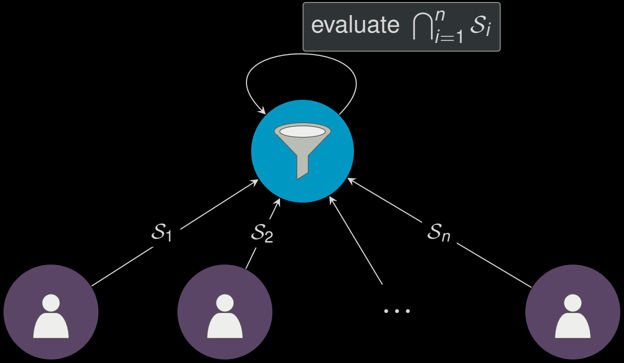
UNIVERSITY OF TWENTE.

Two-Client and Multi-client Functional Encryption for Set Intersection and Variants

Tim van de Kamp   David Stritzl   Willem Jonker   Andreas Peter

ACISP 2019

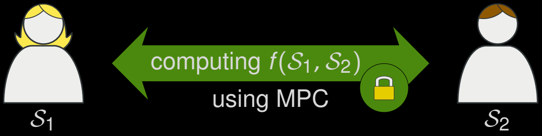
Functional Encryption for Set Operations



- Privacy-preserving information sharing
- Two-client and multi-client constructions for various set operations
- Evaluation using a proof-of-concept implementation

Privacy-Preserving Information Sharing

Private Set Intersection

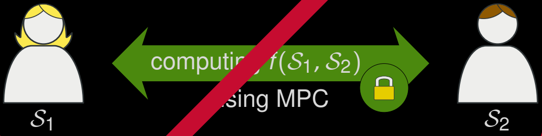


Computes a set operation using an interactive protocol

A participant learns the evaluation result

Privacy-Preserving Information Sharing

Private Set Intersection



Compu s a set op ation using an interactive protocol

A particip nt lea s the evaluation result

Privacy-Preserving Information Sharing

Functional Encryption for Set Operations

Computes a set operation using a non-interactive scheme

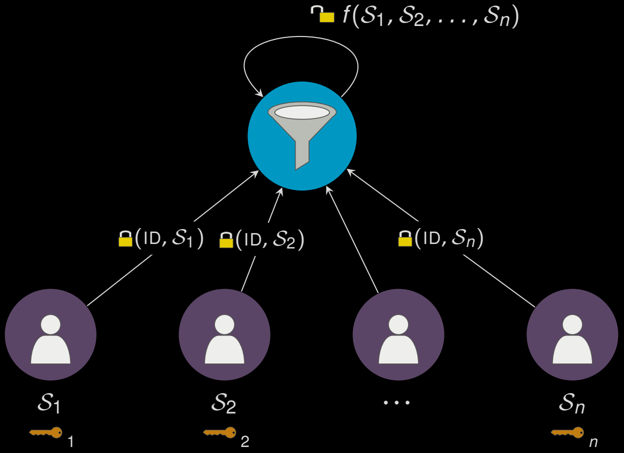
A third-party (the evaluator) learns the evaluation result

Use cases include

- privacy-preserving profiling
- simple data mining
- one-way data sharing

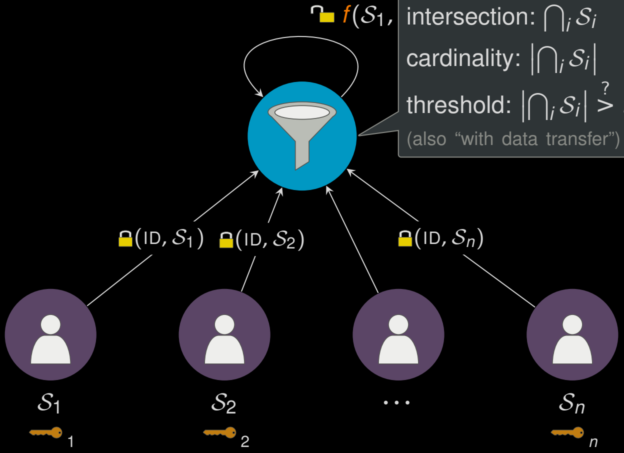
Multi-client Non-interactive Set Intersection

