UNIVERSITY OF TWENTE.

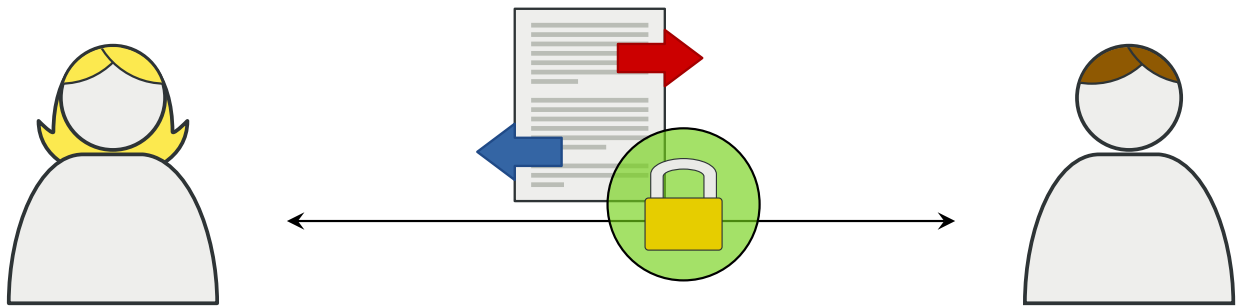
Private Sharing of IOCs and Sightings

(short paper)

Tim van de Kamp **Andreas Peter** **Maarten Everts** **Willem Jonker**

Workshop on Information Sharing and Collaborative Security, 2016

What This Talk Is About: Private Information Sharing

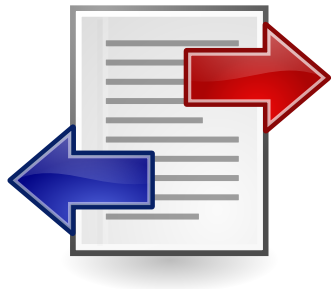


- Privacy-enhanced information sharing
- Simple & existing cryptographic techniques
- Proof-of-concept implementations

Information Sharing in Practice

Clear benefits

- Quicker detection
- Better protection
- Improved situational awareness



Challenge: Sensitive Data

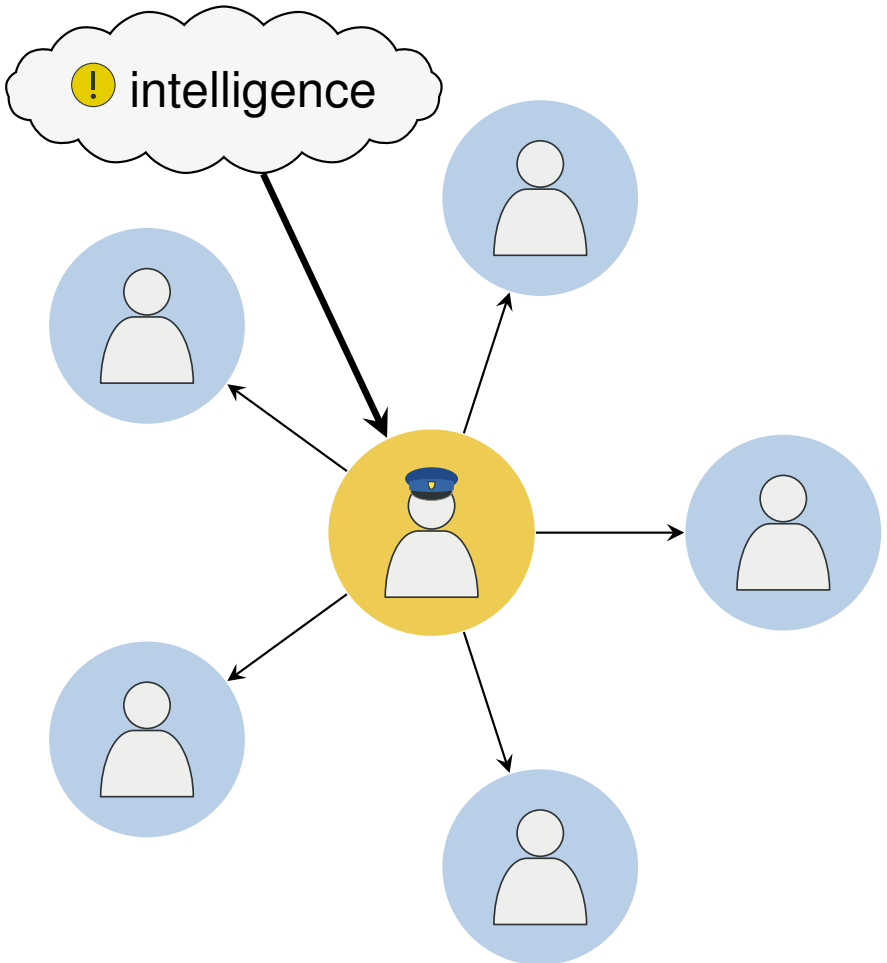
Information leakage due to

- information shared with a compromised party
- freedom of information laws

Leads to

- reputation damage
- notifying and informing attackers

Information Sharing via the Source–Subscriber Model



Source
CERT or
anti-virus company

Subscriber
critical infrastructure
or other company

Type of Security Information Shared by a Source

Source (e.g., CERT or anti-virus company)

Indicators of Compromise (IOCs)
Description of potentially malicious observables using features (IP address, hash of a malicious file, . . .).

Examples (Indicator of Compromise)

- `fileHash = bbd758d9b26404d9b28957af865d1234`
- `(destIP = 198.51.100.43) ∧ (destPort = 80 ∨ destPort = 443)`

Course of Action (COA)
Measures to be taken to address a specific threat.

Example (Course of Action)

If IOC #2043 is matched, kill process *x* and remove files *y* and *z*.

Type of Security Information Shared by a Subscriber

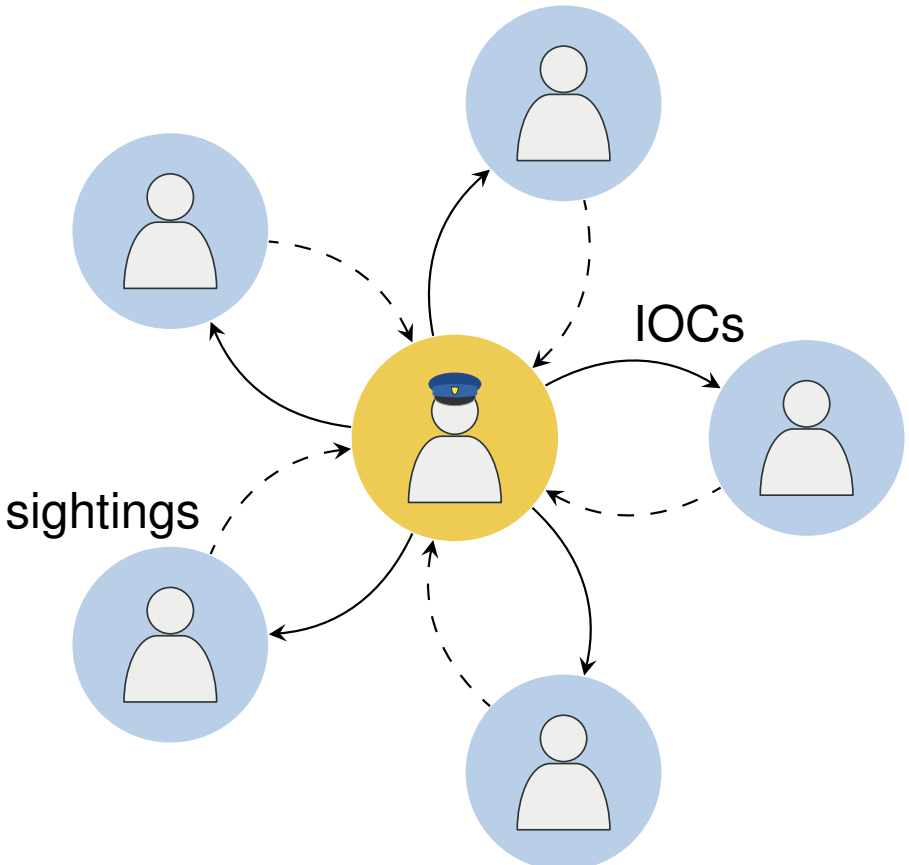
Subscribers (e.g., critical infrastructures or other companies)

