Post-Quantum Public-Key Pseudorandom Correlation Functions for OT

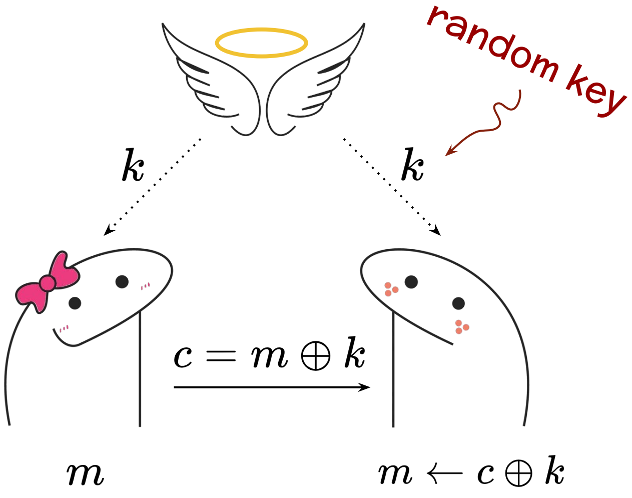
Shweta Agrawal[1], Kaartik Bhushan[2], Geoffroy Couteau[2], and

Mahshid Riahinia[3]

[1] IIT Madras, India.
[2] Université Paris Cité, CNRS, IRIF, Paris, France.
[3] ENS, CNRS, visitor at IRIF, Paris, France.

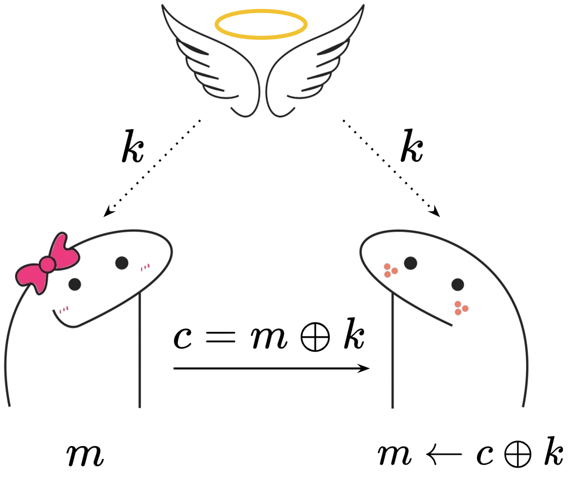
Introduction: Correlated Randomness

Introduction: Correlated Randomness



Symmetric Encryption

Introduction: Correlated Randomness



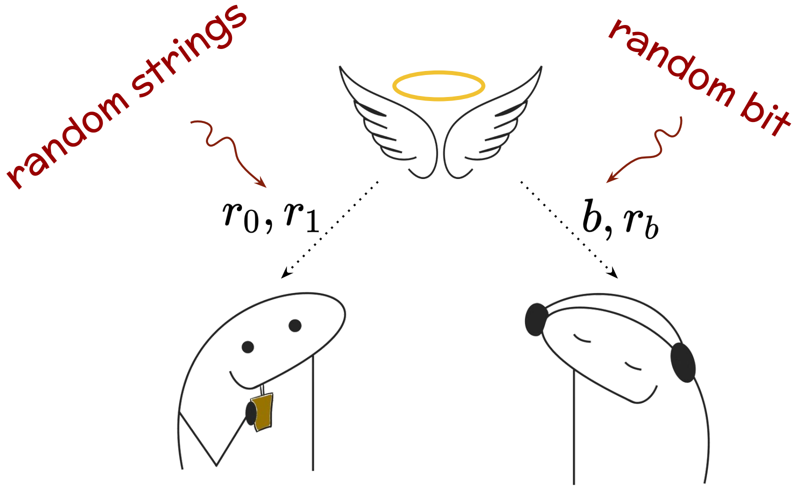
k k

$c = m \oplus k$

m

$m \leftarrow c \oplus k$

Symmetric Encryption



random strings

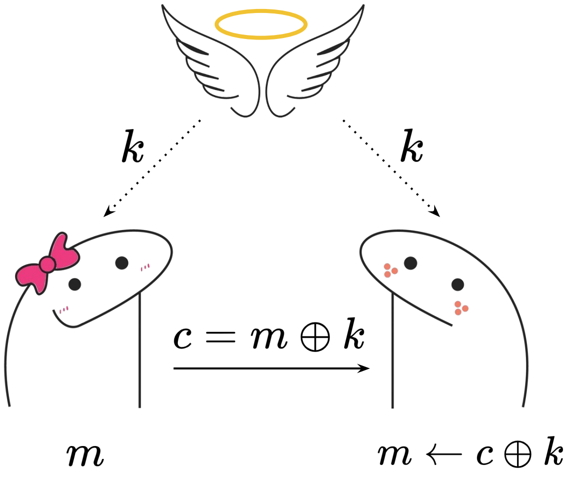
random bit

r_0, r_1

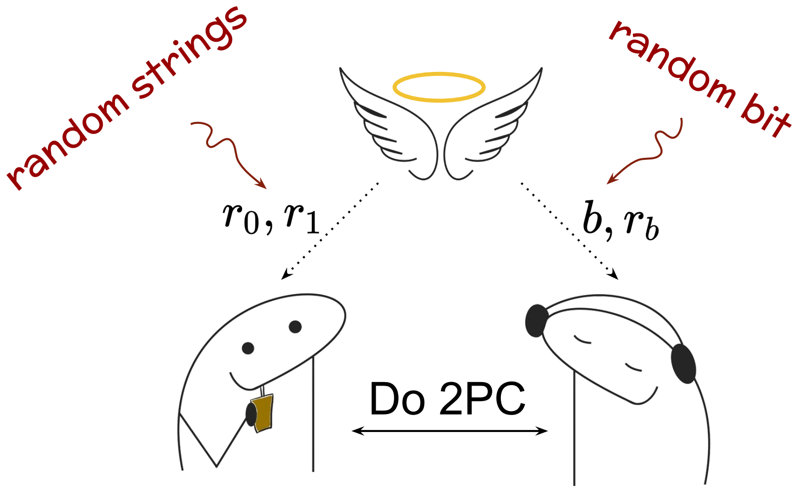
b, r_b

Oblivious Transfer (OT) Correlation

Introduction: Correlated Randomness



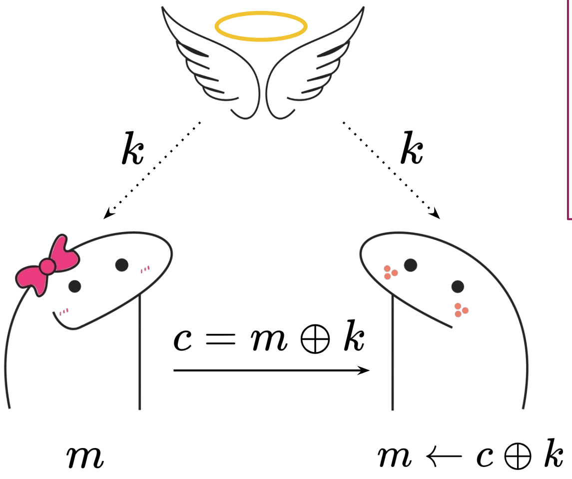
Symmetric Encryption



Oblivious Transfer (OT) Correlation

2PC: 2-Party Computation

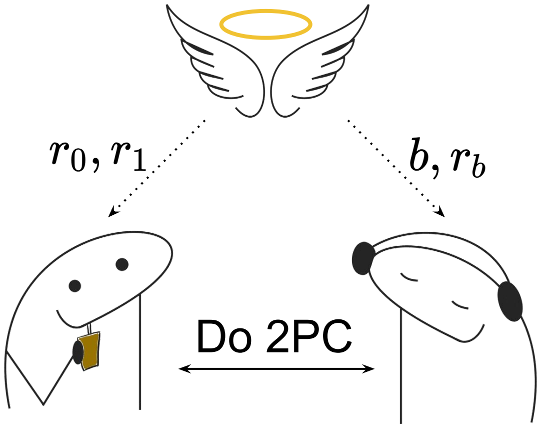
Introduction: Correlated Randomness



Symmetric Encryption

Secure Computation

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



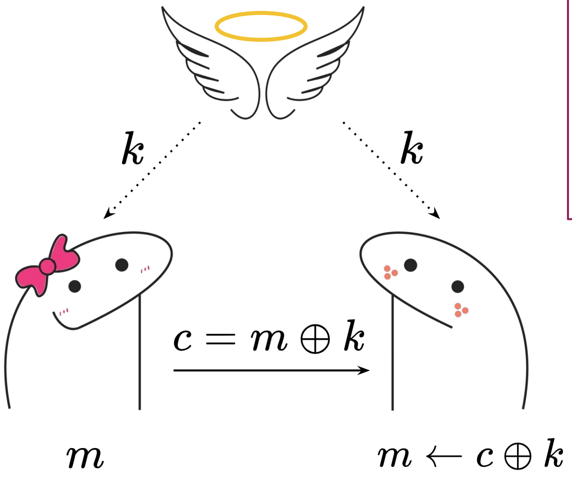
Oblivious Transfer (OT) Correlation

2PC: 2-Party Computation

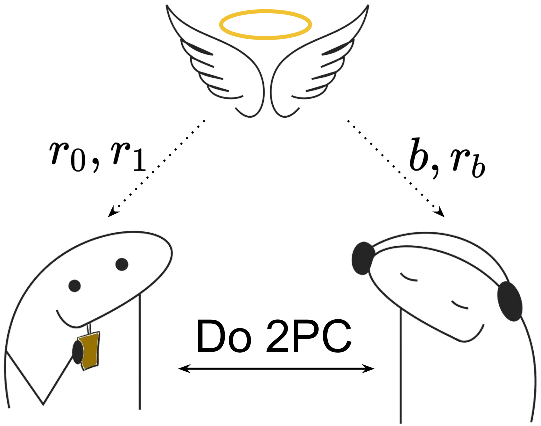
Introduction: Correlated Randomness

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

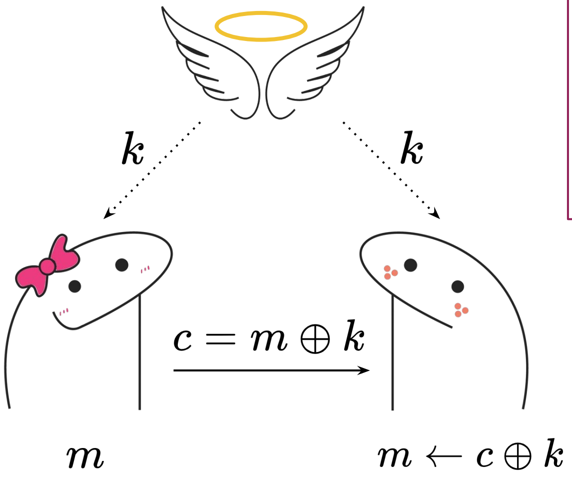
Secure Computation

2PC: 2-Party Computation

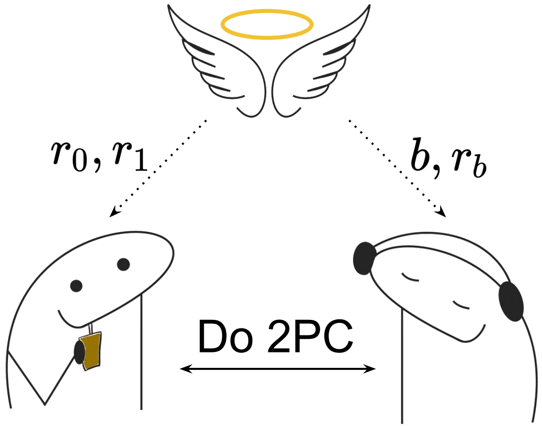
Introduction: Correlated Randomness

Secure Computation

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



Symmetric Encryption



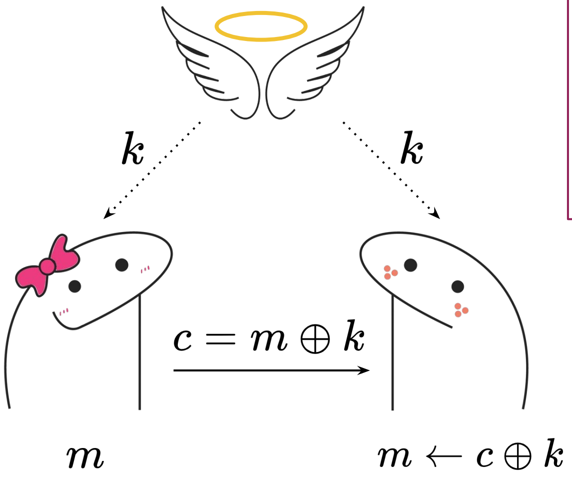
Oblivious Transfer (OT) Correlation

Secure Communication

Fast & Info-Theoretic Secure Computation

2PC: 2-Party Computation

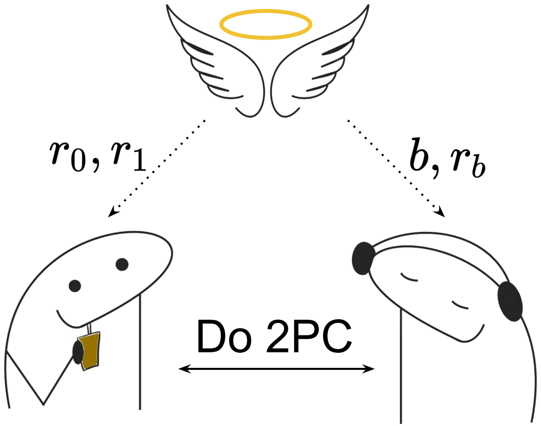
Introduction: Correlated Randomness



Symmetric Encryption

Secure Computation

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



Oblivious Transfer (OT) Correlation

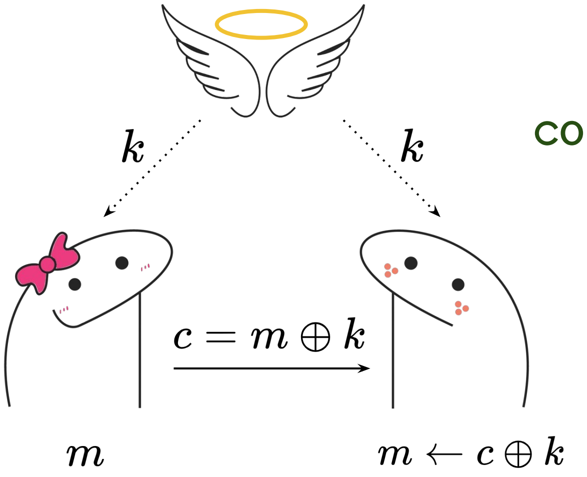
Secure Communication

Fast & Info-Theoretic Secure Computation

2PC: 2-Party Computation

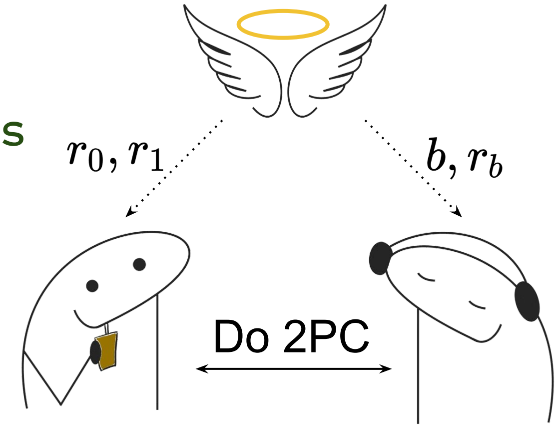
f has n gates : O(n) OT pairs -> send 4 bits per AND

Introduction: Correlated Randomness



Symmetric Encryption

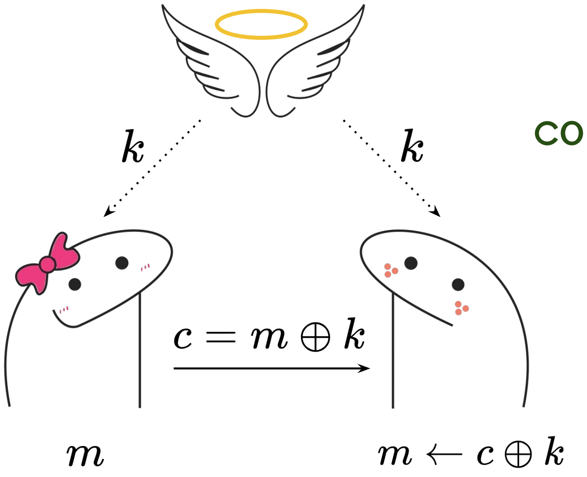
Can we generate correlated randomness on demand?



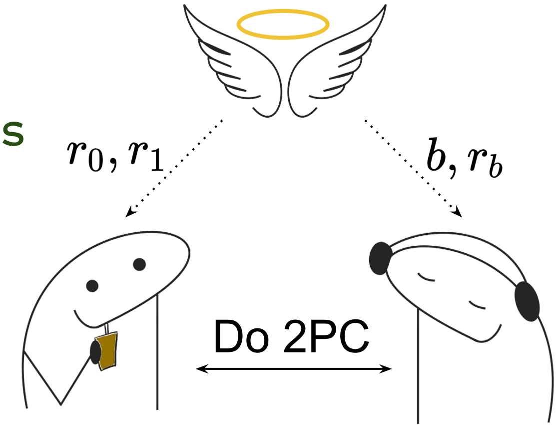
Oblivious Transfer (OT) Correlation

Introduction: Correlated Randomness

Can we generate correlated randomness on demand?



Symmetric Encryption

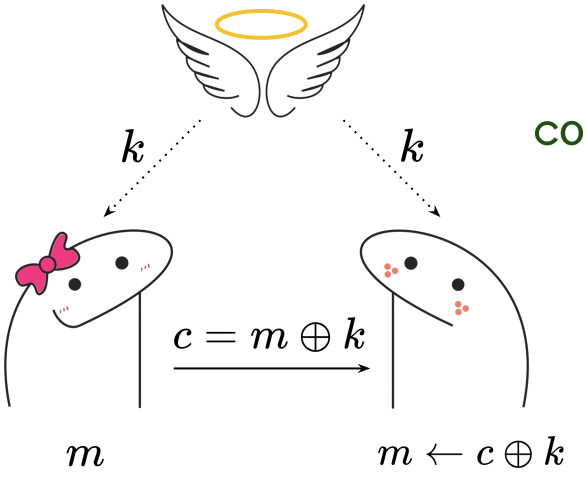


Oblivious Transfer (OT) Correlation

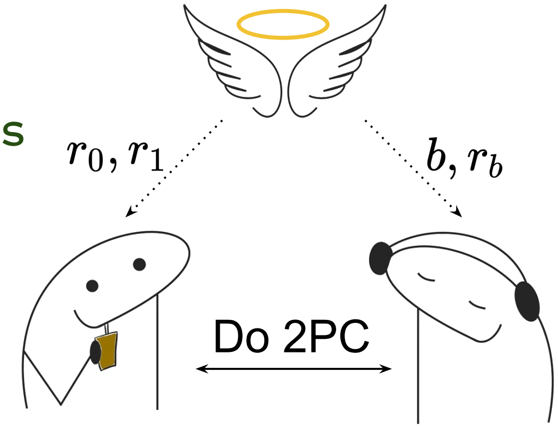
[BCGIKS 19] Pseudorandom Correlation Generators (PCGs)
[BCGIKS 20] Pseudorandom Correlation Functions (PCFs)

Introduction: Correlated Randomness

Can we generate correlated randomness on demand?



