Privacy-aware Secure Region-based Handover for Small Cell Networks in 5G-enabled Mobile Communication

Rabiah Alnashwan, Prosanta Gope *Senior Member, IEEE* , Benjamin Dowling

***Abstract*—The 5G mobile communication network provides seamless communications between users and service providers and promises to achieve several stringent requirements, such as seamless mobility and massive connectivity. Although 5G can offer numerous benefits, security and privacy issues still need to be addressed. For example, the inclusion of small cell networks (SCN) into 5G brings the network closer to the connected users, providing a better quality of services (QoS), resulting in a significant increase in the number of Handover procedures (HO), which will affect the security, latency and efficiency of the network. It is then crucial to design a scheme that supports seamless handovers through secure authentication to avoid the consequences of SCN. To address this issue, this article proposes a secure region-based handover scheme with user anonymity and an efficient revocation mechanism that supports seamless connectivity for SCNs in 5G. In this context, we introduce three privacy-preserving authentication protocols, i.e., initial authentication protocol, intra-region handover protocol and inter-region handover protocol, for dealing with three communication scenarios. To the best of our knowledge, this is the *first* paper to consider the privacy and security in both the intra-region and inter-region handover scenarios in 5G communication. Detailed security and performance analysis of our proposed scheme is presented to show that it is resilient against many security threats, is cost-effective in computation and provides an efficient solution for the 5G enabled mobile communication.**

***Index Terms*—Region-based Handover, 5G, SCN, Authentication, Privacy.**

I. Introduction

THE number of connected devices is continuously increasing, and forecasts predict to reach up to 50 billion connected devices worldwide in 2030 [1]. With this continuous growth, cellular networks have significantly evolved over the generations (1G-5G). The recently deployed 5G network introduces stringent requirements to cope with the increased capacity of connected devices and provide enhanced QoS. These requirements include reduced latency and costs, lower energy consumption, increased network capacity, high data rates, and scalable device connectivity. To achieve all these requirements, 5G mobile communication networks provide a unified, programmable software-centric infrastructure by merging recently developed network technologies, such as cloud computing, software-defined networking (SDN), network function virtualisation (NFV) and Ultra-dense Small Cell Networks (SCN) [2].

R. Alnashwan is with the Department of Computer Science, University of Sheffield and the Department of Computer Science, Imam Mhammad In Saud Uiversity, Riyadh, Saudi Arabia. (E-mail: RAlnashwan@imamu.edu.sa/RAlnashwan1@sheffield.ac.uk)

P. Gope, and B. Dowling are with Department of Computer Science, University of Sheffield, Regent Court, Sheffield S1 4DP, United Kingdom. (E-mail: prosanta.nitdgp@gmail.com/p.gope@sheffield.ac.uk; b.dowling@sheffield.ac.uk)

Ultra-dense SCN technology achieves several 5G requirements: high network density, capacity, and spectrum efficiency. Ultra-dense SCN here refers to low-powered cellular radio access nodes. SCNs aim to increase the density of wireless cells/nodes and reduce the coverage area to approximately 10-100 metres. The increased density of nodes increases network capacity and brings the network closer to the connected users, providing better network throughput with low-powered transmission and increasing the spectrum efficiency. However, to access the new advantages of SCNs, users will need to hop between cells frequently (as the individual node coverage is significantly smaller), which is a process referred to as "Handovers" (HO). Transferring a device's ongoing wireless connection from one cell operated by a base station (BS) to another cell/ BS is commonly known as a handover process in mobile wireless communication.

Although the usage of SCNs in 5G is advantageous in terms of utilising network resources and bringing the user closer to the network, it introduces more latency, security and privacy issues to the network, caused by the increased frequency of HO events in 5G. Since the 3GPP group [3] did not address the possible impact of SCNs on 5G-AKA and HO protocols, this leads to new protocols being introduced to reduce latency caused by frequent HOs in SCNs [4]–[6]. In any cellular network (such as 5G), a secure authentication protocol plays a major role in ensuring users' legitimacy and also establishment of secure symmetric keys between users and services, enabling secure communication after that point. Generally, authenticating communication networks is carried out via Authentication and Key Agreement (AKA) protocols. For 5G authentication, the 3rd Generation Partnership Project GPP(3GPP) specifies two main AKA protocols: 5G-AKA [3] and Extensible Authentication Protocol (EAP-AKA') [7]. Both protocols are relatively similar, with some minor differences in the message flow, and so we focus on 5G-AKA in this work. The 5G-AKA protocol is executed between three main participants, a User (Equipment) UE, a Serving Network SN and the Home Network (HN), and introduces new network algorithms and protocols to handle the authentication and handover procedures between these parties. The HN is responsible for issuing and maintaining users' unique information such as their telephone number, long term ID (known as their

SUPI), long term shared symmetric key, and other UE-related information. Usually, UEs can access services provided by their HN through an intermediate semi-trusted party known as a serving network (SN). For UEs to authenticate to HNs, first *user registration* must occur, where long-term symmetric keys and user credentials (SUPIs and SUCIs) are established between both parties. Now, UEs can securely *authenticate* to HNs and vice-versa by using the 5G-AKA protocol [8]. In 5G-AKA, UEs first submit their (encrypted) SUCI to the HN, allowing the HN to recover the SUPI and identify the UE. The HN then sends a challenge to the UE, followed by a response from the UE. Thus, as seen by the SUCI construction, privacy is considered an equally vital security property in the 5G-AKA authentication and HO protocols. These protocols attempt to preserve user anonymity and untraceability, (often referred to as *strong anonymity*), which are essential for preventing both an unauthorised disclosure of user identity as well as a linking of network activity to a single party. A considerable amount of research has focused on enhancing and analysing 5G-AKA [8]–[11]. These works have addressed the security, privacy and efficiency in 5G-AKA authentication and HO protocols, identifying several weaknesses in 5G-AKA, such as identity replay attacks, attacks on sequence number confidentiality (breaking untraceability) and confusion attacks.

On the other hand, handover is also vital in mobile communication networks, especially in the SCN scenario. The insurance of a continual network connection with the massive deployment of BSs/cells arouses serious challenges to handover procedures in 5G. Therefore, 3GPP specifies a number of handover protocols that address the most common handover scenarios in 5G [3]. From these protocols, we classify them into two main categories: 1) homogeneous handovers and 2) heterogeneous handovers. Homogeneous handovers are operated between BSs within 5G networks, whereas the heterogeneous handovers are done between different networks,i.e. 5G, WiFi and LTE. In this work, we only consider homogeneous handovers within the 5G network. We can further divide the 5G homogeneous handover into sub category based on the used interface defined by the 3GPP standard: Xn-based and N2-based handover. In Xn-based handover, requests are sent directly between two BSs over a pre-defined Xn interface. On the contrary, the N2 handover does not have direct communication between BSs. Handover requests instead are sent to the Access and Mobility Management Function (AMF), which resides in the core network, over the N2 interface. Peltonen, Sasse and Basin [12] present a comprehensive security analysis of these two handover protocols specified in the 5G standard. Notwithstanding the 5G handover protocols, our proposed scheme aims and addresses the inclusion of SCN in 5G networks and introduces a scheme that can provide higher security while preserving users privacy in a region-based framework.

There have been several handover authentication schemes proposed in the literature to overcome some of the vulnerabilities in 5G and also enhance the performance of authentication and HO protocols [4]–[6]. However, to the best of our knowledge, there is no such HO protocol that can achieve *strong anonymity* with *perfect forward secrecy* and *secure inter-region handover* for HO authentication in 5G. Therefore, there is a need for authentication and HO protocol that achieves the desired security properties mandated in 5G networks, such as mutual authentication, user anonymity, user untraceability, extending to SCN settings and achieving seamless user mobility *in* and *between* regions.

A. Related Works

A considerable amount of existing literature analyses 5G-AKA from different security and privacy perspectives [8]–[10]. These studies have identified several weaknesses in the current version of 5G-AKA. Basin et al. [8] provide a comprehensive analysis of the 5G-AKA and discovered some underspecified security requirements in the original specifications. This work identified traceability attacks against the 5G-AKA under the active adversaries. Cremers and Dehnel-Wild [9] analysed 5G-AKA from the security perspective, which revealed a confusion attack. This attack takes advantage of the identity misbinding property to launch an impersonation attack. Borgaonkar et al. [11] also found a logical vulnerability, which breaks the confidentiality of the sequence number due to the usage of XOR and lack of randomness. Braeken [10], on the other hand analysed the 5G-AKA from the privacy perspective. The author discovered that a simple identity replay attack presented against several AKA protocols [13] also threatens 5G-AKA. Accordingly, this work proposed an efficient 5G-AKA protocol that overcomes this attack, as well as addressing location privacy and linkability attacks. However, the proposed protocol provides only in-session unlinkability but not full unlinkability (between sessions): unlinkability holds only if all authentication attempts are successful, otherwise actions can be linked due to the un-updated GUTI values [3]. In addition, the same user location breach is not solved in the proposed protocol. Recently, Zhang et al. [5], Fan et al. [4], and Yan and Ma [6] proposed novel HO and authentication protocols specifically for the 5G environment. In 2020, Fan et al. [4] proposed a secure region-based handover scheme (ReHand) with user anonymity and fast revocation for SCNs. This protocol supports a fast authentication only for users roaming inside a region only, i.e., between HgNBs belonging to the same gNB, using a group secret key. In the initial authentication phase, which will be triggered during inter-region HO, users will send their pseudo-IDs to the AuC, update it and sending it back to the user. However, the ReHand protocol is susceptible to undetected desynchronization in the updated pseudo-ID. ReHand also provides a membership revocation mechanism that is realized by Nyberg's one-way accumulator [14]. However, Nyberg's accumulator efficiency is lower than other accumulators, and it is not dynamic, meaning AuC has to regenerate the revocation list and send it back to regions whenever a user is added or removed from that list, which negatively impacts the protocol efficiency. Next, in 2021 Zhang et al. [5] proposed a universal HO and authentication scheme (RUSH) that exploits chameleon hash functions, blockchain, and Elliptic-Curve Diffie-Hellman (ECDH) key exchange. In this protocol, users are registered with the network using their actual identities and CH values.

Then the authentication server stores users' identities locally and CH values in the Blockchain. Although the protocol supports universality (heterogeneous networks) realized by the Blockchain, user revocation and reply attacks were not considered in RUSH protocol. Additionally, some aspects of blockchain in terms of security and performance have been overlooked. Finally, recently Yan and Ma [6] proposed an efficient handover authentication protocol (LSHA) based on neighbouring BSs in the 5G network. In LSHA, each base station (gNB) has a secret key and session key with neighbouring gNBs generated by the AMF, which are used to secure the handover procedures. Although LSHA protocol is secure against DoS attacks and de-synchronization attacks, it only supports partial PFS and strong anonymity in the HO due to the dependence on the 5G-AKA specified by the 3GPP standard.

