Computing with Lattices: Commitments, Signatures, and Zero-Knowledge

David Wu

March 2020

Cryptography from Lattices

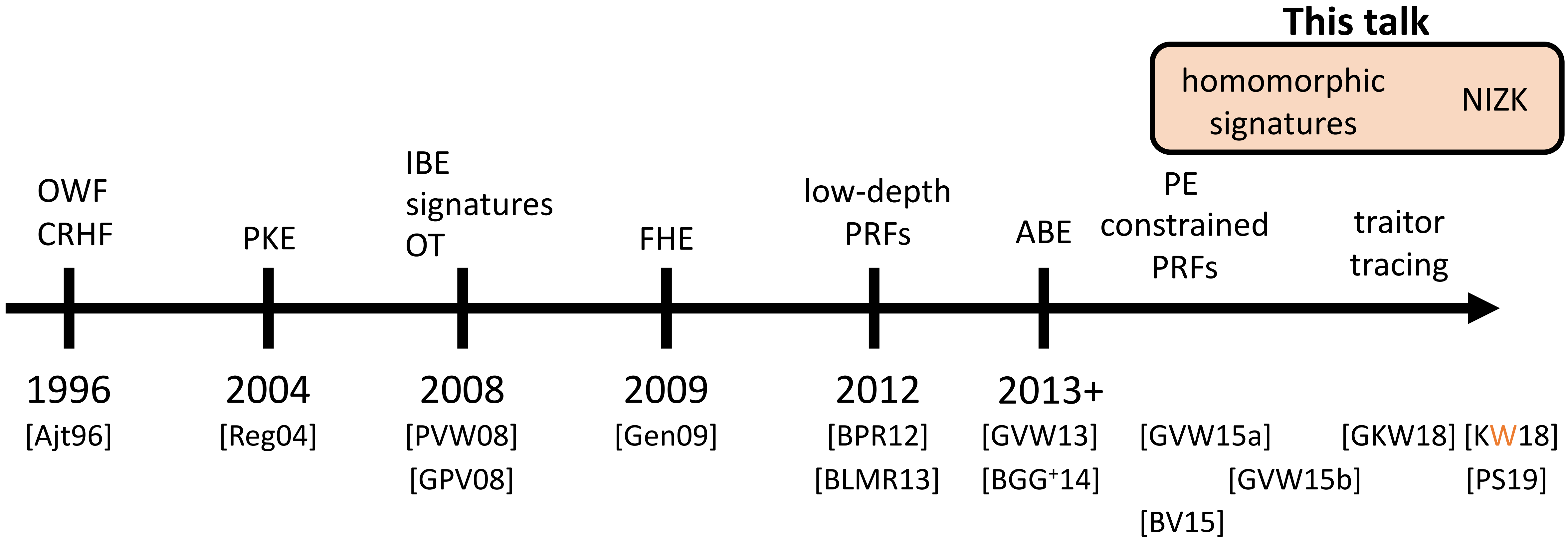
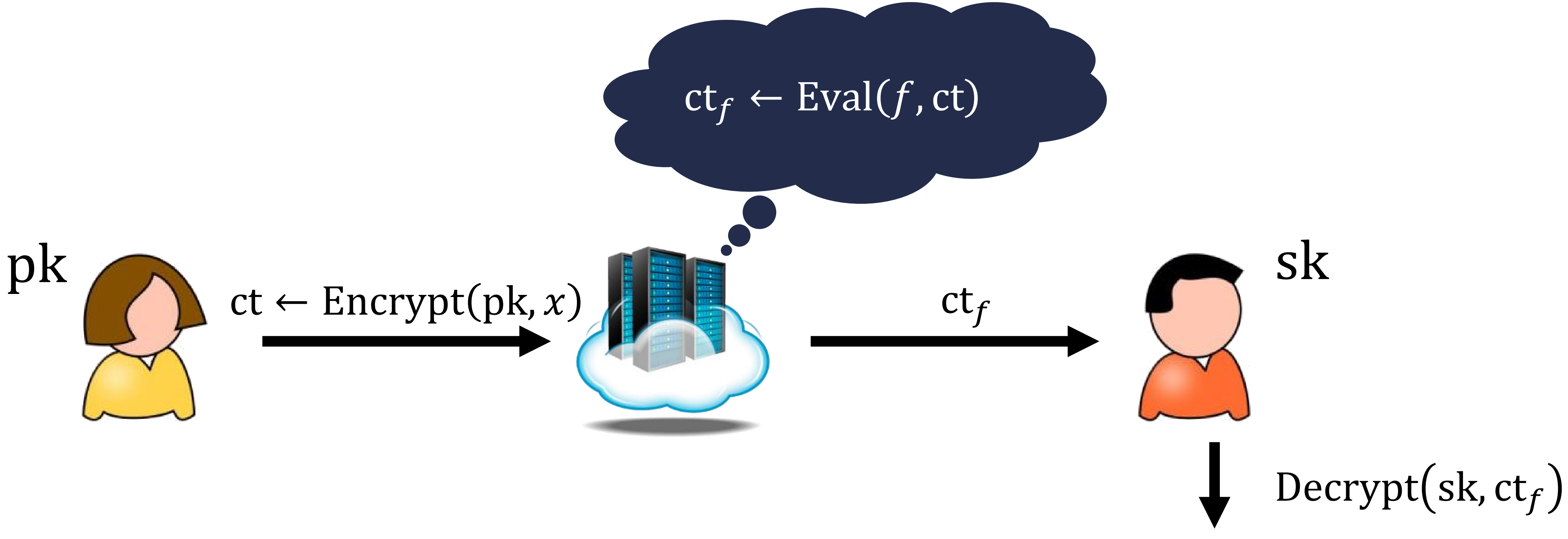


