(Post-Quantum) Pseudorandom Correlation Functions for Oblivious Transfer

A Constrained-PRF Approach

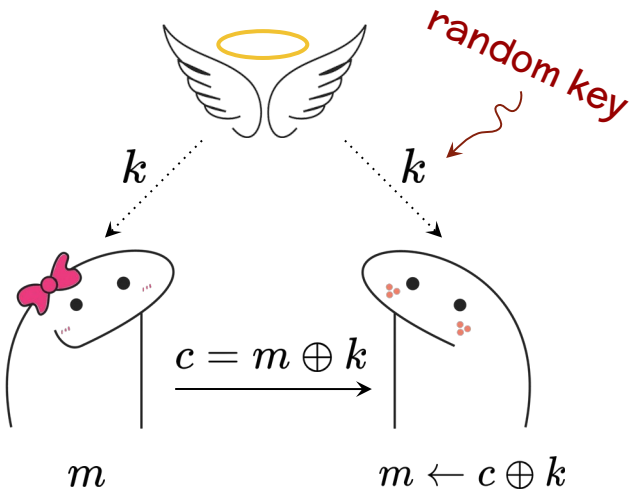
Mahshid Riahinia
IRIF, CNRS

Based on collaborations with

Shweta Agrawal (IIT Madras), Kaartik Bhushan(IRIF), Geoffroy Couteau(IRIF), Pouria Fallahpour (LIP6), and Arthur Herlédan Le Merdy (COSIC)

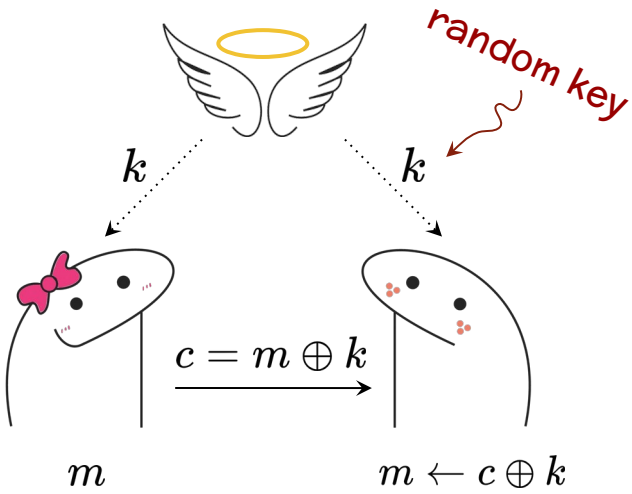
Introduction: Correlated Randomness

Introduction: Correlated Randomness



Symmetric Encryption

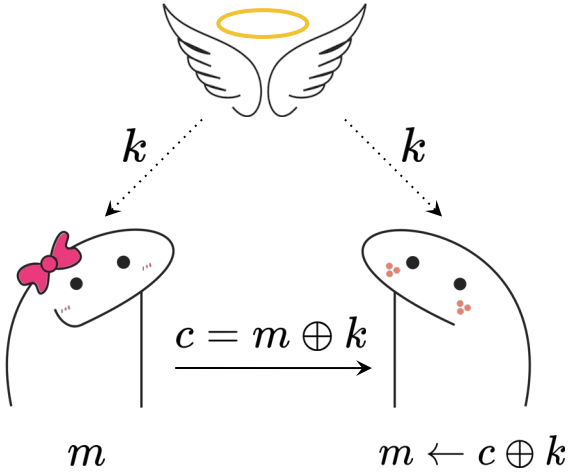
Introduction: Correlated Randomness



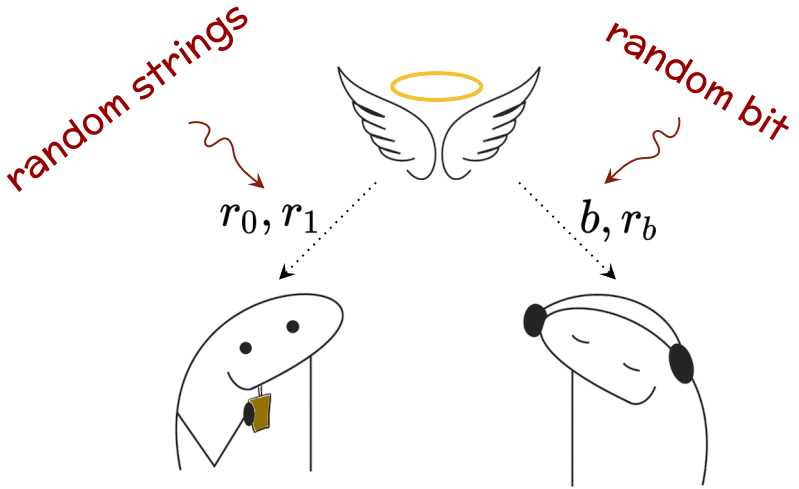
Symmetric Encryption

Secure Communication

Introduction: Correlated Randomness



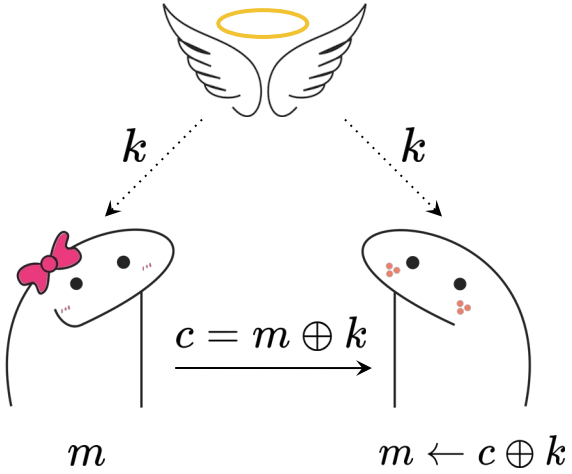
Symmetric Encryption



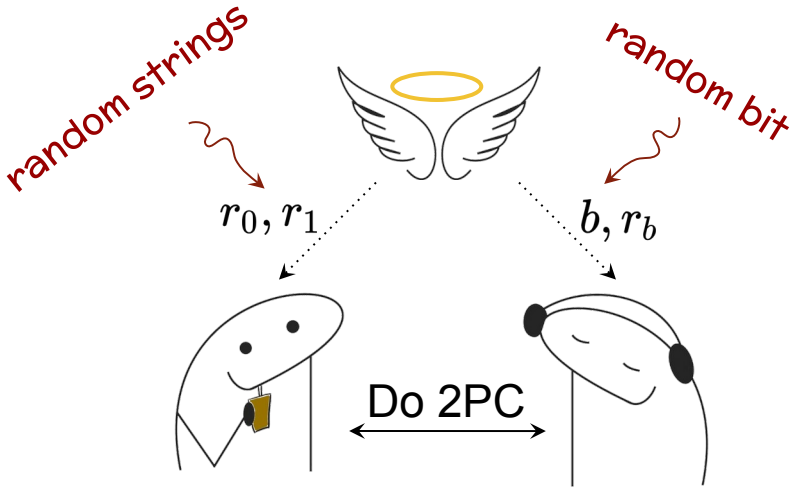
Oblivious Transfer (OT) Correlation

Secure Communication

Introduction: Correlated Randomness



Symmetric Encryption



Oblivious Transfer (OT) Correlation

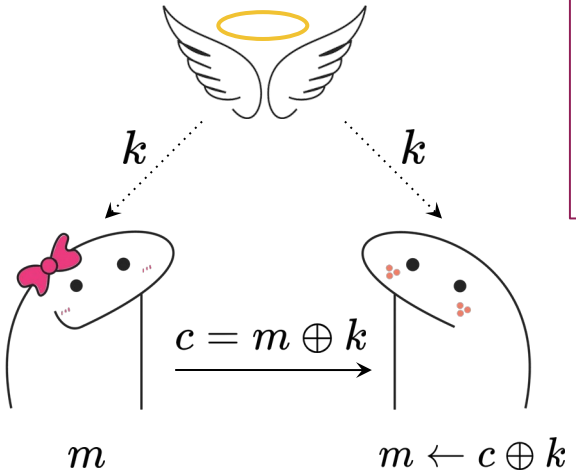
Secure Communication

2PC: 2-Party Computation

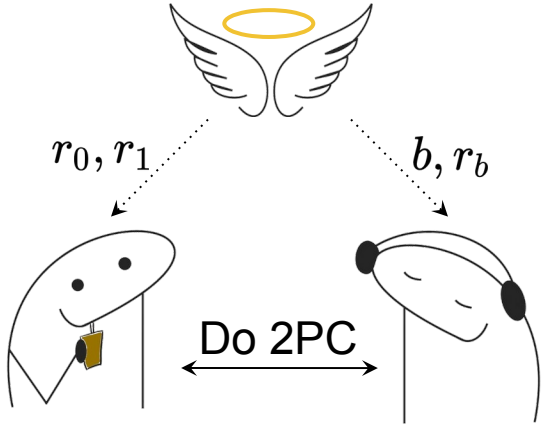
Introduction: Correlated Randomness

Secure Computation

- party 1 has x
- party 2 has y
- Goal: compute f(x,y) without revealing x,y



Symmetric Encryption

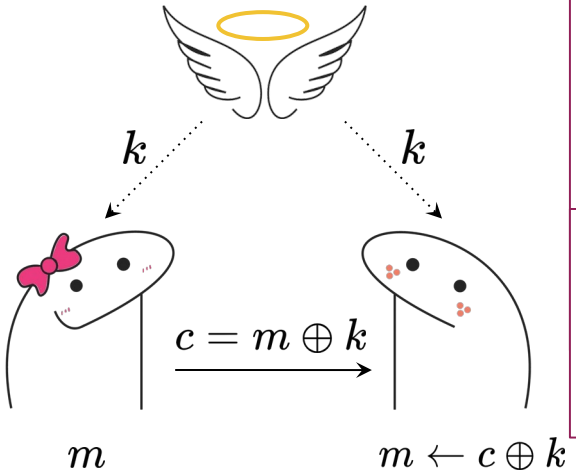


Oblivious Transfer (OT) Correlation

Secure Communication

2PC: 2-Party Computation

Introduction: Correlated Randomness



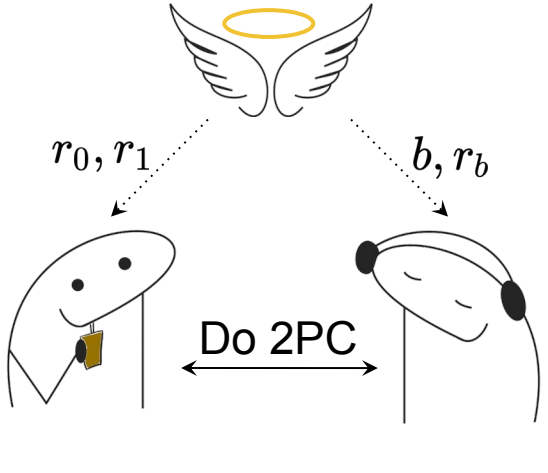
Symmetric Encryption

Secure Computation

- party 1 has x
- party 2 has y
- Goal: compute f(x,y) without revealing x,y

example

Personalized Advertising
- User: interests
- Ad platform: predictor
- Goal: find interesting Ads



Oblivious Transfer (OT) Correlation

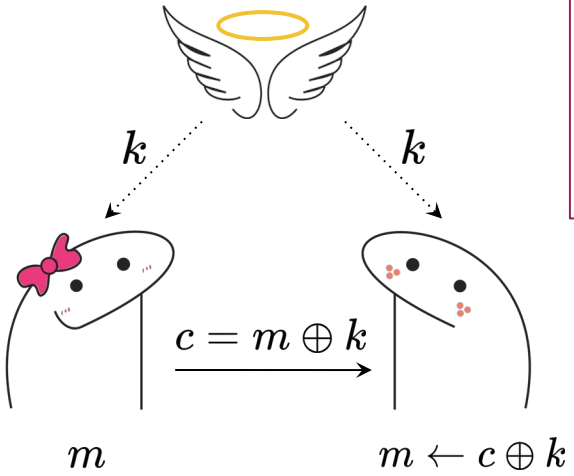
Secure Communication

2PC: 2-Party Computation

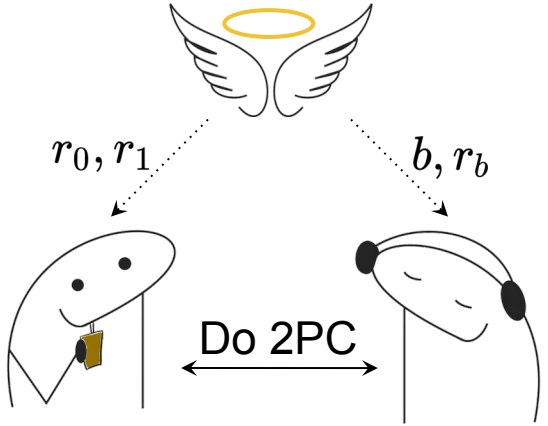
Introduction: Correlated Randomness

Secure Computation

- party 1 has x
- party 2 has y
- Goal: compute f(x,y) without revealing x,y



Symmetric Encryption



Oblivious Transfer (OT) Correlation

Secure Communication

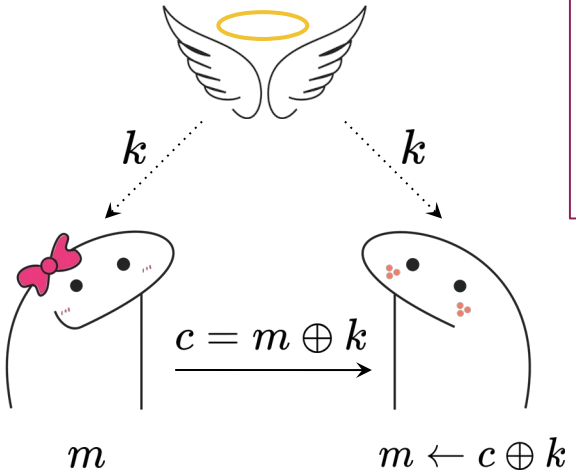
Secure Computation

2PC: 2-Party Computation

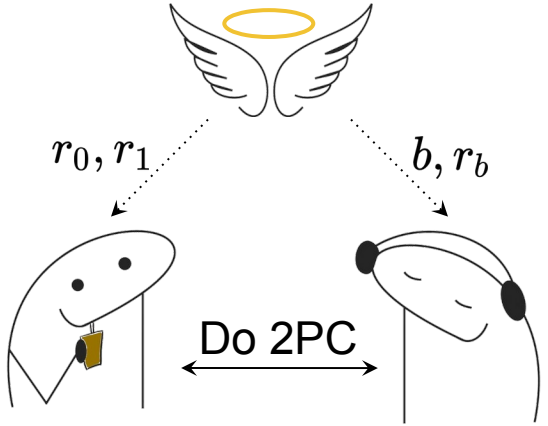
Introduction: Correlated Randomness

Secure Computation

- party 1 has x
- party 2 has y
- Goal: compute f(x,y) without revealing x,y



Symmetric Encryption



Oblivious Transfer (OT) Correlation

Fast & Info-Theoretic

Secure Communication

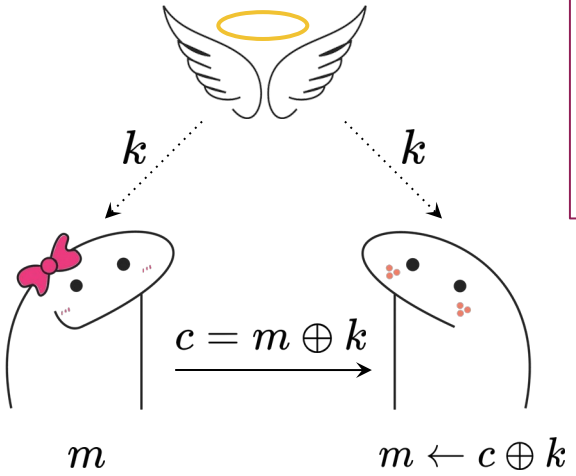
Secure Computation

2PC: 2-Party Computation

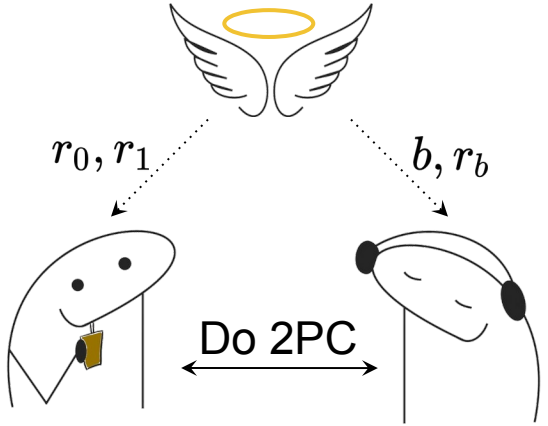
Introduction: Correlated Randomness

Secure Computation

- party 1 has x
- party 2 has y
- Goal: compute f(x,y) without revealing x,y



Symmetric Encryption



Oblivious Transfer (OT) Correlation

Fast & Info-Theoretic

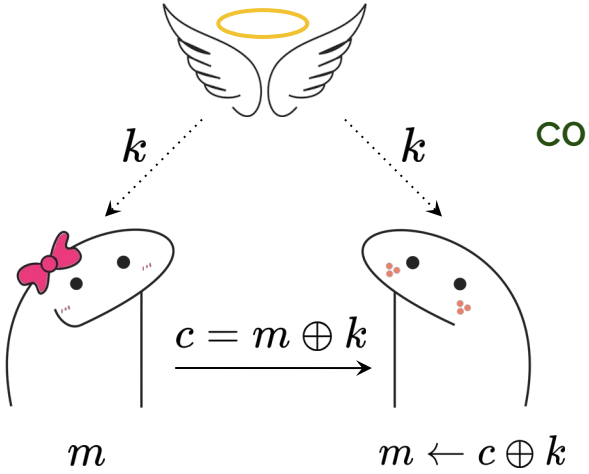
Secure Communication

2PC: 2-Party Computation

Secure Computation

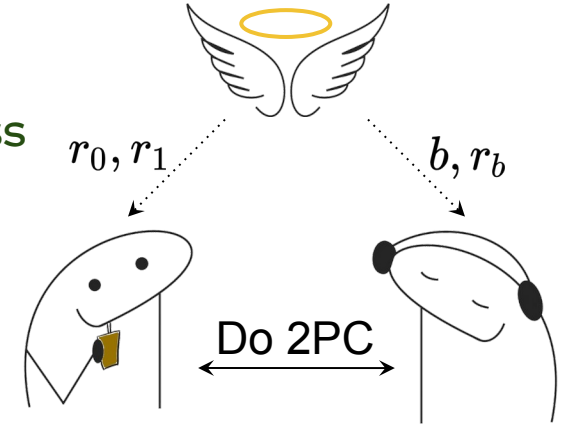
f has n gates : O(n) OT pairs -> send 4 bits per AND

Introduction: Correlated Randomness



Symmetric Encryption

Can we generate correlated randomness on demand?



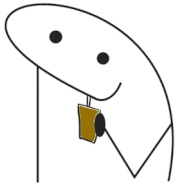
Oblivious Transfer (OT) Correlation

Pseudorandom Correlation Functions

Pseudorandom Correlation Functions [BCGIKS20]

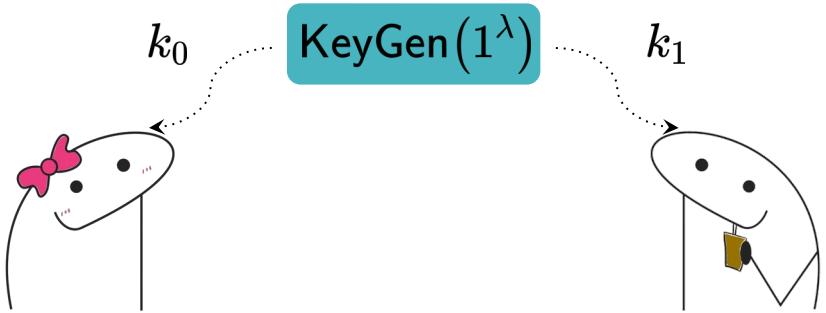
on-demand generation
of
correlated randomness





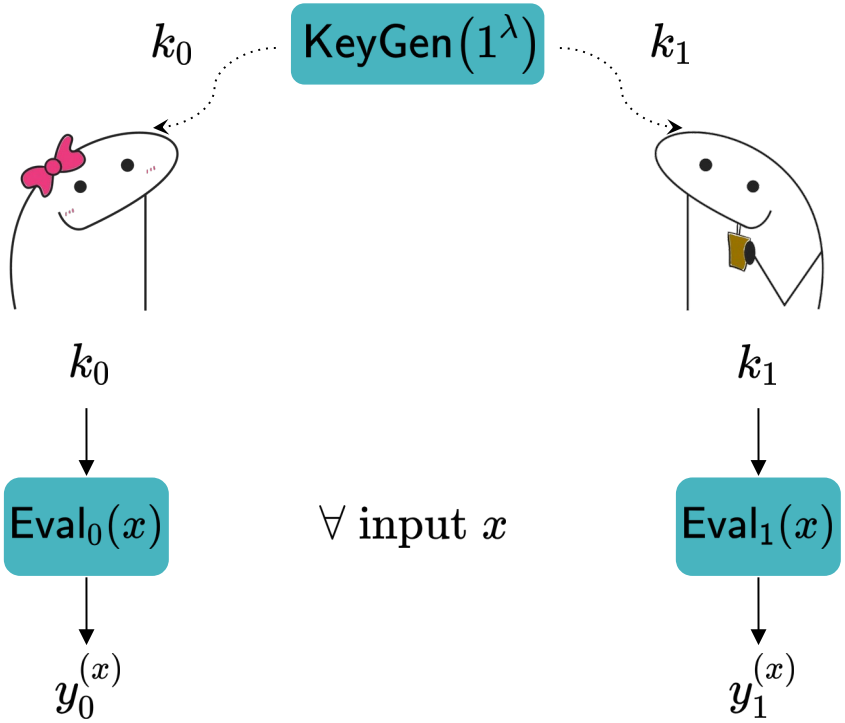
Pseudorandom Correlation Functions [BCGIKS20]

on-demand generation
of
correlated randomness



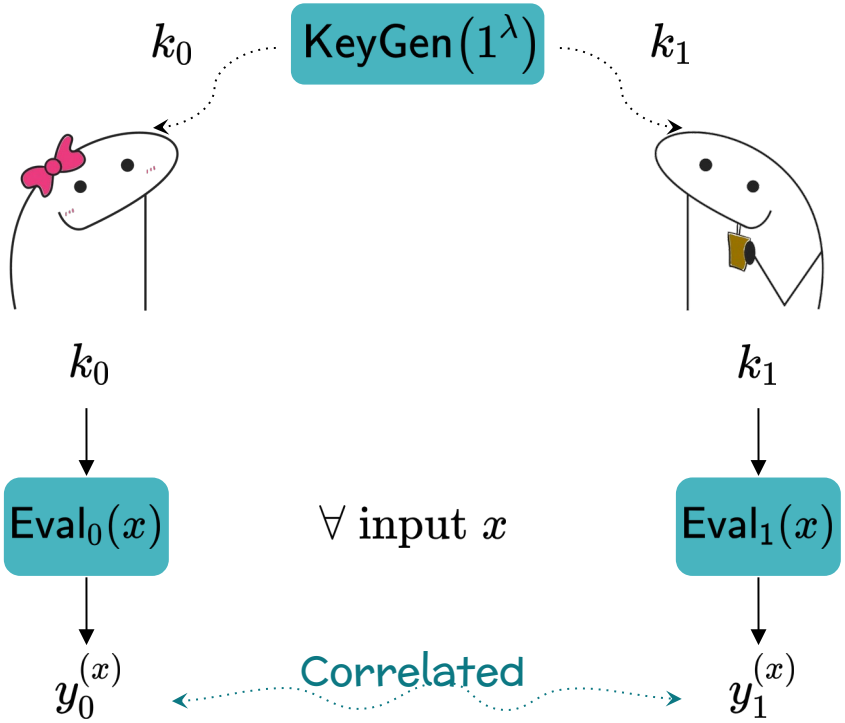
Pseudorandom Correlation Functions [BCGIKS20]

on-demand generation
of
correlated randomness



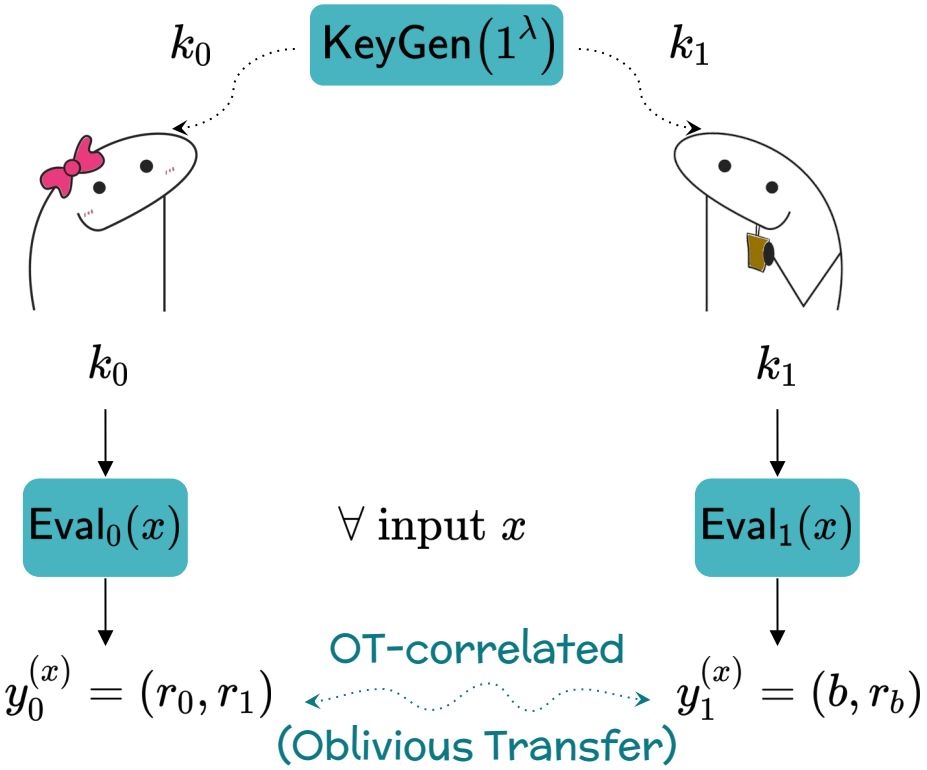
Pseudorandom Correlation Functions [BCGIKS20]

on-demand generation
of
correlated randomness



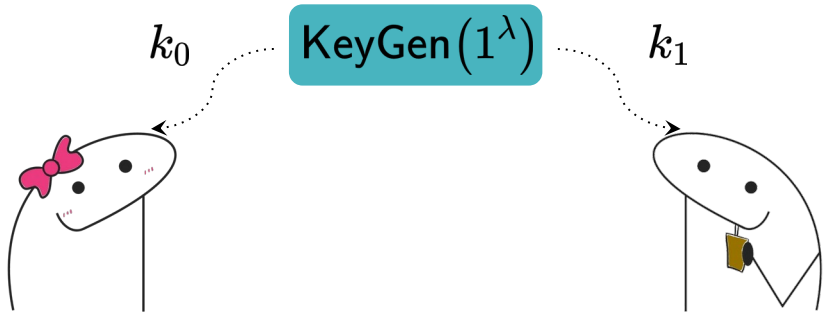
Pseudorandom Correlation Functions [BCGIKS20]

on-demand generation
of
correlated randomness



Pseudorandom Correlation Functions [BCGIKS20]

on-demand generation
of
correlated randomness



k_0 k_1

Eval$_0(x)$ $\forall$ input x Eval$_1(x)$

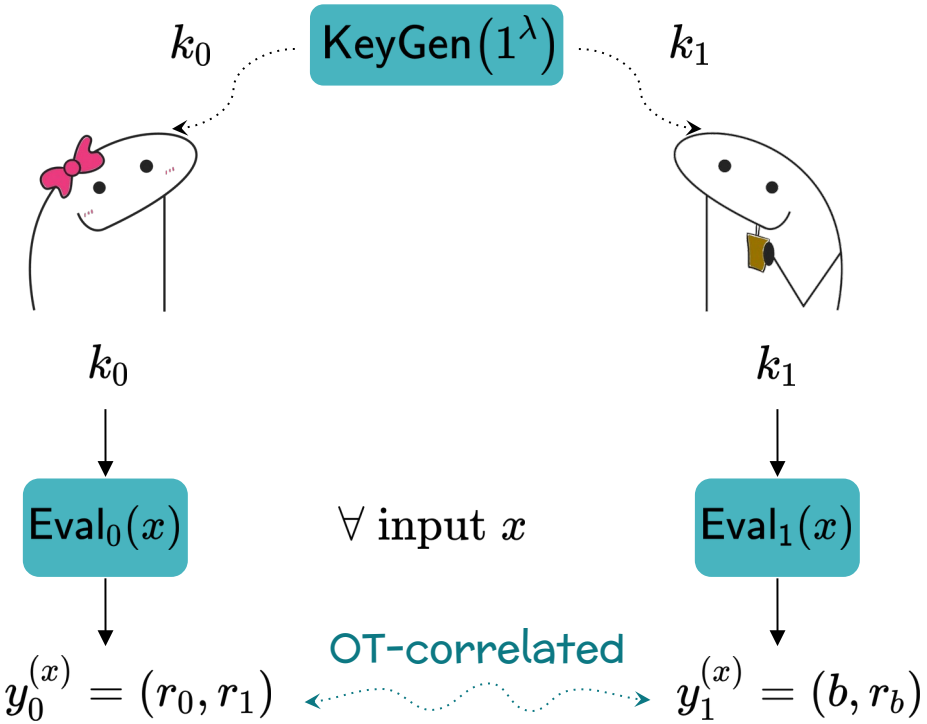
random strings $y_0^{(x)} = (r_0, r_1)$ OT-correlated $y_1^{(x)} = (b, r_b)$ random bit

