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

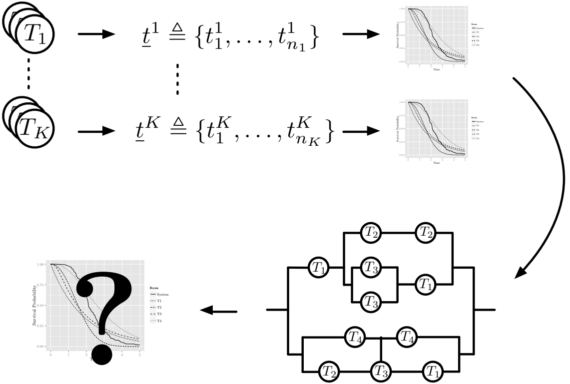
ISBIS 2016
7 June 2016

i-like.org.uk

Introduction

Introduction (I)

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

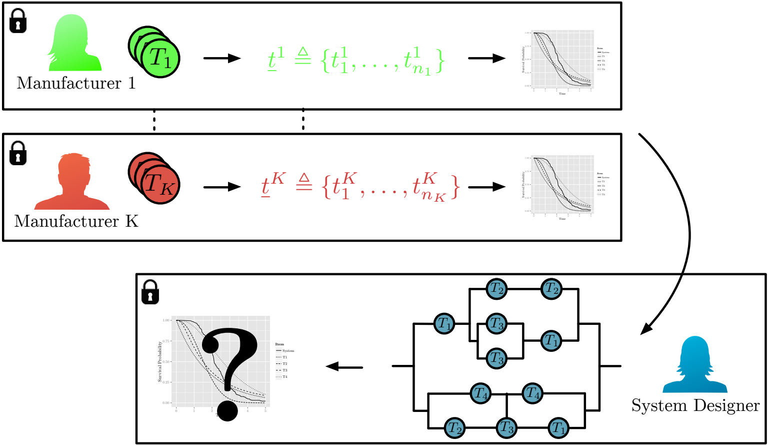


Aslett, L. J. M., Coolen, F. P. A., & Wilson, S. P. (2015). ‘Bayesian inference for reliability of systems and networks using the survival signature’, *Risk Analysis*, **35**(9), 1640–1651.

Introduction (II)

But, what are the privacy requirements of data owners?

New objective: inference on system/network reliability whilst *maintaining privacy requirements* of all parties.



Homomorphic Encryption

Encryption the solution?

Encryption can provide security guarantees …

Easy

$$\texttt{Enc}(k_p, m) \rightleftharpoons c \qquad\qquad \texttt{Dec}(k_s, c) = m$$

Hard without k_s

… but is typically ‘brittle’.

Encryption the solution?

Encryption can provide security guarantees ...

Easy

$\texttt{Enc}(k_p, m) \rightleftharpoons c \qquad \texttt{Dec}(k_s, c) = m$

Hard without k_s

... but is typically 'brittle'.

Rivest et al. (1978) proposed encryption schemes capable of arbitrary addition and multiplication may be possible. Gentry (2009) showed first **fully homomorphic encryption** scheme.

Encryption the solution?

Encryption can provide security guarantees …

$$\texttt{Enc}(k_p, m) \rightleftharpoons c \qquad \texttt{Dec}(k_s, c) = m$$

Easy

Hard without k_s

… but is typically 'brittle'.

Rivest et al. (1978) proposed encryption schemes capable of arbitrary addition and multiplication may be possible. Gentry (2009) showed first **fully homomorphic encryption** scheme.

$$m_1 \qquad m_2 \xrightarrow{+} m_1 + m_2$$

Encryption the solution?

Encryption can provide security guarantees …

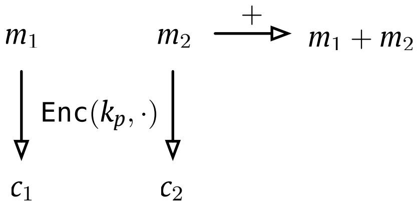
$$\texttt{Enc}(k_p, m) \rightleftharpoons c \qquad\qquad \texttt{Dec}(k_s, c) = m$$

Easy

Hard without k_s

… but is typically ‘brittle’.

Rivest et al. (1978) proposed encryption schemes capable of arbitrary addition and multiplication may be possible. Gentry (2009) showed first **fully homomorphic encryption** scheme.