Figure not drawn to scale

Computing on Encrypted Data

<u>confidentiality</u> for computations

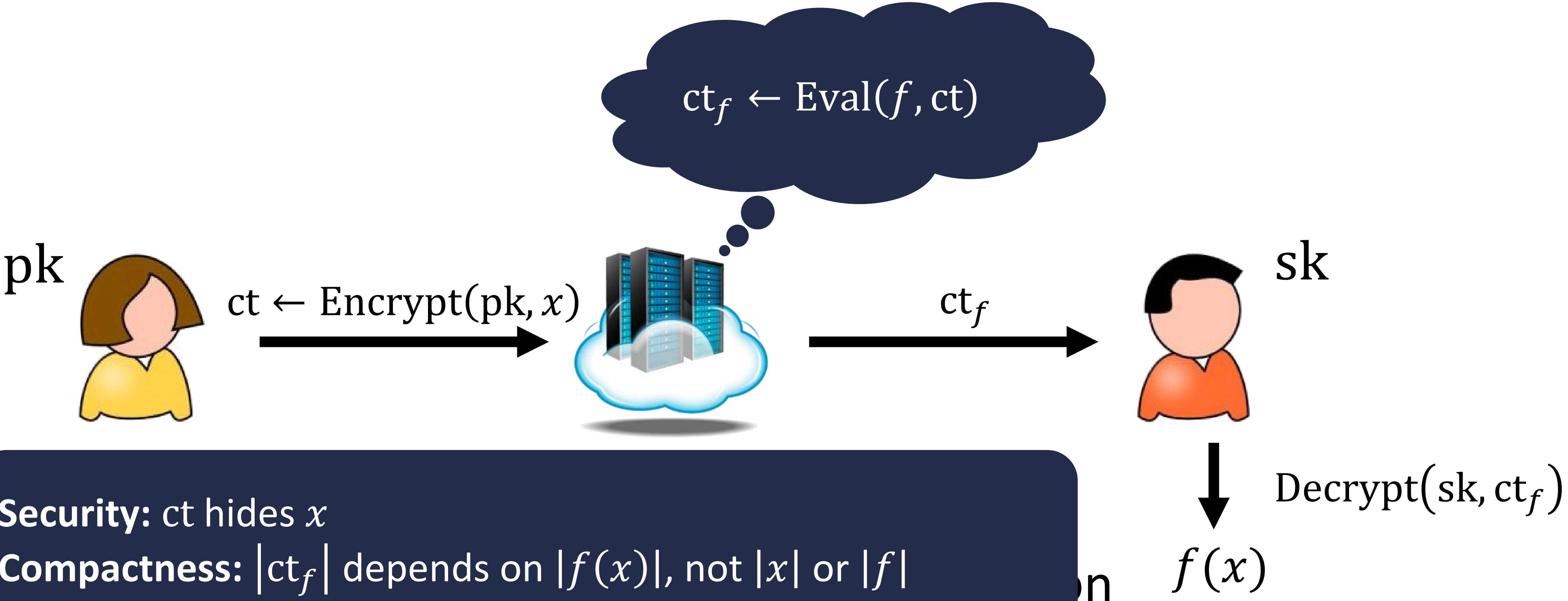


$f(x)$

fully homomorphic encryption

Computing on Encrypted Data

<u>confidentiality</u> for computations

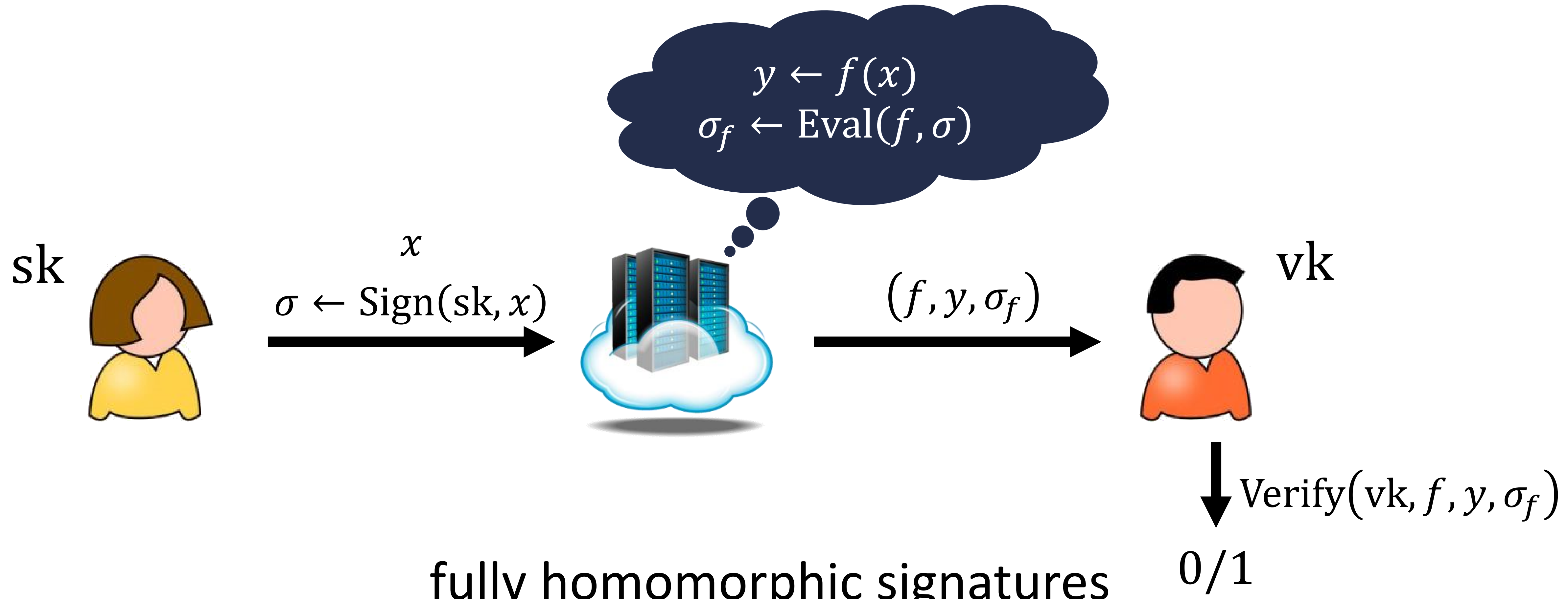


Security: ct hides x

Compactness: $|\mathrm{ct}_f|$ depends on $|f(x)|$, not $|x|$ or $|f|$

Computing on Signed Data

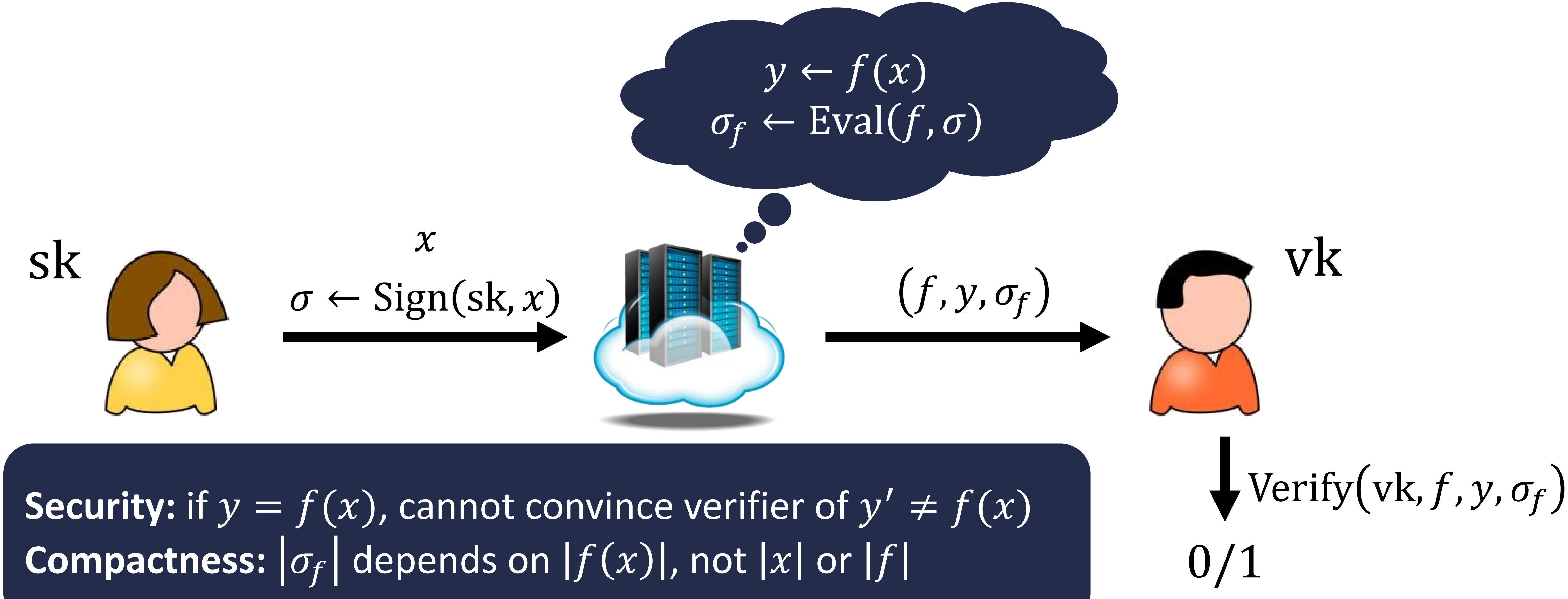
integrity for computations



fully homomorphic signatures

Computing on Signed Data

integrity for computations



Security: if $y = f(x)$, cannot convince verifier of $y' \neq f(x)$
Compactness: $|\sigma_f|$ depends on $|f(x)|$, not $|x|$ or $|f|$

The GSW FHE Scheme

[GSW13]

recall the GSW encryption scheme:

pk: $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ sk: $\boldsymbol{s} \in \mathbb{Z}_q^n$

public key is an **LWE matrix** (columns are LWE samples)

$$\boldsymbol{s}^T\boldsymbol{A} = \boldsymbol{e}^T \approx \boldsymbol{0}^T$$

ciphertext for $x \in \{0,1\}$:

$\boldsymbol{C} = \boldsymbol{AR} + x\boldsymbol{G}$ where $\boldsymbol{R}$ is random short matrix

The GSW FHE Scheme

[GSW13]

recall the GSW encryption scheme:

pk: $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ sk: $\boldsymbol{s} \in \mathbb{Z}_q^{n}$

ciphertext for $x \in \{0,1\}$:

$$\boldsymbol{C} = \boldsymbol{AR} + x\boldsymbol{G}$$ where $\boldsymbol{R}$ is random short matrix