(Oblivious Transfer)

Pseudorandom Correlation Functions [BCGIKS20]

security:

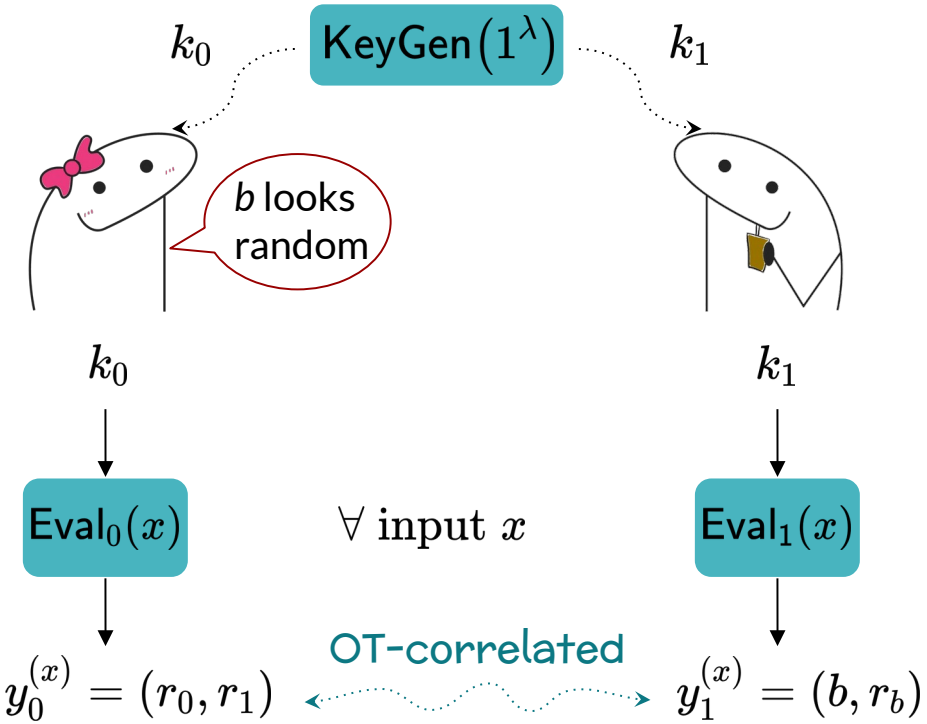
things look random up to correlation



Pseudorandom Correlation Functions [BCGIKS20]

security:

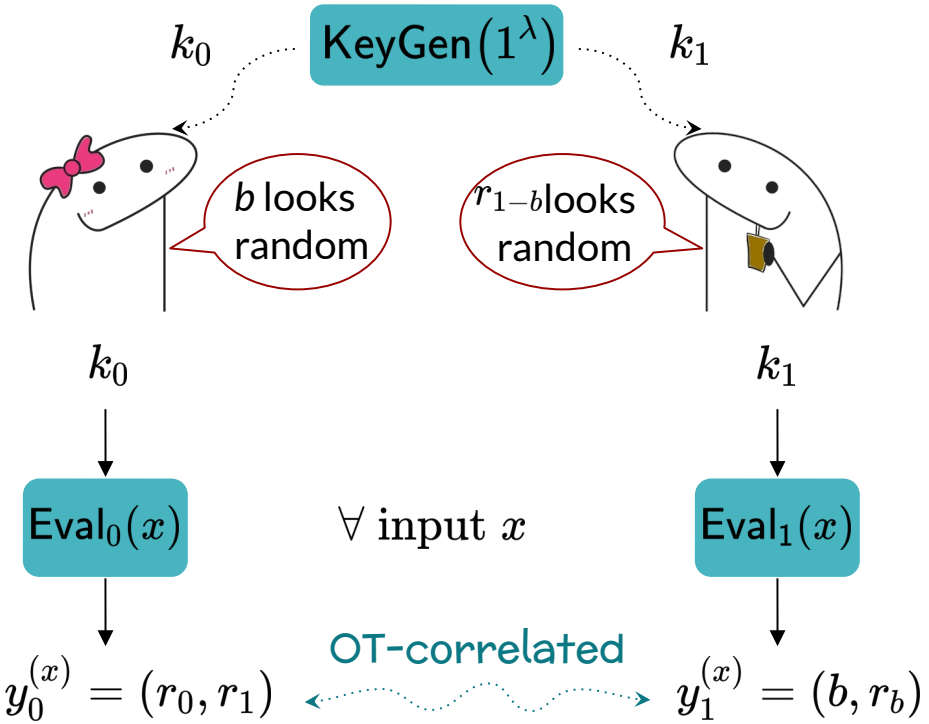
things look random up to correlation



Pseudorandom Correlation Functions [BCGIKS20]

security:

things look random up to correlation

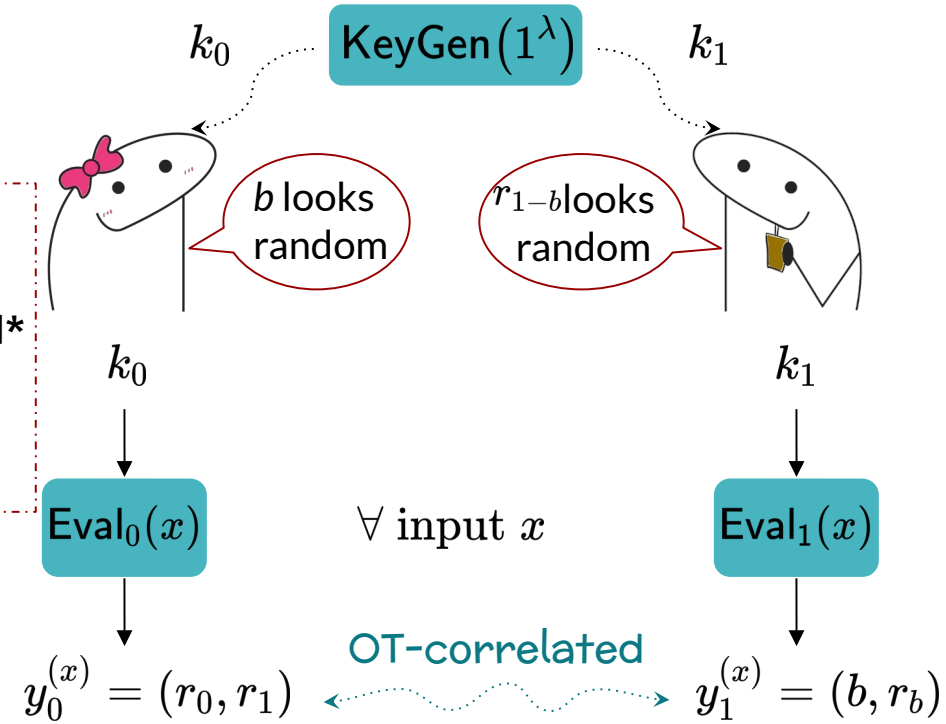


Pseudorandom Correlation Functions [BCGIKS20]

Our contribution:

Efficient* & Compressed*
Post-Quantum PCFs
for
OT Correlations

* Efficiency ~ #OT per second
* Compressed ~ |k_0|, |k_1|

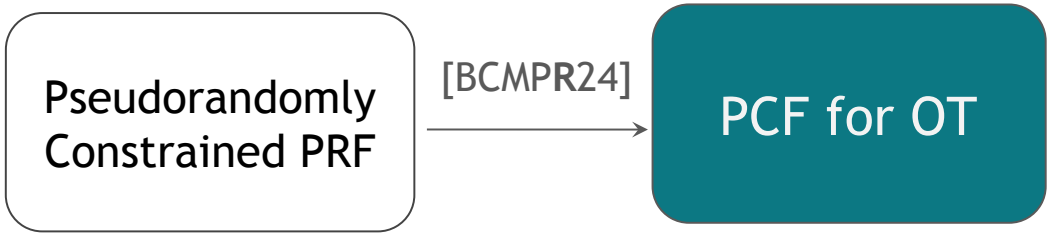


Road Map

Road Map

PCF for OT

Road Map



PRF: Pseudorandom Function

Road Map

[ABCR26]



Secret-Power Ring Learning with Errors

[FHR26]



Parallelization Problem with Auxiliary Inputs

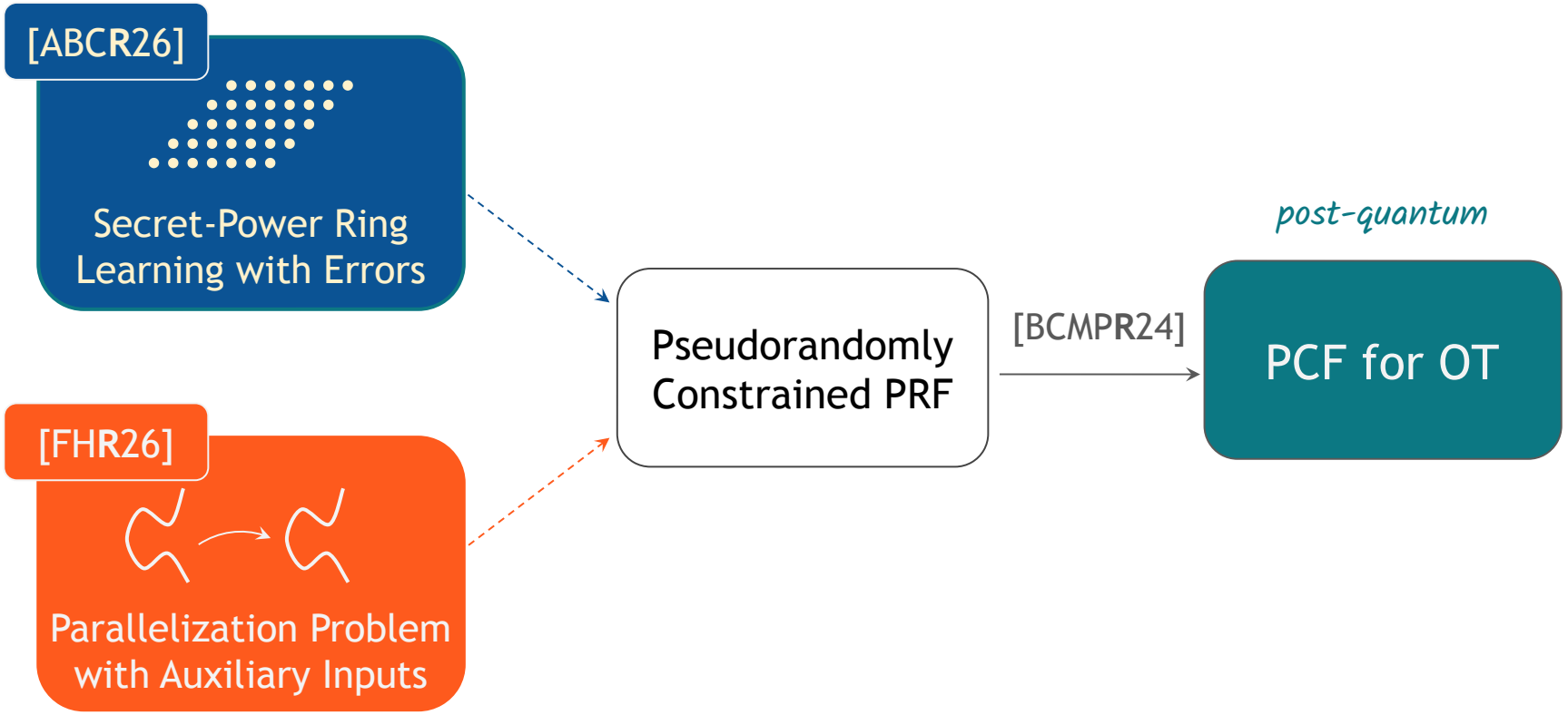
Pseudorandomly Constrained PRF

[BCMPR24]

PCF for OT

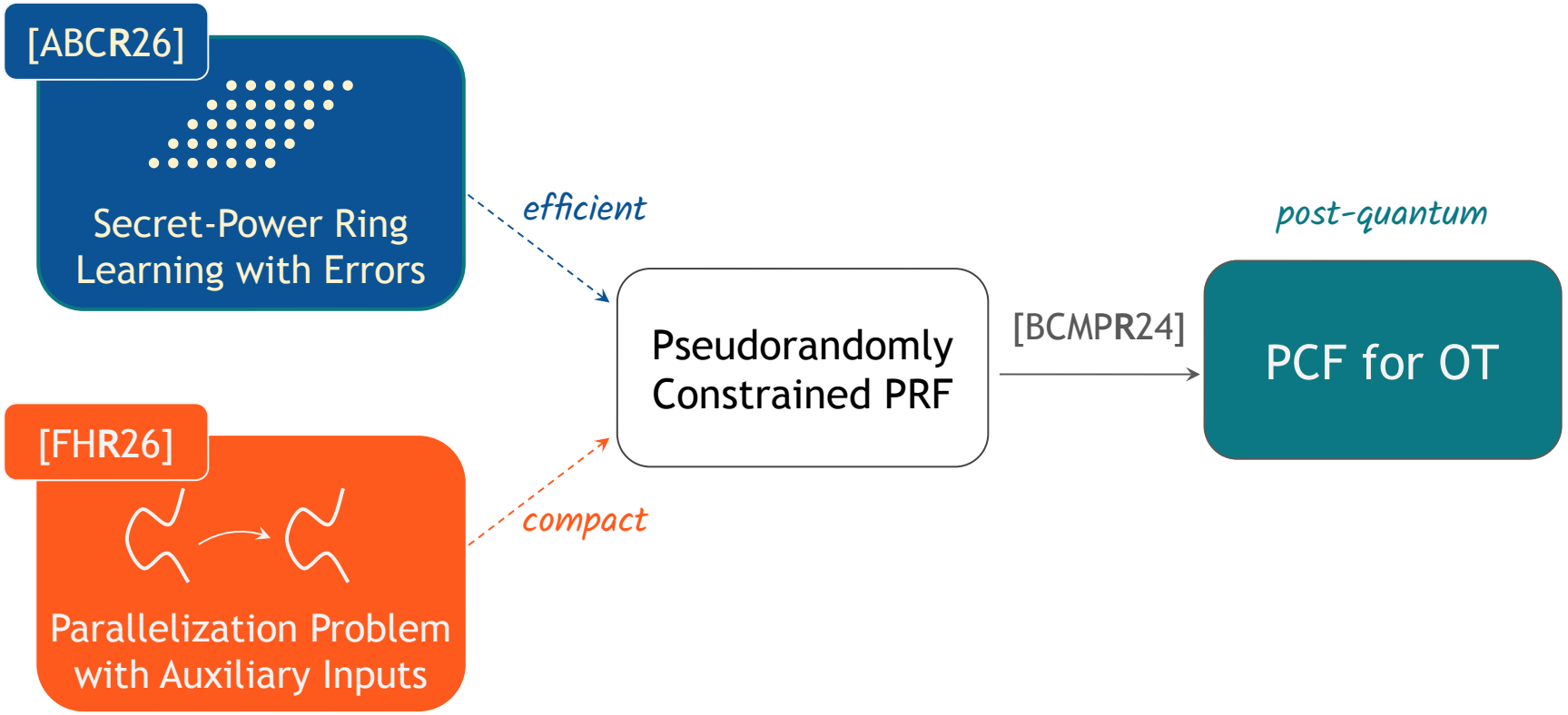
PRF: Pseudorandom Function

Road Map



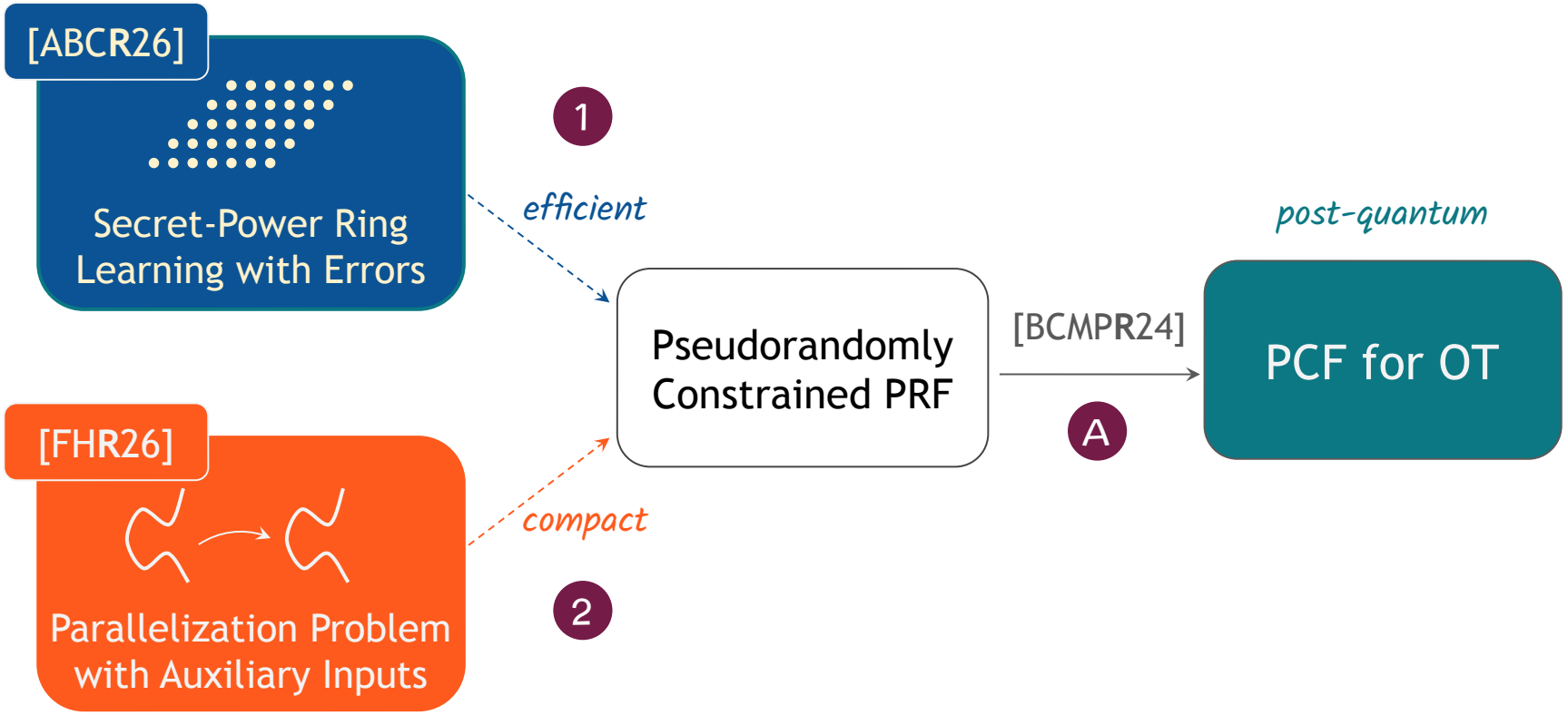
PRF: Pseudorandom Function

Road Map



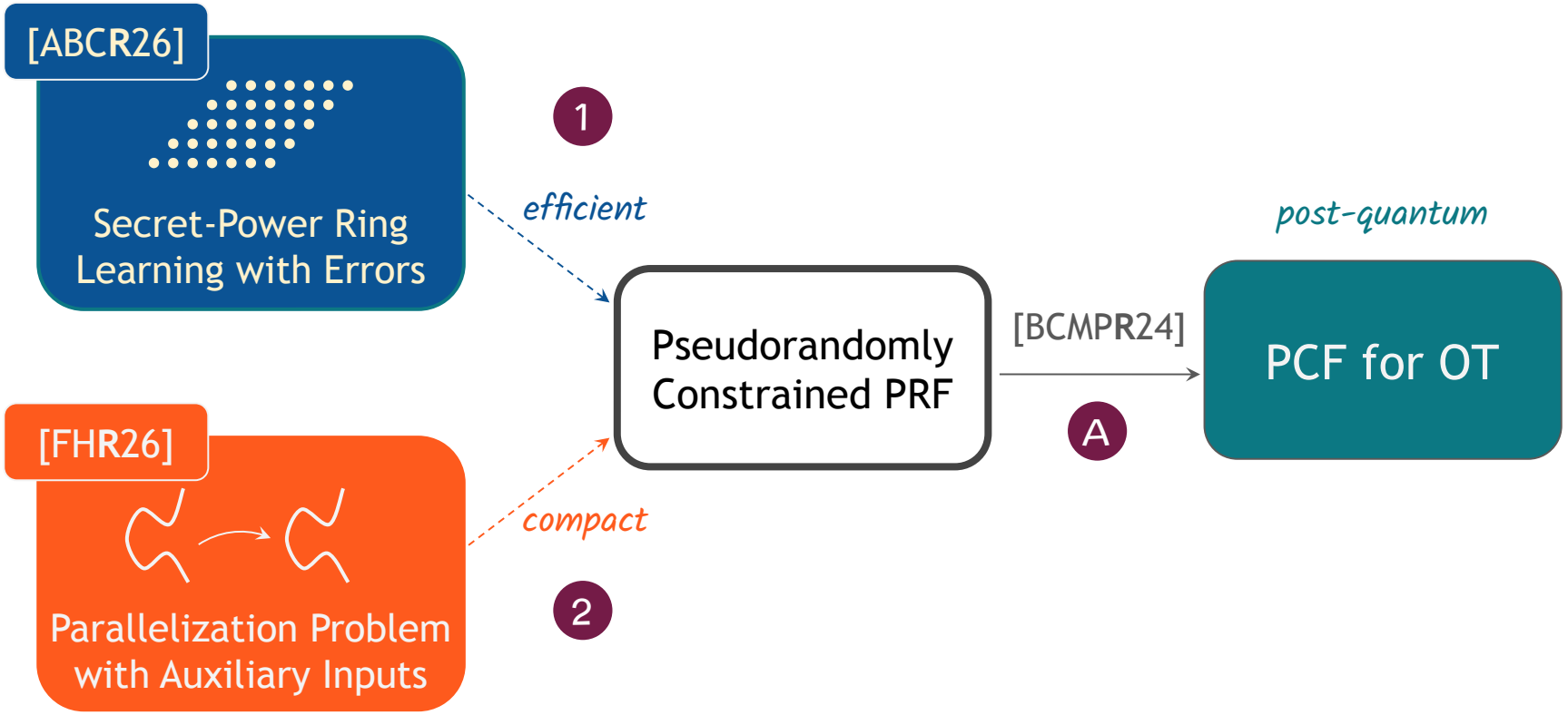
PRF: Pseudorandom Function

Road Map



PRF: Pseudorandom Function

Road Map



PRF: Pseudorandom Function

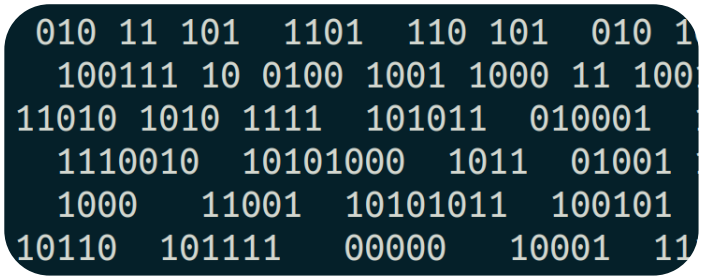
Pseudorandom Functions

Pseudorandom Functions (PRFs) [GGM86]

Definition. Deterministic keyed functions indistinguishable from truly random functions.

$F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$

Set of outputs with msk



Compute using **msk** $\xleftarrow{\$} \mathcal{K}$

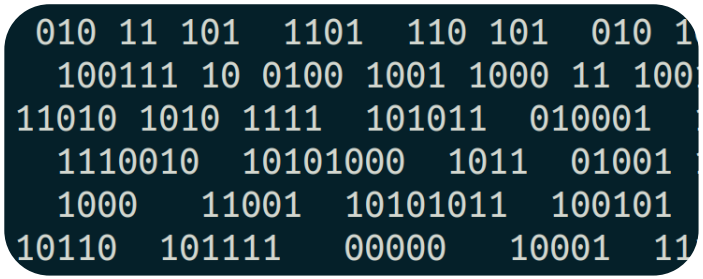


Pseudorandom Functions (PRFs) [GGM86]

Definition. Deterministic keyed functions indistinguishable from truly random functions.

$F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$

Set of outputs with msk



Compute using **msk** $\xleftarrow{\$} \mathcal{K}$



Set of outputs without msk

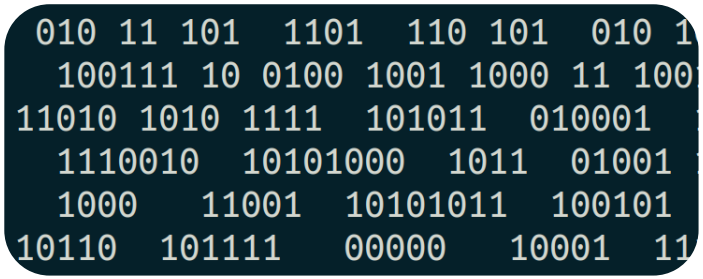


Pseudorandom Functions (PRFs) [GGM86]

Definition. Deterministic keyed functions indistinguishable from truly random functions.

