \Theta \vdash [\varepsilon_0 \leq \varepsilon'_0]_{\varepsilon_l} \qquad \mathbb{E}; \Theta \vdash [\varepsilon_0 \leq 1]_0}{\mathbb{E}; \Theta \vdash \vec{u} \sim_{\varepsilon+\varepsilon'_0+\varepsilon_l} \vec{v}}$$

Global judgement: rewrite rules.
Rewriting rules for other predicates of the logic are similar. We omit them here.

$$\textsf{G}_\varepsilon\textsf{.E:Rewrite}_0\quad \frac{\mathbb{E}; \Theta \vdash \vec{u}\{s\} \sim_{\varepsilon\{s\}} \vec{v}\{s\} \qquad \mathbb{E}; \Theta \vdash [s = r]_0}{\mathbb{E}; \Theta \vdash \vec{u}\{r\} \sim_{\varepsilon\{r\}} \vec{v}\{r\}}$$

$$\textsf{G}_\varepsilon\textsf{.E:Rewrite}\quad \frac{\begin{array}{c}\mathbb{E}; \Theta \vdash \vec{u}\{s\} \sim_{\varepsilon_1\{s\}+\varepsilon_0} \vec{v}\{s\} \qquad \mathbb{E}; \Theta \vdash [s = r]_{\varepsilon_2} \\ \text{if } \{\} \in \mathsf{fv}(\varepsilon_1) \text{ then } \mathbb{E}; \Theta \vdash [\varepsilon_1\{s\} \leq 1]_0 \\ i \stackrel{\mathsf{def}}{=} (\mathbb{1}_{\{\} \in \mathsf{fv}(\vec{u})} + \mathbb{1}_{\{\} \in \mathsf{fv}(\vec{v})} + \mathbb{1}_{\{\} \in \mathsf{fv}(\varepsilon_1)})\end{array}}{\mathbb{E}; \Theta \vdash \vec{u}\{r\} \sim_{\varepsilon_1\{r\}+\varepsilon_0+i\cdot\varepsilon_2} \vec{v}\{r\}}$$

$$\textsf{G}_\varepsilon\textsf{.Reach:Rewrite}_0\quad \frac{\mathbb{E}; \Theta \vdash [\psi\{s\}]_{\varepsilon\{s\}} \qquad \mathbb{E}; \Theta \vdash [s = r]_0}{\mathbb{E}; \Theta \vdash [\psi\{r\}]_{\varepsilon\{r\}}}$$

$$\textsf{G}_\varepsilon\textsf{.Reach:Rewrite}\quad \frac{\begin{array}{c}\mathbb{E}; \Theta \vdash [\psi\{s\}]_{\varepsilon_1\{s\}+\varepsilon_0} \qquad \mathbb{E}; \Theta \vdash [s = r]_{\varepsilon_2} \\ \text{if } \{\} \in \mathsf{fv}(\varepsilon_1) \text{ then } \mathbb{E}; \Theta \vdash [\varepsilon_1\{s\} \leq 1]_0 \\ i \stackrel{\mathsf{def}}{=} (\mathbb{1}_{\{\} \in \mathsf{fv}(\psi)} + \mathbb{1}_{\{\} \in \mathsf{fv}(\varepsilon_1)})\end{array}}{\mathbb{E}; \Theta \vdash [\psi\{r\}]_{\varepsilon_1\{r\}+\varepsilon_0+i\cdot\varepsilon_2}}$$

$$\textsf{G}_\varepsilon\textsf{.Blen:Rewrite}_0\quad \frac{\mathbb{E}; \Theta \vdash \mathsf{blen}_{l\{s\}}(\vec{u}\{s\}) \qquad \mathbb{E}; \Theta \vdash [s = r]_0}{\mathbb{E}; \Theta \vdash \mathsf{blen}_{l\{s\}}(\vec{u}\{r\})}$$

Figure 10. Gobal judgement rules.

Equivalence relation rules.

G$_\varepsilon$.E:REFL
$$\frac{}{\mathbb{E};\Theta \vdash \vec{u} \sim_0 \vec{u}}$$

G$_\varepsilon$.E:SYM
$$\frac{\mathbb{E};\Theta \vdash \vec{u_l} \sim_\varepsilon \vec{u_r}}{\mathbb{E};\Theta \vdash \vec{u_r} \sim_\varepsilon \vec{u_l}}$$

G$_\varepsilon$.E:TRANS
$$\frac{\mathbb{E};\Theta \vdash \vec{u} \sim_{\varepsilon_0} \vec{w} \qquad \mathbb{E};\Theta \vdash \vec{w} \sim_{\varepsilon_1} \vec{v}}{\mathbb{E};\Theta \vdash \vec{u} \sim_{\varepsilon_0+\varepsilon_1} \vec{v}}$$

Structural rules included in the G$_\varepsilon$.E:BI-DEDUCE rule.

In all the rules below, v, v_l, v_r are order-0 terms and f, f_l, f_r are order-1 terms.
In G$_\varepsilon$.E:FA-NAMES, $\mathsf{n_f}$ only occurs in its declaration in $\mathbb{E}$, and t_n is an upper-bound on the time needed by $\mathsf{n_f}$ for a single sampling.

G$_\varepsilon$.E:FA-BASE
$$\frac{\mathbb{E};\Theta \vdash \vec{u}_l \sim_\varepsilon \vec{u}_r \qquad \mathbb{E};\Theta \vdash \mathsf{adv}_{t_v}(v)}{\mathbb{E};\Theta \vdash \vec{u}_l, v \sim_{\varepsilon'} \vec{u}_r, v}$$
where $\varepsilon' \stackrel{\mathsf{def}}{=} \lambda t, \vec{o}.\, \varepsilon\ (t + t_v)\ \vec{o}$

G$_\varepsilon$.E:FA-FUN
$$\frac{\mathbb{E};\Theta \vdash \vec{u}_l \sim_\varepsilon \vec{u}_r \qquad \mathbb{E};\Theta \vdash \mathsf{adv}_{t_f}(f)}{\mathbb{E};\Theta \vdash \vec{u}_l, f \sim_{\varepsilon'} \vec{u}_r, f}$$
where $\varepsilon' \stackrel{\mathsf{def}}{=} \lambda t, \vec{o}, o_f.\, \varepsilon\ (t + o_f \cdot (t + t_f(t)))\ \vec{o}$

G$_\varepsilon$.E:FA-APP
$$\frac{\mathbb{E};\Theta \vdash \vec{u}_l, f_l, v_l \sim_\varepsilon \vec{u}_r, f_r, v_r \qquad \mathbb{E};\Theta \vdash \mathsf{blen}_l(v_l) \mathbin{\tilde{\wedge}} \mathsf{blen}_l(v_r)}{\mathbb{E};\Theta \vdash \vec{u}_l, (f_l\ v_l) \sim_{\varepsilon'} \vec{u}_r, (f_r\ v_r)}$$
where $\varepsilon' \stackrel{\mathsf{def}}{=} \lambda t, \vec{o}.\, \varepsilon\ (t + l + 1)\ \vec{o}\, 1$

G$_\varepsilon$.E:FA-NAMES
$$\frac{\mathbb{E};\Theta \vdash \vec{u}_l \sim_\varepsilon \vec{u}_r}{\mathbb{E};\Theta \vdash \vec{u}_l, \mathsf{n_f} \sim_{\varepsilon'} \vec{u}_r, \mathsf{n_f}}$$
where $\varepsilon' \stackrel{\mathsf{def}}{=} \lambda t, \vec{o}, o_n.\, \varepsilon\ (t + o_n \cdot t_n)\ \vec{o}$

G$_\varepsilon$.E:DUP-BASE
$$\frac{\mathbb{E};\Theta \vdash \vec{u}_l, v_l \sim_\varepsilon \vec{u}_r, v_r}{\mathbb{E};\Theta \vdash \vec{u}_l, v_l, v_l \sim_\varepsilon \vec{u}_r, v_r, v_r}$$

G$_\varepsilon$.E:DUP-FUN
$$\frac{\mathbb{E};\Theta \vdash \vec{u}_l, f_l \sim_\varepsilon \vec{u}_r, f_r}{\mathbb{E};\Theta \vdash \vec{u}_l, f_l, f_l \sim_{\varepsilon'} \vec{u}_r, f_r, f_r}$$
where $\varepsilon' \stackrel{\mathsf{def}}{=} \lambda t, \vec{o}, o_1, o_2.\, \varepsilon\ t\ \vec{o}\ (o_1 + o_2)$

G$_\varepsilon$.E:WEAK
$$\frac{\mathbb{E};\Theta \vdash \vec{u_l}, v_l \sim_\varepsilon \vec{u_r}, v_r}{\mathbb{E};\Theta \vdash \vec{u_l} \sim_\varepsilon \vec{u_r}}$$

G$_\varepsilon$.E:PERM
$$\frac{\mathbb{E};\Theta \vdash u_l^{\pi(1)}, \ldots, u_l^{\pi(n)} \sim_{\pi(\varepsilon)} u_r^{\pi(1)}, \ldots, u_r^{\pi(n)}}{\mathbb{E};\Theta \vdash u_l^1, \ldots, u_l^n \sim_\varepsilon u_r^1, \ldots, u_r^n}$$
where π is a permutation of $\{1, \ldots, n\}$ and $\pi(\varepsilon)$ is defined in Appendix B-A

Reduction rules.

G.β
$$\frac{}{\mathbb{E};\Theta \vdash [(\lambda(x:\tau).t)\ t_1 = t\{x \mapsto t_1\}]_0}$$

G.δ
$$\frac{}{\mathbb{E}, x:\tau = t;\Theta \vdash [x = t]_0}$$

G.LET
$$\frac{}{\mathbb{E};\Theta \vdash [\mathsf{let}\ (x:v) = u\ \mathsf{in}\ = u\{x \mapsto v\}]_0}$$

Induction rules.

L$_\varepsilon$.INDUCTION
$$\frac{\mathbb{E};\Theta \vdash \mathsf{well\text{-}founded}_\tau(<) \qquad \mathbb{E};\Theta;\Gamma \vdash_\varepsilon \forall(x:\tau).(\forall(x_1:\tau).x_1 < x \Rightarrow \psi\{x \mapsto x_1\}) \Rightarrow \psi}{\mathbb{E};\Theta;\Gamma \vdash_\varepsilon \forall(x:\tau).\psi}$$

G$_\varepsilon$.INDUCTION
$$\frac{\mathbb{E};\Theta \vdash \mathsf{well\text{-}founded}_\tau(<) \qquad \mathbb{E};\Theta \vdash \tilde{\forall}(x:\tau).\,(\tilde{\forall}(x_1:\tau).\ [x_1 < x]_0 \mathrel{\tilde{\Rightarrow}} F\{x \mapsto x_1\}) \mathrel{\tilde{\Rightarrow}} F}{\mathbb{E};\Theta \vdash \tilde{\forall}(x:\tau).\,F}$$

Case-study and bi-deduction rules.

See Appendix B-B for a description of G$_\varepsilon$.E:BI-DEDUCE side-conditions, as well as the advantage bound ε'.

G$_\varepsilon$.E:CS
$$\frac{\mathbb{E};\Theta \vdash \vec{u}_l, b_l, v_l \sim_{\varepsilon_1} \vec{u}_r, b_r, \vec{v}_r \qquad \mathbb{E};\Theta \vdash \vec{u}_l, b_l, w_l \sim_{\varepsilon_2} \vec{u}_r, b_r, \vec{w}_r}{\mathbb{E};\Theta \vdash \vec{u}_l, \mathsf{if}\ b_l\ \mathsf{then}\ \vec{v}_l\ \mathsf{else}\ \vec{w}_l \sim_{\varepsilon_1+\varepsilon_2+1} \vec{u}_r, \mathsf{if}\ b_r\ \mathsf{then}\ \vec{v}_r\ \mathsf{else}\ \vec{w}_r}$$

G$_\varepsilon$.E:BI-DEDUCE
$$\frac{\mathbb{E};\Theta \vdash \vec{w}_0, \vec{u} \sim_\varepsilon \vec{w}_1, \vec{v} \qquad \mathbb{E};\Theta \vdash \tilde{\bigwedge}_{i \le n} \mathsf{adv}_{t_i,\vec{o}_i}(C_i) \qquad \mathbb{E};\Theta \vdash \mathsf{blen}_{\vec{l^w}}(\vec{w}_0) \mathbin{\tilde{\wedge}} \mathsf{blen}_{\vec{l^w}}(\vec{w}_1) \qquad \mathbb{E};\Theta \vdash \mathsf{blen}_{\vec{l}}(\vec{u}) \mathbin{\tilde{\wedge}} \mathsf{blen}_{\vec{l}}(\vec{v}) \qquad \mathbb{E};\Theta \vdash \mathsf{blen}_{\vec{l^n}}(\vec{\mathsf{n}})}{\mathbb{E};\Theta \vdash \vec{w}_0, (C_1, \ldots, C_n)\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}} \sim_{\varepsilon'} \vec{w}_1, (C_1, \ldots, C_n)\ \vec{w}_1\ \vec{v}\ \vec{\mathsf{n}}}$$

Figure 11. Remaning of the rules rules.

Probabilistic independence rules.

In the $\mathrm{L}_\varepsilon.\mathrm{FRESH}$, c_{n} *is a bound on the probability that the name* n *selects any precise value. For simplicity we give the rule for one context, but it can easily be extended to vectors of contexts containing the same name.*

$$\mathrm{G}_\varepsilon.\mathrm{E{:}FRESH}\quad \frac{\mathbb{E};\Theta \vdash \left[\phi^{\mathsf{n},i}_{\mathsf{fresh}}(\vec{u}, C(\mathsf{n}_{\mathsf{fresh}}\ ())) \mathbin{\tilde\vee} \phi^{\mathsf{n}_{\mathsf{fresh}},()}_{\mathsf{fresh}}(\vec{u}, C(\mathsf{n}_{\mathsf{fresh}}\ ()))\right]_{\varepsilon_1} \qquad \mathbb{E};\Theta \vdash \vec{u}, C(\mathsf{n}_{\mathsf{fresh}}\ ()) \sim_{\varepsilon_0} \vec{v}}{\mathbb{E};\Theta \vdash \vec{u}, C(\mathsf{n}\ i) \sim_{\varepsilon_0+\varepsilon_1} \vec{v}}$$

$$\mathrm{L}_\varepsilon.\mathrm{FRESH}\quad \frac{}{\mathbb{E};\Theta;\Gamma \vdash_{c_{\mathsf{n}}} \mathsf{n}\ i = u \Rightarrow \neg\phi^{\mathsf{n},i}_{\mathsf{fresh}}(u, i)}$$

Cryptographic rules.

For simplicity we give the cryptographic rules for one context, but it can easily be extended to vectors of contexts containing the same encryption or hash. If $\vec{u} = u_1, \ldots, u_n$ *and* $\vec{v} = v_1, \ldots, v_n$ *are two vectors of the same length, then* $\vec{u}\cdot\vec{v} \stackrel{\mathsf{def}}{=} \sum_i u_i \cdot v_i$ *denotes the scalar product of* $\vec{u}$ *and* $\vec{v}$*. Moreover,* $\vec{1}\cdot\vec{u} \stackrel{\mathsf{def}}{=} \sum_i u_i$ *is the scalar product of* $\vec{u}$ *with the sequence* $1, \ldots, 1$ *of* n *copies of* 1 *(*$\vec{1}$ *is implicitly of length* $\vec{u}$*).*

In the $\mathrm{G}_\varepsilon.\mathrm{PRF}$ *and* $\mathrm{G}_\varepsilon.\mathrm{CCA1}$ *rules,* $\vec{a} \stackrel{\mathsf{def}}{=} \vec{a}_0, \vec{a}_1$ *where* $\vec{a}_0$ *is of order* 0 *and* $\vec{a}_1$ *of order* 1 *and* $\vec{u} \stackrel{\mathsf{def}}{=} \vec{u}_0, \vec{u}_1$ *where* $\vec{u}_0$ *is of order* 0 *and* $\vec{u}_1$ *of order* 1.

$$\mathrm{L}_\varepsilon.\mathrm{EUF}\quad \frac{\mathbb{E};\Theta;\emptyset \vdash^{\mathsf{c}}_{\vec{t}} s, m, i \qquad \mathbb{E};\Theta;\Gamma, \neg(\phi^{\mathsf{k},i}_{\mathsf{key}}(s,m,t) \vee \phi^{\mathsf{k},i}_{\mathsf{sign}}(s,m,t)) \vdash_\varepsilon \psi \qquad \mathbb{E};\Theta \vdash \mathsf{det}(i)}{\mathbb{E};\Theta;\Gamma, \mathsf{verify}\ s\ m\ (\mathsf{pk}\ (\mathsf{k}\ i)) \vdash_{\varepsilon + \varepsilon_{\mathsf{EUF}}(\vec{1}\cdot\vec{t})} \psi}$$

$$\mathrm{G}_\varepsilon.\mathrm{PRF}\quad \frac{\begin{array}{c}\mathbb{E};\Theta;\emptyset \vdash^{\mathsf{c}}_{\vec{t}_{\vec{u}_1}} \vec{u}_1 \qquad \mathbb{E};\Theta;\emptyset \vdash^{\mathsf{c}}_{\vec{t}_{\vec{a}_1}} \vec{a}_1 \qquad \mathbb{E};\Theta;\emptyset \vdash^{\mathsf{c}}_{\vec{t}_0} \vec{u}_0, \vec{a}_0, b, m, i \\ \mathbb{E};\Theta;\emptyset \vdash^{\mathsf{c}}_{t_C, \vec{o}_C} C \qquad \mathbb{E};\Theta \vdash \mathsf{det}(i) \\ \mathbb{E};\Theta \vdash \mathsf{blen}_{\vec{l}}(\vec{a}) \qquad \mathbb{E};\Theta \vdash \mathsf{blen}_{l_{\mathsf{h}}}(\mathsf{hash}\ m\ (\mathsf{k}\ i)) \mathbin{\tilde\wedge} \mathsf{blen}_{l_{\mathsf{h}}}(\mathsf{n}_{\mathsf{fresh}}\ ()) \\ \mathbb{E};\Theta;\emptyset \vdash_{\varepsilon_\phi} \psi^{\mathsf{k},i}_{\mathsf{key}}(\vec{w}, C) \wedge \psi^{\mathsf{k},i}_{\mathsf{msg}}(\vec{w}, C) \qquad \mathbb{E};\Theta \vdash \vec{u}, \mathsf{if}\ b\ \mathsf{then}\ C\ \vec{a}\ (\mathsf{n}_{\mathsf{fresh}}\ ())\ \mathsf{else}\ u_e \sim_\varepsilon \vec{v}\end{array}}{\mathbb{E};\Theta \vdash \vec{u}, \mathsf{if}\ b\ \mathsf{then}\ C\ \vec{a}\ (\mathsf{hash}\ m\ (\mathsf{k}\ i))\ \mathsf{else}\ u_e \sim_{\varepsilon_f} \vec{v}}$$