Symmetric Encryption



Oblivious Transfer (OT) Correlation

[BCGIKS 19] Pseudorandom Correlation Generators (PCGs)

➡ [BCGIKS 20] Pseudorandom Correlation Functions (PCFs)

Pseudorandom Correlation Functions

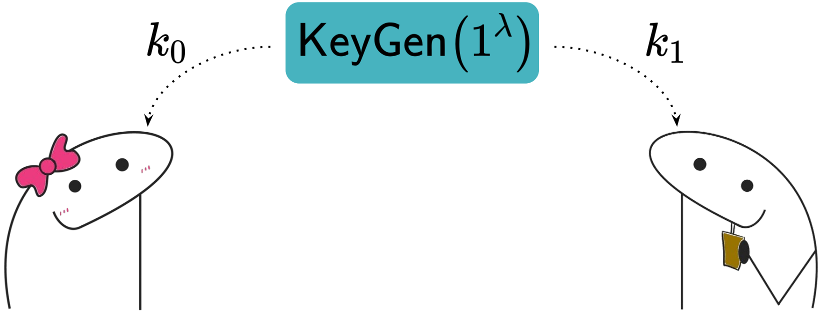
Definition

Pseudorandom Correlation Functions [BCGIKS20]

on-demand generation
of
correlated randomness

Pseudorandom Correlation Functions [BCGIKS20]

on-demand generation
of
correlated randomness



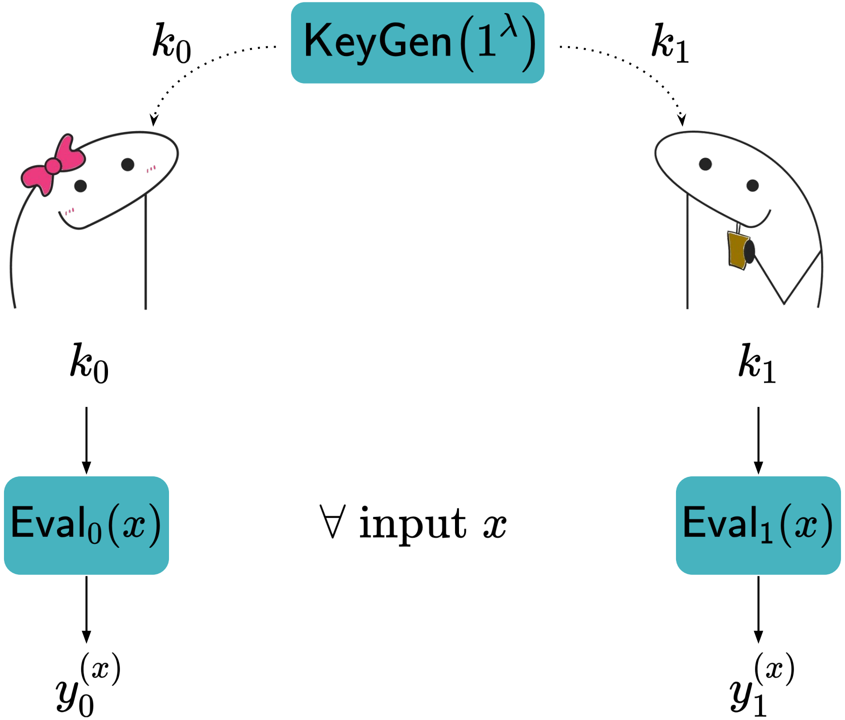
$\mathsf{KeyGen}(1^\lambda)$

k_0

k_1

Pseudorandom Correlation Functions [BCGIKS20]

on-demand generation
of
correlated randomness



$\mathsf{KeyGen}(1^\lambda)$

k_0 k_1

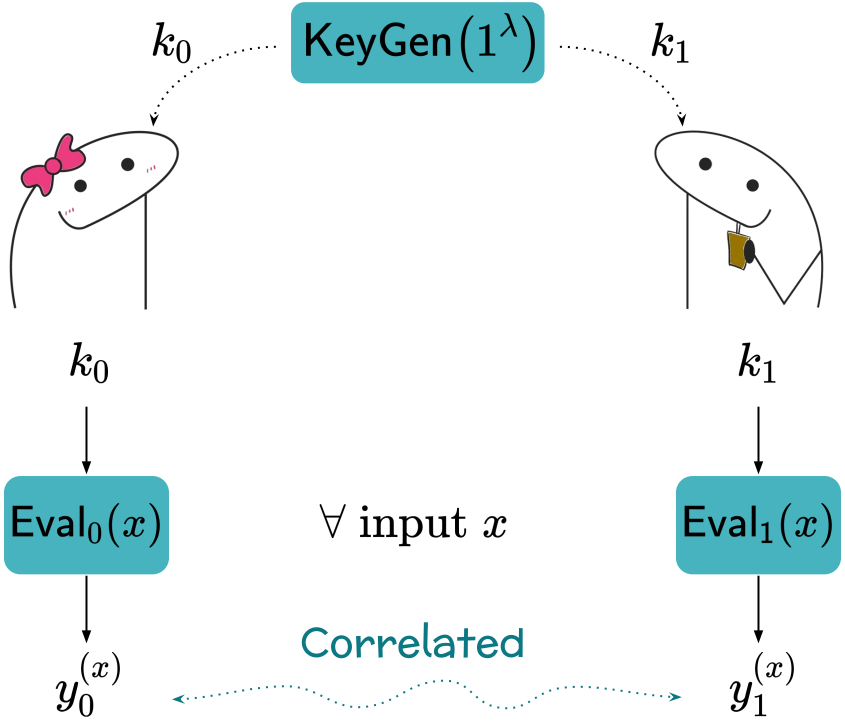
k_0 k_1

$\mathsf{Eval}_0(x)$ $\forall$ input x $\mathsf{Eval}_1(x)$

$y_0^{(x)}$ $y_1^{(x)}$

Pseudorandom Correlation Functions [BCGIKS20]

on-demand generation
of
correlated randomness



KeyGen(1^λ)

k_0 k_1

k_0 k_1

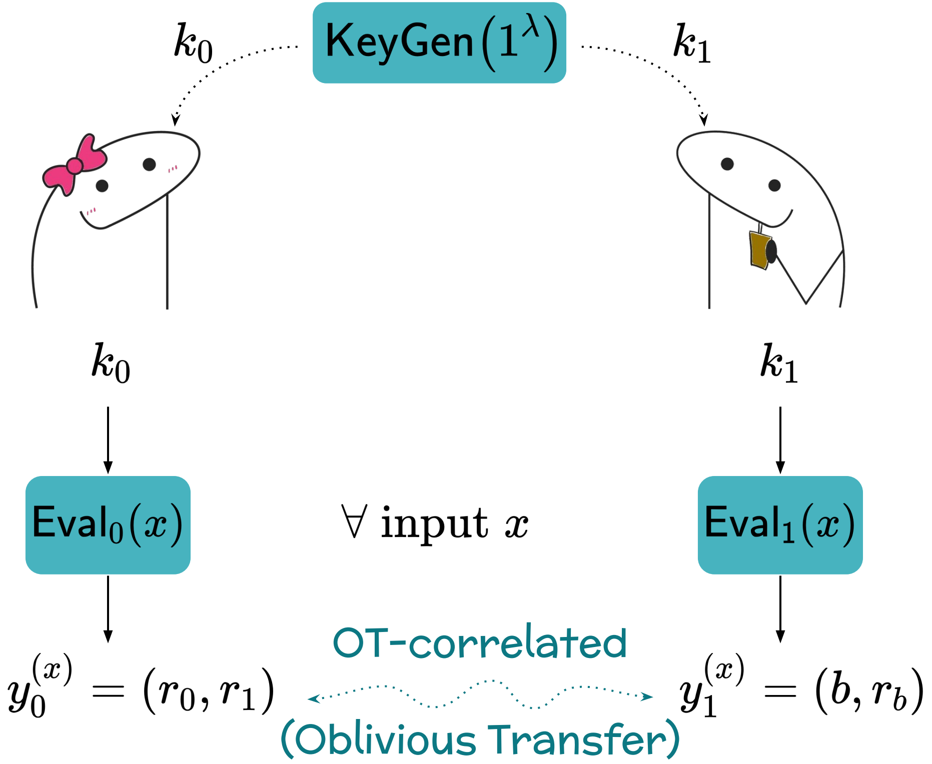
Eval$_0(x)$ $\forall$ input x Eval$_1(x)$

Correlated

$y_0^{(x)}$ $y_1^{(x)}$

Pseudorandom Correlation Functions [BCGIKS20]

on-demand generation
of
correlated randomness



KeyGen(1^λ)

k_0

k_1

k_0

k_1

Eval$_0(x)$

$\forall$ input x

Eval$_1(x)$

$y_0^{(x)} = (r_0, r_1)$

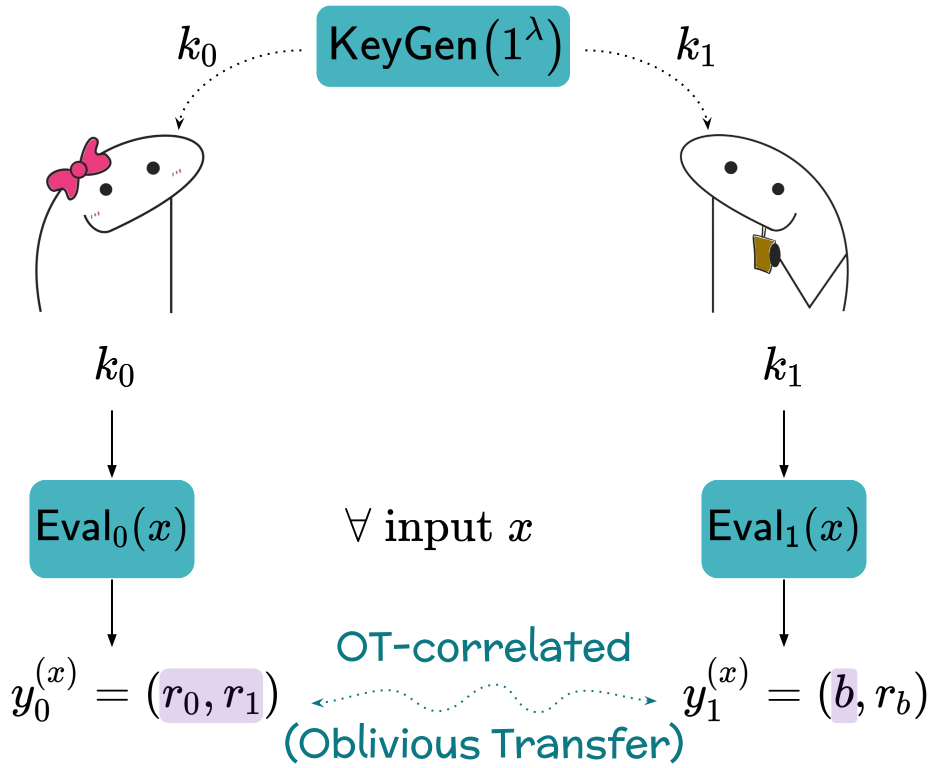
OT-correlated

(Oblivious Transfer)

$y_1^{(x)} = (b, r_b)$

Pseudorandom Correlation Functions [BCGIKS20]

on-demand generation
of
correlated randomness



k_0 KeyGen(1^λ) k_1

k_0 k_1

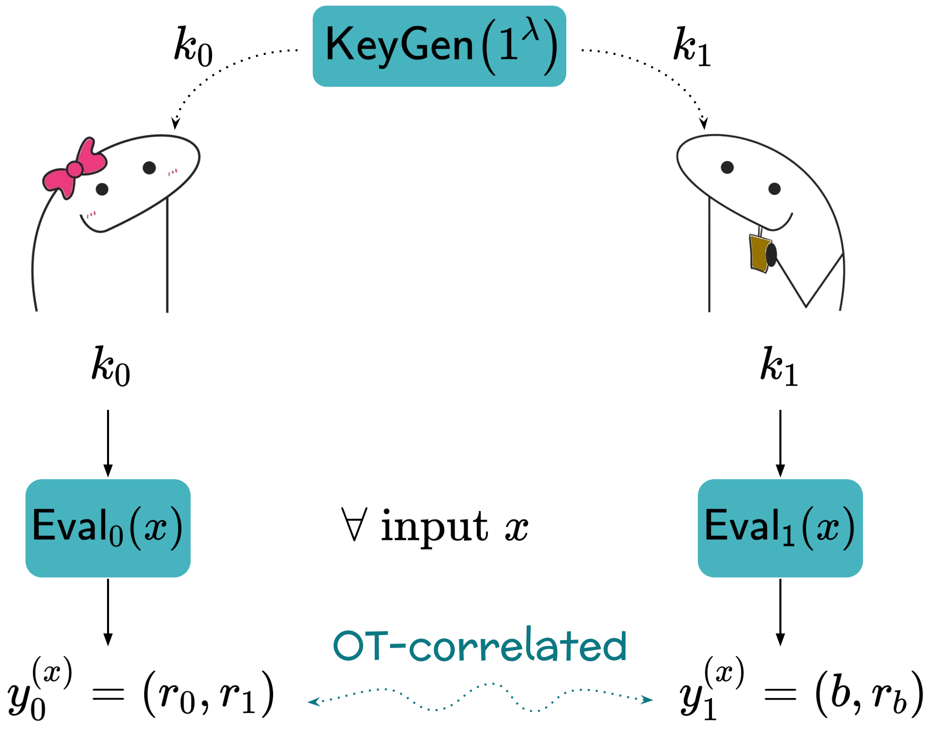
Eval$_0(x)$ $\forall$ input x Eval$_1(x)$

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

Pseudorandom Correlation Functions [BCGIKS20]

security:

things look random up to correlation



$\mathsf{KeyGen}(1^\lambda)$

k_0 k_1

k_0 k_1

$\mathsf{Eval}_0(x)$ $\forall$ input x $\mathsf{Eval}_1(x)$

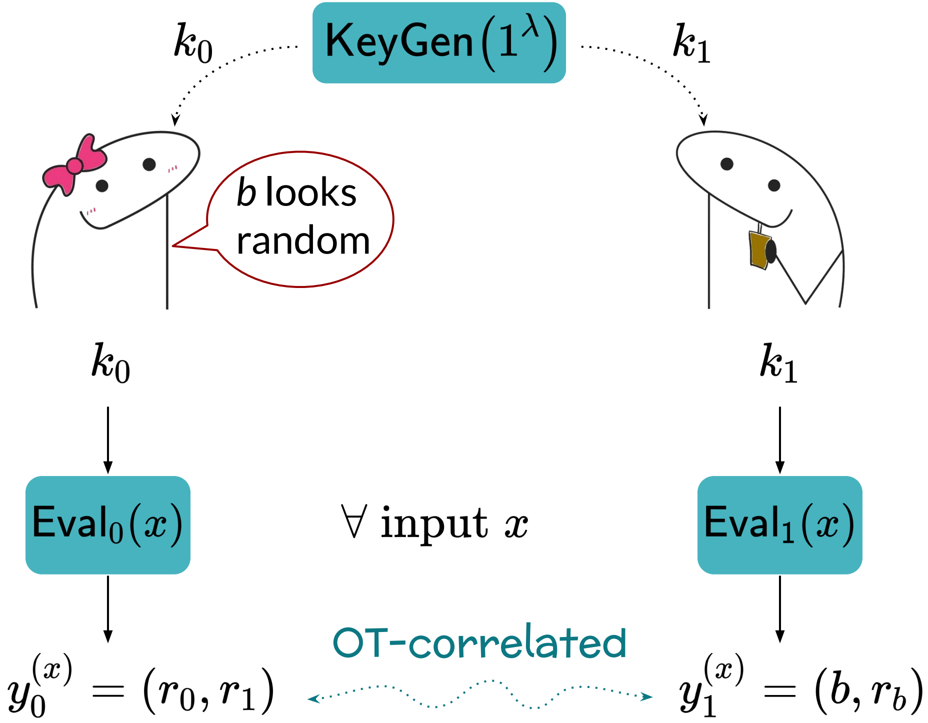
OT-correlated

$y_0^{(x)} = (r_0, r_1)$ $y_1^{(x)} = (b, r_b)$

Pseudorandom Correlation Functions [BCGIKS20]

security:

things look random up to correlation



KeyGen(1^λ)

k_0

k_1

b looks random

k_0

k_1

Eval$_0(x)$

$\forall$ input x

Eval$_1(x)$

OT-correlated

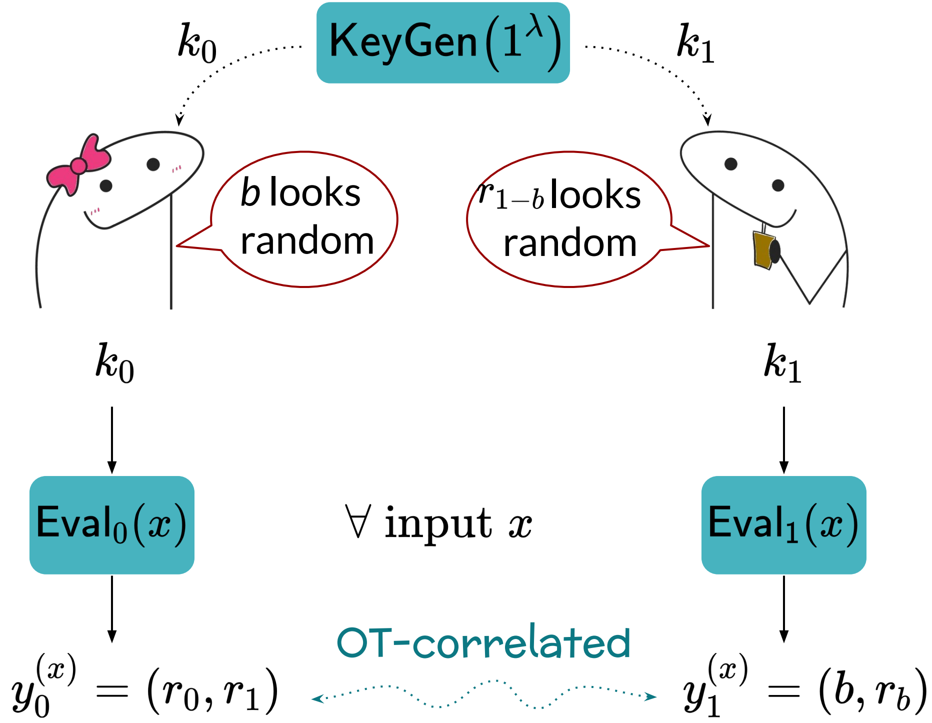
$y_0^{(x)} = (r_0, r_1)$

$y_1^{(x)} = (b, r_b)$

Pseudorandom Correlation Functions [BCGIKS20]

security:

things look random up to correlation



KeyGen(1^λ)

k_0

k_1

b looks random

r_{1-b} looks random

k_0

k_1

Eval$_0(x)$

$\forall$ input x

Eval$_1(x)$

$y_0^{(x)} = (r_0, r_1)$

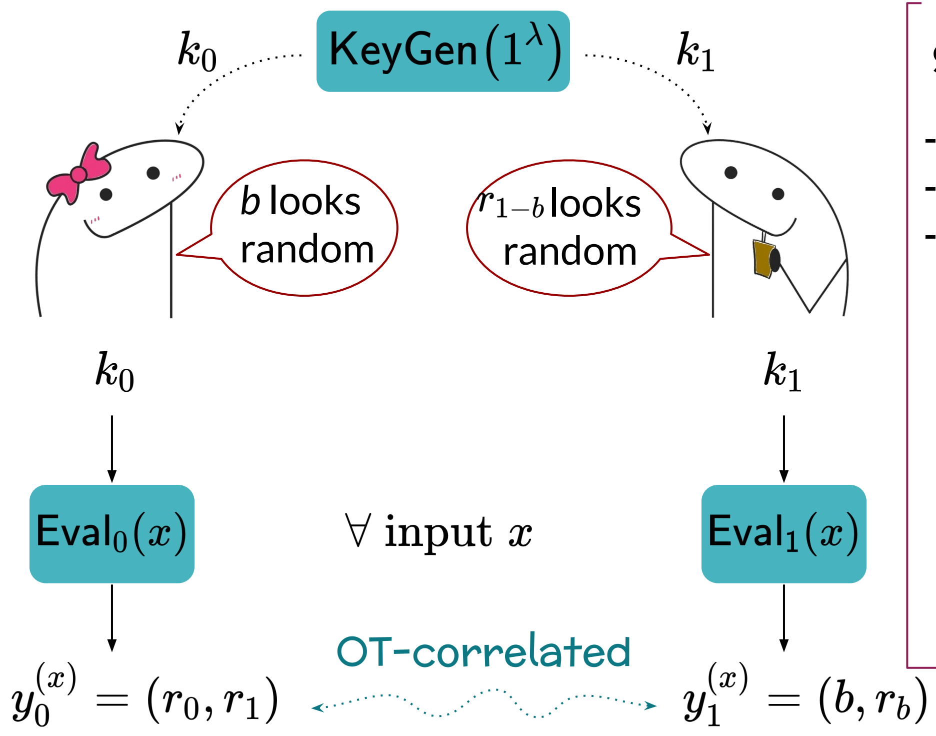
OT-correlated

$y_1^{(x)} = (b, r_b)$

Pseudorandom Correlation Functions [BCGIKS20]

security:

things look random up to correlation



k_0 KeyGen(1^λ) k_1

b looks random

r_{1-b} looks random

k_0 k_1

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

OT-correlated

$y_0^{(x)} = (r_0, r_1)$ $y_1^{(x)} = (b, r_b)$

Application

Secure Computation

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

[GMW87]

|f|=n :

