RUHR-UNIVERSITÄT BOCHUM

A new DDH-based PRF with application to distributed private data analysis

MMC Workshop, 09/08/2017

Filipp Valovich
Horst Görtz Institute for IT Security
Ruhr-University Bochum

hgi
Horst Görtz Institut
für IT-Sicherheit

Decisional Diffie-Hellman

DDH problem

Given (g, q, g^x, g^y, w) for a generator g of a cyclic group $\mathbb{G}$ of order q and $x, y \leftarrow_\$ \mathbb{Z}_q$, decide whether $w = g^{xy}$ or $w \leftarrow_\$ \mathbb{G}$.

Decisional Diffie-Hellman

DDH problem

Given (g, q, g^x, g^y, w) for a generator g of a cyclic group $\mathbb{G}$ of order q and $x, y \leftarrow_\$ \mathbb{Z}_q$, decide whether $w = g^{xy}$ or $w \leftarrow_\$ \mathbb{G}$.

Usually, the DDH problem is considered to be hard in the sub-group $\mathbb{G} = \mathcal{QR}_p$ of $\mathbb{Z}_p^*$ for a large safe prime $p = 2q + 1$.

Decisional Diffie-Hellman

DDH problem

Given (g, q, g^x, g^y, w) for a generator g of a cyclic group $\mathbb{G}$ of order q and $x, y \leftarrow_\$ \mathbb{Z}_q$, decide whether $w = g^{xy}$ or $w \leftarrow_\$ \mathbb{G}$.

Usually, the DDH problem is considered to be hard in the sub-group $\mathbb{G} = \mathcal{QR}_p$ of $\mathbb{Z}_p^*$ for a large safe prime $p = 2q + 1$.

Accordingly, most cryptographic applications based on DDH work in this group.

Decisional Diffie-Hellman

Why $\mathcal{QR}_p$?

The simple Legendre attack does not work in this group.

Decisional Diffie-Hellman

Why $\mathcal{QR}_p$?

The simple Legendre attack does not work in this group.

Idea: use $\mathcal{QR}_{p^2}$

Advantage: computations can be made modulo p^2.

A weak PRF in $\mathcal{QR}_{p^2}$

Theorem

Let q and $p = 2q + 1$ be prime and super-polynomially large in a complexity parameter κ. Then

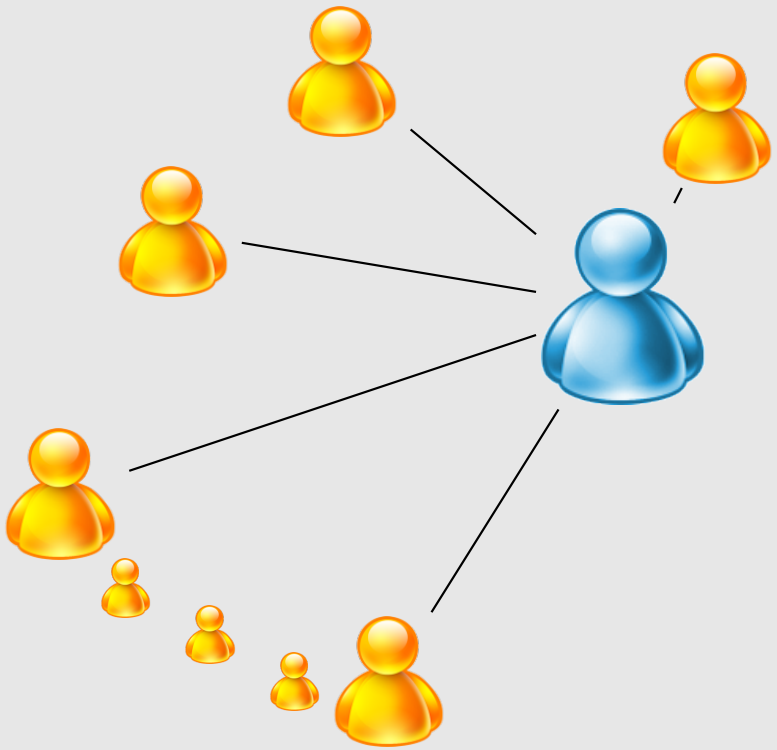
$$\mathcal{F} = \{\mathsf{F}_x : \mathcal{QR}_{p^2} \to \mathcal{QR}_{p^2} \mid \mathsf{F}_x(\alpha) = \alpha^x \bmod p^2\}$$