$F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$

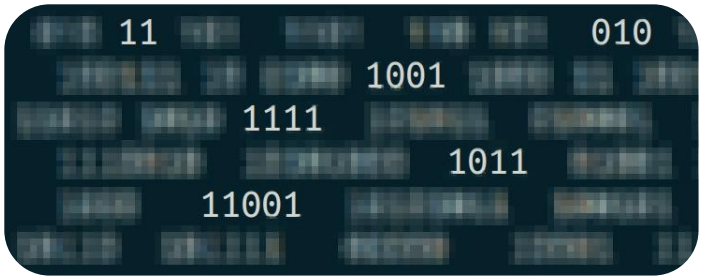
Set of outputs with msk



Compute using msk $\xleftarrow{\$} \mathcal{K}$



Set of outputs without msk



with oracle queries on arbitrary / random inputs

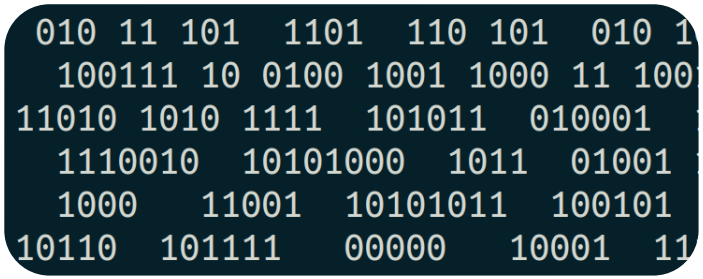
PRF weak PRF

Constrained Pseudorandom Functions

Constrained Pseudorandom Functions (**CPRFs**)

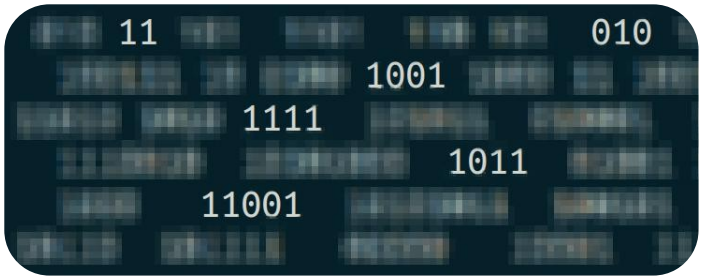
Pseudorandom Functions *with constrained access to the evaluation.*

Set of outputs **with** msk



Compute using **msk** $\xleftarrow{\$} \mathcal{K}$

Set of outputs **without** msk

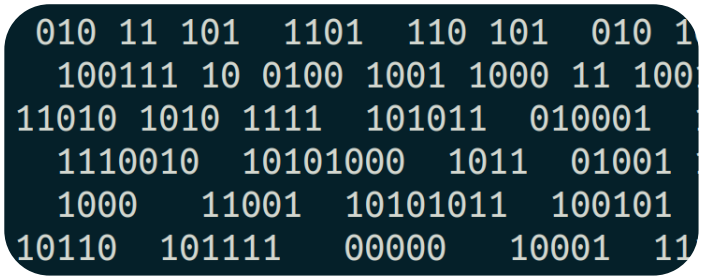


with oracle queries on arbitrary / random inputs

Constrained Pseudorandom Functions (CPRFs)

Pseudorandom Functions *with constrained access to the evaluation.*

Set of outputs **with** msk

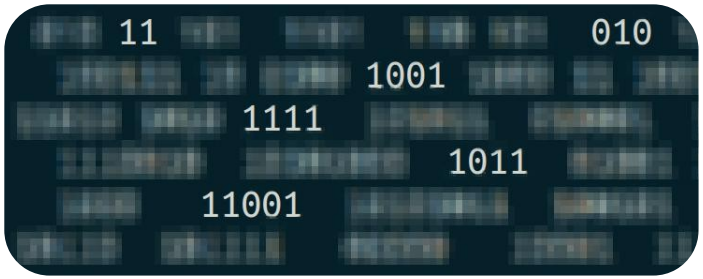


Compute using **msk** $\xleftarrow{\$} \mathcal{K}$

ck

For a subset
$S \subset \mathcal{X}$

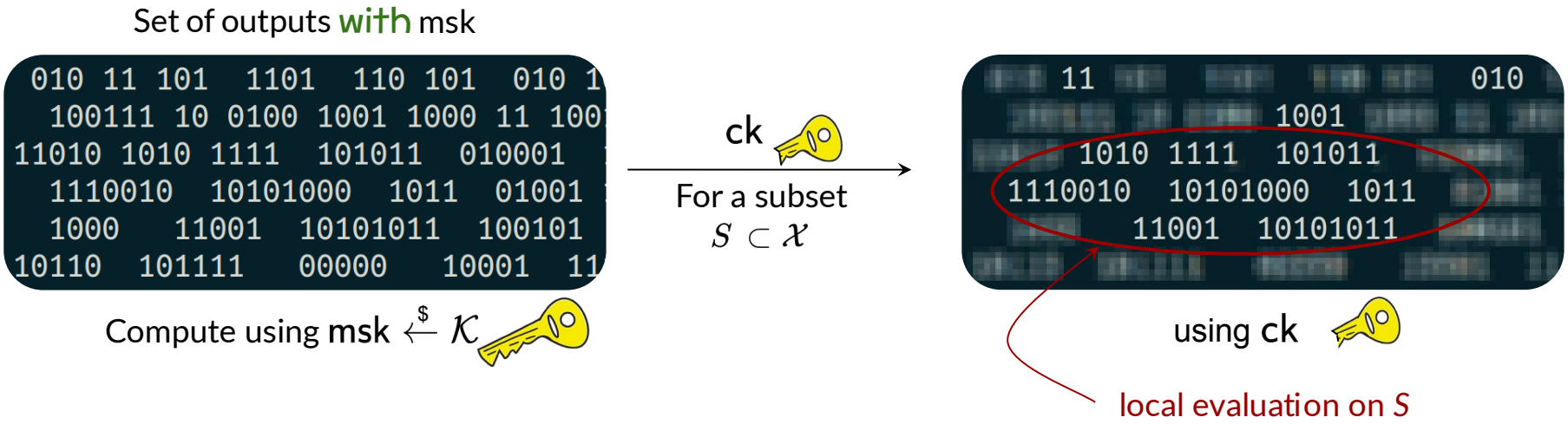
Set of outputs **without** msk



with oracle queries on arbitrary / random inputs

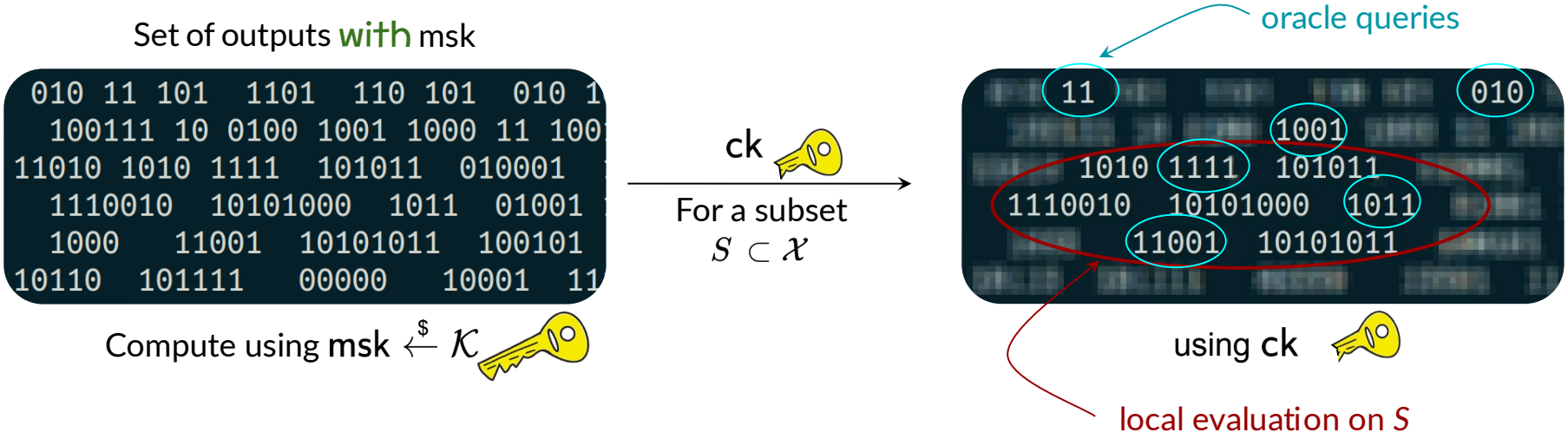
Constrained Pseudorandom Functions (CPRFs)

Pseudorandom Functions *with constrained access to the evaluation.*



Constrained Pseudorandom Functions (CPRFs)

Pseudorandom Functions *with constrained access to the evaluation.*

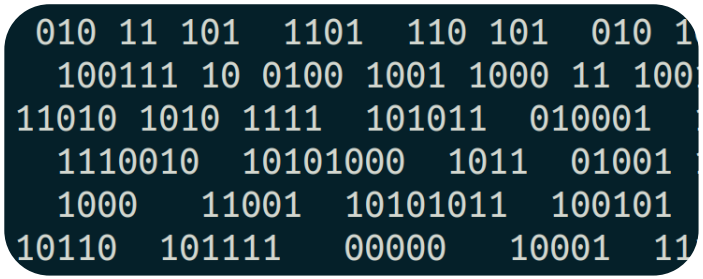


Constrained Pseudorandom Functions (CPRFs)

Pseudorandom Functions *with constrained access to the evaluation.*

ck_S "=" msk ***only*** for all $x \in S$

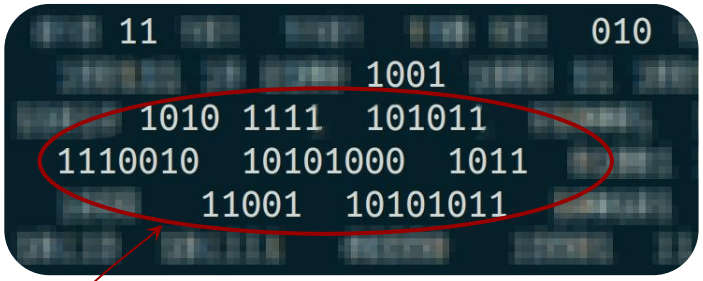
Set of outputs with msk



Compute using **msk** $\xleftarrow{\$} \mathcal{K}$

ck

For a subset
$S \subset \mathcal{X}$



using **ck**

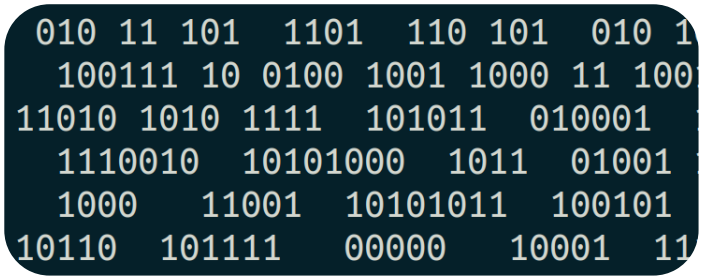
local evaluation on S

Constrained Pseudorandom Functions (CPRFs)

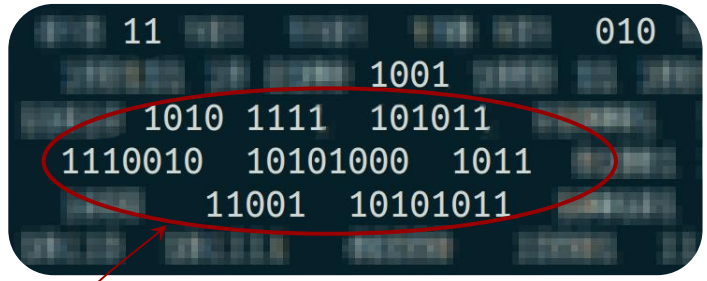
Pseudorandom Functions *with constrained access to the evaluation.*

- Every predicate $F : \mathcal{X} \to \{0,1\}$ defines a subset $S_F = \{x \in \mathcal{X} : F(x) = 0\}$

Set of outputs with msk



Compute using msk $\xleftarrow{\$} \mathcal{K}$



using ck_F

local evaluation on S_F

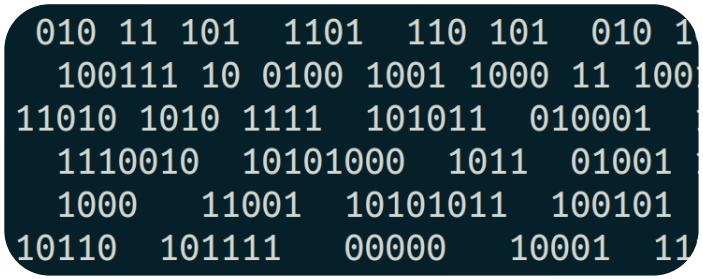
Constrained Pseudorandom Functions (CPRFs)

Pseudorandom Functions *with constrained access to the evaluation.*

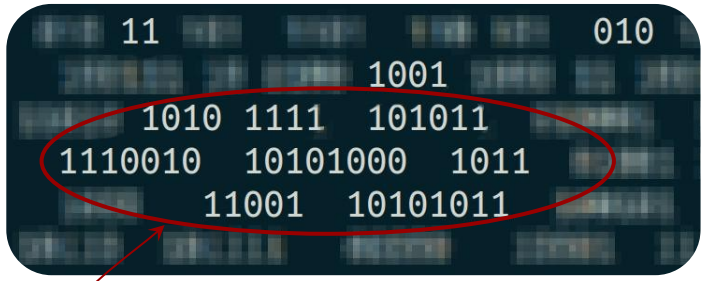
Every predicate $F : \mathcal{X} \to \{0,1\}$ defines a subset $S_F = \{x \in \mathcal{X} : F(x) = 0\}$

(w)PRF ⇝ Pseudorandomly Constrained PRF

Set of outputs with msk



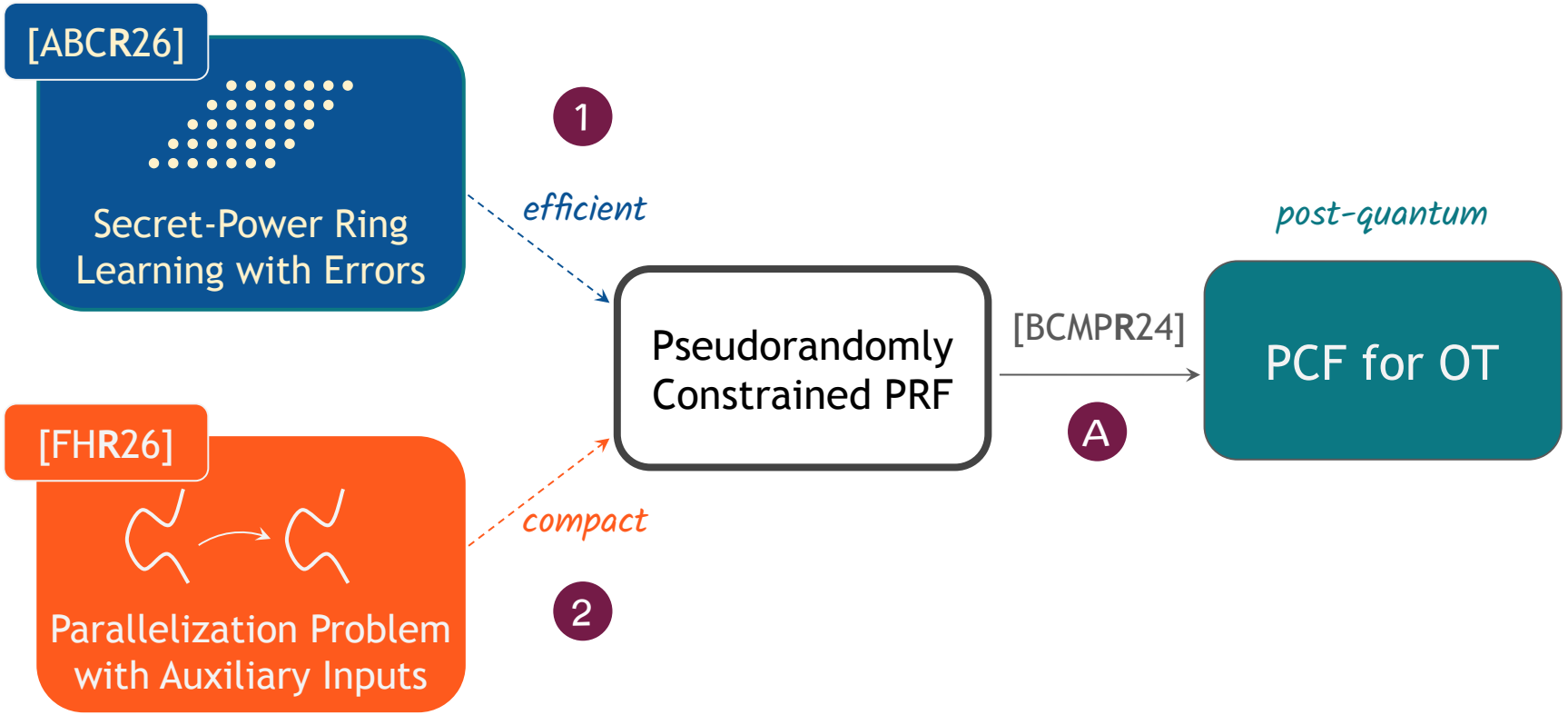
Compute using msk $\xleftarrow{\$} \mathcal{K}$



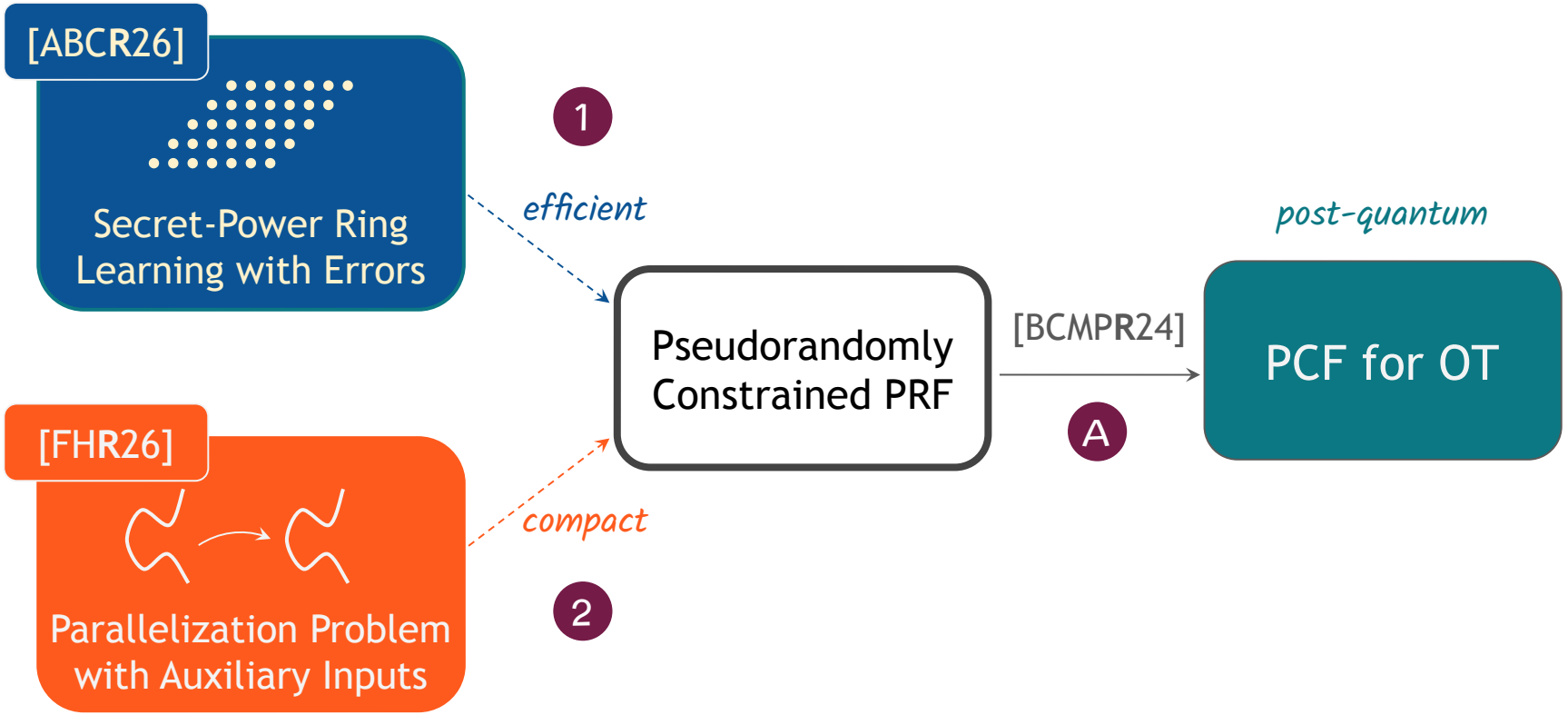
using ck_F

local evaluation on S_F

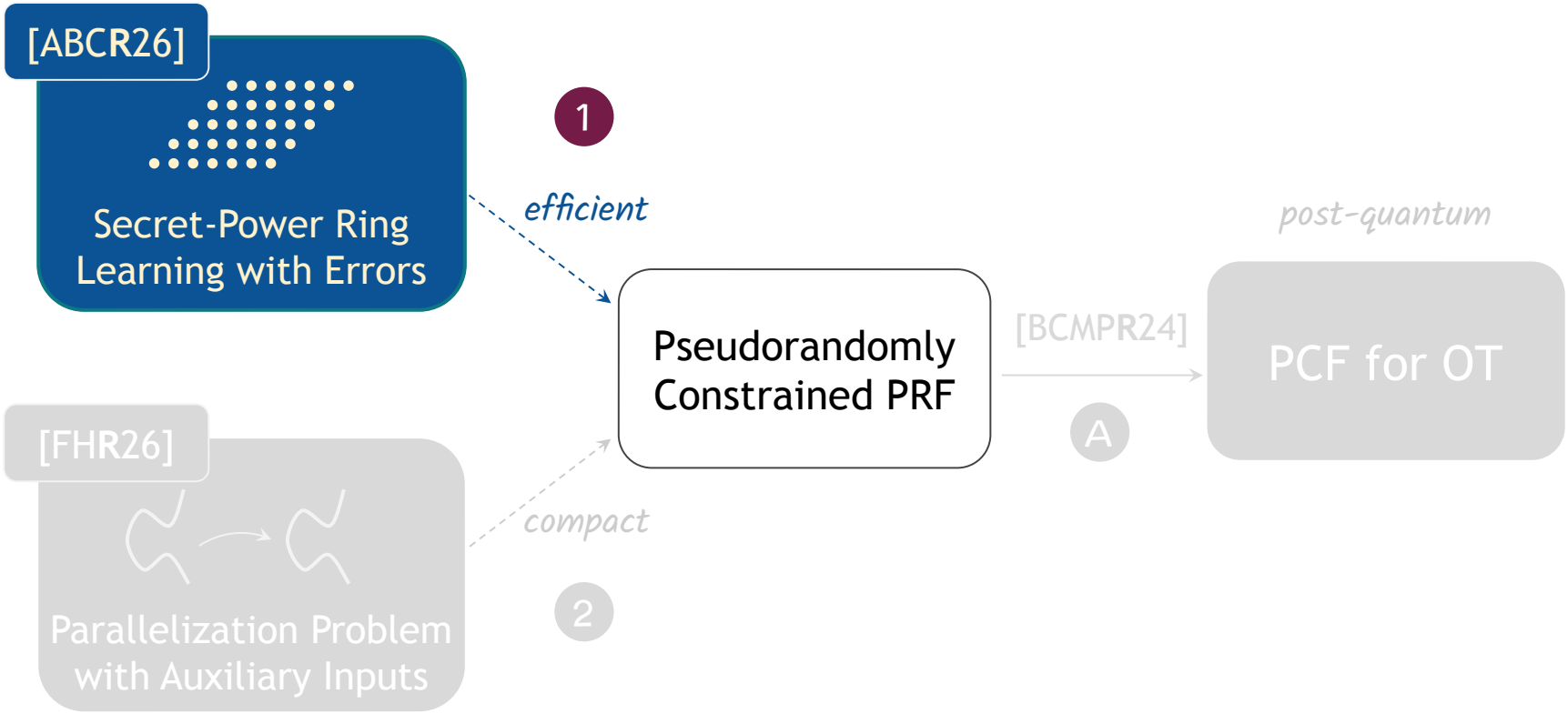
Road Map


[ABCR26]
Secret-Power Ring Learning with Errors
1
efficient
[FHR26]
Parallelization Problem with Auxiliary Inputs
compact
2
Pseudorandomly Constrained PRF
[BCMPR24]
A
post-quantum
PCF for OT

Road Map


[ABCR26]
Secret-Power Ring Learning with Errors
1
efficient
[FHR26]
Parallelization Problem with Auxiliary Inputs
compact
2
Pseudorandomly Constrained PRF
[BCMPR24]
A
post-quantum
PCF for OT

Road Map


[ABCR26]
Secret-Power Ring Learning with Errors
1
efficient
Pseudorandomly Constrained PRF
[BCMPR24]
A
post-quantum
PCF for OT
[FHR26]
Parallelization Problem with Auxiliary Inputs
compact
2

A Pseudorandomly-Constrained PRF from Secret-Power Ring LWE

Ring Learning with Errors (Ring LWE)

Ring LWE

Let $R_q = R/qR$ for some ring R and integer q

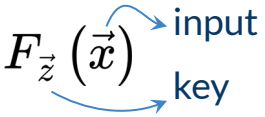
$$(a, as + e) \approx_c (a, b)$$

where $a, s, b \xleftarrow{\$} R_q$, $e \xleftarrow{\$} \chi$

small-norm distribution

Constrained PRFs from Secret-Power Ring LWE

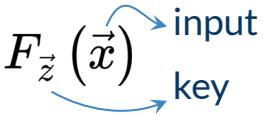
Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a (weak) PRF.



Goal: A CPRF that can generate $\mathsf{ck}_{\vec{z}}$ that evaluates on all $\vec{x}$ *iff* $F_{\vec{z}}(\vec{x}) = 0$.

Constrained PRFs from Secret-Power Ring LWE

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a (weak) PRF.



Goal: A CPRF that can generate $\mathsf{ck}_{\vec{z}}$ that evaluates on all $\vec{x}$ *iff* $F_{\vec{z}}(\vec{x}) = 0$.