O(n) OT correlations

⇓

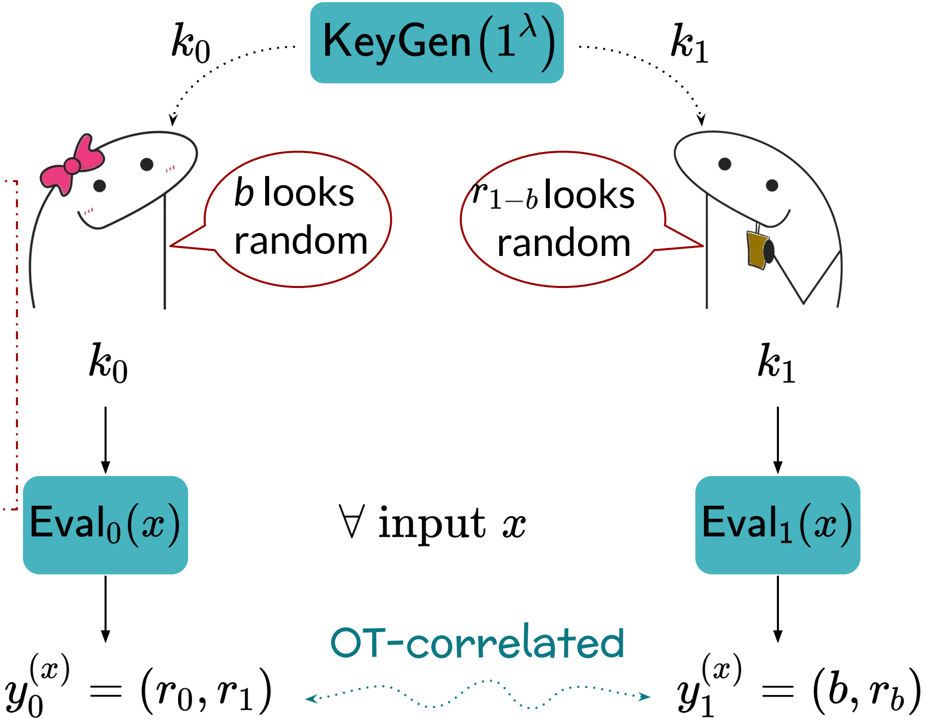
send 4 bits/AND

Pseudorandom Correlation Functions [BCGIKS20]

Our contribution:

Efficient* Post-Quantum Public-Key PCF
for
OT Correlations

* Efficiency ~ #OT per second



$\mathsf{KeyGen}(1^\lambda)$

k_0 k_1

k_0 → $\mathsf{Eval}_0(x)$

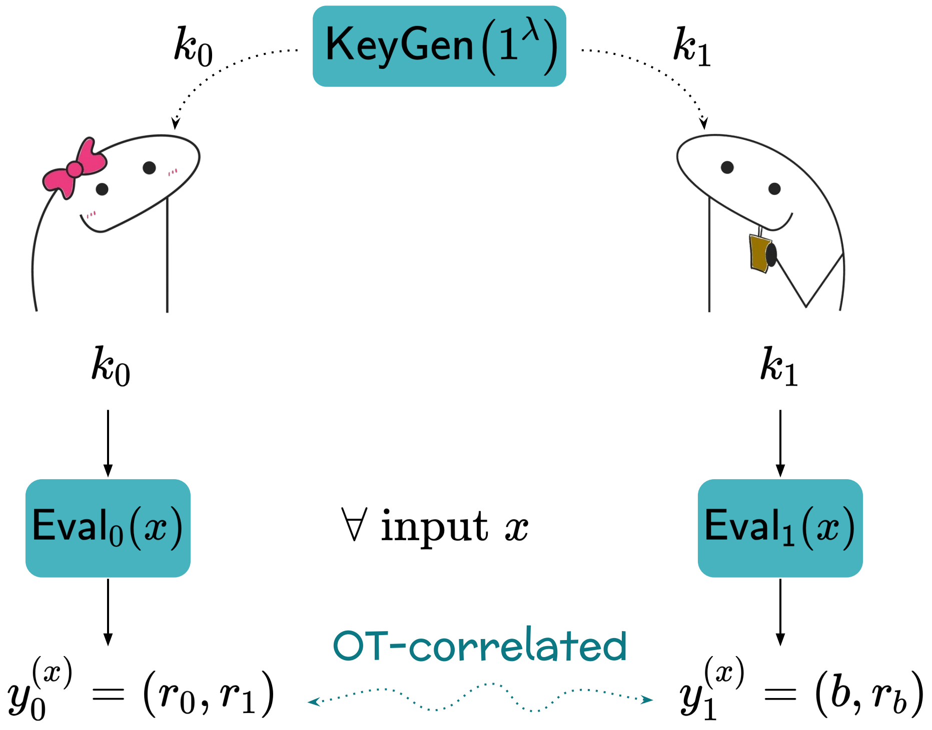
k_1 → $\mathsf{Eval}_1(x)$

$\forall$ input x

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

Public-Key Pseudorandom Correlation Functions

Pseudorandom Correlation Functions [BCGIKS20]



$\mathsf{KeyGen}(1^\lambda)$

k_0 k_1

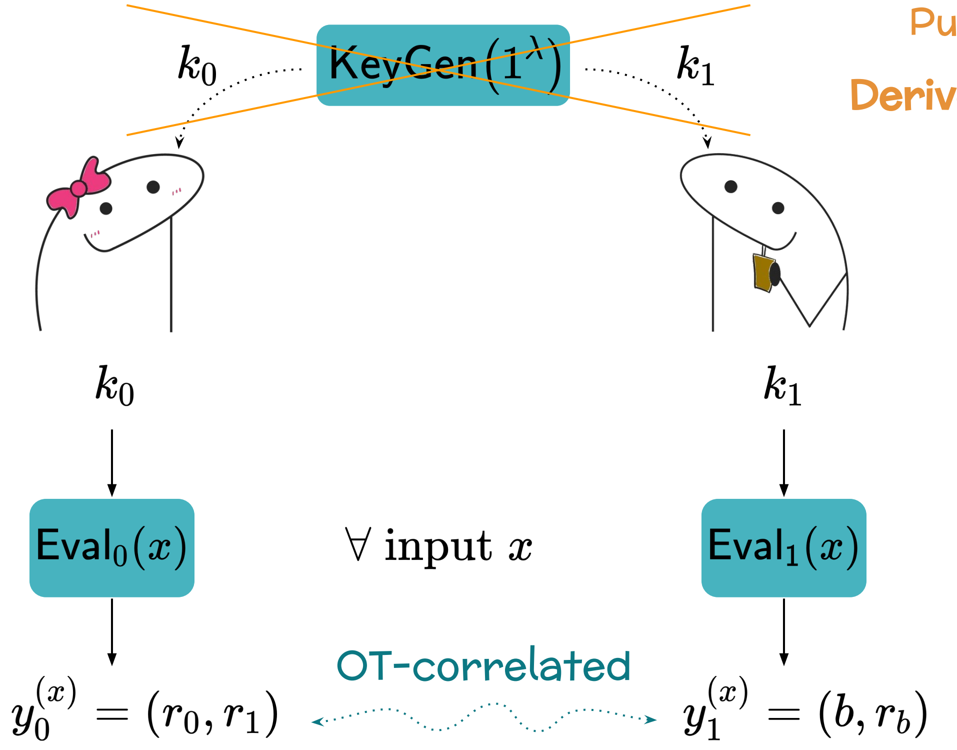
k_0 k_1

$\mathsf{Eval}_0(x)$ $\forall$ input x $\mathsf{Eval}_1(x)$

OT-correlated

$y_0^{(x)} = (r_0, r_1)$ $y_1^{(x)} = (b, r_b)$

Public-Key Pseudorandom Correlation Functions [BCMPR24]



~~$\mathsf{KeyGen}(1^\lambda)$~~

k_0 k_1

k_0 k_1

$\mathsf{Eval}_0(x)$ $\forall$ input x $\mathsf{Eval}_1(x)$

OT-correlated

$y_0^{(x)} = (r_0, r_1)$ $y_1^{(x)} = (b, r_b)$

Public-Key PCF:

Derive keys publicly

Public-Key Pseudorandom Correlation Functions [BCMPR24]

Public-Key Pseudorandom Correlation Functions [BCMP**R**24]

Key Derivation

Evaluation

Public-Key Pseudorandom Correlation Functions [BCMPR24]

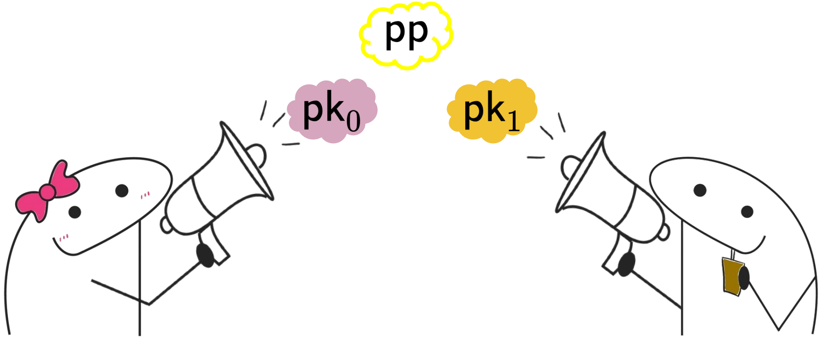
pp

Key Derivation

Evaluation

Public-Key Pseudorandom Correlation Functions [BCMPR24]

Key Derivation



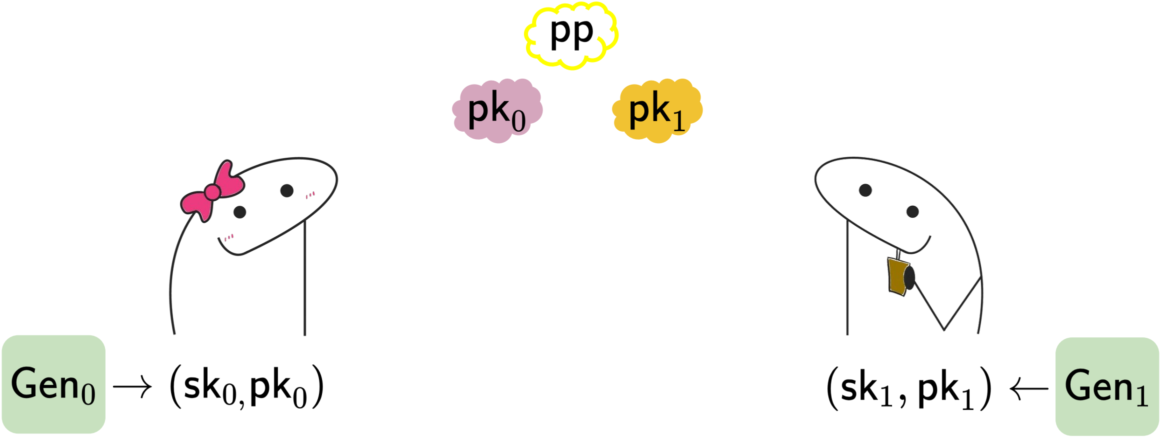
$\mathsf{Gen}_0 \rightarrow (\mathsf{sk}_0, \mathsf{pk}_0)$

$(\mathsf{sk}_1, \mathsf{pk}_1) \leftarrow \mathsf{Gen}_1$

Evaluation

Public-Key Pseudorandom Correlation Functions [BCMPR24]

Key Derivation



pp

pk_0 pk_1

$\boxed{\mathsf{Gen}_0} \rightarrow (\mathsf{sk}_0, \mathsf{pk}_0)$

$(\mathsf{sk}_1, \mathsf{pk}_1) \leftarrow \boxed{\mathsf{Gen}_1}$

Evaluation

Public-Key Pseudorandom Correlation Functions [BCMPR24]

Key Derivation

pp

pk_0 pk_1

$\mathsf{Gen}_0 \rightarrow (\mathsf{sk}_0, \mathsf{pk}_0)$

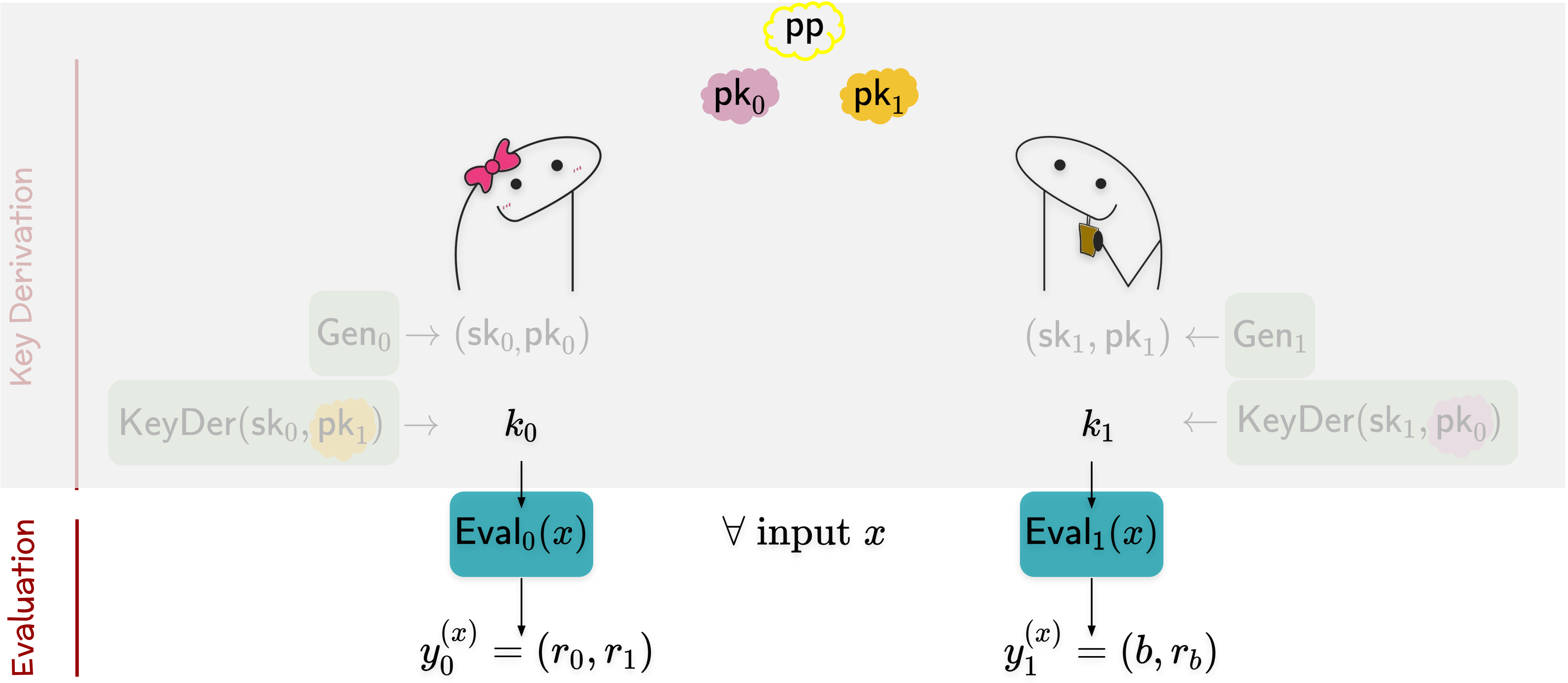
$\mathsf{KeyDer}(\mathsf{sk}_0, \mathsf{pk}_1) \rightarrow k_0$

$(\mathsf{sk}_1, \mathsf{pk}_1) \leftarrow \mathsf{Gen}_1$

$k_1 \leftarrow \mathsf{KeyDer}(\mathsf{sk}_1, \mathsf{pk}_0)$

Evaluation

Public-Key Pseudorandom Correlation Functions [BCMPR24]



pp

pk_0 pk_1

Key Derivation

$\mathsf{Gen}_0 \rightarrow (\mathsf{sk}_0, \mathsf{pk}_0)$

$(\mathsf{sk}_1, \mathsf{pk}_1) \leftarrow \mathsf{Gen}_1$

$\mathsf{KeyDer}(\mathsf{sk}_0, \mathsf{pk}_1) \rightarrow k_0$

$k_1 \leftarrow \mathsf{KeyDer}(\mathsf{sk}_1, \mathsf{pk}_0)$

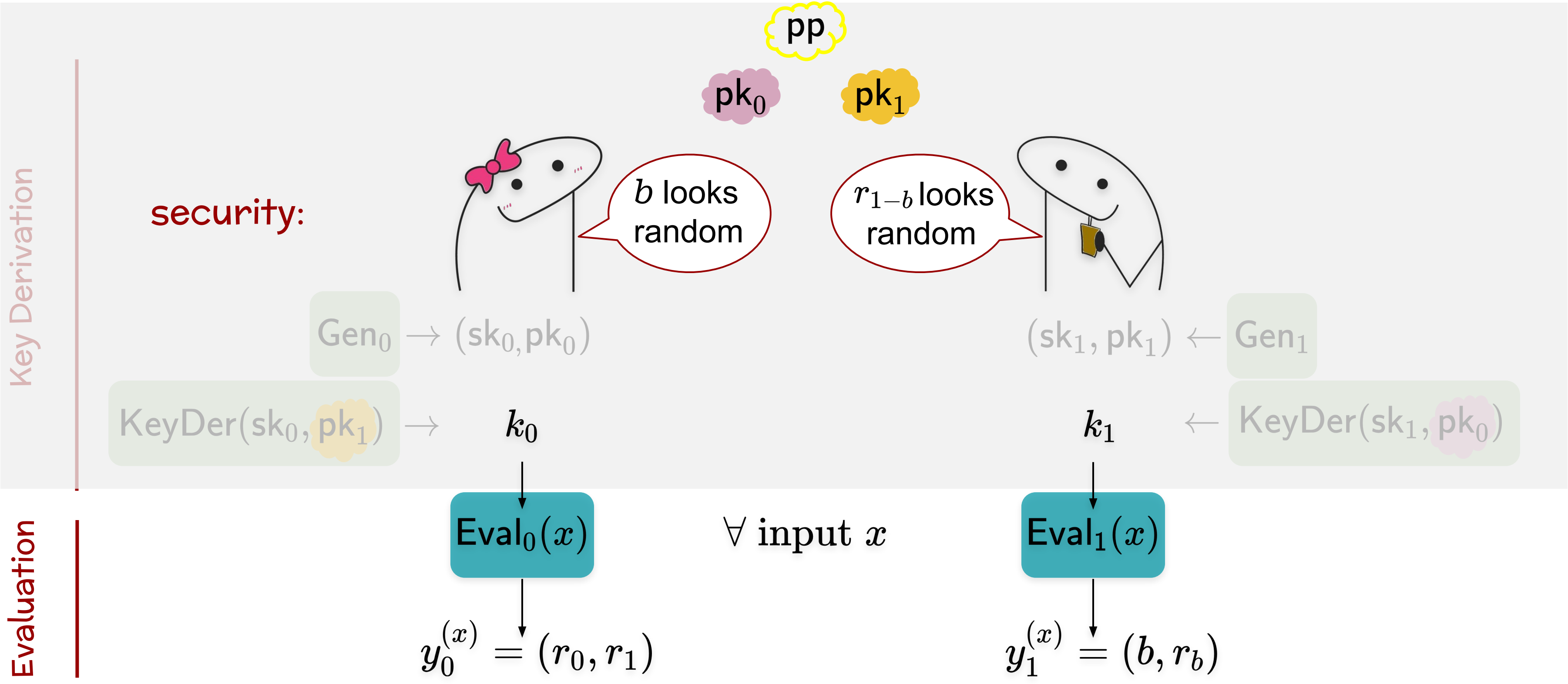
Evaluation

$\mathsf{Eval}_0(x)$ $\forall$ input x $\mathsf{Eval}_1(x)$

$y_0^{(x)} = (r_0, r_1)$

$y_1^{(x)} = (b, r_b)$

Public-Key Pseudorandom Correlation Functions [BCMPR24]