Encryption the solution?

Encryption can provide security guarantees …

$$\texttt{Enc}(k_p, m) \rightleftharpoons c \qquad \texttt{Dec}(k_s, c) = m$$

Easy ($\rightarrow$); Hard without k_s ($\leftarrow$)

… but is typically ‘brittle’.

Rivest et al. (1978) proposed encryption schemes capable of arbitrary addition and multiplication may be possible. Gentry (2009) showed first **fully homomorphic encryption** scheme.

$$\begin{array}{ccccc} m_1 & & m_2 & \xrightarrow{+} & m_1 + m_2 \\ \downarrow & \texttt{Enc}(k_p, \cdot) & \downarrow & & \uparrow \texttt{Dec}(k_s, \cdot) \\ c_1 & & c_2 & \xrightarrow{\oplus} & c_1 \oplus c_2 \end{array}$$

Encryption the solution?

Encryption can provide security guarantees ...

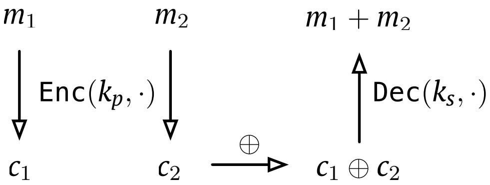
Easy

$\texttt{Enc}(k_p, m) \rightleftharpoons c \qquad \texttt{Dec}(k_s, c) = m$

Hard without k_s

... but is typically ‘brittle’.

Rivest et al. (1978) proposed encryption schemes capable of arbitrary addition and multiplication may be possible. Gentry (2009) showed first **fully homomorphic encryption** scheme.



Formal definition

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, M, that have corresponding operations $\diamond \in \mathcal{F}_C$ acting in cipher text space, C, satisfying the property:

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

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

Formal definition

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, M, that have corresponding operations $\diamond \in \mathcal{F}_C$ acting in cipher text space, C, satisfying the property:

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

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

$\{+, \times\}$ pretty limiting? Note that if $M = \text{GF}(2)$, then:

- $+ \equiv \veebar$, i.e. XOR, 'exclusive or'
- $\times \equiv \wedge$, i.e. AND, 'and'

Moreover, *any* electronic logic gate can be constructed using only XOR and AND gates.

Limitations of homomorphic encryption

1. Message space (what we can encrypt)
   - Commonly only easy to encrypt binary/integers/polynomials
2. Cipher text size (the result of encryption)
   - Present schemes all inflate the size of data substantially (e.g. 1MB $\to$ 16.4GB)
3. Computational cost (computing without decrypting)
   - 1000's additions per sec
   - $\approx$ 50 multiplications per sec
4. Division and comparison operations (equality/inequality checks)
   - Not possible in current schemes!
5. Depth of operations
   - After a certain depth of multiplications, need to 'refresh' cipher text: hugely time consuming, so avoid!

Survival Signature

Survival signature

Coolen & Coolen-Maturi (2012) rethought system signatures (Samaniego 1985) with the objective of retaining separation of structure and component lifetimes for multiple component types.

Survival signature

Coolen & Coolen-Maturi (2012) rethought system signatures (Samaniego 1985) with the objective of retaining separation of structure and component lifetimes for multiple component types.

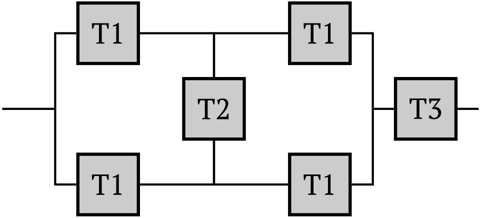
Definition (Survival signature)

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

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

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

Survival signature toy example



T1	T2	T3	Φ	T1	T2	T3	Φ
0	0	1	0	0	1	1	0
1	0	1	0	1	1	1	0
2	0	1	0.33	2	1	1	0.67
3	0	1	1	3	1	1	1
4	0	1	1	4	1	1	1

Table 1: Survival signature for a bridge system, omitting all rows with $T3 = 0$, since $\Phi = 0$ for these.