Functionality



Multi-client Non-interactive Set Intersection

Functionality



FUNCTIONALITIES f

intersection: $\bigcap_i \mathcal{S}_i$

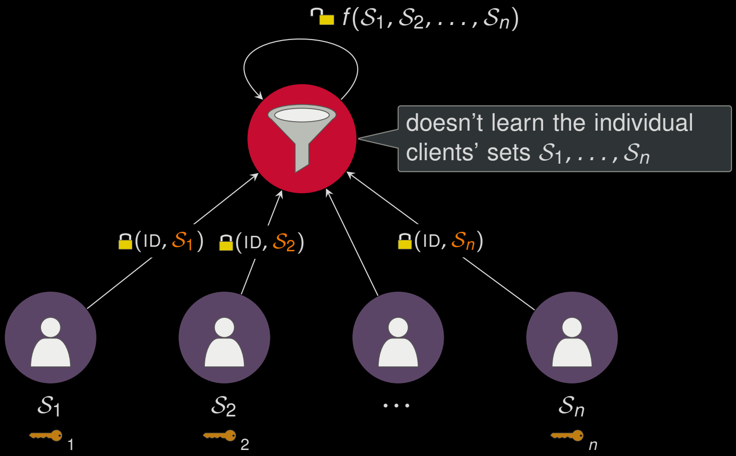
cardinality: $\left|\bigcap_i \mathcal{S}_i\right|$

threshold: $\left|\bigcap_i \mathcal{S}_i\right| \overset{?}{>} t \Rightarrow \bigcap_i \mathcal{S}_i$

(also “with data transfer”)

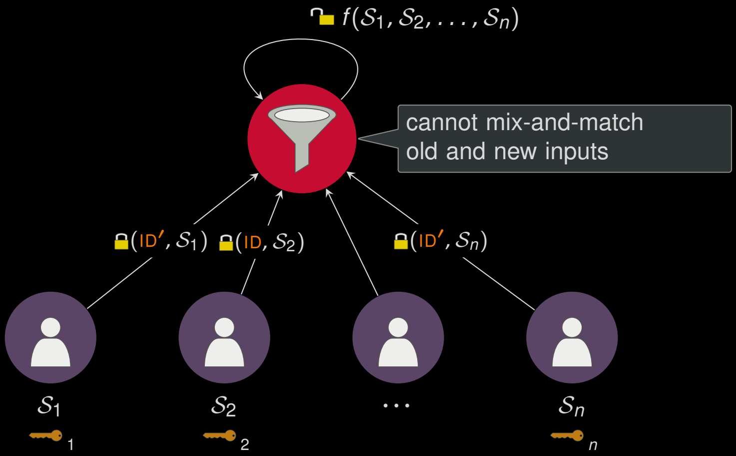
Multi-client Non-interactive Set Intersection

Security Requirements



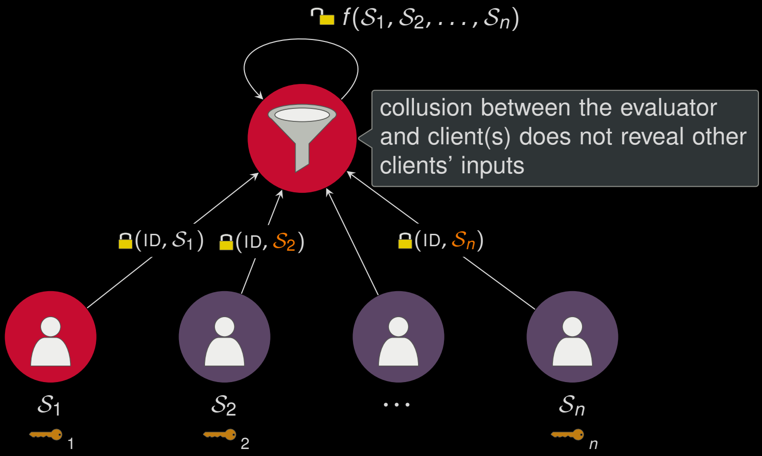
Multi-client Non-interactive Set Intersection