$\boldsymbol{G}$ is the “gadget” matrix:

$$\boldsymbol{G} = \left(1,2,4,\dots,2^{\ell}\right) \otimes \boldsymbol{I}_n \in \mathbb{Z}_q^{n\times n\ell}$$

$\boldsymbol{G}^{-1}: \mathbb{Z}_q^{n\times k} \to \{0,1\}^{n\ell\times k}$ is “binary decomposition”

$$\boldsymbol{G}\boldsymbol{G}^{-1}(\boldsymbol{A}) = \boldsymbol{A}$$

The GSW FHE Scheme

[GSW13]

recall the GSW encryption scheme:

pk: $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ sk: $\boldsymbol{s} \in \mathbb{Z}_q^n$

public key is an **LWE matrix** (columns are LWE samples)

$$\boldsymbol{s}^T\boldsymbol{A} = \boldsymbol{e}^T \approx \boldsymbol{0}^T$$

ciphertext for $x \in \{0,1\}$:

$$\boldsymbol{C} = \boldsymbol{AR} + x\boldsymbol{G}$$ where $\boldsymbol{R}$ is random short matrix

decryption:

$$\boldsymbol{s}^T\boldsymbol{C} = \boldsymbol{s}^T\boldsymbol{AR} + x \cdot \boldsymbol{s}^T\boldsymbol{G} \approx x \cdot \boldsymbol{s}^T\boldsymbol{G}$$

Homomorphic Operations in GSW

[GSW13]

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{R}_1 + x_1\boldsymbol{G} \qquad \boldsymbol{C}_2 = \boldsymbol{A}\boldsymbol{R}_2 + x_2\boldsymbol{G}$$

$$\boldsymbol{C}_+ = \boldsymbol{C}_1 + \boldsymbol{C}_2 \quad = \boldsymbol{A}\underbrace{(\boldsymbol{R}_1 + \boldsymbol{R}_2)}_{\boldsymbol{R}_+} + (x_1 + x_2)\boldsymbol{G}$$

Homomorphic Operations in GSW

[GSW13]

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{R}_1 + x_1\boldsymbol{G} \qquad \boldsymbol{C}_2 = \boldsymbol{A}\boldsymbol{R}_2 + x_2\boldsymbol{G}$$

$$\begin{aligned}\boldsymbol{C}_+ = \boldsymbol{C}_1 + \boldsymbol{C}_2 &= \boldsymbol{A}(\boldsymbol{R}_1 + \boldsymbol{R}_2) + (x_1 + x_2)\boldsymbol{G} \\ &= \boldsymbol{A}\boldsymbol{R}_+ + (x_1 + x_2)\boldsymbol{G}\end{aligned}$$

$$\begin{aligned}\boldsymbol{C}_\times = \boldsymbol{C}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2) &= \boldsymbol{A}\boldsymbol{R}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2) + x_1\boldsymbol{C}_2 \\ &= \boldsymbol{A}\underbrace{(\boldsymbol{R}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2) + x_1\boldsymbol{R}_2)}_{\boldsymbol{R}_\times} + x_1x_2\boldsymbol{G}\end{aligned}$$

Homomorphic Operations in GSW

[GSW13]

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{R}_1 + x_1\boldsymbol{G} \qquad \boldsymbol{C}_2 = \boldsymbol{A}\boldsymbol{R}_2 + x_2\boldsymbol{G}$$

$$\begin{aligned} \boldsymbol{C}_+ = \boldsymbol{C}_1 + \boldsymbol{C}_2 &= \boldsymbol{A}(\boldsymbol{R}_1 + \boldsymbol{R}_2) + (x_1 + x_2)\boldsymbol{G} \\ &= \boldsymbol{A}\boldsymbol{R}_+ + (x_1 + x_2)\boldsymbol{G} \end{aligned}$$

$$\begin{aligned} \boldsymbol{C}_\times = \boldsymbol{C}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2) &= \boldsymbol{A}\boldsymbol{R}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2) + x_1\boldsymbol{C}_2 \\ &= \boldsymbol{A}(\boldsymbol{R}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2) + x_1\boldsymbol{R}_2) + x_1x_2\boldsymbol{G} \\ &= \boldsymbol{A}\boldsymbol{R}_\times + x_1x_2\boldsymbol{G} \end{aligned}$$

Correctness: $\boldsymbol{R}_1, \boldsymbol{R}_2, x_1$ short $\Rightarrow$ $\boldsymbol{R}_+, \boldsymbol{R}_\times$ also short

Homomorphic Operations in GSW

[GSW13]

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{R}_1 + x_1\boldsymbol{G}$$
$$\boldsymbol{C}_2 = \boldsymbol{A}\boldsymbol{R}_2 + x_2\boldsymbol{G}$$
$$\vdots$$
$$\boldsymbol{C}_n = \boldsymbol{A}\boldsymbol{R}_n + x_n\boldsymbol{G}$$

$$\Rightarrow \quad \boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{R}_{f,x} + f(x)\boldsymbol{G}$$

"input-independent" evaluation

$\boldsymbol{C}_f$ is a function of $\boldsymbol{C}_1, \dots, \boldsymbol{C}_n, f$
(and <u>independent</u> of x)

Homomorphic Operations in GSW

[GSW13]

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{R}_1 + x_1\boldsymbol{G} \qquad \boldsymbol{C}_2 = \boldsymbol{A}\boldsymbol{R}_2 + x_2\boldsymbol{G}$$

$$\boldsymbol{C}_+ = \boldsymbol{C}_1 + \boldsymbol{C}_2 = \boldsymbol{A}(\boldsymbol{R}_1 + \boldsymbol{R}_2) + (x_1 + x_2)\boldsymbol{G}$$
$$= \boldsymbol{A}\boldsymbol{R}_+ + (x_1 + x_2)\boldsymbol{G}$$

$$\boldsymbol{C}_\times = \boldsymbol{C}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2) = \boldsymbol{A}(\boldsymbol{R}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2) + x_1\boldsymbol{R}_2) + x_1x_2\boldsymbol{G}$$
$$= \boldsymbol{A}\boldsymbol{R}_\times + x_1x_2\boldsymbol{G}$$

Homomorphic Operations in GSW

[GSW13]

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{R}_1 + x_1\boldsymbol{G} \qquad \boldsymbol{C}_2 = \boldsymbol{A}\boldsymbol{R}_2 + x_2\boldsymbol{G}$$

$$\boldsymbol{C}_+ = \boldsymbol{C}_1 + \boldsymbol{C}_2 = \boldsymbol{A}(\boldsymbol{R}_1 + \boldsymbol{R}_2) + (x_1 + x_2)\boldsymbol{G}$$
$$= \boldsymbol{A}\boldsymbol{R}_+ + (x_1 + x_2)\boldsymbol{G}$$

$$\boldsymbol{C}_\times = \boldsymbol{C}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2) = \boldsymbol{A}(\boldsymbol{R}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2) + x_1\boldsymbol{R}_2) + x_1x_2\boldsymbol{G}$$
$$= \boldsymbol{A}\boldsymbol{R}_\times + x_1x_2\boldsymbol{G}$$

observation: $\boldsymbol{R}_+$ and $\boldsymbol{R}_\times$ is a short linear combination of $\boldsymbol{R}_1$ and $\boldsymbol{R}_2$

The BGG+ Homomorphisms

[BGGHNSVV14]

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{R}_1 + x_1\boldsymbol{G} \quad \cdots \quad \boldsymbol{C}_n = \boldsymbol{A}\boldsymbol{R}_n + x_n\boldsymbol{G}$$

$$\boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{R}_{f,x} + \boldsymbol{f}(x)\boldsymbol{G} \quad \text{where} \quad \boldsymbol{R}_{f,x} = [\boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_n]\boldsymbol{H}_{f,x}$$

and $\boldsymbol{H}_{f,x}$ is short

equivalently:

$$[\boldsymbol{A}\boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{A}\boldsymbol{R}_n]\boldsymbol{H}_{f,x} = \boldsymbol{A}\boldsymbol{R}_{f,x}$$

$$[\boldsymbol{C}_1 - x_1\boldsymbol{G} \mid \cdots \mid \boldsymbol{C}_n - x_n\boldsymbol{G}]\boldsymbol{H}_{f,x} = \boldsymbol{C}_f - f(x)\boldsymbol{G}$$