System lifetimes

Let $C_t^k \in \{0, 1, \ldots, M_k\}$ be random variable denoting number of components of type k surviving at time t. Then, survival function of system lifetime T_S is:

$$\begin{aligned}
\mathbb{P}(T_S > t) &= \sum_{l_1=0}^{M_1} \cdots \sum_{l_K=0}^{M_K} \Phi(l_1, \ldots, l_K)\, \mathbb{P}\left(\bigcap_{k=1}^{K} \{C_t^k = l_k\} \right) \\
&= \sum_{l_1=0}^{M_1} \cdots \sum_{l_K=0}^{M_K} \Phi(l_1, \ldots, l_K) \prod_{k=1}^{K} \mathbb{P}\left(C_t^k = l_k \right)
\end{aligned}$$

if the component types are independent.

System lifetimes

Let $C_t^k \in \{0, 1, \ldots, M_k\}$ be random variable denoting number of components of type k surviving at time t. Then, survival function of system lifetime T_S is:

$$\mathbb{P}(T_S > t) = \sum_{l_1=0}^{M_1} \cdots \sum_{l_K=0}^{M_K} \Phi(l_1, \ldots, l_K)\, \mathbb{P}\left(\bigcap_{k=1}^{K} \{C_t^k = l_k\} \right)$$
$$= \sum_{l_1=0}^{M_1} \cdots \sum_{l_K=0}^{M_K} \Phi(l_1, \ldots, l_K) \prod_{k=1}^{K} \mathbb{P}\left(C_t^k = l_k \right)$$

if the component types are independent.

Note: this is a homogeneous polynomial of degree $K + 1$ in the survival signature and component survival probabilities $\implies$ can evaluate encrypted.

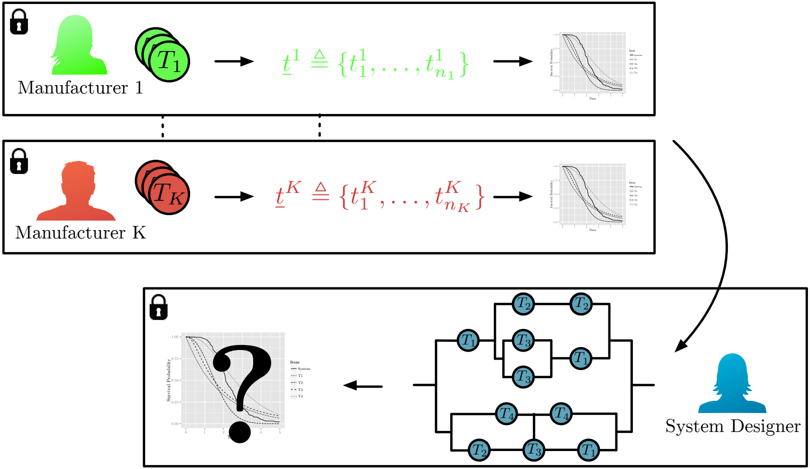
Propagating uncertainty as a Bayesian

$$
\begin{aligned}
&P(T_{S^*} > t \mid \underline{y}_1, \dots \underline{y}_K) \\
&= \int \cdots \int P(T_{S^*} > t \mid p_t^1, \dots p_t^K) P(dp_t^1 \mid \underline{y}_1) \dots P(dp_t^K \mid \underline{y}_K) \\
&= \int \cdots \int \left[\sum_{l_1=0}^{M_1} \cdots \sum_{l_K=0}^{M_K} \Phi(l_1, \dots, l_K) P\left(\bigcap_{k=1}^{K} \{C_t^k = l_k \mid p_t^k\} \right) \right] \\
&\qquad\qquad \times P(dp_t^1 \mid \underline{y}_1) \dots P(dp_t^K \mid \underline{y}_K) \\
&= \sum_{l_1=0}^{M_1} \cdots \sum_{l_K=0}^{M_K} \Phi(l_1, \dots, l_K) \prod_{k=1}^{K} \int P(C_t^k = l_k \mid p_t^k) P(dp_t^k \mid \underline{y}_k)
\end{aligned}
$$

A homogeneous polynomial of degree $K + 1$ in the survival signature and posterior predictive component survival probabilities at each time point $\implies$ can still evaluate encrypted.