where $\vec{w} \stackrel{\mathsf{def}}{=} \vec{u}, \vec{a}, b, m, i$ (note that u_e is *not* in $\vec{w}$) and:

$$t'_C \stackrel{\mathsf{def}}{=} t_C\ \vec{l}\ l_{\mathsf{h}} \qquad \text{and} \qquad \varepsilon_f \stackrel{\mathsf{def}}{=} \lambda t, \vec{o}.\, \varepsilon\ t\ \vec{o} + \varepsilon_\phi + \varepsilon_{\mathsf{PRF}}\big(t + t'_C + \vec{o}\cdot(\vec{t}_{\vec{u}_1}\ t) + \vec{o}_C\cdot(\vec{t}_{\vec{a}_1}\ t'_C) + \vec{1}\cdot\vec{t}_0\big)$$

$$\mathrm{G}_\varepsilon.\mathrm{CCA1}\quad \frac{\begin{array}{c}\mathbb{E};\Theta;\emptyset \vdash^{\mathsf{c}}_{\vec{t}_{\vec{u}_1}} \vec{u}_1 \qquad \mathbb{E};\Theta;\emptyset \vdash^{\mathsf{c}}_{\vec{t}_{\vec{a}_1}} \vec{a}_1 \qquad \mathbb{E};\Theta;\emptyset \vdash^{\mathsf{c}}_{\vec{t}_0} \vec{u}_0, \vec{a}_0, b, m, i_r, i_k \\ \mathbb{E};\Theta;\emptyset \vdash^{\mathsf{c}}_{t_C, \vec{o}_C} C \qquad \mathbb{E};\Theta \vdash \mathsf{det}(i_r) \mathbin{\tilde\wedge} \mathsf{det}(i_k) \\ \mathbb{E};\Theta \vdash \mathsf{blen}_{\vec{l}}(\vec{a}) \qquad \mathbb{E};\Theta \vdash \mathsf{blen}_{l_{\mathsf{e}}}(\mathsf{enc}\ m\ (\mathsf{r}\ i_r)\ (\mathsf{pk}(\mathsf{k}\ i_k))) \mathbin{\tilde\wedge} \mathsf{blen}_{l_{\mathsf{e}}}(\mathsf{enc}\ (0_{\mathsf{len}}(m))\ (\mathsf{r}\ i_r)\ (\mathsf{pk}(\mathsf{k}\ i_k))) \\ \mathbb{E};\Theta;\emptyset \vdash_{\varepsilon_\phi} \phi^{\mathsf{k},i_k}_{\mathsf{key}}(\vec{w}, C) \wedge \phi^{\mathsf{r},i_r}_{\mathsf{rand}}(\vec{w}, C) \wedge \phi^{\mathsf{k},i_k}_{\mathsf{dec}}(C, \vec{u}_1, \vec{a}_1) \\ \mathbb{E};\Theta \vdash \vec{u}, \mathsf{if}\ b\ \mathsf{then}\ C\ \vec{a}\ (\mathsf{enc}\ (0_{\mathsf{len}}(m))\ (\mathsf{r}\ i_r)\ (\mathsf{pk}(\mathsf{k}\ i_k)))\ \mathsf{else}\ u_e \sim_\varepsilon \vec{v}\end{array}}{\mathbb{E};\Theta \vdash \vec{u}, \mathsf{if}\ b\ \mathsf{then}\ C\ \vec{a}\ (\mathsf{enc}\ m\ (\mathsf{r}\ i_r)\ (\mathsf{pk}(\mathsf{k}\ i_k)))\ \mathsf{else}\ u_e \sim_{\varepsilon_f} \vec{v}}$$

where $\vec{w} \stackrel{\mathsf{def}}{=} \vec{u}, \vec{a}, b, m, i_r, i_k$ (note that u_e is *not* in $\vec{w}$) and:

$$t'_C \stackrel{\mathsf{def}}{=} t_C\ \vec{l}\ l_{\mathsf{e}} \qquad \text{and} \qquad \varepsilon_f \stackrel{\mathsf{def}}{=} \lambda t, \vec{o}.\, \varepsilon\ t\ \vec{o} + \varepsilon_\phi + \varepsilon_{\mathsf{CCA}}\big(t + t'_C + \vec{o}\cdot(\vec{t}_{\vec{u}_1}\ t) + \vec{o}_C\cdot(\vec{t}_{\vec{a}_1}\ t'_C) + \vec{1}\cdot\vec{t}_0\big)$$

Figure 12. Probabilistic independence and cryptographic rules.

Count-$\mathsf{CB}_\Pi(p)$ is the number of $\mathrm{G}_\varepsilon.\mathrm{E{:}CS_R}$ or $\mathrm{G}_\varepsilon.\mathrm{E{:}BI\text{-}DEDUCE}$ rules appearing below position p in Π:

$$\text{Count-CB}_\Pi(p) \stackrel{\text{def}}{=} \begin{cases} \left| \{p_0 \in \text{Path}_\Pi(p) \mid R_\Pi(p_0) \in \{\mathrm{G}_\varepsilon.\mathrm{E{:}CS_R}, \mathrm{G}_\varepsilon.\mathrm{E{:}BI\text{-}DEDUCE}\}\} \right| & \text{if } R_\Pi(p) \text{ is a descending rule} \\ 0 & \text{otherwise} \end{cases}$$

Count-$\mathsf{HW}_\Pi(p)$ is the number of $\mathrm{G.WEAK}$ rules appearing below position p in Π:

$$\text{Count-HW}_\Pi(p) \stackrel{\text{def}}{=} \begin{cases} \left| \{p_0 \in \text{Path}_\Pi(p) \mid R_\Pi(p_0) = \mathrm{G.WEAK}\} \right| & \text{if } R_\Pi(p) \text{ is descending rule} \\ 0 & \text{otherwise} \end{cases}$$

We partition $\text{Trunc}(\Pi)$ into the set of positions T_{RD} where the $\mathrm{G}_\varepsilon.\mathrm{E{:}REWRITE_0}$ or $\mathrm{G.DUP}$ rules are applied, and the remaining set of position T_A, i.e.:

$$\begin{aligned} T_{RD} &\stackrel{\text{def}}{=} \{p \in \text{Trunc}(\Pi) \mid R_\Pi(p) \in \{\mathrm{G}_\varepsilon.\mathrm{E{:}REWRITE_0}, \mathrm{G.DUP}\}\} \\ T_A &\stackrel{\text{def}}{=} \{p \in \text{Trunc}(\Pi) \mid R_\Pi(p) \notin \{\mathrm{G}_\varepsilon.\mathrm{E{:}REWRITE_0}, \mathrm{G.DUP}\}\} \end{aligned}$$

The value $\text{Value}_{\blacktriangleright_{AD}}(\Pi) \in \mathbb{N}^3$ of a proof Π is defined as:

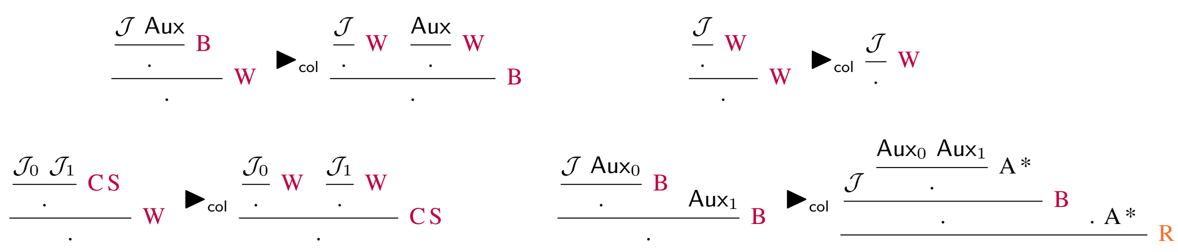
$$\text{Value}_{\blacktriangleright_{AD}}(\Pi) \stackrel{\text{def}}{=} \Big(\sum_{p \in T_A} \text{Count-CB}_\Pi(p), \sum_{p \in T_{RD}} \text{Count-CB}_\Pi(p), \sum_{p \in \text{Trunc}(\Pi)} \text{Count-HW}_\Pi(p) \Big)$$

Our goal is to obtain proofs where no ascending rule appear below a descending rule of the trunk, i.e. a proof such that $\text{Value}_{\blacktriangleright_{AD}}(\Pi) = (0, 0, 0)$.

Figure 13. Definitions of Count-$\mathsf{HW}_\Pi(p)$, Count-$\mathsf{CB}_\Pi(p)$ and $\text{Value}_{\blacktriangleright_{AD}}(\Pi)$.

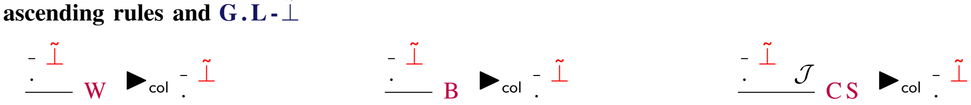
All occurences of $\mathrm{G.AXIOM}$ *are using the same axiom in those collapse rules*

Commutation and merge between ascending rules

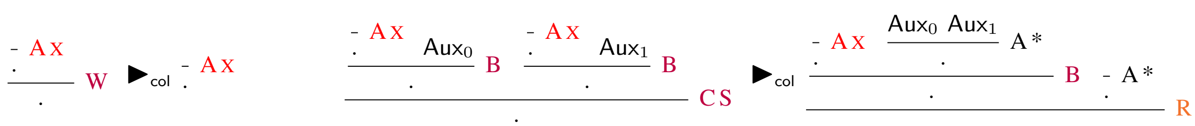


Collapse between ascending rules and $\mathrm{G}_\varepsilon.\mathrm{L\text{-}LOC}{:}\bot$

Collapse between ascending rules and $\mathrm{G.L\text{-}}\tilde{\mathrm{I}}$



Collapse between ascending rules and $\mathrm{G.AXIOM}$



Legend:

CS : $\mathrm{G}_\varepsilon.\mathrm{E{:}CS_R}$ B : $\mathrm{G}_\varepsilon.\mathrm{E{:}BI\text{-}DEDUCE}$ W : $\mathrm{G.WEAK}$ R : $\mathrm{G}_\varepsilon.\mathrm{E{:}REWRITE_0}$ $\tilde{\mathrm{I}}$: $\mathrm{G.L\text{-}}\tilde{\mathrm{I}}$

$\bot$: $\mathrm{G}_\varepsilon.\mathrm{L\text{-}LOC}{:}\bot$ Ax : $\mathrm{G.AXIOM}$ A : any rule

Figure 14. Shape of the collapsing proof transformations.

Appendix D
Soundness of the Proof System

A. Sketch of the soundness proofs

In this section, we give the key ingredients which are necessary to check the soundness of our proof system. Later on, in following sections, we will provide complete proofs for most of the rules that do not use the indistinguishability predicate.

a) Global indistinguishability rules: We sketch the proof of the rules given in Fig. 11:

- G_ε.E:Refl and G_ε.E:Sym. Proofs are trivial.
- G_ε.E:Trans. The proof relies on the triangular inequality.
- G_ε.E:FA-Base. We present this first (simple) reductionistic rule with more details, to serve as an example proof. Consider a machine $\mathcal{A}$ against $\vec{u_l}, v \sim \vec{u_r}, v$. By hypothesis, we have a machine $\mathcal{M}$ computing v in time t_v with error probability at most ε_v. Then, we build $\mathcal{B}$ against $\vec{u_l} \sim \vec{u_r}$ as follows: 1) run $\mathcal{M}$, which yields v (up-to error ε_v) on some tape; 2) then, $\mathcal{B}$ simulates $\mathcal{A}$, using its own input tapes in-place (containing $\vec{u_l}$ or $\vec{u_r}$) for the first input tapes of $\mathcal{A}$, and $\mathcal{M}$'s output tape (which should contain v) as the last input tape of $\mathcal{A}$; finally, $\mathcal{B}$ returns $\mathcal{A}$'s answer.
  $\mathcal{B}$ provides fresh working tapes for $\mathcal{M}$ and for $\mathcal{A}$, without re-using tapes, to ensure that $\mathcal{M}$ and $\mathcal{A}$ working tapes are initially empty.
  Machine $\mathcal{B}$ can forward all oracle calls from $\mathcal{A}$ to its own oracles without any overhead: if $\mathcal{A}$ want to call oracle f_i using T as output tape, then $\mathcal{B}$ does exactly the same. Thus, $\mathcal{B}$ runs in time $t + t_v$ where t is the running time of $\mathcal{A}$.
  We conclude by observing that its advantage is at most $\mathcal{A}$'s advantage, plus two times the error ε_v of $\mathcal{M}$, once per side of the equivalence $\sim$.
- G_ε.E:FA-Fun. Let $\mathcal{A}$ be a machine against $\vec{u_l}, f \sim \vec{u_r}, f$. By hypothesis, let $\mathcal{M}$ be a machine running in time $t_f(|x|)$ (on input x), and such that $\mathcal{M}$ correctly computes $f(x)$ on *all* inputs x, with a probability of error at most ε_f.
  We now build $\mathcal{B}$ against $\vec{u_l} \sim_\varepsilon \vec{u_r}$. $\mathcal{B}$ simulates $\mathcal{A}$, using its input tapes as input tapes for $\mathcal{A}$ (thus incurring no copy overhead), forwarding all oracle calls different from f to its own oracles.
  At this step, it only remains to simulate a call to oracle f. If $\mathcal{A}$ calls f with output tape T, then $\mathcal{B}$ first copies the content x of $\mathcal{A}$'s oracle input tape to an additional tape T_i, and then executes $\mathcal{M}$ using T_i as input tape and T as output tape (which is always possible, even if $\mathcal{M}$'s input and output tapes are identical, *i.e.* $\mathsf{T}_i = \mathsf{T}$).
  $\mathcal{B}$ running time is the running time of $\mathcal{A}$, plus the cost of simulating calls to f. We know that, since $\mathcal{A}$ runs in time at most t, all its oracle calls are on inputs of size at most t. Thus, each call to f is simulated in time t (to copy the input) plus $t_f(t)$ (to run $\mathcal{M}$). Assuming that $\mathcal{A}$ calls f at most o_f times, this yields an overall running time of $t + o_f \cdot (t + t_f(t))$.
  Finally, we conclude by observing that, as for the previous rule, we need to pay twice the error ε_f of $\mathcal{M}$.
- G_ε.E:FA-App. Consider a machine $\mathcal{A}$ against $\vec{u_l}, (f_l\ v_l) \sim \vec{u_r}, (f_r\ v_r)$. We build a machine $\mathcal{B}$ against $\vec{u_l}, f_l, v_l \sim \vec{u_r}, f_r, v_r$: on input $\vec{u}, f, v$ (which is either $\vec{u_l}, f_l, v_l$ or $\vec{u_r}, f_r, v_r$, depending on the side), $\mathcal{B}$ copies v to the oracle input tape; calls oracle f on this oracle tape, which yields $f(v)$ on an additional working tape T; and simulates $\mathcal{A}$, using the tapes containing $\vec{u}$ as first inputs tapes, and T as last input tape.
  $\mathcal{B}$'s running time is $t + l + 1$, decomposed as: $\mathcal{A}$'s running time t, plus the cost of copying v (which is at most l), plus a cost 1 to trigger the special oracle call transition.
- G_ε.E:FA-Names. Adversary $\mathcal{B}$ against the premise simulates Adversary $\mathcal{A}$ against the conclusion, except that it samples values according to the distribution of n_f itself.
- G_ε.E:Dup-Base. Consider an adversary $\mathcal{A}$ against $\vec{u_l}, v_l, v_l \sim \vec{u_r}, v_r, v_r$. We build an adversary $\mathcal{B}$ against $\vec{u_l}, v_l \sim \vec{u_r}, v_r$ by simulating $\mathcal{A}$ using, in place, $\mathcal{B}$'s inputs tapes. The missing input tape T of $\mathcal{A}$, that should contain v (which is v_l or v_r, depending on the side), is copied on-the-fly, as described next.
  Let T_0 be $\mathcal{B}$'s input tape initially containing v. $\mathcal{B}$ uses an additional working tape for T, initially empty, to which it will gradually copy v from T_0, copying i-th bit of v to T at the i-th step of $\mathcal{A}$'s simulation. This is possible by simply having two additional heads, one on T_0 and the other on T, continually advancing to the right, until the head of T_0 reaches the end of v. As far as $\mathcal{A}$ is concerned, T_0 contains v from the beginning, as a bit has always been set before it can reach it. This construction has no running-time overhead, and yields Adversary $\mathcal{B}$ with the same advantage as $\mathcal{A}$.
- G_ε.E:Dup-Fun. Consider an adversary $\mathcal{A}$ against $\vec{u_l}, f_l, f_l \sim \vec{u_r}, f_r, f_r$. Adversary $\mathcal{B}$ against $\vec{u_l}, f_l \sim \vec{u_r}, f_r$ simply simulates $\mathcal{A}$ in-place, on the same input tapes, forwarding each call to the first or second oracle f to its own version of f.
- G_ε.E:Weak. The proof is immediate: $\mathcal{B}$ against the premise simulates $\mathcal{A}$ against the conclusion, in-place, ignoring the inputs that $\mathcal{A}$ does not use.
- G_ε.E:Perm. The proof is also straightforward: $\mathcal{B}$ against the premise simulates $\mathcal{A}$ against the conclusion, in-place, permuting input tapes in $\mathcal{A}$'s transition table according to π.
- G.β and G.δ are trivially proven as properties of our term semantics.
- G_ε.E:CS is a standard CCSA rule. E.g. see [13] for a proof.

- G_ε.E:BI-DEDUCE is proved through a cryptographic reduction simulating the contexts and the sampling of the names, carefully accounting for cost aspects.
- For the two cryptographic rules G_ε.CCA1 and G_ε.PRF, we perform a reduction to the cryptographic game. First, we use the ϕ-condition as an up-to-bad argument in order to ensure that we can compute our terms without needing to compute the key under the cryptograhic hypothesis. (see [17, Propostion 8] for more details about this point). Then, we compute the Boolean and the challenge (along with some other stuff that can be computed at the same time). If the Boolean returns 0, we also abort and return 0. Otherwise, we call the challenge oracle with our challenge, and after that we compute the context that uses the return of the oracle (that is why in the CCA1 game, we have the extra condtion $\phi_{\mathsf{dec}}()$ in order to ensure that our context can be computed without calling the decryption oracle (since we do not have access to it anymore). Finally, we can call the attacker against our assumption and return the same result.