The BGG+ Homomorphisms

[BGGHNSVV14]

"input-independent" evaluation (given $\boldsymbol{C}_1, \ldots, \boldsymbol{C}_n, f$):

$$\boldsymbol{C}_1, \ldots, \boldsymbol{C}_n \mapsto \boldsymbol{C}_f$$

sufficient for FHE

"input-dependent" evaluation (given $\boldsymbol{C}_1, \ldots, \boldsymbol{C}_n, f, x$):

$$[\boldsymbol{C}_1 - x_1\boldsymbol{G} \mid \cdots \mid \boldsymbol{C}_{\boldsymbol{n}} - x_n\boldsymbol{G}]\boldsymbol{H}_{f,x} = \boldsymbol{C}_f - f(x)\boldsymbol{G}$$

applications:

	input-independent evaluation ($\boldsymbol{A}_f$)	input-dependent evaluation ($\boldsymbol{H}_{f,x}$)
attribute-based encryption [BGGHNSVV14]	key-generation	decryption
homomorphic signatures [GVW15]	verification	signing
constrained PRFs [BV15]	normal evaluation	constrained evaluation

GSW as a Homomorphic Commitment

[GVW14]

public parameters $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ (LWE matrix)

$$\boldsymbol{C} = \boldsymbol{A}\boldsymbol{R} + x\boldsymbol{G}$$

commitment

opening (check $\boldsymbol{R}$ short)

message

encryption of x with randomness R

↕

commitment to x with opening R

GSW as a Homomorphic Commitment

[GVW14]

public parameters $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ (LWE matrix)

$$\boldsymbol{C} = \boldsymbol{A}\boldsymbol{R} + x\boldsymbol{G}$$

commitment

opening
(check $\boldsymbol{R}$ short)

message

statistically binding: correctness of GSW (in fact, extractable)

computationally hiding: security of GSW (under LWE)

GSW as a Homomorphic Commitment

[GVW14]

computing on committed values:

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{R}_1 + x_1\boldsymbol{G}$$
$$\boldsymbol{C}_2 = \boldsymbol{A}\boldsymbol{R}_2 + x_2\boldsymbol{G}$$
$$\vdots$$
$$\boldsymbol{C}_n = \boldsymbol{A}\boldsymbol{R}_n + x_n\boldsymbol{G}$$

goal: open the committed value to $y = f(x)$

syntax: $\text{Open}(\text{pp}, c, (f, y), r)$

pp: public parameters

c: commitment

(f, y): value

r: opening

binding:

adversary cannot open c to $(f, y) \neq (f, y')$

Openings are with respect to a value y <u>and</u> a function f

GSW as a Homomorphic Commitment

[GVW14]

computing on committed values:

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{R}_1 + x_1\boldsymbol{G}$$
$$\boldsymbol{C}_2 = \boldsymbol{A}\boldsymbol{R}_2 + x_2\boldsymbol{G}$$
$$\vdots$$
$$\boldsymbol{C}_n = \boldsymbol{A}\boldsymbol{R}_n + x_n\boldsymbol{G}$$

goal: open the committed value to $y = f(x)$

syntax: $\mathrm{Open}(\mathrm{pp}, c, (f, y), r)$

pp: public parameters
c: commitment
(f, y): value
r: opening

binding:

adversary cannot open c to $(f, y) \neq (f, y')$

Application:
preprocessing NIZKs

GSW as a Homomorphic Commitment

[GVW14]

computing on committed values:

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{R}_1 + x_1\boldsymbol{G}$$
$$\boldsymbol{C}_2 = \boldsymbol{A}\boldsymbol{R}_2 + x_2\boldsymbol{G}$$
$$\vdots$$
$$\boldsymbol{C}_n = \boldsymbol{A}\boldsymbol{R}_n + x_n\boldsymbol{G}$$

commitment:

$$\boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{R}_{f,x} + f(x)\boldsymbol{G}$$

$\boldsymbol{C}_f$ is a commitment to $f(x)$ with opening $\boldsymbol{R}_{f,x}$

GSW as a Homomorphic Commitment

[GVW14]

computing on committed values:

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{R}_1 + x_1\boldsymbol{G}$$
$$\boldsymbol{C}_2 = \boldsymbol{A}\boldsymbol{R}_2 + x_2\boldsymbol{G}$$
$$\vdots$$
$$\boldsymbol{C}_n = \boldsymbol{A}\boldsymbol{R}_n + x_n\boldsymbol{G}$$

$\Rightarrow$

commitment:

$$\boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{R}_{f,x} + f(x)\boldsymbol{G}$$

opening:

$$\boldsymbol{R}_{f,x} = [\boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_n]\boldsymbol{H}_{f,x}$$

check opening by computing $\boldsymbol{C}_f$ from $\boldsymbol{C}_1, \dots, \boldsymbol{C}_n$ (does not need to know x) and verifying that $\boldsymbol{R}_{f,x}$ is small and $\boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{R}_{f,x} + f(x)\boldsymbol{G}$

GSW as a Homomorphic Commitment

[GVW14]

computing on committed values:

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{R}_1 + x_1\boldsymbol{G}$$
$$\boldsymbol{C}_2 = \boldsymbol{A}\boldsymbol{R}_2 + x_2\boldsymbol{G}$$
$$\vdots$$
$$\boldsymbol{C}_n = \boldsymbol{A}\boldsymbol{R}_n + x_n\boldsymbol{G}$$

commitment:

$$\boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{R}_{f,x} + f(x)\boldsymbol{G}$$

opening:

$$\boldsymbol{R}_{f,x} = [\boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_n]\boldsymbol{H}_{f,x}$$

"input-independent" evaluation (given $\boldsymbol{C}_1, \ldots, \boldsymbol{C}_n, f$):

$$\boldsymbol{C}_1, \ldots, \boldsymbol{C}_n \mapsto \boldsymbol{C}_f$$

verification

"input-dependent" evaluation (given $\boldsymbol{C}_1, \ldots, \boldsymbol{C}_n, f, x$):

$$[\boldsymbol{C}_1 - x_1\boldsymbol{G} \mid \cdots \mid \boldsymbol{C}_n - x_n\boldsymbol{G}]\boldsymbol{H}_{f,x} = \boldsymbol{C}_f - f(x)\boldsymbol{G}$$

evaluation

From Commitments to Proofs

homomorphic commitments can be used to prove relations on secret values

$C_x \leftarrow \mathrm{Commit}(\mathrm{pp}, x)$

opening for $C_{\mathcal{R},x}$

opening can be viewed as a "proof" on the value $\mathcal{R}(x)$

prover

verifier

compute opening for $C_{\mathcal{R},x}$ to $\mathcal{R}(x)$

compute commitment $C_{\mathcal{R},x}$ from C_x

Goal: prove that a (secret) statement x satisfies some relation $\mathcal{R}$

From Commitments to NIZKs (Dream Version)

$\mathcal{R}(x, w)$: NP relation

common reference string

$C_w \leftarrow \mathrm{Commit}(\mathrm{pp}, w)$

opening for $C_{\mathcal{R}_x, w}$

prover

(x, w)

$\mathcal{R}_x(w) \coloneqq \mathcal{R}(x, w)$

verifier

x

function that depends <u>only</u> on the statement x

verifier checks $C_{\mathcal{R}_x, w}$ opens to 1

From Commitments to NIZKs (Dream Version)

$\mathcal{R}(x, w)$: NP relation

$C_w \leftarrow \text{Commit}(\text{pp}, w)$

opening for $C_{\mathcal{R}_x, w}$

Zero-Knowledge ("proof hides w"):

- C_w hides w (commitment is hiding)
- $C_{\mathcal{R}_x, w}$ is a public function of C_w
- opening to $C_{\mathcal{R}_x, w}$ might leak information about w (can be fixed)