Privacy Preserving Protocol

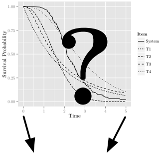
Back to the problem at hand ...



k_s k_p

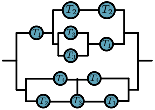
System Designer

ν



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

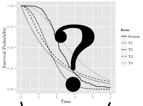
$\Phi(l_1, \ldots, l_K)$



k_s k_p

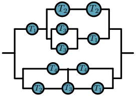
System Designer

ν



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

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

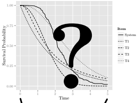


$$\Xi = \begin{pmatrix} 0 & \cdots & 0 & \texttt{Enc}\left(k_p, \lfloor 10^\nu \Phi(0, \dots, 0) \rceil\right) \\ 0 & \cdots & 1 & \texttt{Enc}\left(k_p, \lfloor 10^\nu \Phi(0, \dots, 1) \rceil\right) \\ & \vdots & & \vdots \\ l_1 & \cdots & l_K & \texttt{Enc}\left(k_p, \lfloor 10^\nu \Phi(l_1, \dots,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

k_s 🔒 k_p

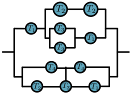
System Designer

ν



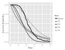
$\underline{t} = \{t_1, \dots, t_T\}$

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

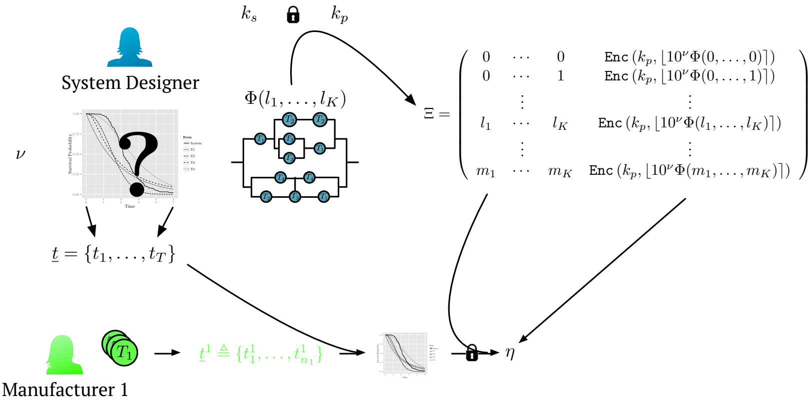


$$\Xi = \begin{pmatrix} 0 & \cdots & 0 & \texttt{Enc}\left(k_p, \lfloor 10^\nu \Phi(0,\dots,0) \rceil\right) \\ 0 & \cdots & 1 & \texttt{Enc}\left(k_p, \lfloor 10^\nu \Phi(0,\dots,1) \rceil\right) \\ & \vdots & & \vdots \\ l_1 & \cdots & l_K & \texttt{Enc}\left(k_p, \lfloor 10^\nu \Phi(l_1,\dots,l_K)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

$\rightarrow \underline{t}^1 \triangleq \{t_1^1, \dots, t_{n_1}^1\} \rightarrow$



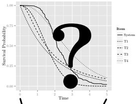
Manufacturer 1


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

k_s 🔒 k_p

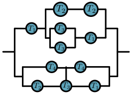
System Designer

ν



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

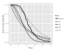
$\Phi(l_1, \ldots, l_K)$



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

Manufacturer 1

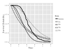
T_1 → $\underline{t}^1 \triangleq \{t_1^1, \ldots, t_{n_1}^1\}$ →