B. Motivation and Contributions

Despite all previous works in this domain, none of the existing protocols in the literature have considered all the 5G's requirements of a fast, secure, privacy-preserving and reliable HO authentication scheme. Most importantly, none of the existing 5G-AKA schemes have considered a secure inter-region HO scenario in the 5G networks. Therefore, there is a need for an authentication and HO scheme that achieves the desired security properties in 5G networks (explained in III-C) and achieves seamless user mobility in and between regions to cope with SCN in 5G network. This paper proposes a region-based HO scheme for SCN. This is the first to achieve secure, privacy-preserving inter-region HO for roaming users in 5G without any additional infrastructural support (such as blockchain). The major contributions of this paper can be summarized as follows:

- A concrete solution for SCN roaming environments in 5G, that provides a secure HO scheme supporting seamless user mobility in and between regions. To the best of our knowledge, this is the *first* solution to achieve secure, privacy-preserving Inter-region HO for roaming users in 5G;
- An effective user membership revocation scheme for a large number of users in 5G using dynamic universal accumulator [15];
- A rigorous formal security analysis of our proposed scheme, showing that our scheme achieves mutual authentication, user unlinkability and secure key exchange.
- A comparative study of the proposed scheme with closely related existing schemes, showing that our scheme is secure and computationally efficient.

C. Paper organisation:

The rest of the paper is organised as follows: Section II presents the preliminaries used in the proposed scheme. Section III introduces the system and adversary models. Section IV presents the proposed secure inter-region HO authentication scheme, with a detailed description of the proposed protocols, including registration, initial authentication, intra-region and inter-region HO protocols. SectionV provides a formal security analysis of our proposed protocols. A performance evaluation and comparison of the proposed scheme with the other related schemes is presented in Section VI. Finally, section VII concludes the paper. We give our notation used in this paper in Table I.

TABLE I
NOTATION USED IN OUR PROPOSED SCHEME.

Notation	Meaning
EID	gNB Identity
ZUID	Zone user ID
HID	HgNB Identity
RU-ID	Region user ID
RID	Region Identity
π_U	non-membership witness
PID,TID	User pseudo IDs
T_U	User subscription validity period
RL_v RL_{new}	Revocation list
k_i	Long-term key
k_s	Session key
$\mathsf{AE.Enc}\{k_i, m\}$	Authenticated encryption
$\mathsf{AE.Dec}\{k_i, m\}$	Authenticated decryption
$CERT_H$	HgNB certificate
$CERT_U$	UE certificate
$pk_{sig}^{\text{AuC}}, sk_{sig}^{\text{AuC}}$	AuC public and secret signing keys
$pk_{san}^{\text{gNB}}, sk_{san}^{\text{gNB}}$	gNB public and secret sanitising keys
$pk_{san}^{\text{HgNB}}, sk_{san}^{\text{HgNB}}$	HgNB public and secret sanitising keys

II. PRELIMINARIES

In this section, we introduce the underlying cryptographic primitives that we require for building the proposed protocols, in particular Sanitisable signatures and accumulators.

1) **Sanitisable Signatures:** A fundamental component of the proposed scheme are Sanitisable Signatures (SanSigs) [16], a signature scheme where signing capabilities can be delegated to another party: the so-called sanitiser. The sanitiser can modify parts of a signed message (generating another valid signature over the modified message) without the original signer's assistance. SanSig requires a pair deterministic functions ADM and MOD, which can indicate if the message was modified correctly, or recover the original message from the modified message to its original message respectively, i.e., $m^* = MOD(m)$ and $ADM(m^*, m) \to \{0, 1\}$. Sanitisable Signatures should satisfy number of security properties: Unforgeability, Immutability, Privacy, Transparency and Accountability. A SanSig is a tuple of algorithms $\mathsf{SanSig} = \{\mathsf{KGen}, \mathsf{Sign}, \mathsf{Sanit}, \mathsf{Verify}, \mathsf{Proof}, \mathsf{Judge}\}$. However, since Proof and Judge are not used in our scheme directly, we omit their description here:
   - **KGen** is a pair of key generation algorithms for the signer and the sanitiser respectively: $(pk_{sig}, sk_{sig}) \leftarrow_{\$} \mathsf{KGen}_{sig}(1^n)$, $(pk_{san}, sk_{san}) \leftarrow_{\$} \mathsf{KGen}_{san}(1^n)$.
   - **Sign** takes as input a message $m \in \{0,1\}^*$, a signer private key sk_{sig}, sanitiser public key pk_{san} and the modifiable message segments (ADM). Sign either outputs a signature σ, or $\perp$ if failed: $\sigma \leftarrow_{\$} \mathsf{Sign}(m, sk_{sig}, pk_{san}, ADM)$.
   - **Sanit** takes as input an original message m, a modification of the original message MOD, a signature

σ, signer public key pk_{sig} and sanitiser private key sk_{san}. Sanit outputs either a modified message m^* and a signature σ^*, or $\perp$ if failed: $(m^*, \sigma^*) \leftarrow_\$ \mathsf{Sanit}(m, MOD, \sigma, pk_{sig}, sk_{san})$.
- **Verify** takes as input a message m, a signature σ and the public keys of the signer pk_{sig} and sanitiser pk_{san}. Verify outputs a bit $b \in \{0, 1\}$, where $b = 1$ if σ verifies message m under pk_{san} and pk_{sig}, and $b = 0$ otherwise: $b \leftarrow \mathsf{Verify}(m, \sigma, pk_{sig}, pk_{san})$.

2) **Accumulator:**
To manage the significant number of connected devices in the network, the proposed system model supports a revocation mechanism that is based on Li, Li, and Xue's dynamic universal accumulator [15]. Their framework provides a non-membership witness for users not in the accumulator. Thus, users must prove their non-membership of the revocation list before accessing the network. Typically in mobile communication networks, the number of joining users is higher than revoked users. Therefore, using an accumulator scheme that supports non-membership witnesses is more efficient than other accumulators. The frequency of updating the accumulator (and witnesses) is less than other accumulators since it is relatively correlated to the number of revoked users, not the joining users.

- **Key Generation:** $\mathsf{KGen_{acc}}$ generates a secret key sk_{acc}. $[(sk_{acc}) \leftarrow_\$ \mathsf{KGen_{acc}}(1^n)]$.
- **Accumulator Generation:** $\mathsf{Gen_{acc}}$ takes as input a secret key sk_{acc}, and the set of values to be accumulated X (Revocation list), which upon initialisation $X \leftarrow \phi$. It returns an accumulator acc. $[(acc) \leftarrow_\$ \mathsf{Gen_{acc}}(sk_{acc}, X)]$.
- **Accumulator Update:** $\mathsf{Update_{acc}}$ takes as input a secret key sk_{acc}, the original accumulator value acc and a new value to be accumulated x^*. It returns the updated accumulator acc^*. $[(acc^*) \leftarrow_\$ \mathsf{Update_{acc}}(sk_{acc}, acc, x^*)]$.
- **Non-membership Witness Generation:** $\mathsf{NonWitCreate}$ takes as input a secret key sk_{acc}, the original accumulator acc, the revocation list X and x^*, where $x^* \notin X$. It returns a non-membership witness c_x for x^*. $[(c_x) \leftarrow_\$ \mathsf{NonWitCreate}(sk_{acc}, acc, X, x^*)]$.
- **Non-membership Witness Verification:** $\mathsf{Verify_{acc}}$ takes as input the original accumulator value acc, a non-membership witness c_x and x. It outputs a bit $b \in \{0, 1\}$, where $b = 1$ if witness c_x holds (hence the value $x \notin X$), and $b = 0$ otherwise. $[b \leftarrow \mathsf{Verify_{acc}}(acc, c_x, x)]$.
- **Non-membership Witness Update** $\mathsf{NonWitUpdate}$ takes as input the original accumulator acc, the updated accumulator acc^*, a (new) accumulated value x^*, an non-accumulated value x and the original non-membership witness c_x. It outputs an updated non-membership witness c_x^*. This is required if a new element x^* has been added to the accumulator acc^*. $[(c_x^*) \leftarrow_\$ \mathsf{NonWitUpdate}(acc, acc^*, x^*, x, c_x)]$

III. System and Adversary model

In this section, we first describe the system model and adversary model of our proposed schemes. Subsequently, we define the security goals of the proposed scheme.

A. System model

Our system model captures the architecture of SCNs in 5G [17], which consists of four major components; the Authentication Center (AuC), the 5G radio base station that connects users to the 5G core network gNB, Home gNB (HgNB) and User Equipment (UE). In SCN, HgNB management System (HeMS) is responsible for configuring the gNB/HgNB according to the operators policy. In our system model, however, we combine HeMS with the AuC. Thus the AuC is responsible for configuring all parties in the system including the HgNB, gNB and UE, where AuC generates certificates, secret and public keys for them. Meanwhile, gNB and HgNB are responsible for connecting users to the core network. Each gNB in our system model manages a group of several HgNBs, creating a *Region* controlled by an gNB, as illustrated in Figure 1. As a result, the gNB is responsible for handling the Inter-region HOs, while HgNB is responsible for handling the Intra-region HOs and key exchange. It is assumed that the communication channels between network entities i.e., AuC, gNB and HgNB are secure, i.e. an authenticated and confidential channel.

Note that for the standard 5G handover scheme [12], the cooperation of AuC (i.e., all 5G core entities) is inevitable. That means the AuC needs to be actively involved during the execution of each handover phase. This will increase the transmission overhead on AuC. Accordingly, it will also increase the required time to perform a handover and affect the security and user privacy. This issue will be exacerbated significantly with the inclusion of SCN in the 5G networks. Hence, in the proposed scheme, each *Region* consists of a gNB and its belonging HgNBs. The legitimacy of users roaming inside a region can be verified by a designated HgNB using the public key of the gNB of the same Region. Meanwhile, users roaming between regions are verified, and their certificates are modified (to preserve user anonymity) by the gNB of the targeted Region (as a sanitiser). Thus, in our proposed system, we do not require the 5G core/AuC to be actively involved or participated during the execution of the handover phases (intra-region and inter-region).