From Commitments to NIZKs (Dream Version)

$\mathcal{R}(x, w)$: NP relation

$C_w \leftarrow \mathrm{Commit}(\mathrm{pp}, w)$ $\longrightarrow$

opening for $C_{\mathcal{R}_x, w}$ $\longrightarrow$

Soundness (for x where $\mathcal{R}_x(w) = 0$ for all w):

- if C_{w^*} is an <u>honestly-generated</u> commitment to some value w^*, then $C_{\mathcal{R}_x, w^*}$ is a commitment to $\mathcal{R}_x(w^*) = 0$ by correctness
- statistical soundness follows by statistical binding

From Commitments to NIZKs (Dream Version)

<u>**Open Problem**</u>**:** NIZK proof of well-formedness of GSW ciphertext $\boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$

$$\exists x \in \{0,1\}, \text{short } \boldsymbol{R} \in \mathbb{Z}_q^{m \times m} : \boldsymbol{C} = \boldsymbol{A}\boldsymbol{R} + x\boldsymbol{G}$$

Would yield <u>direct</u> construction of NIZK for NP (lattice "analog" of [GOS06])

- Construction makes black-box use of cryptography (in contrast to Fiat-Shamir approach [CCHLRRW19, PS19])

Soundness (for x where $\mathcal{R}_x($ $= 0$ for all w):

- if C_{w^*} is an <u>honestly-generated</u> commitment to some value w^*, then $C_{\mathcal{R}_x, w^*}$ is a commitment to $\mathcal{R}_x(w^*) = 0$ by correctness
- statistical soundness follows by statistical binding

From Commitments to Preprocessing NIZKs

[KW18]

$\mathcal{R}(x, w)$: NP relation

$C_w \leftarrow \mathrm{Commit}(\mathrm{pp}, w)$ →

opening for $C_{\mathcal{R}_x, w}$ →

Can we still use this approach to obtain some type of NIZK?

Yes! But in a weaker "preprocessing" or "correlated randomness" model

NIZKs in the Preprocessing Model

[DMP88]

(trusted) setup algorithm generates both proving key k_P and a verification key k_V (statement-independent)

k_P

k_V

prover

$$\pi = \mathrm{Prove}(k_P, x, w)$$

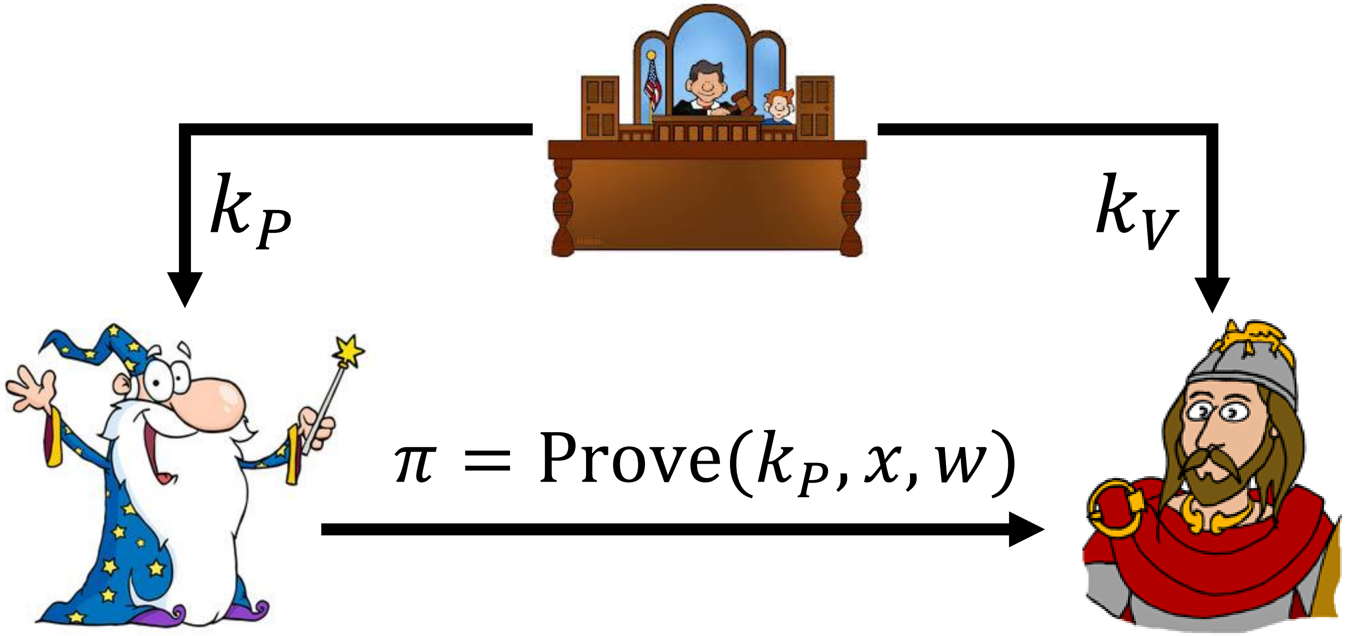
prover algorithm takes proving key k_P, NP statement x, and NP witness w

verifier

$$\mathrm{Verify}(k_V, x, \pi)$$

NIZKs in the Preprocessing Model

[DMP88]



main requirement:
reusability

suffices for many applications of NIZKs

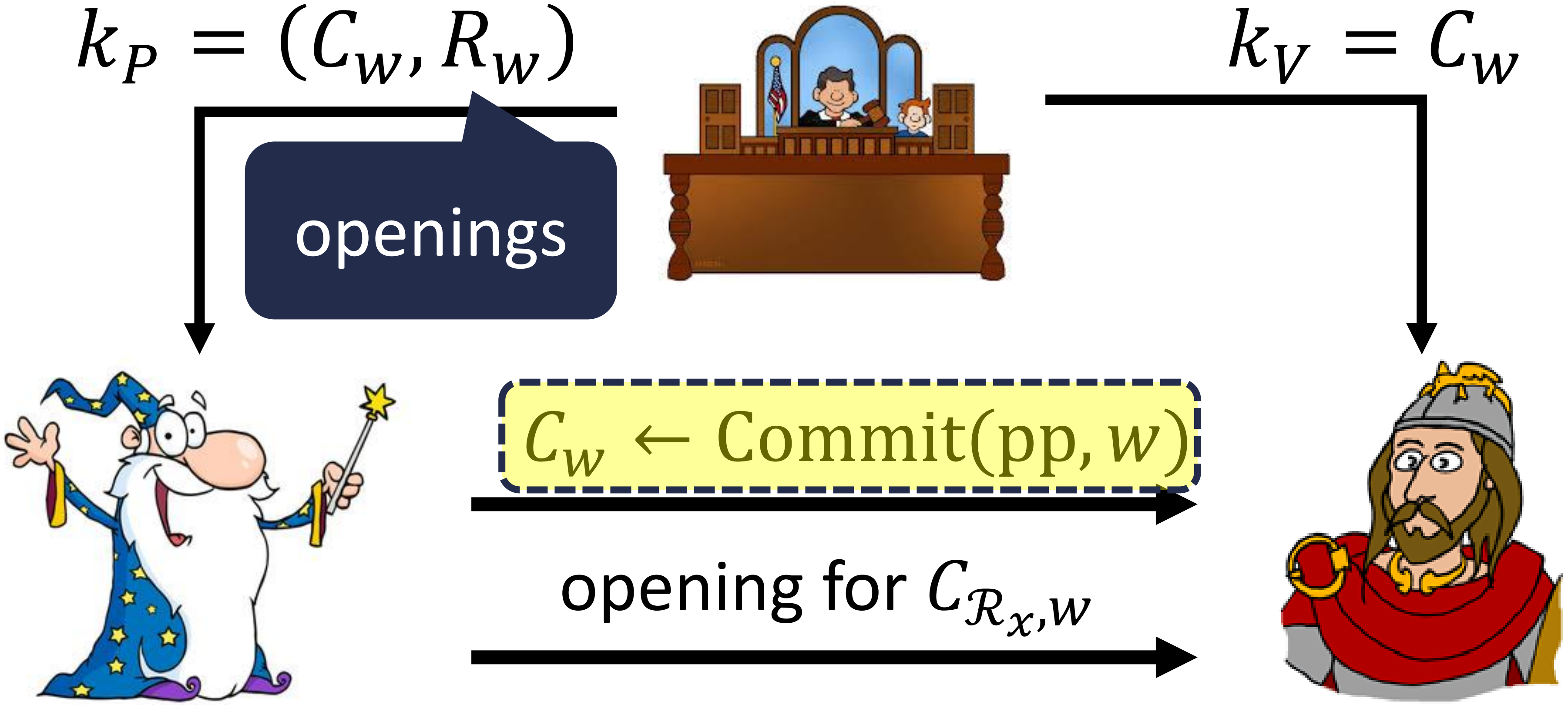
CRS model: k_P and k_V are both public

simpler than CRS model:

- soundness holds assuming k_V is hidden
- zero-knowledge holds assuming k_P is hidden

From Commitments to Preprocessing NIZKs

[KW18]

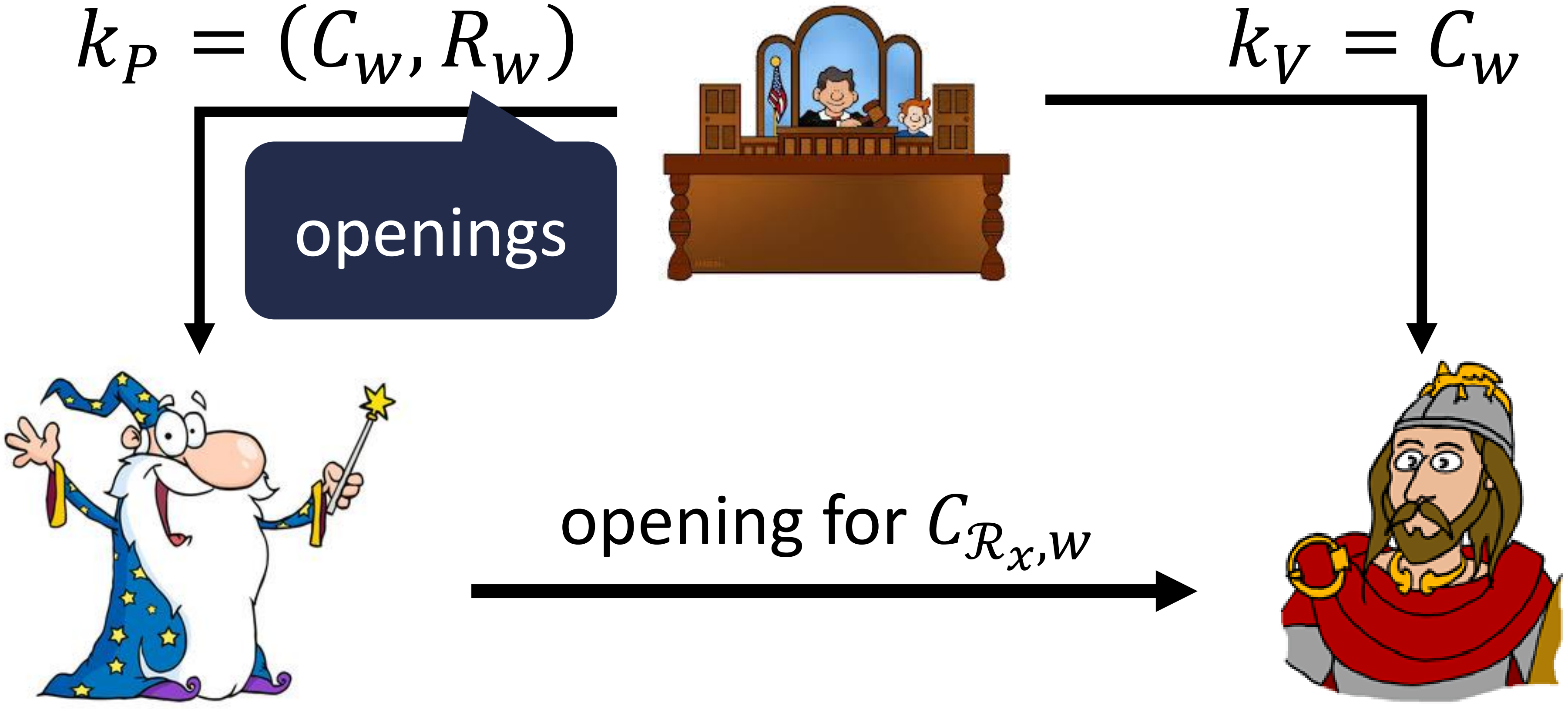


challenge: proving that C_w is a valid commitment

solution: have a trusted party generate it!

From Commitments to Preprocessing NIZKs

[KW18]



problem: preprocessing is <u>witness-dependent</u>

solution: add a layer of indirection

From Commitments to Preprocessing NIZKs

[KW18]

(k, C_k, R_k)

prover is given commitment
and opening to an encryption key k

solution: add a layer of indirection

From Commitments to Preprocessing NIZKs

[KW18]

(k, C_k, R_k)

verifier given commitment to k

C_k

solution: add a layer of indirection

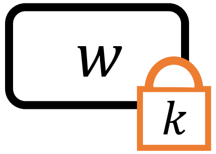
From Commitments to Preprocessing NIZKs

[KW18]

(k, C_k, R_k)

$$f_{x,\mathrm{ct}}(k) = \mathcal{R}\big(x, \mathrm{Decrypt}(k, \mathrm{ct})\big)$$
[Checks that ct encrypts a valid witness]

C_k



opening for $C_{f_{x,\mathrm{ct}},k}$

$$\mathrm{ct} \leftarrow \mathrm{Encrypt}(k, w)$$
[ct is an encryption of the witness w]

solution: add a layer of indirection

From Commitments to Preprocessing NIZKs

[KW18]

(k, C_k, R_k)

C_k

$f_{x,\mathrm{ct}}(k) = \mathcal{R}\big(x, \mathrm{Decrypt}(k, \mathrm{ct})\big)$
[Checks that ct encrypts a valid witness]

w k

opening for $C_{f_{x,\mathrm{ct}},k}$

$\mathrm{ct} \leftarrow \mathrm{Encrypt}(k, w)$
[ct is an encryption of the witness w]

verifier computes $C_{f_{x,\mathrm{ct}},k}$ from (x, ct, C_k) and checks that it opens to 1

From Commitments to Preprocessing NIZKs

[KW18]

(k, C_k, R_k)

C_k

$f_{x,\mathrm{ct}}(k) = \mathcal{R}\big(x, \mathrm{Decrypt}(k, \mathrm{ct})\big)$
[Checks that ct encrypts a valid witness]

w k

opening for $C_{f_{x,\mathrm{ct}},k}$

$\mathrm{ct} \leftarrow \mathrm{Encrypt}(k, w)$
[ct is an encryption of the witness w]

Soundness: $C_{f_{x,\mathrm{ct}},k}$ is a commitment on $f_{x,\mathrm{ct}}(k) = 0$ for all k and a false x; soundness follows by statistical binding of commitment scheme

From Commitments to Preprocessing NIZKs

[KW18]

(k, C_k, R_k)

C_k

$f_{x,\mathrm{ct}}(k) = \mathcal{R}\big(x, \mathrm{Decrypt}(k, \mathrm{ct})\big)$
[Checks that ct encrypts a valid witness]

w k

opening for $C_{f_{x,\mathrm{ct}},k}$

$\mathrm{ct} \leftarrow \mathrm{Encrypt}(k, w)$
[ct is an encryption of the witness w]

Zero-Knowledge: commitment + opening hide k and encryption scheme hides w

From Commitments to Preprocessing NIZKs

[KW18]

can be entirely public!

$k_P = (k, C_k, R_k)$

$k_V = C_k$

$\pi = \text{Prove}(k_P, x, w)$

$\text{Verify}(k_V, x, \pi)$

designated-prover NIZK from homomorphic commitments (under LWE)

From Commitments to Preprocessing NIZKs

[KW18]

can be entirely public!