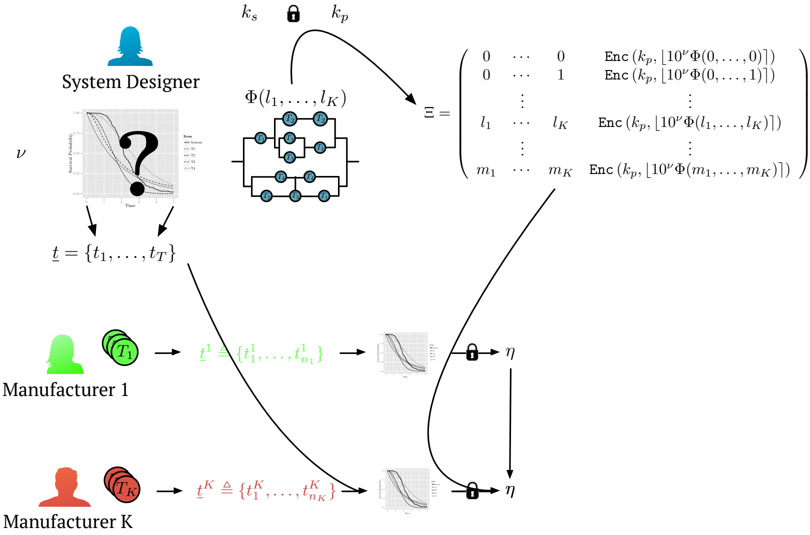
→ 🔒 → η

Manufacturer K

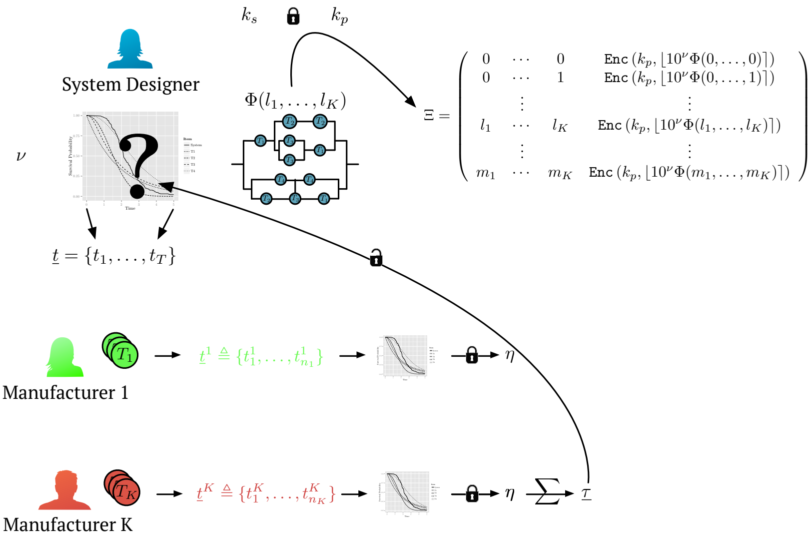
T_K → $\underline{t}^K \triangleq \{t_1^K, \ldots, t_{n_K}^K\}$ →



→ 🔒 → η



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



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
T_1
$\underline{t}^1 \triangleq \{t_1^1, \ldots, t_{n_1}^1\}$
η
Manufacturer K
T_K
$\underline{t}^K \triangleq \{t_1^K, \ldots, t_{n_K}^K\}$
η
$\sum$
$\underline{\tau}$

Example

Example system

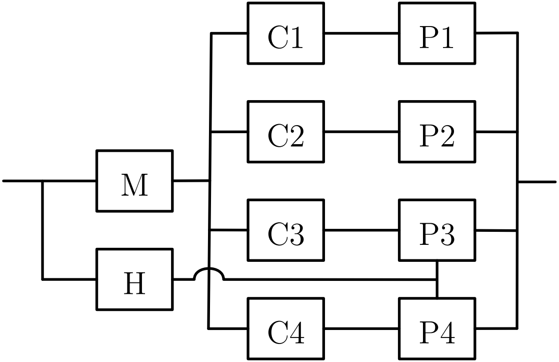


Figure 1: Simple automotive braking system. The master brake cylinder (M) engages all the four wheel brake cylinders (C1 – C4). These in turn each trigger a braking pad assembly (P1 – P4). The hand brake (H) goes directly to the rear brake pad assemblies P3 and P4; the vehicle brakes when at least one of the brake pad assemblies is engaged.

Experimental results

In order to examine the practicality of the problem, perform a full encrypted analysis using Amazon EC2 cloud computing service to mimic a global supply chain.

Role	Physical Server Location	Server Type
System designer	Dublin, Ireland	m4.10xlarge
Manufacturer C	Northern California, USA	m4.10xlarge
Manufacturer H	São Paulo, Brazil	c3.8xlarge
Manufacturer M	Sydney, Australia	r3.4xlarge
Manufacturer P	Tokyo, Japan	i2.8xlarge

Precision was set to $\nu = 5$ and system designer specifies an evenly spaced time grid of 100 points $t \in [0, 5]$.