Sightings
Report of a matched IOC: The observables match the pattern described in the IOC.

Example (Sighting)

In the previous hour, IOC #175 matched 2 times against our network traffic.

Information Sharing via the Source–Subscriber Model



Source
CERT or
anti-virus company

Subscriber
critical infrastructure
or other company

Indicator of Compromise

- IP address
- malicious software hash
- . . .

Sighting
Report of a matched IOC

Why Do We Need Private Information Sharing?

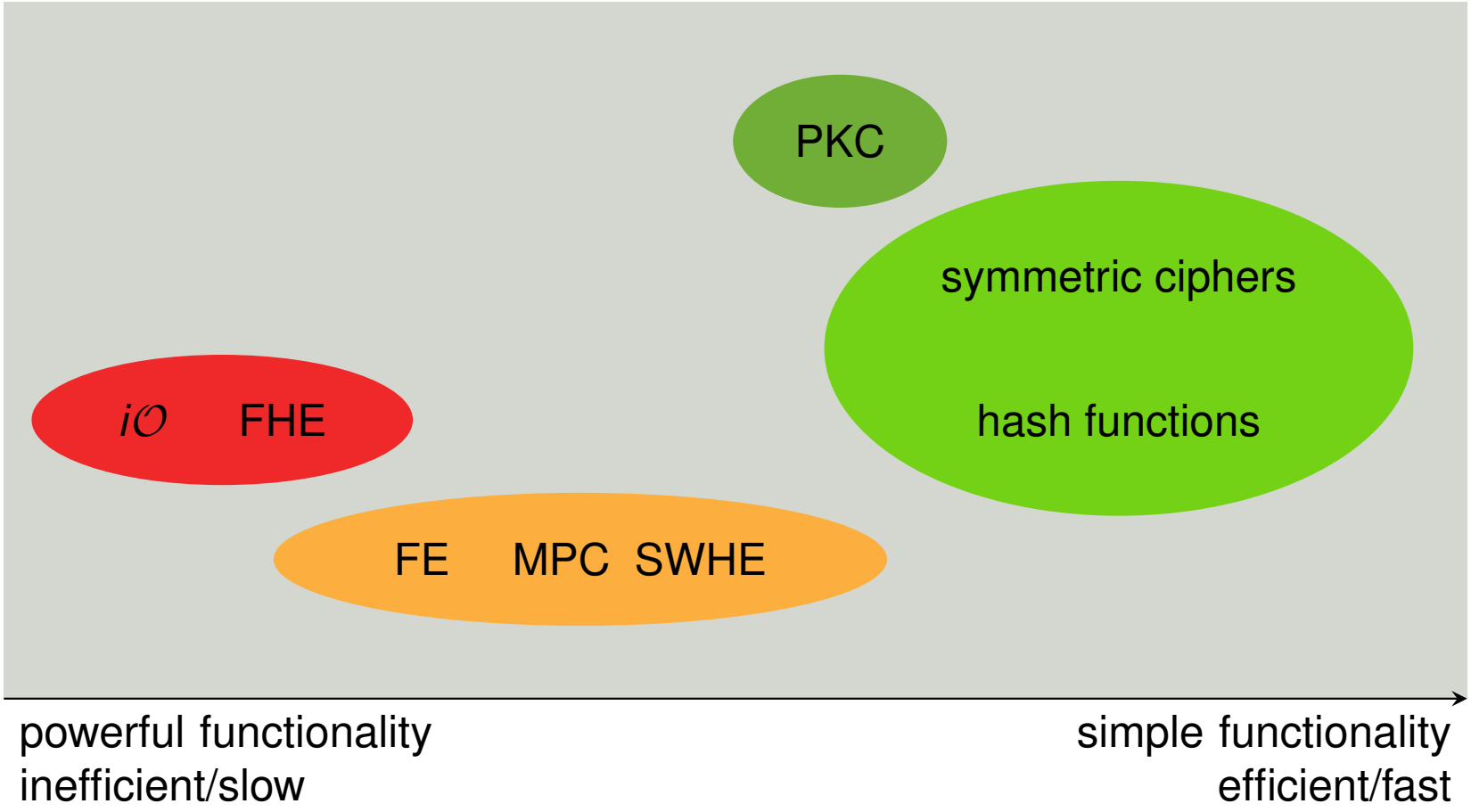
Source (e.g., CERT or anti-virus company)
shares IOCs and COAs

- Prevent attackers from learning the detection technique
- Protect the intellectual property of an anti-virus company