is a family of weak PRFs under the DDH assumption in $\mathcal{QR}_{p^2}$.

Proof by random self-reducibility.

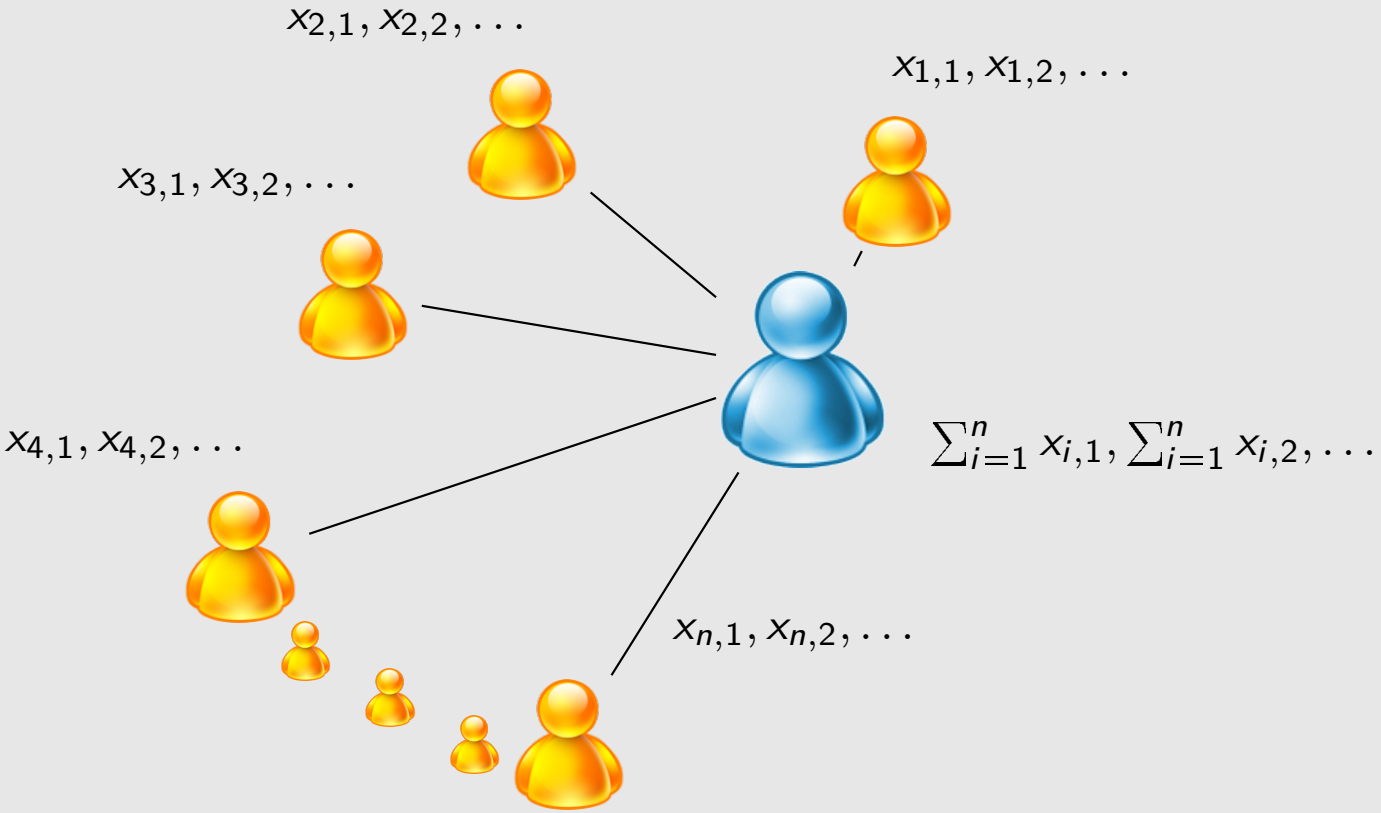
Multi-Party Protocol for Σ

[Shi et al. '11]