(Ring R_q)

Let $P : \{0,1\}^n \times R_q^n \to R_q$ represent F over R_q ; $P(\vec{x}, \vec{z}) = 0 \iff F_{\vec{z}}(\vec{x}) = 0$

A More General Goal: A CPRF that can generate $\mathsf{ck}_{\vec{z}}$ that evaluates on all $\vec{x}$ *iff* $P(\vec{x}, \vec{z}) = 0$.

t : max degree of all $P(\vec{x}, \cdot)$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P\left(\vec{x}, \vec{z}\right) = 0$. $\left(P : \{0,1\}^n \times R_q^n \to R_q\right)$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n, \underset{\text{invertible}}{s}, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}\left(\vec{x}\right) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

$$\left(Y \in R_q : \lfloor Y \rceil_2 = \lfloor Y \cdot (2/q) \rceil\right)$$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P\left(\vec{x}, \vec{z}\right) = 0$. $\left(P : \{0,1\}^n \times R_q^n \to R_q\right)$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}\left(\vec{x}\right) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Constrained Key for $\vec{z} \in \{0,1\}^n$ **?**

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P\left(\vec{x}, \vec{z}\right) = 0$. $\left(P : \{0,1\}^n \times R_q^n \to R_q\right)$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}\left(\vec{x}\right) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Constrained Key for $\vec{z} \in \{0,1\}^n$ **?**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P\left(\vec{x}, \vec{z}\right) = 0$. $\left(P : \{0,1\}^n \times R_q^n \to R_q\right)$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}\left(\vec{x}\right) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Constrained Key for $\vec{z} \in \{0,1\}^n$ **?**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

$$\Rightarrow as \cdot P\left(\vec{x}, \vec{k}/s\right) = as \cdot P\left(\vec{x}, \vec{\ell}/s + \vec{z}\right)$$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P(\vec{x}, \vec{z}) = 0$. $\quad (P : \{0,1\}^n \times R_q^n \to R_q)$

$P(\vec{x}, Y) = \sum_{i=0}^{t} p_i Y^i$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}(\vec{x}) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Constrained Key for $\vec{z} \in \{0,1\}^n$ **?**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

$$\Rightarrow as \cdot P\left(\vec{x}, \vec{k}/s\right) = as \cdot P\left(\vec{x}, \vec{\ell}/s + \vec{z}\right)$$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P(\vec{x}, \vec{z}) = 0$. $\quad (P : \{0,1\}^n \times R_q^n \to R_q)$

$P(\vec{x}, Y) = \sum_{i=0}^{t} p_i Y^i$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}(\vec{x}) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Constrained Key for $\vec{z} \in \{0,1\}^n$ **?**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

$$\Rightarrow as \cdot P\left(\vec{x}, \vec{k}/s\right) = as \cdot P\left(\vec{x}, \vec{\ell}/s + \vec{z}\right)$$

$$= as \cdot \sum_{i=0}^{t} p_i \left(\vec{\ell}/s + \vec{z}\right)^i$$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P(\vec{x}, \vec{z}) = 0$. $\quad (P : \{0,1\}^n \times R_q^n \to R_q)$

$P(\vec{x}, Y) = \sum_{i=0}^{t} p_i Y^i$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}(\vec{x}) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Constrained Key for $\vec{z} \in \{0,1\}^n$ **?**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

$$\Rightarrow as \cdot P\left(\vec{x}, \vec{k}/s\right) = as \cdot P\left(\vec{x}, \vec{\ell}/s + \vec{z}\right)$$

$$= as \cdot \sum_{i=0}^{t} p_i \left(\vec{\ell}/s + \vec{z}\right)^i$$

$$= as \cdot P(\vec{x}, \vec{z}) + \sum_{i=0}^{t} q_i \cdot a \left(\frac{1}{s}\right)^i$$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P\left(\vec{x}, \vec{z}\right) = 0$. $\left(P : \{0,1\}^n \times R_q^n \to R_q\right)$

$P\left(\vec{x}, Y\right) = \sum_{i=0}^{t} p_i Y^i$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}\left(\vec{x}\right) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Constrained Key for $\vec{z} \in \{0,1\}^n$ **?**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

$$\Rightarrow as \cdot P\left(\vec{x}, \vec{k}/s\right) = as \cdot P\left(\vec{x}, \vec{\ell}/s + \vec{z}\right)$$

$$= as \cdot \sum_{i=0}^{t} p_i \left(\vec{\ell}/s + \vec{z}\right)^i$$

$$= as \cdot P\left(\vec{x}, \vec{z}\right) + \sum_{i=0}^{t} q_i \cdot a \left(\frac{1}{s}\right)^i$$

If $P\left(\vec{x}, \vec{z}\right) = 0$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P(\vec{x}, \vec{z}) = 0$. $\quad (P : \{0,1\}^n \times R_q^n \to R_q)$

$P(\vec{x}, Y) = \sum_{i=0}^{t} p_i Y^i$

(Ring R_q)

Master Secret Key :

$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$F_{\mathsf{msk}}(\vec{x}) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$

is a polynomial in 1/s (rounded mod 2) when P(x,z)=0

Constrained Key for $\vec{z} \in \{0,1\}^n$ **?**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

$$\Rightarrow as \cdot P\left(\vec{x}, \vec{k}/s\right) = as \cdot P\left(\vec{x}, \vec{\ell}/s + \vec{z}\right)$$

$$= as \cdot \sum_{i=0}^{t} p_i \left(\vec{\ell}/s + \vec{z}\right)^i$$

$$= as \cdot P(\vec{x}, \vec{z}) + \sum_{i=0}^{t} q_i \cdot a \left(\frac{1}{s}\right)^i$$

If $P(\vec{x}, \vec{z}) = 0$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P(\vec{x}, \vec{z}) = 0$. $\quad (P : \{0,1\}^n \times R_q^n \to R_q)$

$P(\vec{x}, Y) = \sum_{i=0}^{t} p_i Y^i$

(Ring R_q)

Master Secret Key :

$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$F_{\mathsf{msk}}(\vec{x}) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$

is a polynomial in 1/s (rounded mod 2) when P(x,z)=0

Constrained Key for $\vec{z} \in \{0,1\}^n$ **?**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

$$\Rightarrow as \cdot P\left(\vec{x}, \vec{k}/s\right) = as \cdot P\left(\vec{x}, \vec{\ell}/s + \vec{z}\right)$$

$$= as \cdot \sum_{i=0}^{t} p_i \left(\vec{\ell}/s + \vec{z}\right)^i$$

$$= as \cdot P(\vec{x}, \vec{z}) + \sum_{i=0}^{t} q_i \cdot a \left(\frac{1}{s}\right)^i$$

If $P(\vec{x}, \vec{z}) = 0$

depends on $\vec{x}, \vec{z}, \vec{\ell}$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P\left(\vec{x}, \vec{z}\right) = 0$. $\left(P : \{0,1\}^n \times R_q^n \to R_q\right)$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}\left(\vec{x}\right) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Constrained Key for $\vec{z} \in \{0,1\}^n$ **:**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P\left(\vec{x}, \vec{z}\right) = 0$. $\left(P : \{0,1\}^n \times R_q^n \to R_q\right)$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}\left(\vec{x}\right) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Constrained Key for $\vec{z} \in \{0,1\}^n$ **:**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

$$\mathsf{ck}_{\vec{z}} := \left(\vec{\ell}, \left(\mathcal{A}_i = a \cdot (1/s)^i + e_i\right)_{i \in [0, t-1]}, \vec{z}\right)$$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P\left(\vec{x}, \vec{z}\right) = 0$. $\left(P : \{0,1\}^n \times R_q^n \to R_q\right)$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}\left(\vec{x}\right) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Constrained Key for $\vec{z} \in \{0,1\}^n$ **:**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

$$\mathsf{ck}_{\vec{z}} := \left(\vec{\ell}, \left(\mathcal{A}_i = a \cdot (1/s)^i + e_i\right)_{i \in [0, t-1]}, \vec{z}\right)$$

Constrained Evaluation :

1. Find c_i's such that

$$P\left(\vec{x}, \vec{\ell}/S + \vec{z}\right) = P\left(\vec{x}, \vec{z}\right) + \sum_{i=1}^{t} c_i (1/S)^i$$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P(\vec{x}, \vec{z}) = 0$. $\quad (P : \{0,1\}^n \times R_q^n \to R_q)$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}(\vec{x}) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Constrained Key for $\vec{z} \in \{0,1\}^n$ **:**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

$$\mathsf{ck}_{\vec{z}} := \left(\vec{\ell}, \left(\mathcal{A}_i = a \cdot (1/s)^i + e_i\right)_{i \in [0, t-1]}, \vec{z}\right)$$

Constrained Evaluation :

1. Find c_i's such that

symbolic variable

$$P\left(\vec{x}, \vec{\ell}/S + \vec{z}\right) = P(\vec{x}, \vec{z}) + \sum_{i=1}^{t} c_i (1/S)^i$$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P(\vec{x}, \vec{z}) = 0$. $\quad (P : \{0,1\}^n \times R_q^n \to R_q)$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}(\vec{x}) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Constrained Key for $\vec{z} \in \{0,1\}^n$ **:**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

$$\mathsf{ck}_{\vec{z}} := \left(\vec{\ell}, \left(\mathcal{A}_i = a \cdot (1/s)^i + e_i\right)_{i \in [0, t-1]}, \vec{z}\right)$$

Constrained Evaluation :

1. Find c_i's such that (*symbolic variable*)

$$P\left(\vec{x}, \vec{\ell}/S + \vec{z}\right) = P(\vec{x}, \vec{z}) + \sum_{i=1}^{t} c_i (1/S)^i$$

2. Output $\lfloor \sum_{i=0}^{t-1} c_i \cdot \mathcal{A}_i \rceil_2$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P(\vec{x}, \vec{z}) = 0$. $\quad (P : \{0,1\}^n \times R_q^n \to R_q)$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}(\vec{x}) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Equal when P(x,z)=0

Constrained Key for $\vec{z} \in \{0,1\}^n$ **:**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

$$\mathsf{ck}_{\vec{z}} := \left(\vec{\ell}, \left(\mathcal{A}_i = a \cdot (1/s)^i + e_i\right)_{i \in [0, t-1]}, \vec{z}\right)$$

Constrained Evaluation :

1. Find c_i's such that (*symbolic variable*)

$$P\left(\vec{x}, \vec{\ell}/S + \vec{z}\right) = P(\vec{x}, \vec{z}) + \sum_{i=1}^{t} c_i (1/S)^i$$

2. Output $\lfloor \sum_{i=0}^{t-1} c_i \cdot \mathcal{A}_i \rceil_2$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P(\vec{x}, \vec{z}) = 0$. $\quad (P : \{0,1\}^n \times R_q^n \to R_q)$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}(\vec{x}) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Equal when P(x,z)=0 & error small

Constrained Key for $\vec{z} \in \{0,1\}^n$ **:**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

$$\mathsf{ck}_{\vec{z}} := \left(\vec{\ell}, \left(\mathcal{A}_i = a \cdot (1/s)^i + e_i\right)_{i \in [0, t-1]}, \vec{z}\right)$$

Constrained Evaluation :

1. Find c_i's such that (*symbolic variable*)

$$P\left(\vec{x}, \vec{\ell}/S + \vec{z}\right) = P(\vec{x}, \vec{z}) + \sum_{i=1}^{t} c_i (1/S)^i$$

2. Output $\lfloor \sum_{i=0}^{t-1} c_i \cdot \mathcal{A}_i \rceil_2$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P(\vec{x}, \vec{z}) = 0$. $\quad (P : \{0,1\}^n \times R_q^n \to R_q)$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n,\ s, a \xleftarrow{\$} R_q\right)$$

small *small*

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}(\vec{x}) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Equal when P(x,z)=0 & error small

Constrained Key for $\vec{z} \in \{0,1\}^n$ **:**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$ *small*

$$\mathsf{ck}_{\vec{z}} := \left(\vec{\ell}, \left(\mathcal{A}_i = a \cdot (1/s)^i + e_i\right)_{i \in [0, t-1]}, \vec{z}\right)$$

Constrained Evaluation :

1. Find c_i's such that *symbolic variable*

$$P\left(\vec{x}, \vec{\ell}/S + \vec{z}\right) = P(\vec{x}, \vec{z}) + \sum_{i=1}^{t} c_i (1/S)^i$$

2. Output $\lfloor \sum_{i=0}^{t-1} c_i \cdot \mathcal{A}_i \rceil_2$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P(\vec{x}, \vec{z}) = 0$. $\quad (P : \{0,1\}^n \times R_q^n \to R_q)$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n, \underset{\text{small}}{s}, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}(\vec{x}) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Security

$as + e$ looks random given $\left(a \cdot (1/s)^i + e_i\right)_i$

(Secret-Power Ring LWE)

Constrained Key for $\vec{z} \in \{0,1\}^n$ **:**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

$$\mathsf{ck}_{\vec{z}} := \left(\vec{\ell}, \left(\mathcal{A}_i = a \cdot (1/s)^i + e_i\right)_{i \in [0, t-1]}, \vec{z}\right)$$

Constrained Evaluation :

1. Find c_i's such that (*symbolic variable*)

$$P\left(\vec{x}, \vec{\ell}/S + \vec{z}\right) = P(\vec{x}, \vec{z}) + \sum_{i=1}^{t} c_i (1/S)^i$$

2. Output $\lfloor \sum_{i=0}^{t-1} c_i \cdot \mathcal{A}_i \rceil_2$

Constrained PRFs from Secret-Power Ring LWE

Constraint: $\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ *iff* $P(\vec{x}, \vec{z}) = 0$. $\quad (P : \{0,1\}^n \times R_q^n \to R_q)$

(Ring R_q)

Master Secret Key :

$$\mathsf{msk} := \left((k_1, \ldots, k_n) \xleftarrow{\$} R_q^n, \underset{\text{small}}{s}, a \xleftarrow{\$} R_q\right)$$

Evaluation on $\vec{x} = \overbrace{x_1, x_2, \ldots, x_n}^{\text{binary}}$ **:**

$$F_{\mathsf{msk}}(\vec{x}) := \lfloor as \cdot P\left(\vec{x}, \vec{k}/s\right) \rceil_2$$

Security

$as + e$ looks random given $\left(a \cdot (1/s)^i + e_i\right)_i$

(Secret-Power Ring LWE)

Constrained Key for $\vec{z} \in \{0,1\}^n$ **:**

Let $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

$$\mathsf{ck}_{\vec{z}} := \left(\vec{\ell}, \left(\mathcal{A}_i = a \cdot (1/s)^i + e_i\right)_{i \in [0, t-1]}, \vec{z}\right)$$

Constrained Evaluation :

1. Find c_i's such that (*symbolic variable*)

$$P\left(\vec{x}, \vec{\ell}/S + \vec{z}\right) = P(\vec{x}, \vec{z}) + \sum_{i=1}^{t} c_i (1/S)^i$$

2. Output $\lfloor \sum_{i=0}^{t-1} c_i \cdot \mathcal{A}_i \rceil_2$

+ Random Oracle to hash the output

Comparison with Other (Public-Key) PCFs

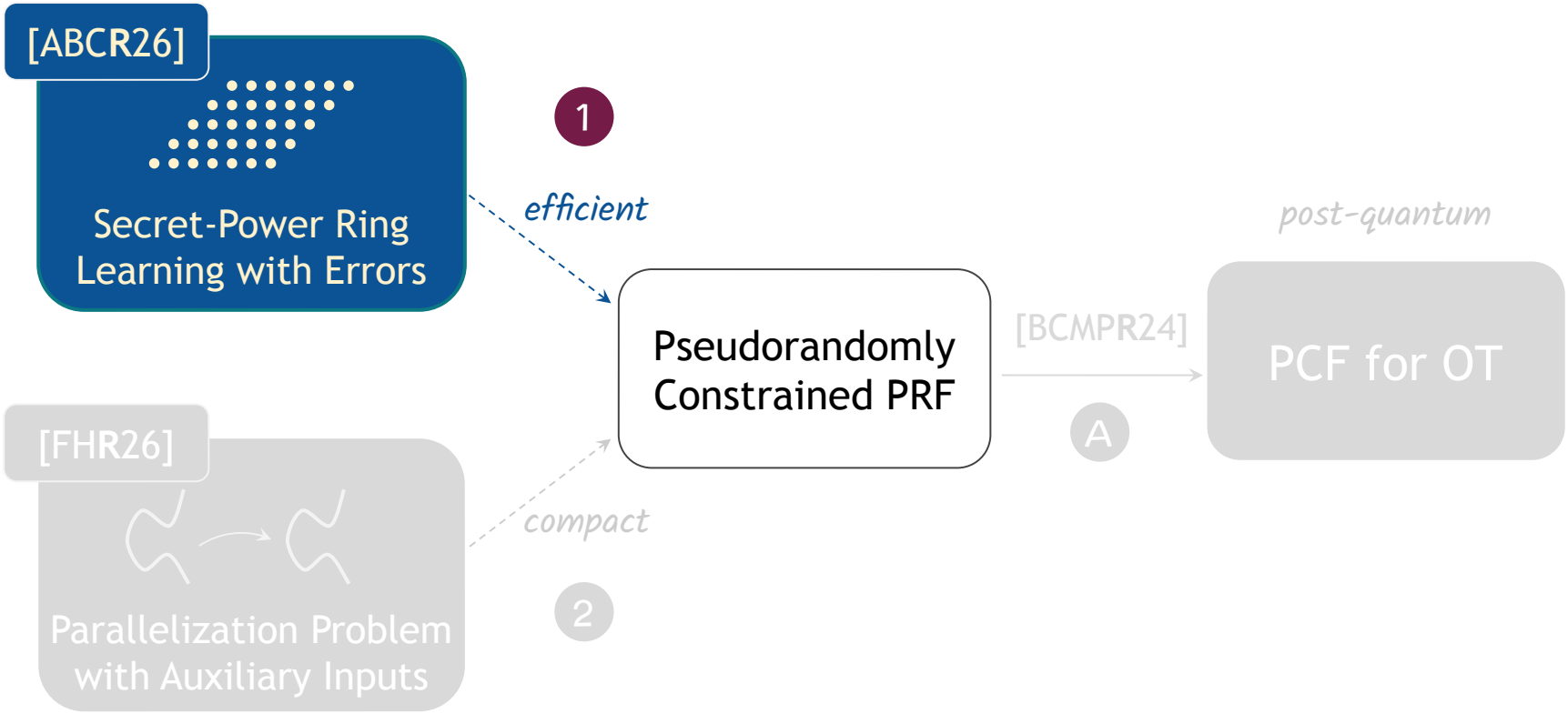
Our PK-PCF =
Our CPRF from secret-power RLWE
+ Goldreich-Applebaum-Raykov weak PRF
+ a public-key setup inspired from "succinct HSS"

Work	Post-Quantum	OT Variant	Key Size	OT/sec
[OSY21]	✗	OT	small	1
[BCMP**R**24]	✗	OT	30 kB	30k
[CDDKS24]	✓	List OT	~ GB	1.2M
This Work	✓	OT	52 GB	540-1k
	✓	OT	4.6 GB	190-450

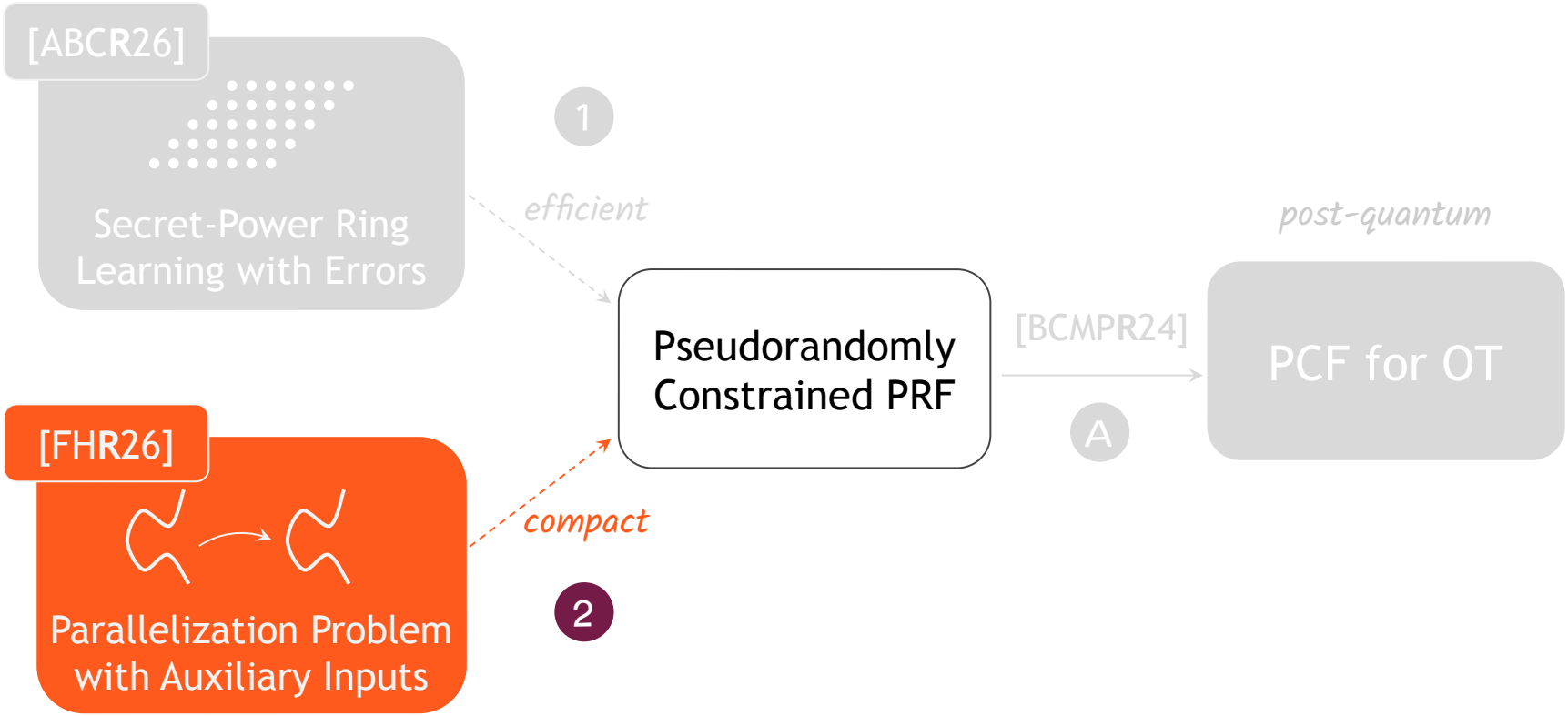
All works additionally use random oracles

HSS: Homomorphic Secret Sharing

Road Map


[ABCR26]
Secret-Power Ring Learning with Errors
1
efficient
Pseudorandomly Constrained PRF
[BCMPR24]
A
post-quantum
PCF for OT
[FHR26]
Parallelization Problem with Auxiliary Inputs
compact
2

Road Map


[ABCR26]
Secret-Power Ring Learning with Errors
1
efficient
post-quantum
Pseudorandomly Constrained PRF
[BCMPR24]
PCF for OT
A
[FHR26]
Parallelization Problem with Auxiliary Inputs
compact
2

Isogeny-Based Naor-Reingold Pseudorandomly-Constrained PRF

Group Actions

$(G, T, \star)$ is an (Abelian Effective) Group Action if

1. $\langle G, \cdot \rangle$ is a finite Abelian group
2. T is an arbitrary finite set
3. $\star : G \times T \to T$ is an associative function, i.e., $g \star (h \star t) = (g \cdot h) \star t$
4. $\star$ is efficiently computable (effective)

"The group G acts on the set T via $\star$"

Group Actions

$(G, T, \star)$ is an (Abelian Effective) Group Action if

1. $\langle G, \cdot \rangle$ is a finite Abelian group
2. T is an arbitrary finite set
3. $\star : G \times T \to T$ is an associative function, i.e., $g \star (h \star t) = (g \cdot h) \star t$
4. $\star$ is efficiently computable (effective)

"The group G acts on the set T via $\star$"

Skipping some (important) details

Group Actions

Group Actions

$(G, T, \star)$ is an (Abelian Effective) Group Action if

1. $\langle G, \cdot \rangle$ is a finite Abelian group
2. T is an arbitrary finite set
3. $\star : G \times T \to T$ is an associative function, i.e., $g \star (h \star t) = (g \cdot h) \star t$
4. $\star$ is efficiently computable (effective)

"The group G acts on the set T via $\star$"

Isogeny-Based Instantiation [qt-Pegasis]: A specific instantiation is the action of class group of a quadratic field on elliptic curves

Skipping some (important) details

Group Actions

Group Actions

$(G, T, \star)$ is an (Abelian Effective) Group Action if

1. $\langle G, \cdot \rangle$ is a finite Abelian group
2. T is an arbitrary finite set
3. $\star : G \times T \to T$ is an associative function, i.e., $g \star (h \star t) = (g \cdot h) \star t$
4. $\star$ is efficiently computable (effective)

"The group G acts on the set T via $\star$"

Isogeny-Based Instantiation [qt-Pegasis]: A specific instantiation is the action of class group of a quadratic field on elliptic curves

A way to "save" group-based cryptography in a quantum world

Skipping some (important) details

Group Actions

Group Actions

$(G, T, \star)$ is an (Abelian Effective) Group Action if

1. $\langle G, \cdot \rangle$ is a finite Abelian group
2. T is an arbitrary finite set
3. $\star : G \times T \to T$ is an associative function, i.e., $g \star (h \star t) = (g \cdot h) \star t$
4. $\star$ is efficiently computable (effective)

"The group G acts on the set T via $\star$"

Isogeny-Based Instantiation [qt-Pegasis]: A specific instantiation is the action of class group of a quadratic field on elliptic curves

A way to "save" group-based cryptography in a quantum world

➡ replace group operations by group actions;

Skipping some (important) details

Group Actions

Group Actions

$(G, T, \star)$ is an (Abelian Effective) Group Action if

1. $\langle G, \cdot \rangle$ is a finite Abelian group
2. T is an arbitrary finite set
3. $\star : G \times T \to T$ is an associative function, i.e., $g \star (h \star t) = (g \cdot h) \star t$
4. $\star$ is efficiently computable (effective)

"The group G acts on the set T via $\star$"

Isogeny-Based Instantiation [qt-Pegasis]: A specific instantiation is the action of class group of a quadratic field on elliptic curves

A way to "save" group-based cryptography in a quantum world

➡ replace group operations by group actions; $t^a \to a \star t$ ✓

Skipping some (important) details

Group Actions

Group Actions

$(G, T, \star)$ is an (Abelian Effective) Group Action if

1. $\langle G, \cdot \rangle$ is a finite Abelian group
2. T is an arbitrary finite set
3. $\star : G \times T \to T$ is an associative function, i.e., $g \star (h \star t) = (g \cdot h) \star t$
4. $\star$ is efficiently computable (effective)

"The group G acts on the set T via $\star$"

Isogeny-Based Instantiation [qt-Pegasis]: A specific instantiation is the action of class group of a quadratic field on elliptic curves

A way to "save" group-based cryptography in a quantum world

➡ replace group operations by group actions;

$$\begin{cases} t^a \to a \star t & \checkmark \\ t^a \cdot t'^b \to (a \star t) \cdot (b \star t') \end{cases}$$

Skipping some (important) details

Group Actions

Group Actions

$(G, T, \star)$ is an (Abelian Effective) Group Action if

1. $\langle G, \cdot \rangle$ is a finite Abelian group
2. T is an arbitrary finite set
3. $\star : G \times T \to T$ is an associative function, i.e., $g \star (h \star t) = (g \cdot h) \star t$
4. $\star$ is efficiently computable (effective)

"The group G acts on the set T via $\star$"

Isogeny-Based Instantiation [qt-Pegasis]: A specific instantiation is the action of class group of a quadratic field on elliptic curves

A way to "save" group-based cryptography in a quantum world

➡ replace group operations by group actions;

$$\begin{cases} t^a \to a \star t & \checkmark \\ t^a \cdot t'^b \to (a \star t) \cdot (b \star t') & \times \end{cases}$$

Skipping some (important) details

Naor-Reingold PRF (In terms of EGA)