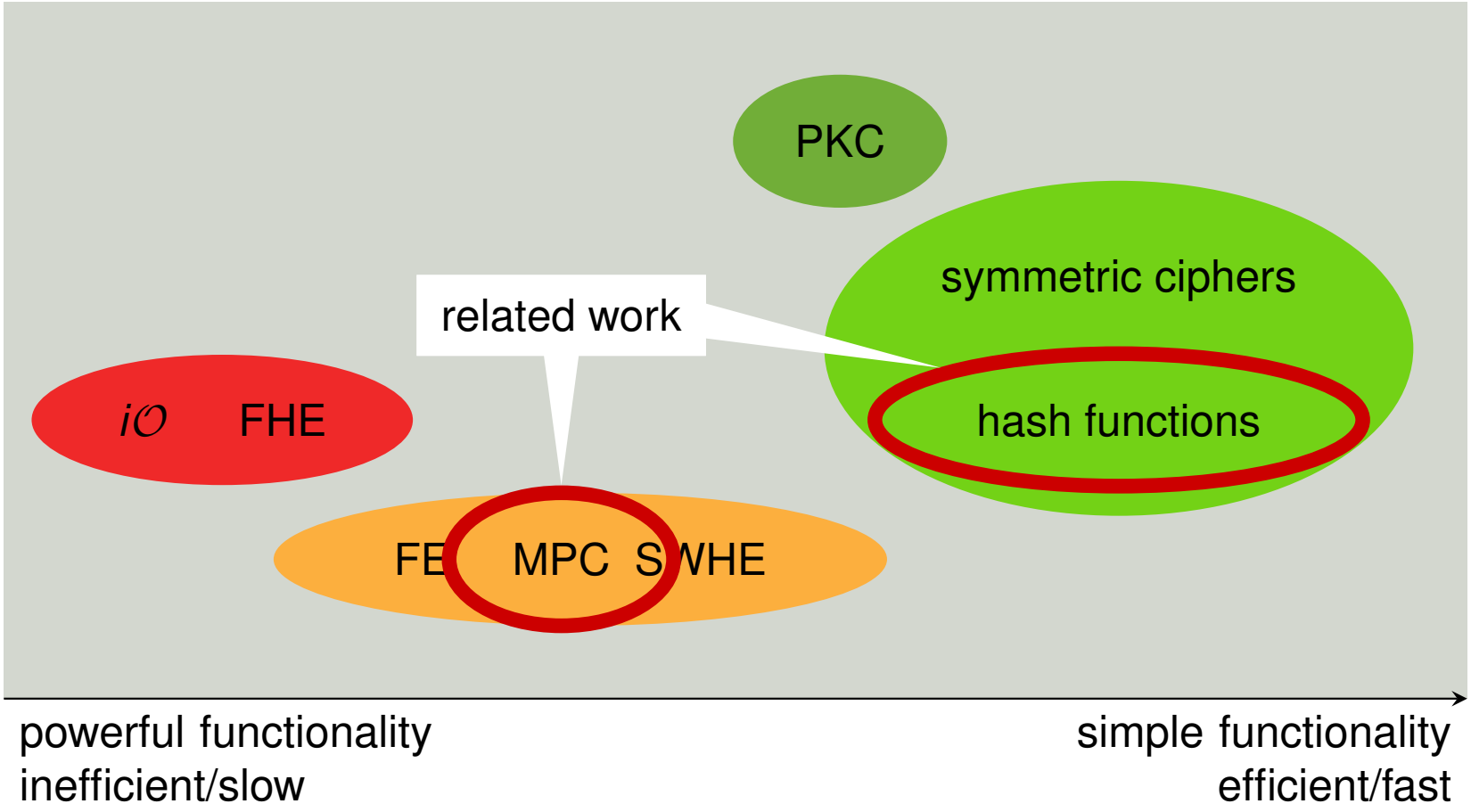
Subscribers (e.g., critical infrastructures or other companies)
share sightings

- Prevent attackers from learning they are detected
- Avoid reputation damage

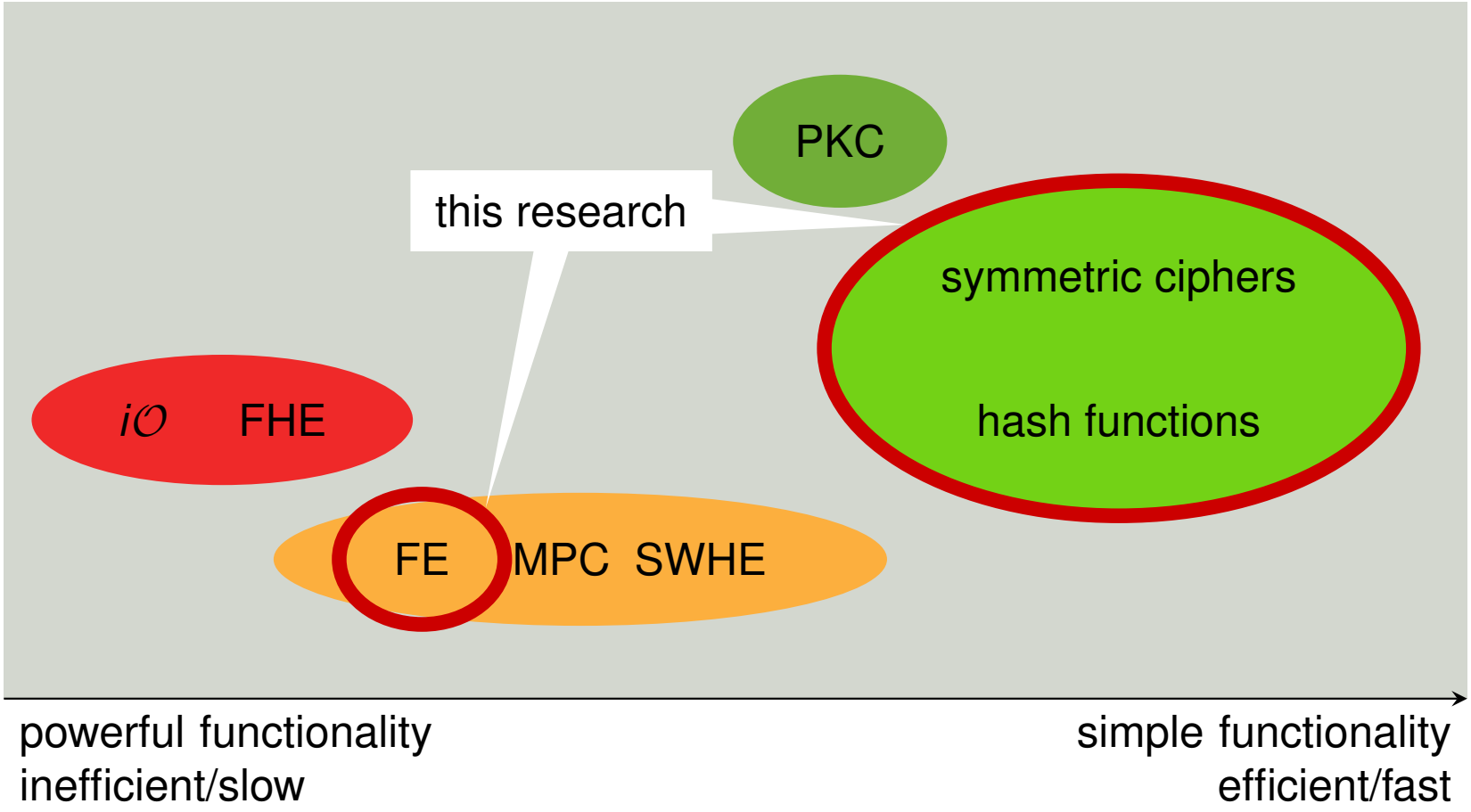
Private Information Sharing through Cryptography



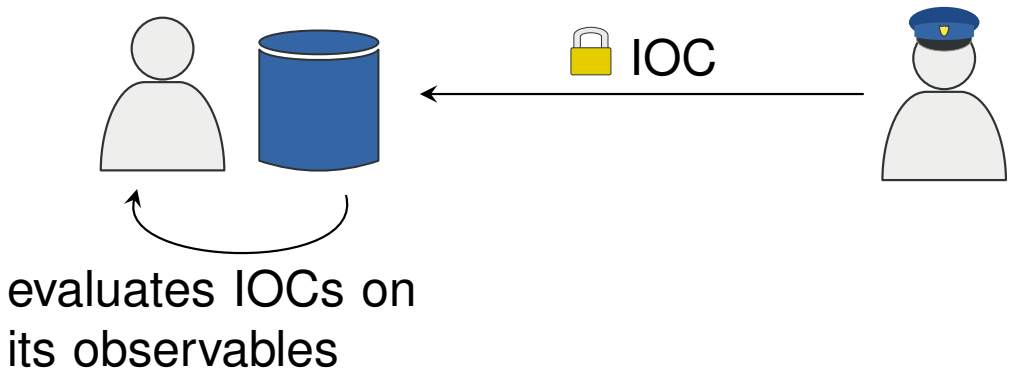
Private Information Sharing through Cryptography