Security Requirements



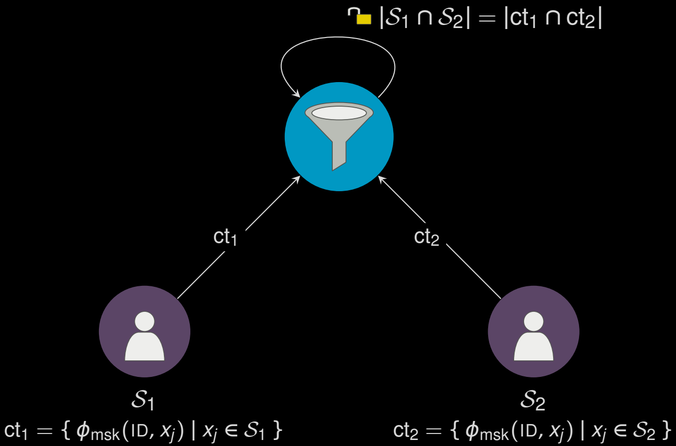
Multi-client Non-interactive Set Intersection

Security Requirements



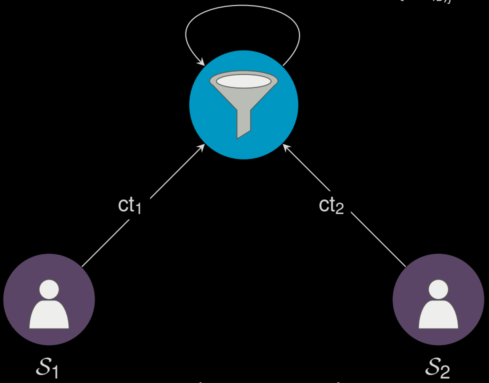
Construction: Two-Client Set Intersection Cardinality

Construction: Two-Client Set Intersection Cardinality



Construction: Two-Client Set Intersection

$\mathcal{S}_1 \cap \mathcal{S}_2 = \left\{ \phi^{-1}_{k_{\mathrm{ID},j}}(c) \mid c \in \mathrm{ct}_1 \cap \mathrm{ct}_2 \right\}$



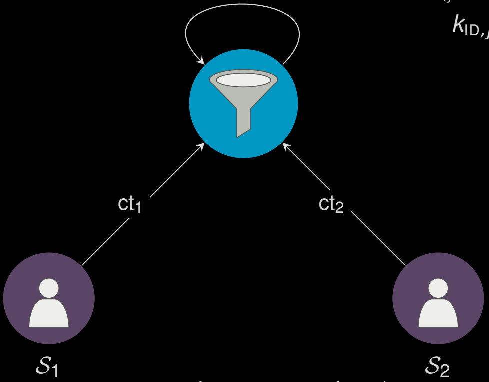
$\mathrm{ct}_1 = \left\{ \left(\phi_{k_{\mathrm{ID},j}}(x_j) \right) \mid x_j \in \mathcal{S}_1 \right\}$ $\mathrm{ct}_2 = \left\{ \left(\phi_{k_{\mathrm{ID},j}}(x_j) \right) \mid x_j \in \mathcal{S}_2 \right\}$

$$k_{\mathrm{ID},j} = \phi_{\mathrm{msk}}(\mathrm{ID}, x_j)$$

Construction: Two-Client Set Intersection

$$\mathcal{S}_1 \cap \mathcal{S}_2 = \left\{ \phi^{-1}_{k_{\mathrm{ID},j}}(c) \mid c \in \mathrm{ct}_1 \cap \mathrm{ct}_2 \right\}$$

$$k_{\mathrm{ID},j} = k_{\mathrm{ID},j}^{\mathrm{usk}_1} \cdot k_{\mathrm{ID},j}^{\mathrm{usk}_2}$$



