Cryptographically secure multiparty evaluation of system reliability

Louis J. M. Aslett (aslett@stats.ox.ac.uk)

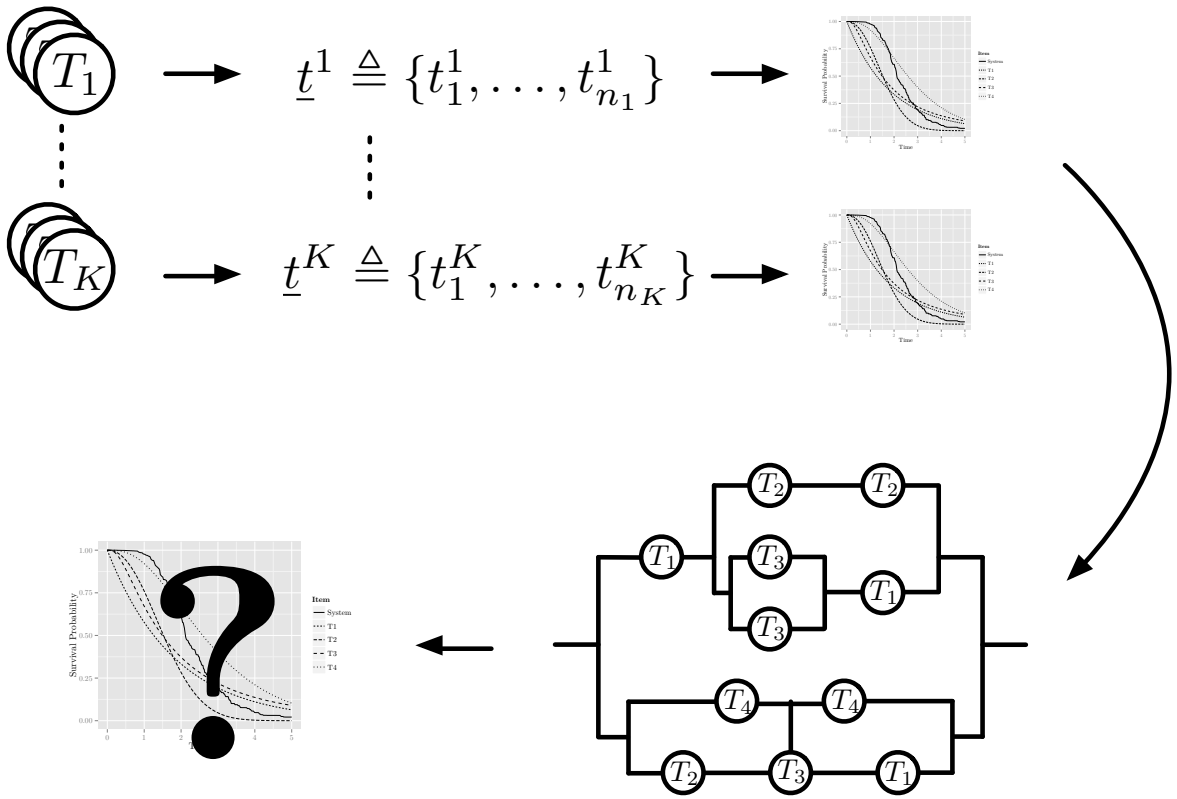
Department of Statistics, University of Oxford
and Corpus Christi College, Oxford

CASI 2015
12 May 2015

Introduction

Introduction (I)

Objective: inference on system/network reliability given component test data.