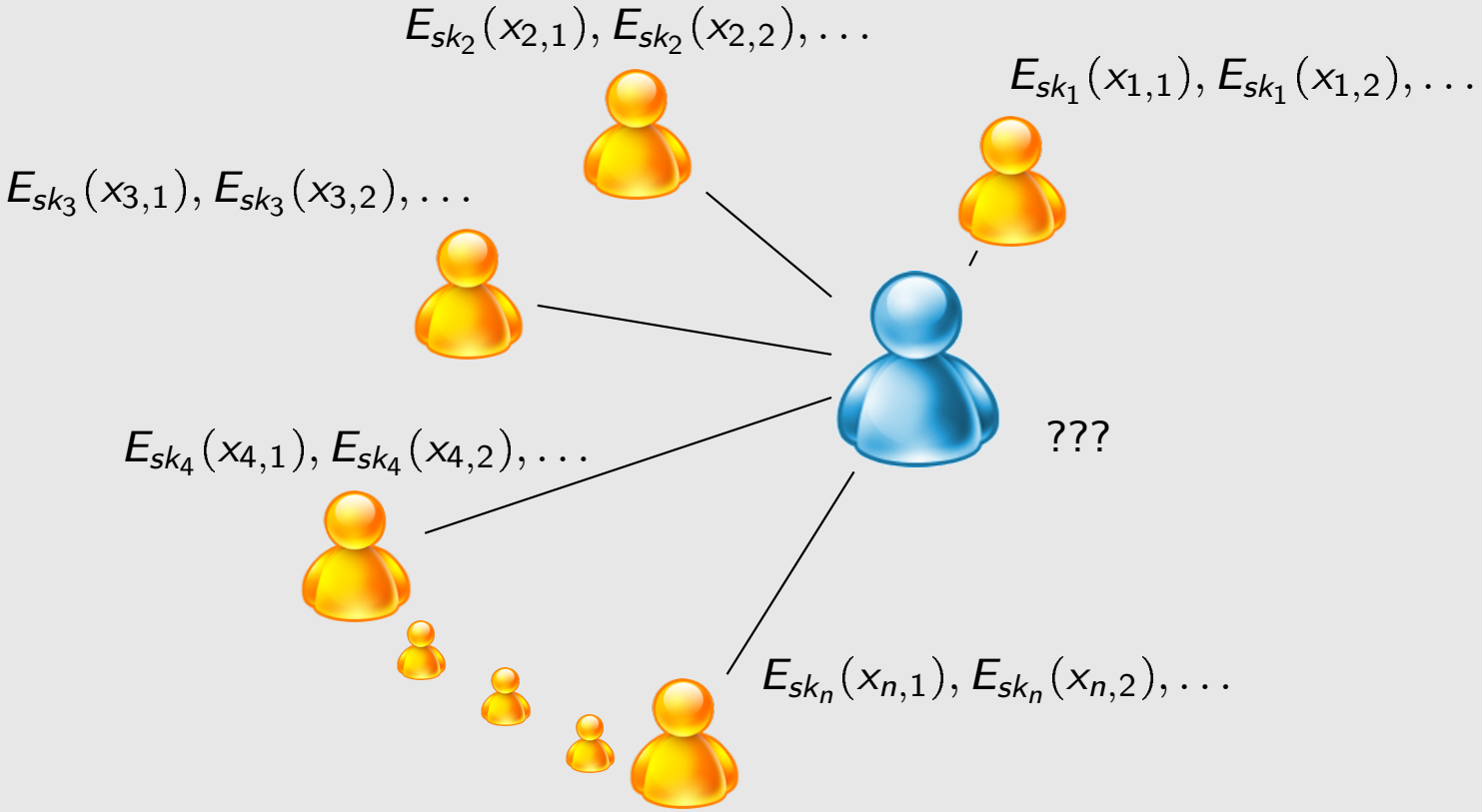
Multi-Party Protocol for Σ

[Shi et al. '11]