Computational cost (I)

Role	Action	Timing / Size
System designer Dublin, Ireland	Generation of (k_p, k_s)	0.3 secs

Computational cost (I)

Role	Action	Timing / Size
System designer Dublin, Ireland	Generation of (k_p, k_s) Encryption of $\Xi^{(\Phi)}$	0.3 secs 1 min 41.1 secs

Computational cost (I)

Role	Action	Timing / Size
System designer Dublin, Ireland	Generation of (k_p, k_s)	0.3 secs
	Encryption of $\Xi^{(\Phi)}$	1 min 41.1 secs
	Saving $\Xi^{(\Phi)}$ to disk	2 min 41.3 secs

Computational cost (I)

Role	Action	Timing / Size	
System designer Dublin, Ireland	Generation of (k_p, k_s)		0.3 secs
	Encryption of $\Xi^{(\Phi)}$	1 min	41.1 secs
	Saving $\Xi^{(\Phi)}$ to disk	2 min	41.3 secs
	Compressing $\Xi^{(\Phi)}$ on disk		48.0 secs
	Size of $\Xi^{(\Phi)}$ on disk	5.5GB	

Computational cost (I)

Role	Action	Timing / Size	
System designer Dublin, Ireland	Generation of (k_p, k_s)		0.3 secs
	Encryption of $\Xi^{(\Phi)}$	1 min	41.1 secs
	Saving $\Xi^{(\Phi)}$ to disk	2 min	41.3 secs
	Compressing $\Xi^{(\Phi)}$ on disk		48.0 secs
	Size of $\Xi^{(\Phi)}$ on disk	5.5GB	
Transfer $\Xi^{(\Phi)}$ to Manufacturer C		11 min	37.5 secs
Manufacturer C Northern California, USA			

Computational cost (I)

Role	**Action**	**Timing / Size**	
System designer Dublin, Ireland	Generation of (k_p, k_s)		0.3 secs
	Encryption of $\Xi^{(\Phi)}$	1 min	41.1 secs
	Saving $\Xi^{(\Phi)}$ to disk	2 min	41.3 secs
	Compressing $\Xi^{(\Phi)}$ on disk		48.0 secs
	Size of $\Xi^{(\Phi)}$ on disk	5.5GB	
Transfer $\Xi^{(\Phi)}$ to Manufacturer C		11 min	37.5 secs
Manufacturer C Northern California, USA	Decompress & load $\Xi^{(\Phi)}$ from disk	10 min	22.4 secs

Computational cost (I)

Role	Action	Timing / Size	
System designer Dublin, Ireland	Generation of (k_p, k_s)		0.3 secs
	Encryption of $\Xi^{(\Phi)}$	1 min	41.1 secs
	Saving $\Xi^{(\Phi)}$ to disk	2 min	41.3 secs
	Compressing $\Xi^{(\Phi)}$ on disk		48.0 secs
	Size of $\Xi^{(\Phi)}$ on disk	5.5GB	
Transfer $\Xi^{(\Phi)}$ to Manufacturer C		11 min	37.5 secs
Manufacturer C Northern California, USA	Decompress & load $\Xi^{(\Phi)}$ from disk	10 min	22.4 secs
	Update $\Xi^{(\Phi)}$	6 min	18.3 secs

Computational cost (I)

Role	**Action**	**Timing / Size**	
System designer Dublin, Ireland	Generation of (k_p, k_s)		0.3 secs
	Encryption of $\Xi^{(\Phi)}$	1 min	41.1 secs
	Saving $\Xi^{(\Phi)}$ to disk	2 min	41.3 secs
	Compressing $\Xi^{(\Phi)}$ on disk		48.0 secs
	Size of $\Xi^{(\Phi)}$ on disk	5.5GB	
Transfer $\Xi^{(\Phi)}$ to Manufacturer C		11 min	37.5 secs
Manufacturer C Northern California, USA	Decompress & load $\Xi^{(\Phi)}$ from disk	10 min	22.4 secs
	Update $\Xi^{(\Phi)}$	6 min	18.3 secs
	Saving & compressing $\Xi^{(\Phi)}$ to disk	2 min	9.8 secs