$k_P = (k, C_k, R_k)$

$k_V = C_k$

Using homomorphic commitments to construct correlation-intractable hash functions ⇒ <u>full NIZKs</u> for NP from LWE [PS19]!

$, w)$

$\mathrm{Verify}(k_V, x, \pi)$

<u>designated-prover</u> NIZK from homomorphic commitments (under LWE)

Back to Homomorphic Commitments

[GVW14]

computing on committed values:

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{R}_1 + x_1\boldsymbol{G}$$
$$\boldsymbol{C}_2 = \boldsymbol{A}\boldsymbol{R}_2 + x_2\boldsymbol{G}$$
$$\vdots$$
$$\boldsymbol{C}_n = \boldsymbol{A}\boldsymbol{R}_n + x_n\boldsymbol{G}$$

commitment:

$$\boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{R}_{f,x} + f(x)\boldsymbol{G}$$

opening:

$$\boldsymbol{R}_{f,x} = [\boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_n]\boldsymbol{H}_{f,x}$$

Requirement (for ZK): openings hides x up to what is revealed by $f(x)$ ("context-hiding")

not true as written since $\boldsymbol{R}_{f,x}$ leaks information about $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_n$

Back to Homomorphic Commitments

[GVW14]

computing on committed values:

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{R}_1 + x_1\boldsymbol{G}$$
$$\boldsymbol{C}_2 = \boldsymbol{A}\boldsymbol{R}_2 + x_2\boldsymbol{G}$$
$$\vdots$$
$$\boldsymbol{C}_n = \boldsymbol{A}\boldsymbol{R}_n + x_n\boldsymbol{G}$$

commitment:

$$\boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{R}_{f,x} + f(x)\boldsymbol{G}$$

opening:

$$\boldsymbol{R}_{f,x} = [\boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_n]\boldsymbol{H}_{f,x}$$

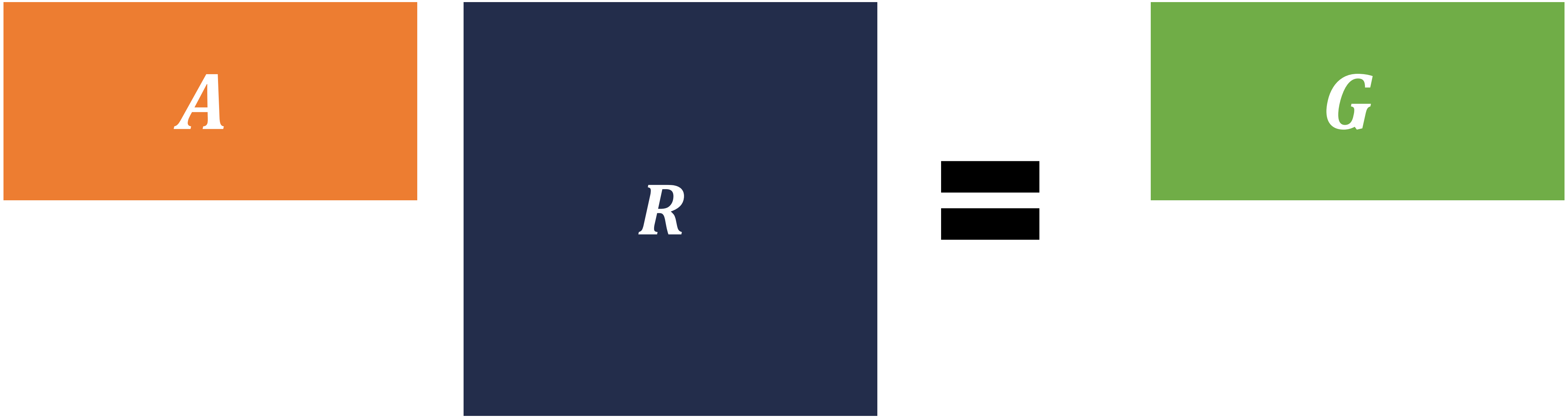
Requirement (for ZK): openings hides x up to what is revealed by $f(x)$ ("context-hiding")

Context-Hiding: public parameters $\boldsymbol{A}$, commitments $\boldsymbol{C}_1, \ldots, \boldsymbol{C}_n$ and opening $\boldsymbol{R}_{f,x}$ can be simulated given only $\big(f, f(x)\big)$

Another Ingredient: Lattice Trapdoors

[Ajt99, GPV08, AP09, CHKP10, MP12, LW15]

gadget trapdoors [MP12]



random matrix $\boldsymbol{A}$

short matrix
(trapdoor) $\boldsymbol{R}$

gadget matrix $\boldsymbol{G}$

Another Ingredient: Lattice Trapdoors

[Ajt99, GPV08, AP09, CHKP10, MP12, LW15]

gadget trapdoors [MP12]

short $\boldsymbol{R}$ such that $\boldsymbol{A}\boldsymbol{R} = \boldsymbol{G}$

enables preimage sampling for SIS:

- let $f_{\boldsymbol{A}}(\boldsymbol{x}) \coloneqq \boldsymbol{A}\boldsymbol{x}$
- given $\boldsymbol{u} = f_{\boldsymbol{A}}(\boldsymbol{x})$ and $\boldsymbol{R}$, can sample short $\boldsymbol{x}'$ where

$$f_{\boldsymbol{A}}(\boldsymbol{x}') = \boldsymbol{u}$$

and $\boldsymbol{x}'$ is Gaussian-distributed

Another Ingredient: Lattice Trapdoors

[Ajt99, GPV08, AP09, CHKP10, MP12, LW15]

suppose $\boldsymbol{A} = [\boldsymbol{A}_1 | \boldsymbol{A}_2]$

two possible trapdoors:

- if $\boldsymbol{R}_1$ is trapdoor for $\boldsymbol{A}_1$, then $\boldsymbol{A}_1 \boldsymbol{R}_1 = \boldsymbol{G}$ and

$$[\boldsymbol{A}_1 | \boldsymbol{A}_2] \cdot \begin{bmatrix} \boldsymbol{R}_1 \\ \boldsymbol{0} \end{bmatrix} = \boldsymbol{G}$$

simulation

- if $\boldsymbol{A}_2 = \boldsymbol{A}_1 \boldsymbol{R}_2 \pm \boldsymbol{G}$ for short $\boldsymbol{R}_2$, then

$$[\boldsymbol{A}_1 | \boldsymbol{A}_2] \cdot \begin{bmatrix} \mp \boldsymbol{R}_2 \\ \boldsymbol{I} \end{bmatrix} = \boldsymbol{G}$$

real

two statistically-indistinguishable ways to sample $f_{\boldsymbol{A}}^{-1}(\boldsymbol{u})$

Context-Hiding for Commitments

[GVW14]

computing on committed values:

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{R}_1 + x_1\boldsymbol{G}$$

$$\boldsymbol{C}_2 = \boldsymbol{A}\boldsymbol{R}_2 + x_2\boldsymbol{G}$$

$$\vdots$$

$$\boldsymbol{C}_n = \boldsymbol{A}\boldsymbol{R}_n + x_n\boldsymbol{G}$$

$\Rightarrow$

commitment:

$$\boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{R}_{f,x} + f(x)\boldsymbol{G}$$

opening:

$$\boldsymbol{R}_{f,x} = [\boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_n]\boldsymbol{H}_{f,x}$$

Context-Hiding: public parameters $\boldsymbol{A}$, commitments $\boldsymbol{C}_1, \ldots, \boldsymbol{C}_n$ and opening $\boldsymbol{R}_{f,x}$ can be simulated given only $\big(f, f(x)\big)$

Context-Hiding for Commitments

[GVW14]

for simplicity: only support openings to $f(x) = 1$

suffices for zero-knowledge
(can consider $f, \bar{f}$ more generally)

commitment:

$$\boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{R}_{f,x} + f(x)\boldsymbol{G}$$

opening:

$$\boldsymbol{R}_{f,x} = [\boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_n]\boldsymbol{H}_{f,x}$$

Context-Hiding: public parameters $\boldsymbol{A}$, commitments $\boldsymbol{C}_1, \dots, \boldsymbol{C}_n$ and opening $\boldsymbol{R}_{f,x}$ can be simulated given only $\big(f, f(x)\big)$