Our Contributions

Contributions

Efficient Public-Key PCF for OT Correlations
from Lattices

Secret-Power Ring
Learning with Errors

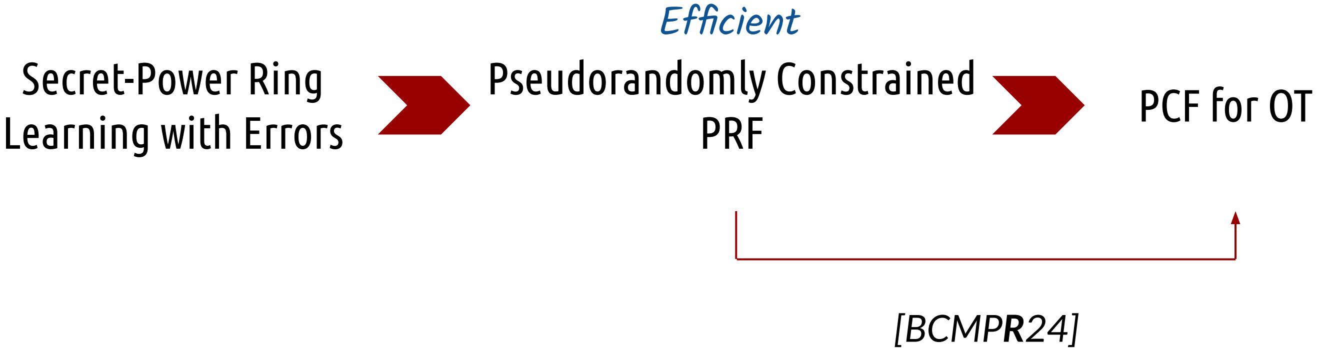
Contributions

Efficient Public-Key PCF for OT Correlations from Lattices

Secret-Power Ring Learning with Errors ➤ *Efficient* Pseudorandomly Constrained PRF

Contributions

Efficient Public-Key PCF for OT Correlations from Lattices



Secret-Power Ring Learning with Errors

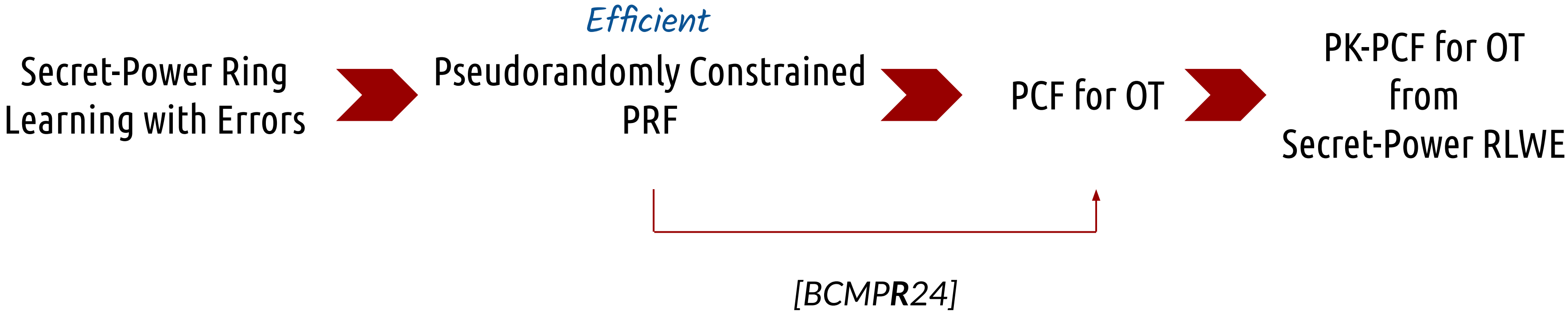
Efficient
Pseudorandomly Constrained PRF

PCF for OT

*[BCMP**R**24]*

Contributions

Efficient Public-Key PCF for OT Correlations from Lattices



Secret-Power Ring Learning with Errors

Efficient Pseudorandomly Constrained PRF

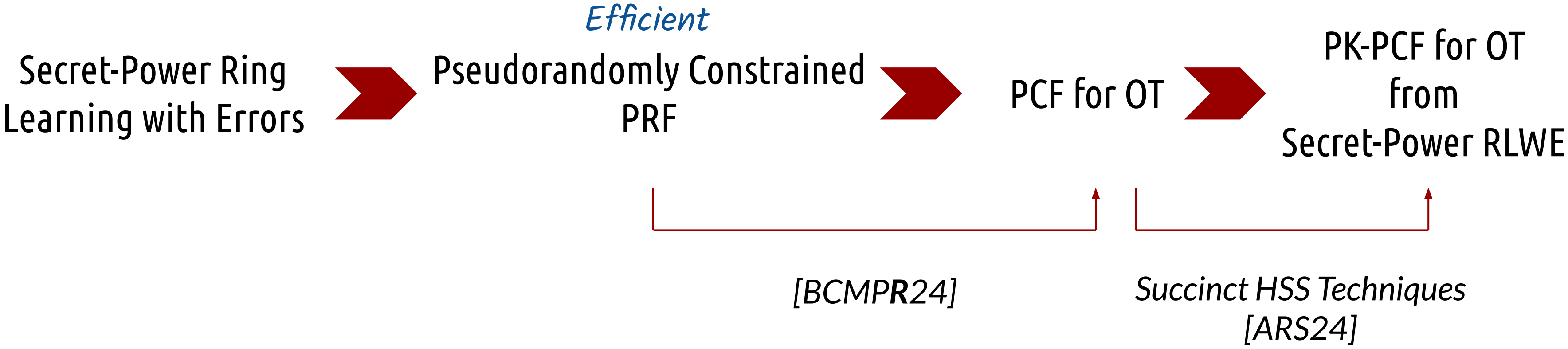
PCF for OT

PK-PCF for OT from Secret-Power RLWE

*[BCMP**R**24]*

Contributions

Efficient Public-Key PCF for OT Correlations from Lattices



Secret-Power Ring Learning with Errors

Efficient Pseudorandomly Constrained PRF

PCF for OT

PK-PCF for OT from Secret-Power RLWE

*[BCMP**R**24]*

Succinct HSS Techniques [ARS24]

HSS: Homomorphic Secret Sharing

Contributions

Efficient Public-Key PCF for OT Correlations from Lattices

In this talk

Secret-Power Ring Learning with Errors

Efficient

Pseudorandomly Constrained PRF

PCF for OT

PK-PCF for OT from Secret-Power RLWE

Contributions

Efficient Public-Key PCF for OT Correlations from Lattices

In this talk

Secret-Power Ring Learning with Errors

Efficient

Pseudorandomly Constrained PRF

PCF for OT

PK-PCF for OT from Secret-Power RLWE

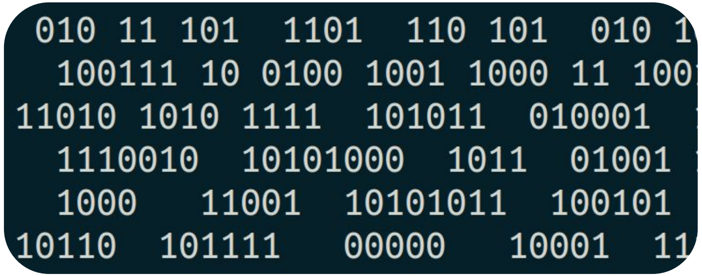
Pseudorandom Functions

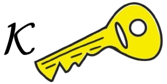
Pseudorandom Functions (PRFs) [GGM86]

Definition. Deterministic keyed functions indistinguishable from truly random functions.

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

Set of outputs with msk



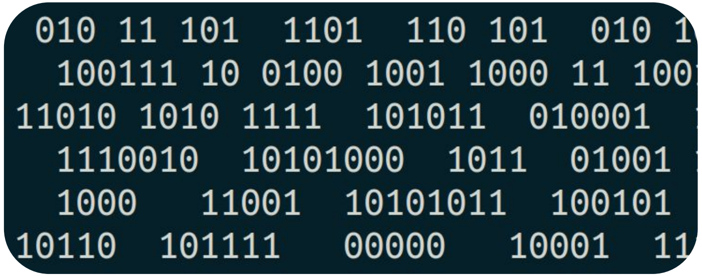
Compute using **msk** $\xleftarrow{\$} \mathcal{K}$ 

Pseudorandom Functions (PRFs) [GGM86]

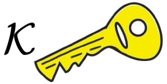
Definition. Deterministic keyed functions indistinguishable from truly random functions.

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

Set of outputs with msk



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



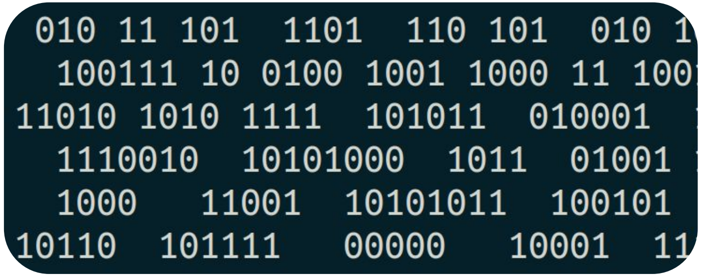
Set of outputs without msk

Pseudorandom Functions (PRFs) [GGM86]

Definition. Deterministic keyed functions indistinguishable from truly random functions.

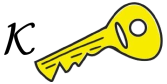
$F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$

Set of outputs with msk

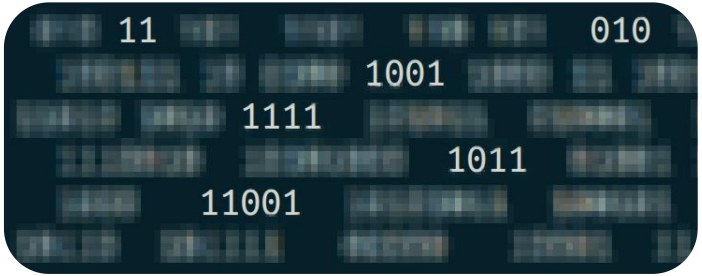


```
 010 11 101  1101  110 101  010
   100111 10 0100 1001 1000 11
11010 1010 1111  101011  010001
   1110010  10101000  1011  01001
   1000    11001  10101011  100101
10110  101111   00000   10001  11
```

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



Set of outputs without msk



with oracle queries on $\underline{\text{arbitrary}}$ / $\underline{\text{random}}$ inputs

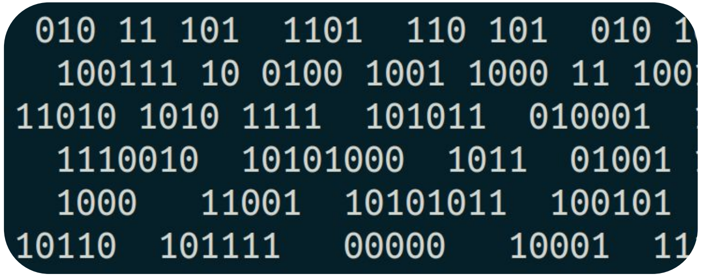
PRF   weak PRF

Constrained Pseudorandom Functions

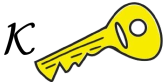
Constrained Pseudorandom Functions (CPRFs)[BW13,KPTZ13,BGI14]

Pseudorandom Functions *with constrained access to the evaluation.*

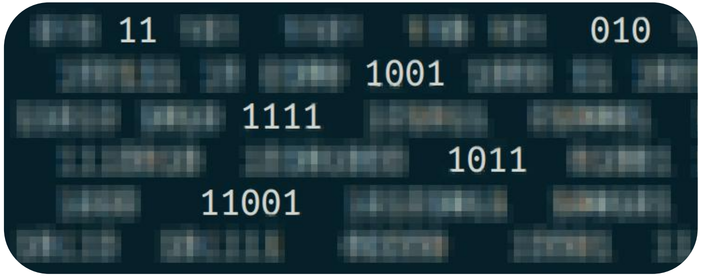
Set of outputs with msk



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



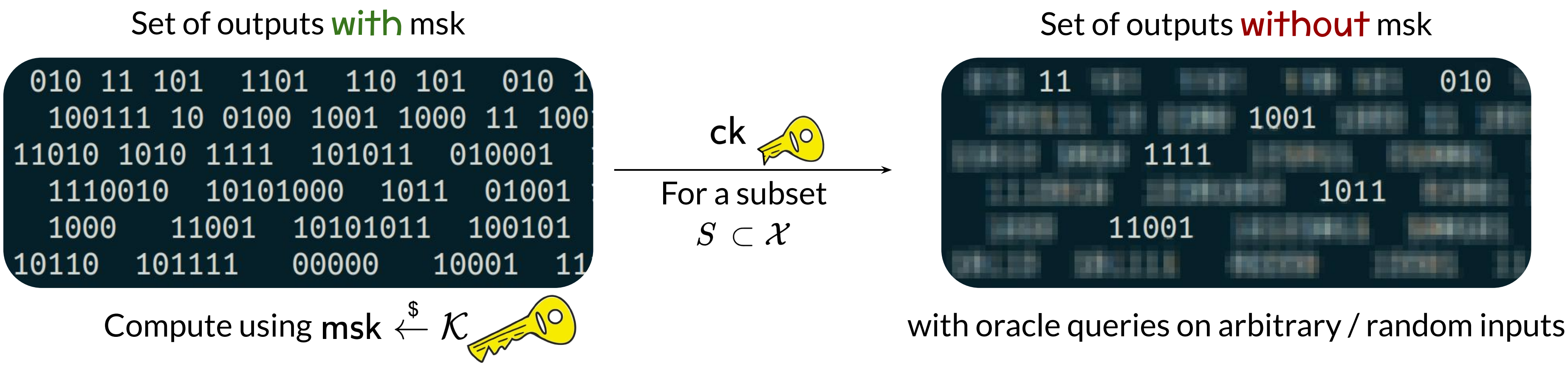
Set of outputs without msk



with oracle queries on arbitrary / random inputs

Constrained Pseudorandom Functions (CPRFs)[BW13,KPTZ13,BGI14]

Pseudorandom Functions *with constrained access to the evaluation.*



Set of outputs with msk

ck

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

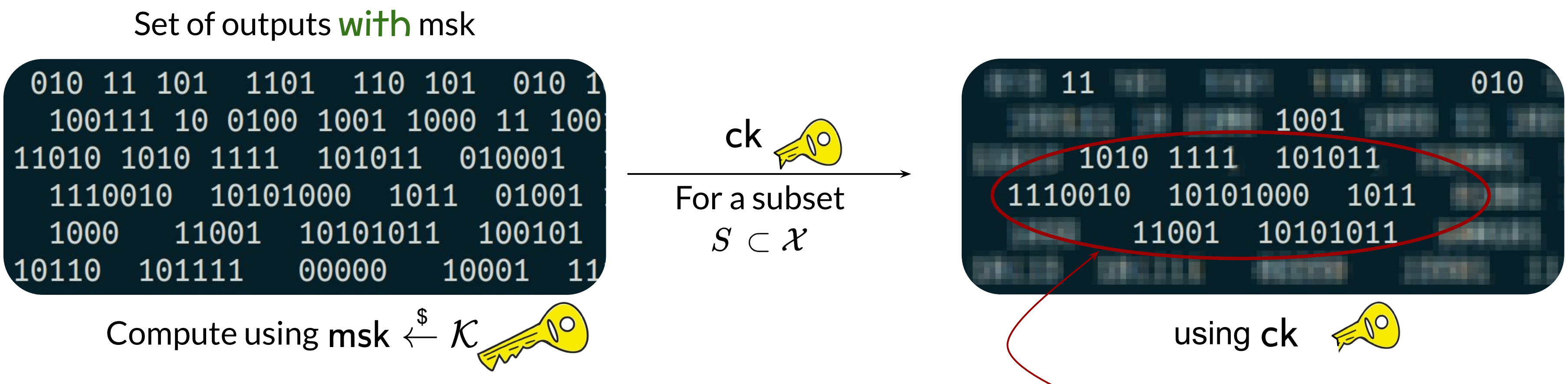
Set of outputs without msk

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

with oracle queries on arbitrary / random inputs

Constrained Pseudorandom Functions (CPRFs)[BW13,KPTZ13,BGI14]

Pseudorandom Functions *with constrained access to the evaluation.*



Set of outputs with msk

ck

For a subset

$S \subset \mathcal{X}$

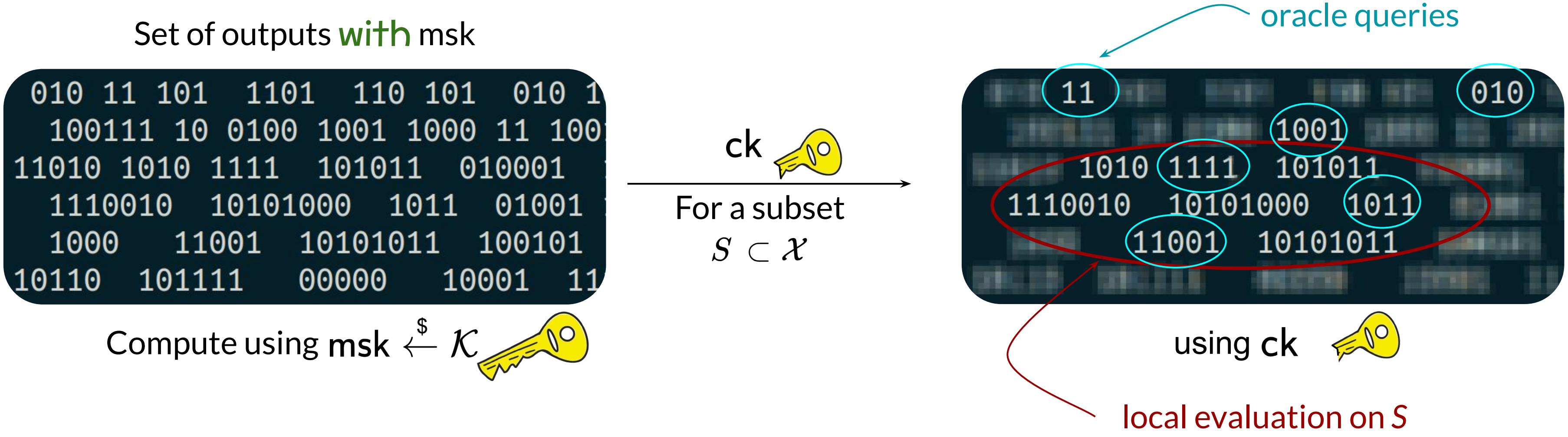
Compute using **msk** $\xleftarrow{\$} \mathcal{K}$

using **ck**

local evaluation on *S*

Constrained Pseudorandom Functions (CPRFs)[BW13,KPTZ13,BGI14]