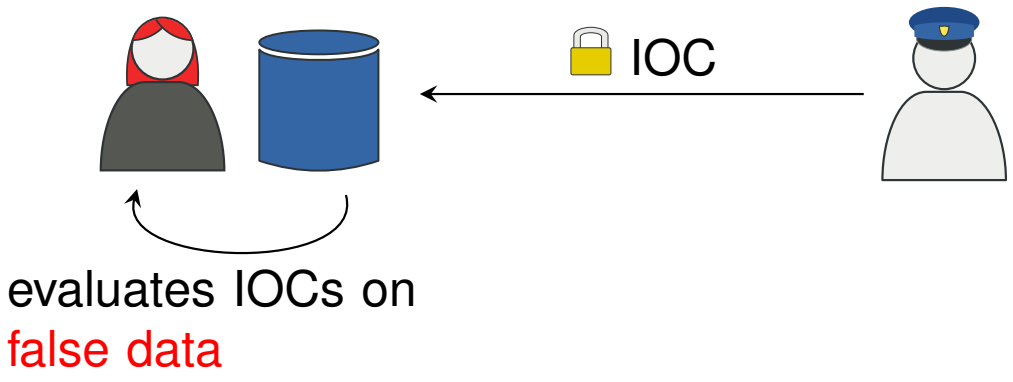
Private Information Sharing through Cryptography



Scenario for Private IOC Sharing



Scenario for Private IOC Sharing



Inherent to the Scenario

Subscriber can evaluate an IOC with false data.

Our Approach to Private IOC Sharing

1. Write the IOC in disjunctive normal form.

$$(\texttt{destIP} = 198.51.100.43 \land \texttt{destPort} = 80) \lor (\texttt{destIP} = 198.51.100.43 \land \texttt{destPort} = 443)$$

2. Split the IOC rule into subrules at every `OR` gate.

$$\text{IOC}_1\colon \texttt{destIP} = 198.51.100.43 \land \texttt{destPort} = 80$$
$$\text{IOC}_2\colon \texttt{destIP} = 198.51.100.43 \land \texttt{destPort} = 443$$

3. Concatenate the feature values, choose a salt and the number of iterations, and derive a symmetric encryption key

$$k = \text{KDF}(198.51.100.43 \,\|\, 80, \texttt{salt}, \texttt{iterations})$$

Example (Cryptographic IOC)

$(\text{AES}_k(\text{COA}), \text{“}\texttt{destIP,destPort}\text{”}, \texttt{salt}, \texttt{iterations})$

Our Approach to Private IOC Sharing

1. Write the IOC in disjunctive normal form.

$$(\texttt{destIP} = 198.51.100.43 \land \texttt{destPort} = 80) \lor (\texttt{destIP} = 198.51.100.43 \land \texttt{destPort} = 443)$$

2. Split the IOC rule into subrules at every `OR` gate.

IOC_1: $\texttt{destIP} = 198.51.100.43 \land \texttt{destPort} = 80$
IOC_2: $\texttt{destIP} = 198.51.100.$

prevents precomputation attacks

3. Concatenate the feature values, choose a salt and the number of iterations, and derive a symmetric encryption key

$$k = \text{KDF}(198.51.100.43 \,\|\, 80, \texttt{salt}, \texttt{iterations})$$

Example (Cryptographic IOC)

$(\text{AES}_k(\text{COA}), \text{“}\texttt{destIP,destPort}\text{”}, \texttt{salt}, \texttt{iterations})$

Our Approach to Private IOC Sharing

1. Write the IOC in disjunctive normal form.

```
(destIP = 198.51.100.43 ∧ destPort = 80) ∨
(destIP = 198.51.100.43 ∧ destPort = 443)
```

2. Split the IOC rule into subrules at every `OR` gate.

IOC_1: `destIP = 198.51.100.43 ∧ destPort = 80`
IOC_2: `3 ∧ destPort = 443`

influences evaluation time

3. Concatenate the feature values, choose a salt and the number of iterations, and derive a symmetric encryption key

$$k = \mathrm{KDF}(\texttt{198.51.100.43} \,\|\, \texttt{80}, \texttt{salt}, \texttt{iterations})$$

Example (Cryptographic IOC)

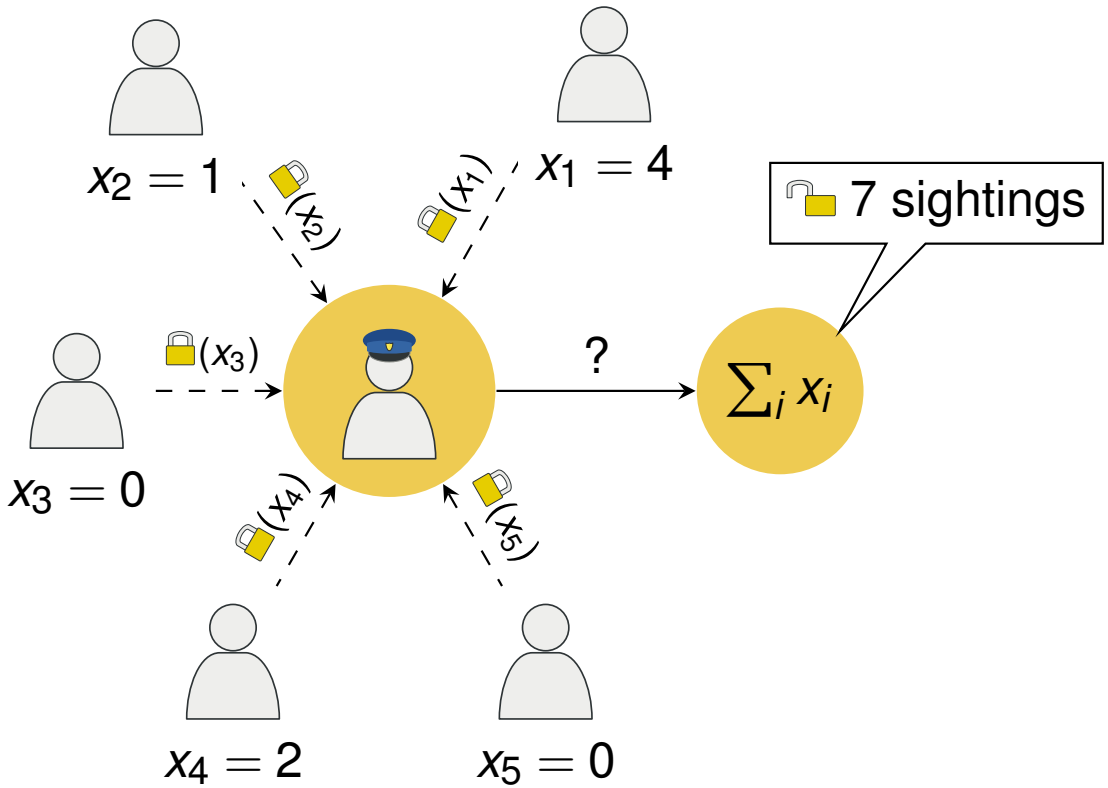
$(\mathrm{AES}_k(\mathrm{COA}), \text{“}\texttt{destIP,destPort}\text{”}, \texttt{salt}, \texttt{iterations})$