Context-Hiding for Commitments

[GVW14]

for simplicity: only support openings to $f(x) = 1$

opening can be used to obtain trapdoor for

$$[\boldsymbol{A} \mid \boldsymbol{C}_f] = [\boldsymbol{A} \mid \boldsymbol{A}\boldsymbol{R}_{f,x} + \boldsymbol{G}]$$

if simulator chooses $\boldsymbol{A}$, can choose $\boldsymbol{A}$ with trapdoor

if commitments are well-formed, committer also has trapdoor

commitment:

$$\boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{R}_{f,x} + f(x)\boldsymbol{G}$$

opening:

$$\boldsymbol{R}_{f,x} = [\boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_n]\boldsymbol{H}_{f,x}$$

Context-Hiding: public parameters $\boldsymbol{A}$, commitments $\boldsymbol{C}_1, \ldots, \boldsymbol{C}_n$ and opening $\boldsymbol{R}_{f,x}$ can be simulated given only $\big(f, f(x)\big)$

Context-Hiding for Commitments

[GVW14]

for simplicity: only support openings to $f(x) = 1$

opening can be used to obtain trapdoor for

$$[\boldsymbol{A} \mid \boldsymbol{C}_f] = [\boldsymbol{A} \mid \boldsymbol{A}\boldsymbol{R}_{f,x} + \boldsymbol{G}]$$

idea: include random target vector $\boldsymbol{u}$ in public parameters

opening: short vector $\boldsymbol{v}$ such that

$$[\boldsymbol{A} \mid \boldsymbol{C}_f]\boldsymbol{v} = \boldsymbol{u}$$

commitment:

$$\boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{R}_{f,x} + f(x)\boldsymbol{G}$$

opening:

$$\boldsymbol{R}_{f,x} = [\boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_n]\boldsymbol{H}_{f,x}$$

Context-Hiding: public parameters $\boldsymbol{A}$, commitments $\boldsymbol{C}_1, \dots, \boldsymbol{C}_n$ and opening $\boldsymbol{R}_{f,x}$ can be simulated given only $\big(f, f(x)\big)$

Context-Hiding for Commitments

[GVW14]

real scheme:

public parameters:

- LWE matrix $\boldsymbol{A}$
- sample random $\boldsymbol{u}$

commitments:

- $\boldsymbol{C}_i \leftarrow \boldsymbol{A}\boldsymbol{R}_i + x_i\boldsymbol{G}$

opening:

- compute $\boldsymbol{C}_f$ from $\boldsymbol{C}_1, \dots, \boldsymbol{C}_n$
- sample short $\boldsymbol{v}$ such that
$$[\boldsymbol{A} \mid \boldsymbol{C}_f]\boldsymbol{v} = \boldsymbol{u}$$
using $\boldsymbol{R}_{f,x} \leftarrow [\boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_n]\boldsymbol{H}_{f,x}$

to simulate:

public parameters:

- sample $\boldsymbol{A}$ with trapdoor $\boldsymbol{R}$
- sample random $\boldsymbol{u}$

LWE

commitments:

- sample random matrices $\boldsymbol{C}_i$

LHL

opening:

- compute $\boldsymbol{C}_f$ from $\boldsymbol{C}_1, \dots, \boldsymbol{C}_n$
- sample short $\boldsymbol{v}$ such that
$$[\boldsymbol{A} \mid \boldsymbol{C}_f]\boldsymbol{v} = \boldsymbol{u}$$
using $\boldsymbol{R}$

sampling

Context-Hiding: public parameters $\boldsymbol{A}$, commitments $\boldsymbol{C}_1, \dots, \boldsymbol{C}_n$ and opening $\boldsymbol{R}_{f,x}$ can be simulated given only $\big(f, f(x)\big)$

Dual-Mode Homomorphic Commitments

[GVW14]

public parameters $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ (LWE matrix)

$$\boldsymbol{C} = \boldsymbol{A}\boldsymbol{R} + x\boldsymbol{G}$$

commitment

opening
(check $\boldsymbol{R}$ short)

message

statistically binding: correctness of GSW (in fact, extractable)

computationally hiding: security of GSW (under LWE)

Dual-Mode Homomorphic Commitments

[GVW14]

public parameters $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ (uniformly random)

$$\boldsymbol{C} = \boldsymbol{A}\boldsymbol{R} + x\boldsymbol{G}$$

commitment

opening
(check $\boldsymbol{R}$ short)

message

statistically hiding: leftover hash lemma (in fact, equivocable)

computational binding: switch $\boldsymbol{A}$ to LWE matrix

Homomorphic Signatures

[GVW14]

public parameters $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ (uniformly random)

$$\boldsymbol{C} = \boldsymbol{A}\boldsymbol{R} + x\boldsymbol{G}$$

public parameters

signature
(check $\boldsymbol{R}$ short)

message

equivocation ⇒ signature

Homomorphic Signatures

[GVW14]

public parameters $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ (uniformly random)

$$\boldsymbol{C} = \boldsymbol{A}\boldsymbol{R} + x\boldsymbol{G}$$

public parameters

signature
(check $\boldsymbol{R}$ short)

message

verification key: random $\boldsymbol{A}, \boldsymbol{C}_1, \dots, \boldsymbol{C}_n$

signing key: trapdoor for $\boldsymbol{A}$

Homomorphic Signatures

[GVW14]

vk: $\boldsymbol{A}, \boldsymbol{C}_1, \ldots, \boldsymbol{C}_n \in \mathbb{Z}_q^{n \times m}$
sk: trapdoor for $\boldsymbol{A}$

signature on $x \in \{0,1\}^n$:

$\quad$ short $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_n \in \mathbb{Z}_q^{n \times m}$

$\quad$ where $\boldsymbol{C}_i = \boldsymbol{A}\boldsymbol{R}_i + x_i \boldsymbol{G}$

compute f on signatures:

$$\boldsymbol{R}_{f,x} = [\boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_n] \boldsymbol{H}_{f,x}$$

verify signature $\boldsymbol{R}$ on $\left(f, f(x)\right)$

$$\boldsymbol{C}_1, \ldots, \boldsymbol{C}_n, f \mapsto \boldsymbol{C}_f$$

check $\boldsymbol{A}\boldsymbol{R} + f(x)\boldsymbol{G} = \boldsymbol{C}_f$

unforgeability follows from binding property of the commitment scheme

Summary

GSW ciphertexts:

$$\boldsymbol{C}_i = \boldsymbol{A}\boldsymbol{R}_i + x_i \boldsymbol{G}$$

"input-independent" evaluation (given $\boldsymbol{C}_1, \dots, \boldsymbol{C}_n, f$):

$$\boldsymbol{C}_1, \dots, \boldsymbol{C}_n \mapsto \boldsymbol{C}_f$$

"input-dependent" evaluation (given $\boldsymbol{C}_1, \dots, \boldsymbol{C}_n, f, x$):

$$[\boldsymbol{C}_1 - x_1 \boldsymbol{G} \mid \cdots \mid \boldsymbol{C}_n - x_n \boldsymbol{G}]\boldsymbol{H}_{f,x} = \boldsymbol{C}_f - f(x)\boldsymbol{G}$$

$\boldsymbol{A}$ is LWE matrix ⇒ extractable commitments

$\boldsymbol{A}$ is uniform ⇒ equivocable commitments (homomorphic signatures)

homomorphic commitments/signatures ⇒ designated-prover NIZKs

Open Questions

NIZK proof of well-formedness of GSW ciphertexts?

<u>Fully</u> homomorphic commitments/signatures from lattices?

$$\boldsymbol{R}_{f,x} = [\boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_n]\boldsymbol{H}_{f,x}$$

$\left\|H_{f,x}\right\|$ scales with <u>exponentially</u> in the depth d of the function f, so modulus $q > 2^{O(d)}$

Open Questions

NIZK proof of well-formedness of GSW ciphertexts?

Fully homomorphic commitments/signatures from lattices?

$$\boldsymbol{R}_{f,x} = [\boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_n]\boldsymbol{H}_{f,x}$$

Short public parameters without random oracles?

Thank you!