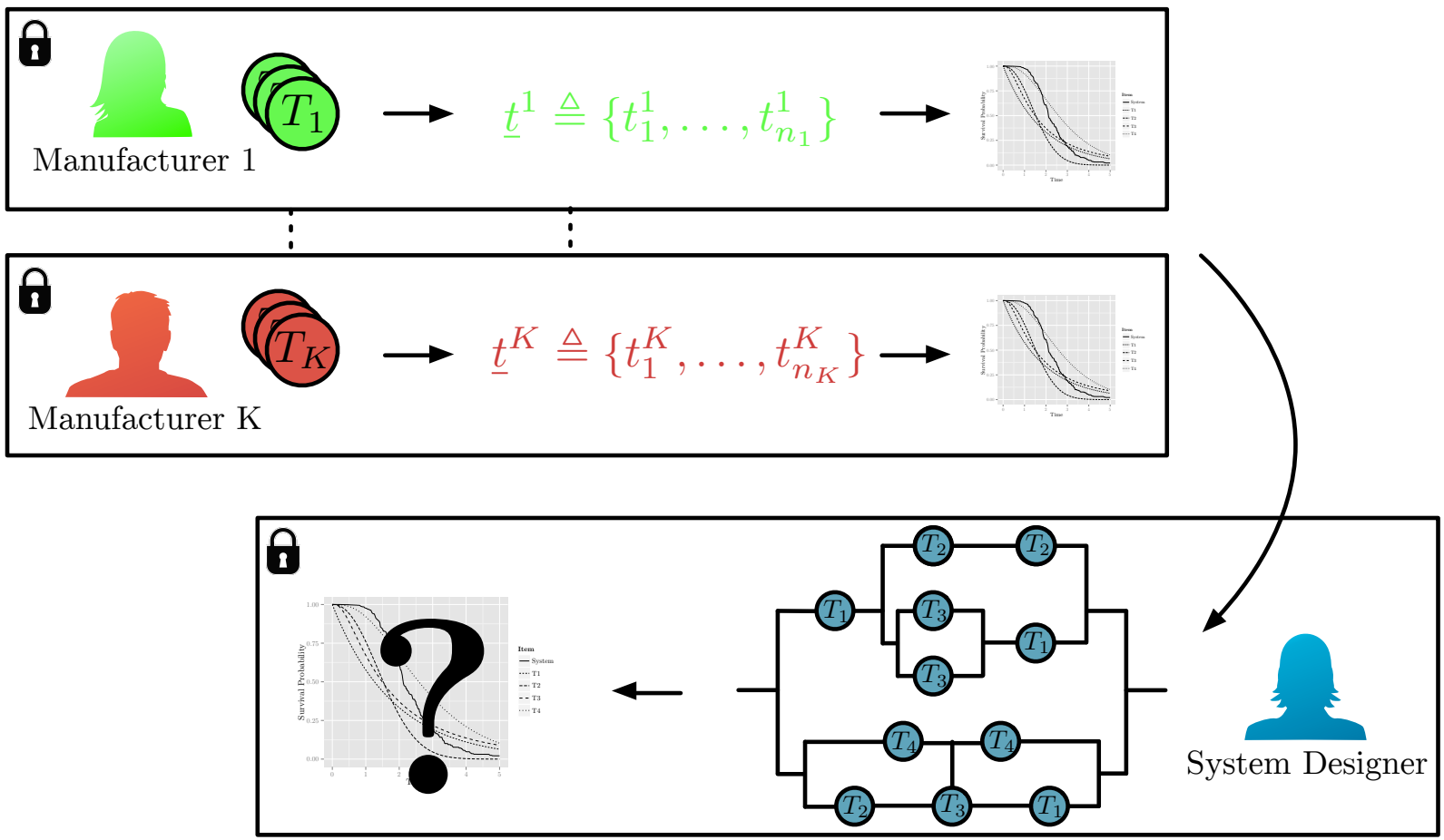


Aslett, L. J. M., Coolen, F. P. A., & Wilson, S. P. (2014). Bayesian inference for reliability of systems and networks using the survival signature. *Risk Analysis*.

Introduction (II)

But, what are the privacy requirements of data owners?

New objective: inference on system/network reliability *maintaining privacy*.



Introduction (III)

Developments in cryptography in 2009 solved an open problem which existed since 1978.

We'll see these developments enable preservation of privacy, almost completely, because the survival signature allows system lifetime to be expressed as a low order homogeneous polynomial.

$$\mathbb{P}(T_S > t) \overset{iid}{=} \sum_{l_1=0}^{m_1} \cdots \sum_{l_K=0}^{m_K} \left[\Phi(l_1, \ldots, l_K) \prod_{k=1}^{K} \binom{m_k}{l_k} [F_k(t)]^{m_k - l_k} [\bar{F}_k(t)]^{l_k} \right]$$

An accessible background on emerging area of encryption and statistics appearing soon:

Aslett, L. J. M., Esperança, P., & Holmes, C. C. (2015). Secure statistical analysis. *Technical report, University of Oxford*.

Bayesian Inference

Component inference (non-parametric I)

Or, non-parametrically we can observe that at fixed time t, probability a component of type k functions is Bernoulli(p_t^k) for some unknown p_t^k.

$\implies$ number functioning at time t in iid batch of n_k is Binomial(n_k, p_t^k).

Let $S_t^k \in \{0, 1, \ldots, n_k\}$ be number of working components in test batch of n_k components of type k. Then,

$$S_t^k \sim \text{Binomial}(n_k, p_t^k) \;\; \forall\, t > 0$$

Given the same test data $\underline{t}^k = \{t_1^k, \ldots, t_{n_k}^k\}$, for each t we can form corresponding observation from Binomial model

$$s_t^k \triangleq \sum_{i=1}^{n_k} \mathbb{I}(t_i^k > t)$$

Component inference (non-parametric II)

Taking prior $p_t^k \sim \text{Beta}(\alpha_t^k, \beta_t^k)$, exploit conjugacy result

$$p_t^k \mid s_t^k \sim \text{Beta}(\alpha_t^k + s_t^k, \beta_t^k + n_k - s_t^k)$$

Then, posterior predictive for number of components surviving in a new batch of m_k components is

$$C_t^k \mid s_t^k \sim \text{Beta-binomial}(m_k, \alpha_t^k + s_t^k, \beta_t^k + n_k - s_t^k)$$

Component inference (non-parametric II)

Taking prior $p_t^k \sim \text{Beta}(\alpha_t^k, \beta_t^k)$, exploit conjugacy result

$$p_t^k \mid s_t^k \sim \text{Beta}(\alpha_t^k + s_t^k, \beta_t^k + n_k - s_t^k)$$

Then, posterior predictive for number of components surviving in a new batch of m_k components is

$$C_t^k \mid s_t^k \sim \text{Beta-binomial}(m_k, \alpha_t^k + s_t^k, \beta_t^k + n_k - s_t^k)$$

Summary: for any fixed t, s_t^k provides a minimal sufficient statistic for computing posterior predictive distribution of the number of components surviving to t in a new batch, without any parametric model for component lifetime being assumed.

Survival signature

Coolen & Coolen-Maturi (2012) rethought signatures with the objective of retaining separation of structure and component lifetimes for multiple component types.