Private IOC Sharing: Proof-of-Concept Implementation

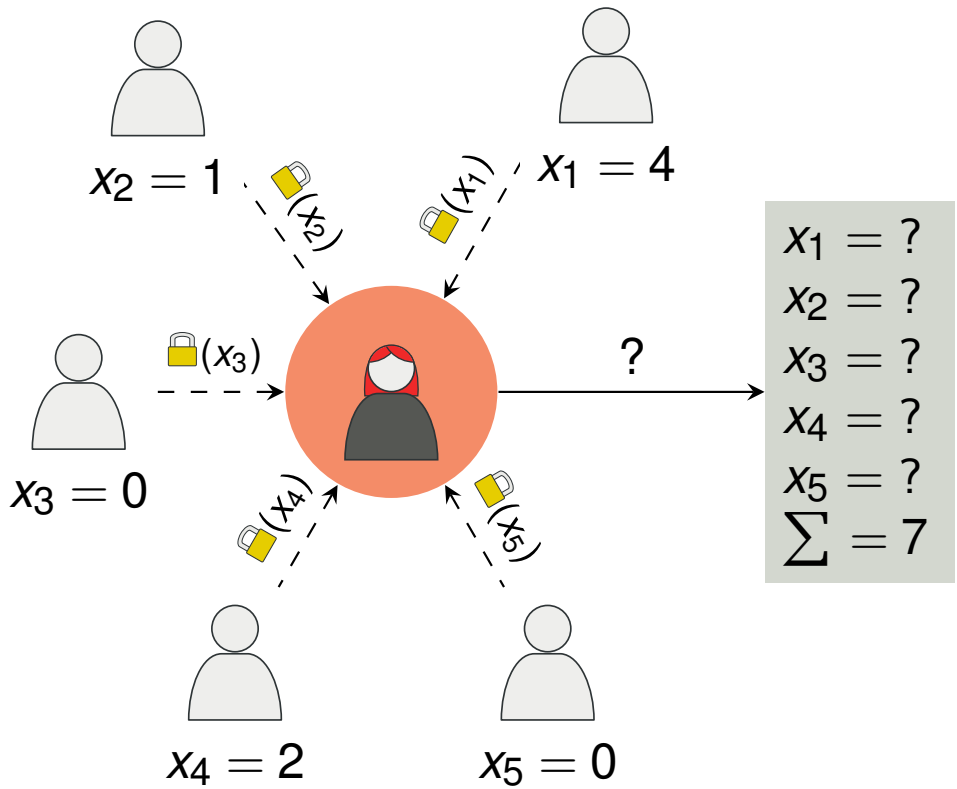
- Python wrapper for Bro [CRIPTIM]
- Key derivation functions: HKDF and PBKDF2 using SHA-256
- Encryption using AES

- Cryptographic overhead: depends on number of iterations
  - Minimal overhead per evaluation (e.g., per network flow): $\pm 40\,\mu s$ per IOC

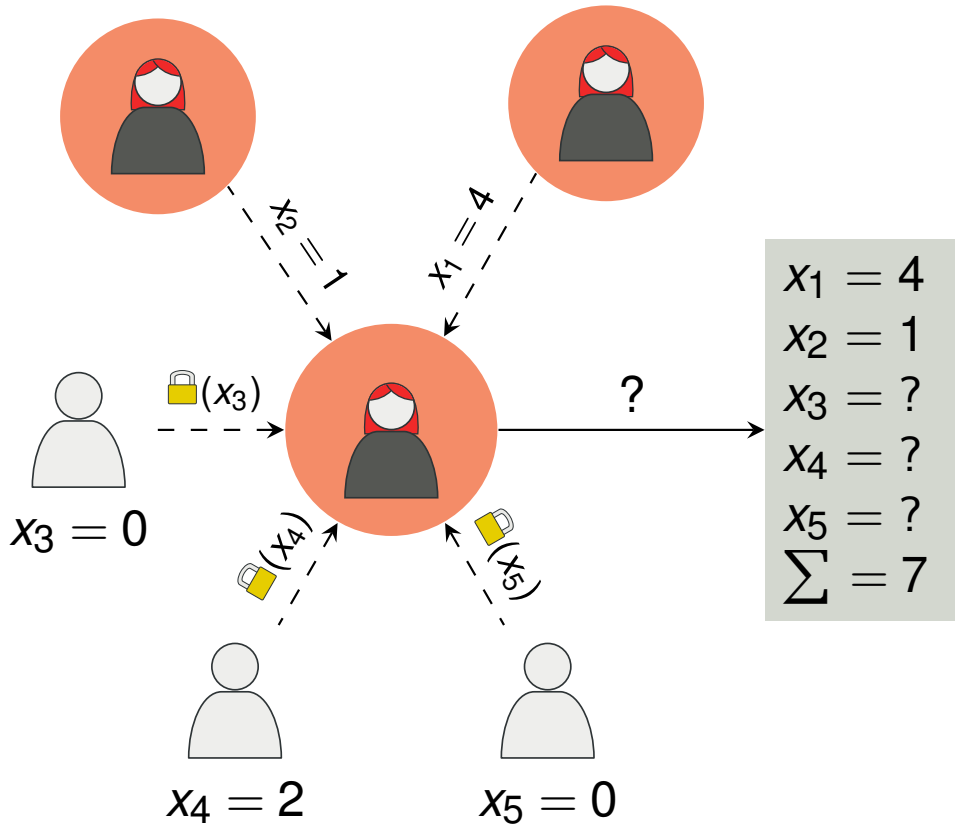
Scenario for Private Reporting of Sightings



Scenario for Private Reporting of Sightings



Scenario for Private Reporting of Sightings



Properties of Our Approach

- Source only learns the sum, *not the individual values* of the subscribers.
- All subscribers need to contribute to the computation, otherwise the source can learn the individual values

$$x_j = \sum_i x_i - \sum_{i \in [n] \setminus j} x_i$$

- Can be used for more specific counts

  e.g., number of matches being false positive

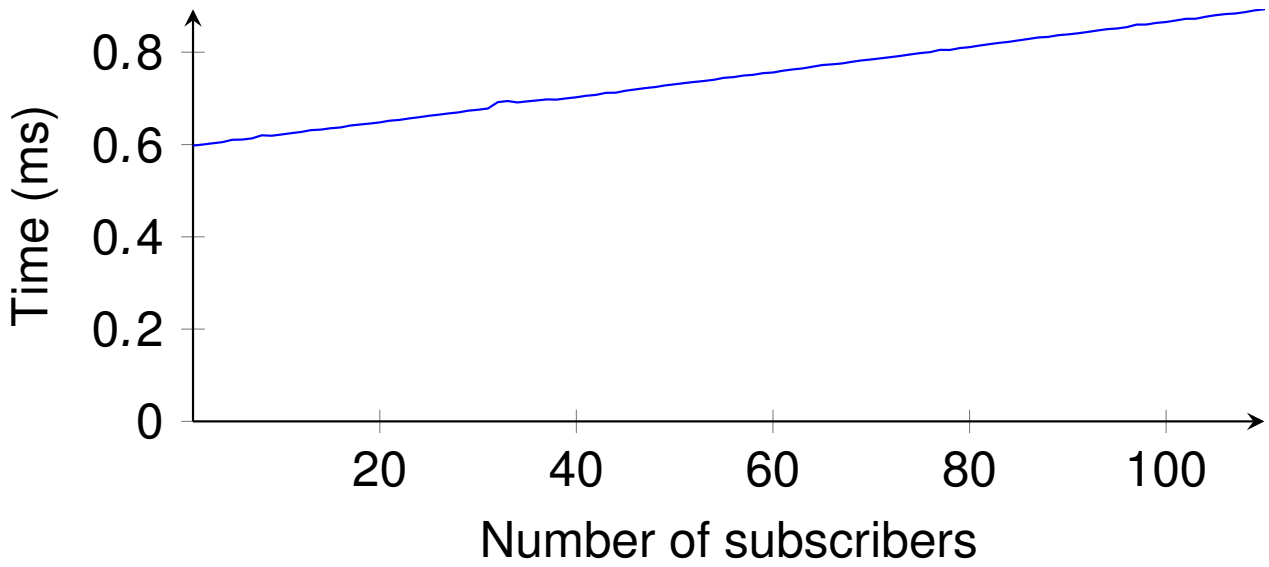
Proof-of-Concept Implementation of Private Reporting of Sightings