B. Auxillary Lemmas

Proposition 2. *Let $\mathbb{E}$ a valid environment, ϕ a boolean term and ε a term of type $\overline{\mathsf{real}}$ such that $\mathbb{E} \vdash \forall(x:\tau).\phi : \mathsf{bool}$. For all model $\mathbb{M}$ of $\mathbb{E}$, we have:*

$$\mathbb{M} : \mathbb{E} \models [\forall(x:\tau).\phi]_\varepsilon \text{ iff. } \mathbb{M} : \mathbb{E} \models \tilde{\forall}(x:\tau).\,[\phi]_\varepsilon$$

Proof. The proof is exactly the same than the one of the analogue properity in [17, Proposition 2]. Notice that the exact same proof work since x cannot appear in ε since $[\forall(x:\tau).\phi]_\varepsilon$ is well-typed. □

C. Local Judgement: Left Local Rules

- L_ε.L-$\forall$*:*
  Let $\mathbb{M}$ be a model such that $\mathbb{M} : \mathbb{E} \models \Theta$.
  Let $\eta \in \mathbb{N}$, $\rho \in \mathbb{T}_{\mathbb{M},\eta}$:
  $[\![\forall(x:\tau).\phi]\!]_{\mathbb{M}}^{\eta,\rho} = 1$ imply that $[\![\phi\{x \mapsto t\}]\!]_{\mathbb{M}}^{\eta,\rho} = 1$ since $\mathbb{E} \vdash t : \tau$.
  Therefore, since $[\![\neg((\wedge\Gamma) \wedge \forall(x:\tau).\phi \Rightarrow \psi)]\!]_{\mathbb{M}}^{\eta,\rho} = [\![(\wedge\Gamma) \wedge \forall(x:\tau).\phi \wedge \neg\psi]\!]_{\mathbb{M}}^{\eta,\rho}$ and $[\![\neg((\wedge\Gamma) \wedge \phi\{x \mapsto t\} \Rightarrow \psi)]\!]_{\mathbb{M}}^{\eta,\rho} = [\![(\wedge\Gamma) \wedge \phi\{x \mapsto t\} \wedge \neg\psi]\!]_{\mathbb{M}}^{\eta,\rho}$.
  So, $[\![\neg((\wedge\Gamma) \wedge \forall(x:\tau).\phi \Rightarrow \psi)]\!]_{\mathbb{M}}^{\eta,\rho} = 1$ imply that $[\![\neg((\wedge\Gamma) \wedge \phi\{x \mapsto t\} \Rightarrow \psi)]\!]_{\mathbb{M}}^{\eta,\rho} = 1$.
  Therefore, for every $\eta \in \mathbb{N}$,
  $$\begin{aligned} & \mathsf{Pr}_{\rho \in \mathbb{T}_{\mathbb{M},\eta}}\left(\neg((\wedge\Gamma) \wedge \forall(x:\tau).\phi \Rightarrow \psi)\right) \\ \leq\ & \mathsf{Pr}_{\rho \in \mathbb{T}_{\mathbb{M},\eta}}\left(\neg((\wedge\Gamma) \wedge \phi\{x \mapsto t\} \Rightarrow \psi)\right) \\ \leq\ & \mathsf{E}_\rho([\![\varepsilon]\!]_{\mathbb{M}}^{\eta,\rho}), \end{aligned}$$
  which clearly imply the soundness of the rule L_ε.L-$\forall$.
- L_ε.L-$\exists$*:*
  Let $\mathbb{M}$ be a model of $\mathbb{E}$.
  We have to show that, assuming:
  $$\mathbb{M} \models \tilde{\forall}(x:\tau).(\tilde{\wedge}\Theta) \tilde{\Rightarrow} [((\wedge\Gamma) \wedge \phi) \Rightarrow \psi)]_\varepsilon$$
  (This is equivalent to have that the premise of the rule holds for all model that are extension of $\mathbb{M}$ for the new declaration in $\mathbb{E}$, $x:\tau$) We have:
  $$\mathbb{M} \models (\tilde{\wedge}\Theta) \tilde{\Rightarrow} [((\wedge\Gamma) \wedge (\exists(x:\tau).\phi) \Rightarrow \psi)]_\varepsilon$$
  In fact, this is even a equivalence Indeed, the last equation holds iff.
  $$\mathbb{M} \models (\tilde{\wedge}\Theta) \tilde{\Rightarrow} [\forall(x:\tau).((\wedge\Gamma) \wedge \phi) \Rightarrow \psi)]_\varepsilon$$
  holds (since x doesn't appear in Γ or ψ). By Proposition 2, that holds iff.
  $$\mathbb{M} \models (\tilde{\wedge}\Theta) \tilde{\Rightarrow} \tilde{\forall}(x:\tau).\,[((\wedge\Gamma) \wedge \phi) \Rightarrow \psi)]_\varepsilon$$
  holds, and that finally if and only if our assumption holds since x doesn't appear in Θ.
- L_ε.L-$\Rightarrow$*:*
  Let $\mathbb{M}$ be a model such that $\mathbb{M} : \mathbb{E} \models \Theta$.
  Let $\eta \in \mathbb{N}$, $\rho \in \mathbb{T}_{\mathbb{M},\eta}$. We have that:
  $$\begin{aligned} & [\![\neg((\wedge\Gamma) \wedge (\phi_0 \Rightarrow \phi_1) \Rightarrow \psi)]\!]_{\mathbb{M}}^{\eta,\rho} \\ =\ & [\![((\wedge\Gamma) \wedge \neg\phi_0 \wedge \neg\psi) \vee ((\wedge\Gamma) \wedge \phi_1 \wedge \neg\psi)]\!]_{\mathbb{M}}^{\eta,\rho} \end{aligned}$$

is equal to 1 when either $[\![\neg((\wedge\Gamma) \Rightarrow \phi_0)]\!]_{\mathbb{M}}^{\eta;\rho} = [\![(\wedge\Gamma) \wedge \neg\phi_0]\!]_{\mathbb{M}}^{\eta;\rho}$ is equal to 1 or $[\![\neg(((\wedge\Gamma) \wedge \phi_1) \Rightarrow \psi)]\!]_{\mathbb{M}}^{\eta;\rho} = [\![(\wedge\Gamma) \wedge \phi_1 \wedge \neg\psi]\!]_{\mathbb{M}}^{\eta;\rho}$ is equal to 1. Therefore, for every $\eta \in \mathbb{N}$:

$$\begin{array}{ll} & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg((\wedge\Gamma) \wedge (\phi_0 \Rightarrow \phi_1) \Rightarrow \psi)]\!]_{\mathbb{M}}^{\eta;\rho}\right) \\ \leq & \begin{array}{l} \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg((\wedge\Gamma) \Rightarrow \phi_0)]\!]_{\mathbb{M}}^{\eta;\rho}\right) \\ +\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg(((\wedge\Gamma) \wedge \phi_1) \Rightarrow \psi)]\!]_{\mathbb{M}}^{\eta;\rho}\right) \end{array} \\ \leq & \mathsf{E}_\rho([\![\varepsilon_0]\!]_{\mathbb{M}}^{\eta;\rho}) + \mathsf{E}_\rho([\![\varepsilon_1]\!]_{\mathbb{M}}^{\eta;\rho}) \end{array}$$

which clearly imply the soundness of the rule $\mathrm{L}_\varepsilon.\mathrm{L}\text{-}\Rightarrow$.

- $\mathrm{L}_\varepsilon.\mathrm{L}\text{-}\wedge$*:* The premise and the conclusion clearly have the exact same semantic.
- $\mathrm{L}_\varepsilon.\mathrm{L}\text{-}\vee$*:*
  Let $\mathbb{M}$ be a model such that $\mathbb{M} : \mathbb{E} \models \Theta$.
  Let $\eta \in \mathbb{N}$, $\rho \in \mathbb{T}_{\mathbb{M},\eta}$. Then:
  $$[\![\neg(((\wedge\Gamma) \wedge (\phi_0 \vee \phi_1)) \Rightarrow \psi)]\!]_{\mathbb{M}}^{\eta;\rho} = [\![((\wedge\Gamma) \wedge \phi_0 \wedge \neg\psi) \vee ((\wedge\Gamma) \wedge \phi_1 \wedge \neg\psi)]\!]_{\mathbb{M}}^{\eta;\rho}.$$
  Therefore, for every $\eta \in \mathbb{N}$:
  $$\begin{array}{ll} & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg(((\wedge\Gamma) \wedge (\phi_0 \vee \phi_1)) \Rightarrow \psi)]\!]_{\mathbb{M}}^{\eta;\rho}\right) \\ \leq & \begin{array}{l} \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg((\wedge\Gamma) \wedge \phi_0) \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta;\rho}\right) \\ +\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg(((\wedge\Gamma) \wedge \phi_1) \Rightarrow \psi)]\!]_{\mathbb{M}}^{\eta;\rho}\right) \end{array} \\ \leq & \mathsf{E}_\rho([\![\varepsilon_0]\!]_{\mathbb{M}}^{\eta;\rho}) + \mathsf{E}_\rho([\![\varepsilon_1]\!]_{\mathbb{M}}^{\eta;\rho}) \end{array}$$
  which clearly imply the soundness of the rule $\mathrm{L}_\varepsilon.\mathrm{L}\text{-}\vee$.
- $\mathrm{L}_\varepsilon.\mathrm{L}\text{-}\bot$*:*
  Let $\mathbb{M}$ be a model such that $\mathbb{M} : \mathbb{E} \models \Theta$.
  Let $\eta \in \mathbb{N}$, $\rho \in \mathbb{T}_{\mathbb{M},\eta}$. Then:
  $$[\![(\wedge\Gamma) \wedge \bot \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta;\rho} = 1.$$
  Therefore, for every $\eta \in \mathbb{N}$:
  $$\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\neg\, [\![(\wedge\Gamma) \wedge \bot \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta;\rho}\right) \leq 0$$
  which clearly imply the soundness of the rule $\mathrm{L}_\varepsilon.\mathrm{L}\text{-}\bot$.

D. Local Judgement: Left Global Rules

- $\mathrm{L}_\varepsilon.\mathrm{L}\text{-}\tilde{\forall}$*:*
  Let $\mathbb{M}$ be a model such that $\mathbb{M} : \mathbb{E} \models (\wedge\Theta) \wedge \forall(x : \tau).F$
  Then $\mathbb{M} \models (\wedge\Theta) \wedge F\{x \mapsto t\}$ (since $\mathbb{E} \vdash t : \tau$).
  Therefore, $\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg(\wedge\Gamma \Rightarrow \phi)]\!]_{\mathbb{M}}^{\eta;\rho}\right) \leq \mathsf{E}_\rho([\![\varepsilon]\!]_{\mathbb{M}}^{\eta;\rho})$.
- $\mathrm{L}_\varepsilon.\mathrm{L}\text{-}\tilde{\exists}$*:*
  Let $\mathbb{M}$ be a model of $\mathbb{E}$.
  We want to show that:
  $$\mathbb{M} \models (\wedge\Theta \wedge \tilde{\exists}(x : \tau).F) \tilde{\Rightarrow} [(\wedge\Gamma) \Rightarrow \phi]_\varepsilon\,,$$
  which is equivalent to (since x does not appear in Θ, Γ and ϕ)
  $$\mathbb{M} \models \tilde{\forall}(x : \tau).((\wedge\Theta \wedge F) \tilde{\Rightarrow} [(\wedge\Gamma) \Rightarrow \phi]_\varepsilon).$$
  That is exactly the premise of the rule $\mathrm{L}_\varepsilon.\mathrm{L}\text{-}\tilde{\exists}$.
- $\mathrm{L}_\varepsilon.\mathrm{L}\text{-}\tilde{\Rightarrow}$*:*
  Let $\mathbb{M}$ be a model such that $\mathbb{M} : \mathbb{E} \models \Theta, (F_0 \tilde{\Rightarrow} F_1)$.
  Then, by the first premise, we have $\mathbb{M} \models F_0$, then we have $\mathbb{M} \models F_1$ since $\mathbb{M} \models F_0 \tilde{\Rightarrow} F_1$.
  Therefore, by the second premise, $\mathbb{M} \models [\wedge\Gamma \Rightarrow \psi]_\varepsilon$ which prove the soundness of $\mathrm{L}_\varepsilon.\mathrm{L}\text{-}\tilde{\Rightarrow}$
- $\mathrm{L}_\varepsilon.\mathrm{L}\text{-}\tilde{\wedge}$*:* The premise and the conclusion clearly have the exact same semantic.
- $\mathrm{L}_\varepsilon.\mathrm{L}\text{-}\tilde{\vee}$*:*
  Let $\mathbb{M}$ be a model such that $\mathbb{M} : \mathbb{E} \models \Theta, (F_0 \tilde{\vee} F_1)$.
  Then $\mathbb{M} \models \Theta, F_0$ or $\mathbb{M} \models \Theta, F_1$.
  Therefore, by the premises, $\mathbb{M} \models [\wedge\Gamma \Rightarrow \psi]_\varepsilon$.
- $\mathrm{L}_\varepsilon.\mathrm{L}\text{-}\tilde{\bot}$*:*
  Let $\mathbb{M}$ be a model such that $\mathbb{M} : \mathbb{E} \models \Theta, \tilde{\bot}$.
  Then, $\mathbb{M} \models [\wedge\Gamma \Rightarrow \psi]_\varepsilon$.

E. Local Judgement: Right Rules

- L_{ε}.R-$\forall$*:*
  Let $\mathbb{M}$ be a model such that $\mathbb{M} : \mathbb{E} \models \tilde{\forall}(x : \tau).(\wedge\Theta) \tilde{\Rightarrow} [(\wedge\Gamma \Rightarrow \phi)]_{\varepsilon}$.
  By Proposition 2, $\mathbb{M} : \mathbb{E} \models (\wedge\Theta) \tilde{\Rightarrow} \tilde{\forall}(x : \tau). [(\wedge\Gamma \Rightarrow \phi)]_{\varepsilon}$.
  Therefore gives: $\mathbb{M} : \mathbb{E} \models (\wedge\Theta) \tilde{\Rightarrow} [\forall(x : \tau).(\wedge\Gamma \Rightarrow \phi)]_{\varepsilon}$.
  Then (since x doesn't appear in Γ), $\mathbb{M} : \mathbb{E} \models (\wedge\Theta) \tilde{\Rightarrow} [\wedge\Gamma \Rightarrow \forall(x :).\phi]_{\varepsilon}$.
  which is exactly the conclusion
- L_{ε}.R-$\exists$*:*
  Let $\mathbb{M}$ be a model such that $\mathbb{M} \models \Theta$.
  Let $\eta \in \mathbb{N}$, $\rho \in \mathbb{T}_{\mathbb{M},\eta}$.
  Assume that $[\![\neg((\wedge\Gamma) \Rightarrow \phi\{x \mapsto t\})]\!]_{\mathbb{M}}^{\eta,\rho} = 0$.
  Then $[\![\wedge\Gamma]\!]_{\mathbb{M}}^{\eta,\rho} = 0$ and $[\![\neg\phi\{x \mapsto t\}]\!]_{\mathbb{M}}^{\eta,\rho} = 0$.
  Therefore, $[\![\neg\exists(x : \tau).\phi]\!]_{\mathbb{M}}^{\eta,\rho} = 0$.
  So, $[\![\neg((\wedge\Gamma) \Rightarrow \exists(x : \tau).\phi)]\!]_{\mathbb{M}}^{\eta,\rho} = 0$.
  Finally, for every $\eta \in \mathbb{N}$:

$$\begin{aligned} & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg((\wedge\Gamma) \Rightarrow \exists(x : \tau).\phi)]\!]_{\mathbb{M}}^{\eta,\rho}\right) \\ \leq\ & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg((\wedge\Gamma) \Rightarrow \phi\{x \mapsto t\})]\!]_{\mathbb{M}}^{\eta,\rho}\right) \\ \leq\ & \mathsf{E}_{\rho}([\![\varepsilon]\!]_{\mathbb{M}}^{\eta,\rho}). \end{aligned}$$

- L_{ε}.R-$\Rightarrow$*:*
  Let $\mathbb{M}$ be a model such that $\mathbb{M} \models \Theta$.
  Let $\eta \in \mathbb{N}$, $\rho \in \mathbb{T}_{\mathbb{M},\eta}$.

$$[\![\neg(\wedge\Gamma \Rightarrow (\psi \Rightarrow \phi))]\!]_{\mathbb{M}}^{\eta,\rho} = [\![\neg(\wedge\Gamma \wedge \psi \Rightarrow \phi)]\!]_{\mathbb{M}}^{\eta,\rho}$$

F. Local Judgement: Other Rules

- L_{ε}.REWRITE*:*
  Let $\mathbb{M}$ be a model such that $\mathbb{M} \models \Theta$.
  Let $\eta \in \mathbb{N}$,

$$\begin{aligned} & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg((\wedge\Gamma) \Rightarrow \phi\{t\})]\!]_{\mathbb{M}}^{\eta,\rho}\right) \\ =\ & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg((\wedge\Gamma) \Rightarrow \phi\{t\})]\!]_{\mathbb{M}}^{\eta,\rho} \wedge [\![\neg((\wedge\Gamma) \Rightarrow s = t)]\!]_{\mathbb{M}}^{\eta,\rho}\right) + \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg((\wedge\Gamma) \Rightarrow \phi\{t\})]\!]_{\mathbb{M}}^{\eta,\rho} \wedge [\![\neg((\wedge\Gamma) \Rightarrow \neg(s = t))]\!]_{\mathbb{M}}^{\eta,\rho}\right) \\ =\ & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg((\wedge\Gamma) \Rightarrow (\phi\{t\} \wedge s = t))]\!]_{\mathbb{M}}^{\eta,\rho}\right) + \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg((\wedge\Gamma) \Rightarrow (\phi\{t\} \wedge \neg s = t))]\!]_{\mathbb{M}}^{\eta,\rho}\right) \\ =\ & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg((\wedge\Gamma) \Rightarrow (\phi\{s\} \wedge s = t))]\!]_{\mathbb{M}}^{\eta,\rho}\right) + \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg((\wedge\Gamma) \Rightarrow (\phi\{t\} \wedge \neg s = t))]\!]_{\mathbb{M}}^{\eta,\rho}\right) \\ \leq\ & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg((\wedge\Gamma) \Rightarrow \phi\{s\})]\!]_{\mathbb{M}}^{\eta,\rho}\right) + \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg((\wedge\Gamma) \Rightarrow \neg s = t)]\!]_{\mathbb{M}}^{\eta,\rho}\right) \\ \leq\ & \mathsf{E}_{\rho}([\![\varepsilon_0]\!]_{\mathbb{M}}^{\eta,\rho}) + \mathsf{E}_{\rho}([\![\varepsilon_1]\!]_{\mathbb{M}}^{\eta,\rho}) \end{aligned}$$

- L_{ε}.AXIOM*:*
  Let $\mathbb{M}$ be a model such that $\mathbb{M} \models \Theta$, then $\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\neg(\wedge\Gamma \wedge \phi \Rightarrow \phi)]\!]_{\mathbb{M}}^{\eta,\rho}\right) \leq 0$.
- L_{ε}.ABSURD*:*
  Let $\mathbb{M}$ be a model such that $\mathbb{M} \models \Theta$, then:

$$\begin{aligned} & [\![\neg((\wedge\Gamma) \wedge (\phi \Rightarrow \bot) \Rightarrow \bot)]\!]_{\mathbb{M}}^{\eta,\rho} \\ =\ & [\![\neg((\wedge\Gamma) \Rightarrow (\phi \Rightarrow \bot) \Rightarrow \bot)]\!]_{\mathbb{M}}^{\eta,\rho} \\ =\ & [\![\neg((\wedge\Gamma) \Rightarrow \neg\neg\phi)]\!]_{\mathbb{M}}^{\eta,\rho} \\ =\ & [\![\neg(\wedge\Gamma \Rightarrow \phi)]\!]_{\mathbb{M}}^{\eta,\rho}. \end{aligned}$$