Definition (Survival signature)

Consider a system comprising K component types, with m_k components of type $k \in \{1, \ldots, K\}$. Then the *survival signature* $\Phi(l_1, \ldots, l_K)$, with $l_k \in \{0, 1, \ldots, m_k\}$, is the probability that the system functions given precisely l_k of its components of type k function.

$$\Phi(l_1, \ldots, l_K) = \left[\prod_{k=1}^{K} \binom{m_k}{l_k}^{-1} \right] \sum_{\underline{x} \in S_{l_1, \ldots, l_K}} \varphi(\underline{x})$$

where $S_{l_1, \ldots, l_K} = \{\underline{x} : \sum_{i=1}^{m_k} x_i^k = l_k \quad \forall\, k\}$

Propagate uncertainty: survival signature

$$
\begin{aligned}
&P(T_{S^*} > t \,|\, s_t^1, \ldots s_t^K) \\
&= \int \cdots \int P(T_{S^*} > t \,|\, p_t^1, \ldots p_t^K) P(p_t^1 \,|\, s_t^1) \ldots P(p_t^K \,|\, s_t^K)\, dp_t^1 \ldots dp_t^K \\
&= \int \cdots \int \left[\sum_{l_1=0}^{m_1} \cdots \sum_{l_K=0}^{m_K} \Phi(l_1, \ldots, l_K) P\left(\bigcap_{k=1}^{K} \{C_t^k = l_k \,|\, p_t^k\} \right) \right] \\
&\qquad \times P(p_t^1 \,|\, s_t^1) \ldots P(p_t^K \,|\, s_t^K)\, dp_t^1 \ldots dp_t^K \\
&= \sum_{l_1=0}^{m_1} \cdots \sum_{l_K=0}^{m_K} \Phi(l_1, \ldots, l_K) \prod_{k=1}^{K} \int P(C_t^k = l_k \,|\, p_t^k) P(p_t^k \,|\, s_t^k)\, dp_t^k
\end{aligned}
$$

Final term post pred of l_k comp of type k surviving to t.

Homomorphic Encryption

Introduction to cryptography

- Unencrypted number, $m \in M$, is referred to as a *message*.
- Encrypted version, $c \in C$, is referred to as a *cipher text*.
- Pair of 'keys' (k_s, k_p), secret and public.
- Injective map (*not* function), $\texttt{Enc} : M \to C$.
- Surjective function, $\texttt{Dec} : C \to M$.

Fundamental point

$$\texttt{Enc}(k_p, m) \rightleftharpoons c$$

Easy

Hard without k_s

$$\texttt{Dec}(k_s, c) = m$$

$\therefore$ crucial relation:

$$m = \texttt{Dec}(k_s, \texttt{Enc}(k_p, m)) \quad \forall\, m \in M$$

'Brittle' encryption

Most cryptography schemes are 'brittle' in that we can't manipulate the contents of the mathematical vault: must decrypt to compute, then encrypt the result. i.e. seems only useful for shipping round static data!

In other words, if

$$c_1 = \mathsf{Enc}(k_p, m_1)$$
$$c_2 = \mathsf{Enc}(k_p, m_2)$$

then in general, for a given function $g(\cdot,\cdot)$, $\nexists\, f(\cdot,\cdot)$ (not requiring k_s) such that

$$\mathsf{Dec}(k_s, f(c_1, c_2)) = g(m_1, m_2) \quad \forall\, m_1, m_2 \in M$$

Homomorphic encryption

Rivest et al. (1978) hypothesised that a limited set of functions may be possible to compute encrypted: specifically those involving addition and multiplication (theoretically exciting $\rightarrow$ computational complexity & polynomial approx).

Definition (Homomorphic encryption scheme)

An encryption scheme is said to be *homomorphic* if there is a set of operations $\circ \in \mathcal{F}_M$ acting in message space (such as addition) that have corresponding operations $\diamond \in \mathcal{F}_C$ acting in cipher text space satisfying the property:

$$\mathtt{Dec}(k_s, \mathtt{Enc}(k_p, m_1) \diamond \mathtt{Enc}(k_p, m_2)) = m_1 \circ m_2 \quad \forall\, m_1, m_2 \in M$$

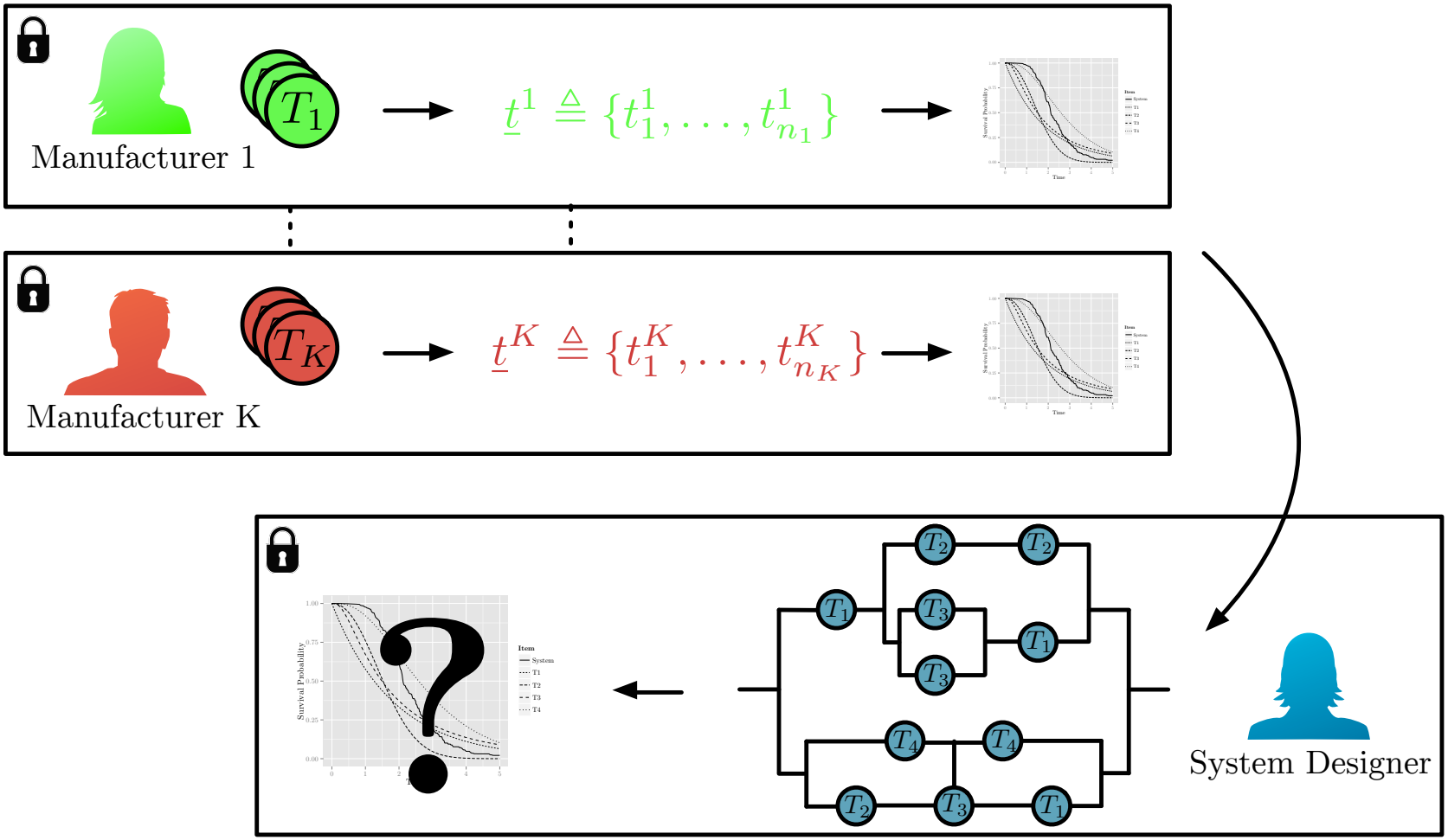
A scheme is *fully homomorphic* if $\mathcal{F}_M = \{+, \times\}$ and an arbitrary number of such operations are possible.