Privacy-preserving aggregation scheme [Shi et al. 2011]

- Python implementation [CRIPTIM]
- P-256 elliptic curve (≈ 128 bit security)

Results

- Encryption time (for a single subscriber): 0.58 ms
- Aggregate ciphertexts and decrypt



Summary

- Efficient, existing cryptography for private information sharing
- Cryptographic constructions for practical use
  - IOCs: speed–privacy trade-off (minimal overhead: < 0.05 ms)
  - Sightings: encryption and decryption in < 1 ms

- Outlook
  - Evaluation using real sensitive data, in real systems
  - Other types of information sharing using cryptographic techniques

Questions?

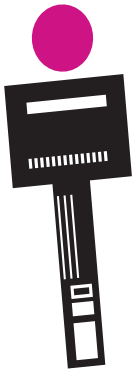
Contact: t.r.vandekamp@utwente.nl

NWO TNO National Cyber Security Centre *Ministry of Security and Justice* Ministry of the Interior and Kingdom Relations

References

[CRIPTIM] *Implementations of Private Information Sharing Schemes*. CRIPTIM consortium. URL: https://github.com/CRIPTIM/.

[Shi et al. 2011] E. Shi, T. H. Chan, E. G. Rieffel, R. Chow, and D. Song. "Privacy-Preserving Aggregation of Time-Series Data." In: *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. 2011.



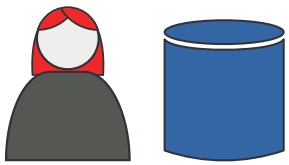
Appendix

1. Questions
   - Details about Using a Salt
   - Details about Substring Matching
   - Details about Traitor Tracing
   - Privacy-Preserving Aggregation [Shi et al. 2011]

Details about Using a Salt

Definition (Salt)

A salt is a large, public, random number.
Due to the randomness, it is unpredictable.

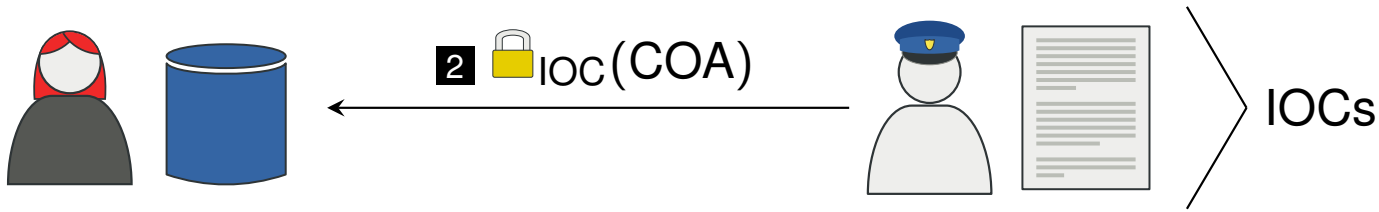


1 precomputes many potential IOCs

Details about Using a Salt

Definition (Salt)

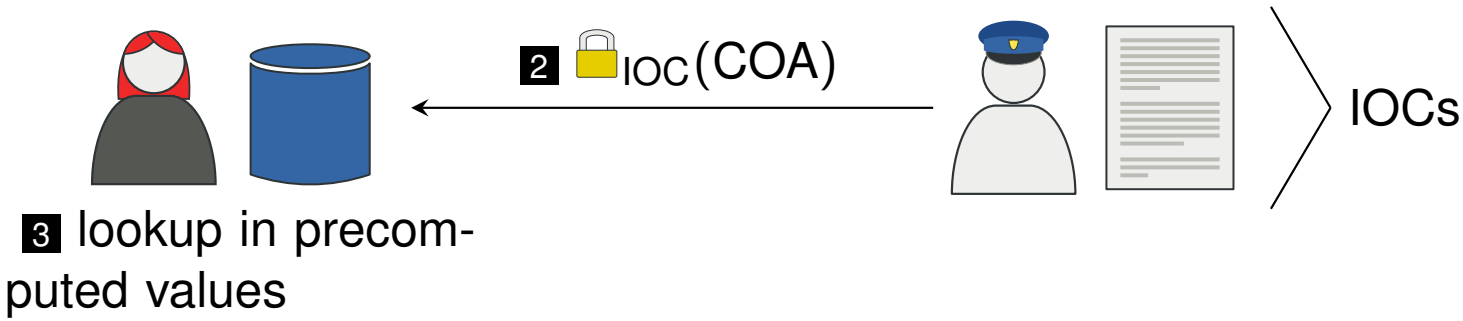
A salt is a large, public, random number.
Due to the randomness, it is unpredictable.



Details about Using a Salt

Definition (Salt)

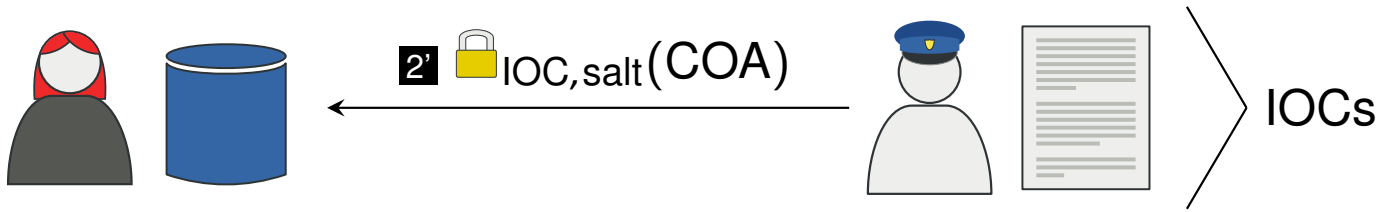
A salt is a large, public, random number.
Due to the randomness, it is unpredictable.