- L_{ε}.CUT-LOC*:*
  Let $\mathbb{M}$ be a model such that $\mathbb{M} \models \Theta$, then

$$\begin{aligned} & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\neg\, [\![\wedge\Gamma \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta,\rho}\right) \\ =\ & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\neg([\![\wedge\Gamma \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta,\rho} \wedge [\![\wedge\Gamma \Rightarrow \phi]\!]_{\mathbb{M}}^{\eta,\rho})\right) + \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\neg([\![\wedge\Gamma \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta,\rho} \wedge \neg\, [\![\wedge\Gamma \Rightarrow \phi]\!]_{\mathbb{M}}^{\eta,\rho})\right) \\ =\ & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\neg([\![\wedge\Gamma \wedge \phi \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta,\rho}) \wedge [\![\wedge\Gamma \Rightarrow \phi]\!]_{\mathbb{M}}^{\eta,\rho}\right) + \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\neg([\![\wedge\Gamma \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta,\rho}) \wedge \neg([\![\wedge\Gamma \Rightarrow \phi]\!]_{\mathbb{M}}^{\eta,\rho})\right) \\ \leq\ & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\neg([\![\wedge\Gamma \wedge \phi \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta,\rho})\right) + \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\neg[\![\wedge\Gamma \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta,\rho}\right) \\ \leq\ & \mathsf{E}_{\rho}([\![\varepsilon_0]\!]_{\mathbb{M}}^{\eta,\rho}) + \mathsf{E}_{\rho}([\![\varepsilon_1]\!]_{\mathbb{M}}^{\eta,\rho}) \end{aligned}$$

- $\mathrm{L}_\varepsilon.\textsc{Cut-Glob}$*:*
Let $\mathbb{M}$ be a model such that $\mathbb{M} \models \Theta$, then by the first premise, $\mathbb{M} \models F$. Therefore $\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta,\rho}) \leq \mathsf{E}_\rho([\![\varepsilon]\!]_{\mathbb{M}}^{\eta,\rho})$
- $\mathrm{L}_\varepsilon.\textsc{Weak}$*:*
Let $\mathbb{M}$ be a model such that $\mathbb{M} \models \Theta_0, \Theta_1$, then $\mathbb{M} \models \Theta_0$. Therefore:

$$\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma_0\Gamma_1 \Rightarrow \phi]\!]_{\mathbb{M}}^{\eta,\rho}) \leq \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma_0 \Rightarrow \phi]\!]_{\mathbb{M}}^{\eta,\rho}) \leq \mathsf{E}_\rho([\![\varepsilon]\!]_{\mathbb{M}}^{\eta,\rho}).$$

G. Local Judgement: ε Weakening Rules

- $\mathrm{L}_\varepsilon.\textsc{Weak}_0$*:*
Let $\mathbb{M}$ be a model such that $\mathbb{M} \models \Theta$, then $\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\neg [\![\varepsilon \leq \varepsilon']\!]_{\mathbb{M}}^{\eta,\rho}\right) \leq 0$ by the second premise, and since for every $\eta \in \mathbb{N}$, we have that $\mathbb{T}_{\mathbb{M},\eta}$ are finite, and we use the uniform metric, this is equivalent to:

$$\forall\eta \in \mathbb{N}, \forall\rho \in \mathbb{T}_{\mathbb{M},\eta}, [\![\varepsilon]\!]_{\mathbb{M}}^{\eta,\rho} \leq [\![\varepsilon']\!]_{\mathbb{M}}^{\eta,\rho}$$

Thus:

$$\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma \Rightarrow \phi]\!]_{\mathbb{M}}^{\eta,\rho}) \leq \mathsf{E}_\rho([\![\varepsilon]\!]_{\mathbb{M}}^{\eta,\rho}) \leq \mathsf{E}_\rho([\![\varepsilon']\!]_{\mathbb{M}}^{\eta,\rho}).$$

- $\mathrm{L}_\varepsilon.\textsc{Weak}_\varepsilon$*:*
Let $\mathbb{M}$ be a model such that $\mathbb{M} \models \Theta$, then $\forall\eta \in \mathbb{N}, \forall\rho \in \mathbb{T}_{\mathbb{M},\eta}, \varepsilon_0 \leq 1$ by the third premise. Then, for every $\eta \in \mathbb{N}$,

$$\begin{aligned}
& \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma \Rightarrow \phi]\!]_{\mathbb{M}}^{\eta,\rho}) \\
\leq\ & \mathsf{E}_\rho([\![\varepsilon]\!]_{\mathbb{M}}^{\eta,\rho}) + \mathsf{E}_\rho([\![\varepsilon_0]\!]_{\mathbb{M}}^{\eta,\rho}) \\
\leq\ & \mathsf{E}_\rho([\![\varepsilon]\!]_{\mathbb{M}}^{\eta,\rho}) + \mathsf{E}_\rho([\![\varepsilon_0]\!]_{\mathbb{M}}^{\eta,\rho}\, \mathbb{1}_{[\![\varepsilon_0\leq\varepsilon'_0]\!]_{\mathbb{M}}^{\eta,\rho}}) + \mathsf{E}_\rho([\![\varepsilon_0]\!]_{\mathbb{M}}^{\eta,\rho}\, \mathbb{1}_{\neg[\![\varepsilon_0\leq\varepsilon'_0]\!]_{\mathbb{M}}^{\eta,\rho}}) \\
\leq\ & \mathsf{E}_\rho([\![\varepsilon]\!]_{\mathbb{M}}^{\eta,\rho}) + \mathsf{E}_\rho([\![\varepsilon'_0]\!]_{\mathbb{M}}^{\eta,\rho}\, \mathbb{1}_{[\![\varepsilon_0\leq\varepsilon'_0]\!]_{\mathbb{M}}^{\eta,\rho}}) + \mathsf{E}_\rho(\mathbb{1}_{\neg[\![\varepsilon_0\leq\varepsilon'_0]\!]_{\mathbb{M}}^{\eta,\rho}}) \\
\leq\ & \mathsf{E}_\rho([\![\varepsilon]\!]_{\mathbb{M}}^{\eta,\rho}) + \mathsf{E}_\rho([\![\varepsilon'_0]\!]_{\mathbb{M}}^{\eta,\rho}\, \mathbb{1}_{[\![\varepsilon_0\leq\varepsilon'_0]\!]_{\mathbb{M}}^{\eta,\rho}}) + \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left([\![\varepsilon_0 \leq \varepsilon'_0]\!]_{\mathbb{M}}^{\eta,\rho}\right) \\
\leq\ & \mathsf{E}_\rho([\![\varepsilon]\!]_{\mathbb{M}}^{\eta,\rho}) + \mathsf{E}_\rho([\![\varepsilon'_0]\!]_{\mathbb{M}}^{\eta,\rho}) + \mathsf{E}_\rho([\![\varepsilon_1]\!]_{\mathbb{M}}^{\eta,\rho}) \\
\leq\ & \mathsf{E}_\rho([\![\varepsilon + \varepsilon'_0 + \varepsilon_1]\!]_{\mathbb{M}}^{\eta,\rho})
\end{aligned}$$

H. Mixed Judgement Rules

- $\mathrm{L}_\varepsilon.\textsc{ByGlob}$ *and* $\mathrm{G}_\varepsilon.\textsc{ByLoc}$*:*
The premise and the conclusion have the exact same semantic.
- $\mathrm{L}_\varepsilon.\textsc{Localise}$*:*
Let $\mathbb{M}$ be a model such that $\mathbb{M} \models \Theta, [\phi]_{\varepsilon_1}$, then $\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\phi]\!]_{\mathbb{M}}^{\eta,\rho}) \leq \mathsf{E}_\rho([\![\varepsilon_1]\!]_{\mathbb{M}}^{\eta,\rho})$ and since, $\mathbb{M} \models \Theta$ by the premise, $\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma \wedge \phi \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta,\rho}) \leq \mathsf{E}_\rho(\varepsilon_0)$.
Therefore,

$$\begin{aligned}
& \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta,\rho}) \\
=\ & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta,\rho} \wedge [\![\phi]\!]_{\mathbb{M}}^{\eta,\rho}) + \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta,\rho} \wedge \neg [\![\phi]\!]_{\mathbb{M}}^{\eta,\rho}) \\
\leq\ & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma \wedge \phi \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta,\rho}) + \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\phi]\!]_{\mathbb{M}}^{\eta,\rho}) \\
\leq\ & \mathsf{E}_\rho([\![\varepsilon_0]\!]_{\mathbb{M}}^{\eta,\rho}) + \mathsf{E}_\rho([\![\varepsilon_1]\!]_{\mathbb{M}}^{\eta,\rho})
\end{aligned}$$

- $\mathrm{L}_\varepsilon.\textsc{Rewrite-Equiv}$*:*
Let $\mathbb{M}$ be a model such that $\mathbb{M} \models \Theta$. Since the adversary $\mathcal{A}_{\mathsf{bool}}$, that get a boolean as input, and send back the opposite boolean, is a adversary against the equivalence in the second premise in time 1. Then,

$$|\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma_0 \Rightarrow \phi_0]\!]_{\mathbb{M}}^{\eta,\rho}) - \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma_1 \Rightarrow \phi_1]\!]_{\mathbb{M}}^{\eta,\rho})| \leq \mathsf{E}_\rho([\![\varepsilon_0]\!]_{\mathbb{M}}^{\eta,\rho}(1)).$$

Therefore,

$$\begin{aligned}
& \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma_0 \Rightarrow \phi_0]\!]_{\mathbb{M}}^{\eta,\rho}) \\
=\ & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma_0 \Rightarrow \phi_0]\!]_{\mathbb{M}}^{\eta,\rho}) + \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma_1 \Rightarrow \phi_1]\!]_{\mathbb{M}}^{\eta,\rho}) - \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma_1 \Rightarrow \phi_1]\!]_{\mathbb{M}}^{\eta,\rho}) \\
\leq\ & \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma_1 \Rightarrow \phi_1]\!]_{\mathbb{M}}^{\eta,\rho}) + |\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma_0 \Rightarrow \phi_0]\!]_{\mathbb{M}}^{\eta,\rho}) - \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\wedge\Gamma_1 \Rightarrow \phi_0]\!]_{\mathbb{M}}^{\eta,\rho})| \\
\leq\ & \mathsf{E}_\rho([\![\varepsilon_1]\!]_{\mathbb{M}}^{\eta,\rho}) + \mathsf{E}_\rho([\![\varepsilon_0(1)]\!]_{\mathbb{M}}^{\eta,\rho}).
\end{aligned}$$

I. Global Judgement: Left and Right Rules

We omit the proofs of the left and right rules for the global judgements, as they are standard.

J. Global Judgement: Local and Global Relations

All those rules could be deduced form the case analysis on boolean rules $\dfrac{\mathsf{const}(\phi)}{[\phi]_0 \tilde{\vee} [\neg\phi]_0}$ and the other rules. (As well, as their right counterpart that we omit.)

- *G$_\varepsilon$.L-Loc:$\Rightarrow$:*
  Let $\mathbb{M}$ a model such that $\mathbb{M} \models \Theta$.
  By the second premise, there exists $c \in \cap_{\eta\in\mathbb{N}} [\![\mathsf{bool}]\!]^{\eta}_{\mathbb{M}} = \{0,1\}$ such that $\forall \eta \in \mathbb{N}, \forall \rho \in \mathbb{T}_{\mathbb{M},\eta}, [\![\phi]\!]^{\eta,\rho}_{\mathbb{M}} = c$ Then, by case disjonction:
  - <u>case c = 0:</u> For every $\eta \in \mathbb{N}$, $\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\phi]\!]^{\eta,\rho}_{\mathbb{M}}) = \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\top) = 1$
    Therefore, $\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\phi]\!]^{\eta,\rho}_{\mathbb{M}}) \leq 0 \Rightarrow \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg) \leq \mathsf{E}_\rho([\![\varepsilon]\!]^{\eta,\rho}_{\mathbb{M}})$ holds
    i.e $\mathbb{M} \models [\phi]_0 \tilde{\Rightarrow} [\psi]_0$.
    And, by the first premise, $\mathbb{M} \models F$.
  - <u>case c = 1:</u> We want to show that $\mathbb{M} \models [\phi \Rightarrow \psi]_\varepsilon \tilde{\Rightarrow} F$. So assuming that $\mathbb{M} \models [\phi \Rightarrow \psi]_\varepsilon$, let's show that $\mathbb{M} \models F$.
    For every $\eta \in \mathbb{N}$, we have $\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\phi \Rightarrow \psi]\!]^{\eta,\rho}_{\mathbb{M}}) = \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}([\![\psi]\!]^{\eta,\rho}_{\mathbb{M}}) \leq \mathsf{E}_\rho([\![\varepsilon]\!]^{\eta,\rho}_{\mathbb{M}})$.
    Therefore, $\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\phi]\!]^{\eta,\rho}_{\mathbb{M}}) \leq 0 \Rightarrow \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\psi]\!]^{\eta,\rho}_{\mathbb{M}}) \leq \mathsf{E}_\rho([\![\varepsilon]\!]^{\eta,\rho}_{\mathbb{M}})$ holds
    i.e $\mathbb{M} \models [\phi]_0 \tilde{\Rightarrow} [\psi]_\varepsilon$.
    And, by the first premise, $\mathbb{M} \models F$.
- *G$_\varepsilon$.L-Loc:$\vee$:*
  Let $\mathbb{M}$ a model such that $\mathbb{M} \models \Theta$.
  By the third premise, there exists $c \ \in \cap_{\eta\in\mathbb{N}} [\![\mathsf{bool}]\!]^{\eta}_{\mathbb{M}} = \{0,1\}$ such that $\forall \eta \in \mathbb{N}, \forall \rho \in \mathbb{T}_{\mathbb{M},\eta}, [\![\phi]\!]^{\eta,\rho}_{\mathbb{M}} = c$ (by symmetry of ψ and ϕ here, we can only consider the case where $\mathsf{const}(\phi)$ holds).
  We want to show that $\mathbb{M} \models [\phi \vee \psi]_\varepsilon \tilde{\Rightarrow} F$. Therefore, we assume $\mathbb{M} \models [\phi \vee \psi]_\varepsilon$ Then, by case disjonction:
  - <u>case c = 0:</u> For every $\eta \in \mathbb{N}$,
    $\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![psi]\!]^{\eta,\rho}_{\mathbb{M}}) = \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}([\![\neg\phi \wedge \neg\psi]\!]^{\eta,\rho}_{\mathbb{M}}) = \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\phi \vee \psi]\!]^{\eta,\rho}_{\mathbb{M}}) \leq \mathsf{E}_\rho([\![\varepsilon]\!]^{\eta,\rho}_{\mathbb{M}})$ holds
    i.e $\mathbb{M} \models [\psi]_\varepsilon$
    And, by the second premise, $\mathbb{M} \models F$
  - <u>case c = 1:</u> For every $\eta \in \mathbb{N}$,
    Therefore, $\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\phi]\!]^{\eta,\rho}_{\mathbb{M}}) = \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\bot) = \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}([\![\neg\phi \wedge \neg\psi]\!]^{\eta,\rho}_{\mathbb{M}}) = \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\phi \vee \psi]\!]^{\eta,\rho}_{\mathbb{M}}) \leq \mathsf{E}_\rho([\![\varepsilon]\!]^{\eta,\rho}_{\mathbb{M}})$ holds
    i.e $\mathbb{M} \models [\phi]_{ve}$
    And, by the first premise, $\mathbb{M} \models F$
- *G$_\varepsilon$.L-$\tilde{\forall}$-$\forall$and G$_\varepsilon$.L-$\forall$-$\tilde{\forall}$:*
  Direct by Proposition 2
- *G$_\varepsilon$.L-Loc:$\forall$:*
  Let $\mathbb{M}$ a model such that $\mathbb{M} \models \Theta$.
  We want to prove that $\mathbb{M} \models [\forall(x:\tau).\psi]_\varepsilon \tilde{\Rightarrow} F$.
  Then, we can assume $\mathbb{M} \models [\forall(x:\tau).\psi]_\varepsilon$ to prove $\mathbb{M} \models F$
  Which imply by Proposition 2, $\mathbb{M} \models \tilde{\forall}(x:\tau).\,[\psi]_\varepsilon$
  Therefore, in particular, $\mathbb{M} \models [\psi]_\varepsilon \{x \mapsto u\}$ since $\mathbb{E} \vdash u : \tau$.
  And since, x cannot appear in ε,$\mathbb{M} \models [\psi\{x \mapsto u\}]_\varepsilon$
  Finally, by the premise, $\mathbb{M} \models F$.
- *G$_\varepsilon$.L-Loc:$\wedge$:*
  Let $\mathbb{M}$ a model such that $\mathbb{M} \models \Theta$.
  We want to prove that $\mathbb{M} \models [\psi \wedge \phi]_\varepsilon \tilde{\Rightarrow} F$.
  Then, we can assume $\mathbb{M} \models [\psi \wedge \phi]_\varepsilon$ to prove $\mathbb{M} \models F$
  Therefore we have that, for every $\eta \in \mathbb{N}$,
  $$\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\psi]\!]^{\eta,\rho}_{\mathbb{M}}) \leq \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}([\![\neg\psi \vee \neg\phi]\!]^{\eta,\rho}_{\mathbb{M}}) = \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\psi \wedge \phi]\!]^{\eta,\rho}_{\mathbb{M}}) \leq \mathsf{E}_\rho([\![\varepsilon]\!]^{\eta,\rho}_{\mathbb{M}})$$
  and
  $$\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\phi]\!]^{\eta,\rho}_{\mathbb{M}}) \leq \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}([\![\neg\psi \vee \neg\phi]\!]^{\eta,\rho}_{\mathbb{M}}) = \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\psi \wedge \phi]\!]^{\eta,\rho}_{\mathbb{M}}) \leq \mathsf{E}_\rho([\![\varepsilon]\!]^{\eta,\rho}_{\mathbb{M}})$$
  So, $\mathbb{M} \models [\phi]_\varepsilon, [\psi]_\varepsilon$.
  Then, by the premise, $\mathbb{M} \models F$.
- *G$_\varepsilon$.L-Loc:$\bot$:*
  Let $\mathbb{M}$ a model such that $\mathbb{M} \models \Theta$.