B. Adversary Model

In our system model, a user communicates with other network entities, i.e., HgNBs and gNBs, through the public/insecure channels. Hence, in our adversary model, we allow an adversary $\mathcal{A}$ to control the public channels fully; therefore, $\mathcal{A}$ can intercept, delete, insert and modify any message. Finally, $\mathcal{A}$ can leak long-term and per-session secrets, capturing device-compromising attackers. User privacy is considered an essential property in 5G-based mobile communication, so $\mathcal{A}$ may also try to break User anonymity by linking distinct "challenge" protocol executions of the same user, capturing linkability attacks. To strengthen our adversary model, we allow $\mathcal{A}$ to schedule session initialisation, thus all sessions are initialised with owners chosen by the adversary, except the "challenge" sessions, which are instead initialised with a pair of potential owners, i.e. $\mathcal{A}$ must distinguish which party owns the "challenge" session. In addition, we wish to ensure that an

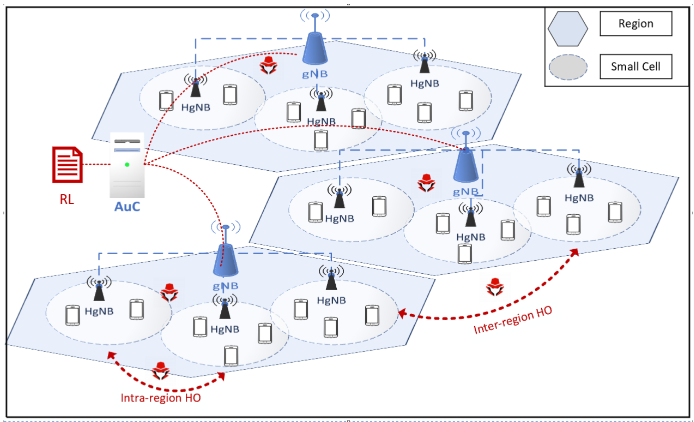

Fig. 1. System model [Hexagon shape → a region managed by one gNB, Oval shape → small cell emulating SCN.]

adversary cannot break authentication, nor learn session keys established during the proposed handover schemes. In Section V, we present security experiments capturing these notions.

C. Security Goals

Our proposed privacy-preserving handover protocols should achieve the following security goals:

Mutual authentication: It is essential to guarantee the authenticity of the communicating parties for both the network components and the UEs. Otherwise, this may cause various security threats such as MITM and impersonation attacks. We provide details of this security experiment in Section V-A.

Strong anonymity: Privacy is one of the major security requirements in 5G, where users' identities should never be transmitted in plaintext. However, encryption alone is not sufficient for preserving user privacy, as user identities can be revealed by honest-but-curious network components. To address this, our schemes replace users' long-term identities with (encrypted) temporary identifiers. Providing user anonymity is not sufficient for fulfilling the privacy requirements in 5G. Although users' identities are anonymised, attackers could link distinct sessions to a single user, causing traceability attacks. Our scheme achieves security against traceability attacks even in the SCN, where $\mathcal{A}$ can monitor network traffic between the small cells. We provide details of the security experiment in Section V-B.

Perfect forward secrecy: Ensuring the security of previously-computed session keys after long-term secrets are compromised is essential for 5G. Ephemeral Diffie-Hellman key exchange (authenticated via sanitisable signatures) allows our proposed scheme to achieve this notion. Use of SCNs increases the frequency of HO protocol executions, which shortens the window of session key compromise. We provide details of this security experiment in Section V-C.

Effective revocation management: Since the number of joining users to the 5G network is continuously increasing, providing a subscription management mechanism is essential. Therefore, we utilise the universal accumulators for our proposed protocol's revocation list (RL).

IV. Secure Region-based Handover Scheme

Here we introduce our proposed handover scheme consisting of *four* phases: *Registration*, *Initial authentication*, *Intra-region HO*, and *Inter-region HO*.

The *Registration* phase registers gNBs, HgNBs and new users in the network, generating the initialisation parameters for the network parties (AuC, gNB and HgNB) (where AuC creates SanSig key pairs for gNBs and certificates for HgNB). Additionally, AuC generates and shares a long-term secret key with the User and pseudo-identities (PIDs & TIDs) for user anonymity. Then AuC initialises the user membership revocation list (RL), which is initially empty. The *Initial Authentication* phase issues certificates for new users in the network (via SanSig) using their PIDs. The *Intra-Region HO* phase allows users to roam inside a region (between two HgNBs owned by a single gNB) to mutually authenticate the target HgNB using their certificates', and establish a shared secret key. The *Inter-Region HO* phase allows users to roam between regions (between two HgNBs controlled by different gNBs) to mutually authenticate the target gNB and establish a shared secret key.

A. Registration Phase

In the registration phase of the proposed scheme, we assume that the communication channels between the parties (i.e. AuC, gNB, HgNB, UE) are secure. During the execution of the registration phase, AuC generates the required credentials for all participants, including the HgNB certificate, HgNB sanitising keys, gNB sanitising keys, UE pseudo-identities (TID, PID), UE long term key (k_i) and the revocation list (RL). Our registration phase is divided into three parts: UE registration, $\mathrm{gNB}/\mathrm{HgNB}$ registration, and accumulator initialisation, which are described as follows.

1) **UE Registration**: In order to register into the network, each UE_i needs to share his/her essential information with the AuC via a secure channel. Upon receiving the registration request, the AuC then generates a long-term secret key k_i, a pseudo-identity (PID_i) and a temporary ID (TID_i) for each user, where $\mathrm{PID}_i, \mathrm{TID}_i \leftarrow_\$ \{0,1\}^n$.
2) **gNB/HgNB Registration**: Each gNB and HgNB needs to register to the network and share the essential registration

information with the AuC. Upon receiving the registration request, the AuC then generates a signing key pair for itself and HgNBs i.e., $(pk_{sig}^{\mathrm{AuC}}, sk_{sig}^{\mathrm{AuC}}) \leftarrow_{\$}$ $\mathsf{SanSig.KGen}_{sig}(1^n)$, $(pk_{san}^{\mathrm{HgNB}}, sk_{san}^{\mathrm{HgNB}}) \leftarrow_{\$}$ $\mathsf{SanSig.KGen}_{san}(1^n)$. Next, AuC signs the HgNB_i certificate ($CERT_H = CERT_{fix}^{H}||CERT_{mod}^{H}$) for each HgNB in the network: $\sigma_H \leftarrow_{\$} \mathsf{SanSig.Sign}(CERT_H, sk_{sig}^{\mathrm{AuC}}, pk_{san}^{\mathrm{HgNB}}, ADM(CERT_{mod}^{H}))$. Hereafter, AuC generates signing and sanitising keys for itself and gNBs: $(pk_{sig}^{\mathrm{AuC}}, sk_{sig}^{\mathrm{AuC}}) \leftarrow_{\$}$ $\mathsf{SanSig.KGen}_{sig}(1^n)$,$(pk_{san}^{\mathrm{gNB}}, sk_{san}^{\mathrm{gNB}}) \leftarrow_{\$}$ $\mathsf{SanSig.KGen}_{san}(1^n)$. These pairs of keys will be used to sign users' certificates ($CERT_U$) in the initial authentication phase, and sanitise users' certificates in the inter-region phase. To expedite the registration process, AuC can execute this step offline.

3) **Accumulator Initialisation**: To initialise the accumulator/revocation list, first the AuC generates a secret accumulator key $(sk_{acc}) \leftarrow_{\$} \mathsf{KGen}_{\mathsf{acc}}(1^n)$ and also creates the revocation list $RL \leftarrow_{\$} \mathsf{Gen}_{\mathsf{acc}}(sk_{acc}, X)$, where X is initially empty.

B. Initial authentication

Each registered user who wants to join the network needs to participate in the initial authentication phase of our proposed scheme. During the execution of this protocol, the AuC generates credentials/certificates for new users, which will be used in the subsequent phases (Handover protocols). In this protocol, gNBs are passive entities, where they are only responsible for forwarding messages between HgNBs and UEs. Therefore, we combine the HgNB and gNB into one entity in this protocol. This protocol consists of the following steps and is illustrated in Figure 2.

Step $\mathbf{A_1}$: HgNB $\rightarrow$ UE: $\mathbf{M_1}$: $[CERT_H^*, \sigma_H^*, g^h]$.
When a new UE enters the coverage area of HgNB, HgNB samples h and computes g^h. Next, HgNB updates their certificate (the modifiable part) , i.e. $CERT_{mod}^{*H} = \mathrm{HID}\|g^h$ (preventing replay attacks). Then HgNB sanitises the updated certificate $CERT_H = CERT_{fix}^{H}\|CERT_{mod}^{*H}$, using the sanitising algorithm SanSig.Sanit, and composes a message $\mathbf{M_1}$, sending $\mathbf{M_1}$ to UE.
Step $\mathbf{A_2}$:UE $\rightarrow$ HgNB/gNB:
$\mathbf{M_2}$:$[\mathsf{AE.Enc}\{k_s, M_{A_0}||\mathrm{TID}\}, g^{r_u}]$.
Upon receiving $\mathbf{M_1}$, UE verifies the HgNB certificate $CERT_H$ using the SanSig verification algorithm SanSig.Verify, containing g^h (preventing MITM attacks). If successful, UE samples (r_{id}, r_u), and computes the session keys (sk_i, k_s). Next, UE encrypts $(\mathrm{PID}||r_{id})$ using the long-term key k_i shared with AuC, to generate the message $\mathbf{M_{A_0}}$. Afterwards, UE encrypts $(M_{A_0}||\mathrm{TID})$ with k_s (preventing linkability), and sends the message $\mathbf{M_2}$ to HgNB.
Step $\mathbf{A_3}$: HgNB/gNB $\rightarrow$ AuC:
$\mathbf{M_3}$: $[M_{A_0}, \mathrm{TID}, \mathrm{HID}, \mathrm{EID}, \mathrm{RID}]$.
Upon receiving the response message $\mathbf{M_2}$, HgNB computes (sk_i, k_s) to decrypt $\mathbf{M_2}$. Next HgNB forwards the decrypted message along with the user pseudo-identities and region identities to AuC.

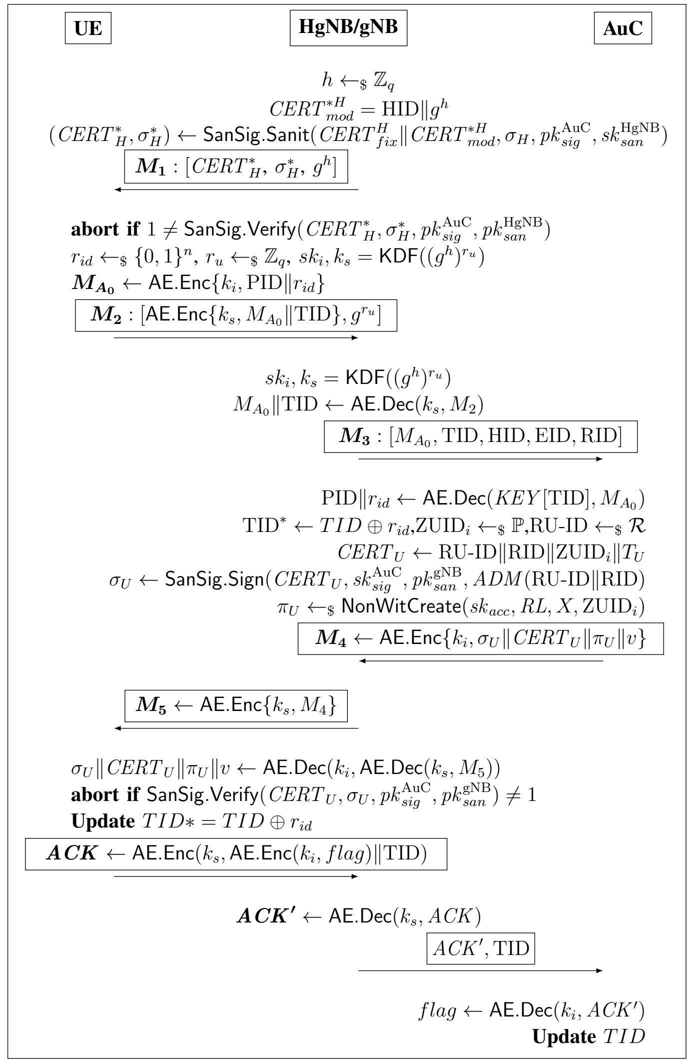

Fig. 2. The Initial Authentication Phase of our proposed 5G Secure Handover Scheme. The descriptions of each algorithm can be found in Section II.