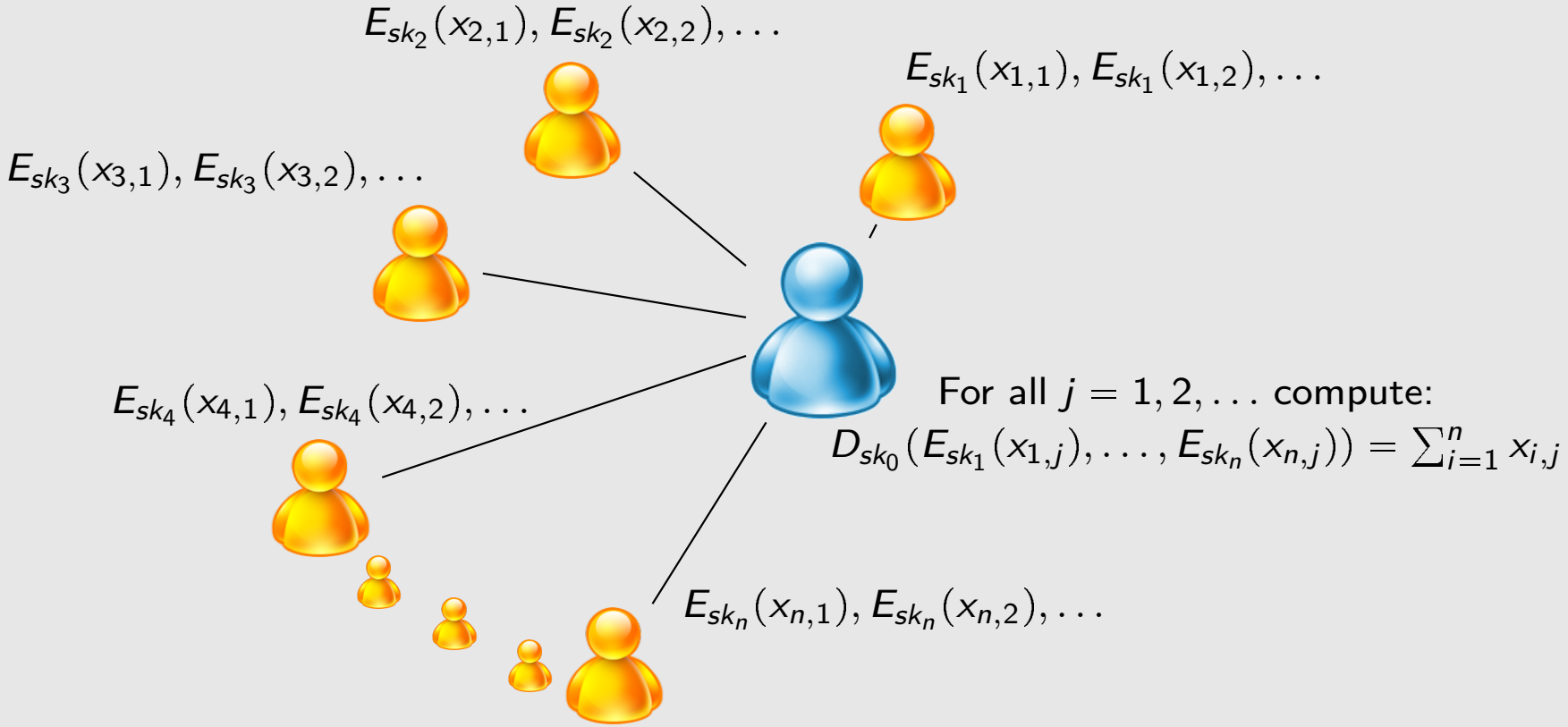
Multi-Party Protocol for Σ

[Shi et al. '11]