Pseudorandom Functions *with constrained access to the evaluation.*



Set of outputs with msk

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

ck

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

oracle queries

using **ck**

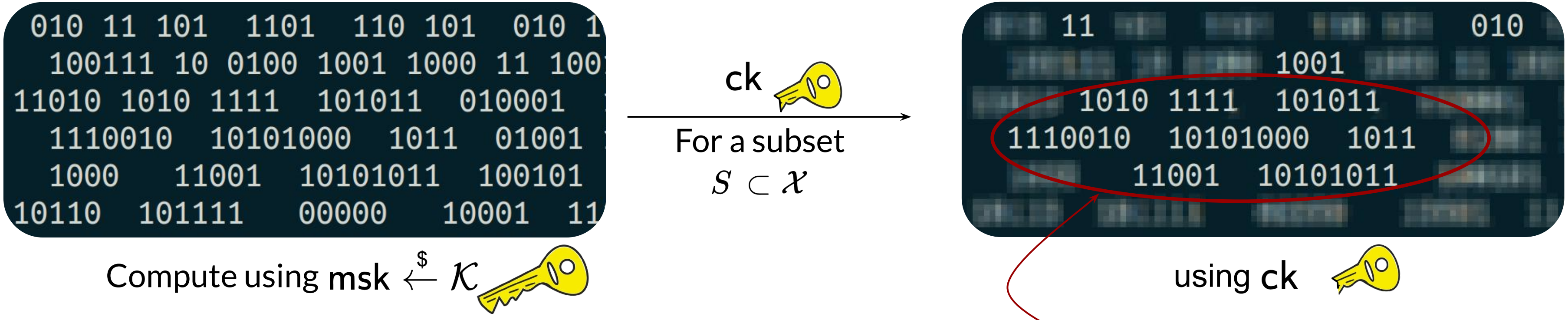
local evaluation on *S*

Constrained Pseudorandom Functions (CPRFs)[BW13,KPTZ13,BGI14]

Pseudorandom Functions *with constrained access to the evaluation.*

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

Set of outputs with msk



ck

For a subset

$S \subset \mathcal{X}$

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

using **ck**

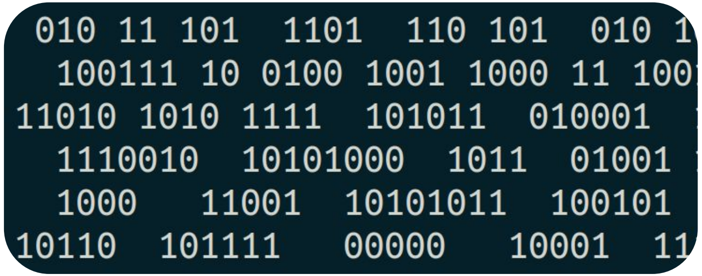
local evaluation on *S*

Constrained Pseudorandom Functions (CPRFs)[BW13,KPTZ13,BGI14]

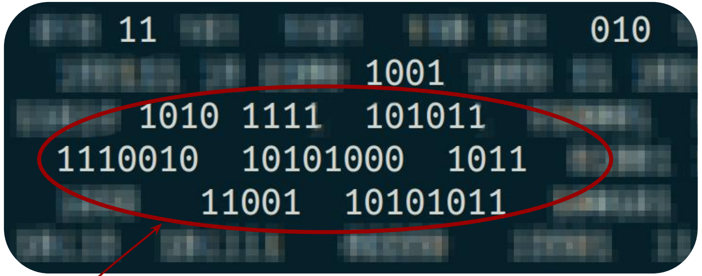
Pseudorandom Functions *with constrained access to the evaluation.*

- 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** $\overset{\$}{\leftarrow} \mathcal{K}$



using $\textbf{ck}_F$

local evaluation on S_F

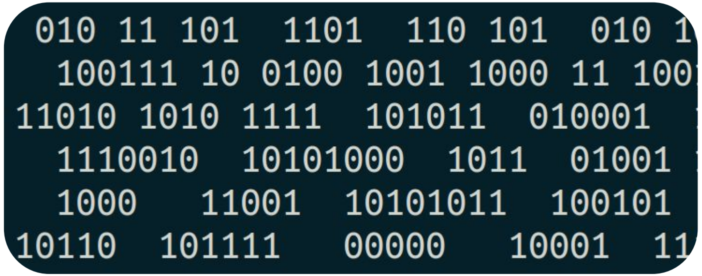
Constrained Pseudorandom Functions (CPRFs)[BW13,KPTZ13,BGI14]

Pseudorandom Functions *with constrained access to the evaluation.*

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

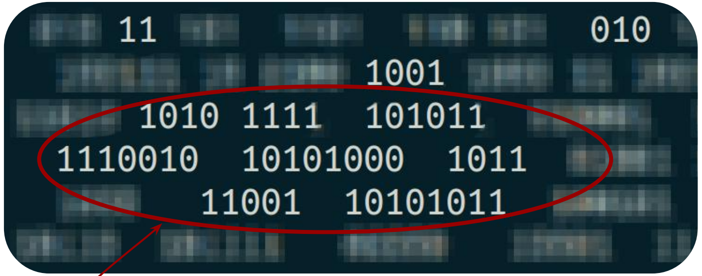
(w)PRF ⤳ Pseudorandomly Constrained PRF

Set of outputs with msk



```
010 11 101  1101  110 101  010 1
 100111 10 0100 1001 1000 11 100
11010 1010 1111  101011  010001
 1110010  10101000  1011  01001
 1000   11001  10101011  100101
10110  101111   00000   10001  11
```

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



```
  11                        010
           1001
     1010 1111  101011
1110010  10101000  1011
        11001  10101011
```

using $\mathbf{ck}_F$

local evaluation on S_F

Pseudorandom Correlation Functions
for
Oblivious Transfer

from pseudorandomly constrained PRFs

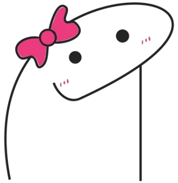
PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

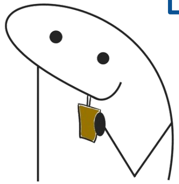
PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

- wPRF $F_{\mathsf{k}} : \mathcal{X} \rightarrow \{0,1\}$

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

- wPRF $F_{\mathsf{k}} : \mathcal{X} \rightarrow \{0,1\}$
- CPRF for F_{k} and $\overline{F_{\mathsf{k}}}$





PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

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

can generate a **ck** for either:

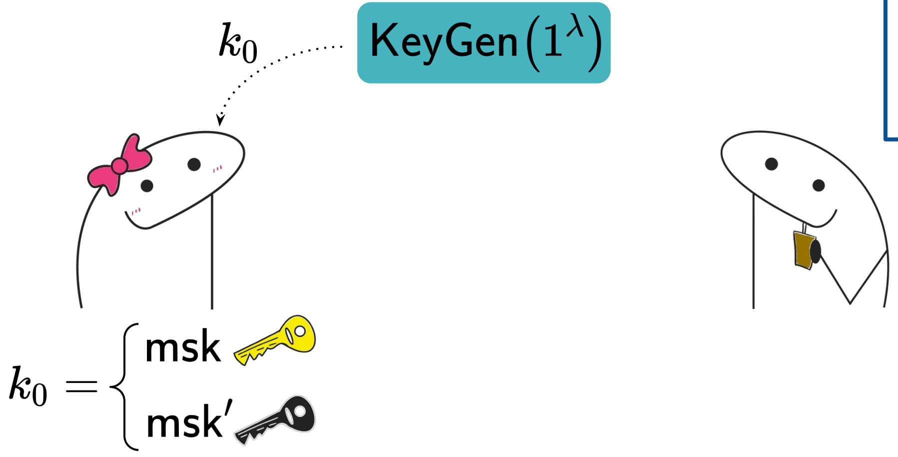
-any **x** s.t. **F_k(x)=0**

or

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

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

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



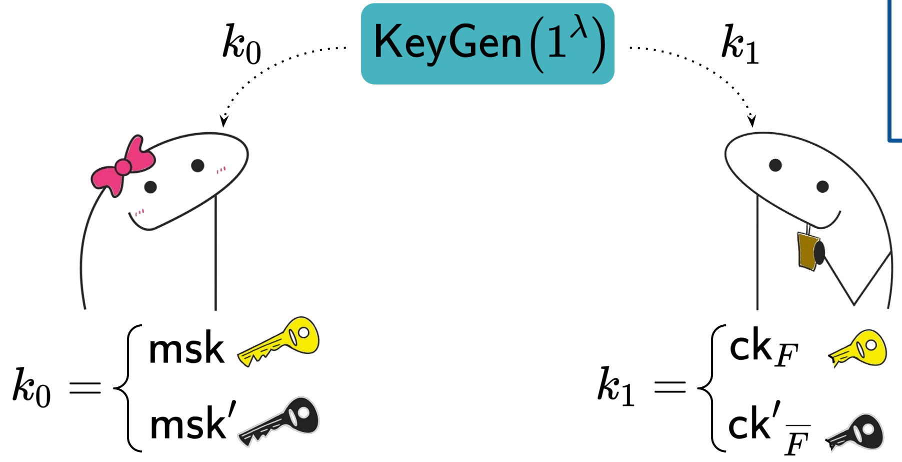
k_0

$\mathsf{KeyGen}(1^\lambda)$

$$k_0 = \begin{cases} \mathsf{msk} \\ \mathsf{msk}' \end{cases}$$

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

- wPRF $F_{\mathsf{k}} : \mathcal{X} \rightarrow \{0,1\}$
- CPRF for F_{k} and $\overline{F_{\mathsf{k}}}$



KeyGen(1^λ)

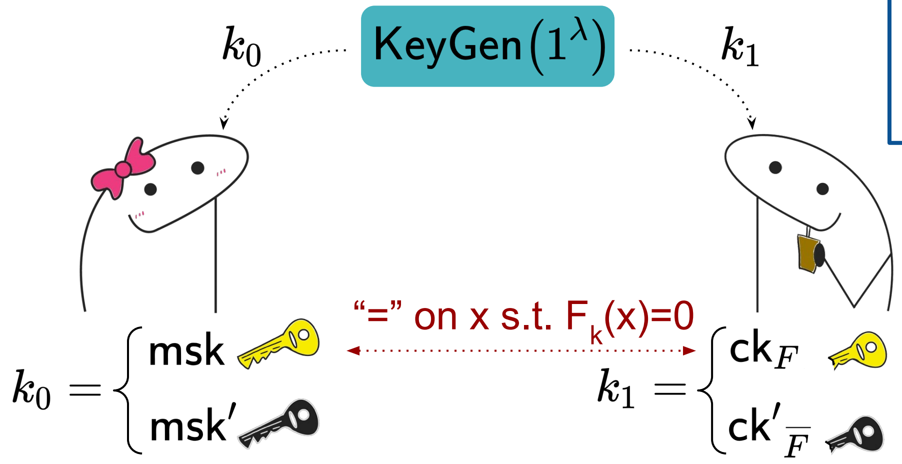
k_0 k_1

$$k_0 = \begin{cases} \mathsf{msk} \\ \mathsf{msk}' \end{cases} \qquad k_1 = \begin{cases} \mathsf{ck}_F \\ \mathsf{ck}'_{\overline{F}} \end{cases}, \; \mathsf{k}$$

(wPRF key)

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

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



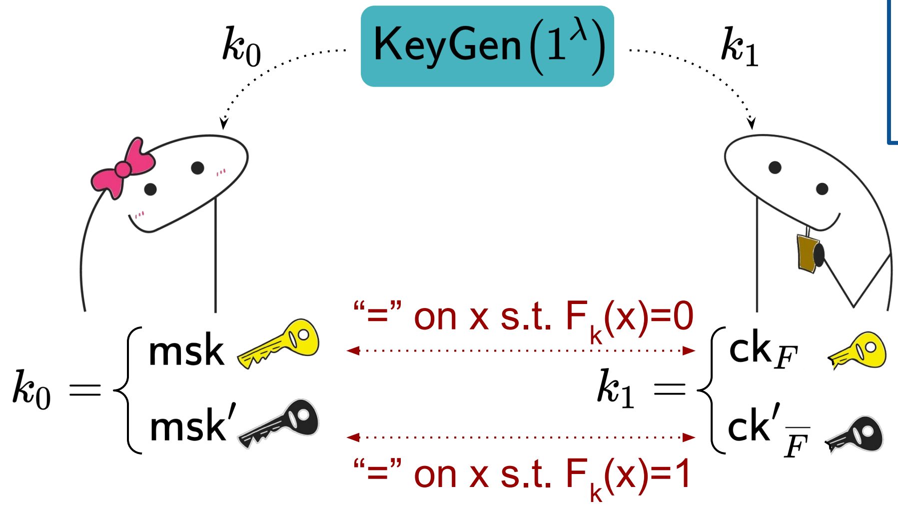
$$k_0 = \begin{cases} \text{msk} \\ \text{msk}' \end{cases} \qquad k_1 = \begin{cases} \text{ck}_F \\ \text{ck}'_{\overline{F}} \end{cases}$$

, k (wPRF key)

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

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

- CPRF for F_k and $\overline{F_k}$



$\mathsf{KeyGen}(1^\lambda)$

k_0 k_1

$k_0 = \begin{cases} \mathsf{msk} \\ \mathsf{msk}' \end{cases}$

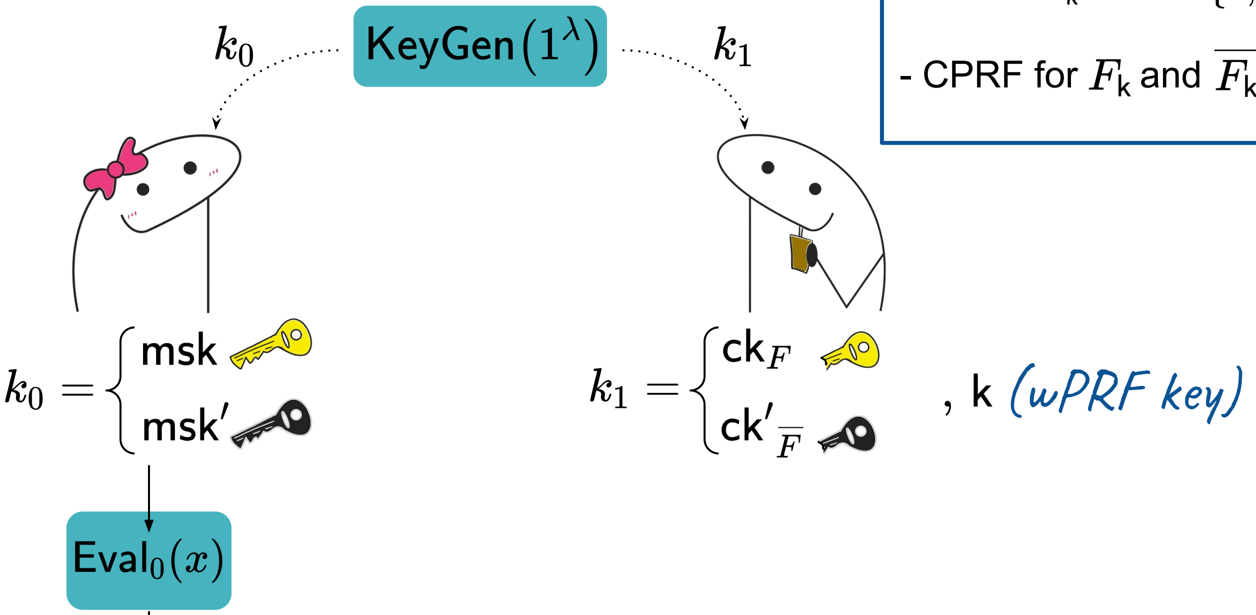
"=" on x s.t. $F_k(x)=0$

"=" on x s.t. $F_k(x)=1$

$k_1 = \begin{cases} \mathsf{ck}_F \\ \mathsf{ck}'_{\overline{F}} \end{cases}$, k *(wPRF key)*

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

- wPRF $F_{\mathsf{k}} : \mathcal{X} \rightarrow \{0,1\}$
- CPRF for F_{k} and $\overline{F_{\mathsf{k}}}$



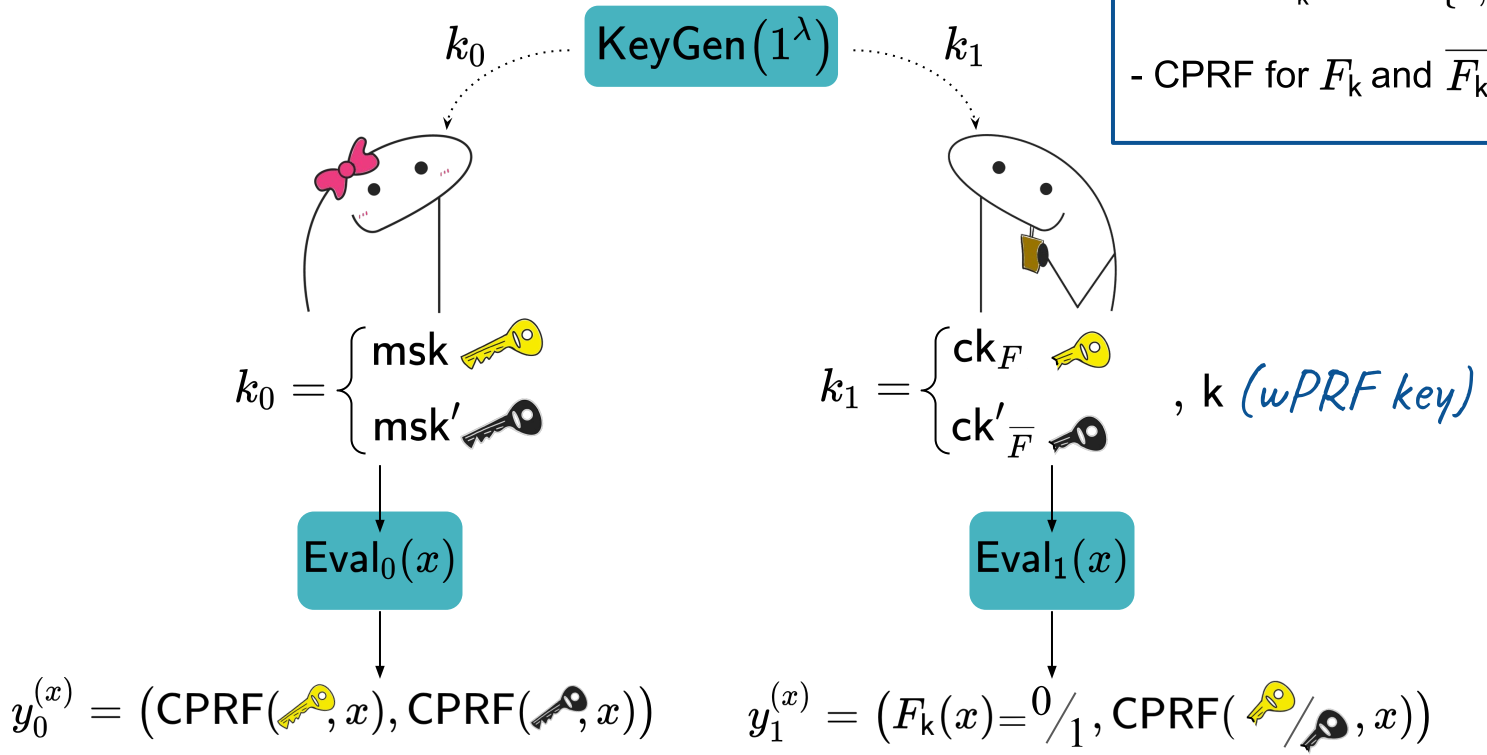
$k_0 = \begin{cases} \mathsf{msk} \text{ 🔑} \\ \mathsf{msk}' \text{ 🗝} \end{cases}$