Limitations of homomorphic encryption

1. Message space
   - Commonly only easy to encrypt binary/integers
2. Cipher text size
   - Present schemes all inflate the size of data substantially (e.g. 1MB $\rightarrow$ 16.4GB)
3. Computational cost
   - 1000's additions per sec
   - $\approx$ 50 multiplications per sec
4. Division and comparison operations
   - Impossible!
5. Depth of operations
   - After a certain depth of multiplications, need to 'refresh' cipher text: hugely time consuming, so avoid!

Privacy Preserving Protocol

Back to the problem at hand ...

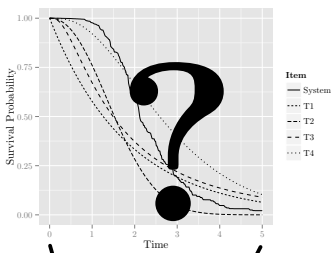


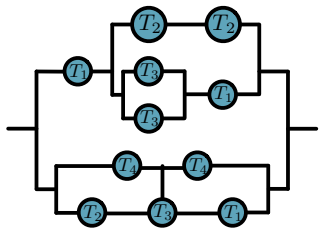
k_s k_p

System Designer

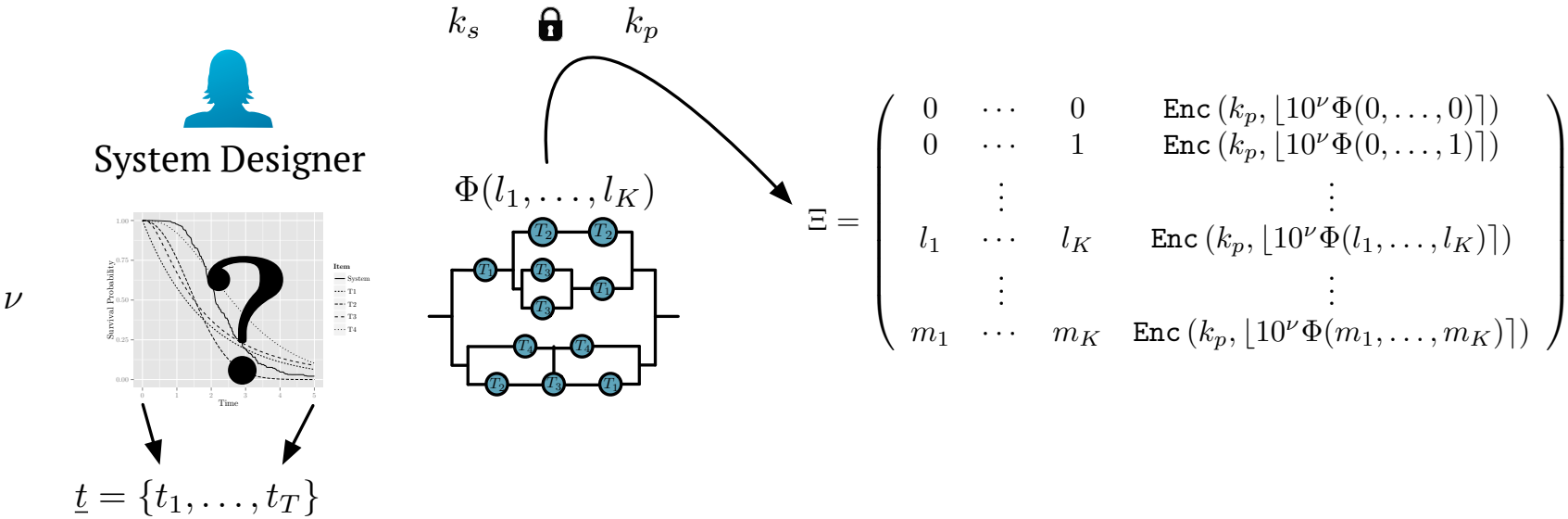