Step $\mathbf{A_4}$: AuC $\rightarrow$ HgNB/gNB:
$\mathbf{M_4}$: $[\mathsf{AE.Enc}\{k_i, \sigma_U\|CERT_U\|\pi_U\|v)\}]$.
AuC retrieves the long term key k_i of UE using TID, and decrypts $\mathbf{M_{A_0}}$, to recover (PID, r_{id}). Next, AuC computes a new temporary user identifier TID^*, and generates a user ID (ZUID_i), which will be the user's identifier in the revocation list RL. AuC creates and signs $CERT_U$ by generating the "fixed" part of the UE certificate $CERT_{fix}^{U} = \mathrm{ZUID}_i\|T_U$ (where T_U is a user subscription validity period), and the "modifiable" region-specific part of the UE certificate $CERT_{mod}^{U} = \mathrm{RU\text{-}ID}\|\mathrm{RID}$ (where RU-ID a region-user ID and RID is the region ID). Then AuC signs both parts of the UE certificate generating $CERT_U \leftarrow$ SanSig.Sign. Next, AuC generates a non-membership witness $(\pi_U) \leftarrow$ NonWitCreate, and specifies the version v of RL, corresponding to the version of RL from which π_U was generated. AuC then stores ZUID_i, TID_i and TID_i^* (to prevent de-synchronisation), and encrypts π_U, UE certificate and its signature using k_i, to generate the message $\mathbf{M_4}$ sending $\mathbf{M_4}$ to the HgNB/gNB.

Step $\mathbf{A_5}$: HgNB → UE: $\mathbf{M_5}$: [AE.Enc$\{k_s, M_4\}$]
HgNB/gNB encrypts $\mathbf{M_4}$ using the session key k_s (preventing linkability) to generate the message $\mathbf{M_5}$, sending $\mathbf{M_5}$ to the UE.

Step $\mathbf{A_6}$: UE → AuC: **ACK** :[AE.Enc(k_s, (AE.Enc($k_i, flag$), TID))]
Upon receiving $\mathbf{M_5}$, UE recovers $(\sigma_U, CERT_U, \pi_U, v)$, and verifies their certificate, using SanSig.Verify$(CERT_U, \sigma_U)$. If verification fails, UE terminates the execution of the protocol. Otherwise, the user then updates TID*, and sends an acknowledgement **ACK**, an encryption of an acknowledgement flag $flag$ and the user's TID, which is encrypted using the user long term key k_i and TID, and then encrypted again using the ephemeral key k_s to HgNB.

Step $\mathbf{A_7}$: HgNB → AuC: ACK' : $[ACK', \mathrm{TID}]$
HgNB/gNB decrypts **ACK** using the session key k_s (preventing linkability) to generate the message ACK', sending ACK', TID to the AuC.

Step $\mathbf{A_8}$: Upon receiving ACK, AuC recovers k_i (using the old TID), and uses it to decrypt ACK, then Auc updates the TID^*. If ACK was not received within the pre-specified time window, AuC deletes TID*. AuC will continue to maintain both TID and TID*. Details of this protocol is depicted in Figure 2.

Remark 1: To prevent de-synchronisation (DoS attacks) [18] AuC maintains both (TID, TID*) values until receiving the ACK message. However, to prevent DoS attacks without compromising the privacy of the UE, we can use the previous solution proposed in [19] that overcomes de-synchronisation attacks by utilising a family of temporary PIDs instead of a single TID.

C. Intra-region Handover

The intra-region handover protocol will be executed when a user remains under the same region where he/she was in but roams to a different small-cell under authority of a different HgNB i.e., between HgNBs belonging to the same region. The intra-region HO protocol is described below, and illustrated in Figure 3.

Step $\mathbf{B_1}$: HgNB → UE: $\mathbf{M_1}$: $[CERT^*_H, \sigma^*_H, g^h]$.
This step proceeds identically to **Step $\mathbf{A_1}$** of the initial authentication phase. In this regard, when a new user enters into the coverage area of new HgNB, the HgNB sanitises his/her certificate, and composes a message $\mathbf{M_1}$, then sending $\mathbf{M_1}$ to UE.

Step $\mathbf{B_2}$: UE → HgNB:
$\mathbf{M_2}$:[AE.Enc$\{k_s, CERT_U||\sigma_U||\pi_U||v\}, g^{r_u}$] .
Upon receiving the message $\mathbf{M_1}$, UE verifies the HgNB certificate $CERT_H$ and the DH public keyshare g^h, using SanSig.Verify$(CERT^*_H, \sigma^*_H)$. If successful, UE samples r_u and computes session keys sk_i, k_s. Next UE composes a message $\mathbf{M_2}$ and encrypts it using k_s. The encrypted part of M_2 consist of $CERT_U$, σ_U, π_U and v, which is the user's certificate, certificate signature, non-membership witness and the accumulator version of which π_U was created from, respectively. Finally, UE sends $\mathbf{M_2}$ to HgNB.

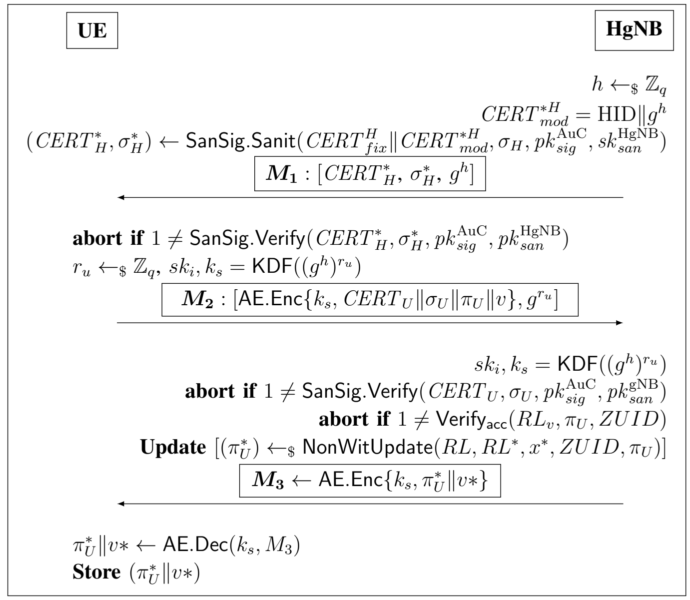

Fig. 3. The Intra-region Handover Protocol of our proposed 5G Secure Handover Scheme. Descriptions of each algorithm can be found in Section II.

Step $\mathbf{B_3}$: HgNB → UE: $\mathbf{M_3}$: [AE.Enc$\{k_s, \pi^*_U||v^*\}$].
Upon receiving the response message $\mathbf{M_2}$, HgNB generates the session keys sk_i, k_s, to decrypt $\mathbf{M_2}$. Subsequently, HgNB verifies UE's certificate using SanSig.Verify$(CERT_U, \sigma_{UE})$. If successful, HgNB recovers the accumulator version v and checks if $v_i = v_{RL}$, to check if RL has been updated. If not, HgNB checks if the UE has been revoked by calling Verify$_{\mathsf{acc}}(ZUID_i, ..)$. Otherwise, if the revocation list has been updated, where $v_i \neq v_{RL}$, HgNB checks if $ZUID_i$ has been accumulated in the updated RL. If not, HgNB updates the non-membership witness π^*_U (where x^* is the new unrevoked UE). Finally, HgNB encrypts and sends $\mathbf{M_3}$ to UE, which they will maintain for future communications. Details of this protocol is depicted in Figure 3.

D. Inter-region Handover

When a user moves to a different region, then they need to execute the inter-region handover phase of our proposed scheme, which is described below, and illustrated in Figure 4:

Step $\mathbf{C_1}$: HgNB → UE: $\mathbf{M_1}$: $[CERT^*_H, \sigma^*_H, g^h]$.
This step proceeds identically to **Step $\mathbf{A_1}$** of the initial authentication phase. In this regard, for the new users entering the coverage area of HgNB, the HgNB sanitises his/her certificate, and composes a message $\mathbf{M_1}$, then sending $\mathbf{M_1}$ to UE.

Step $\mathbf{C_2}$: UE → HgNB:
$\mathbf{M_2}$:[AE.Enc$\{k_s, CERT_U||\sigma_U||\pi_U|||v\}, g^{r_u}$].
This step proceeds identically to **Step $\mathbf{B_2}$** of the intra-region HO phase. In this regard, UE verifies $\mathbf{M_1}$, compute a session key. UE then composes $\mathbf{M_2}$, encrypt it using the session key then send it to HgNB.

Step $\mathbf{C_3}$: HgNB → gNB: $\mathbf{M_3}$: $[CERT_U||\sigma_U||\pi_U||v]$. Upon the arrival of $\mathbf{M_2}$, HgNB generates the session keys sk_i, k_s

UE **HgNB** **gNB**

$h \leftarrow_\$ \mathbb{Z}_q$

$CERT^{*H}_{mod} = \text{HID} \| g^h$

$(CERT^*_H, \sigma^*_H) \leftarrow \mathsf{SanSig.Sanit}(CERT_H, CERT^{*H}_{mod}, \sigma_H, pk^{\text{AuC}}_{sig}, sk^{\text{HgNB}}_{san})$

$\boldsymbol{M_1} : [CERT^*_H, \sigma^*_H, g^h]$ (HgNB → UE)

abort if $1 \neq \mathsf{SanSig.Verify}(CERT^*_H, \sigma^*_H, pk^{\text{AuC}}_{sig}, pk^{\text{HgNB}}_{san})$

$r_u \leftarrow_\$ \mathbb{Z}_q,\ sk_i, k_s = \mathsf{KDF}((g^h)^{r_u})$

$\boldsymbol{M_2} : [\mathsf{AE.Enc}\{k_s, CERT_U \| \sigma_U \| \pi_U \| v\}, g^{r_u}]$ (UE → HgNB)