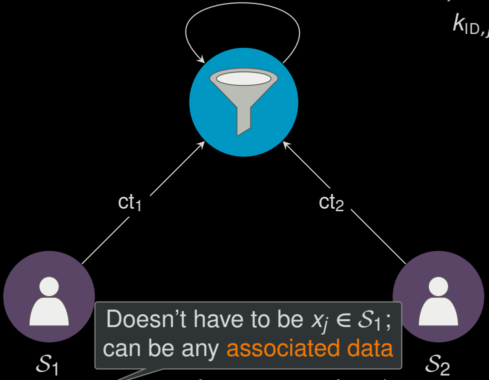
$$\mathrm{ct}_1 = \left\{ \left(k_{\mathrm{ID},j}^{\mathrm{usk}_1}, \phi_{k_{\mathrm{ID},j}}(x_j) \right) \mid x_j \in \mathcal{S}_1 \right\} \qquad \mathrm{ct}_2 = \left\{ \left(k_{\mathrm{ID},j}^{\mathrm{usk}_2}, \phi_{k_{\mathrm{ID},j}}(x_j) \right) \mid x_j \in \mathcal{S}_2 \right\}$$

$$\mathrm{usk}_1 + \mathrm{usk}_2 = 1$$
$$k_{\mathrm{ID},j} = \phi_{\mathrm{msk}}(\mathrm{ID}, x_j)$$

Construction: Two-Client Set Intersection

$\mathcal{S}_1 \cap \mathcal{S}_2 = \left\{ \phi^{-1}_{k_{\mathsf{ID},j}}(c) \mid c \in \mathsf{ct}_1 \cap \mathsf{ct}_2 \right\}$

$k_{\mathsf{ID},j} = k_{\mathsf{ID},j}^{\mathsf{usk}_1} \cdot k_{\mathsf{ID},j}^{\mathsf{usk}_2}$



Doesn't have to be $x_j \in \mathcal{S}_1$;
can be any associated data

$\mathsf{ct}_1 = \left\{ \left(k_{\mathsf{ID},j}^{\mathsf{usk}_1}, \phi_{k_{\mathsf{ID},j}}(x_j) \right) \mid x_j \in \mathcal{S}_1 \right\}$

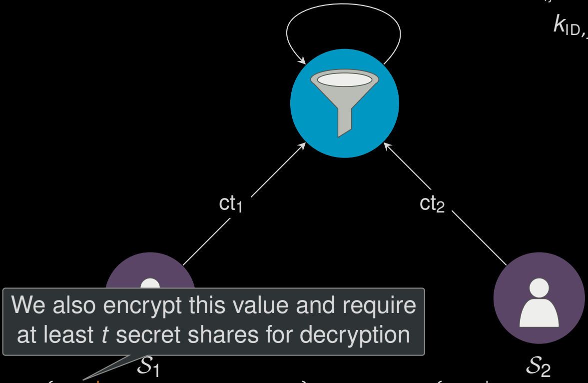
$\mathsf{ct}_2 = \left\{ \left(k_{\mathsf{ID},j}^{\mathsf{usk}_2}, \phi_{k_{\mathsf{ID},j}}(x_j) \right) \mid x_j \in \mathcal{S}_2 \right\}$

$$\mathsf{usk}_1 + \mathsf{usk}_2 = 1$$
$$k_{\mathsf{ID},j} = \phi_{\mathsf{msk}}(\mathsf{ID}, x_j)$$

Intuition: Two-Client **Threshold** Set Intersection

$$\mathcal{S}_1 \cap \mathcal{S}_2 = \left\{ \phi^{-1}_{k_{\mathrm{ID},j}}(c) \mid c \in \mathrm{ct}_1 \cap \mathrm{ct}_2 \right\}$$