For every $\eta \in \mathbb{N}$, we have $\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\bot]\!]^{\eta,\rho}_{\mathbb{M}}) = \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\top) = 1$.
Therefore,$\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg [\![\bot]\!]^{\eta,\rho}_{\mathbb{M}}) \leq 0 \Rightarrow F$ holds. i.e $\mathbb{M} \models [\bot]_0 \tilde{\Rightarrow} F$.

K. Global Judgement: ε-Weakening Rules

- G$_\varepsilon$.REACH:ε-WEAK$_0$:
This rule can be deduced by some other rules L$_\varepsilon$.BYGLOB,G$_\varepsilon$.BYLOC and L$_\varepsilon$.WEAK$_0$.
- G$_\varepsilon$.REACH:ε-WEAK$_0$:
This rule can be deduced by some other rules L$_\varepsilon$.BYGLOB,G$_\varepsilon$.BYLOC and L$_\varepsilon$.WEAK$_\varepsilon$.
- G$_\varepsilon$.E:ε-WEAK$_0$:
Let $\mathbb{M}$ be a model such that $\mathbb{M} \models \Theta$.
By the first premise, we have that $\forall \eta \in \mathbb{N}, \forall \rho \in \mathbb{T}_{\mathbb{M},\eta}, \varepsilon \leq \varepsilon'$. where $\leq$ is the pointwise order on function.
Let $\eta \in \mathbb{N}$, Let $\mathcal{A}$ be a attacker against the game ($\vec{u}$,$\vec{v}$). we denote $\vec{u} = \vec{u}_0, \vec{u}_1$ for the term of order 0 and 1 in $\vec{u}$. (And we do the same for $\vec{v}$) Then, by the second premise,
$$\left|\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\mathcal{A}^{[\![\vec{u}_1]\!]^{\eta,\rho}_{\mathbb{M}}}(1^\eta, [\![\vec{u}_0]\!]^{\eta,\rho}_{\mathbb{M}}, \rho_a)\right) - \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\mathcal{A}^{[\![\vec{v}_1]\!]^{\eta,\rho}_{\mathbb{M}}}(1^\eta, [\![\vec{v}_0]\!]^{\eta,\rho}_{\mathbb{M}}, \rho_a)\right)\right| \leq \mathsf{E}_\rho([\![\varepsilon]\!]^{\eta,\rho}_{\mathbb{M}}(\mathsf{time}^\eta_{\mathcal{A}}, \mathsf{calls}^\eta_{\mathcal{A}}))$$
Therefore, we have:
$$\left|\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\mathcal{A}^{[\![\vec{u}_1]\!]^{\eta,\rho}_{\mathbb{M}}}(1^\eta, [\![\vec{u}_0]\!]^{\eta,\rho}_{\mathbb{M}}, \rho_a)\right) - \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\mathcal{A}^{[\![\vec{v}_1]\!]^{\eta,\rho}_{\mathbb{M}}}(1^\eta, [\![\vec{v}_0]\!]^{\eta,\rho}_{\mathbb{M}}, \rho_a)\right)\right| \leq \mathsf{E}_\rho([\![\varepsilon']\!]^{\eta,\rho}_{\mathbb{M}}(\mathsf{time}^\eta_{\mathcal{A}}, \mathsf{calls}^\eta_{\mathcal{A}})).$$
So, $\mathbb{M} \models \vec{u} \sim_{\varepsilon'} \vec{v}$
- G$_\varepsilon$.E:ε-WEAK$_0$:
Let $\mathbb{M}$ be a model such that $\mathbb{M} \models \Theta$.
By the third premise, we have that $\forall \eta \in \mathbb{N}, \forall \rho \in \mathbb{T}_{\mathbb{M},\eta}, \varepsilon \leq 1'$. where $\leq$ is the pointwise order on function.
By the second premise, we have that $\forall \eta \in \mathbb{N}, \forall \rho$ Let $\eta \in \mathbb{N}$, Let $\mathcal{A}$ be a attacker against the game ($\vec{u}$,$\vec{v}$). we denote $\vec{u} = \vec{u}_0, \vec{u}_1$ for the term of order 0 and 1 in $\vec{u}$. (And we do the same for $\vec{v}$).

  Then, by the first premise,
$$\left|\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\mathcal{A}^{[\![\vec{u}_1]\!]^{\eta,\rho}_{\mathbb{M}}}(1^\eta, [\![\vec{u}_0]\!]^{\eta,\rho}_{\mathbb{M}}, \rho_a)\right) - \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\mathcal{A}^{[\![\vec{v}_1]\!]^{\eta,\rho}_{\mathbb{M}}}(1^\eta, [\![\vec{v}_0]\!]^{\eta,\rho}_{\mathbb{M}}, \rho_a)\right)\right| \leq \mathsf{E}_\rho([\![\varepsilon_0]\!]^{\eta,\rho}_{\mathbb{M}}(\mathsf{time}^\eta_{\mathcal{A}}, \mathsf{calls}^\eta_{\mathcal{A}}))$$
And we have that:
$$\begin{aligned} & \mathsf{E}_\rho([\![\varepsilon_0]\!]^{\eta,\rho}_{\mathbb{M}}(\mathsf{time}^\eta_{\mathcal{A}}, \mathsf{calls}^\eta_{\mathcal{A}})) \\ = \; & \mathsf{E}_\rho([\![\varepsilon_0]\!]^{\eta,\rho}_{\mathbb{M}}(\mathsf{time}^\eta_{\mathcal{A}}, \mathsf{calls}^\eta_{\mathcal{A}})\mathbb{1}_{[\![\varepsilon_0]\!]^{\eta,\rho}_{\mathbb{M}} \leq [\![\varepsilon'_0]\!]^{\eta,\rho}_{\mathbb{M}}}) + \mathsf{E}_\rho([\![\varepsilon_0]\!]^{\eta,\rho}_{\mathbb{M}}(\mathsf{time}^\eta_{\mathcal{A}}, \mathsf{calls}^\eta_{\mathcal{A}})\mathbb{1}_{\neg([\![\varepsilon_0]\!]^{\eta,\rho}_{\mathbb{M}} \leq [\![\varepsilon'_0]\!]^{\eta,\rho}_{\mathbb{M}})}) \\ \leq \; & \mathsf{E}_\rho([\![\varepsilon'_0]\!]^{\eta,\rho}_{\mathbb{M}}(\mathsf{time}^\eta_{\mathcal{A}}, \mathsf{calls}^\eta_{\mathcal{A}})\mathbb{1}_{[\![\varepsilon_0]\!]^{\eta,\rho}_{\mathbb{M}} \leq [\![\varepsilon'_0]\!]^{\eta,\rho}_{\mathbb{M}}}) + \mathsf{E}_\rho(\mathbb{1}_{\neg([\![\varepsilon_0]\!]^{\eta,\rho}_{\mathbb{M}} \leq [\![\varepsilon'_0]\!]^{\eta,\rho}_{\mathbb{M}})}) \\ = \; & \mathsf{E}_\rho([\![\varepsilon'_0]\!]^{\eta,\rho}_{\mathbb{M}}(\mathsf{time}^\eta_{\mathcal{A}}, \mathsf{calls}^\eta_{\mathcal{A}})) + \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\neg([\![\varepsilon_0 \leq \varepsilon'_0]\!]^{\eta,\rho}_{\mathbb{M}})\right) \end{aligned}$$
Therefore, by the second premise, we have:
$$\left|\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\mathcal{A}^{[\![\vec{u}_1]\!]^{\eta,\rho}_{\mathbb{M}}}(1^\eta, [\![\vec{u}_0]\!]^{\eta,\rho}_{\mathbb{M}}, \rho_a)\right) - \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}\left(\mathcal{A}^{[\![\vec{v}_1]\!]^{\eta,\rho}_{\mathbb{M}}}(1^\eta, [\![\vec{v}_0]\!]^{\eta,\rho}_{\mathbb{M}}, \rho_a)\right)\right| \leq \mathsf{E}_\rho([\![\varepsilon'_0]\!]^{\eta,\rho}_{\mathbb{M}}(\mathsf{time}^\eta_{\mathcal{A}}, \mathsf{calls}^\eta_{\mathcal{A}})) + \mathsf{E}_\rho([\![\varepsilon_1]\!]^{\eta,\rho}_{\mathbb{M}}).$$
So, $\mathbb{M} \models \vec{u} \sim_{\varepsilon'_0+\varepsilon_1} \vec{v}$.

L. Induction Rules

- G$_\varepsilon$.INDUCTION:
Let $\mathbb{M}$ be a model such that $\mathbb{M} \models \Theta$.
Then by the first premise of the rule, we have that $\mathbb{M} \models \mathsf{well\text{-}founded}_\tau(<_\tau)$. So, we have that
$$\mathbb{M} \models [\forall(l : \mathsf{nat} \to \tau).\neg(\forall(i, j : \mathsf{nat}).i < j \to l\ j <_\tau l\ i)]_0$$
Therefore, since the interpretation of $<$ is always $<$, and the one of nat is $\mathbb{N}$,
$$\forall \eta \in \mathbb{N}, \forall \rho \in \mathbb{T}_{\mathbb{M},\eta}, \forall l \in \mathcal{F}(\mathbb{N}, [\![\tau]\!]^{\eta,\rho}_{\mathbb{M}}), \exists i \in [\![\tau]\!]^{\eta,\rho}_{\mathbb{M}}, \exists j \in [\![\tau]\!]^{\eta,\rho}_{\mathbb{M}}, i < j \wedge \neg(l\ j\ [\![<]\!]^{\eta,\rho}_{\mathbb{M}}\ l\ x)$$
Which exactly mean that for every η in $\mathbb{N}$ and every ρ in $\mathbb{T}_{\mathbb{M},\eta}$, $[\![<]\!]^{\eta,\rho}_{\mathbb{M}}$ is well-founded. Recall that $\mathbb{RV}(\tau)$ is the set of random variables over τ. (i.e $\mathbb{RV}(\tau)$ is equal to $\prod_{\eta\in\mathbb{N}}(\mathbb{T}_{\mathbb{M},\eta} \to [\![\tau]\!]^{\eta,\rho}_{\mathbb{M}})$).
Therefore we can define the order $<_{SPW}$ over $\mathbb{RV}(\tau)$ as such: for every X, Y in $\mathbb{RV}(\tau)$, $X <_{SPW} Y$, if and only if, $\forall \eta \in \mathbb{N}, \forall \rho \in \mathbb{T}_{\mathbb{M},\eta}, X_\eta(\rho)\ [\![<]\!]^{\eta,\rho}_{\mathbb{M}}\ Y_\eta(\rho)$. We can notice, that it is in fact an well-founded function when for every η in $\mathbb{N}$ and every ρ in $\mathbb{T}_{\mathbb{M},\eta}$, $[\![<]\!]^{\eta,\rho}_{\mathbb{M}}$ is also well-founded.

By the second premise, we have that

$$\mathbb{M} \models \tilde{\forall}(x : \tau).(\tilde{\forall}(y : \tau).\, [x <_\tau \; y]_0 \tilde{\Rightarrow} F\{x \mapsto y\}) \tilde{\Rightarrow} F$$

That give,

$$\forall X \in \mathbb{RV}(\tau), (\forall Y \in \mathbb{RV}(\tau).(\forall \eta \in \mathbb{N}, \forall \rho \in \mathbb{T}_{\mathbb{M},\eta}, X_\eta(\rho)\, [\![<]\!]_{\mathbb{M}}^{\eta,\rho}\, Y_\eta(\rho)) \Rightarrow [\![F]\!]_{\mathbb{M}}\mathbb{M}[x \mapsto Y]) \Rightarrow [\![F]\!]_{\mathbb{M}}$$

which is exactly the induction principle on $\mathbb{RV}(\tau)$ over the well-founded order $<_{SPW}$. Therefore, we have that $\forall X \in \mathbb{RV}(\tau).F$ holds, and this is exactly the conclusion of the rule.

- L_ε.INDUCTION:
  Let $\mathbb{M}$ be a model such that $\mathbb{M} \models \Theta$.
  Then by the first premise of the rule, we have that $\mathbb{M} \models \mathsf{well\text{-}founded}_\tau(<_\tau)$. So, we have that $\mathbb{M} \models \mathsf{det}(<_\tau)$. Therefore, there exists $(<_\eta)_{\eta\in\mathbb{N}}$ such that $\forall \eta \in \mathbb{N}, \forall \rho \in \mathbb{T}_{\mathbb{M},\eta}, [\![<_\tau]\!]_{\mathbb{M}}^{\eta,\rho} = <_\eta$.
  We also have that

  $$\mathbb{M} \models [\forall (l : \mathsf{nat} \to \tau).\neg(\forall (i, j : \mathsf{nat}).i < j \to l\; j <_\tau l\; i)]_0$$

  Therefore, since the interpretation of $<$ is always $<$, and the one of nat is $\mathbb{N}$,

  $$\forall \eta \in \mathbb{N}, \forall \rho \in \mathbb{T}_{\mathbb{M},\eta}, \forall l \in \mathcal{F}(\mathbb{N}, [\![\tau]\!]_{\mathbb{M}}^{\eta,\rho}), \exists i \in [\![\tau]\!]_{\mathbb{M}}^{\eta,\rho}, \exists j \in [\![\tau]\!]_{\mathbb{M}}^{\eta,\rho}, i < j \wedge \neg(l\; j <_\eta l\; x)$$

  Which exactly mean that for every η in $\mathbb{N}$, $<_\eta$ is well-founded.
  Let $\eta \in \mathbb{N}$, $\rho \in \mathbb{T}_{\mathbb{M},\eta}$ such that $[\![\wedge\Gamma]\!]_{\mathbb{M}}^{\eta,\rho} = 1$ and $[\![\forall(x : \tau).(\forall(y : \tau).(x <_\tau y) \Rightarrow \psi\{x \mapsto y\}) \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta,\rho} = 1$. Then, we have that $\forall x \in [\![\tau]\!]_{\mathbb{M}}^{\eta,\rho}.(\forall y \in [\![\tau]\!]_{\mathbb{M}}^{\eta,\rho}.(x <_\eta y) \Rightarrow ([\![\psi\{x \mapsto y\}]\!]_{\mathbb{M}}^{\eta,\rho} = 1)) \Rightarrow ([\![\psi]\!]_{\mathbb{M}}^{\eta,\rho} = 1)$. Which, by induction on $[\![\tau]\!]_{\mathbb{M}}^{\eta,\rho}$ over the well-founded order $<_\eta$ give that $\forall x \in [\![\tau]\!]_{\mathbb{M}}^{\eta,\rho}.\, [\![\psi]\!]_{\mathbb{M}}^{\eta,\rho} = 1$. Therefore we have that:

  $$[\![\wedge\Gamma \Rightarrow \forall(x : \tau).(\forall(y : \tau).(x <_\tau y) \Rightarrow \psi\{x \mapsto y\}) \Rightarrow \psi\}]\!]_{\mathbb{M}}^{\eta,\rho} = 1$$

  implies that:

  $$[\![\wedge\Gamma \Rightarrow \forall(x : \tau).\psi]\!]_{\mathbb{M}}^{\eta,\rho} = 1$$

  Which is equivalent to say that:

  $$\neg([\![\wedge\Gamma \Rightarrow \forall(x : \tau).\psi]\!]_{\mathbb{M}}^{\eta,\rho}) = 1$$

  which implies that:

  $$\neg([\![\wedge\Gamma \Rightarrow \forall(x : \tau).(\forall(y : \tau).(x <_\tau y) \Rightarrow \psi\{x \mapsto y\}) \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta,\rho}) = 1$$

  Which finally give that, for every η in $\mathbb{N}$:

  $$\begin{aligned}\mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg([\![\wedge\Gamma \Rightarrow \forall(x : \tau).\psi]\!]_{\mathbb{M}}^{\eta,\rho})) &\leq \mathsf{Pr}_{\rho\in\mathbb{T}_{\mathbb{M},\eta}}(\neg([\![\wedge\Gamma \Rightarrow \forall(x : \tau).(\forall(y : \tau).(x <_\tau y) \Rightarrow \psi\{x \mapsto y\}) \Rightarrow \psi]\!]_{\mathbb{M}}^{\eta,\rho}))\\ &\leq \mathsf{E}_\rho(\varepsilon)\end{aligned}$$

APPENDIX E
PROOF TRANSFORMATIONS: COMMUTATIONS

In this section, we present the detail of $\blacktriangleright_{\mathsf{AD}}$, which is constitued of the commutation of G_ε.E:CS$_\mathrm{R}$, G_ε.E:BI-DEDUCE and G.WEAK with:

- G_ε.E:REWRITE$_0$
- G_ε.E:FRESH
- The cryptographic rules : G_ε.PRF, G_ε.CCA1
- the rules in Fig. 10 in section left rules and the section local and global relations (except for G.L-$\tilde{\forall}$ and G_ε.L-LOC:$\vee$)
- G.CUT, G.DUP

We show the commutation in detail of G_ε.E:REWRITE$_0$, G_ε.E:FRESH and G_ε.CCA1. We don't show it for G_ε.PRF since it is almost identical to G_ε.CCA1. Same, the rest of the rules, we show some examples but not all of them since most of them are almost identical or with very little change.