$k_1 = \begin{cases} \mathsf{ck}_F \text{ 🔑} \\ \mathsf{ck}'_{\overline{F}} \text{ 🗝} \end{cases}$, k (wPRF key)

$y_0^{(x)} = (\mathsf{CPRF}(\text{🔑}, x), \mathsf{CPRF}(\text{🗝}, x))$

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

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



KeyGen(1^λ)

k_0

k_1

$$k_0 = \begin{cases} \mathsf{msk}\ \text{🔑} \\ \mathsf{msk}'\ \text{🗝} \end{cases}$$

$$k_1 = \begin{cases} \mathsf{ck}_F\ \text{🔑} \\ \mathsf{ck}'_{\overline{F}}\ \text{🗝} \end{cases}, \ \mathsf{k}$$ (wPRF key)

Eval$_0(x)$

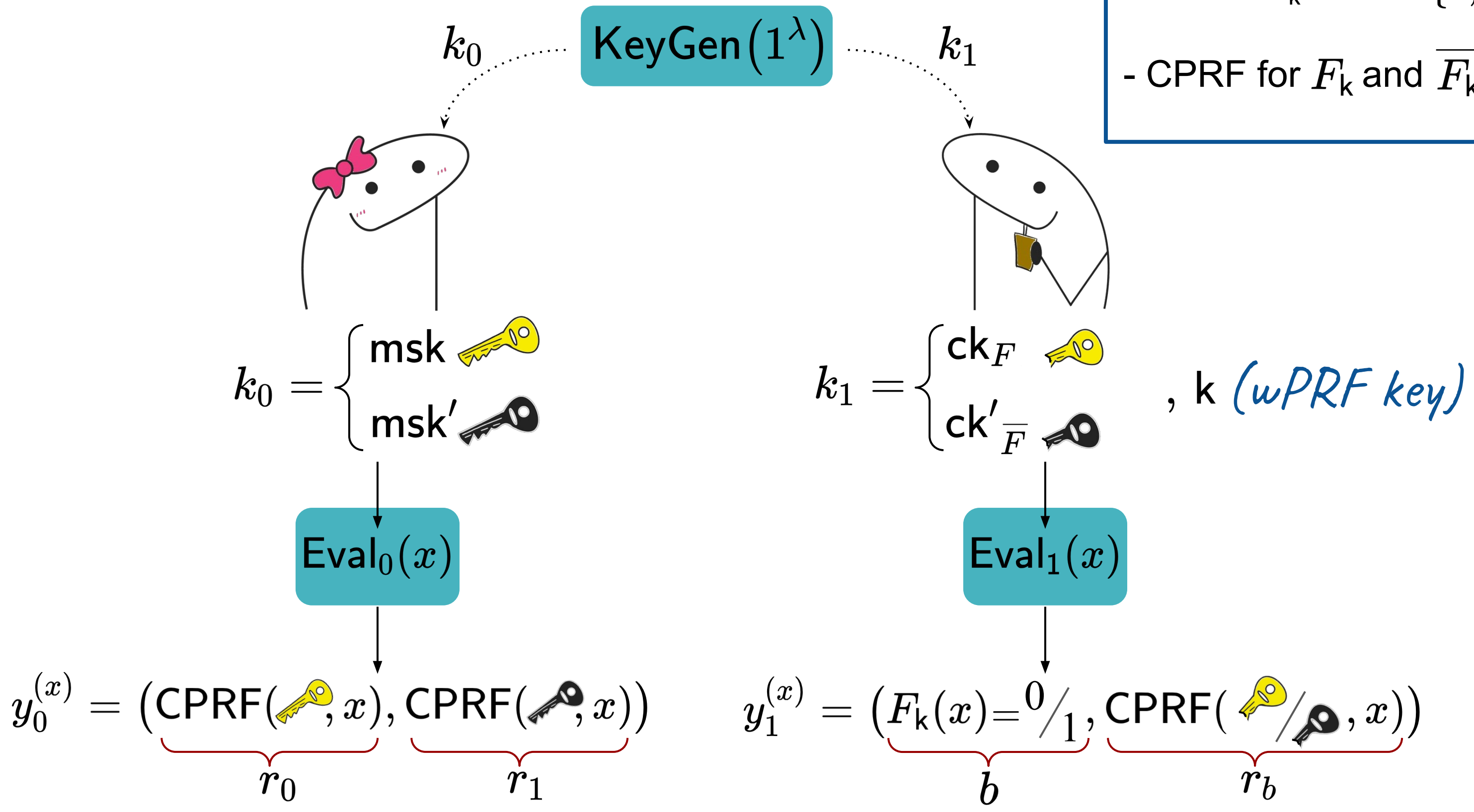
Eval$_1(x)$

$$y_0^{(x)} = (\mathsf{CPRF}(\text{🔑}, x), \mathsf{CPRF}(\text{🗝}, x))$$

$$y_1^{(x)} = (F_{\mathsf{k}}(x) = {}^0/_1, \mathsf{CPRF}(\text{🔑}/\text{🗝}, x))$$

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

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



$$k_0 = \begin{cases} \text{msk } 🔑 \\ \text{msk}' \ 🗝 \end{cases}$$

$$k_1 = \begin{cases} \text{ck}_F \ 🔑 \\ \text{ck}'_{\overline{F}} \ 🗝 \end{cases}, \text{ k}$$ (wPRF key)

$$y_0^{(x)} = (\underbrace{\text{CPRF}(🔑, x)}_{r_0}, \underbrace{\text{CPRF}(🗝, x)}_{r_1})$$

$$y_1^{(x)} = (\underbrace{F_k(x) = {}^0/_1}_{b}, \underbrace{\text{CPRF}(🔑/🗝, x)}_{r_b})$$

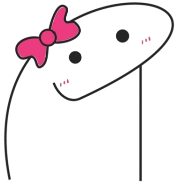
PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

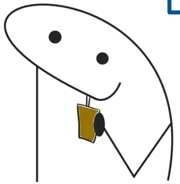
- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$

$\mathsf{KeyGen}(1^\lambda)$

k_0

k_1





$$k_0 = \begin{cases} \mathsf{msk}\ \text{🔑} \\ \mathsf{msk}'\ \text{🗝} \end{cases}$$

$$k_1 = \begin{cases} \mathsf{ck}_F\ \text{🔑} \\ \mathsf{ck}'_{\overline{F}}\ \text{🗝} \end{cases}, \ \mathsf{k}$$ (wPRF key)

$\mathsf{Eval}_0(x)$

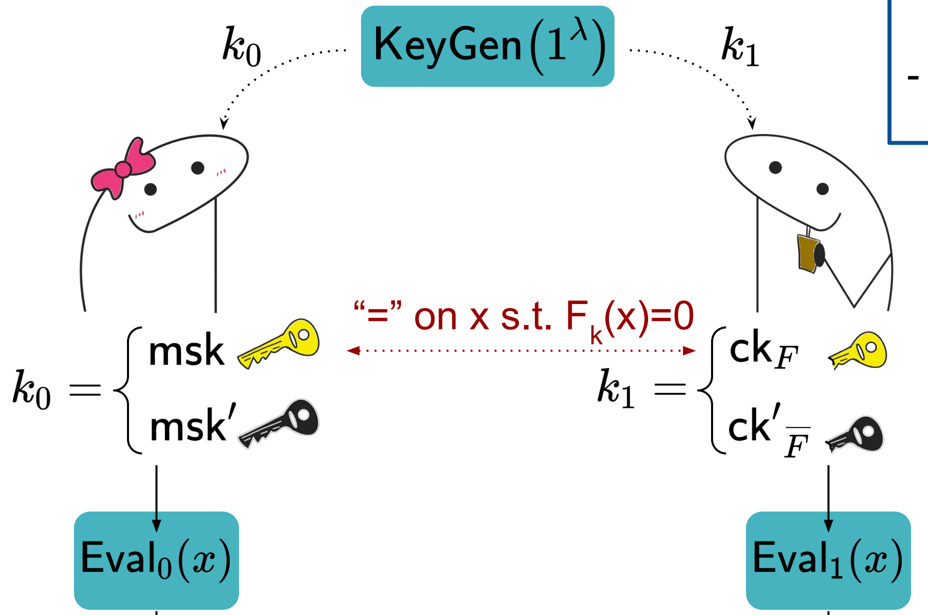
$\mathsf{Eval}_1(x)$

$$y_0^{(x)} = (\underbrace{\mathsf{CPRF}(\text{🔑}, x)}_{r_0}, \underbrace{\mathsf{CPRF}(\text{🗝}, x)}_{r_1})$$

$$y_1^{(x)} = (F_k(x) = 0, \mathsf{CPRF}(\text{🔑}, x))$$

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

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



$k_0 = \begin{cases} \text{msk 🔑} \\ \text{msk}' \text{ 🗝} \end{cases}$

"=" on x s.t. $F_k(x)=0$

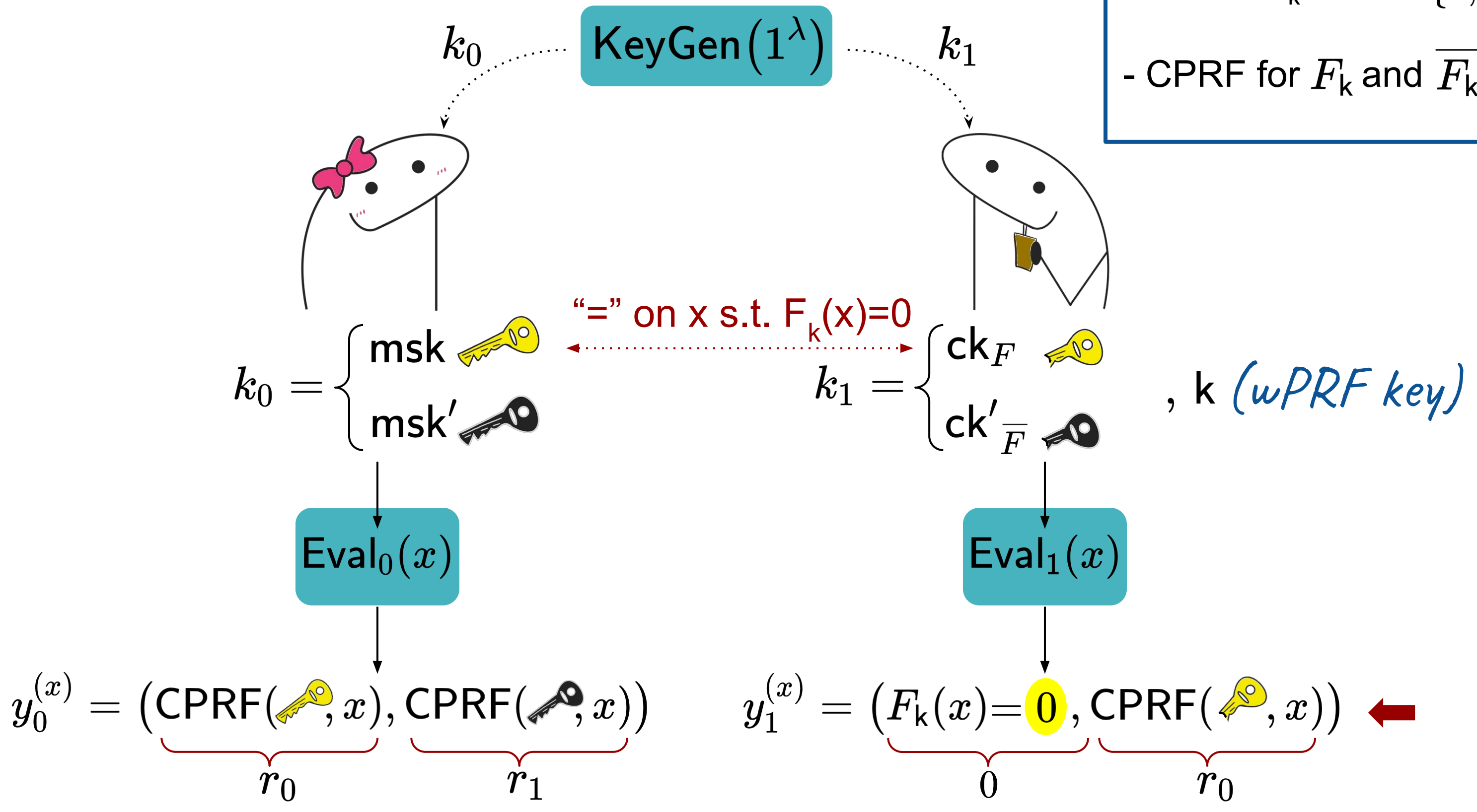
$k_1 = \begin{cases} \text{ck}_F \text{ 🔑} \\ \text{ck}'_{\overline{F}} \text{ 🗝} \end{cases}$, k *(wPRF key)*

$$y_0^{(x)} = (\underbrace{\text{CPRF}(\text{🔑}, x)}_{r_0}, \underbrace{\text{CPRF}(\text{🗝}, x)}_{r_1})$$

$$y_1^{(x)} = (F_k(x) = 0, \text{CPRF}(\text{🔑}, x))$$

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

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



$\mathsf{KeyGen}(1^\lambda)$

k_0 k_1

“=” on x s.t. $F_k(x)=0$

$k_0 = \begin{cases} \mathsf{msk} \text{ 🔑} \\ \mathsf{msk}' \text{ 🗝} \end{cases}$

$k_1 = \begin{cases} \mathsf{ck}_F \text{ 🔑} \\ \mathsf{ck}'_{\overline{F}} \text{ 🗝} \end{cases}$, k (wPRF key)

$\mathsf{Eval}_0(x)$

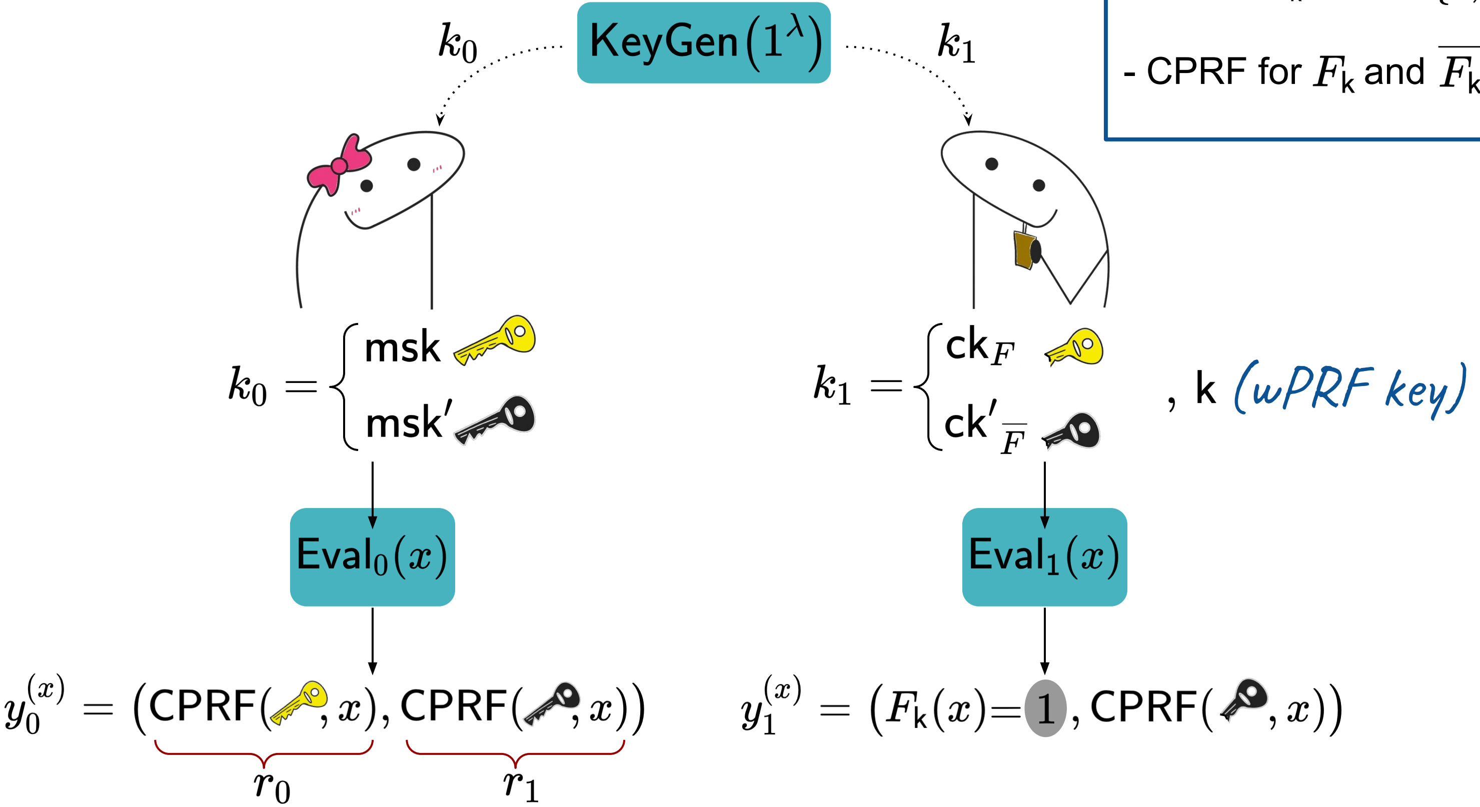
$\mathsf{Eval}_1(x)$

$$y_0^{(x)} = (\underbrace{\mathsf{CPRF}(\text{🔑}, x)}_{r_0}, \underbrace{\mathsf{CPRF}(\text{🗝}, x)}_{r_1})$$

$$y_1^{(x)} = (\underbrace{F_k(x) = 0}_{0}, \underbrace{\mathsf{CPRF}(\text{🔑}, x)}_{r_0})$$ ⬅

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

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



KeyGen(1^λ)

k_0 k_1

$$k_0 = \begin{cases} \text{msk } \text{🔑} \\ \text{msk}' \text{ 🗝} \end{cases}$$

$$k_1 = \begin{cases} \text{ck}_F \text{ 🔑} \\ \text{ck}'_{\overline{F}} \text{ 🗝} \end{cases}$$, k (wPRF key)