Details about Using a Salt

Definition (Salt)

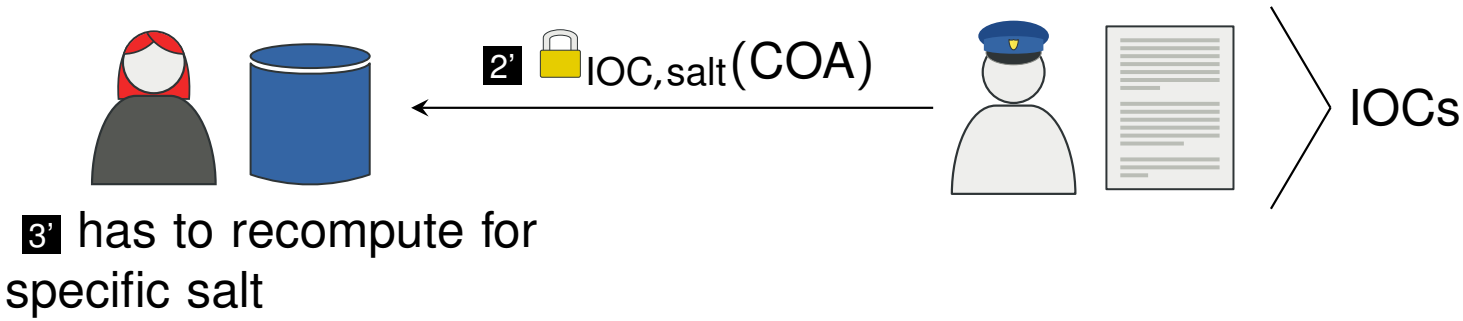
A salt is a large, public, random number.
Due to the randomness, it is unpredictable.



Details about Using a Salt

Definition (Salt)

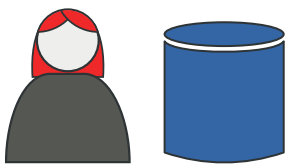
A salt is a large, public, random number.
Due to the randomness, it is unpredictable.



Details about Using a Salt

Definition (Salt)

A salt is a large, public, random number.
Due to the randomness, it is unpredictable.



If using a randomized block cipher modes of operation, no salt is needed.

question overview

Details about Substring Matching

Example (Substring matching)

IOC: `content=abc ∧ offset=4 ∧ depth=6`

	≤ 3	4	5	6	7	8	9	≥ 10	match?
IOC_1	...	a	b	c	...				✗
IOC_2	...		a	b	c	...			✗
IOC_3	...			a	b	c	...		✓
IOC_4	...				a	b	c	...	✗
Observable	...			a	b	c	...		

◂ question overview

Details about Traitor Tracing

Example (Traitor Tracing)

Include an identifier of the subscriber in the cryptographic IOCs:

$(\text{AES}_{k_{\text{ID}}}(\text{COA}), \text{“}\texttt{ID},\texttt{destIP},\texttt{destPort}\text{”}, \texttt{salt}, \texttt{iterations})$

◂ question overview

Privacy-Preserving Aggregation [Shi et al. 2011]

Setup $g \in \mathbb{G}, \quad \mathrm{SK}_i \in_R \mathbb{Z}_p, \quad \mathrm{AK} = -\sum_i \mathrm{SK}_i$

Encryption $\mathrm{CT}_{i,\mathrm{ID}} = g^{x_{i,\mathrm{ID}}} H(\mathrm{ID})^{\mathrm{SK}_i}$

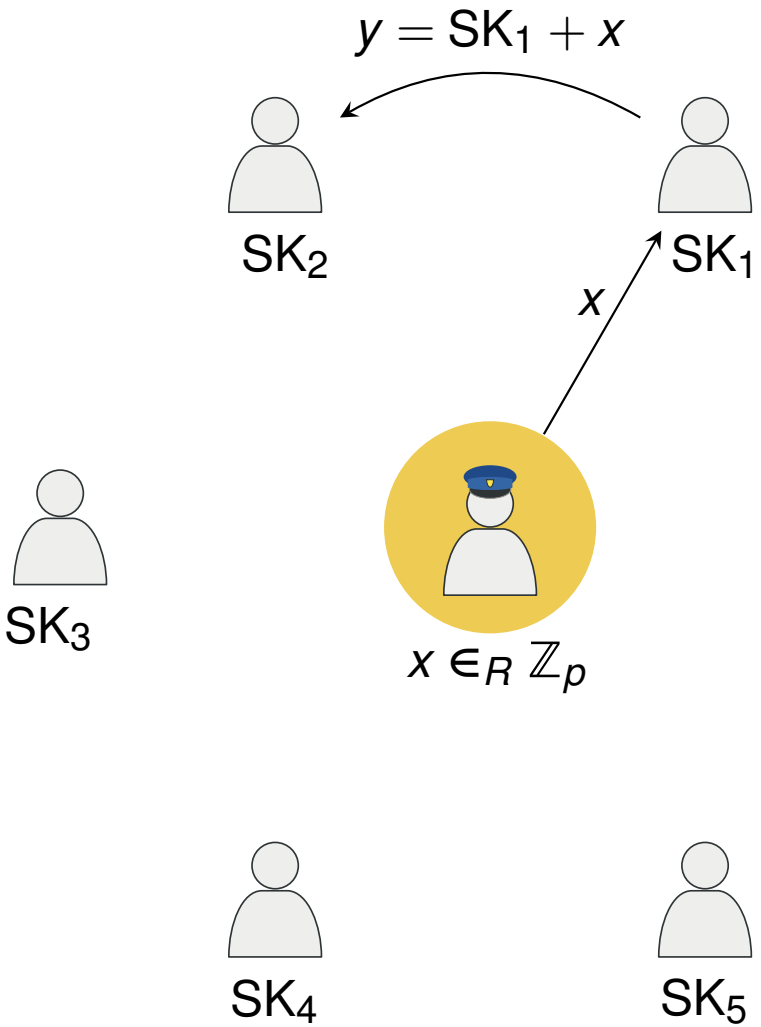
Aggregation $V = H(\mathrm{ID})^{\mathrm{AK}} \prod_i \mathrm{CT}_{i,\mathrm{ID}} = \prod_i g^{x_{i,\mathrm{ID}}}$