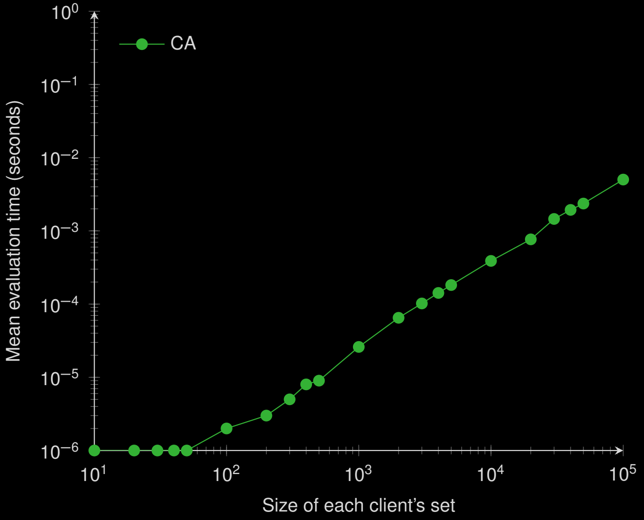
$$k_{\mathrm{ID},j} = k_{\mathrm{ID},j}^{\mathrm{usk}_1} \cdot k_{\mathrm{ID},j}^{\mathrm{usk}_2}$$



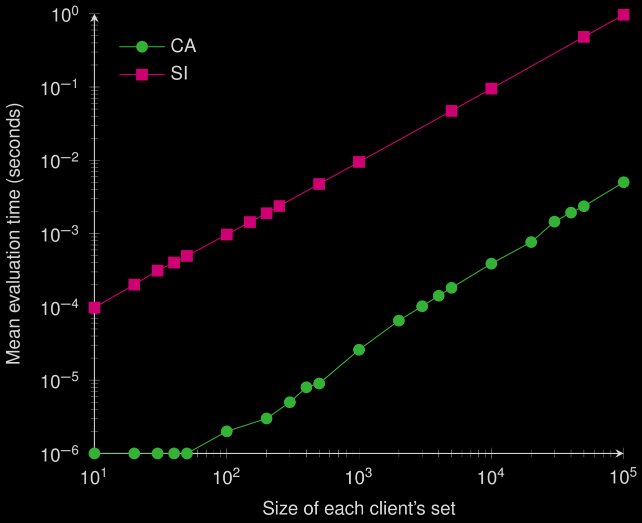
$$\mathrm{ct}_1 = \left\{ \left(k_{\mathrm{ID},j}^{\mathrm{usk}_1}, \phi_{k_{\mathrm{ID},j}}(x_j) \right) \mid x_j \in \mathcal{S}_1 \right\} \qquad \mathrm{ct}_2 = \left\{ \left(k_{\mathrm{ID},j}^{\mathrm{usk}_2}, \phi_{k_{\mathrm{ID},j}}(x_j) \right) \mid x_j \in \mathcal{S}_2 \right\}$$

$$\mathrm{usk}_1 + \mathrm{usk}_2 = 1$$
$$k_{\mathrm{ID},j} = \phi_{\mathrm{msk}}(\mathrm{ID}, x_j)$$