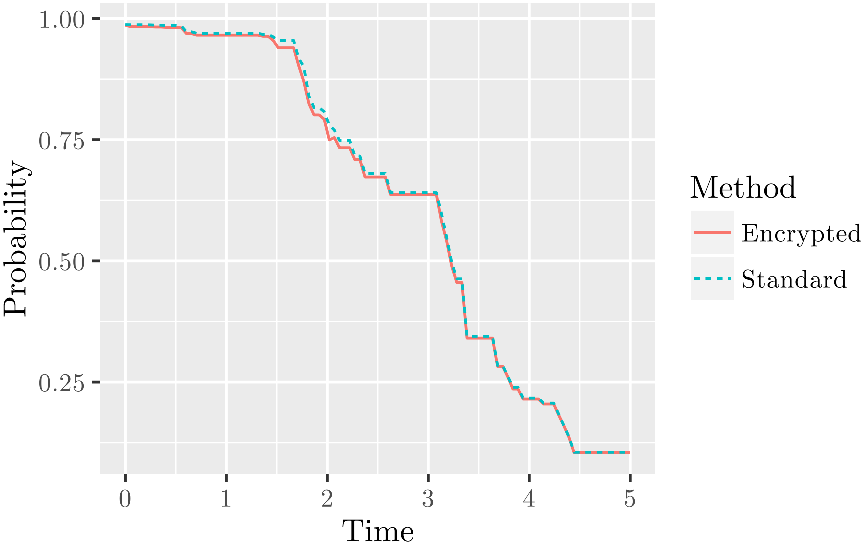
Computational cost (I)

Role	Action	Timing / Size	
System designer Dublin, Ireland	Generation of (k_p, k_s)		0.3 secs
	Encryption of $\Xi^{(\Phi)}$	1 min	41.1 secs
	Saving $\Xi^{(\Phi)}$ to disk	2 min	41.3 secs
	Compressing $\Xi^{(\Phi)}$ on disk		48.0 secs
	Size of $\Xi^{(\Phi)}$ on disk	5.5GB	
Transfer $\Xi^{(\Phi)}$ to Manufacturer C		11 min	37.5 secs
Manufacturer C Northern California, USA	Decompress & load $\Xi^{(\Phi)}$ from disk	10 min	22.4 secs
	Update $\Xi^{(\Phi)}$	6 min	18.3 secs
	Saving & compressing $\Xi^{(\Phi)}$ to disk	2 min	9.8 secs
Transfer $\Xi^{(\Phi)}$ to Manufacturer H		11 min	24.4 secs
Manufacturer H São Paulo, Brazil	Decompress & load $\Xi^{(\Phi)}$ from disk	10 min	13.2 secs
	Update $\Xi^{(\Phi)}$	7 min	23.1 secs
	Saving & compressing $\Xi^{(\Phi)}$ to disk	4 min	45.2 secs
Transfer $\Xi^{(\Phi)}$ to Manufacturer M		20 min	16.5 secs
Manufacturer M Sydney, Australia	Decompress & load $\Xi^{(\Phi)}$ from disk	9 min	41.0 secs
	Update $\Xi^{(\Phi)}$	11 min	28.2 secs
	Saving & compressing $\Xi^{(\Phi)}$ to disk	2 min	54.2 secs

Computational cost (II)

Role	**Action**	**Timing / Size**		
	Transfer $\Xi^{(\Phi)}$ to Manufacturer P		6 min	40.7 secs
Manufacturer P Tokyo, Japan	Decompress & load $\Xi^{(\Phi)}$ from disk		9 min	57.1 secs
	Update $\Xi^{(\Phi)}$		7 min	13.5 secs
	Compute ξ			6.1 secs
	Saving & compressing ξ to disk			2.5 secs
	Size of ξ on disk	58.4MB		
	Transfer ξ to System Designer			39.5 secs
System designer Dublin, Ireland	Decompress & load ξ from disk			5.9 secs
	Decryption of ξ			8.6 secs
Total:		2 hr	18 min	38.4 secs

Result


1.00
0.75
0.50
0.25
Probability
0
1
2
3
4
5
Time
Method
Encrypted
Standard

References

Aslett, L. J. M., Coolen, F. P. A., & Wilson, S. P. (2015). Bayesian inference for reliability of systems and networks using the survival signature. *Risk Analysis*, 35/9: 1640–51. DOI: 10.1111/risa.12228

Aslett, L. J. M., Esperança, P. M., & Holmes, C. C. (2015). *A review of homomorphic encryption and software tools for encrypted statistical machine learning*. University of Oxford. Retrieved from <http://arxiv.org/abs/1508.06574>

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.

Gentry, C. (2009). *A fully homomorphic encryption scheme* (PhD thesis). Stanford University. Retrieved from <crypto.stanford.edu/craig>

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

Samaniego, F. J. (1985). On closure of the IFR class under formation of coherent systems. *IEEE Transactions on Reliability*, 34/1: 69–72. DOI: 10.1109/TR.1985.5221935