Multi-Party Protocol for Σ

[Shi et al. '11]



Private Stream Aggregation

Definition [Shi et al. '11]

Let κ be a security parameter, $\mathcal{D}$ a set and $n = \text{poly}(\kappa)$, $\lambda = \text{poly}(\kappa)$. A Private Stream Aggregation (PSA) scheme $\Sigma = (\text{Setup}, \text{Enc}, \text{Dec})$ is defined by three ppt algorithms:

Setup: $(\text{pp}, T, s_0, s_1, \ldots, s_n) \leftarrow \text{Setup}(1^\kappa)$ with public parameters pp, $T = \{t_1, \ldots, t_\lambda\}$ and secret keys s_i for all $i = 1, \ldots, n$.

Enc: For $t_j \in T$ and all $i = 1, \ldots, n$:

$$c_{i,j} \leftarrow \text{Enc}_{s_i}(t_j, x_{i,j}) \text{ for } x_{i,j} \in \mathcal{D}.$$

Dec: Compute $\sum_{i=1}^{n} x'_{i,j} = \text{Dec}_{s_0}(t_j, c_{1,j}, \ldots, c_{n,j})$ for $t_j \in T$ and ciphers $c_{1,j}, \ldots, c_{n,j}$. For all $t_j \in T$ and $x_{1,j}, \ldots, x_{n,j} \in \mathcal{D}$ the following holds:

$$\text{Dec}_{s_0}(t_j, \text{Enc}_{s_1}(t_j, x_{1,j}), \ldots, \text{Enc}_{s_n}(t_j, x_{n,j})) = \sum_{i=1}^{n} x_{i,j}.$$

Security of a PSA scheme

Informal Definition [Shi et al. '11]

A PSA scheme is secure if for all ppt adversaries with control over a coalition of compromised users, the generated ciphers are indistinguishable under a CPA.

PSA scheme constructions

Example based on DDH [Shi et al. '11]

Let $p = 2q + 1$ be a safe prime and g a generator of $\mathcal{QR}_p$. Let $H : T \to \mathcal{QR}_p$ be a random oracle. For all $i = 1, \ldots, n$ choose $s_i \leftarrow_\$ \mathbb{Z}_q$ and $s_0 = -\sum_{i=1}^{n} s_i \bmod q$.

Enc: compute $c_{i,j} = H(t_j)^{s_i} \cdot g^{x_{i,j}} \bmod p$ with $x_{i,j} \in \mathbb{Z}_m$.

Dec: compute $V_j \equiv H(t_j)^{s_0} \cdot \prod_{i=1}^{n} c_{i,j} \equiv g^{\sum_{i=1}^{n} x_{i,j}} \bmod p$ and take the discrete logarithm.

PSA scheme

PSA scheme constructions

Shi et al. 2011: secure PSA scheme for sum-queries based on DDH-assumption.

PSA scheme

PSA scheme constructions

Shi et al. 2011: secure PSA scheme for sum-queries based on DDH-assumption.

Problem: decryption is not efficient in general, security only in random oracle model.

PSA scheme

PSA scheme constructions

Shi et al. 2011: secure PSA scheme for sum-queries based on DDH-assumption.

Problem: decryption is not efficient in general, security only in random oracle model.

Our solution: generalized scheme based on variete assumptions; give an instantiation based on our PRF with efficient decryption.

