Fast Public-Key Silent OT and More from Constrained Naor-Reingold

Dung Bui[1], Geoffroy Couteau[1], Pierre Meyer[2], Alain Passelègue[3], and Mahshid Riahinia[4]

[1] Université Paris Cité, CNRS, IRIF, Paris, France.
[2] Aarhus Universitet, Denmark.
[3] CryptoLab, France.
[4] ENS de Lyon, Laboratoire LIP, France.

EUROCRYPT 2024 - Zurich

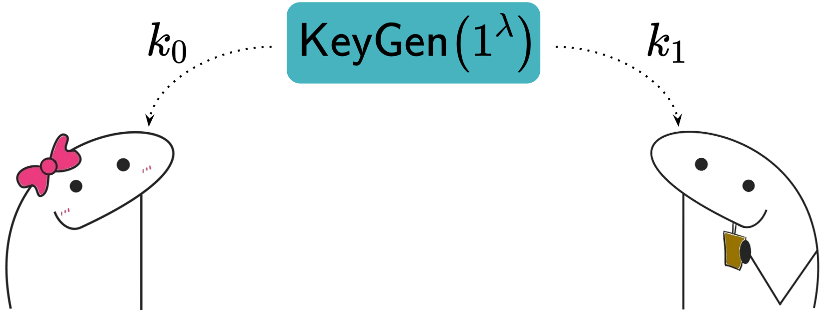
Pseudorandom Correlation Functions

Pseudorandom Correlation Functions (PCFs) [BCGIKS 20]

on-demand generation
of
correlated randomness

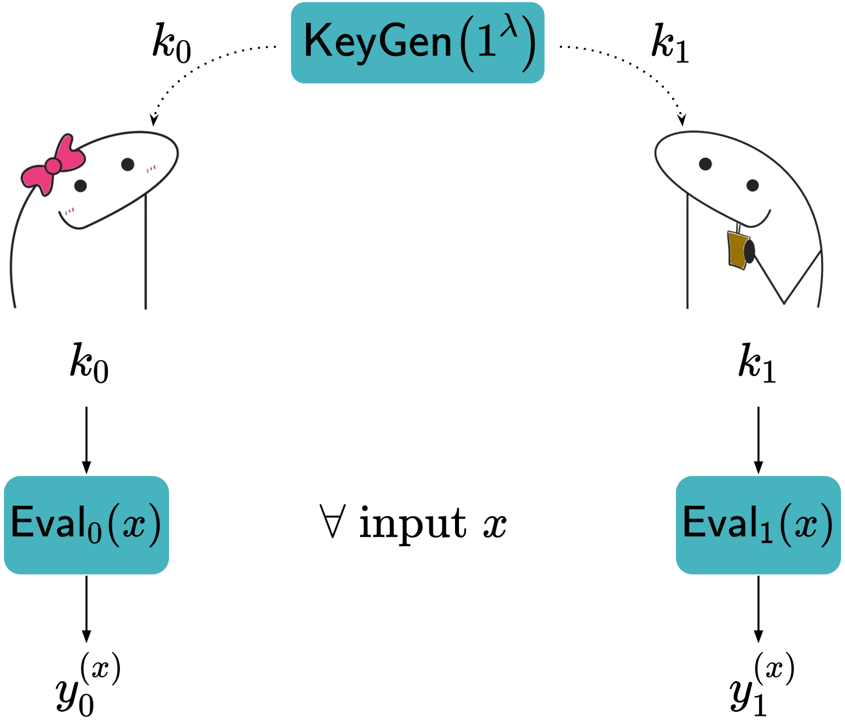
Pseudorandom Correlation Functions (PCFs) [BCGIKS 20]