We will use G.WEAK and G.DUP without mention it (except in the commutation of G.L-$\tilde{\wedge}$ and G_ε.E:CS as an example). Same with the use rule of the family of rewritting without error, we will not mention the equality we are rewritting for the sake of readability (except in the commutation of G_ε.E:REWRITE$_0$). . We also simplify quite a lot the expression of the upper-bound given by the G_ε.E:BI-DEDUCE rule in order to make the rules readable (see Appendix B-B for more details)

As for the $\blacktriangleright_{\mathsf{col}}$, we limit ourself the Fig. 14 since this level of detail is enough to see and be able to complete it. For a bit more detail, in most compicated collasping rule, the one with G.AXIOM and G_{ε}.E:CS$_{\mathsf{R}}$. The term at the conclusion is of the form

$$\vec{u}, \mathsf{if}\ b\ \vec{u}\ \mathsf{then}\ C\ \vec{u}\ \vec{n}\ \mathsf{else}\ C'\vec{u}\ \vec{n}'$$

(and the same thing with $\vec{v}$ on the other side of the equivalece), with the assumption that b, C and C' can be computed by the adversary form $\vec{u}$ in polynomial time. Then we can show that the term

$$\lambda\vec{x}\ \vec{y}.\mathsf{if}\ b\ \vec{x}\ \mathsf{then}\ C\ \vec{x}\ \vec{y}\ \mathsf{else}\ C'\ \vec{x}\ \vec{y}$$

can also be computed by the adversary in polynomial time. Therefore, we can collapse the case-study as shown in the sketch in Fig. 14

Commutation between $\mathrm{G}_\varepsilon.\mathrm{E{:}R{\scriptstyle EWRITE}}_0$ and the ascending rules

With $\mathrm{G}_\varepsilon.\mathrm{E{:}CS}_\mathrm{R}$

$$\dfrac{\dfrac{\dfrac{\Pi_0}{\mathbb{E};\Theta\vdash\vec{u}_0,\vec{v}_0\{s\}\sim_{\varepsilon_r\{s\}}\vec{u}_1,\vec{v}_1\{s\}}\quad\dfrac{\Pi_=}{\mathbb{E};\Theta\vdash[s=r]_0}}{\mathbb{E};\Theta\vdash\vec{u}_0,\vec{v}_0\{r\}\sim_{\varepsilon_r\{r\}}\vec{u}_1,\vec{v}_1\{r\}}\;\mathrm{G}_\varepsilon.\mathrm{E{:}REWRITE}_0\quad\dfrac{\Pi_1}{\mathbb{E};\Theta\vdash\vec{u}_0,\vec{w}_0\sim_{\varepsilon_l}\vec{u}_1,\vec{w}_1}\quad\dfrac{\Pi_C}{\mathbb{E};\Theta\vdash\mathsf{adv}_{t_C,\vec{\sigma}_C}(C)}\quad\dfrac{\Pi_l}{\mathsf{blen}_{\vec{l}}(\vec{u}_0)\,\tilde{\wedge}\,\mathsf{blen}_{\vec{l}}(\vec{u}_1)}}{\mathbb{E};\Theta\vdash\vec{u}_0,\mathsf{if}\ C\ \vec{u}_0\ \mathsf{then}\ \vec{v}_0\{r\}\ \mathsf{else}\ \vec{w}_0\sim_{\lambda t\vec{\sigma}.\varepsilon_r\{r\}(t+t_C)(\vec{\sigma}+\vec{\sigma}_C)+\varepsilon_l(t+t_C)(\vec{\sigma}+\vec{\sigma}_C)}\vec{u}_1,\mathsf{if}\ C\ \vec{u}_1\ \mathsf{then}\ \vec{v}_1\{r\}\ \mathsf{else}\ \vec{w}_1}\;\mathrm{G}_\varepsilon.\mathrm{E{:}CS}_\mathrm{R}$$

$$\blacktriangleright^{\mathrm{CS}}_{\mathrm{REWRITE}_0}$$

$$\dfrac{\dfrac{\dfrac{\Pi_0}{\mathbb{E};\Theta\vdash\vec{u}_0,\vec{v}_0\{s\}\sim_{\varepsilon_r\{s\}}\vec{u}_1,\vec{v}_1\{s\}}\quad\dfrac{\Pi_1}{\mathbb{E};\Theta\vdash\vec{u}_0,\vec{w}_0\sim_{\varepsilon_l}\vec{u}_1,\vec{w}_1}\quad\dfrac{\Pi_C}{\mathbb{E};\Theta\vdash\mathsf{adv}_{t_C,\vec{\sigma}_C}(C)}\quad\dfrac{\Pi_l}{\mathsf{blen}_{\vec{l}}(\vec{u}_0)\,\tilde{\wedge}\,\mathsf{blen}_{\vec{l}}(\vec{u}_1)}}{\mathbb{E};\Theta\vdash\vec{u}_0,\mathsf{if}\ C\ \vec{u}_0\ \mathsf{then}\ \vec{v}_0\{s\}\ \mathsf{else}\ \vec{w}_0\sim_{\lambda t\vec{\sigma}.\varepsilon_r\{s\}(t+t_C)(\vec{\sigma}+\vec{\sigma}_C)+\varepsilon_l(t+t_C)(\vec{\sigma}+\vec{\sigma}_C)}\vec{u}_1,\mathsf{if}\ C\ \vec{u}_1\ \mathsf{then}\ \vec{v}_1\{s\}\ \mathsf{else}\ \vec{w}_1}\;\mathrm{G}_\varepsilon.\mathrm{E{:}CS}_\mathrm{R}\quad\dfrac{\Pi_=}{\mathbb{E};\Theta\vdash[s=r]_0}}{\mathbb{E};\Theta\vdash\vec{u}_0,\mathsf{if}\ C\ \vec{u}_0\ \mathsf{then}\ \vec{v}_0\{r\}\ \mathsf{else}\ \vec{w}_0\sim_{\lambda t\vec{\sigma}.\varepsilon_r\{r\}(t+t_C)(\vec{\sigma}+\vec{\sigma}_C)+\varepsilon_l(t+t_C)(\vec{\sigma}+\vec{\sigma}_C)}\vec{u}_1,\mathsf{if}\ C\ \vec{u}_1\ \mathsf{then}\ \vec{v}_1\{r\}\ \mathsf{else}\ \vec{w}_1}\;\mathrm{G}_\varepsilon.\mathrm{E{:}REWRITE}_0$$

With $\mathrm{G}_\varepsilon.\mathrm{E{:}BI\text{-}DEDUCE}$

For lisibility reason, we don't show the derivation of ε along the transformation

$$\dfrac{\dfrac{\dfrac{\Pi_0}{\mathbb{E};\Theta\vdash\vec{w}_0,\vec{u}\{s\}\sim_{\varepsilon_0\{s\}}\vec{w}_1,\vec{v}\{s\}}\quad\dfrac{\Pi_=}{\mathbb{E};\Theta\vdash[s=r]_0}}{\mathbb{E};\Theta\vdash\vec{w}_0,\vec{u}\{r\}\sim_{\varepsilon_0\{r\}}\vec{w}_1,\vec{v}\{r\}}\;\mathrm{G}_\varepsilon.\mathrm{E{:}REWRITE}_0\quad\dfrac{\Pi_C}{\mathbb{E};\Theta\vdash\tilde{\bigwedge}_{1\le i\le n}\mathsf{adv}_{t_i,\vec{\sigma}_i}(C_i)}\quad\dfrac{\Pi_l}{\mathbb{E};\Theta\vdash\mathsf{blen}_{\vec{l}}(\vec{u}\{r\})\wedge\mathbb{E};\Theta\vdash\mathsf{blen}_{\vec{l}}(\vec{v}\{r\})}\quad\dfrac{\Pi_{l\vec{w}}}{\mathbb{E};\Theta\vdash\mathsf{blen}_{l\vec{w}}(\vec{w}_0)\wedge\mathbb{E};\Theta\vdash\mathsf{blen}_{l\vec{w}}(\vec{w}_1)}\quad\dfrac{\Pi_{l\vec{n}}}{\mathbb{E};\Theta\vdash\mathsf{blen}_{l\vec{n}}(\vec{n})}}{\mathbb{E};\Theta\vdash\vec{w}_0,(C_1,\dots,C_n)(\vec{w}_0,\vec{u}\{r\},\vec{n})\sim_{\varepsilon'\{r\}}\vec{w}_1,(C_1,\dots,C_n)(\vec{w}_1,\vec{v}\{r\},\vec{n})}\;\mathrm{G}_\varepsilon.\mathrm{E{:}BI\text{-}DEDUCE}$$

$$\blacktriangleright^{\mathrm{BI\text{-}DEDUCE}}_{\mathrm{REWRITE}_0}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\Pi_l}{\mathbb{E};\Theta\vdash\mathsf{blen}_{\vec{l}}(\vec{u}\{r\})\wedge\mathbb{E};\Theta\vdash\mathsf{blen}_{\vec{l}}(\vec{v}\{r\})}\quad\dfrac{\Pi_=}{\mathbb{E};\Theta\vdash[s=r]_0}}{\mathbb{E};\Theta\vdash\mathbb{E};\Theta\vdash\mathsf{blen}_{\vec{l}}(\vec{u}\{s\})\wedge\mathbb{E};\Theta\vdash\mathsf{blen}_{\vec{l}}(\vec{v}\{s\})}\;\mathrm{G}_\varepsilon.\mathrm{BLEN{:}REWRITE}_0\quad\dfrac{\Pi_0}{\mathbb{E};\Theta\vdash\vec{u}\{s\}\sim_{\varepsilon_0\{s\}}\vec{v}\{s\}}\quad\dfrac{\Pi_C}{\mathbb{E};\Theta\vdash\tilde{\bigwedge}_{1\le i\le n}\mathsf{adv}_{t_i,\vec{\sigma}_i}(C_i)}\quad\dfrac{\Pi_l}{\mathbb{E};\Theta\vdash\mathsf{blen}_{\vec{l}}(\vec{u}\{r\})\wedge\mathbb{E};\Theta\vdash\mathsf{blen}_{\vec{l}}(\vec{v}\{r\})}\quad\dfrac{\Pi_{l\vec{w}}}{\mathbb{E};\Theta\vdash\mathsf{blen}_{l\vec{w}}(\vec{w}_0)\wedge\mathbb{E};\Theta\vdash\mathsf{blen}_{l\vec{w}}(\vec{w}_1)}\quad\dfrac{\Pi_{l\vec{n}}}{\mathbb{E};\Theta\vdash\mathsf{blen}_{l\vec{n}}(\vec{n})}}{\mathbb{E};\Theta\vdash\vec{w}_0,(C_1,\dots,C_n)(\vec{w}_0,\vec{u}\{s\},\vec{n})\sim_{\varepsilon'\{s\}}\vec{w}_1,(C_1,\dots,C_n)(\vec{w}_1,\vec{v}\{s\},\vec{n})}\;\mathrm{G}_\varepsilon.\mathrm{E{:}BI\text{-}DEDUCE}\quad\dfrac{\Pi_=}{\mathbb{E};\Theta\vdash[s=r]_0}}{\mathbb{E};\Theta\vdash\vec{w}_0,(C_1,\dots,C_n)(\vec{w}_0,\vec{u}\{r\},\vec{n})\sim_{\varepsilon'\{r\}}\vec{w}_1,(C_1,\dots,C_n)(\vec{w}_1,\vec{v}\{r\},\vec{n})}\;\mathrm{G}_\varepsilon.\mathrm{E{:}REWRITE}_0$$

With $\mathrm{G.WEAK}$

$$\dfrac{\dfrac{\dfrac{\Pi_0}{\mathbb{E};\Theta_0\vdash\vec{u}\{s\}\sim_{\varepsilon\{s\}}\vec{v}\{s\}}\quad\dfrac{\Pi_=}{\mathbb{E};\Theta_0\vdash[s=r]_0}}{\mathbb{E};\Theta_0\vdash\vec{u}\{r\}\sim_{\varepsilon\{r\}}\vec{v}\{r\}}\;\mathrm{G}_\varepsilon.\mathrm{E{:}REWRITE}_0}{\mathbb{E};\Theta_0,\Theta_1\vdash\vec{u}\{r\}\sim_{\varepsilon\{r\}}\vec{v}\{r\}}\;\mathrm{G.WEAK}\quad\blacktriangleright^{\mathrm{WEAK}}_{\mathrm{REWRITE}_0}\quad\dfrac{\dfrac{\dfrac{\Pi_0}{\mathbb{E};\Theta_0\vdash\vec{u}\{s\}\sim_{\varepsilon\{s\}}\vec{v}\{s\}}}{\mathbb{E};\Theta_0,\Theta_1\vdash\vec{u}\{r\}\sim_{\varepsilon\{r\}}\vec{v}\{r\}}\;\mathrm{G.WEAK}\quad\dfrac{\dfrac{\Pi_=}{\mathbb{E};\Theta_0\vdash[s=r]_0}}{\mathbb{E};\Theta_0\vdash[s=r]_0}\;\mathrm{G.WEAK}}{\mathbb{E};\Theta_0,\Theta_1\vdash\vec{u}\{r\}\sim_{\varepsilon\{r\}}\vec{v}\{r\}}\;\mathrm{G}_\varepsilon.\mathrm{E{:}REWRITE}_0$$

Commutation between G_ε.E:FRESH and the ascending rules

We omit the commutation with G.WEAK *since it is exactly the kind as one with* G_ε.E:REWRITE$_0$ *where the* G.WEAK *is move upward in all the premises of* G_ε.E:FRESH

With G_ε.E:CS$_\mathrm{R}$

Since the auxilary proofs of case-study are not changed by the transformation, we don't write them, same thing for the upper-bound. And we also show the transformation for only one case-study since it is very similar with multiples case-studies.

$$\dfrac{\dfrac{\dfrac{\Pi_l}{\mathbb{E};\Theta \vdash \vec{u}_0, C(\mathsf{n_{fresh}}\ ()) \sim \vec{u}_1, v} \quad \dfrac{\Pi_\mathsf{n}}{\mathbb{E};\Theta \vdash \left[\phi^{\mathsf{n},i}_{\mathsf{fresh}}(\vec{u}_0, C(\mathsf{n_{fresh}}\ ())) \vee \phi^{\mathsf{n_{fresh}}}_{\mathsf{fresh}}(\vec{u}_0, C(\mathsf{n_{fresh}}\ ()))\right]}}{\mathbb{E};\Theta \vdash \vec{u}_0, C(\mathsf{n}\ i) \sim \vec{u}_1, v_1}\ \mathrm{G}_\varepsilon.\mathrm{E{:}FRESH} \quad \dfrac{\Pi_r}{\mathbb{E};\Theta \vdash \vec{u}_0, w_0 \sim \vec{u}_1, w_1}}{\mathbb{E};\Theta \vdash \vec{u}_0, \mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ C(\mathsf{n}\ i)\ \mathsf{else}\ w_0 \sim \vec{u}_1, \mathsf{if}\ b\ \vec{u}_1\ \mathsf{then}\ v\ \mathsf{else}\ w_1}\ \mathrm{G}_\varepsilon.\mathrm{E{:}CS_R}$$

$\blacktriangleright^{\mathrm{CS}}_{\mathrm{FRESH}}$

$$\dfrac{\dfrac{\dfrac{\Pi_l}{\mathbb{E};\Theta \vdash \vec{u}_0, C(\mathsf{n_{fresh}}\ ()) \sim \vec{u}_1, v} \quad \dfrac{\Pi_r}{\mathbb{E};\Theta \vdash \vec{u}_0, w_0 \sim \vec{u}_1, w_1}}{\mathbb{E};\Theta \vdash \vec{u}_0, \mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ C(\mathsf{n_{fresh}}\ ())\ \mathsf{else}\ w_0 \sim \vec{u}_1, \mathsf{if}\ b\ \vec{u}_1\ \mathsf{then}\ v\ \mathsf{else}\ w_1}\ \mathrm{G}_\varepsilon.\mathrm{E{:}CS_R} \quad \dfrac{\Pi_\mathsf{n}}{\mathbb{E};\Theta \vdash \begin{bmatrix}\phi^{\mathsf{n},i}_{\mathsf{fresh}}(\vec{u}_0, \mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ C(\mathsf{n_{fresh}}\ ())\ \mathsf{else}\ w_0) \\ \vee \\ \phi^{\mathsf{n_{fresh}}}_{\mathsf{fresh}}(\vec{u}_0, \mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ C(\mathsf{n_{fresh}}\ ())\ \mathsf{else}\ w_0)\end{bmatrix}}}{\mathbb{E};\Theta \vdash \vec{u}_0, \mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ C(\mathsf{n}\ i)\ \mathsf{else}\ w_0 \sim \vec{u}_1, \mathsf{if}\ b\ \vec{u}_1\ \mathsf{then}\ v\ \mathsf{else}\ w_1}\ \mathrm{G}_\varepsilon.\mathrm{E{:}FRESH}$$

Since we can take $b\ \vec{u}_0 \wedge \phi^{\mathsf{n},i}_{\mathsf{fresh}}(\vec{u}_0, C(\mathsf{n_{fresh}}\ ()))$for $\phi^{\mathsf{n},i}_{\mathsf{fresh}}(\vec{u}_0, \mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ C(\mathsf{n_{fresh}}\ ())\ \mathsf{else}\ w_0)$ (We assume that $\mathsf{n}\ i$ is always require for w_0) and $\neg(b\ \vec{u}_0) \vee \phi^{\mathsf{n_{fresh}},()}_{\mathsf{fresh}}(\vec{u}_0, C(\mathsf{n_{fresh}}\ ()))$ for $\phi^{\mathsf{n_{fresh}}}_{\mathsf{fresh}}(\vec{u}_0, \mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ C(\mathsf{n_{fresh}}\ ())\ \mathsf{else}\ w_0)$ (since $\mathsf{n_{fresh}}$ doesn't appear in w_0)

With G_ε.E:BI-DEDUCE

Since the upper-bound is not changed by the transformation, we don't write it. And we also show the transformation for only one context since it is very similar with multiples context. The added G_ε.E:REWRITE$_0$ *are on equality that hold immediately with* G.β

$$\dfrac{\dfrac{\dfrac{\Pi}{\mathbb{E};\Theta \vdash \vec{w}_0, \vec{u}, C(\mathsf{n_{fresh}}\ ()) \sim \vec{w}_0, \vec{v}, v_1} \quad \dfrac{\Pi_\mathsf{n}}{\mathbb{E};\Theta \vdash \left[\phi^{\mathsf{n},i}_{\mathsf{fresh}}(\vec{w}_0, \vec{u}, C(\mathsf{n_{fresh}}\ ())) \vee \phi^{\mathsf{n_{fresh}}}_{\mathsf{fresh}}(\vec{w}_0, \vec{u}, C(\mathsf{n_{fresh}}\ ()))\right]}}{\mathbb{E};\Theta \vdash \vec{u}, \vec{u}_0, C(\mathsf{n}\ i) \sim \vec{v}, \vec{v}_0, v_1}\ \mathrm{G}_\varepsilon.\mathrm{E{:}FRESH} \quad \dfrac{\Pi_D}{\mathbb{E};\Theta \vdash \mathsf{adv}_{t_D,\vec{\sigma}_D}(D)} \quad \dfrac{\Pi_{l\vec{w}}}{\mathbb{E};\Theta \vdash \mathsf{blen}_{l\vec{w}}(\vec{w}_0)\ \tilde{\wedge}\ \mathsf{blen}_{l\vec{w}}(\vec{w}_1)} \quad \dfrac{\Pi_l}{\mathbb{E};\Theta \vdash \mathsf{blen}_{\vec{l}}(\vec{u})\ \tilde{\wedge}\ \mathsf{blen}_{\vec{l}}(\vec{v})} \quad \dfrac{\Pi_n}{\mathbb{E};\Theta \vdash \mathsf{blen}_{l\vec{n}}(\vec{n})}}{\mathbb{E};\Theta \vdash \vec{w}_0, D\ \vec{w}_0\ \vec{u}\ (C(\mathsf{n}\ i))\ \vec{n} \sim \vec{w}_1, D\ \vec{w}_1\ \vec{v}\ v_1\ \vec{n}}\ \mathrm{G}_\varepsilon.\mathrm{E{:}BI\text{-}DEDUCE}$$