$sk_i, k_s = \mathsf{KDF}((g^h)^{r_u})$

$CERT_U \| \sigma_U \| \pi_U \| v \leftarrow \mathsf{AE.Dec}(k_s, M_2)$

$\boldsymbol{M_3} : [CERT_U \| \sigma_U \| \pi_U \| v]$ (HgNB → gNB)

abort if $1 \neq \mathsf{SanSig.Verify}(CERT_U, \sigma U, pk^{\text{AuC}}_{sig}, pk^{\text{gNB}}_{san})$

abort if $1 \neq \mathsf{Verify}_{\mathsf{acc}}(RL_v, \pi_U, ZUID)$

Update $[(\pi^*_U) \leftarrow_\$ \mathsf{NonWitUpdate}(RL, RL^*, x^*, ZUID, \pi_U)]$

$\text{RU-ID} \leftarrow_\$ \mathcal{R}$

$CERT^{U^*}_{mod} = \text{RU-ID}^* \| RID^*$

$(CERT^*_U, \sigma^*_U) \leftarrow \mathsf{SanSig.Sanit}(CERT^{*U}_{fix}, CERT^{U^*}_{mod}, \sigma_U, pk^{\text{AuC}}_{sig}, sk^{\text{gNB}}_{san})$

$\boldsymbol{M_4} : [\sigma_{U^*} \| CERT_{U^*} \| \pi_{U^*} \| v^*]$ (gNB → HgNB)

$\boldsymbol{M_5} \leftarrow \mathsf{AE.Enc}\{k_s, M_4\}$ (HgNB → UE)

$\sigma^*_U \| CERT^*_U \| \pi_{U^*} \| v^*] \leftarrow \mathsf{AE.Dec}(k_e, M_5))$

abort if $\mathsf{SanSig.Verify}(\sigma^*_U, CERT^*_U, pk^{\text{AuC}}_{sig}, pk^{\text{gNB}}_{san}) \neq 1$

Store $(\pi^*_U \| v^*)$

Fig. 4. The Inter-region Handover Phase of our proposed 5G Secure Handover Scheme. The descriptions of each algorithm can be found in Section II.

to decrypt $\mathbf{M_2}$, then forwards the (decrypted) message to gNB.

Step $\mathbf{C_4}$: gNB → HgNB: $\mathbf{M_4}$: $[\sigma^*_U \| CERT^*_U \| \pi^*_U \| v*]$. After receiving the response message $\mathbf{M_3}$, gNB verifies the user's certificate using the SanSig verification algorithm, i.e. $\mathsf{SanSig.Verify}(CERT_U, \sigma_U)$. If successful, HgNB retrieves the accumulator version v and checks if $v_i = v_{RL}$, to see if RL has been updated. If not, HgNB checks if the UE has been revoked by using $\mathsf{Verify}_{\mathsf{acc}}(ZUID_i)$. Otherwise, if the revocation list has been updated (and $v_i \neq v_{RL}$) HgNB checks whether $ZUID_i$ is added in the later version of the RL. If not, HgNB updates the non-membership witness $\pi^*_U \leftarrow \mathsf{NonWitUpdate}(.)$ (where x^* is the new non-revoked UE). Subsequently gNB updates the region-user identifier $RU-ID^*_i$, updates the "modifiable" region-specific part of the UE certificate $cert^{*U}_{mod}$, and updates the user certificate accordingly, where $CERT^*_U = cert^{*U}_{mod} || cert^U_{fix}$. After, gNB sanitises UE $CERT_U \leftarrow \mathsf{SanSig.Sanit}(.)$. Finally, gNB composes $\mathbf{M_4}$, sending $\mathbf{M_4}$ to HgNB.

Step $\mathbf{C_5}$: HgNB → UE: $\mathbf{M_5}$: $[\mathsf{AE.Enc}\{k_s, M_4\}]$. Upon receiving the message $\mathbf{M_4}$, HgNB encrypts it using the session key k_s, to generate $\mathbf{M_5}$, sending $\mathbf{M_5}$ to the UE.

Step $\mathbf{C_6}$: Upon receiving the encrypted message $\mathbf{M_5}$, the UE recovers $(\sigma^*_U, CERT^*_U, \pi^*_U, v*)$, and verifies the certificate signature, using SanSig verification algorithm i.e. $\mathsf{SanSig.Verify}(CERT^*_U, \sigma^*_U)$. If verification fails, UE terminates the execution of the protocol. Otherwise, the user updates their certificate and RU-ID. Details of this protocol is depicted in Figure 4.

V. Security Analysis

This section provides a formal proof that our protocols achieve mutual authentication, key indistinguishability and unlinkability. Note that each of our proofs proceeds as a series of game-hops, where we incrementally change the experiment and demonstrate at the end that the adversary cannot win (nor detect the changes) with non-negligible probability. We begin by analysing the MA-security of each of our protocols in turn.

A. Mutual Authentication security

Here we discuss the mutual authentication security of our protocols. Due to space constraints, we only discuss the details of the proof of MA-security for the Initial Authentication scheme since it's the most technically interesting. The full version of each proof is available in Appendix C of Supplementary Material.

Theorem 1: MA**-security of Initial Authentication**. Initial Authentication depicted in Figure 2 is MA-secure under the cleanness predicate defined in [Appendix-B, Definition5][1]. For any PPT algorithm $\mathcal{A}$ against the MA experiment, $\mathbf{Adv}^{\mathsf{MA},\mathbf{clean}}_{\Pi,n_P,n_S,\mathcal{A}}(\lambda)$ is negligible assuming the EUFCMA security of SanSig, Auth security of AE, the KDF security of KDF and the DDH assumption.

Proof: First, we recall that in order to win the MA-security experiment, that $\mathcal{A}$ cannot issue a $\mathsf{Corrupt}(i)$ query before a session π^s_i accepts such that $\mathcal{C}$ terminates the game and outputs 1, nor can it issue a $\mathsf{StateReveal}(i, s)$, nor a $\mathsf{StateReveal}(\text{AuC}, s)$ query (where $\pi^{s'}_{\text{AuC}}$ received messages from π^s_i).

We divide the proof into two cases: the first where the UE accepts messages $\mathbf{M_1}$ and $\mathbf{M_4}$ without an honest matching AuC partner. We denote $\mathcal{A}$'s advantage in **Case 1** as $\mathbf{Adv}^{\mathsf{MA},\mathbf{clean},\mathsf{C1}}_{\Pi,n_P,n_S,\mathcal{A}}(\lambda)$. The second case is when the AuC accepts messages $\mathbf{M_3}$ and **ACK** without an honest matching UE partner. We denote $\mathcal{A}$'s advantage in **Case 1** as $\mathbf{Adv}^{\mathsf{MA},\mathbf{clean},\mathsf{C2}}_{\Pi,n_P,n_S,\mathcal{A}}(\lambda)$. It is clear that

$$\mathbf{Adv}^{\mathsf{MA},\mathbf{clean}}_{\Pi,n_P,n_S,\mathcal{A}}(\lambda) \leq \mathbf{Adv}^{\mathsf{MA},\mathbf{clean},\mathsf{C1}}_{\Pi,n_P,n_S,\mathcal{A}}(\lambda) + \mathbf{Adv}^{\mathsf{MA},\mathbf{clean},\mathsf{C2}}_{\Pi,n_P,n_S,\mathcal{A}}(\lambda).$$

Case 1: UE **accepts messages $\mathbf{M_1}$ and $\mathbf{M_4}$ without an honest matching** AuC **partner.**

Game $A_{1.0}$: This is the original mutual authentication experiment described in [Appendix B-A][1]:

$$\mathbf{Adv}^{\mathsf{MA},\mathbf{clean},\mathsf{C1}}_{\Pi,n_P,n_S,\mathcal{A}}(\lambda) \leq \mathbf{Adv}_{G_{A_{1.0}}}$$

Game $A_{1.1}$: Here we introduce an abort event, where the challenger aborts if $\mathcal{A}$ produces a valid signature σ that verifies under pk^{AuC}_{sig} and pk^{HgNB}_{san}. At the beginning of the experiment, we initialise a SanSig challenger $\mathcal{C}$, that outputs $pk^{\mathcal{C}}_{sig}$ and $pk^{\mathcal{C}}_{san}$, which we embed into the AuC and HgNB respectively. Then any time AuC or HgNB needs to generate

[1]The full version of the security analysis and the security framework is available in the Supplementary Material.

a signature, we query SanSig.Sign to sign a message m. Now, we trigger the abort event that occurs whenever $\mathcal{A}$ produces a valid signature. Thus, the probability that $\mathcal{A}$ triggers the abort event is bounded by the EUFCMA security of SanSig. Due to the page limit, the security of SanSig has been included in the [Appendix A, Definition 4] of the supplementary material :

$$\mathbf{Adv}_{G_{A_{1.0}}} \leq \mathbf{Adv}_{G_{A_{1.1}}} + \mathbf{Adv}^{\text{EUFCMA}}_{\mathsf{SanSig}}.$$

Game $A_{1.2}$: In this game we guess the first session π_i^s to accept without a matching partner, such that $\pi_i.role = UE$. Since there are at most n_P parties running n_S sessions, the probability of session π_i^s accepts without a matching partner is:

$$\mathbf{Adv}_{G_{A_{1.1}}} \leq n_P \cdot n_S \cdot \mathbf{Adv}_{G_{A_{1.2}}}.$$

Game $A_{1.3}$: Here we introduce another abort event. That is triggers if $\mathcal{A}$ sends a Diffie-Hellman public keyshare g^h to the session π_i^s, i.e. session π_i^s receives g^h that is not from an honest HgNB. Since this requires a signature over g^h, and by **Game** $A_{1.1}$ we abort if $\mathcal{A}$ generates a valid signature over any message m, it follows that:

$$\mathbf{Adv}_{G_{A_{1.2}}} \leq \mathbf{Adv}_{G_{A_{1.3}}}.$$

Game $A_{1.4}$: In this game, we replace g^h, g^{r_u} and g^{hr_u} computed honestly in the protocol execution with g^a, g^b, g^c respectively, from a DDH challenger. By the definition of Decisional Diffie-Hellman, a, b, c are sampled uniformly at random from $\mathbb{Z}_q$, and independent of the protocol execution. Thus any $\mathcal{A}$ that can distinguish **Game** $A_{1.3}$ from **Game** $A_{1.4}$ can break the DDH assumption [Appendix-A,Definition 1][1]. Thus it follows that:

$$\mathbf{Adv}_{G_{A_{1.3}}} \leq \mathbf{Adv}_{G_{A_{1.4}}} + \mathbf{Adv}^{G,g,q}_{\mathsf{DDH}}.$$

Game $A_{1.5}$: In this game we replace the session and encryption keys sk_i, k_s with uniformly random values $\hat{sk_i}, \hat{k_s}$ by interacting with a KDF challenger. Since $sk_i, k_s \leftarrow \mathsf{KDF}(g^c)$ and by **Game** $A_{1.4}$ g^c is already uniformly random and independent, this change is sound. Any $\mathcal{A}$ that can distinguish **Game** $A_{1.4}$ from **Game** $A_{1.5}$ can be used to break KDF security defined in [Appendix A-Definition 1] on the supplementary material. Thus:

$$\mathbf{Adv}_{G_{A_{1.4}}} \leq \mathbf{Adv}_{G_{A_{1.5}}} + \mathbf{Adv}^{\text{KDF}}_{\mathsf{KDF}}.$$