on-demand generation
of
correlated randomness



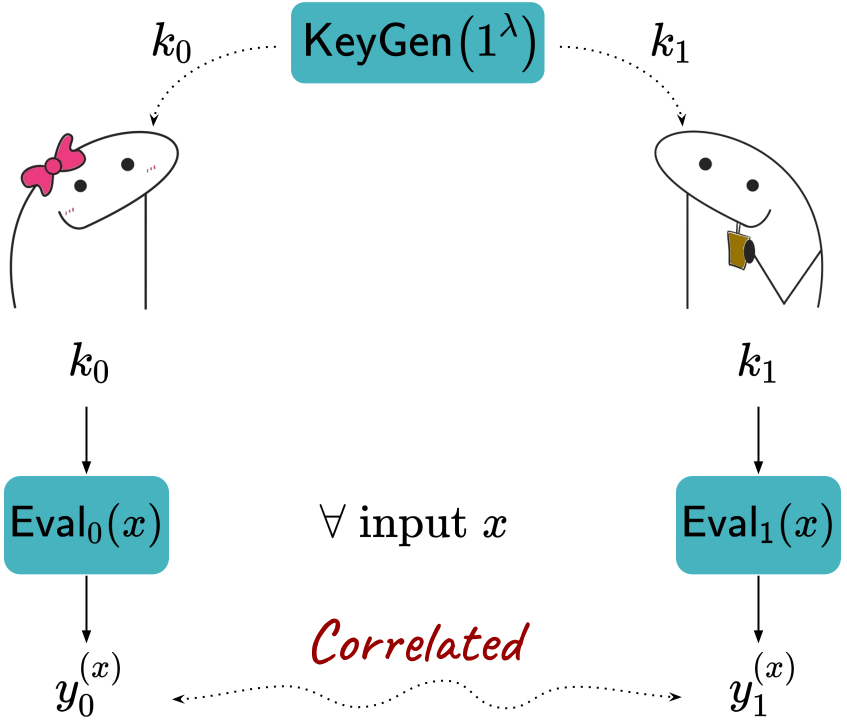
Pseudorandom Correlation Functions (PCFs) [BCGIKS 20]

on-demand generation
of
correlated randomness



Pseudorandom Correlation Functions (PCFs) [BCGIKS 20]

on-demand generation
of
correlated randomness

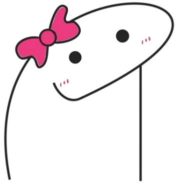


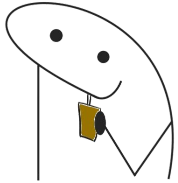
Pseudorandom Correlation Functions (PCFs) [BCGIKS 20]

on-demand generation
of
correlated randomness

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

k_0 $\qquad$ k_1





$k_0 \qquad k_1$

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

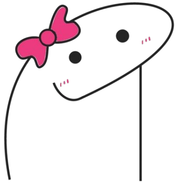
$y_0^{(x)} = (r_0, r_1)$ $\qquad$ OT-correlated (Oblivious Transfer) $\qquad$ $y_1^{(x)} = (b, r_b)$

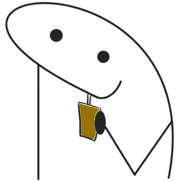
Pseudorandom Correlation Functions (PCFs) [BCGIKS 20]