Eval$_0(x)$

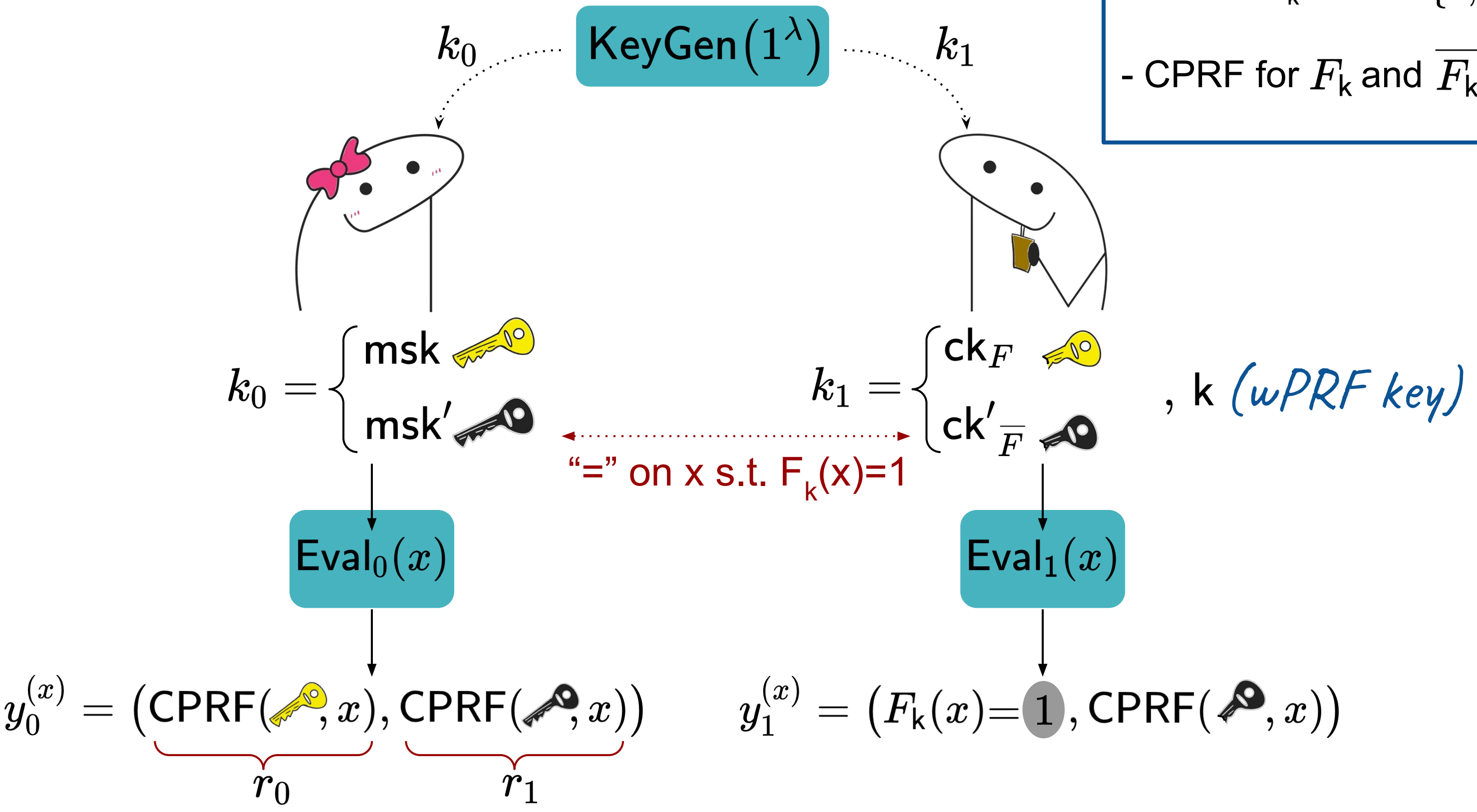
Eval$_1(x)$

$$y_0^{(x)} = (\underbrace{\text{CPRF}(\text{🔑}, x)}_{r_0}, \underbrace{\text{CPRF}(\text{🗝}, x)}_{r_1})$$

$$y_1^{(x)} = (F_k(x) = 1, \text{CPRF}(\text{🗝}, x))$$

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

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



$\mathsf{KeyGen}(1^\lambda)$

k_0 k_1

$$k_0 = \begin{cases} \mathsf{msk} \; 🔑 \\ \mathsf{msk}' \; 🗝 \end{cases}$$

$$k_1 = \begin{cases} \mathsf{ck}_F \; 🔑 \\ \mathsf{ck}'_{\overline{F}} \; 🗝 \end{cases}, \; \mathsf{k}$$ (wPRF key)

“=” on x s.t. $F_k(x)=1$

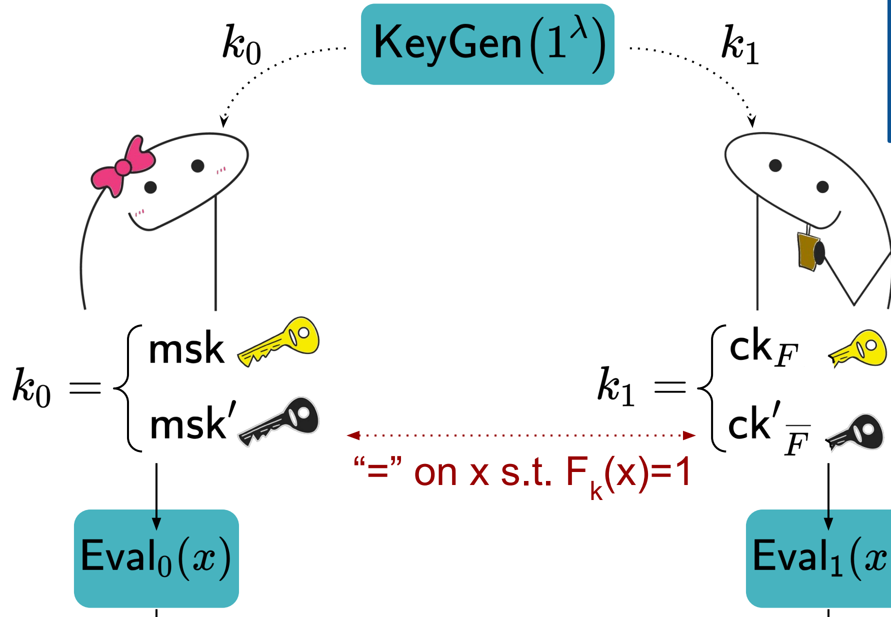
$\mathsf{Eval}_0(x)$ $\mathsf{Eval}_1(x)$

$$y_0^{(x)} = (\underbrace{\mathsf{CPRF}(🔑, x)}_{r_0}, \underbrace{\mathsf{CPRF}(🗝, x)}_{r_1})$$

$$y_1^{(x)} = (F_{\mathsf{k}}(x) = 1, \mathsf{CPRF}(🗝, x))$$

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

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



KeyGen(1^λ)

k_0

k_1

$k_0 = \{$ msk 🔑, msk$'$ 🗝 $\}$

$k_1 = \{$ ck$_F$ 🔑, ck$'_{\overline{F}}$ 🗝 $\}$, k *(wPRF key)*

"=" on x s.t. $F_k(x)$=1

Eval$_0(x)$

Eval$_1(x)$

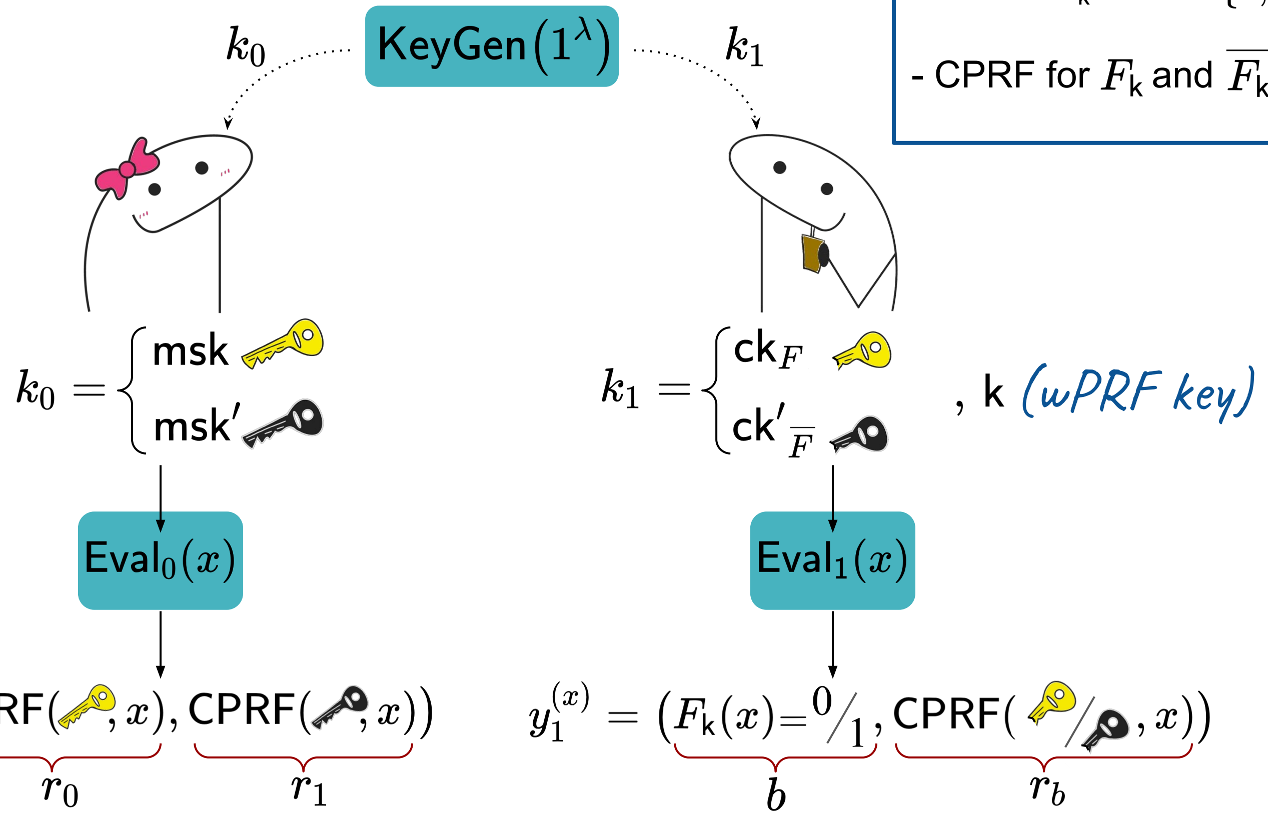
$$y_0^{(x)} = (\underbrace{\text{CPRF}(\text{🔑}, x)}_{r_0}, \underbrace{\text{CPRF}(\text{🗝}, x)}_{r_1})$$

$$y_1^{(x)} = (\underbrace{F_k(x) = \boxed{1}}_{1}, \underbrace{\text{CPRF}(\text{🗝}, x)}_{r_1})$$

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

OT-correlated ✓

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



KeyGen(1^λ)

k_0 k_1

$$k_0 = \begin{cases} \text{msk} \ 🔑 \\ \text{msk}' \ 🔑 \end{cases}$$

$$k_1 = \begin{cases} \text{ck}_F \ 🔑 \\ \text{ck}'_{\overline{F}} \ 🔑 \end{cases}, \text{k}$$

(wPRF key)

Eval$_0(x)$

Eval$_1(x)$

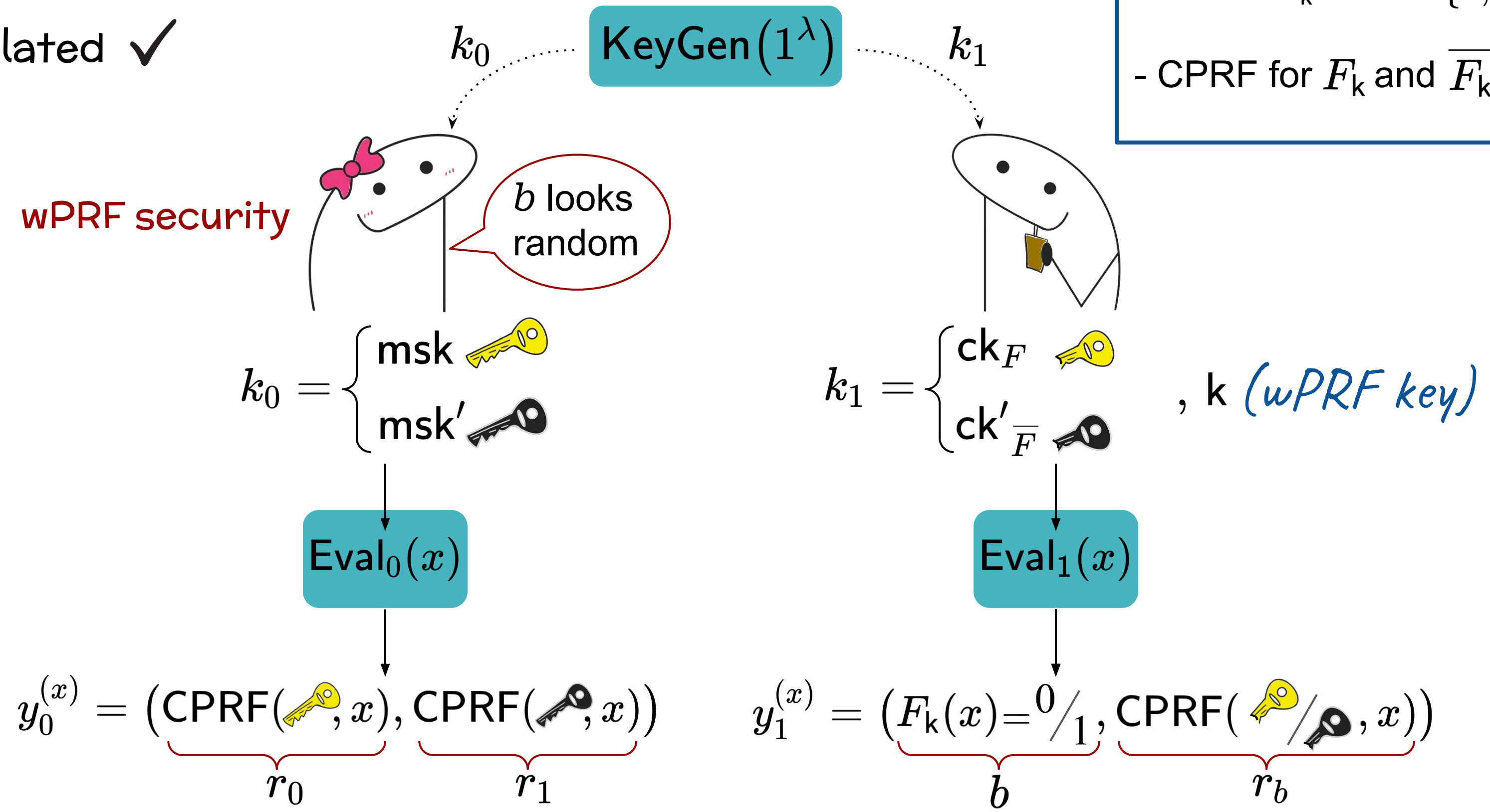
$$y_0^{(x)} = (\underbrace{\text{CPRF}(🔑, x)}_{r_0}, \underbrace{\text{CPRF}(🔑, x)}_{r_1})$$

$$y_1^{(x)} = (\underbrace{F_k(x) = {}^0/_1}_{b}, \underbrace{\text{CPRF}(🔑/🔑, x)}_{r_b})$$

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

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

OT-correlated ✓



wPRF security

b looks random

$\text{KeyGen}(1^\lambda)$

k_0 k_1

$$k_0 = \begin{cases} \text{msk} \ 🔑 \\ \text{msk}' \ 🗝 \end{cases}$$

$$k_1 = \begin{cases} \text{ck}_F \ 🔑 \\ \text{ck}'_{\overline{F}} \ 🗝 \end{cases}, \ \text{k}$$ (wPRF key)

$\text{Eval}_0(x)$

$\text{Eval}_1(x)$

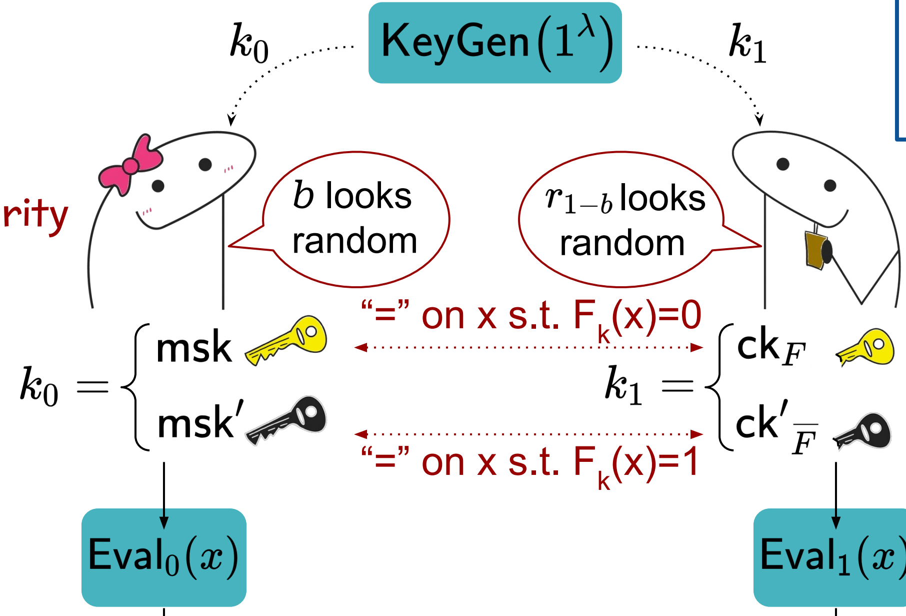
$$y_0^{(x)} = (\underbrace{\text{CPRF}(🔑, x)}_{r_0}, \underbrace{\text{CPRF}(🗝, x)}_{r_1})$$

$$y_1^{(x)} = (\underbrace{F_k(x) = {}^0/_1}_{b}, \underbrace{\text{CPRF}(🔑/🗝, x)}_{r_b})$$

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

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

OT-correlated ✓



$\text{KeyGen}(1^\lambda)$

k_0 k_1

wPRF security

b looks random

r_{1-b} looks random

CPRF security

"=" on x s.t. $F_k(x)=0$

$$k_0 = \begin{cases} \text{msk } 🔑 \\ \text{msk}' \ 🗝 \end{cases} \qquad k_1 = \begin{cases} \text{ck}_F \ 🔑 \\ \text{ck}'_{\overline{F}} \ 🗝 \end{cases}, \text{ k } (wPRF\ key)$$

"=" on x s.t. $F_k(x)=1$

$\text{Eval}_0(x)$ $\text{Eval}_1(x)$

$$y_0^{(x)} = (\underbrace{\text{CPRF}(🔑, x)}_{r_0}, \underbrace{\text{CPRF}(🗝, x)}_{r_1})$$

$$y_1^{(x)} = (\underbrace{F_k(x) = {}^0/_1}_{b}, \underbrace{\text{CPRF}(🔑/🗝, x)}_{r_b})$$

PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

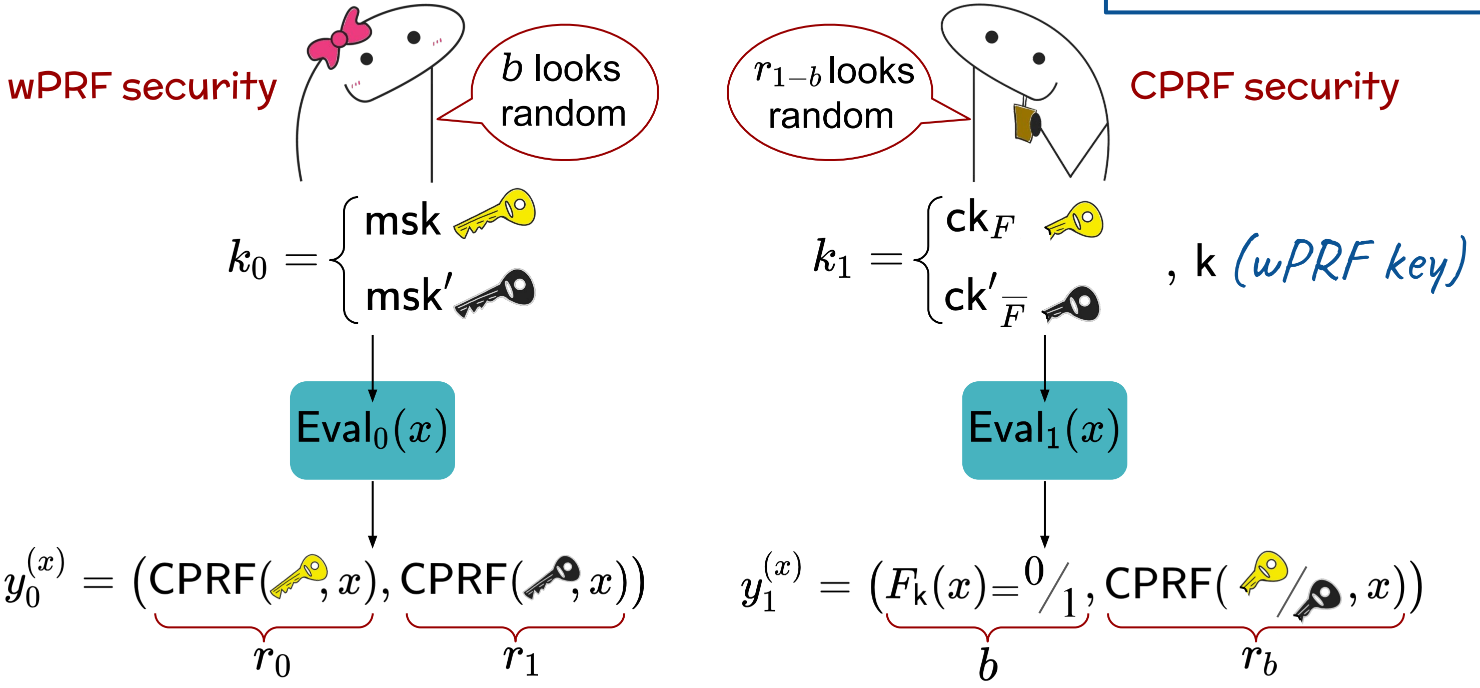
- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$