$(\mathbb{G}, T, \star)$ is an Abelian EGA

Master Secret Key :

$$\mathsf{msk} := (t \xleftarrow{\$} T, (g_1, \ldots, g_n) \xleftarrow{\$} \mathbb{G})$$

Evaluation on $\vec{x} = \underset{n}{x_1, x_2, \ldots, x_n}$ **:**

$$F_{\mathsf{msk}}(x) := \prod_{i=1} g_i^{x_i} \star t$$

Naor-Reingold Constrained PRF for inner-product membership

inner-product **membership** constraint: $\mathsf{ck}_{(\vec{z},S)}$ can evaluate on all $\vec{x}$ *iff* $\langle \vec{x}, \vec{z} \rangle \in S$

$(\mathbb{G}, T, \star)$ is an Abelian EGA

Master Secret Key :

$\mathsf{msk} := (t \xleftarrow{\$} T, (g_1, \ldots, g_n) \xleftarrow{\$} \mathbb{G})$

Evaluation on $\vec{x} = \underset{n}{x_1, x_2, \ldots, x_n}$ **:**

$$F_{\mathsf{msk}}(x) := \prod_{i=1} g_i^{x_i} \star t$$

Naor-Reingold Constrained PRF for inner-product membership

inner-product **membership** constraint: $\mathsf{ck}_{(\vec{z},S)}$ can evaluate on all $\vec{x}$ iff $\langle \vec{x}, \vec{z} \rangle \in S$

$(\mathbb{G}, T, \star)$ is an Abelian EGA

Master Secret Key :

$$\mathsf{msk} := (t \xleftarrow{\$} T, (g_1, \ldots, g_n) \xleftarrow{\$} \mathbb{G})$$

Evaluation on $\vec{x} = x_1, x_2, \ldots, x_n$ **:**

$$F_{\mathsf{msk}}(x) := \prod_{i=1}^{n} g_i^{x_i} \star t$$

Many weak PRFs can be expressed as IPM predicates

CPRF for IPM ➡ *Pseudorandomly-Constrained PRF*

Naor-Reingold Constrained PRF

inner-product **membership** constraint: $\mathsf{ck}_{(\vec{z},S)}$ can evaluate on all $\vec{x}$ *iff* $\langle \vec{x}, \vec{z} \rangle \in S$

$(\mathbb{G}, T, \star)$ is an Abelian EGA

Master Secret Key :

$$\mathsf{msk} := (t \xleftarrow{\$} T, (g_1, \ldots, g_n) \xleftarrow{\$} \mathbb{G})$$

Evaluation on $\vec{x} = x_1, x_2, \ldots, x_n$ **:**

$$F_{\mathsf{msk}}(x) := \prod_{i=1}^{n} g_i^{x_i} \star t$$

Constrained Key for $(\vec{z} \in \{0,1\}^n, S \subseteq [n])$**:**

Constrained Evaluation:

Naor-Reingold Constrained PRF

inner-product **membership** constraint: $\mathsf{ck}_{(\vec{z},S)}$ can evaluate on all $\vec{x}$ *iff* $\langle \vec{x}, \vec{z} \rangle \in S$

$(\mathbb{G}, T, \star)$ is an Abelian EGA

Master Secret Key :

$$\mathsf{msk} := (t \xleftarrow{\$} T, (g_1, \ldots, g_n) \xleftarrow{\$} \mathbb{G})$$

Evaluation on $\vec{x} = x_1, x_2, \ldots, x_n$ **:**

$$F_{\mathsf{msk}}(x) := \prod_{i=1}^{n} g_i^{x_i} \star t$$

Constrained Key for $(\vec{z} \in \{0,1\}^n, S \subseteq [n])$**:**

$$\mathsf{ck}_{(\vec{z},S)} := \left(\left\{ g_i \cdot r^{-z_i} \right\}_{i \in [n]}, (r^s \star t)_{s \in S}, \vec{z} \right)$$

$(r \xleftarrow{\$} \mathbb{G})$

Constrained Evaluation:

Naor-Reingold Constrained PRF

inner-product **membership** constraint: $\mathsf{ck}_{(\vec{z},S)}$ can evaluate on all $\vec{x}$ *iff* $\langle \vec{x}, \vec{z} \rangle \in S$

$(\mathbb{G}, T, \star)$ is an Abelian EGA

Master Secret Key :

$$\mathsf{msk} := (t \xleftarrow{\$} T, (g_1, \ldots, g_n) \xleftarrow{\$} \mathbb{G})$$

Evaluation on $\vec{x} = x_1, x_2, \ldots, x_n$ **:**

$$F_{\mathsf{msk}}(x) := \prod_{i=1}^{n} g_i^{x_i} \star t$$

Constrained Key for $(\vec{z} \in \{0,1\}^n, S \subseteq [n])$**:**

$$\mathsf{ck}_{(\vec{z},S)} := \left(\left\{ g_i \cdot r^{-z_i} \right\}_{i \in [n]}, (r^s \star t)_{s \in S}, \vec{z} \right)$$

$(r \xleftarrow{\$} \mathbb{G})$

Constrained Evaluation:

$$F_{\mathsf{ck}_{(\vec{z},S)}}(x) = \prod_{i=1}^{n} \left(g_i \cdot r^{-z_i} \right)^{x_i} \star (r^s \star t)$$

$$= \prod_{i=1}^{n} g_i^{x_i} \cdot r^{-\langle \vec{x}, \vec{z} \rangle} \cdot r^s \star t$$

Naor-Reingold Constrained PRF

inner-product **membership** constraint: $\mathsf{ck}_{(\vec{z},S)}$ can evaluate on all $\vec{x}$ *iff* $\langle \vec{x}, \vec{z} \rangle \in S$

$(\mathbb{G}, T, \star)$ is an Abelian EGA

Master Secret Key :

$$\mathsf{msk} := (t \xleftarrow{\$} T, (g_1, \ldots, g_n) \xleftarrow{\$} \mathbb{G})$$

Evaluation on $\vec{x} = x_1, x_2, \ldots, x_n$ **:**

$$F_{\mathsf{msk}}(x) := \prod_{i=1}^{n} g_i^{x_i} \star t$$

equal if

$$\exists s \in S : \langle \vec{x}, \vec{z} \rangle = s$$

Constrained Key for $(\vec{z} \in \{0,1\}^n, S \subseteq [n])$**:**

$$\mathsf{ck}_{(\vec{z},S)} := \left(\left\{ g_i \cdot r^{-z_i} \right\}_{i \in [n]}, (r^s \star t)_{s \in S}, \vec{z} \right)$$

$(r \xleftarrow{\$} \mathbb{G})$

Constrained Evaluation:

$$F_{\mathsf{ck}_{(\vec{z},S)}}(x) = \prod_{i=1}^{n} \left(g_i \cdot r^{-z_i} \right)^{x_i} \star (r^s \star t)$$

$$= \prod_{i=1}^{n} g_i^{x_i} \cdot r^{-\langle \vec{x}, \vec{z} \rangle} \cdot r^s \star t$$

Naor-Reingold Constrained PRF

inner-product **membership** constraint: $\mathsf{ck}_{(\vec{z},S)}$ can evaluate on all $\vec{x}$ *iff* $\langle \vec{x}, \vec{z} \rangle \in S$

$(\mathbb{G}, T, \star)$ is an Abelian EGA

Master Secret Key :

$$\mathsf{msk} := (t \xleftarrow{\$} T, (g_1, \ldots, g_n) \xleftarrow{\$} \mathbb{G})$$

Evaluation on $\vec{x} = x_1, x_2, \ldots, x_n$ **:**

$$F_{\mathsf{msk}}(x) := \prod_{i=1}^{n} g_i^{x_i} \star t$$

equal if

$$\exists s \in S : \langle \vec{x}, \vec{z} \rangle = s$$

Constrained Key for $(\vec{z} \in \{0,1\}^n, S \subseteq [n])$**:**

$$\mathsf{ck}_{(\vec{z},S)} := \left(\left\{ g_i \cdot r^{-z_i} \right\}_{i \in [n]}, (r^s \star t)_{s \in S}, \vec{z} \right)$$

$(r \xleftarrow{\$} \mathbb{G})$

Constrained Evaluation:

$$F_{\mathsf{ck}_{(\vec{z},S)}}(x) = \prod_{i=1}^{n} \left(g_i \cdot r^{-z_i} \right)^{x_i} \star (r^s \star t)$$

$$= \prod_{i=1}^{n} g_i^{x_i} \cdot r^{-\langle \vec{x}, \vec{z} \rangle} \cdot r^s \star t$$

No-Evaluation Unpredictability

$r^{\langle \vec{x}, \vec{z} \rangle} \star t$ is hard to compute given $(r^s \star t)_{s \in S}$

(S-Power Parallelization Problem)

Naor-Reingold Constrained PRF

inner-product **membership** constraint: $\mathsf{ck}_{(\vec{z},S)}$ can evaluate on all $\vec{x}$ *iff* $\langle \vec{x}, \vec{z} \rangle \in S$

$(\mathbb{G}, T, \star)$ is an Abelian EGA

Master Secret Key :

$$\mathsf{msk} := (t \xleftarrow{\$} T, (g_1, \ldots, g_n) \xleftarrow{\$} \mathbb{G})$$

Evaluation on $\vec{x} = x_1, x_2, \ldots, x_n$ **:**

$$F_{\mathsf{msk}}(x) := \prod_{i=1}^{n} g_i^{x_i} \star t$$

equal if

$$\exists s \in S : \langle \vec{x}, \vec{z} \rangle = s$$

Constrained Key for $(\vec{z} \in \{0,1\}^n, S \subseteq [n])$**:**

$$\mathsf{ck}_{(\vec{z},S)} := \left(\left\{ g_i \cdot r^{-z_i} \right\}_{i \in [n]}, (r^s \star t)_{s \in S}, \vec{z} \right)$$

$(r \xleftarrow{\$} \mathbb{G})$

Constrained Evaluation:

$$F_{\mathsf{ck}_{(\vec{z},S)}}(x) = \prod_{i=1}^{n} \left(g_i \cdot r^{-z_i} \right)^{x_i} \star (r^s \star t)$$

$$= \prod_{i=1}^{n} g_i^{x_i} \cdot r^{-\langle \vec{x}, \vec{z} \rangle} \cdot r^s \star t$$

No-Evaluation Unpredictability

$r^{\langle \vec{x}, \vec{z} \rangle} \star t$ is hard to compute given $(r^s \star t)_{s \in S}$

(S-Power Parallelization Problem)

Full pseudorandomness via (quantum) random oracle

Assumption Analysis - Overview

(S is defined by a wPRF)

S-Power Parallelization

- Given $\left(r^s \star t\right)_{s \in S}$
- Compute $r^v \star t$
  $v \notin S$

Assumption Analysis - Overview

Vectorization Problem

- Given $r \star t$, t
- Compute r

Parallelization Problem

- Given $r \star t$, $r' \star t$, t
- Compute $rr' \star t$

(S is defined by a wPRF)

S-Power Parallelization

- Given $\left(r^s \star t\right)_{s \in S}$
- Compute $r^v \star t$
  $v \notin S$

Assumption Analysis - Overview

Vectorization Problem

- Given $r \star t$, t
- Compute r

$\longleftrightarrow$

Parallelization Problem

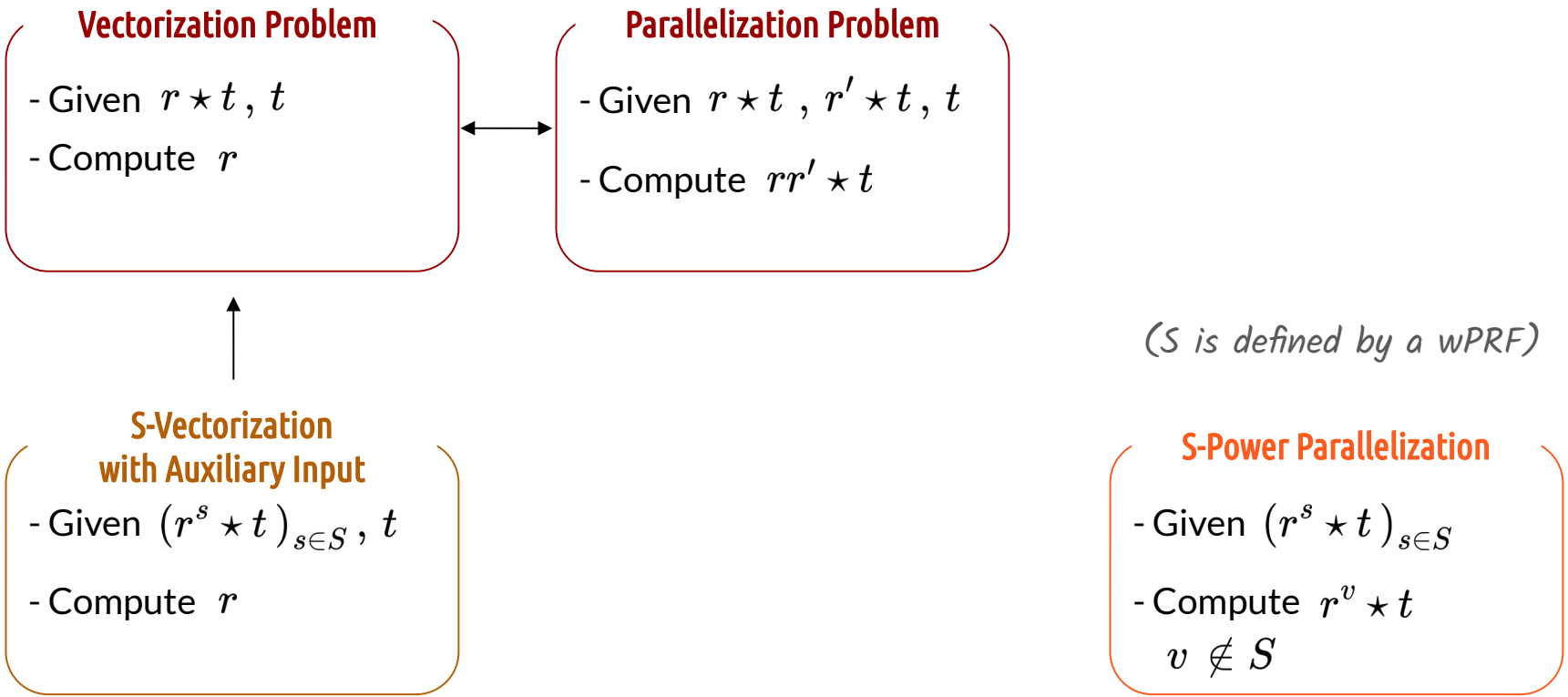
- Given $r \star t$, $r' \star t$, t
- Compute $rr' \star t$

(S is defined by a wPRF)

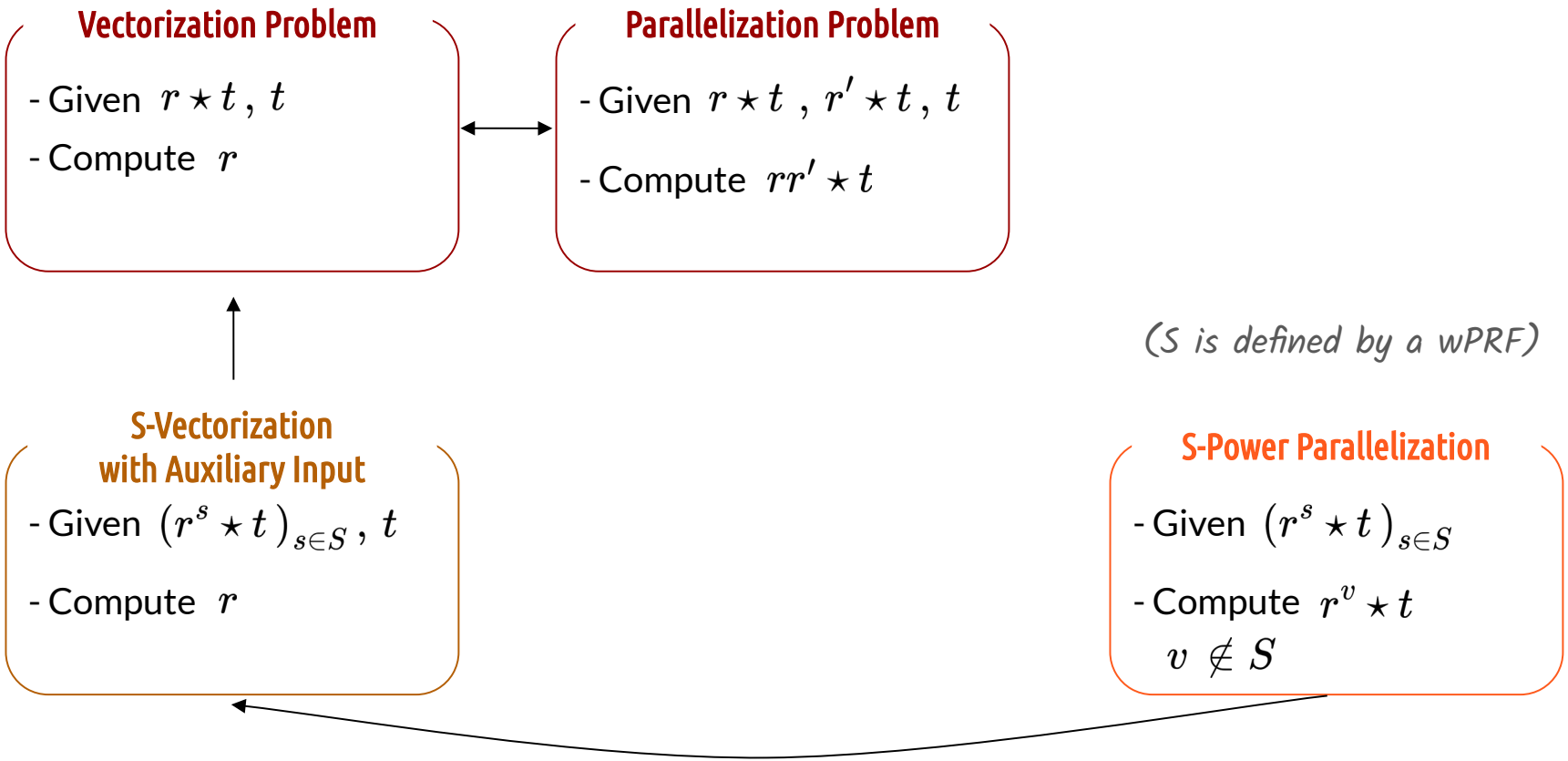
S-Power Parallelization

- Given $\left(r^s \star t\right)_{s \in S}$
- Compute $r^v \star t$
  $v \notin S$