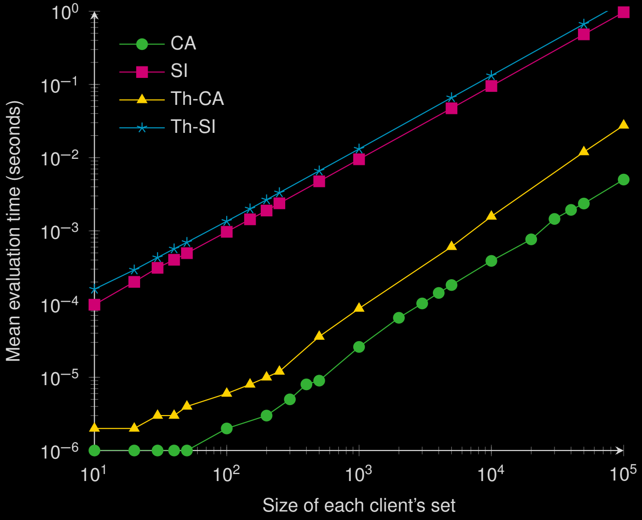
Efficiency of the 2C-FE Constructions



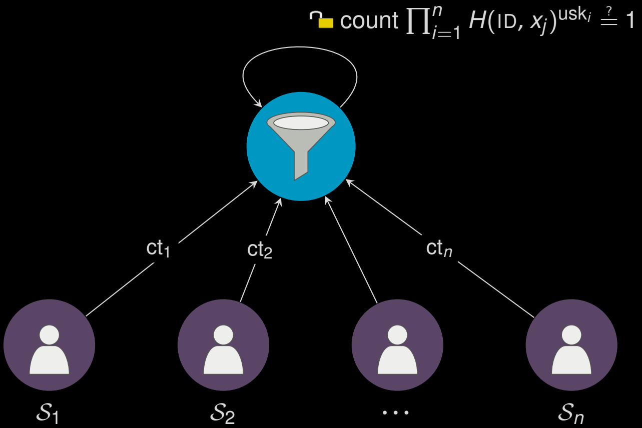
Efficiency of the 2C-FE Constructions



Efficiency of the 2C-FE Constructions



Construction: Multi-client Set Intersection Cardinality



$$\text{ct}_i = \{ H(\text{ID}, x_j)^{\text{usk}_i} \mid x_j \in \mathcal{S}_i \}$$

$$\sum_{i=1}^{n} \text{usk}_i = 0$$

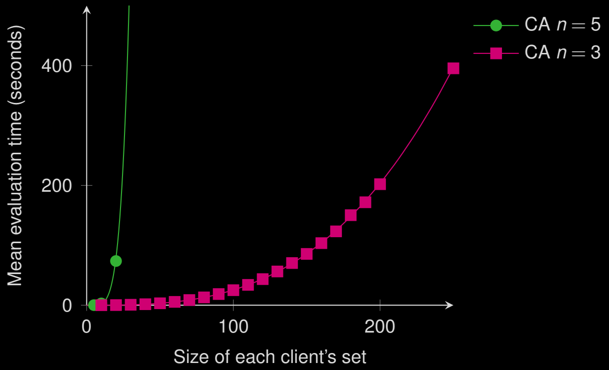
Efficiency of the MC-FE Construction

Theoretical

Polynomial in the number of set elements per client:

$$\mathcal{O}(\prod_i |\mathcal{S}_i|)$$

Practice



Improved Set Intersection Cardinality Scheme

Intuition

1. Compute the set intersection $\bigcap_i \mathcal{S}_i$ "in the encrypted domain";
2. For some client i', determine how many set elements $e_j \in \mathcal{S}_{i'}$ are in the encrypted set intersection, i.e.,

$$\left| \left\{ e_j \mid e_j \in \bigcap_{i=1}^{n} \mathcal{S}_i, e_j \in \mathcal{S}_{i'} \right\} \right| .$$

Improved Set Intersection Cardinality Scheme

Intuition

1. Compute the set intersection $\bigcap_i \mathcal{S}_i$ "in the encrypted domain";
2. For some client i', determine how many set elements $e_j \in \mathcal{S}_{i'}$ are in the encrypted set intersection, i.e.,

$$\left| \left\{ e_j \mid e_j \in \bigcap_{i=1}^{n} \mathcal{S}_i, e_j \in \mathcal{S}_{i'} \right\} \right| .$$

"Tools"

- Bloom filters → to represent sets in a single data structure
- Homomorphic encryption → to compute in the encrypted domain
- Functional encryption → to determine whether an element is in a set

Preliminaries: Bloom filters

Set Intersection

	bs[1]	bs[2]	bs[3]	bs[4]	bs[5]	bs[6]	bs[7]	bs[8]	bs[9]
$\mathcal{S}_1$	0	1	0	1	1	1	0	0	0
$\cap$					$\wedge$				
$\mathcal{S}_2$	0	0	0	1	0	1	0	0	1
					$=$				
$\mathcal{S}_1 \cap \mathcal{S}_2$	0	0	0	1	0	1	0	0	0

Construction (simplified)