Game $A_{1.6}$: In this game, we introduce an abort event that occurs if π_i^s decrypts a valid ciphertext keyed by $\hat{sk_i}$, but the ciphertext was not produced by an honest AuC session. Specifically, we initialise an AE challenger that is queried whenever the challenger needs to encrypt or decrypt with $\hat{sk_i}$. The abort event only triggers if $\mathcal{A}$ can produce a valid ciphertext, and we can submit the valid ciphertext to the AE challenger to break the security of the security of the AE scheme. By **Game** $A_{1.5}$ $\hat{sk_i}$ is already uniformly random and independent and this replacement is sound. Any $\mathcal{A}$ that can trigger the abort event can break the Auth security of the AE scheme [Appendix A-Definition 2][1]. This implies:

$$\mathbf{Adv}_{G_{A_{1.5}}} \leq \mathbf{Adv}_{G_{A_{1.6}}} + \mathbf{Adv}^{\text{Auth}}_{\mathsf{AE}}.$$

Game $A_{1.7}$: In this game, the session π_i will only accept $\mathbf{M_1}$ from HgNB and $\mathbf{M_4}$ from AuC if they are honest partners. $\mathcal{A}$ cannot produce a valid ciphertext by **Game** $A_{1.6}$, and $\mathcal{A}$ cannot produce a valid signature by **Game** $A_{1.1}$. Thus the advantage of $\mathcal{A}$ in winning the MA-security experiment is negligible.

$$\mathbf{Adv}_{G_{A_{1.7}}} = 0.$$

Case 2: AuC **accepts messages** $\mathbf{M_3}$ **and ACK without an honest matching** UE **partner.** In this case, we assume that the first session to accept without a matching partner is owned by AuC.

Game $A_{2.0}$: This is the original mutual authentication game described in [Appendix B-A][1]:

$$\mathbf{Adv}^{\mathsf{MA},\mathbf{clean},\mathsf{C2}}_{\Pi,n_P,n_S,\mathcal{A}}(\lambda) \leq \mathbf{Adv}_{G_{A_{2.0}}}.$$

Game $A_{2.1}$: In this game, we guess the index i of the first AuC session that accepts without a matching partner such that their partner is owned by UE_i, i.e. $\pi^s_{\text{AuC}}.PID = \text{UE}_i$, introducing a factor of n_P in $\mathcal{A}$'s advantage:

$$\mathbf{Adv}_{G_{A_{2.0}}} \leq n_P \cdot \mathbf{Adv}_{G_{A_{2.1}}}.$$

Game $A_{2.2}$: As per the definition of **Case 2**, $\mathcal{A}$ cannot issue a $\mathsf{Corrupt}(i)$ query before the AuC session accepts without a matching partner. In this game, we introduce an abort event that triggers if the first π^t_{AuC} to accept without a matching partner accepts a ciphertext $\mathbf{M_3}$ that was not output from a matching partner session π_i^s. Specifically, we initialise an Auth challenger that is queried whenever $\mathcal{C}$ needs to encrypt or decrypt with k_i. The abort event only triggers if $\mathcal{A}$ can produce a valid ciphertext, and we can submit the valid ciphertext to the Auth challenger to break the Auth security of the AE scheme. Since k_i is uniformly random and cannot be leaked to $\mathcal{A}$, this replacement is sound. Thus, any $\mathcal{A}$ that triggers this abort event can be used to break the Auth security of AE [Appendix A-Definition 2][1], thus:

$$\mathbf{Adv}_{G_{A_{2.1}}} \leq \mathbf{Adv}_{G_{A_{2.2}}} + \mathbf{Adv}^{\text{Auth}}_{\mathsf{AE}}.$$

Game $A_{2.3}$: Here we introduce a similar abort event that triggers if π^t_{AuC} accepts a ciphertext **ACK** that was not output from a matching partner session π_i^s. The changes introduced to **Game** $A_{2.3}$ follow from **Game** $A_{2.2}$, and thus introduces no new advantage for $\mathcal{A}$. Thus:

$$\mathbf{Adv}_{G_{A_{2.2}}} \leq \mathbf{Adv}_{G_{A_{2.3}}}.$$

Game $A_{2.4}$: In this game, the π^t_{AuC} only accepts $\mathbf{M_3}$ and **ACK** from an honest matching partner. Thus, summing the probabilities we find that the $\mathcal{A}$ has negligible advantage in winning the MA-security experiment.:

$$\mathbf{Adv}_{G_{A_{2.4}}} = 0$$

The analysis of the MA-security of the Intra- and Inter-region Handovers proceed very similarly, and due to space constraints we merely give the theorem statement in the main body, and point to the supplementary material for more details, in [Appendix C].

Theorem 2: MA**-security of Intra-region and Inter-region Handover**. The Intra-region and Inter-region Handover protocols described in Section IV are MA-secure under the cleanness predicate defined in [Appendix B- Definition 5][1]. For any PPT algorithm $\mathcal{A}$ against the MA experiment, $\mathbf{Adv}^{\mathsf{MA},\mathbf{clean}}_{\Pi,n_P,n_S,\mathcal{A}}(\lambda)$ is negligible assuming the EUFCMA security of SanSig, Auth security of AE, the KDF security of KDF and the DDH assumption.

B. Unlinkability

Here we discuss the unlinkability security of our protocols. In these experiments, the $\mathcal{A}$ can issue a $\mathsf{Test}(i, j)$ query, which initialises a new session π_b owned by either party i, or party j, based on a bit b sampled by the challenger. Thus, we consider a strong notion of anonymity where $\mathcal{A}$ can win simply by linking the "test" session to another protocol execution where it knows the identity of the UE. Thus, we capture user anonymity, and unlinkability. Due to space constraints, we only discuss the details of the proof of Unlink security for the Inter-region Handover scheme, since its the most technically interesting. The analysis of the Initial Authentication and Intra-region protocols proceed identically. We begin by stating the results of our analysis for the Initial Authentication and Intra-region Handover scheme.

Theorem 3: Unlink**-security of Initial Authentication and Intra-region Handover**. Initial Authentication and Intra-region Handover protocols described in Section IV are unlinkable under the cleanness predicate available in [AppendixB-C,-Definition 9] of the supplementary material. For any PPT algorithm $\mathcal{A}$ against the Unlink experiment, $\mathbf{Adv}^{\mathsf{Unlink},\mathbf{clean}}_{\Pi,n_P,n_S,\mathcal{A}}(\lambda)$ is negligible assuming the EUFCMA security of SanSig, Auth security of AE, the KDF security of KDF and the DDH assumption.

Next, we analyse the Unlink-security of the Inter-region Handover scheme.

Theorem 4: Unlink**-security of Inter-region Handover**. The Inter-region Handover scheme depicted in Figure 4 is unlinkable under the cleanness predicate in [Appendix B-Definition 9][1]. For any PPT algorithm $\mathcal{A}$ against the Unlink experiment, $\mathbf{Adv}^{\mathsf{Unlink},\mathbf{clean}}_{\Pi,n_P,n_S,\mathcal{A}}(\lambda)$ is negligible assuming the EUFCMA security of SanSig, Auth security of AE, the KDF security of KDF and the DDH assumption.

Proof: First, we recall that in order to win the Unlink-security experiment, that $\mathcal{A}$ cannot issue a $\mathsf{Corrupt}(i)$ query before a session π_i^s accepts such that $\mathcal{C}$ terminate the game and outputs 1, nor can it issue a $\mathsf{StateReveal}(i, s)$, nor a $\mathsf{StateReveal}(\text{HgNB}, s)$ query (where $\pi^{s'}_{\text{HgNB}}$ received messages from π_i^s). As before, we proceed via a sequence of games.

Game B_0: This is the original unlinkability experiment described in [Appendix A-C][1]:

$$\mathbf{Adv}^{\mathsf{Unlink},\mathbf{clean}}_{\Pi,n_P,n_S,\mathcal{A}}(\lambda) \leq \mathbf{Adv}_{G_{B_0}}.$$

Game B_1: In this game we introduce an abort event, where the challenger aborts if $\mathcal{A}$ produces a valid signature σ that verifies under pk^{AuC}_{sig} and pk^{HgNB}_{san} or pk^{AuC}_{sig} and pk^{gNB}_{san}. At the beginning of this game, we initialise a pair of SanSig challengers which output $pk^{\mathcal{C}}_{sig}$ and $pk^{\mathcal{C}}_{san}$, which we embed into AuC, HgNB and gNB. Then every time AuC, HgNB or gNB needs to generate a signature, we query SanSig.Sign to sign a message m. Now, we trigger the abort event that occurs whenever $\mathcal{A}$ produces a valid signature. Thus, the probability that $\mathcal{A}$ triggers the abort event is bounded by the EUFCMA security of SanSig, defined in [Appendix A-Definition 4][1]:

$$\mathbf{Adv}_{G_{B_0}} \leq \mathbf{Adv}_{G_{B_1}} + 2 \cdot \mathbf{Adv}^{\text{EUFCMA}}_{\mathsf{SanSig}}.$$

Game B_2: In this game, we guess the first session π_i^s to accept without a matching partner, such that $\pi_i^s.role = \text{UE}$. We also introduce another abort event that triggers if $\mathcal{A}$ sends a Diffie-Hellman public keyshare g^h to the session π_i^s, i.e. session π_i^s receives g^h that is not from an honest HgNB. Since this requires a signature over g^h, and by **Game** B_1 we abort if $\mathcal{A}$ generates a valid signature over any message m, this introduces no additional bound. Since there are n_P parties running at most n_S sessions, this introduces the following bound:

$$\mathbf{Adv}_{G_{B_1}} \leq n_P \cdot n_S \cdot \mathbf{Adv}_{G_2}.$$

Game B_3: In this game, we replace g^h, g^{r_u} and g^{hr_u} computed honestly in the protocol execution with g^a, g^b, g^c respectively, from a DDH challenger. By the definition of Decisional Diffie-Hellman, a, b, c are sampled uniformly at random from $\mathbb{Z}_q$, and independent of the protocol execution. Thus any $\mathcal{A}$ that can distinguish **Game** B_2 from **Game** B_3 can break the DDH assumption [Appendix A-Definition 1][1]. Thus it follows that:

$$\mathbf{Adv}_{G_{B_2}} \leq \mathbf{Adv}_{G_{B_3}} + \mathbf{Adv}^{G,g,q}_{DDH}.$$