PSA scheme constructions: main theorem

Informal Theorem

In the non-adaptive query model, a secure PSA scheme can be built upon any *key-homomorphic weak PRF* F.

PSA scheme constructions: instantiations

Suitable assumptions

1. Random Oracle Model: DDH, DCR, HR, k-LIN
2. Standard model: DLWE, DDH

PSA scheme constructions: instantiations

Example based on DDH

Let $q > m \cdot n$ and $p = 2q + 1$ be prime. For all $i = 1, \ldots, n$ choose $s_i \leftarrow_\$ \mathbb{Z}_{pq}$ and $s_0 = -\sum_{i=1}^{n} s_i \bmod pq$.

PSA scheme constructions: instantiations

Example based on DDH

Let $q > m \cdot n$ and $p = 2q + 1$ be prime. For all $i = 1, \ldots, n$ choose $s_i \leftarrow_\$ \mathbb{Z}_{pq}$ and $s_0 = -\sum_{i=1}^{n} s_i \bmod pq$.

Set $\mathsf{F}_{s_i}(t_j) = t_j^{s_i} \bmod p^2$ for $t_j \leftarrow_\$ QR_{p^2}$, $j = 1, 2, \ldots$.

PSA scheme constructions: instantiations

Example based on DDH

Let $q > m \cdot n$ and $p = 2q + 1$ be prime. For all $i = 1, \ldots, n$ choose $s_i \leftarrow_\$ \mathbb{Z}_{pq}$ and $s_0 = -\sum_{i=1}^{n} s_i \bmod pq$.

Set $\mathsf{F}_{s_i}(t_j) = t_j^{s_i} \bmod p^2$ for $t_j \leftarrow_\$ QR_{p^2}$, $j = 1, 2, \ldots$.

Enc: compute $c_{i,j} = \mathsf{F}_{s_i}(t_j) \cdot (1 + p \cdot x_{i,j}) \bmod p^2$ with $x_{i,j} \in \mathbb{Z}_m$.

PSA scheme constructions: instantiations

Example based on DDH

Let $q > m \cdot n$ and $p = 2q + 1$ be prime. For all $i = 1, \ldots, n$ choose $s_i \leftarrow_\$ \mathbb{Z}_{pq}$ and $s_0 = -\sum_{i=1}^{n} s_i \bmod pq$.

Set $\mathsf{F}_{s_i}(t_j) = t_j^{s_i} \bmod p^2$ for $t_j \leftarrow_\$ QR_{p^2}$, $j = 1, 2, \ldots$.

Enc: compute $c_{i,j} = \mathsf{F}_{s_i}(t_j) \cdot (1 + p \cdot x_{i,j}) \bmod p^2$ with $x_{i,j} \in \mathbb{Z}_m$.

Dec: compute $V_j \in \{1 - p \cdot mn, \ldots, 1 + p \cdot mn\}$ with

$$V_j \equiv \mathsf{F}_{s_0}(t_j) \cdot \prod_{i=1}^{n} c_{i,j}$$

PSA scheme constructions: instantiations

Example based on DDH

Let $q > m \cdot n$ and $p = 2q + 1$ be prime. For all $i = 1, \ldots, n$ choose $s_i \leftarrow_\$ \mathbb{Z}_{pq}$ and $s_0 = -\sum_{i=1}^{n} s_i \bmod pq$.

Set $\mathsf{F}_{s_i}(t_j) = t_j^{s_i} \bmod p^2$ for $t_j \leftarrow_\$ QR_{p^2}$, $j = 1, 2, \ldots$.

Enc: compute $c_{i,j} = \mathsf{F}_{s_i}(t_j) \cdot (1 + p \cdot x_{i,j}) \bmod p^2$ with $x_{i,j} \in \mathbb{Z}_m$.