Set Intersection using Secret Sharing

	bs[1]	bs[2]	bs[3]	bs[4]	bs[5]	bs[6]	bs[7]	bs[8]	bs[9]
Enc($\mathcal{S}_1$)	$r_{1,1}$	$s_{1,2}$	$r_{1,3}$	$s_{1,4}$	$s_{1,5}$	$s_{1,6}$	$r_{1,7}$	$r_{1,8}$	$r_{1,9}$
					+				
Enc($\mathcal{S}_2$)	$r_{2,1}$	$r_{2,2}$	$r_{2,3}$	$s_{2,4}$	$r_{2,5}$	$s_{2,6}$	$r_{2,7}$	$r_{2,8}$	$s_{2,9}$
					=				
Enc($\mathcal{S}_1 \cap \mathcal{S}_2$)	$\tilde{r}_1$	$\tilde{r}_2$	$\tilde{r}_3$	1	$\tilde{r}_5$	1	$\tilde{r}_7$	$\tilde{r}_8$	$\tilde{r}_9$

Construction (simplified)

Set Intersection using Secret Sharing

	bs[1]	bs[2]	bs[3]	bs[4]	bs[5]	bs[6]	bs[7]	bs[8]	bs[9]
$\mathrm{Enc}(\mathcal{S}_1)$	$r_{1,1}$	$s_{1,2}$	$r_{1,3}$	$s_{1,4}$	$s_{1,5}$	$s_{1,6}$	$r_{1,7}$	$r_{1,8}$	$r_{1,9}$
+									
$\mathrm{Enc}(\mathcal{S}_2)$	$r_{2,1}$	$r_{2,2}$	$r_{2,3}$	$s_{2,4}$	$r_{2,5}$	$s_{2,6}$	$r_{2,7}$	$r_{2,8}$	$s_{2,9}$
=									
$\mathrm{Enc}(\mathcal{S}_1 \cap \mathcal{S}_2)$	$\tilde{r}_1$	$\tilde{r}_2$	$\tilde{r}_3$	1	$\tilde{r}_5$	1	$\tilde{r}_7$	$\tilde{r}_8$	$\tilde{r}_9$

Encrypt$(\mathrm{usk}_i, \mathrm{ID}, \mathcal{S}_i)$

$H(\mathrm{ID}, \ell)^{r_{i,\ell}}$ if $\mathrm{bs}[\ell] = 0$;

$H(\mathrm{ID}, \ell)^{s_{i,\ell}}$ if $\mathrm{bs}[\ell] = 1$

Construction (simplified)

Set Intersection using Secret Sharing

	bs[1]	bs[2]	bs[3]	bs[4]	bs[5]	bs[6]	bs[7]	bs[8]	bs[9]
$\mathrm{Enc}(\mathcal{S}_1)$	$r_{1,1}$	$s_{1,2}$	$r_{1,3}$	$s_{1,4}$	$s_{1,5}$	$s_{1,6}$	$r_{1,7}$	$r_{1,8}$	$r_{1,9}$
					+				
$\mathrm{Enc}(\mathcal{S}_2)$	$r_{2,1}$	$r_{2,2}$	$r_{2,3}$	$s_{2,4}$	$r_{2,5}$	$s_{2,6}$	$r_{2,7}$	$r_{2,8}$	$s_{2,9}$
					=				
$\mathrm{Enc}(\mathcal{S}_1 \cap \mathcal{S}_2)$	$\tilde{r}_1$	$\tilde{r}_2$	$\tilde{r}_3$	1	$\tilde{r}_5$	1	$\tilde{r}_7$	$\tilde{r}_8$	$\tilde{r}_9$

Encrypt$(\mathsf{usk}_i, \mathrm{ID}, \mathcal{S}_i)$

$H(\mathrm{ID}, \ell)^{r_{i,\ell}}$ if $\mathsf{bs}[\ell] = 0$;

$H(\mathrm{ID}, \ell)^{s_{i,\ell}}$ if $\mathsf{bs}[\ell] = 1$

Evaluate$(\mathsf{ct}_1, \ldots, \mathsf{ct}_n)$

$$H(\mathrm{ID}, \ell)^{s_{0,\ell}} \cdot \left(\prod_{i=1}^{n} H(\mathrm{ID}, \ell)^{s_{i,\ell}}\right)$$