$\blacktriangleright^{\mathrm{BI\text{-}DEDUCE}}_{\mathrm{FRESH}}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Pi}{\mathbb{E};\Theta \vdash \vec{w}_0, \vec{u}, C(\mathsf{n_{fresh}}\ ()) \sim \vec{w}_0, \vec{v}, v_1} \quad \dfrac{\Pi_D}{\mathbb{E};\Theta \vdash \mathsf{adv}_{t_D,\vec{\sigma}_D}(D)} \quad \dfrac{\Pi_{l\vec{w}}}{\mathbb{E};\Theta \vdash \mathsf{blen}_{l\vec{w}}(\vec{w}_0)\ \tilde{\wedge}\ \mathsf{blen}_{l\vec{w}}(\vec{w}_1)} \quad \dfrac{\Pi_l}{\mathbb{E};\Theta \vdash \mathsf{blen}_{\vec{l}}(\vec{u})\ \tilde{\wedge}\ \mathsf{blen}_{\vec{l}}(\vec{v})} \quad \dfrac{\Pi_n}{\mathbb{E};\Theta \vdash \mathsf{blen}_{l\vec{n}}(\vec{n})}}{\mathbb{E};\Theta \vdash \vec{w}_0, D\ \vec{w}_0\ \vec{u}\ (C(\mathsf{n_{fresh}}\ ()))\ \vec{n} \sim \vec{w}_1, D\ \vec{w}_1\ \vec{v}\ v_1\ \vec{n}}\ \mathrm{G}_\varepsilon.\mathrm{E{:}BI\text{-}DEDUCE}}{\mathbb{E};\Theta \vdash \vec{w}_0, (\lambda x.D\ \vec{w}_0\ \vec{u}\ (C\ x)\ \vec{n})(\mathsf{n_{fresh}}\ ()) \sim \vec{w}_1, D\ \vec{w}_1\ \vec{v}\ v_1\ \vec{n}}\ \mathrm{G}_\varepsilon.\mathrm{E{:}REWRITE_0} \quad \dfrac{\Pi_\mathsf{n}}{\mathbb{E};\Theta \vdash \left[\phi^{\mathsf{n},i}_{\mathsf{fresh}}(\vec{w}_0, \vec{u}, (\lambda x.D\ \vec{w}_0\ \vec{u}\ (C\ x)\ \vec{n})(\mathsf{n_{fresh}}\ ())) \vee \phi^{\mathsf{n_{fresh}}}_{\mathsf{fresh}}(\vec{w}_0, \vec{u}, (\lambda x.D\ \vec{w}_0\ \vec{u}\ (C\ x)\ \vec{n})(\mathsf{n_{fresh}}\ ()))\right]}}{\mathbb{E};\Theta \vdash \vec{w}_0, (\lambda x.D\ \vec{w}_0\ \vec{u}\ (C\ x)\ \vec{n})(\mathsf{n}\ i) \sim \vec{w}_1, D\ \vec{w}_1\ \vec{v}\ v_1\ \vec{n}}\ \mathrm{G}_\varepsilon.\mathrm{E{:}FRESH}}{\mathbb{E};\Theta \vdash \vec{w}_0, D\ \vec{w}_0\ \vec{u}\ (C(\mathsf{n}\ i))\ \vec{n} \sim \vec{w}_1, D\ \vec{w}_1\ \vec{v}\ v_1\ \vec{n}}\ \mathrm{G}_\varepsilon.\mathrm{E{:}REWRITE_0}$$

Where the two freshness condition $\phi_{\mathsf{fresh}}()$ after transformation can be equal to those right before the transformation since D contains no name and $\mathsf{n_{fresh}}$ cannot appear in $\vec{n}$.

Commutation between $\mathrm{G}_{\varepsilon}.\mathrm{CCA1}$ and the ascending rules

With $\mathrm{G}_{\varepsilon}.\mathrm{E{:}CS}_{\mathsf{R}}$

We omit the auxilary proof obligation of $\mathrm{G}_{\varepsilon}.\mathrm{E{:}CS}_{\mathsf{R}}$ since there is no difficulty here (note that one of them is to prove that $\mathsf{adv}(b_0)$ which allows to derive the computation of $b_0\ u_0 \mathrel{\tilde\wedge} b$). We show the commutation with only one case-study, the case with multiple case-study is extremely similar. We also omit the details on the upper-bound. We show a case where $\vec{u}_0$ and $\vec{\alpha}$ are vector of terms of kind 1.

$$
\dfrac{
\dfrac{
\dfrac{\Pi_l}{\dfrac{\Pi_{\mathsf{len}}}{\dfrac{\dfrac{\Pi_i}{\mathbb{E};\Theta \vdash \mathsf{det}(i_\mathsf{r}) \mathrel{\tilde\wedge} \mathsf{det}(i_\mathsf{k})} \quad \dfrac{\dfrac{\Pi}{\mathbb{E};\Theta;\mathsf{\vec{a}} \vdash^{\mathsf{c}}_{t} \vec{u}_0, b, i_\mathsf{r}, i_\mathsf{k}, \vec{\alpha}} \quad \dfrac{\Pi_C}{\mathbb{E};\Theta;\mathsf{\vec{a}} \vdash^{\mathsf{c}}_{t_C,\vec{\sigma}_C} C} \quad \Pi_\phi}{\mathbb{E};\Theta;\emptyset \vdash_{\varepsilon_\psi} \phi^{\mathsf{k},i_\mathsf{k}}_{\mathsf{key}}(\vec{u}_0, b, i_\mathsf{r}, i_\mathsf{k}, \vec{\alpha}, C) \wedge \phi^{\mathsf{r},i_\mathsf{r}}_{\mathsf{rand}}(\vec{u}_0, b, i_\mathsf{r}, i_\mathsf{k}, \vec{\alpha}, C) \wedge \phi^{\mathsf{k},i_\mathsf{k}}_{\mathsf{dec}}(C)}}{\mathsf{blen}_l(\vec{a}, \mathsf{enc}\ m\ (\mathsf{r}\ i_\mathsf{r})\ (\mathsf{pk}(k\ i_\mathsf{k}))) \mathrel{\tilde\wedge} \mathsf{blen}_l(\vec{a}, \mathsf{enc}\ (0_{\mathsf{len}}\ m)\ (\mathsf{r}\ i_\mathsf{r})\ (\mathsf{pk}(k\ i_\mathsf{k})))}}}{\mathbb{E};\Theta \vdash \vec{u}_0, \mathsf{if}\ b\ \mathsf{then}\ C(\vec{a}, \mathsf{enc}\ (0_{\mathsf{len}}(m))\ (\mathsf{r}\ i_\mathsf{r})\ (\mathsf{pk}(k\ i_\mathsf{k})))\ \mathsf{else}\ v_0 \sim_{\varepsilon_l} \vec{u}_1, v_1}
}{\mathbb{E};\Theta \vdash \vec{u}_0, \mathsf{if}\ b\ \mathsf{then}\ C(\vec{a}, \mathsf{enc}\ m\ (\mathsf{r}\ i_\mathsf{r})\ (\mathsf{pk}(k\ i_\mathsf{k})))\ \mathsf{else}\ v_0 \sim_{\varepsilon_r+\varepsilon_{\mathrm{CCA}_1}+\varepsilon_{\mathrm{aux}}} \vec{u}_1, v_1}\ \mathrm{G}_{\varepsilon}.\mathrm{CCA1}
\quad
\dfrac{\Pi_r}{\mathbb{E};\Theta \vdash \vec{u}_0, w_0 \sim_{\varepsilon_r} \vec{u}_1, w_1}
}{\mathbb{E};\Theta \vdash \vec{u}_0, \mathsf{if}\ b_0\ \vec{u}_0\ \mathsf{then}\ \mathsf{if}\ b\ \mathsf{then}\ C(\vec{a}, \mathsf{enc}\ m\ (\mathsf{r}\ i_\mathsf{r})\ (\mathsf{pk}(k\ i_\mathsf{k})))\ \mathsf{else}\ v_0\ \mathsf{else}\ w_0 \sim_{\varepsilon_r+\varepsilon_{\mathrm{CCA}_1}+\varepsilon_{\mathrm{aux}}+\varepsilon_l} \vec{u}_1, \mathsf{if}\ b_0\ \vec{u}_1\ \mathsf{then}\ v_1\ \mathsf{else}\ w_1}\ \mathrm{G}_{\varepsilon}.\mathrm{E{:}CS}_{\mathsf{R}}
$$

$$\blacktriangleright^{\mathrm{CS}}_{\mathrm{CCA1}}$$

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{\Pi_l}{\mathbb{E};\Theta \vdash \vec{u}_0, \mathsf{if}\ b\ \mathsf{then}\ C(\vec{a}, \mathsf{enc}\ (0_{\mathsf{len}}(m))\ (\mathsf{r}\ i_\mathsf{r})\ (\mathsf{pk}(k\ i_\mathsf{k})))\ \mathsf{else}\ v_0 \sim_{\varepsilon'_l} \vec{u}_1, v_1}
\quad
\dfrac{\Pi_r}{\mathbb{E};\Theta \vdash \vec{u}_0, w_0 \sim_{\varepsilon'_r} \vec{u}_1, w_1}
}{\mathbb{E};\Theta \vdash \vec{u}_0, \mathsf{if}\ b_0\ \vec{u}_0\ \mathsf{then}\ \mathsf{if}\ b\ \mathsf{then}\ C(\vec{a}, \mathsf{enc}\ (0_{\mathsf{len}} m)\ (\mathsf{r}\ i_\mathsf{r})\ (\mathsf{pk}(k\ i_\mathsf{k})))\ \mathsf{else}\ v_0\ \mathsf{else}\ w_0 \sim_{\varepsilon'_r+\varepsilon'_l} \vec{u}_1, \mathsf{if}\ b_0\ \vec{u}_0\ \mathsf{then}\ v_1\ \mathsf{else}\ w_1}\ \mathrm{G}_{\varepsilon}.\mathrm{E{:}CS}_{\mathsf{R}}
}{\mathbb{E};\Theta \vdash \vec{u}_0, \mathsf{if}\ b_0\ \vec{u}_0 \wedge b\ \mathsf{then}\ C(\vec{a}, \mathsf{enc}\ (0_{\mathsf{len}} m)\ (\mathsf{r}\ i_\mathsf{r})\ (\mathsf{pk}(k\ i_\mathsf{k})))\ \mathsf{else}\ \mathsf{if}\ b\ \mathsf{then}\ v_0\ \mathsf{else}\ w_0 \sim_{\varepsilon'_r+\varepsilon'_l} \vec{u}_1, \mathsf{if}\ b_0\ \vec{u}_0\ \mathsf{then}\ v_1\ \mathsf{else}\ w_1}\ \mathrm{G}_{\varepsilon}.\mathrm{E{:}R{\small EWRITE}}_0
\quad
\dfrac{\Pi_{\mathsf{len}}}{\dfrac{\dfrac{\Pi_i}{\mathbb{E};\Theta \vdash \mathsf{det}(i_\mathsf{r}) \mathrel{\tilde\wedge} \mathsf{det}(i_\mathsf{k})} \quad \dfrac{\dfrac{\Pi'}{\mathbb{E};\Theta;\mathsf{\vec{a}} \vdash^{\mathsf{c}}_{t'} \vec{u}_0, b_0\ \vec{u}_0 \wedge b, i_\mathsf{r}, i_\mathsf{k}, \vec{\alpha}} \quad \dfrac{\Pi_C}{\mathbb{E};\Theta;\mathsf{\vec{a}} \vdash^{\mathsf{c}}_{t_C,\vec{\sigma}_C} C} \quad \Pi_\phi}{\mathbb{E};\Theta;\emptyset \vdash_{\varepsilon_\psi} \phi^{\mathsf{k},i_\mathsf{k}}_{\mathsf{key}}(\vec{u}_0, b_0\ \vec{u}_0 \wedge b, i_\mathsf{r}, i_\mathsf{k}, \vec{\alpha}, C) \wedge \phi^{\mathsf{r},i_\mathsf{r}}_{\mathsf{rand}}(\vec{u}_0, b_0\ \vec{u}_0 \wedge b, i_\mathsf{r}, i_\mathsf{k}, \vec{\alpha}, C) \wedge \phi^{\mathsf{k},i_\mathsf{k}}_{\mathsf{dec}}(C)}}{\mathsf{blen}_l(\vec{a}, \mathsf{enc}\ m\ (\mathsf{r}\ i_\mathsf{r})\ (\mathsf{pk}(k\ i_\mathsf{k}))) \mathrel{\tilde\wedge} \mathsf{blen}_l(\vec{a}, \mathsf{enc}\ (0_{\mathsf{len}}\ m)\ (\mathsf{r}\ i_\mathsf{r})\ (\mathsf{pk}(k\ i_\mathsf{k})))}}
}{\mathbb{E};\Theta \vdash \vec{u}_0, \mathsf{if}\ b_0\ \vec{u}_0 \wedge b\ \mathsf{then}\ C(\vec{a}, \mathsf{enc}\ m\ (\mathsf{r}\ i_\mathsf{r})\ (\mathsf{pk}(k\ i_\mathsf{k})))\ \mathsf{else}\ \mathsf{if}\ b\ \mathsf{then}\ v_0\ \mathsf{else}\ w_0 \sim_{\varepsilon'_r+\varepsilon'_{\mathrm{CCA}_1}+\varepsilon'_{\mathrm{aux}}+\varepsilon'_l} \vec{u}_1, \mathsf{if}\ b_0\ \vec{u}_1\ \mathsf{then}\ v_1\ \mathsf{else}\ w_1}\ \mathrm{G}_{\varepsilon}.\mathrm{CCA1}
}{\mathbb{E};\Theta \vdash \vec{u}_0, \mathsf{if}\ b_0\ \vec{u}_0\ \mathsf{then}\ \mathsf{if}\ b\ \mathsf{then}\ C(\vec{a}, \mathsf{enc}\ m\ (\mathsf{r}\ i_\mathsf{r})\ (\mathsf{pk}(k\ i_\mathsf{k})))\ \mathsf{else}\ v_0\ \mathsf{else}\ w_0 \sim_{\varepsilon'_r+\varepsilon'_{\mathrm{CCA}_1}+\varepsilon'_{\mathrm{aux}}+\varepsilon'_l} \vec{u}_1, \mathsf{if}\ b_0\ \vec{u}_0\ \mathsf{then}\ v_1\ \mathsf{else}\ w_1}\ \mathrm{G}_{\varepsilon}.\mathrm{E{:}R{\small EWRITE}}_0
$$

The commutation between $\mathrm{G}_{\varepsilon}.\mathrm{CCA1}$ and $\mathrm{G}_{\varepsilon}.\mathrm{E{:}B{\small I}\text{-}D{\small EDUCE}}$ is quite similar, the main point is that we can change

$$D\vec{u}\ \vec{u}_0\ \mathsf{if}\ b\ \mathsf{then}\ C(\vec{a}, \mathsf{enc}\ m\ (\mathsf{r}\ i_\mathsf{r})\ (\mathsf{pk}(k\ i_\mathsf{k})))\ \mathsf{else}\ v_0\vec{n}$$

(where D is the context for the $\mathrm{G}_{\varepsilon}.\mathrm{E{:}B{\small I}\text{-}D{\small EDUCE}}$ rule) to

$$(\lambda\vec{x}\ \vec{y}\ \vec{z}\ h.(D\ \vec{x}\ \vec{y}\ \vec{z}\ h\ \vec{n}))\vec{u}\ \vec{u}_0\ \vec{\alpha}\ \mathsf{enc}\ m\ (\mathsf{r}\ i_\mathsf{r})\ (\mathsf{pk}(k\ i_\mathsf{k}))$$

with $\mathrm{G}_{\varepsilon}.\mathrm{E{:}R{\small EWRITE}}_0$ and that if we have $\mathbb{E};\Theta;\mathsf{\vec{a}} \vdash^{\mathsf{c}}_{t_C,\vec{\sigma}_C} C$ and $\mathbb{E};\Theta \vdash \mathsf{adv}_{t,\vec{\sigma}}()$ with all the annotation being polynomial (see Appendix C-E for a exact definition) then we can deduce that $\mathbb{E};\Theta;\mathsf{\vec{a}} \vdash^{\mathsf{c}}_{t',\vec{\sigma}'} \lambda\vec{x}\ \vec{y}\ \vec{z}\ h.(D\ \vec{x}\ \vec{y}\ \vec{z}\ h\ \vec{n})$ with t' and $\vec{\sigma}'$ also polynomial. And the $\phi_{\mathsf{key}}()$,$\phi_{\mathsf{rand}}()$,$\phi_{\mathsf{dec}}()$ are still valid for this new context since D is without names and $\vec{n}$ are names that do not appear in the rest of the terms. Therefore, any occcurences of k or r in this new context can only come from C and are thus already taken care off by the previous conditions.

We omit the commutation with $\mathrm{G}.\mathrm{W{\small EAK}}$ since it is similar to every other commutation of $\mathrm{G}.\mathrm{W{\small EAK}}$ but with more auxilary proofs.