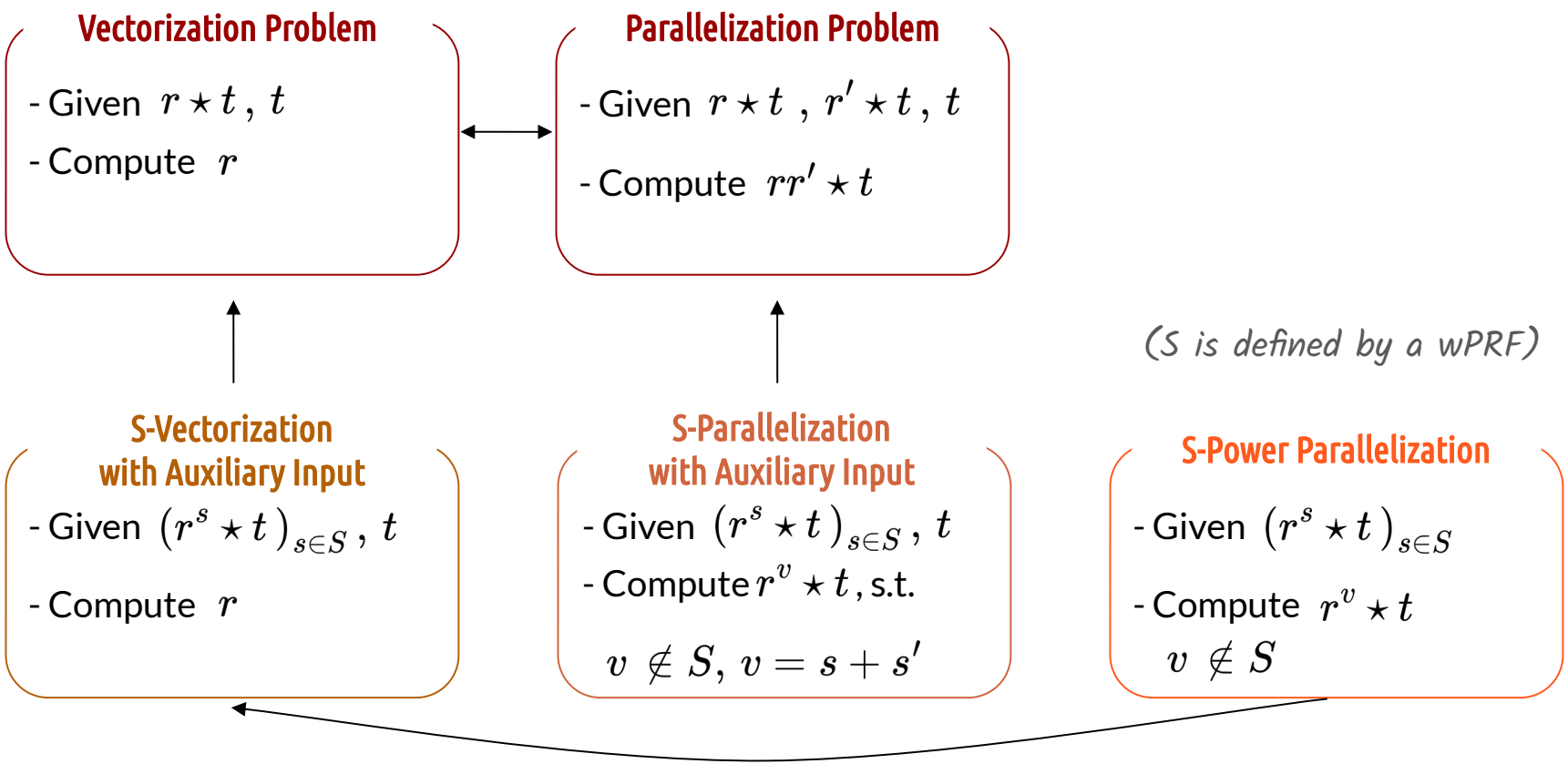
Assumption Analysis - Overview



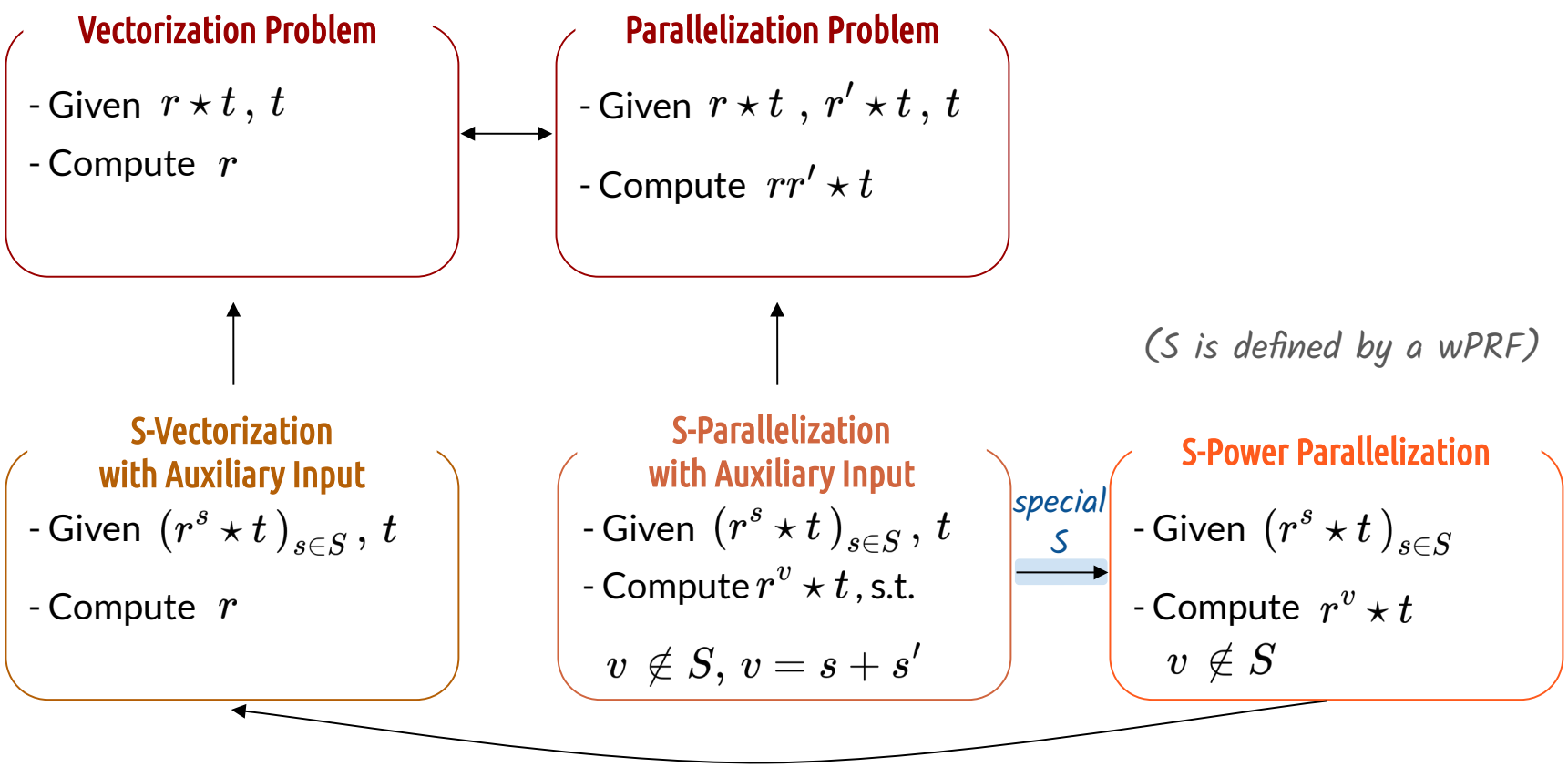
Assumption Analysis - Overview



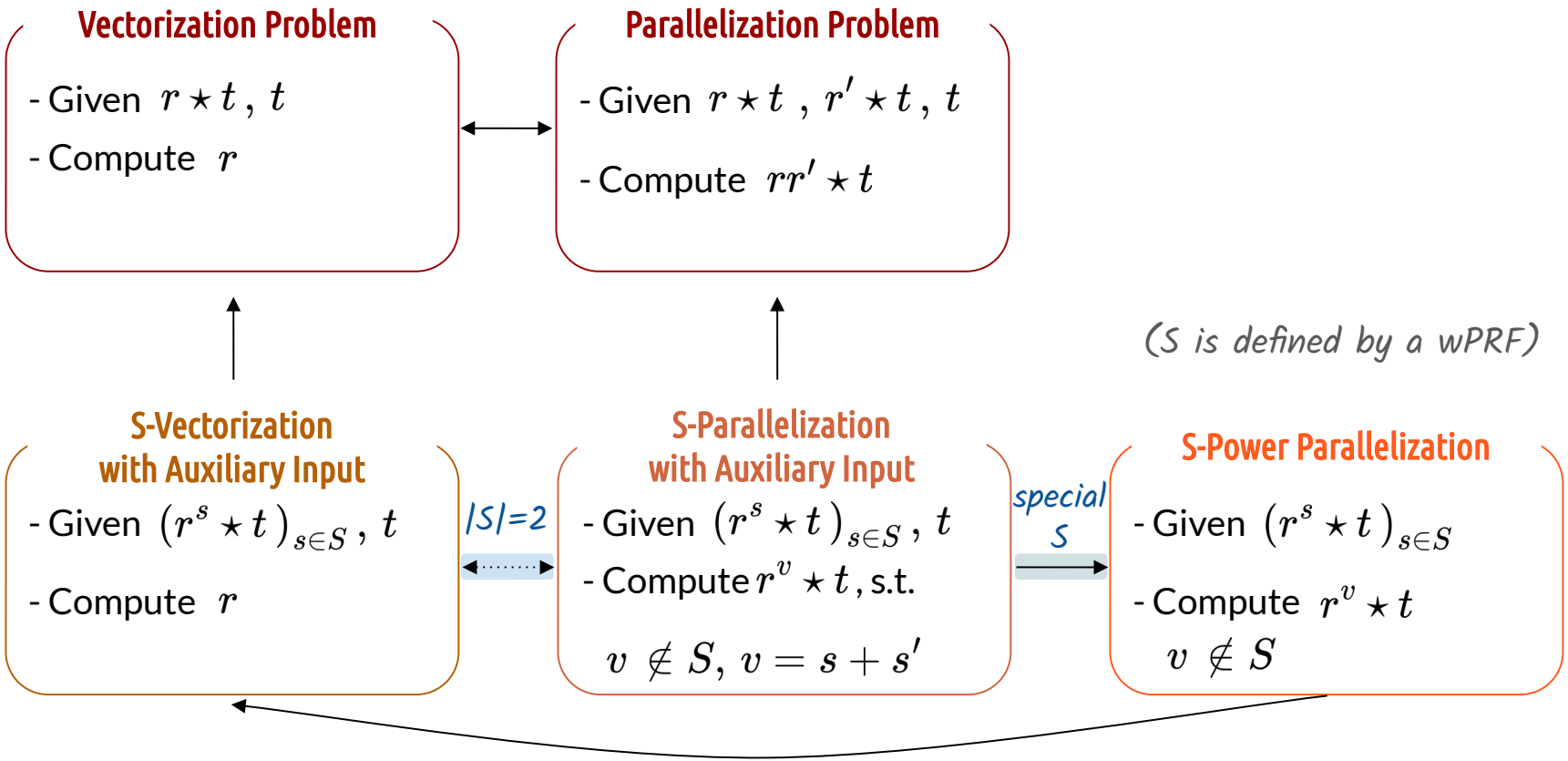
Assumption Analysis - Overview



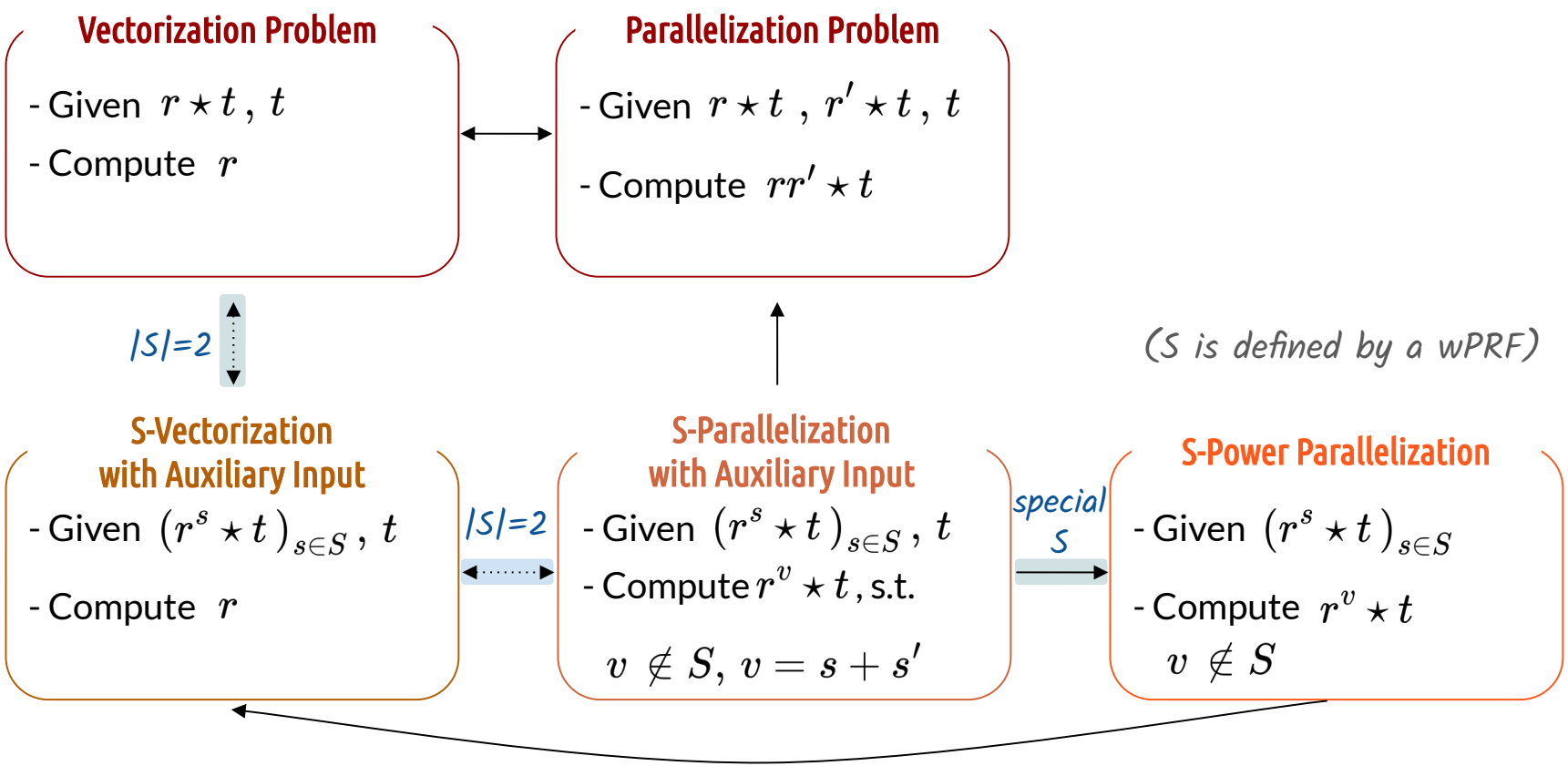
Assumption Analysis - Overview



Assumption Analysis - Overview



Assumption Analysis - Overview

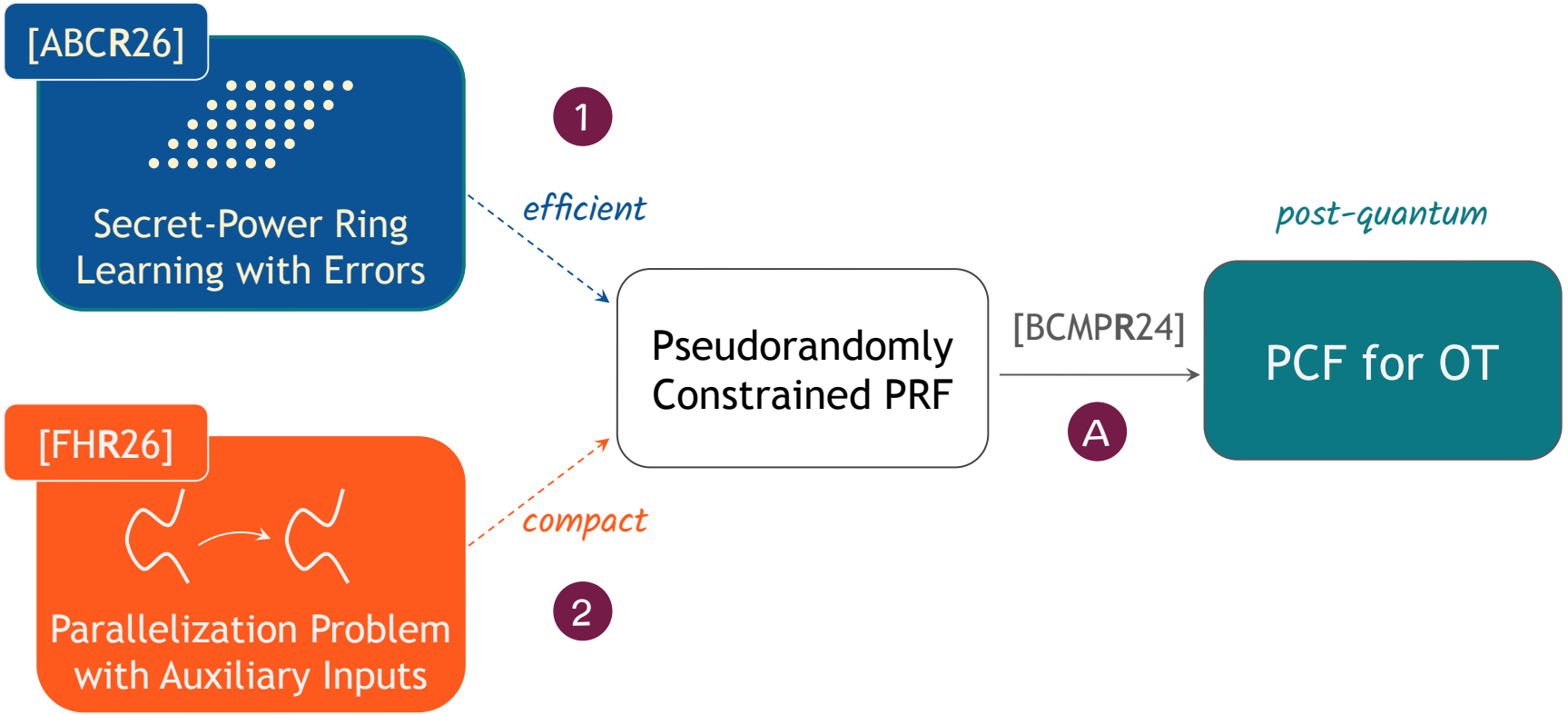


Comparison with Other Post-Quantum PCFs

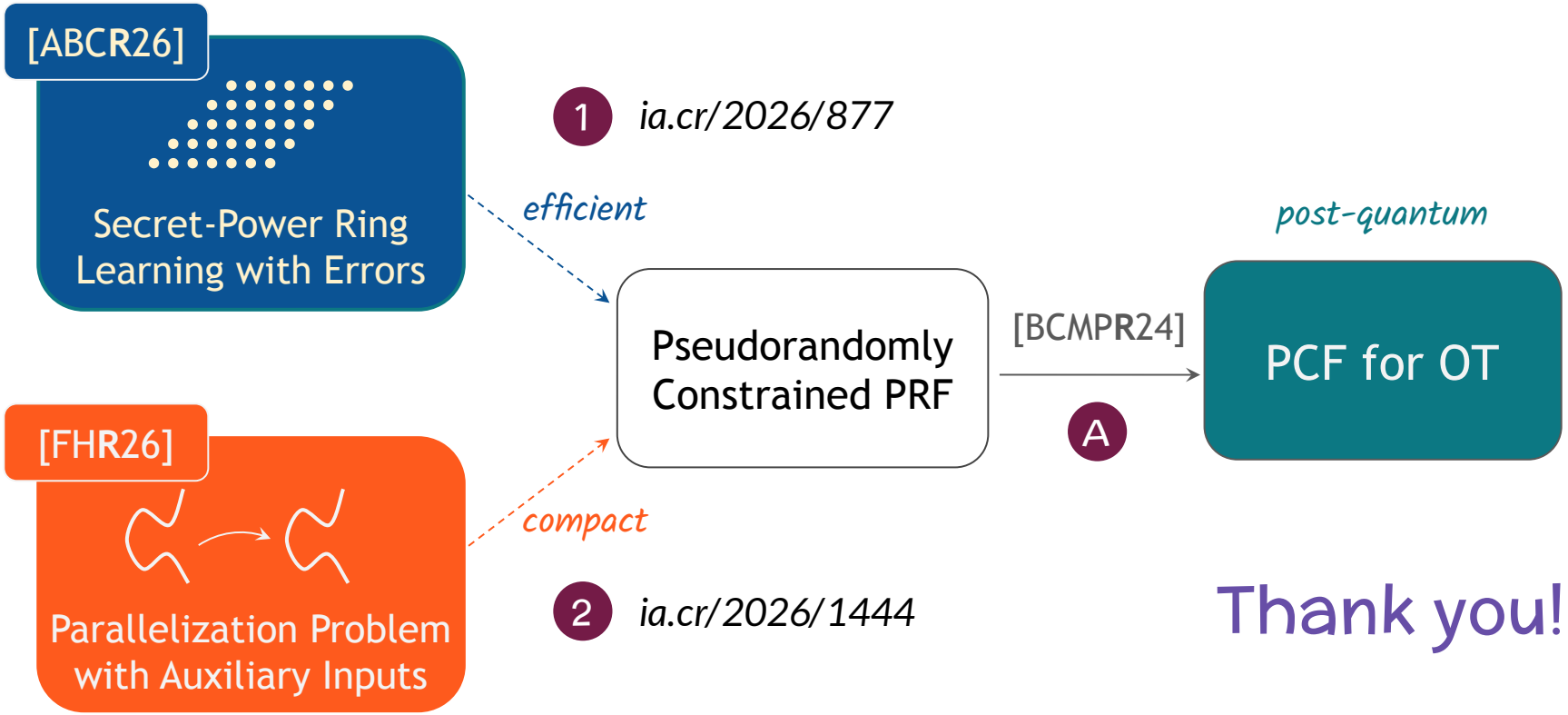
Work	Assumption	Asymptotic	Key Sizes (kB)		OT/sec
[BCG+20]	Ring-LWE (FHE)	✓	>1,000,000		✗
[BCG+20] [CD23]	VD-LPN	✗	2000	2000	1k
[BCG+22]	EA-LPN	✗	370	370	118k
[BCM+25]	Sparse LPN	✗	2812	638	507k
[HRK25]	Ring-LWE (FHE)	✓	>1,000,000		9
This Work	Parallelization with Auxiliary Inputs	✓	0.016	104	6.5

All works additionally use random oracles

Road Map


[ABCR26]
Secret-Power Ring Learning with Errors
1
efficient
Pseudorandomly Constrained PRF
[BCMPR24]
A
post-quantum
PCF for OT
[FHR26]
Parallelization Problem with Auxiliary Inputs
compact
2

Road Map


[ABCR26]
Secret-Power Ring Learning with Errors
1
ia.cr/2026/877
efficient
post-quantum
Pseudorandomly Constrained PRF
[BCMPR24]
A
PCF for OT
[FHR26]
Parallelization Problem with Auxiliary Inputs
compact
2
ia.cr/2026/1444
Thank you!

References

[AR16] B. Applebaum and P. Raykov. Fast pseudorandom functions based on expander graphs.

[ARS24] D. Abram, L. Roy, P. Scholl. Succinct Homomorphic Secret Sharing.

[BCGIKS19] E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl, and P. Scholl. Efficient pseudorandom correlation generators: Silent OT extension and more.

[BCGIKS20] E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl, and P. Scholl. Correlated pseudorandom functions from variable-density LPN.

[BCMPR24] D. Bui, G. Couteau, P. Meyer, A. Passelègue, M. Riahinia. Fast Public-Key Silent OT and More from Constrained Naor-Reingold.

[BPR12] A. Banerjee, C. Peikert, and A. Rosen. Pseudorandom functions and lattices.

[BW13] D. Boneh and B. Waters. Constrained pseudorandom functions and their applications.

[GGM86] O. Goldreich, S. Goldwasser, and S. Micali. How to construct random functions.

References

[GMW87] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority.

[Gol00] O. Goldreich. Candidate one-way functions based on expander graphs.

[KPTZ13] A. Kiayias, S. Papadopoulos, N. Triandopoulos, and T. Zacharias. Delegatable pseudorandom functions and applications.

Road Map

[ABCR26]

Secret-Power Ring Learning with Errors

1

efficient

[FHR26]

Parallelization Problem with Auxiliary Inputs

compact

2

Pseudorandomly Constrained PRF

[BCMPR24]

A

post-quantum

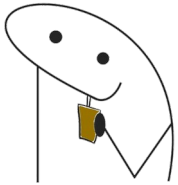
PCF for OT

Pseudorandom Correlation Functions for Oblivious Transfer

from pseudorandomly constrained PRFs

PCF for OT from Pseudorandomly Constrained PRFs

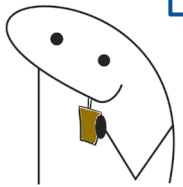




PCF for OT from Pseudorandomly Constrained PRFs

- wPRF $F_k : \mathcal{X} \to \{0,1\}$

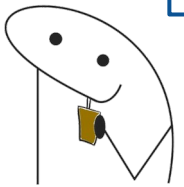




PCF for OT from Pseudorandomly Constrained PRFs

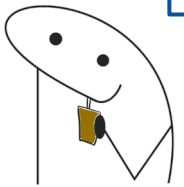
- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$





PCF for OT from Pseudorandomly Constrained PRFs





- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$

can generate a **ck** for either:

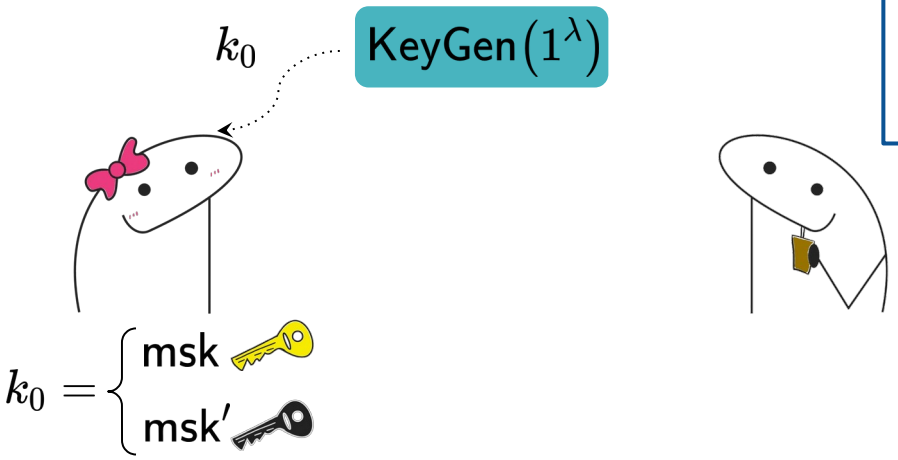
-any **x** s.t. $F_k(x)=0$

or

-any **x** s.t. $F_k(x)=1$

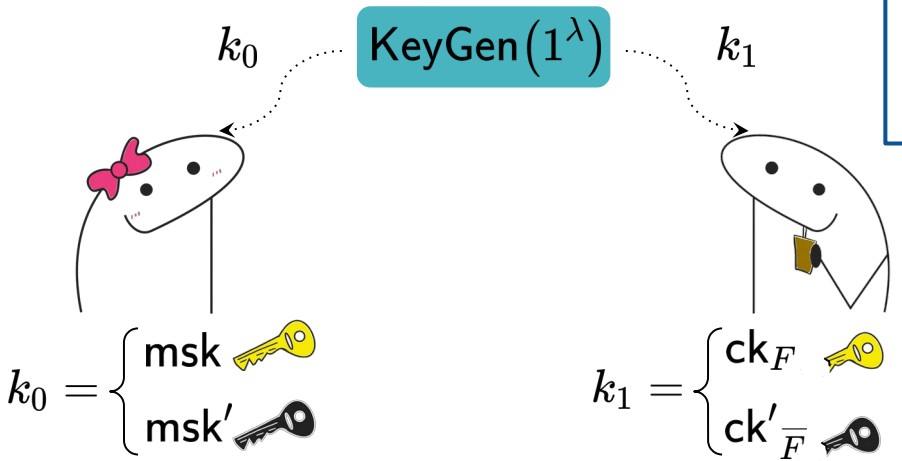
PCF for OT from Pseudorandomly Constrained PRFs

- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$



PCF for OT from Pseudorandomly Constrained PRFs

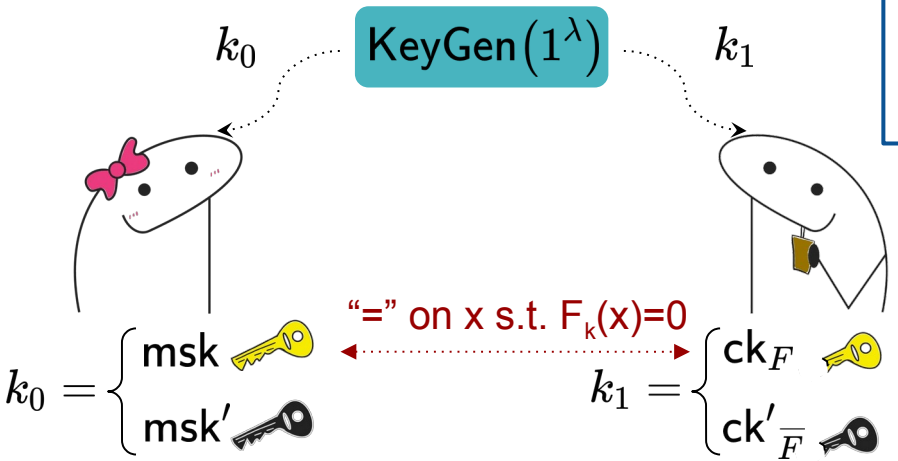
- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$



, k *(wPRF key)*

PCF for OT from Pseudorandomly Constrained PRFs

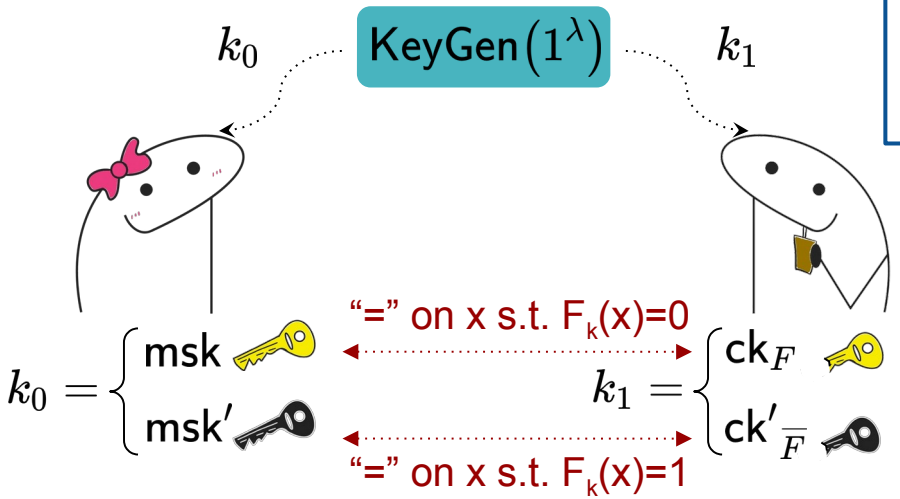
- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$



, k *(wPRF key)*

PCF for OT from Pseudorandomly Constrained PRFs

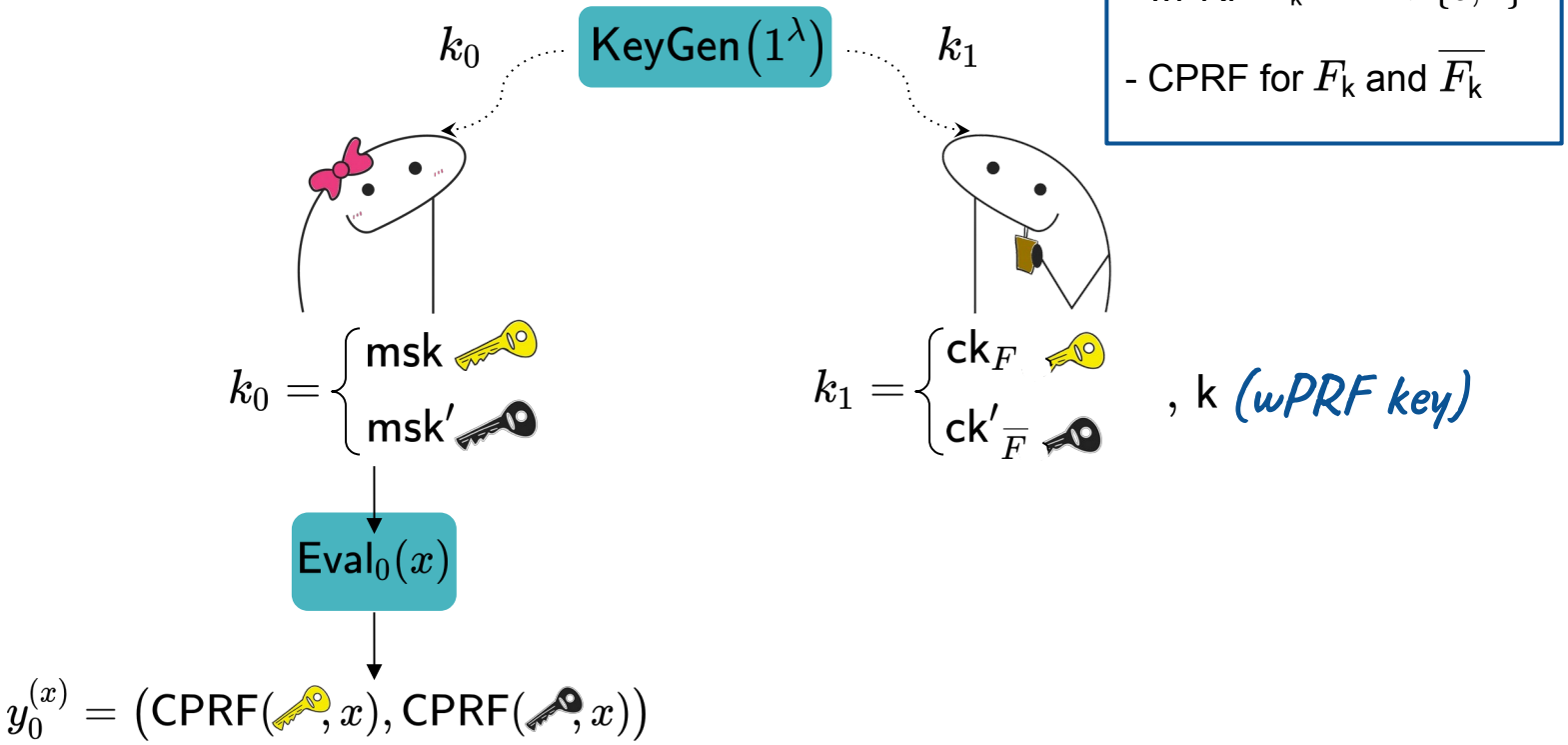
- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$