OT-correlated ✓

Secure ✓

KeyGen(1^λ)

k_0 k_1



wPRF security

b looks random

r_{1-b} looks random

CPRF security

$$k_0 = \begin{cases} \text{msk } 🔑 \\ \text{msk}' \text{ 🗝} \end{cases}$$

$$k_1 = \begin{cases} \text{ck}_F \text{ 🔑} \\ \text{ck}'_{\overline{F}} \text{ 🗝} \end{cases}, \text{ k}$$

(wPRF key)

Eval$_0(x)$

Eval$_1(x)$

$$y_0^{(x)} = (\underbrace{\text{CPRF}(🔑, x)}_{r_0}, \underbrace{\text{CPRF}(🗝, x)}_{r_1})$$

$$y_1^{(x)} = (\underbrace{F_k(x) = {}^0/_1}_{b}, \underbrace{\text{CPRF}(🔑/🗝, x)}_{r_b})$$

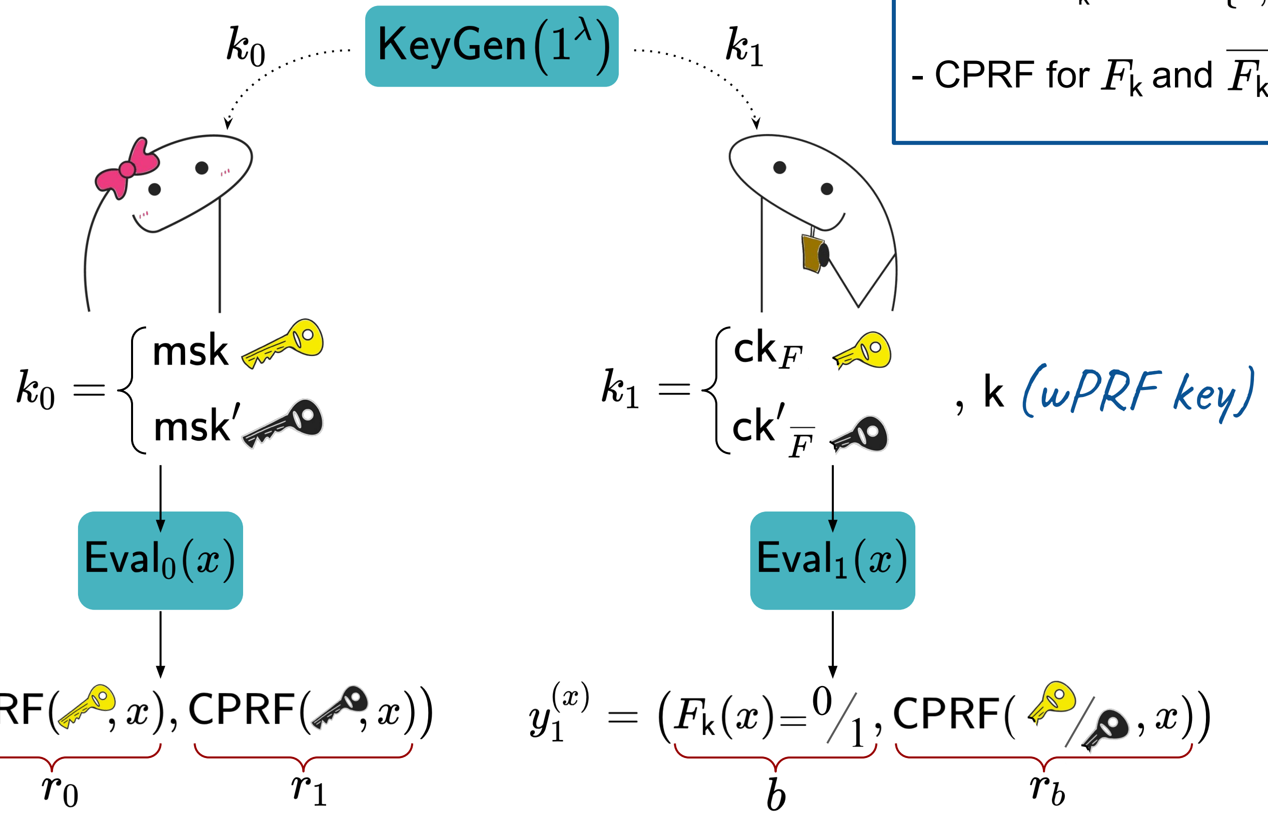
PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

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

OT-correlated ✓

Secure ✓

Precomputable



$\mathsf{KeyGen}(1^\lambda)$

k_0 k_1

$$k_0 = \begin{cases} \mathsf{msk}\ \text{🔑} \\ \mathsf{msk}'\ \text{🗝} \end{cases}$$

$$k_1 = \begin{cases} \mathsf{ck}_F\ \text{🔑} \\ \mathsf{ck}'_{\overline{F}}\ \text{🗝} \end{cases}, \ \mathsf{k}$$

(wPRF key)

$\mathsf{Eval}_0(x)$

$\mathsf{Eval}_1(x)$

$$y_0^{(x)} = (\underbrace{\mathsf{CPRF}(\text{🔑}, x)}_{r_0}, \underbrace{\mathsf{CPRF}(\text{🗝}, x)}_{r_1})$$

$$y_1^{(x)} = (\underbrace{F_{\mathsf{k}}(x) = {}^0\!/_1}_{b}, \underbrace{\mathsf{CPRF}(\text{🔑}/\text{🗝}, x)}_{r_b})$$

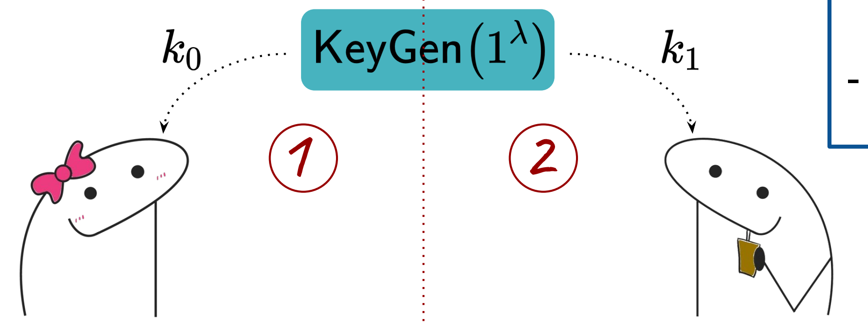
PCF for OT from Pseudorandomly Constrained PRFs [BCMPR24]

OT-correlated ✓

Secure ✓

Precomputable

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



$k_0 = \begin{cases} \text{msk} & 🔑 \\ \text{msk}' & 🗝 \end{cases}$

$k_1 = \begin{cases} \text{ck}_F & 🔑 \\ \text{ck}'_{\overline{F}} & 🗝 \end{cases}$, k (wPRF key)

Eval$_0(x)$

Eval$_1(x)$

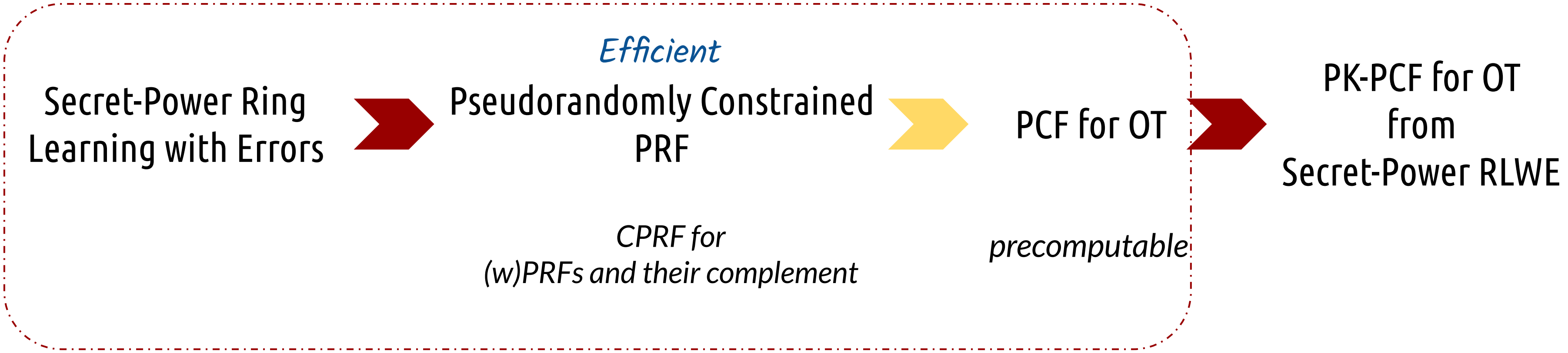
$y_0^{(x)} = (\underbrace{\text{CPRF}(🔑, x)}_{r_0}, \underbrace{\text{CPRF}(🗝, x)}_{r_1})$

$y_1^{(x)} = (\underbrace{F_k(x) = {}^0\!/_1}_{b}, \underbrace{\text{CPRF}(🔑/🗝, x)}_{r_b})$

Contributions

Efficient Public-Key PCF for OT Correlations from Lattices

In this talk



Secret-Power Ring Learning with Errors

Efficient
Pseudorandomly Constrained PRF

CPRF for
(w)PRFs and their complement

PCF for OT

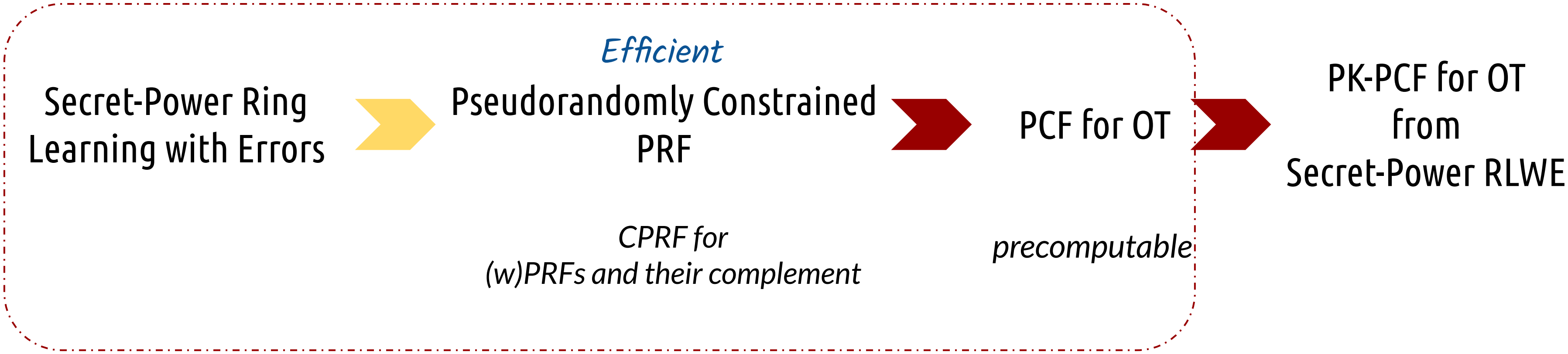
precomputable

PK-PCF for OT
from
Secret-Power RLWE

Contributions

Efficient Public-Key PCF for OT Correlations from Lattices

In this talk



Secret-Power Ring Learning with Errors

Efficient

Pseudorandomly Constrained PRF

CPRF for (w)PRFs and their complement

PCF for OT

precomputable

PK-PCF for OT from Secret-Power RLWE

A PRF
from
Ring LWE

PRFs from Ring LWE

(Ring R_q)

- **Master Secret Key :**

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

PRFs from Ring LWE

$P : \{0,1\}^n \times R_q^n \to R_q$

(Ring R_q)

- **Master Secret Key :**

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

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

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

PRFs from Ring LWE

$P : \{0,1\}^n \times R_q^n \to R_q$

(Ring R_q)

- **Master Secret Key :**

  msk $:= \left((k_1, \dots, k_n) \overset{\$}{\leftarrow} R_q^n,\ s, a \overset{\$}{\leftarrow} R_q\right)$

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

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

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

PRFs from Ring LWE

$P : \{0,1\}^n \times R_q^n \to R_q$ *(with range invertible in R_q)*

(Ring R_q)

- **Master Secret Key :**

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

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

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

No-Evaluation Security

$as + e$ looks random

(Ring LWE)

PRFs from Ring LWE

$P : \{0,1\}^n \times R_q^n \to R_q$ *(with range invertible in R_q)*

(Ring R_q)

- **Master Secret Key :**

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

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

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

No-Evaluation Security

$as + e$ looks random

(Ring LWE)

Full security via Random Oracle

A Constrained PRF
from
Secret-Power Ring LWE

Constrained PRFs from Secret-Power Ring LWE

(Ring R_q)

- **Master Secret Key :**

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

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

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

Constrained PRFs from Secret-Power Ring LWE

Constraint: 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 :**

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

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

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

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

Constrained PRFs from Secret-Power Ring LWE

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

(Ring R_q)

- **Master Secret Key :**

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

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

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

- **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 :**

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

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

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

Constrained PRFs from Secret-Power Ring LWE

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

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

(Ring R_q)

- **Master Secret Key :**

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

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

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

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

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

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

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 :**

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

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

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

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

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

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

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

Constrained PRFs from Secret-Power Ring LWE

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

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

(Ring R_q)

- **Master Secret Key :**

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

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

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

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

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

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

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

  $$=as\cdot P\left(\vec{x},\vec{z}\right)+as\cdot\frac{1}{s}(\cdots)$$

Constrained PRFs from Secret-Power Ring LWE

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

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

(Ring R_q)

- **Master Secret Key :**

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

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

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

$$= as \cdot P\left(\vec{x}, \vec{z}\right) + as \cdot \frac{1}{s} Q\left(\vec{x}, \vec{z}, 1/s, \vec{\ell}\right)$$

Constrained PRFs from Secret-Power Ring LWE

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

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

(Ring R_q)

- **Master Secret Key :**

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

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

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

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

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

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

  $=as\cdot P\left(\vec{x},\vec{z}\right)+a\cdot Q\left(\vec{x},\vec{z},1/s,\vec{\ell}\right)$

Constrained PRFs from Secret-Power Ring LWE

Constraint: **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 :**

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

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

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

  $$= as \cdot P\left(\vec{x}, \vec{z}\right) + a \cdot Q\left(\vec{x}, \vec{z}, 1/s, \vec{\ell}\right)$$

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

Constrained PRFs from Secret-Power Ring LWE

Constraint: 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 :**

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

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

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

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

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

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

  $$= as \cdot P\left(\vec{x}, \vec{z}\right) + a \cdot Q\left(\vec{x}, \vec{z}, 1/s, \vec{\ell}\right)$$

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

  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 $P\left(\vec{x}, \vec{z}\right) = 0$ $\quad\left(P : \{0,1\}^n \times R_q^n \to R_q\right)$

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

(Ring R_q)

- **Master Secret Key :**

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

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

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

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

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

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

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

  $= as \cdot P\left(\vec{x}, \vec{z}\right) + a \cdot Q\left(\vec{x}, \vec{z}, 1/s, \vec{\ell}\right)$

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

  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 $P\left(\vec{x}, \vec{z}\right) = 0$ $\quad \left(P : \{0,1\}^n \times R_q^n \to R_q\right)$

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

(Ring R_q)

- **Master Secret Key :**

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

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

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

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

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

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

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

  $= as \cdot P\left(\vec{x}, \vec{z}\right) + a \cdot Q\left(\vec{x}, \vec{z}, 1/s, \vec{\ell}\right)$

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

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

  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 :**

  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: 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 :**

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

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

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

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

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

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

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 :**

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

- **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: 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 :**

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

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

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

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

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

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

- **Constrained Evaluation :**

  ① Find c$_i$'s such that

  symbolic variable

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

Constrained PRFs from Secret-Power Ring LWE

Constraint: 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

  symbolic variable

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

  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 $P\left(\vec{x}, \vec{z}\right) = 0$ $\left(P : \{0,1\}^n \times R_q^n \to R_q\right)$

(Ring R_q)

- **Master Secret Key :**

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

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

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

Equal when P(x,z)=0

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

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

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

- **Constrained Evaluation :**

  ① Find c_i's such that

  symbolic variable

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

  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 $P\left(\vec{x}, \vec{z}\right) = 0$ $\left(P : \{0,1\}^n \times R_q^n \to R_q\right)$

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

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

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

symbolic variable

Constrained PRFs from Secret-Power Ring LWE

Constraint: 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 :**

$$\textbf{msk} := \Big((k_1,\overset{\text{small}}{\ldots},k_n) \xleftarrow{\$} R_q^n,\ \overset{\text{small}}{s}, a \xleftarrow{\$} R_q\Big)$$

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

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

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

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

- **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: 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 :**

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

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

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

No-Evaluation 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 $\vec{\ell} = \vec{k} - s \cdot \vec{z}$

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

- **Constrained Evaluation :**

① Find c$_i$'s such that

symbolic variable

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

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 $P\left(\vec{x}, \vec{z}\right) = 0$ $\left(P : \{0,1\}^n \times R_q^n \to R_q\right)$

(Ring R_q)

- **Master Secret Key :**

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

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

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

No-Evaluation 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

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

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

Full security via random oracle

So What?

Our PK-PCF =
Our CPRF from secret-power RLWE
+ Goldreich-Applebaum-Raykov weak PRF ([Gol00,AR16])
+ public-key setup à la succinct HSS ([ARP24])

Work	Post-Quantum	OT Variant	Key-Size	OT/sec
[OSY21]	✗	OT	small	1
[BCMP**R**24]	✗	OT	small	30k
[CDDKS24]	✓	List OT	5.5 MB	1.2M
This Work	✓	OT	567 MB	540-1k
	✓	OT	200 MB	190-450k

All works use random oracles

Summary

Efficient Public-Key PCF for OT Correlations from Lattices

Thank You!

Secret-Power Ring Learning with Errors

Efficient
Pseudorandomly Constrained PRF

CPRF for (w)PRFs and their complement

PCF for OT

precomputable

PK-PCF for OT from Secret-Power RLWE

obtained via succinct HSS techniques

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.

[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.

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

References

[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.

GAR wPRF
as
a constraint

Goldreich-Applebaum-Raykov weak PRF

[Gol00,AR16]

GAR weak PRF

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

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

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

[Gol00,AR16]

GAR weak PRF

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

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

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 $O(\kappa+\tau)$