Game B_4: In this game the challenger replaces the session and encryption keys sk_i, k_s with uniformly random values $\hat{sk_i}, \hat{k_s}$ by interacting with a KDF challenger. Since $sk_i, k_s \leftarrow \mathsf{KDF}(g^c)$ and by **Game** B_3 g^c is already uniformly random and independent, this change is sound. Any $\mathcal{A}$ that can distinguish **Game** B_3 from **Game** B_4 can be used to break KDF security [Appendix A-Definition 1][3]). Thus:

$$\mathbf{Adv}_{G_{B_3}} \leq \mathbf{Adv}_{G_{B_4}} + \mathbf{Adv}^{\text{KDF}}_{\mathsf{KDF}}.$$

Game B_5: In this game, we replace the computation of the ciphertext $c = \mathsf{Enc}(sk_i, CERT_U \| \sigma_U \| \pi_U \| v)$ with $\hat{c} = \mathsf{Enc}(\hat{sk_i}, rand)$, where $rand \leftarrow_\$ \{0,1\}^L$ and $L = |CERT_U \| \sigma_U \| \pi_U \| v|$, and the computation of the ciphertext $c^* = \mathsf{Enc}(sk_i, CERT^*_U \| \sigma^*_U \| \pi^*_U \| v^*)$ with $\hat{c^*} = \mathsf{Enc}(\hat{sk_i}, rand^*)$ where $rand^* \leftarrow_\$ \{0,1\}^{L^*}$ and $L^* = |CERT^*_U \| \sigma^*_U \| \pi^*_U \| v^*|$. We do so by interacting with an encryption challenger whenever $\hat{sk_i}$ is used by the challenger to encrypt a message, and issuing either an Enc oracle call $(CERT_U \| \sigma_U \| \pi_U \| v, rand)$ or $(CERT^*_U \| \sigma^*_U \| \pi^*_U \| v^*, rand^*)$. Note that if the bit b sampled by the challenger is 0, then we are in **Game** B_4, and otherwise we are in **Game** B_5. Since $\hat{sk_i}$ is (by **Game** B_5) uniformly random and independent, this change is sound. Any adversary $\mathcal{A}$ that can distinguish between **Game** B_4 and **Game** B_5 can be used to break the security of AE, and thus:

$$\mathbf{Adv}_{G_{B_4}} \leq \mathbf{Adv}_{G_{B_5}} + \mathbf{Adv}^{\text{Conf}}_{\mathsf{AE}}$$

[1]The full version of the security analysis and the security framework is available in the Supplementary Material.

TABLE II
FEATURES COMPARISON.

Features	MA	SA	PFS	SRM	SIHO
5G [3]	YES	NO	NO	NO	NO
ReHand [4]	YES	YES	NO	YES	NO
RUSH [5]	YES	Partial	Partial	NO	YES
LSHA [6]	YES	Partial	Partial	NO	NO
Ours	YES	YES	YES	YES	YES

MA:Mutual Authentication, **SA**:Strong Anonymity, **PFS**: Perfect Forward Secrecy, **SRM**: Secure Revocation Management, **SIHO**: Secure Inter-region HO supports

Game B_6: In this game we highlight that the channel between the HgNB and the gNB is assumed to be secure, thus $\mathcal{A}$ cannot compromise any underlying plaintext sent between HgNB and gNB, and all messages sent to and from π_b are uniformly random and independent of the bit b sampled by the challenger. Thus it follows that $\mathcal{A}$ has no advantage in guessing the bit b, and summing the probabilities $\mathcal{A}$ has negligible advantage in winning the Unlink game. Thus:

$$\mathbf{Adv}_{G_{B_6}} = 0.$$

C. Key Indistinguishability

Here we discuss the key indistinguishability security of our scheme. In the KIND game, the goal of $\mathcal{A}$ is to distinguish between either the real key generated by the test session π_i^s, or a completely random key sampled uniformly at random from the same distributing, capturing a strong notion of key secrecy. Due to space constraints, we only discuss the details of the proof of KIND security for the Intra-region Handover, since its the most concise, and all other proofs proceed similarly. We begin by stating the results of our analysis for the Initial Authentication and Inter-region Handover scheme.

***Theorem** 5:* KIND**-security of Initial Authentication and Inter-region Handover**. Initial Authentication and Inter-region Handover protocols described in Section IV achieves KIND-security under the cleanness predicate in [Appendix B-Definition 7][1]. For any PPT algorithm $\mathcal{A}$ against the KIND experiment, $\mathbf{Adv}^{\mathsf{KIND},\mathbf{clean}}_{\Pi,n_P,n_S,\mathcal{A}}(\lambda)$ is negligible assuming the EU-FCMA security of SanSig, Auth security of AE, the KDF security of KDF and the DDH assumption.

Next, we analyse the KIND-security of the Intra-region Handover scheme.

***Theorem** 6:* KIND**-security of Intra-region Handover**. The Intra-region Handover scheme described in Figure 3 is KIND-secure under the cleanness predicate in [Appendix B-Definition 7][1]. For any PPT algorithm $\mathcal{A}$ against the KIND experiment, $\mathbf{Adv}^{\mathsf{KIND},\mathbf{clean}}_{\Pi,n_P,n_S,\mathcal{A}}(\lambda)$ is negligible assuming the EU-FCMA security of SanSig, Auth security of AE, the KDF security of KDF and the DDH assumption.

Proof: We proceed via a sequence of games.

Game C_0: This is the original KIND experiment described in [Appendix B-B][1]:

$$\mathbf{Exp}^{\mathsf{KIND},\mathbf{clean}}_{\Pi,n_P,n_S,\mathcal{A}}(\lambda) \leq Adv_{G_{C_0}}.$$

Game C_1: In this game, we introduce an abort event that triggers if $\mathcal{C}$ guesses a session $\pi_{i^*}^{s^*}$ and $\mathcal{A}$ issues a Test query to a session π_i^s where $i \neq i^*$ and $s \neq s^*$. Since there are at most $(n_S \cdot n_P)$ such sessions, this introduces the bound:

$$\mathbf{Adv}_{G_{C_0}} \leq n_S \cdot n_P \cdot \mathbf{Adv}_{C_{C_1}}.$$

Game C_2: Here we introduce a new abort event, if the test session π_i^s accepts any message from a non-honest HgNB / UE. This exactly matches the MA-experiment, where the $\mathcal{A}$ attempts to inject messages from HgNB or UE. Thus, this game is bounded by the probability of $\mathcal{A}$ breaking the MA-security of the Intra-region HO phase, and thus:

$$\mathbf{Adv}_{G_{C_1}} \leq \mathbf{Adv}^{\mathsf{MA},\mathbf{clean}}_{\Pi,n_P,n_S,\mathcal{A}}(\lambda) + \mathbf{Adv}_{G_{C_2}}$$

Game C_3: In this game, we replace g^h, g^{r_u} and g^{hr_u} computed honestly in the protocol execution with g^a, g^b, g^c respectively, from DDH challenger. By the definition of Decisional Diffie-Hellman, a, b, c are sampled uniformly at random from $\mathbb{Z}_q$, and independent of the protocol execution. Thus any $\mathcal{A}$ that can distinguish **Game** C_2 from **Game** C_3 can break the DDH assumption [Appendix A-Definition 1][1]. Thus it follows that:

$$\mathbf{Adv}_{G_{C_2}} \leq \mathbf{Adv}_{G_{C_3}} + \mathbf{Adv}^{G,g,q}_{DDH}.$$

Game C_4: In this game the challenger replaces the encryption and session keys sk_i, k_s with uniformly random values $\hat{sk_i}, \hat{k_s}$ by interacting with a KDF challenger. Since $sk_i, k_s \leftarrow \mathsf{KDF}(g^c)$ and by **Game** C_3 g^c is already uniformly random and independent, this change is sound. Any $\mathcal{A}$ that can distinguish **Game** C_3 from **Game** C_4 can be used to break KDF security [Appendix A-Definition 1][3]). Thus:

$$\mathbf{Adv}_{G_{C_3}} \leq \mathbf{Adv}_{G_{C_4}} + \mathbf{Adv}^{\mathrm{KDF}}_{\mathsf{KDF}}.$$

Game C_5: We highlight that as a result of these changes, the session key $\hat{sk_i}$ is now uniformly random and independent of the protocol execution regardless of the bit b sampled by $\mathcal{C}$, thus $\mathcal{A}$ has no advantage in guessing the bit b:

$$\mathbf{Adv}_{G_{C_5}} = 0.$$

VI. PERFORMANCE EVALUATION AND COMPARISON

The main objective of the proposed scheme is to provide the required security properties (as discussed in Section III-C) and to ensure a reasonable computational overhead. We compare the security of our scheme with state of the art protocols introduced in previous literature [3], [4], [5], [6]. Table II shows that all previously proposed schemes achieve mutual authentication but most [3], [4], [5], [6] fail to achieve *all* security properties required of 5G. For instance, 5G-AKA does not support strong anonymity and forward secrecy. Thus, schemes that use the original 5G-AKA protocol as their initial authentication phase can not support the strong anonymity and forward secrecy. RUSH [5] and LSHA [6] protocols, for example, support PFS and anonymity in handover. Nevertheless, due to their dependency on the standard 5G-AKA, their overall schemes provide only partial support for the former security properties. Next, from Table II, we see that only ReHand [4] provides revocation management. Still, the performance of their revocation decreases when the number of users increases, which is required for the scalability that 5G

TABLE III
TIME COSTS OF CRYPTOGRAPHY OPERATIONS.

Notation	T_P	T_{SM}	T_{MSM}	T_E	T_{MAC}	T_H	T_{PRG}	T_{AES}	T_{ECC}	T_{Mod}
T_{UE} (ms)	13.199	0.926	1.150	1.205	0.103	0.167	0.294	0.804	12.130	0.008
T_{Sys} (ms)	7.479	0.235	0.294	0.340	0.071	0.089	0.1273	0.427	10.922	0.001

T_P: pairing operation, T_{SM}: scalar multiplication, T_{MSM}: multi elliptic curve scalar multiplication, T_E: exponentiation operation, T_{MAC}: Massage authentication operations(Hmac-SHA256), T_H: Hash operations(SHA-256), T_{PRG}: Random number generators,T_{AES}:Symmetric encryption/decryption operations, T_{ECC}: Asymmetric encryption/decryption operations, T_{Mod}: Modular operations

TABLE IV
PERFORMANCE COMPARISON BASED ON COMPUTATIONAL COST
(INITIAL AUTHENTICATION).