Dec: compute $V_j \in \{1 - p \cdot mn, \ldots, 1 + p \cdot mn\}$ with

$$V_j \equiv \mathsf{F}_{s_0}(t_j) \cdot \prod_{i=1}^{n} c_{i,j} \equiv \mathsf{F}_{s_0}(t_j) \cdot \prod_{i=1}^{n} \mathsf{F}_{s_i}(t_j) \cdot (1 + p \cdot x_{i,j})$$

PSA scheme constructions: instantiations

Example based on DDH

Let $q > m \cdot n$ and $p = 2q + 1$ be prime. For all $i = 1, \ldots, n$ choose $s_i \leftarrow_\$ \mathbb{Z}_{pq}$ and $s_0 = -\sum_{i=1}^{n} s_i \bmod pq$.

Set $\mathsf{F}_{s_i}(t_j) = t_j^{s_i} \bmod p^2$ for $t_j \leftarrow_\$ QR_{p^2}$, $j = 1, 2, \ldots$.

Enc: compute $c_{i,j} = \mathsf{F}_{s_i}(t_j) \cdot (1 + p \cdot x_{i,j}) \bmod p^2$ with $x_{i,j} \in \mathbb{Z}_m$.

Dec: compute $V_j \in \{1 - p \cdot mn, \ldots, 1 + p \cdot mn\}$ with

$$V_j \equiv \mathsf{F}_{s_0}(t_j) \cdot \prod_{i=1}^{n} c_{i,j} \equiv \mathsf{F}_{s_0}(t_j) \cdot \prod_{i=1}^{n} \mathsf{F}_{s_i}(t_j) \cdot (1 + p \cdot x_{i,j})$$

$$\equiv 1 + p \cdot \sum_{i=1}^{n} x_{i,j} + p^2 \cdot \sum_{i,i' \in [n], i' \neq i} x_{i,j} x_{i',j} + \ldots + p^n \cdot \prod_{i=1}^{n} x_{i,j}$$

PSA scheme constructions: instantiations

Example based on DDH

Let $q > m \cdot n$ and $p = 2q + 1$ be prime. For all $i = 1, \ldots, n$ choose $s_i \leftarrow_\$ \mathbb{Z}_{pq}$ and $s_0 = -\sum_{i=1}^{n} s_i \bmod pq$.

Set $\mathsf{F}_{s_i}(t_j) = t_j^{s_i} \bmod p^2$ for $t_j \leftarrow_\$ QR_{p^2}$, $j = 1, 2, \ldots$.

Enc: compute $c_{i,j} = \mathsf{F}_{s_i}(t_j) \cdot (1 + p \cdot x_{i,j}) \bmod p^2$ with $x_{i,j} \in \mathbb{Z}_m$.

Dec: compute $V_j \in \{1 - p \cdot mn, \ldots, 1 + p \cdot mn\}$ with

$$V_j \equiv \mathsf{F}_{s_0}(t_j) \cdot \prod_{i=1}^{n} c_{i,j} \equiv \mathsf{F}_{s_0}(t_j) \cdot \prod_{i=1}^{n} \mathsf{F}_{s_i}(t_j) \cdot (1 + p \cdot x_{i,j})$$

$$\equiv 1 + p \cdot \sum_{i=1}^{n} x_{i,j} + p^2 \cdot \sum_{i,i' \in [n], i' \neq i} x_{i,j} x_{i',j} + \ldots + p^n \cdot \prod_{i=1}^{n} x_{i,j}$$

$$\equiv 1 + p \cdot \sum_{i=1}^{n} x_{i,j} \bmod p^2 \text{ and compute } \sum_{i=1}^{n} x_{i,j} = \frac{1}{p}(V_j - 1)$$

PSA scheme constructions: instantiations

Conclusion

Compared to **Shi et al. 2011**, our solution always has an efficient decryption and is secure in the standard model.

RUHR-UNIVERSITÄT BOCHUM

Many thanks for your attention!

QUESTIONS?

Horst Görtz Institut für IT-Sicherheit