$\Phi(l_1, \ldots, l_K)$

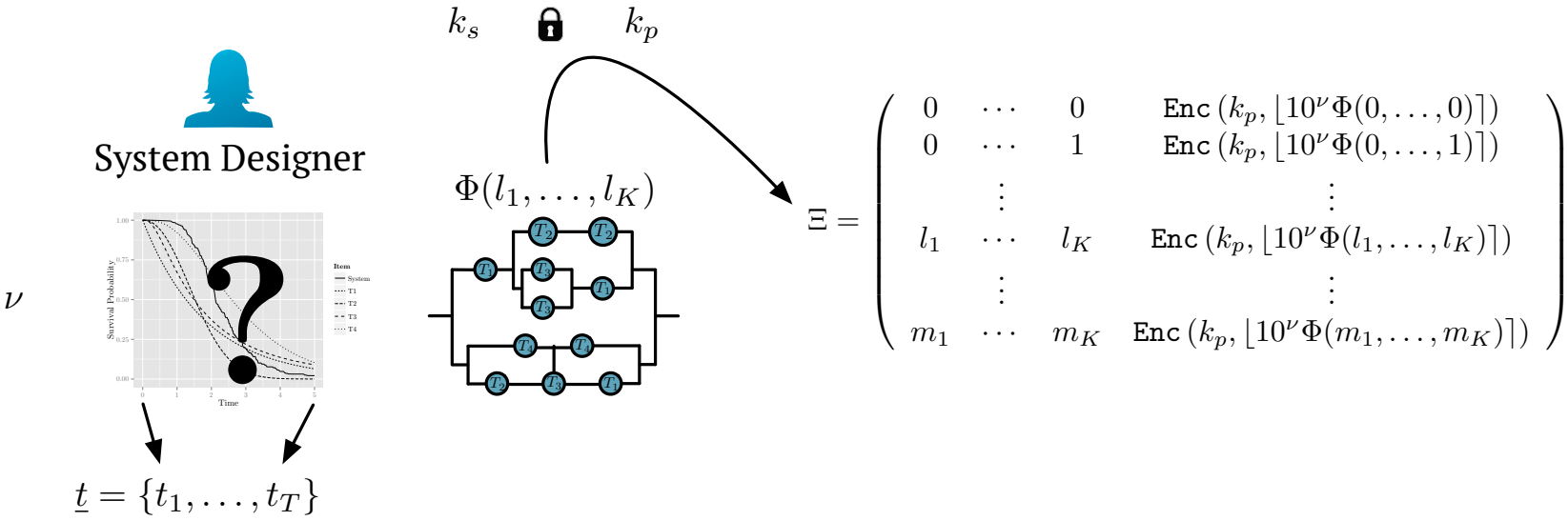
ν

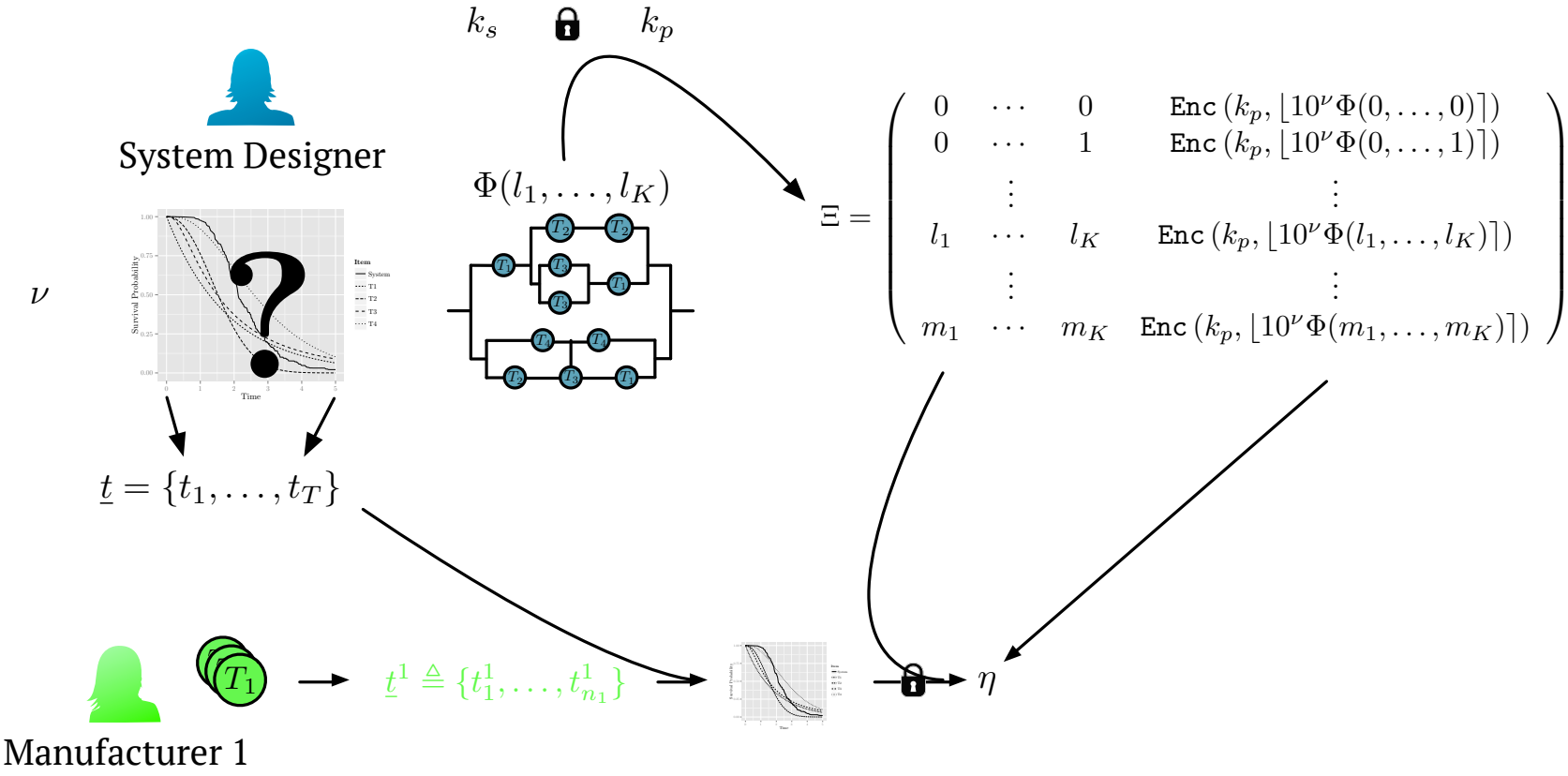


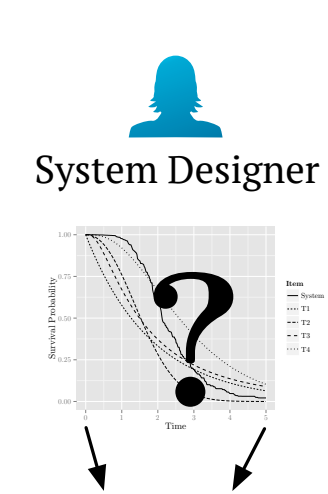


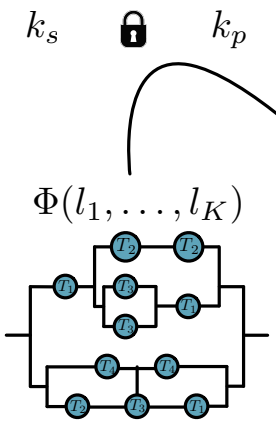
$\underline{t} = \{t_1, \ldots, t_T\}$


k_s
k_p
System Designer
ν
$\Phi(l_1, \ldots, l_K)$
$\underline{t} = \{t_1, \ldots, t_T\}$
$\Xi =$
$\begin{pmatrix} 0 & \cdots & 0 & \texttt{Enc}\left(k_p, \lfloor 10^\nu \Phi(0, \ldots, 0) \rceil\right) \\ 0 & \cdots & 1 & \texttt{Enc}\left(k_p, \lfloor 10^\nu \Phi(0, \ldots, 1) \rceil\right) \\ & \vdots & & \vdots \\ l_1 & \cdots & l_K & \texttt{Enc}\left(k_p, \lfloor 10^\nu \Phi(l_1, \ldots, l_K) \rceil\right) \\ & \vdots & & \vdots \\ m_1 & \cdots & m_K & \texttt{Enc}\left(k_p, \lfloor 10^\nu \Phi(m_1, \ldots, m_K) \rceil\right) \end{pmatrix}$