Protocol	Entity	Initial authentication	Total time (ms)
Conventional 5G-AKA [3]	T_{UE}	$4T_{PRG} + 2T_{MAC} + T_{AES}$	$\approx$ 2.186
	T_{Sys}	$3T_{PRG} + 1T_{MAC} + 2T_H + T_{ECC}$	$\approx$ 11.553
ReHand [4]	T_{UE}	$2T_{AES} + 4T_H + T_{PRG}$	$\approx$ 2.57
	T_{Sys}	$3T_{AES} + 5T_H + T_{PRG}$	$\approx$ 1.8533
RUSH [5]	T_{UE}	$7T_{PRG} + 2T_{MAC} + T_{ECC} + 3T_H + T_E + 5T_{Mod} + 3T_{SM}$	$\approx$ 18.918
	T_{Sys}	$4T_{PRG} + 1T_{MAC} + 3T_H + T_{ECC} + 2T_{SM} + 3T_{Mod}$	$\approx$ 12.2422
LSHA [6]	T_{UE}	$4T_{PRG} + 2T_{MAC} + T_{AES}$	$\approx$ 2.188
	T_{Sys}	$3T_{PRG} + 1T_{MAC} + 2T_H + T_{ECC}$	$\approx$ 11.5529
OURs	T_{UE}	$3T_{PRG} + 5T_{AES} + T_H + T_P + 7T_E + T_{Mod}$	$\approx$ 26.631
	T_{Sys}	$7T_{PRG} + 3T_H + 5T_{AES} + 10T_E + 2T_{Mod}$	$\approx$ 6.693

TABLE V
PERFORMANCE COMPARISON BASED ON COMPUTATIONAL COST
(INTRA-REGION HANDOVER).

Protocol	Entity	Intra-region Handover	Total time (ms)
Conventional 5G-AKA [3]	T_{UE}	$4T_{AES} + T_{PRG}$	$\approx$ 3.51
	T_{Sys}	$4T_{AES} + T_{PGR}$	$\approx$ 1.835
ReHand [4]	T_{UE}	$T_{PGR} + 3T_H + T_{AES}$	$\approx$ 1.599
	T_{Sys}	$T_{PRG} + 5T_H + 2T_{AES}$	$\approx$ 1.426
RUSH [5]	T_{UE}	$3T_{PRG} + T_{SM} + 5T_H + T_E + T_{Mod}$	$\approx$ 2.856
	T_{Sys}	$2T_{PRG} + T_{SM} + 6T_H + T_E + T_{Mod}$	$\approx$ 1.365
LSHA [6]	T_{UE}	$2T_{PRG} + T_{MAC} + 4T_{AES}$	$\approx$ 3.907
	T_{Sys}	$7T_{PRG} + T_{MAC} + 6T_{AES} + 12T_{Mod}$	$\approx$ 3.536
OURs	T_{UE}	$2T_{PGR} + 2T_{AES} + T_h + T_E + T_{Mod}$	$\approx$ 3.555
	T_{Sys}	$5T_{PGR} + 2T_{AES} + T_P + T_h + 7T_E + T_{Mod}$	$\approx$ 11.42

TABLE VI
COMPUTATIONAL COST OF THE INTER-REGION HANDOVER.

Protocol	Entity	Inter-region Handover	Total time (ms)
OURs	T_{UE}	$2T_{PGR} + 2T_{AES} + T_H + T_P + 7T_E + T_{Mod}$	$\approx$ 23.96
	T_{Sys}	$6T_{PGR} + 2T_{AES} + 2T_H + T_P + 15T_E + T_{Mod}$	$\approx$ 14.37

schemes must achieve. While LUSH [5] achieves inter-region HO, their proposed solution requires blockchain technologies, and the security and the performance of the blockchain in the authentication and handover schemes have been overlooked. In contrast, our proposed scheme can achieve a secure inter-region HO without the use of blockchain.

Next, we evaluate and compare the performance of the proposed scheme with the existing related works. We assume that all the aggregated network entities (AuC, HgNB, gNB) have higher computational capabilities than UE. Now, we conduct simulations of the cryptographic operations used by various schemes on a Dell Inspiron machine with i7 core, 2.30GHz CPU and 16.0 GB RAM (operating as the aggregated network entities as per the scheme). To simulate the UE/smartphone, we use the Android studio emulator (Nexus 6) that runs Android API Tiramisu and is equipped with 1.5GB RAM with a six-core 3.0GHz processor. To implement the required cryptographic operations of our proposed scheme and the related works we used the java pairing-based cryptography (JPBC) [20] and Java Cryptography Extension (JCE) [21]. Table III shows the computation cost of the underlying cryptographic primitives, and use this to measure the overall computational cost of the protocols.

Table IV presents the computational cost of the initial authentication protocols, which shows that the conventional 5G-AKA protocol is cheapest in terms of computational cost. However, the conventional 5G-AKA protocol does not support strong anonymity and forward secrecy properties. On the contrary, our proposed protocol achieves all security properties (demonstrated in Section V and Appendix-C of the supplementary material). Our proposed scheme introduces computational overhead compared to existing solutions, as shown in Table IV and Table V, required to achieve stronger security properties. Furthermore, our schemes are more flexible, supporting more secure handover settings in the 5G-based mobile communication environments. Finally, Table VI presents the computational cost of inter-region HO of our proposed protocol only. Although RUSH supports the inter-region HO using blockchain, as previously discussed, the computational impact of using blockchain technologies in RUSH has been overlooked. For the Inter-region HO, our protocol requires approximately 23.96 ms and 14.37 ms on UE and system components (HgNB, gNB), respectively. Since we are the *first*, up to our knowledge, that provides a secure inter-region HO solution without the assistance of a third party (AuC) or the intervention of external technology (blockchain), we consider this to be an acceptable performance for our setting. Additionally, our scheme targets the SCN scenario, which reduces the geographical distance between the users and BSs. Hence, latency generated by the geographical distance is reduced in the SCN scenario in 5G, which plays in favour of our scheme's latency. In order to further reduce the online computational cost, the network components (AuC, gNB and HgNB) can perform *Batch Verification* for verifying users' certificates, where the batch verification can be defined as a method for verifying a large number of digital signatures simultaneously to accelerate signature verification process. The computational overhead of both signing and verifying of sanitisable signatures requires several pairing operations, which requires significant processing time. To resolve this issue, in our scheme, both the signers and verifiers (i.e., network components and UE) can pre-compute the majority of the required pairing operations for signing and verifying sanitisable signatures. In this way, our proposed scheme can reduce the number of pairing operations during the execution of the protocols, and that optimises the computational cost.

VII. Conclusion

This paper highlights a need for a secure handover scheme that supports seamless mobility in 5G, specifically for a setting that supports SCNs. We evaluate the limitations of the existing solutions, which are insufficient for realising 5G stringent requirements of secure, privacy-preserving and reliable handover authentication mechanisms. This paper introduces an asymmetric-key-based authenticated key exchange and handover protocol that preserves user privacy and network security while providing a seamless region-based handover mechanism and an effective membership revocation management. We prove that all proposed protocols achieve strong mutual authentication, key indistinguishability and strong user anonymity, through the use of the underlying secure cryptographic functions, such as sanitisable signatures, ephemeral Diffie-Hellman key exchange, key derivation functions and authenticated encryption. The proposed 'privacy-aware secure region-based handover protocol for small-cell networks in 5G-enabled mobile communication' achieved the required security properties for roaming users in SCN 5G networks. Finally, we evaluated the performance of our proposed schemes, and compared them with existing solutions for 5G, and demonstrated that our schemes compare well. As for future work, we will be focusing on addressing the heterogeneity of the 5G networks (HetNets) with SCN by designing a cross-layer-based authentication protocol.

References

[1] A. Holst, "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by communications technology," Oct. 2021.

[2] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, "A Survey on Security Aspects for 3GPP 5G Networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 170–195, 2020. Conference Name: IEEE Communications Surveys & Tutorials.

[3] E. 3rd Generation Partnership Project (3GPP), "Security architecture and procedures for 5G System," Technical Specification version 16.3.0 Release 16, 3GPP, Aug. 2020.

[4] C.-I. Fan, J.-J. Huang, M.-Z. Zhong, R.-H. Hsu, W.-T. Chen, and J. Lee, "ReHand: Secure Region-Based Fast Handover With User Anonymity for Small Cell Networks in Mobile Communications," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 927–942, 2020.

[5] Y. Zhang, R. H. Deng, E. Bertino, and D. Zheng, "Robust and Universal Seamless Handover Authentication in 5G HetNets," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, pp. 858–874, Mar. 2021.

[6] X. Yan and M. Ma, "A lightweight and secure handover authentication scheme for 5G network using neighbour base stations," *Journal of Network and Computer Applications*, vol. 193, p. 103204, Nov. 2021.

[7] J. Arkko, V. Lehtovirta, and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')," Request for Comments RFC 5448, Internet Engineering Task Force, May 2009. Num Pages: 29.

[8] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A Formal Analysis of 5G Authentication," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, (New York, NY, USA), pp. 1383–1396, Association for Computing Machinery, Oct. 2018.

[9] C. Cremers and M. Dehnel-Wild, "Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion," (San Diego, CA, USA), Feb. 2019.

[10] A. Braeken, "Symmetric key based 5G AKA authentication protocol satisfying anonymity and unlinkability," *Computer Networks*, vol. 181, p. 107424, Nov. 2020.

[11] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, "New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols," Tech. Rep. 1175, 2018.

[12] A. Peltonen, R. Sasse, and D. Basin, "A comprehensive formal analysis of 5G handover," in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '21, (New York, NY, USA), pp. 1–12, Association for Computing Machinery, June 2021.

[13] P.-A. Fouque, C. Onete, and B. Richard, "Achieving Better Privacy for the 3GPP AKA Protocol," Tech. Rep. 480, 2016.

[14] K. Nyberg, "Fast accumulated hashing," in *Fast Software Encryption* (D. Gollmann, ed.), Lecture Notes in Computer Science, (Berlin, Heidelberg), pp. 83–87, Springer, 1996.

[15] J. Li, N. Li, and R. Xue, "Universal Accumulators with Efficient Nonmembership Proofs," in *Applied Cryptography and Network Security* (J. Katz and M. Yung, eds.), Lecture Notes in Computer Science, (Berlin, Heidelberg), pp. 253–269, Springer, 2007.

[16] G. Ateniese, D. H. Chou, B. de Medeiros, and G. Tsudik, "Sanitizable Signatures," in *Computer Security – ESORICS 2005* (S. d. C. di Vimercati, P. Syverson, and D. Gollmann, eds.), Lecture Notes in Computer Science, (Berlin, Heidelberg), pp. 159–177, Springer, 2005.

[17] 3GPP, "ETSI TS 133 320 V15.0.0 (2018-07) - Universal Mobile Telecommunications System (UMTS); LTE; Security of Home Node B (HNB) / Home evolved Node B (HeNB) (3GPP TS 33.320 version 15.0.0 Release 15)," Tech. Rep. V15.0.0, 2018.

[18] P. Gope, J. Lee, and T. Q. S. Quek, "Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Networks," *IEEE Sensors Journal*, vol. 17, pp. 498–503, Jan. 2017.

[19] P. Gope, "LAAP: Lightweight anonymous authentication protocol for D2D-Aided fog computing paradigm," *Computers & Security*, vol. 86, pp. 223–237, Sept. 2019.

[20] A. De Caro and V. Iovino, *jPBC: Java pairing based cryptography*. Proceedings of the 16th IEEE Symposium on Computers and Communications, ISCC 2011, IEEE, 2011.

[21] O. Technology Network., "Java Cryptography Architecture (JCA) Reference Guide."