Decryption $\mathrm{dlog}_g V = \sum_i x_{i,\mathrm{ID}}$

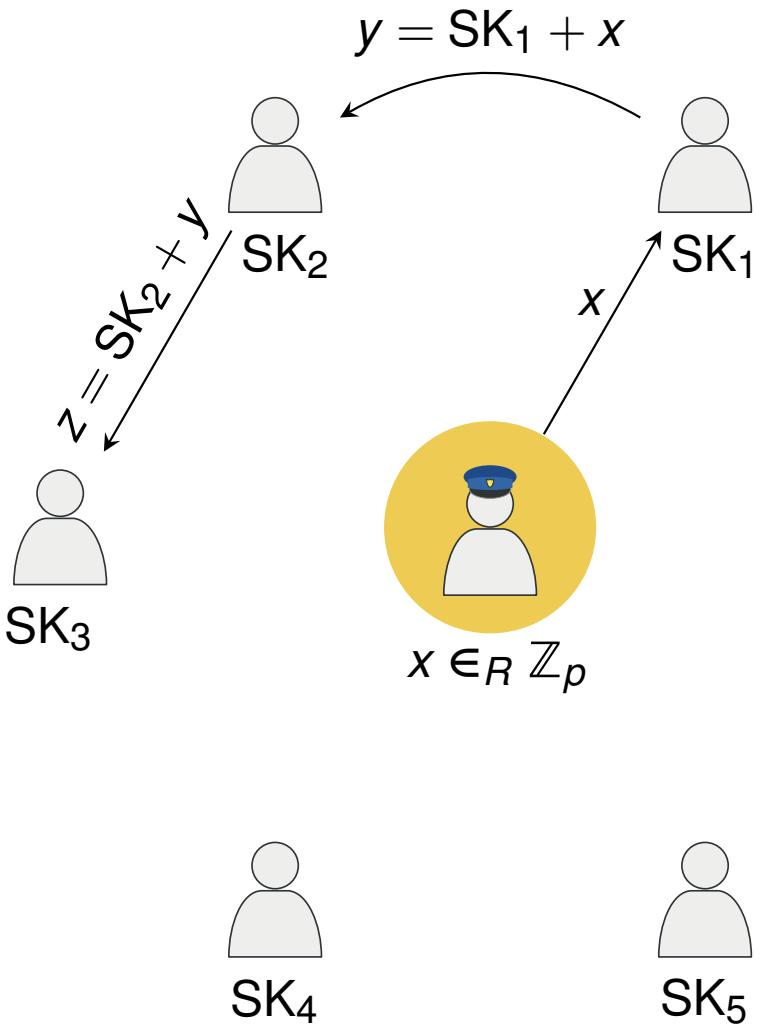
◂ question overview

Privacy-Preserving Aggregation Setup Using MPC

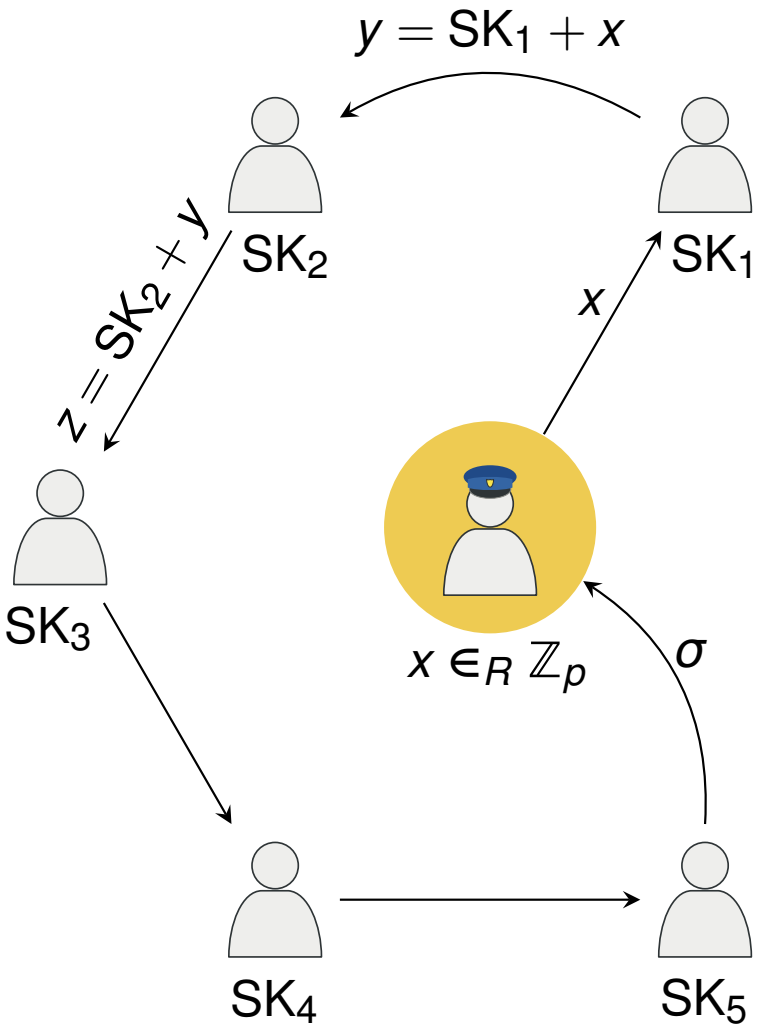
Privacy-Preserving Aggregation Setup Using MPC



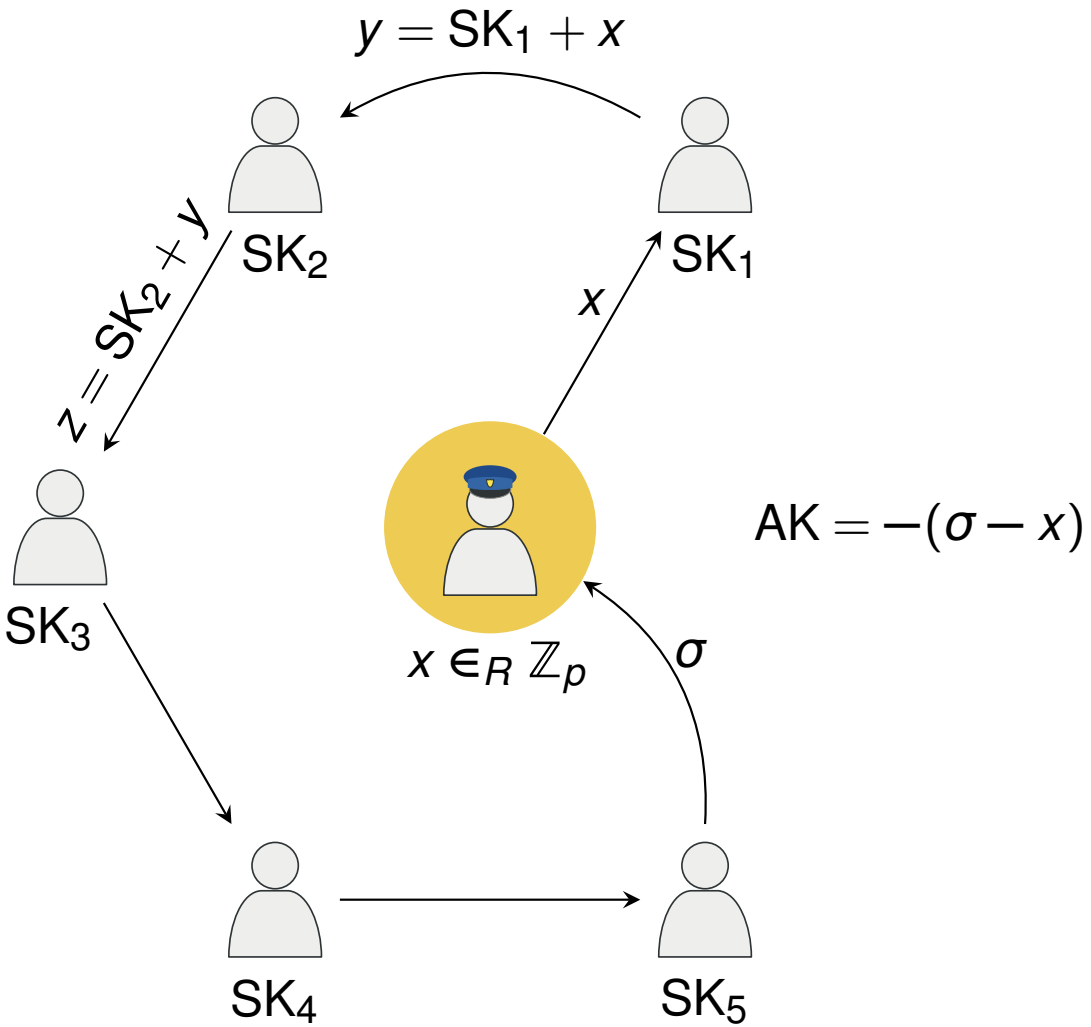
Privacy-Preserving Aggregation Setup Using MPC



Privacy-Preserving Aggregation Setup Using MPC



Privacy-Preserving Aggregation Setup Using MPC



◂ question overview