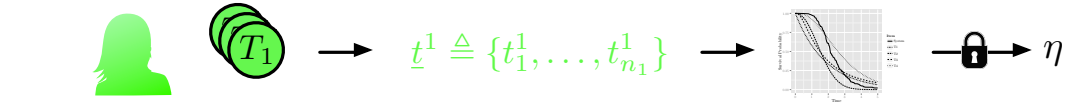

k_s
k_p
System Designer
$\Phi(l_1, \ldots, l_K)$
ν
$\underline{t} = \{t_1, \ldots, t_T\}$
$\Xi =$
$\begin{pmatrix} 0 & \cdots & 0 & \texttt{Enc}\left(k_p, \lfloor 10^\nu \Phi(0, \ldots, 0) \rceil\right) \\ 0 & \cdots & 1 & \texttt{Enc}\left(k_p, \lfloor 10^\nu \Phi(0, \ldots, 1) \rceil\right) \\ & \vdots & & \vdots \\ l_1 & \cdots & l_K & \texttt{Enc}\left(k_p, \lfloor 10^\nu \Phi(l_1, \ldots, l_K) \rceil\right) \\ & \vdots & & \vdots \\ m_1 & \cdots & m_K & \texttt{Enc}\left(k_p, \lfloor 10^\nu \Phi(m_1, \ldots, m_K) \rceil\right) \end{pmatrix}$
Manufacturer 1
$\underline{t}^1 \triangleq \{t_1^1, \ldots, t_{n_1}^1\}$