Commutation between G.L-$\tilde\exists$ and the ascending rules

With G_ε.E:CS$_\mathrm{R}$

Since the auxilary proofs of case-study are changed by the transformation exactly as the other branch, we don't write them. We also omit the upper-bound And we also show the transformation for only one case-study since it is very similar with multiples case-studies.

$$\dfrac{\dfrac{\dfrac{\Pi_l}{\mathbb{E}, x:\tau; \Theta, F \vdash \vec{u}_0, v_0 \sim \vec{u}_1, v_1}}{\mathbb{E}; \Theta, \tilde{\exists}(x:\tau).F \vdash \vec{u}_0, v_0 \sim \vec{u}_1, v_1}\ \text{G.L-}\tilde{\exists} \qquad \dfrac{\Pi_r}{\mathbb{E}; \Theta, \tilde{\exists}(x:\tau).F \vdash \vec{u}_0, w_0 \sim \vec{u}_1, w_1}}{\mathbb{E}; \Theta, \tilde{\exists}(x:\tau).F \vdash \vec{u}_0, \mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ v_0\ \mathsf{else}\ w_0 \sim \vec{u}_1, \mathsf{if}\ b\ \vec{u}_1\ \mathsf{then}\ v_1\ \mathsf{else}\ w_1}\ \mathrm{G}_\varepsilon\text{.E:CS}_\mathrm{R} \qquad \blacktriangleright^{\mathrm{CS}}_{\tilde{\exists}}$$

$$\dfrac{\dfrac{\dfrac{\Pi_l}{\mathbb{E}, x:\tau; \Theta, F \vdash \vec{u}_0, v_0 \sim \vec{u}_1, v_1} \qquad \dfrac{\Pi_r}{\mathbb{E}; \Theta, \tilde{\exists}(x:\tau).F \vdash \vec{u}_0, w_0 \sim \vec{u}_1, w_1}}{\mathbb{E}, x:\tau; \Theta, \tilde{\exists}(y:\tau).F, F \vdash \vec{u}_0, \mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ v_0\ \mathsf{else}\ w_0 \sim \vec{u}_1, \mathsf{if}\ b\ \vec{u}_1\ \mathsf{then}\ v_1\ \mathsf{else}\ w_1}\ \mathrm{G}_\varepsilon\text{.E:CS}_\mathrm{R}}{\mathbb{E}; \Theta, \tilde{\exists}(x:\tau).F \vdash \vec{u}_0, \mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ v_0\ \mathsf{else}\ w_0 \sim \vec{u}_1, \mathsf{if}\ b\ \vec{u}_1\ \mathsf{then}\ v_1\ \mathsf{else}\ w_1}\ \text{G.L-}\tilde{\exists}$$

With G_ε.E:Bi-Deduce

$$\dfrac{\dfrac{\dfrac{\Pi}{\mathbb{E}, (x:\tau); \Theta, F \vdash \vec{u} \sim_\varepsilon \vec{v}}}{\mathbb{E}; \Theta, \tilde{\exists}(x:\tau).F \vdash \vec{u} \sim_\varepsilon \vec{v}}\ \text{G.L-}\tilde{\exists} \quad \dfrac{\Pi_C}{\mathbb{E}; \Theta, \tilde{\exists}(x:\tau).F \vdash \tilde{\bigwedge}_{i \le n} \mathsf{adv}_{t_i, \vec{o}_i}(C_i)} \quad \dfrac{\Pi_w}{\mathbb{E}; \Theta, \tilde{\exists}(x:\tau).F \vdash \mathsf{blen}_{l^{\vec{w}}}(\vec{w}_0)\ \tilde{\wedge}\ \mathsf{blen}_{l^{\vec{w}}}(\vec{w}_1)} \quad \dfrac{\Pi_a}{\mathbb{E}; \Theta, \tilde{\exists}(x:\tau).F \vdash \mathsf{blen}_{\vec{l}}(\vec{u})\ \tilde{\wedge}\ \mathsf{blen}_{\vec{l}}(\vec{v})} \quad \dfrac{\Pi_\mathsf{n}}{\mathbb{E}; \Theta, \tilde{\exists}(x:\tau).F \vdash \mathsf{blen}_{l^{\vec{n}}}(\mathsf{n})}}{\mathbb{E}; \Theta, \tilde{\exists}(x:\tau).F \vdash \vec{w}_0, (C_1, \ldots, C_n)\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}} \sim_{\varepsilon'} \vec{w}_1, (C_1, \ldots, C_n)\ \vec{w}_1\ \vec{v}\ \vec{\mathsf{n}}}\ \mathrm{G}_\varepsilon\text{.E:Bi-Deduce}$$

$$\blacktriangleright^{\text{Bi-Deduce}}_{\tilde{\exists}} \qquad \dfrac{\dfrac{\dfrac{\Pi}{\mathbb{E}, (x:\tau); \Theta, F \vdash \vec{u} \sim_\varepsilon \vec{v}} \quad \dfrac{\Pi_w}{\mathbb{E}; \Theta, \tilde{\exists}(x:\tau).F \vdash \mathsf{blen}_{l^{\vec{w}}}(\vec{w}_0)\ \tilde{\wedge}\ \mathsf{blen}_{l^{\vec{w}}}(\vec{w}_1)} \quad \dfrac{\Pi_a}{\mathbb{E}; \Theta, \tilde{\exists}(x:\tau).F \vdash \mathsf{blen}_{\vec{l}}(\vec{u})\ \tilde{\wedge}\ \mathsf{blen}_{\vec{l}}(\vec{v})} \quad \dfrac{\Pi_\mathsf{n}}{\mathbb{E}; \Theta, \tilde{\exists}(x:\tau).F \vdash \mathsf{blen}_{l^{\vec{n}}}(\mathsf{n})}}{\mathbb{E}, (x:\tau); \Theta, \tilde{\exists}(y:\tau).F, F \vdash \vec{w}_0, (C_1, \ldots, C_n)\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}} \sim_{\varepsilon'} \vec{w}_1, (C_1, \ldots, C_n)\ \vec{w}_1\ \vec{v}\ \vec{\mathsf{n}}}\ \mathrm{G}_\varepsilon\text{.E:Bi-Deduce}}{\mathbb{E}; \Theta, \tilde{\exists}(x:\tau).F \vdash \vec{w}_0, (C_1, \ldots, C_n)\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}} \sim_{\varepsilon'} \vec{w}_1, (C_1, \ldots, C_n)\ \vec{w}_1\ \vec{v}\ \vec{\mathsf{n}}}\ \text{G.L-}\tilde{\wedge}$$

With G.Weak

$$\dfrac{\dfrac{\dfrac{\Pi}{\mathbb{E}, (x:\tau); \Theta_0, F \vdash F_0}}{\mathbb{E}; \Theta_0, \tilde{\exists}(x:\tau).F \vdash F_0}\ \text{G.L-}\tilde{\exists}}{\mathbb{E}; \Theta_0, \tilde{\exists}(x:\tau).F, \Theta_1 \vdash F_0}\ \text{G.Weak} \qquad \blacktriangleright^{\text{Weak}}_{\tilde{\exists}} \qquad \dfrac{\dfrac{\dfrac{\Pi}{\mathbb{E}, (x:\tau); \Theta_0, F \vdash F_0}}{\mathbb{E}, (x:\tau); \Theta_0, F, \Theta_1 \vdash F_0}\ \text{G.Weak}}{\mathbb{E}; \Theta_0, \tilde{\exists}(x:\tau).F, \Theta_1 \vdash F_0}\ \text{G.L-}\tilde{\exists}$$

Commutation between $\mathbf{G.L\text{-}\tilde{\wedge}}$ and the ascending rules

With $\mathbf{G_\varepsilon.E{:}CS_R}$

Since the auxilary proofs of case-study are changed by the transformation exactly as the other branch, we don't write them. We also omit the upper-bound And we also show the transformation for only one case-study since it is very similar with multiples case-studies.

$$\dfrac{\dfrac{\dfrac{\Pi_l}{\mathbb{E};\Theta,F_0,F_1 \vdash \vec{u}_0,v_0 \sim \vec{u}_1,v_1}}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1 \vdash \vec{u}_0,v_0 \sim \vec{u}_1,v_1}\ \text{G.L-}\tilde{\wedge} \qquad \dfrac{\Pi_r}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1 \vdash \vec{u}_0,w_0 \sim \vec{u}_1,w_1}}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1 \vdash \vec{u}_0,\mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ v_0\ \mathsf{else}\ w_0 \sim \vec{u}_1,\mathsf{if}\ b\ \vec{u}_1\ \mathsf{then}\ v_1\ \mathsf{else}\ w_1}\ \text{G}_\varepsilon.\text{E:CS}_\text{R} \qquad \blacktriangleright^{\text{CS}}_{\tilde{\wedge}}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Pi_l}{\mathbb{E};\Theta,F_0,F_1 \vdash \vec{u}_0,v_0 \sim \vec{u}_1,v_1}}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1,F_0,F_1 \vdash \vec{u}_0,v_0 \sim \vec{u}_1,v_1}\ \text{G.Weak} \qquad \dfrac{\dfrac{\Pi_r}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1 \vdash \vec{u}_0,w_0 \sim \vec{u}_1,w_1}}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1,F_0,F_1 \vdash \vec{u}_0,w_0 \sim \vec{u}_1,w_1}\ \text{G.Weak}}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1,F_0,F_1 \vdash \vec{u}_0,\mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ v_0\ \mathsf{else}\ w_0 \sim \vec{u}_1,\mathsf{if}\ b\ \vec{u}_1\ \mathsf{then}\ v_1\ \mathsf{else}\ w_1}\ \text{G}_\varepsilon.\text{E:CS}_\text{R}}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1,F_0\,\tilde{\wedge}\,F_1 \vdash \vec{u}_0,\mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ v_0\ \mathsf{else}\ w_0 \sim \vec{u}_1,\mathsf{if}\ b\ \vec{u}_1\ \mathsf{then}\ v_1\ \mathsf{else}\ w_1}\ \text{G.L-}\tilde{\wedge}}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1 \vdash \vec{u}_0,\mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ v_0\ \mathsf{else}\ w_0 \sim \vec{u}_1,\mathsf{if}\ b\ \vec{u}_1\ \mathsf{then}\ v_1\ \mathsf{else}\ w_1}\ \text{G.Dup}$$

With $\mathbf{G_\varepsilon.E{:}Bi\text{-}Deduce}$

$$\dfrac{\dfrac{\dfrac{\Pi}{\mathbb{E};\Theta,F_0,F_1 \vdash \vec{u} \sim_\varepsilon \vec{v}}}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1 \vdash \vec{u} \sim_\varepsilon \vec{v}}\ \text{G.L-}\tilde{\wedge} \qquad \dfrac{\Pi_C}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1 \vdash \tilde{\bigwedge}_{i\le n}\mathsf{adv}_{t_i,\vec{o}_i}(C_i)} \qquad \dfrac{\Pi_w}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1 \vdash \mathsf{blen}_{l_{\vec{w}}}(\vec{w}_0)\,\tilde{\wedge}\,\mathsf{blen}_{l_{\vec{w}}}(\vec{w}_1)} \qquad \dfrac{\Pi_a}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1 \vdash \mathsf{blen}_{\vec{l}}(\vec{u})\,\tilde{\wedge}\,\mathsf{blen}_{\vec{l}}(\vec{v})} \qquad \dfrac{\Pi_\mathsf{n}}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1 \vdash \mathsf{blen}_{l_{\vec{n}}}(\mathsf{n})}}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1 \vdash \vec{w}_0,(C_1,\dots,C_n)\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}} \sim_{\varepsilon'} \vec{w}_1,(C_1,\dots,C_n)\ \vec{w}_1\ \vec{v}\ \vec{\mathsf{n}}}\ \text{G}_\varepsilon.\text{E:Bi-Deduce}$$

$$\blacktriangleright^{\text{Bi-Deduce}}_{\tilde{\wedge}}$$

$$\dfrac{\dfrac{\dfrac{\Pi}{\mathbb{E};\Theta,F_0,F_1 \vdash \vec{u} \sim_\varepsilon \vec{v}} \qquad \dfrac{\Pi_C}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1 \vdash \tilde{\bigwedge}_{i\le n}\mathsf{adv}_{t_i,\vec{o}_i}(C_i)} \qquad \dfrac{\Pi_w}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1 \vdash \mathsf{blen}_{l_{\vec{w}}}(\vec{w}_0)\,\tilde{\wedge}\,\mathsf{blen}_{l_{\vec{w}}}(\vec{w}_1)} \qquad \dfrac{\Pi_a}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1 \vdash \mathsf{blen}_{\vec{l}}(\vec{u})\,\tilde{\wedge}\,\mathsf{blen}_{\vec{l}}(\vec{v})} \qquad \dfrac{\Pi_\mathsf{n}}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1 \vdash \mathsf{blen}_{l_{\vec{n}}}(\mathsf{n})}}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1,F_0,F_1 \vdash \vec{w}_0,(C_1,\dots,C_n)\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}} \sim_{\varepsilon'} \vec{w}_1,(C_1,\dots,C_n)\ \vec{w}_1\ \vec{v}\ \vec{\mathsf{n}}}\ \text{G}_\varepsilon.\text{E:Bi-Deduce}}{\mathbb{E};\Theta,F_0\,\tilde{\wedge}\,F_1 \vdash \vec{w}_0,(C_1,\dots,C_n)\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}} \sim_{\varepsilon'} (C_1,\dots,C_n)\ \vec{w}_0\ \vec{v}\ \vec{\mathsf{n}}}\ \text{G.L-}\tilde{\wedge}$$

With $\mathbf{G.Weak}$

$$\dfrac{\dfrac{\dfrac{\Pi}{\mathbb{E};\Theta_0,F_0,F_1 \vdash F}}{\mathbb{E};\Theta_0,F_0\,\tilde{\wedge}\,F_1 \vdash F}\ \text{G.L-}\tilde{\wedge}}{\mathbb{E};\Theta_0,F_0\,\tilde{\wedge}\,F_1,\Theta_1 \vdash F}\ \text{G.Weak} \qquad \blacktriangleright^{\text{Weak}}_{\tilde{\wedge}} \qquad \dfrac{\dfrac{\dfrac{\Pi}{\mathbb{E};\Theta_0,F_0,F_1 \vdash F}}{\mathbb{E};\Theta_0,F_0,F_1,\Theta_1 \vdash F}\ \text{G.Weak}}{\mathbb{E};\Theta_0,F_0\,\tilde{\wedge}\,F_1,\Theta_1 \vdash F}\ \text{G.L-}\tilde{\wedge}$$

Commutation between G.Cut and the ascending rules

Since the auxilary proofs of case-study are changed by the transformation exactly as the other branch, we don't write them. We also omit the upper-bound And we also show the transformation for only one case-study since it is very similar with multiples case-studies.

$$\dfrac{\dfrac{\dfrac{\Pi_c}{\mathbb{E};\Theta\vdash F}\quad \dfrac{\Pi_l}{\mathbb{E};\Theta,F\vdash \vec{u}_0,v_0\sim\vec{u}_1,v_1}}{\mathbb{E};\Theta\vdash\vec{u}_0,v_0\sim\vec{u}_1,v_1}\,\text{G.Cut}\quad \dfrac{\Pi_r}{\mathbb{E};\Theta\vdash \vec{u}_0,w_0\sim\vec{u}_1,w_1}}{\mathbb{E};\Theta\vdash \vec{u}_0,\mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ v_0\ \mathsf{else}\ w_0\sim \vec{u}_1,\mathsf{if}\ b\ \vec{u}_1\ \mathsf{then}\ v_1\ \mathsf{else}\ w_1}\,\text{G}_\varepsilon\text{.E:CS}_\text{R}\qquad \blacktriangleright^{\text{CS}}_{\text{Cut}}$$

$$\dfrac{\dfrac{\Pi_c}{\mathbb{E};\Theta\vdash F}\quad \dfrac{\dfrac{\Pi_l}{\mathbb{E};\Theta,F\vdash \vec{u}_0,v_0\sim\vec{u}_1,v_1}\quad\dfrac{\Pi_r}{\mathbb{E};\Theta\vdash \vec{u}_0,w_0\sim\vec{u}_1,w_1}}{\mathbb{E};\Theta,F\vdash \vec{u}_0,\mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ v_0\ \mathsf{else}\ w_0\sim \vec{u}_1,\mathsf{if}\ b\ \vec{u}_1\ \mathsf{then}\ v_1\ \mathsf{else}\ w_1}\,\text{G}_\varepsilon\text{.E:CS}_\text{R}}{\mathbb{E};\Theta\vdash \vec{u}_0,\mathsf{if}\ b\ \vec{u}_0\ \mathsf{then}\ v_0\ \mathsf{else}\ w_0\sim_{\varepsilon_l+\varepsilon_r} \vec{u}_1,\mathsf{if}\ b\ \vec{u}_1\ \mathsf{then}\ v_1\ \mathsf{else}\ w_1}\,\text{G.Cut}$$

With G_ε.E:Bi-Deduce

$$\dfrac{\dfrac{\Pi_F}{\mathbb{E};\Theta\vdash F}\quad\dfrac{\Pi}{\mathbb{E};\Theta,F\vdash\vec{u}\sim_\varepsilon\vec{v}}}{\mathbb{E};\Theta\vdash\vec{u}\sim_\varepsilon\vec{v}}\,\text{G.Cut}$$

$$\dfrac{\dfrac{\Pi_C}{\mathbb{E};\Theta\vdash\tilde{\bigwedge}_{i\le n}\mathsf{adv}_{t_i,\vec{\sigma}_i}(C_i)}\quad\dfrac{\Pi_w}{\mathbb{E};\Theta\vdash,\mathsf{blen}_{l^{\vec{w}}}(\vec{w}_0)\,\tilde{\wedge}\,\mathsf{blen}_{l^{\vec{w}}}(\vec{w}_1)}\quad\dfrac{\Pi_a}{\mathbb{E};\Theta\vdash,\mathsf{blen}_{\vec{l}}(\vec{u})\,\tilde{\wedge}\,\mathsf{blen}_{\vec{l}}(\vec{v})}\quad\dfrac{\Pi_{\mathsf{n}}}{\mathbb{E};\Theta\vdash\mathsf{blen}_{l^{\vec{n}}}(\mathsf{n})}}{\mathbb{E};\Theta\vdash\vec{w}_0,(C_1,\dots,C_n)\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}}\sim_{\varepsilon'}\vec{w}_1,(C_1,\dots,C_n)\ \vec{w}_1\ \vec{v}\ \vec{\mathsf{n}}}\,\text{G}_\varepsilon\text{.E:Bi-Deduce}$$

$$\blacktriangleright^{\text{Bi-Deduce}}_{\text{Cut}}$$

$$\dfrac{\dfrac{\Pi_F}{\mathbb{E};\Theta\vdash F}\quad\dfrac{\dfrac{\Pi}{\mathbb{E};\Theta,F\vdash\vec{u}\sim_\varepsilon\vec{v}}\quad\dfrac{\Pi_C}{\mathbb{E};\Theta\vdash\tilde{\bigwedge}_{i\le n}\mathsf{adv}_{t_i,\vec{\sigma}_i}(C_i)}\quad\dfrac{\Pi_w}{\mathbb{E};\Theta\vdash,\mathsf{blen}_{l^{\vec{w}}}(\vec{w}_0)\,\tilde{\wedge}\,\mathsf{blen}_{l^{\vec{w}}}(\vec{w}_1)}\quad\dfrac{\Pi_a}{\mathbb{E};\Theta\vdash,\mathsf{blen}_{\vec{l}}(\vec{u})\,\tilde{\wedge}\,\mathsf{blen}_{\vec{l}}(\vec{v})}\quad\dfrac{\Pi_{\mathsf{n}}}{\mathbb{E};\Theta\vdash\mathsf{blen}_{l^{\vec{n}}}(\mathsf{n})}}{\mathbb{E};\Theta,F\vdash\vec{w}_0,(C_1,\dots,C_n)\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}}\sim_{\varepsilon'}\vec{w}_1,(C_1,\dots,C_n)\ \vec{w}_1\ \vec{v}\ \vec{\mathsf{n}}}\,\text{G}_\varepsilon\text{.E:Bi-Deduce}}{\mathbb{E};\Theta\vdash\vec{w}_0,(C_1,\dots,C_n)\ \vec{w}_0\ \vec{u}\ \vec{\mathsf{n}}\sim_{\varepsilon'}\vec{w}_1,(C_1,\dots,C_n)\ \vec{w}_1\ \vec{v}\ \vec{\mathsf{n}}}\,\text{G.Cut}$$

With G.Weak

$$\dfrac{\dfrac{\dfrac{\Pi_F}{\mathbb{E};\Theta\vdash F}\quad\dfrac{\Pi}{\mathbb{E};\Theta_0,F\vdash F_0}}{\mathbb{E};\Theta_0\vdash F_0}\,\text{G.Cut}}{\mathbb{E};\Theta_0,\Theta_1\vdash F_0}\,\text{G.Weak}\qquad\blacktriangleright^{\text{Weak}}_{\text{Cut}}\qquad\dfrac{\dfrac{\Pi_F}{\mathbb{E};\Theta\vdash F}\quad\dfrac{\dfrac{\Pi}{\mathbb{E};\Theta_0,F\vdash F_0}}{\mathbb{E};\Theta_0,F,\Theta_1\vdash F_0}\,\text{G.Weak}}{\mathbb{E};\Theta_0,\Theta_1\vdash F_0}\,\text{G.Cut}$$