Construction (simplified)

Set Intersection using Secret Sharing

	bs[1]	bs[2]	bs[3]	bs[4]	bs[5]	bs[6]	bs[7]	bs[8]	bs[9]
Enc								$r_{1,8}$	$r_{1,9}$
Enc								$_{2,8}$	$s_{2,9}$
Enc($\mathcal{S}_1 \cap \mathcal{S}_2$)	r_1	r_2	r_3	1	r_5	1	r_7	$\tilde{r}_8$	$\tilde{r}_9$

Actual construction is more involved:

- element testing uses $\left(H(\text{ID}, \ell)^{s_{0,\ell}} g^{t \cdot r}\right) \cdot \prod_{i=1}^{n} H(\text{ID}, \ell)^{s_{i,\ell}} \stackrel{?}{=} (g^r)^{t'}$
- using Shamir secret sharing instead of additive secret sharing

Encrypt(usk$_i$, ID, $\mathcal{S}_i$)

$H(\text{ID}, \ell)^{r_{i,\ell}}$ if $\text{bs}[\ell] = 0$;

$H(\text{ID}, \ell)^{s_{i,\ell}}$ if $\text{bs}[\ell] = 1$

Evaluate(ct$_1, \ldots,$ ct$_n$)

$$H(\text{ID}, \ell)^{s_{0,\ell}} \cdot \left(\prod_{i=1}^{n} H(\text{ID}, \ell)^{s_{i,\ell}}\right)$$

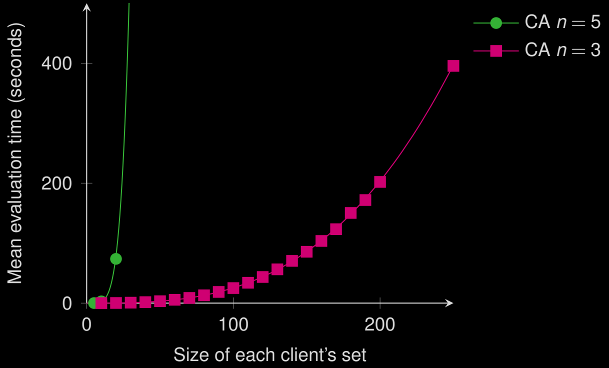
Efficiency of the MC-FE Construction

Theoretical

Polynomial in the number of set elements per client:

$$\mathcal{O}(x^2)$$

Practice



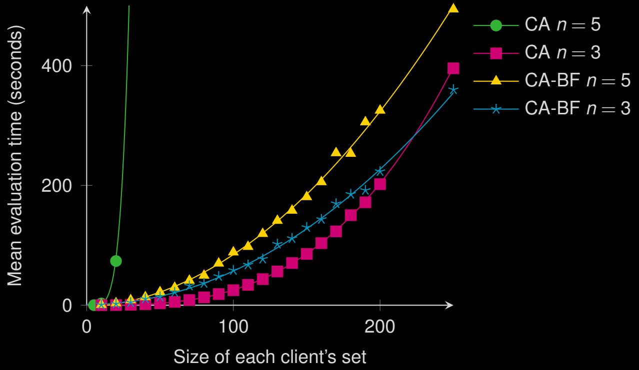
Efficiency of the MC-FE Construction

Theoretical

Polynomial in the number of set elements per client:

$$\mathcal{O}(x^2)$$

Practice



Summary

- Non-interactive privacy-preserving information sharing
- Efficient two-client constructions for various set operations
- Theoretical constructions for various multi-client set operations

Summary

- Non-interactive privacy-preserving information sharing
- Efficient two-client constructions for various set operations
- Theoretical constructions for various multi-client set operations

Interested?

Implementation: `https://github.com/CRIPTIM/nipsi`

Contact: `t.r.vandekamp@utwente.nl`

UNIVERSITY OF TWENTE.

NWO

TNO

National Cyber Security Centre
Ministry of Security and Justice

Ministry of the Interior and
Kingdom Relations