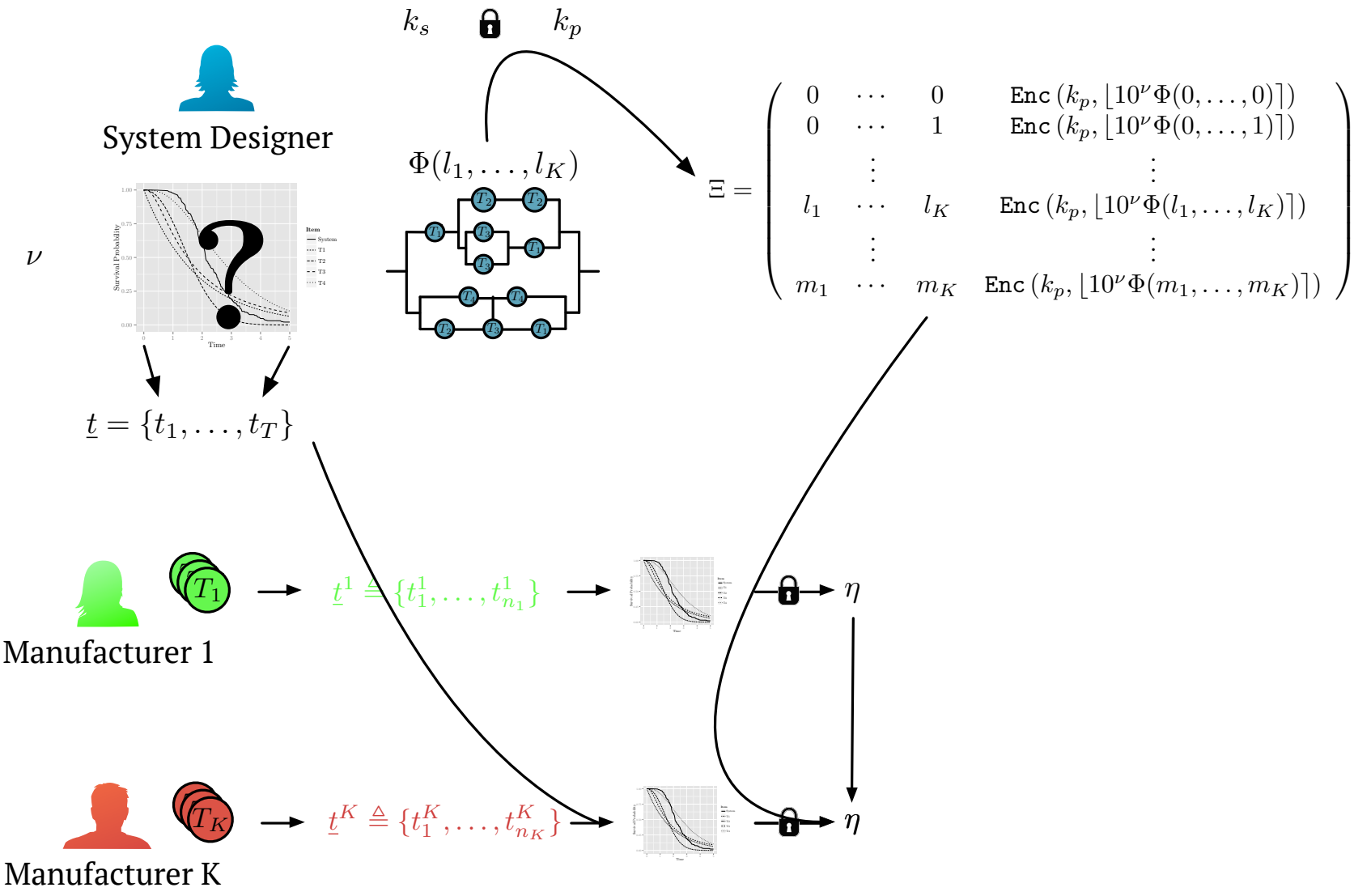

k_s
k_p
System Designer
$\Phi(l_1, \ldots, l_K)$
$\Xi =$
$\begin{pmatrix} 0 & \cdots & 0 & \texttt{Enc}\,(k_p, \lfloor 10^\nu \Phi(0, \ldots, 0) \rceil) \\ 0 & \cdots & 1 & \texttt{Enc}\,(k_p, \lfloor 10^\nu \Phi(0, \ldots, 1) \rceil) \\ & \vdots & & \vdots \\ l_1 & \cdots & l_K & \texttt{Enc}\,(k_p, \lfloor 10^\nu \Phi(l_1, \ldots, l_K) \rceil) \\ & \vdots & & \vdots \\ m_1 & \cdots & m_K & \texttt{Enc}\,(k_p, \lfloor 10^\nu \Phi(m_1, \ldots, m_K) \rceil) \end{pmatrix}$
ν
Survival Probability
Time
Item
System
T1
T2
T3
T4
$\underline{t} = \{t_1, \ldots, t_T\}$
T_1
$\underline{t}^1 \triangleq \{t_1^1, \ldots, t_{n_1}^1\}$
η
Manufacturer 1