, k *(wPRF key)*

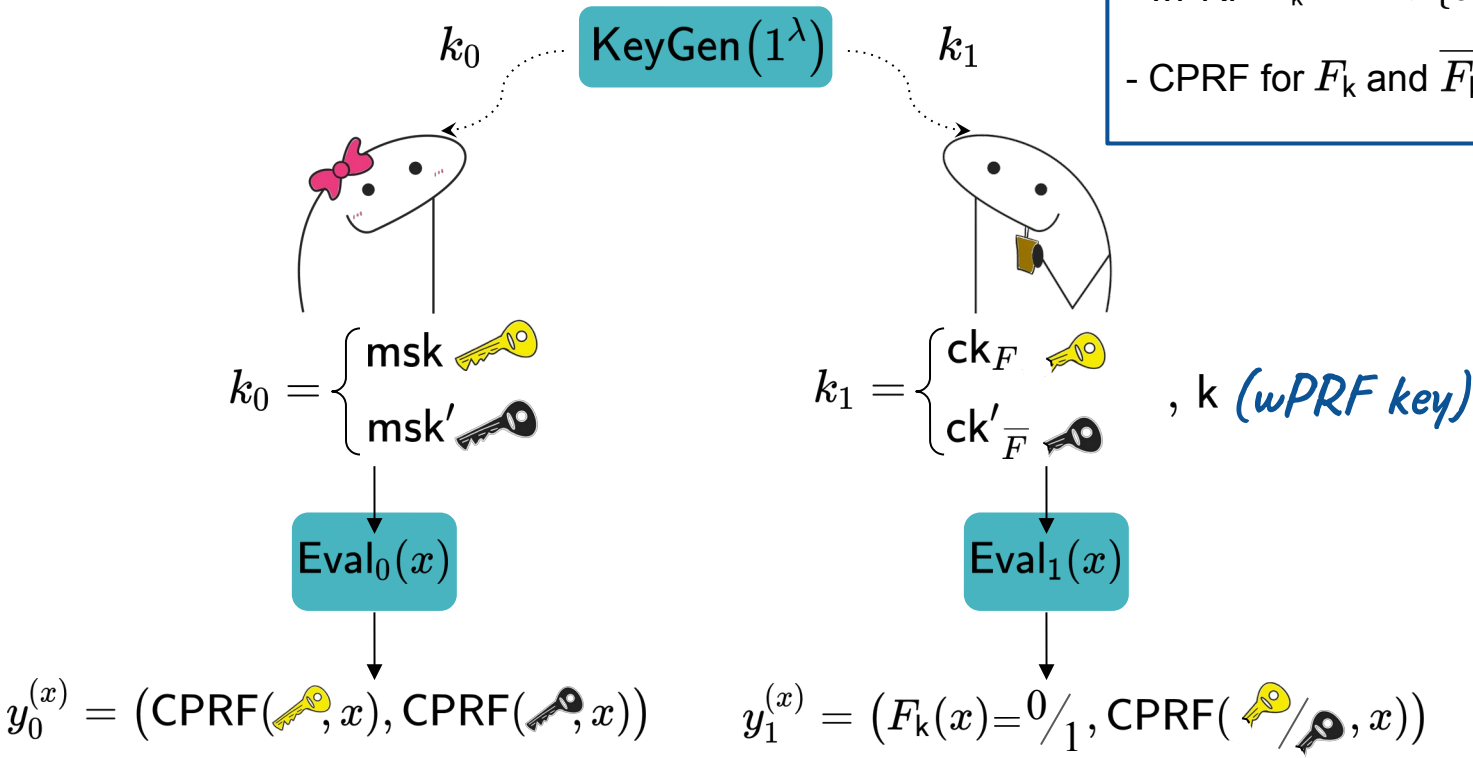
PCF for OT from Pseudorandomly Constrained PRFs

- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$



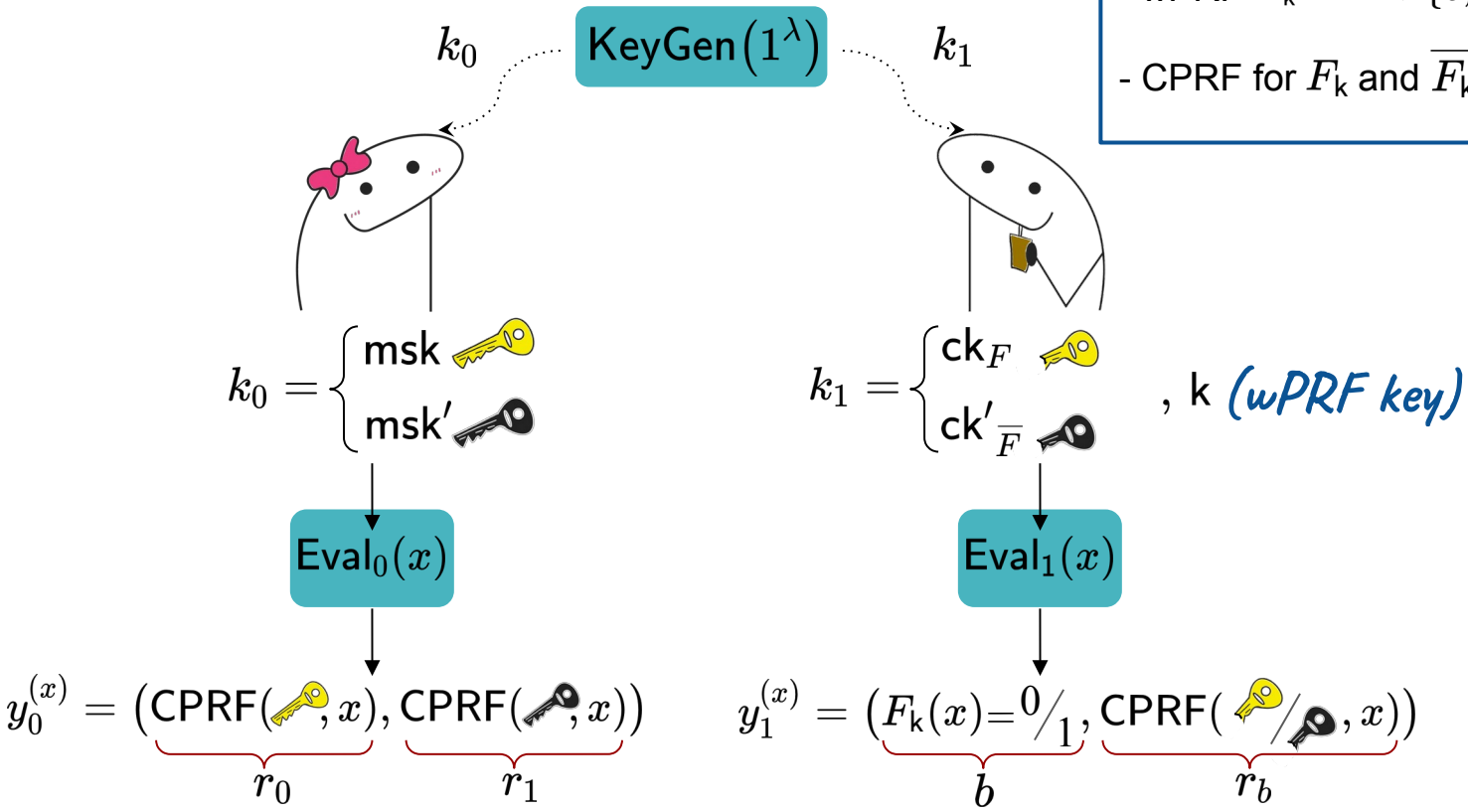
PCF for OT from Pseudorandomly Constrained PRFs

- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$



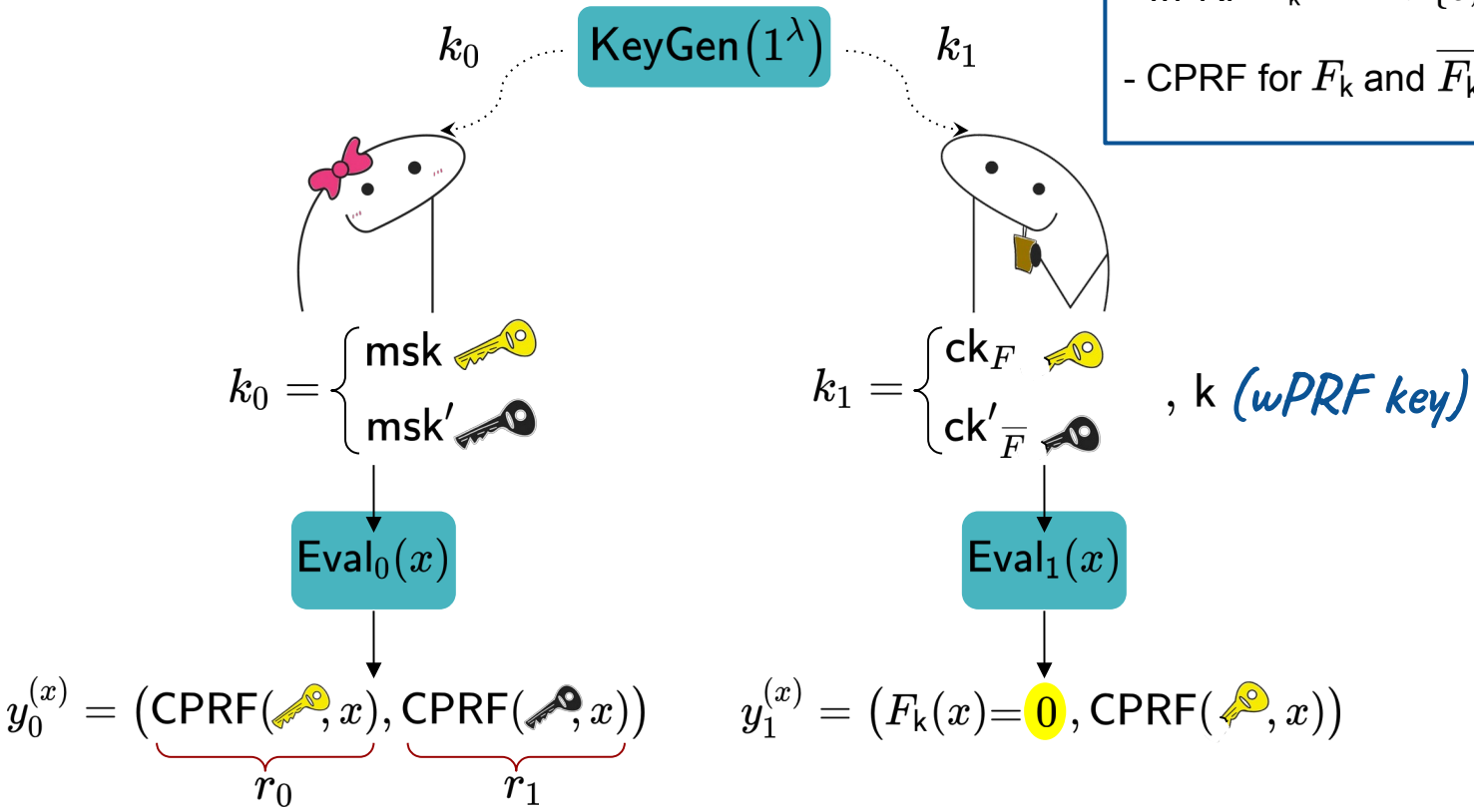
PCF for OT from Pseudorandomly Constrained PRFs

- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$



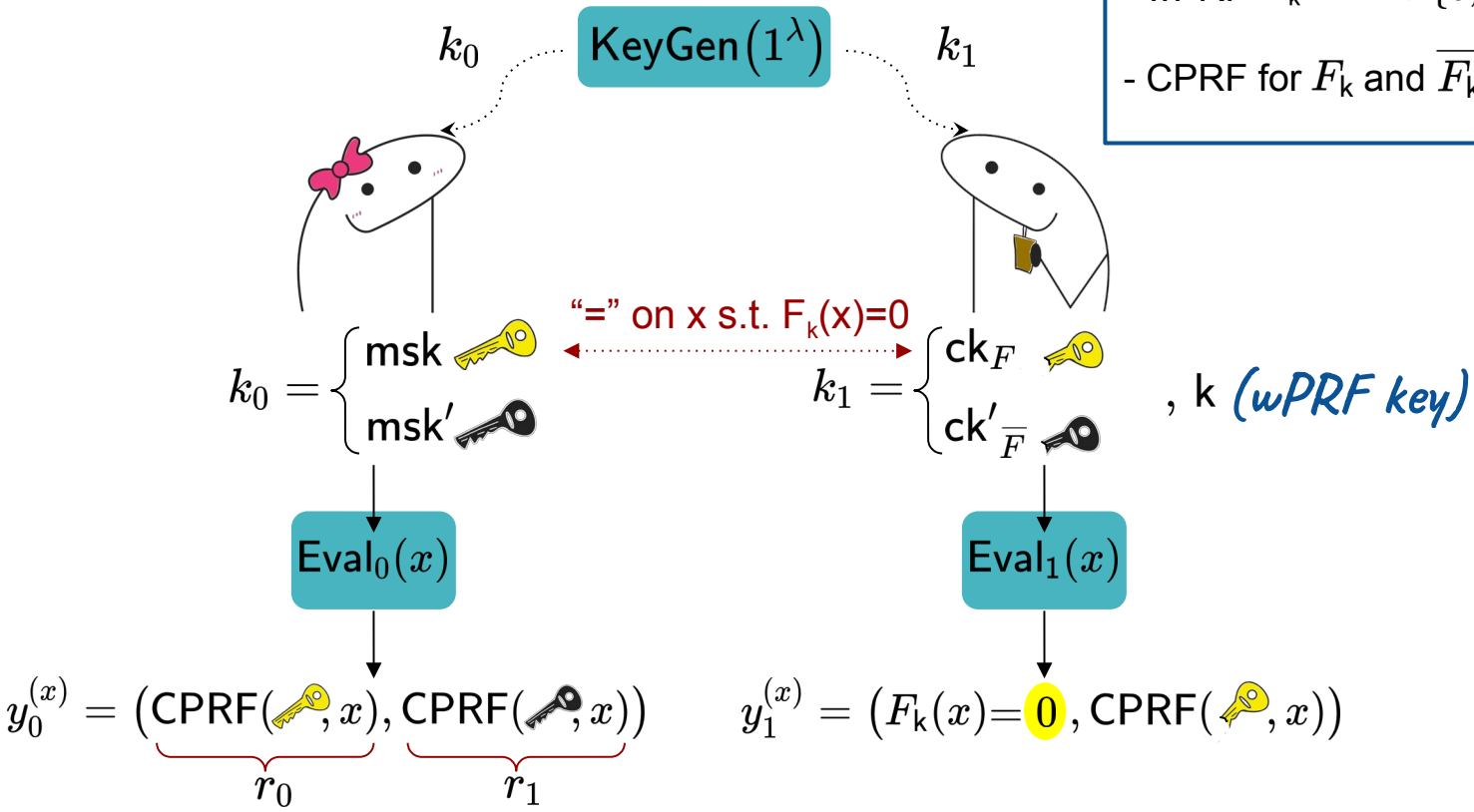
PCF for OT from Pseudorandomly Constrained PRFs

- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$



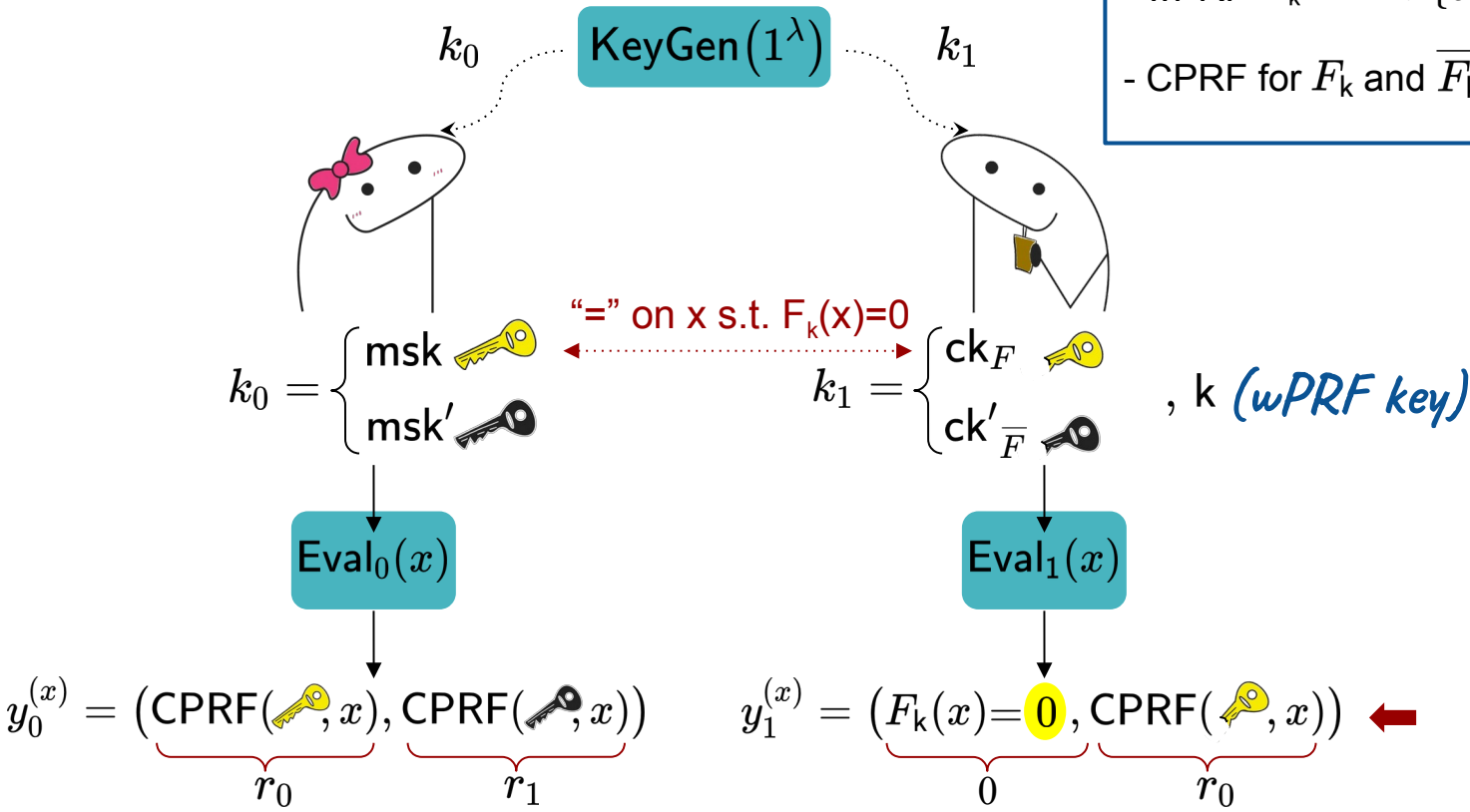
PCF for OT from Pseudorandomly Constrained PRFs

- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$



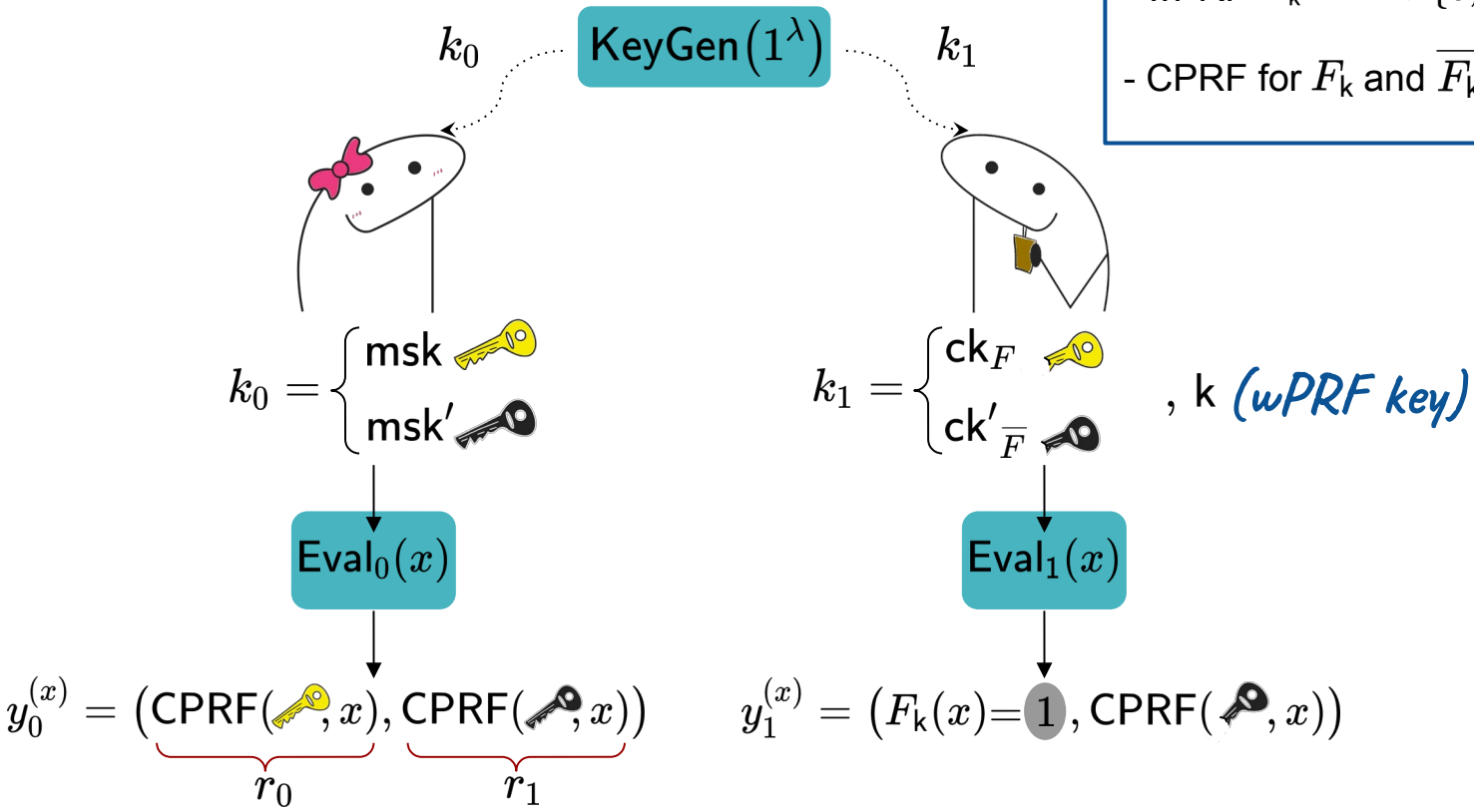
PCF for OT from Pseudorandomly Constrained PRFs

- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$



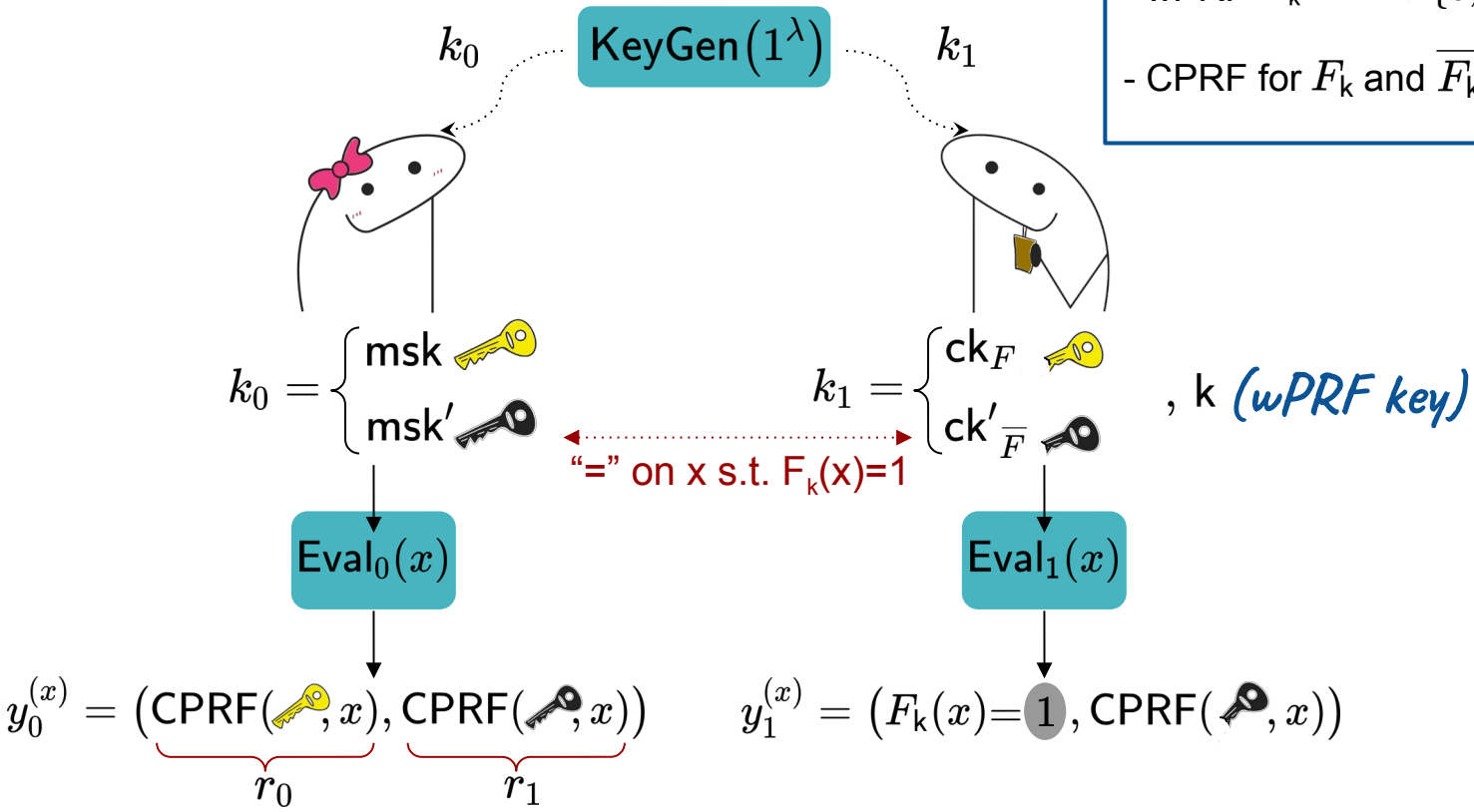
PCF for OT from Pseudorandomly Constrained PRFs

- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$



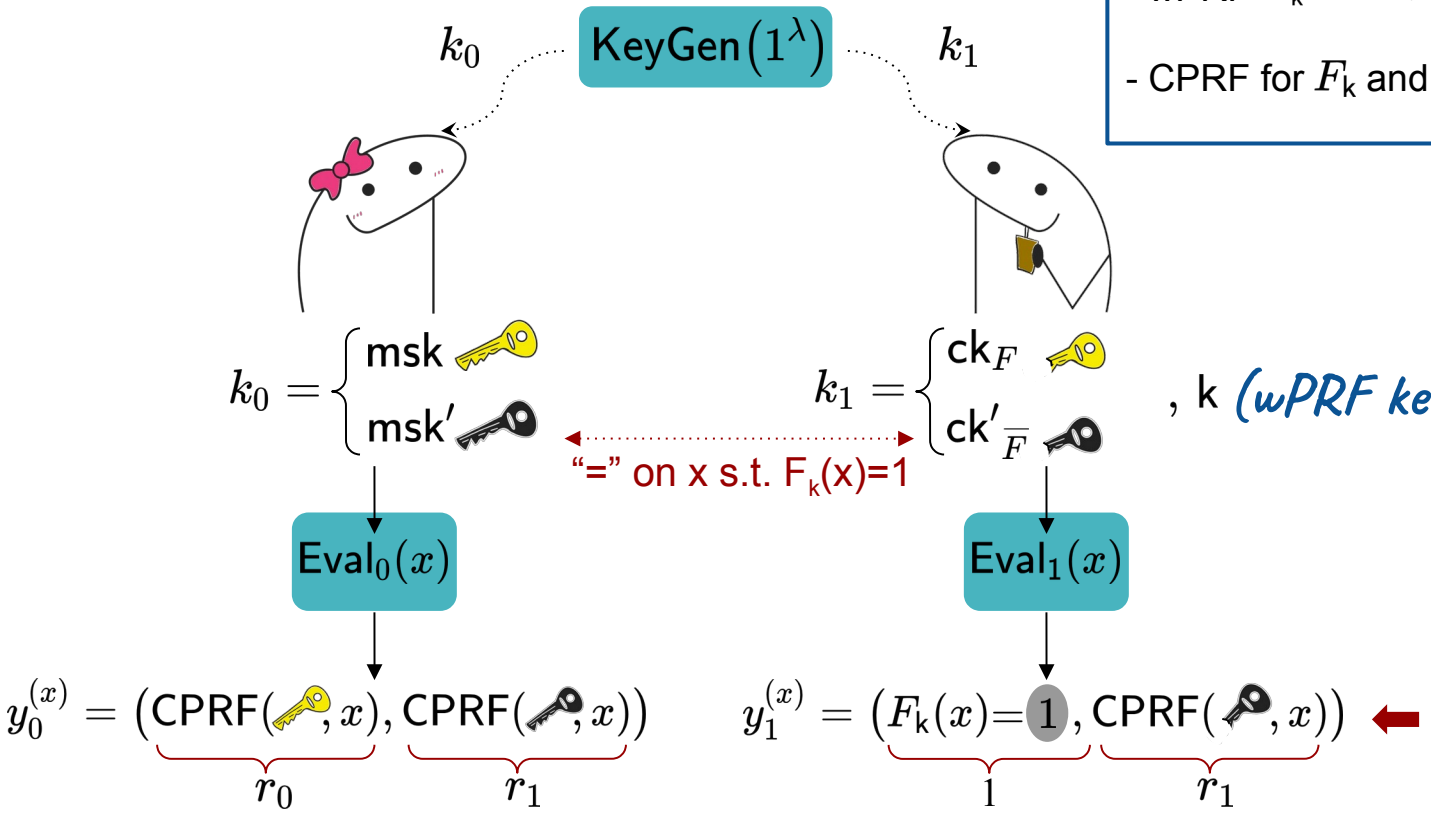
PCF for OT from Pseudorandomly Constrained PRFs

- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$



PCF for OT from Pseudorandomly Constrained PRFs

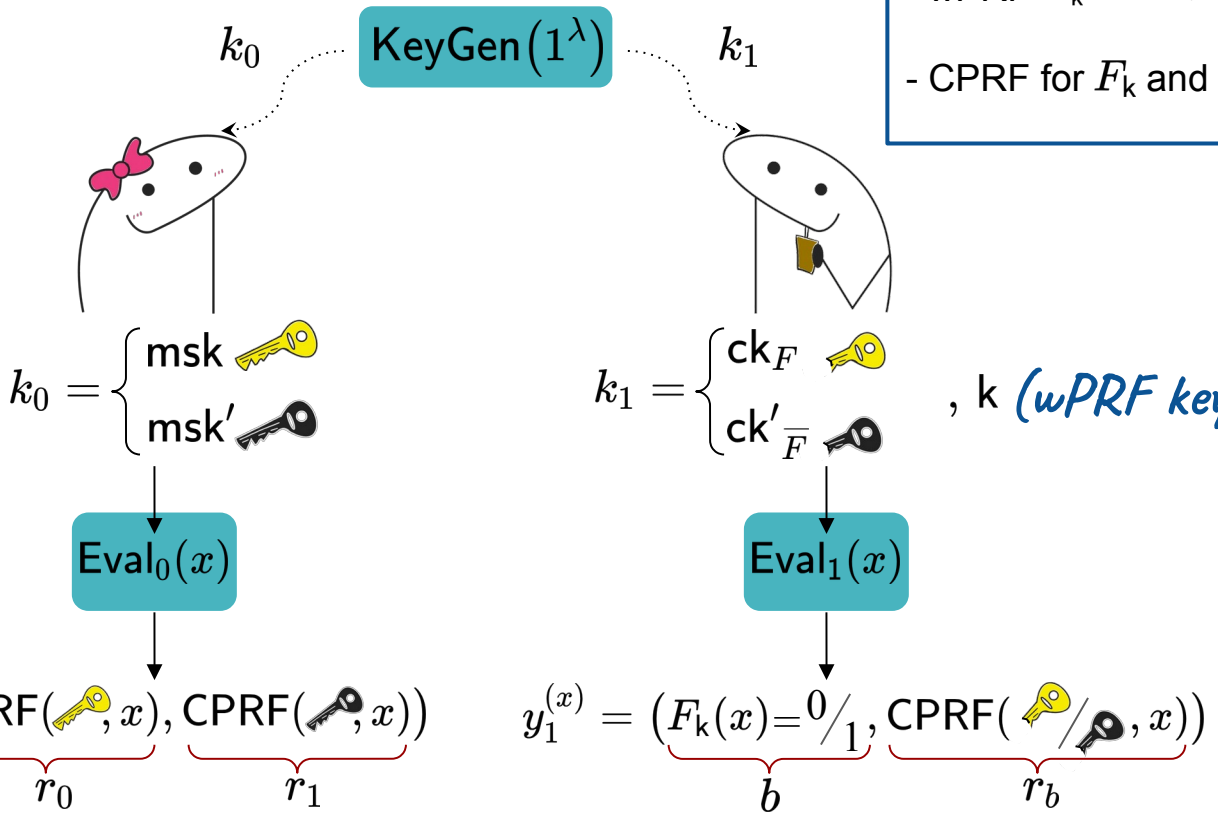
- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$



PCF for OT from Pseudorandomly Constrained PRFs

- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$

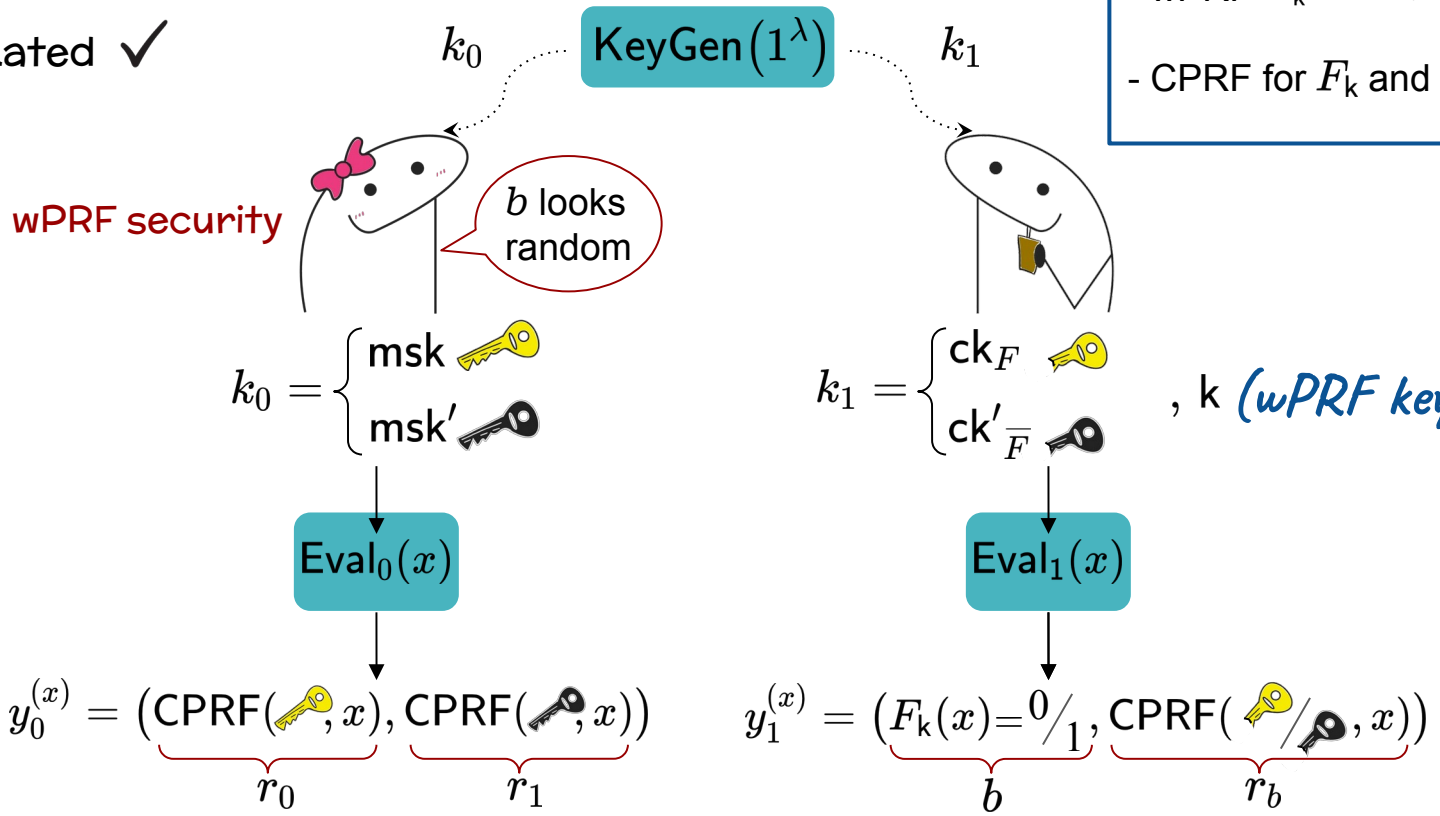
OT-correlated ✓



PCF for OT from Pseudorandomly Constrained PRFs

- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$

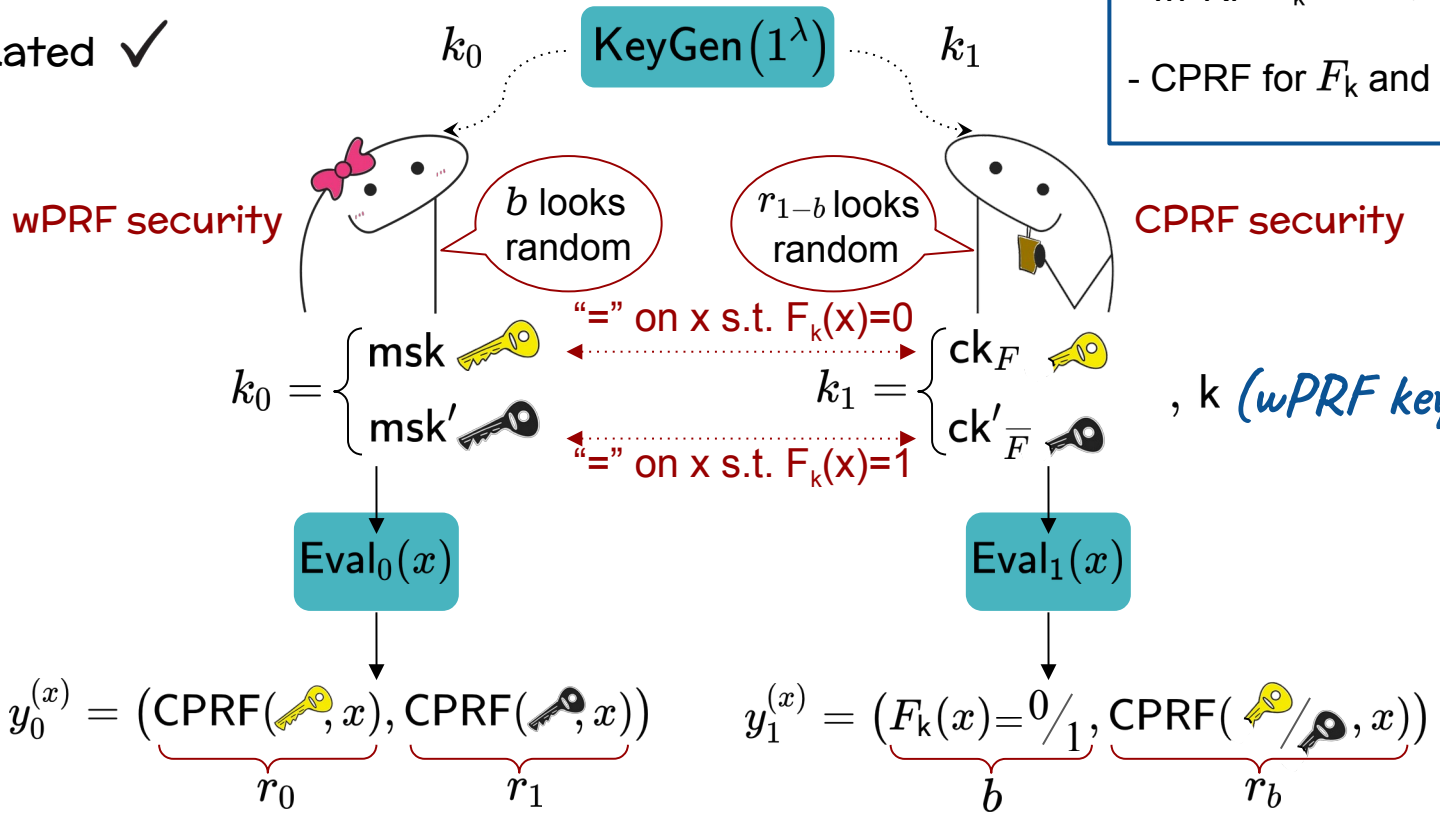
OT-correlated ✓



PCF for OT from Pseudorandomly Constrained PRFs

- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$

OT-correlated ✓

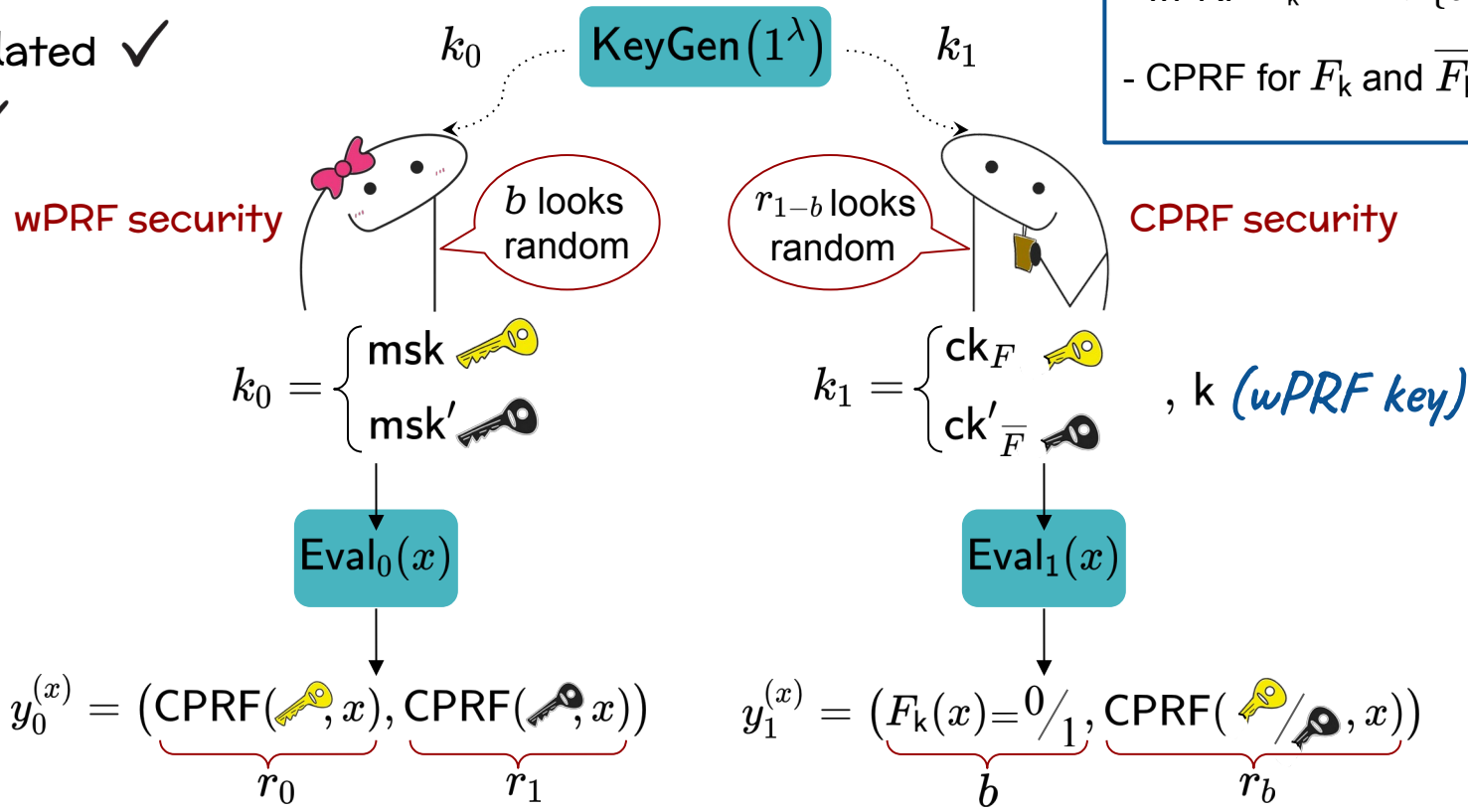


PCF for OT from Pseudorandomly Constrained PRFs

- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$

OT-correlated ✓

Secure ✓



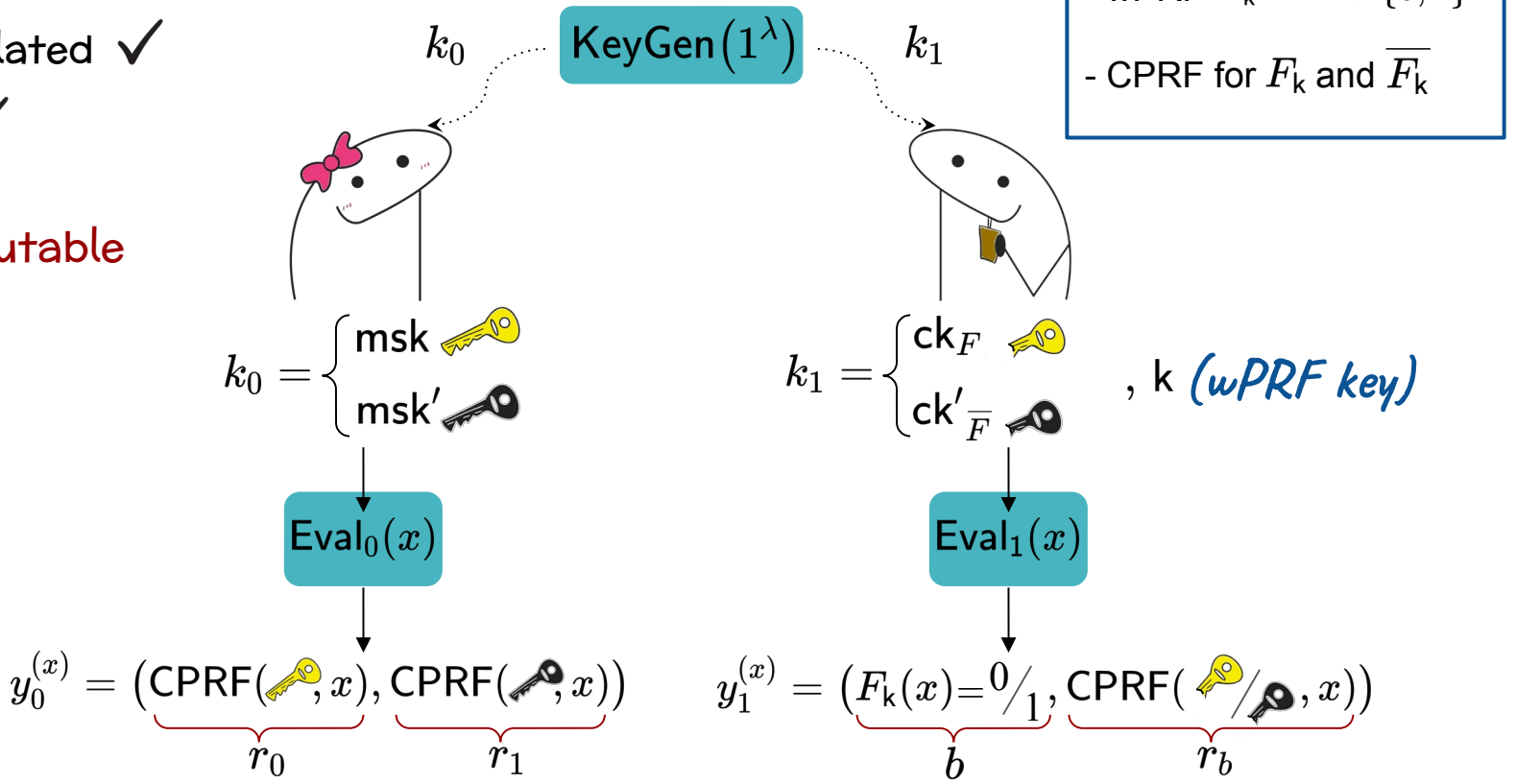
PCF for OT from Pseudorandomly Constrained PRFs

OT-correlated ✓

Secure ✓

Precomputable

- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$



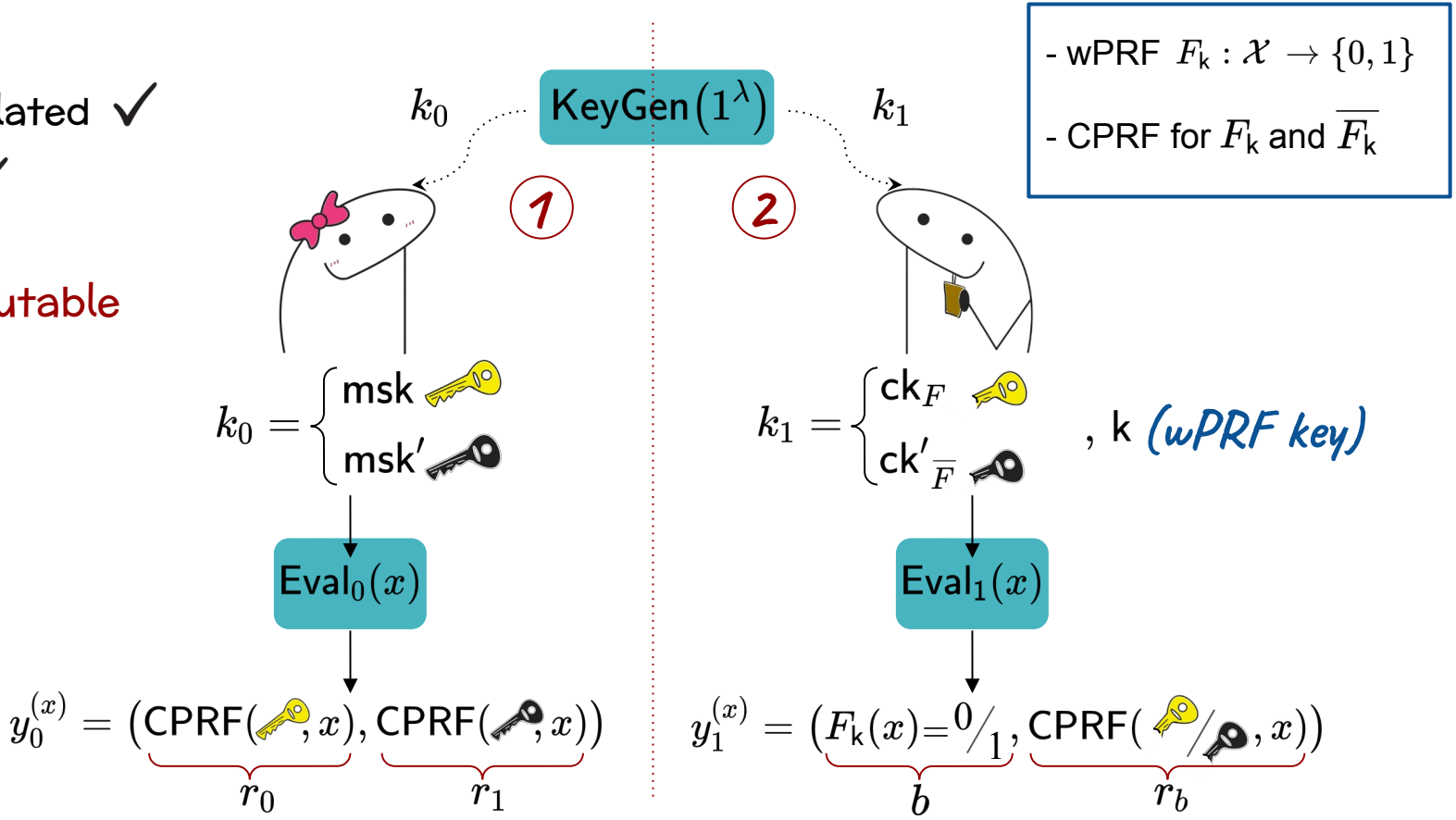
PCF for OT from Pseudorandomly Constrained PRFs

OT-correlated ✓

Secure ✓

Precomputable

- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$



GAR wPRF
as
a constraint

Goldreich-Applebaum-Raykov weak PRF

GAR weak PRF

$\vec{z} \in \{0,1\}^n$, $\vec{x} \in \{0,1\}^{\kappa+\tau}$

$$F\left(\vec{z}, \vec{x}\right) = \mathsf{XOR}_\kappa\text{-}\mathsf{MAJ}_\tau\left(\vec{z}\left[x_1\right], \ldots, \vec{z}\left[x_{\kappa+\tau}\right]\right) \in \{0,1\}$$

where

$$\mathsf{XOR}_\kappa\text{-}\mathsf{MAJ}_\tau\left(b_1, \ldots, b_{\kappa+\tau}\right) = \mathsf{XOR}_\kappa\left(b_1, \ldots, b_\kappa\right) \oplus \mathsf{MAJ}\left(b_{\kappa+1}, \ldots, b_{\kappa+\tau}\right)$$

Goldreich-Applebaum-Raykov weak PRF

GAR weak PRF

$\vec{z} \in \{0,1\}^n$, $\vec{x} \in \{0,1\}^{\kappa+\tau}$

$$F\left(\vec{z},\vec{x}\right) = \mathsf{XOR}_\kappa\text{-}\mathsf{MAJ}_\tau\left(\vec{z}\left[x_1\right],\ldots,\vec{z}\left[x_{\kappa+\tau}\right]\right) \in \{0,1\}$$

where

$$\mathsf{XOR}_\kappa\text{-}\mathsf{MAJ}_\tau\left(b_1,\ldots,b_{\kappa+\tau}\right) = \mathsf{XOR}_\kappa\left(b_1,\ldots,b_\kappa\right) \oplus \mathsf{MAJ}\left(b_{\kappa+1},\ldots,b_{\kappa+\tau}\right)$$

We find two polynomials P and $\overline{P}$ over R_q such that

$$P_{\kappa,\tau}\left(\vec{x},\vec{z}\right) = 0 \iff F\left(\vec{x},\vec{z}\right) = 0$$

$$\overline{P}_{\kappa,\tau}\left(\vec{x},\vec{z}\right) = 0 \iff F\left(\vec{x},\vec{z}\right) = 1$$

Degree $O(\kappa+\tau)$