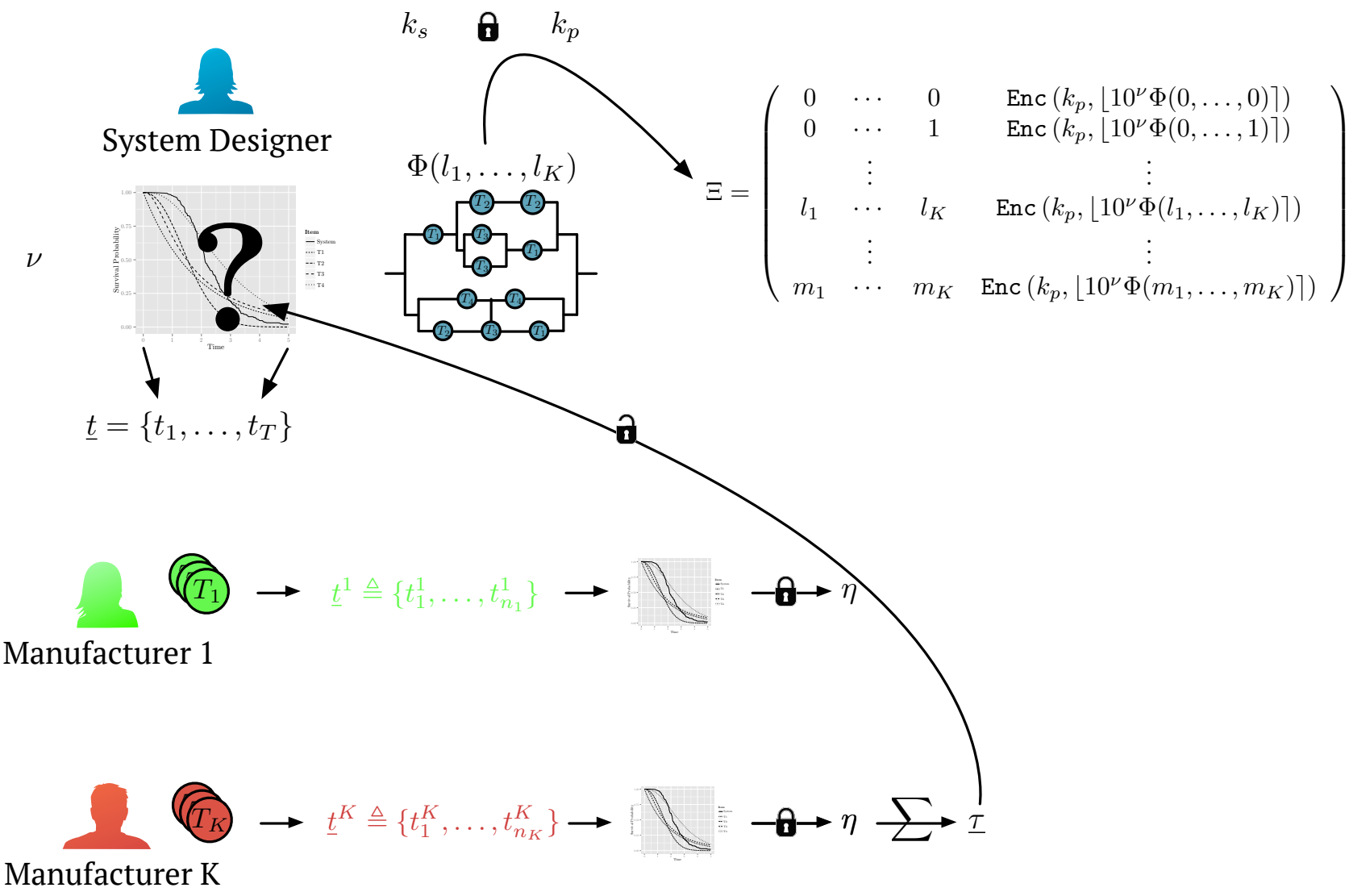




$$\Xi = \begin{pmatrix} 0 & \cdots & 0 & \texttt{Enc}\left(k_p, \lfloor 10^{\nu}\Phi(0,\ldots,0)\rceil\right) \\ 0 & \cdots & 1 & \texttt{Enc}\left(k_p, \lfloor 10^{\nu}\Phi(0,\ldots,1)\rceil\right) \\ & \vdots & & \vdots \\ l_1 & \cdots & l_K & \texttt{Enc}\left(k_p, \lfloor 10^{\nu}\Phi(l_1,\ldots,l_K)\rceil\right) \\ & \vdots & & \vdots \\ m_1 & \cdots & m_K & \texttt{Enc}\left(k_p, \lfloor 10^{\nu}\Phi(m_1,\ldots,m_K)\rceil\right) \end{pmatrix}$$




k_s
k_p
System Designer
$\Phi(l_1, \ldots, l_K)$
$\Xi =$
$\begin{pmatrix} 0 & \cdots & 0 & \texttt{Enc}\,(k_p, \lfloor 10^\nu \Phi(0, \ldots, 0) \rceil) \\ 0 & \cdots & 1 & \texttt{Enc}\,(k_p, \lfloor 10^\nu \Phi(0, \ldots, 1) \rceil) \\ & \vdots & & \vdots \\ l_1 & \cdots & l_K & \texttt{Enc}\,(k_p, \lfloor 10^\nu \Phi(l_1, \ldots, l_K) \rceil) \\ & \vdots & & \vdots \\ m_1 & \cdots & m_K & \texttt{Enc}\,(k_p, \lfloor 10^\nu \Phi(m_1, \ldots, m_K) \rceil) \end{pmatrix}$
ν
$\underline{t} = \{t_1, \ldots, t_T\}$
$\underline{t}^1 \triangleq \{t_1^1, \ldots, t_{n_1}^1\}$
η
Manufacturer 1
$\underline{t}^K \triangleq \{t_1^K, \ldots, t_{n_K}^K\}$
η
Manufacturer K


k_s
k_p
System Designer
$\Phi(l_1, \ldots, l_K)$
$\Xi = \begin{pmatrix} 0 & \cdots & 0 & \texttt{Enc}\,(k_p, \lfloor 10^\nu \Phi(0, \ldots, 0) \rceil) \\ 0 & \cdots & 1 & \texttt{Enc}\,(k_p, \lfloor 10^\nu \Phi(0, \ldots, 1) \rceil) \\ & \vdots & & \vdots \\ l_1 & \cdots & l_K & \texttt{Enc}\,(k_p, \lfloor 10^\nu \Phi(l_1, \ldots, l_K) \rceil) \\ & \vdots & & \vdots \\ m_1 & \cdots & m_K & \texttt{Enc}\,(k_p, \lfloor 10^\nu \Phi(m_1, \ldots, m_K) \rceil) \end{pmatrix}$
ν
$\underline{t} = \{t_1, \ldots, t_T\}$
T_1
$\underline{t}^1 \triangleq \{t_1^1, \ldots, t_{n_1}^1\}$
η
Manufacturer 1
T_K
$\underline{t}^K \triangleq \{t_1^K, \ldots, t_{n_K}^K\}$
η
$\sum$
$\underline{\tau}$
Manufacturer K

References

Aslett, L. J. M., Coolen, F. P. A., & Wilson, S. P. (2014). Bayesian inference for reliability of systems and networks using the survival signature. *Risk Analysis*.

Aslett, L. J. M., Esperança, P., & Holmes, C. C. (2015). *Secure statistical analysis*. University of Oxford.

Coolen, F. P. A., & Coolen-Maturi, T. (2012). Generalizing the signature to systems with multiple types of components. *Complex systems and dependability*, pp. 115–30. Springer.

Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. *Foundations of Secure Computation*, 4/11: 169–80.