on-demand generation
of
correlated randomness

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

k_0 $\quad$ k_1





k_0 $\quad$ k_1

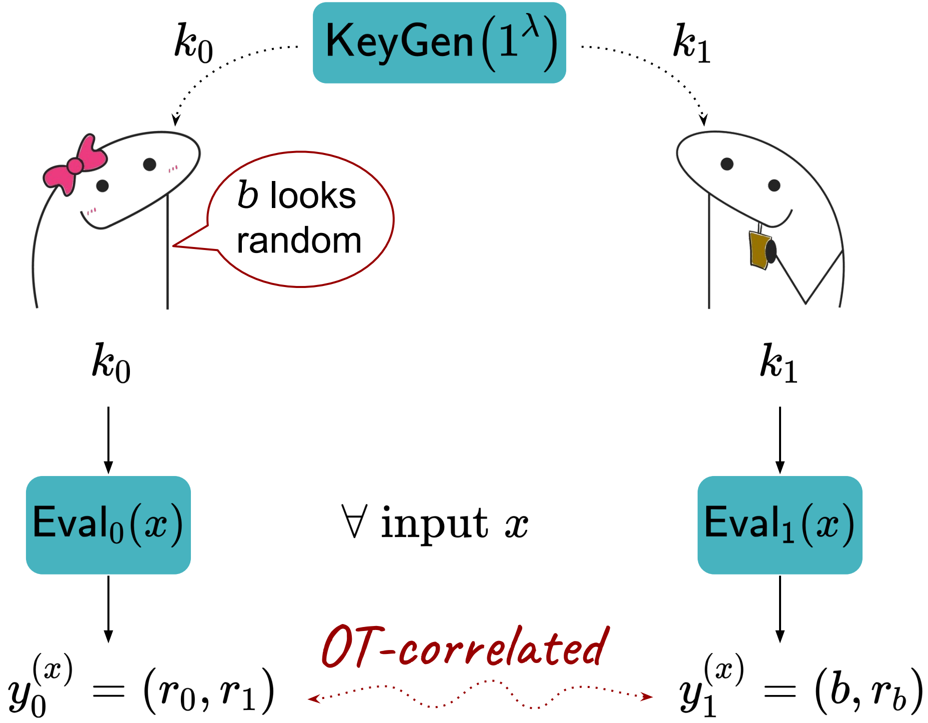
$\mathsf{Eval}_0(x)$ $\quad$ $\forall$ input x $\quad$ $\mathsf{Eval}_1(x)$

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

Pseudorandom Correlation Functions (PCFs) [BCGIKS 20]

on-demand generation
of
correlated randomness

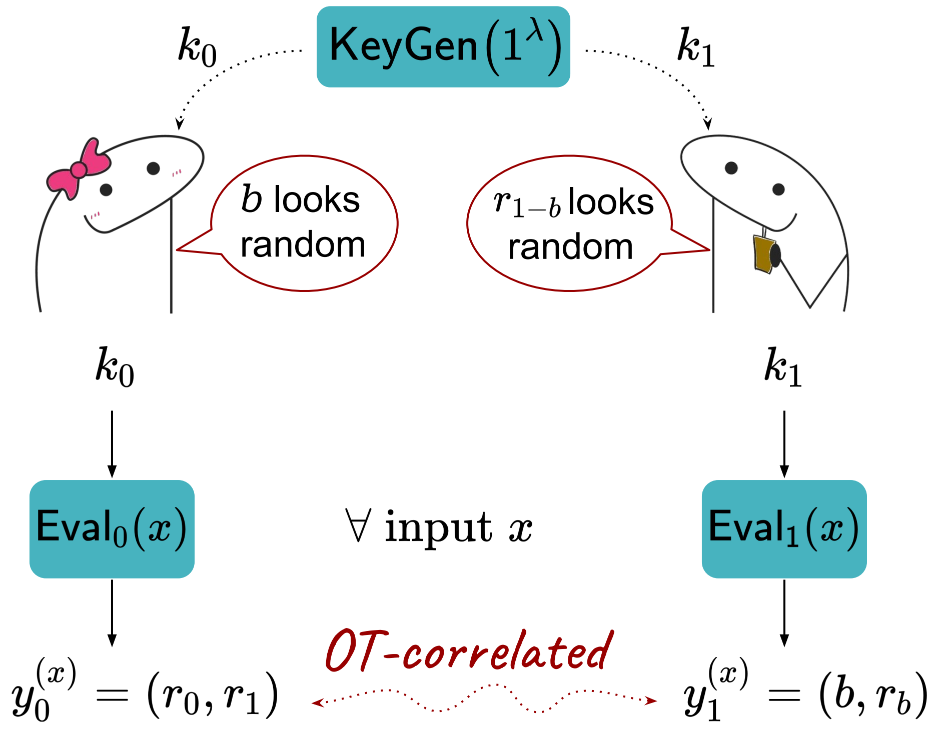
security:



Pseudorandom Correlation Functions (PCFs) [BCGIKS 20]

on-demand generation
of
correlated randomness

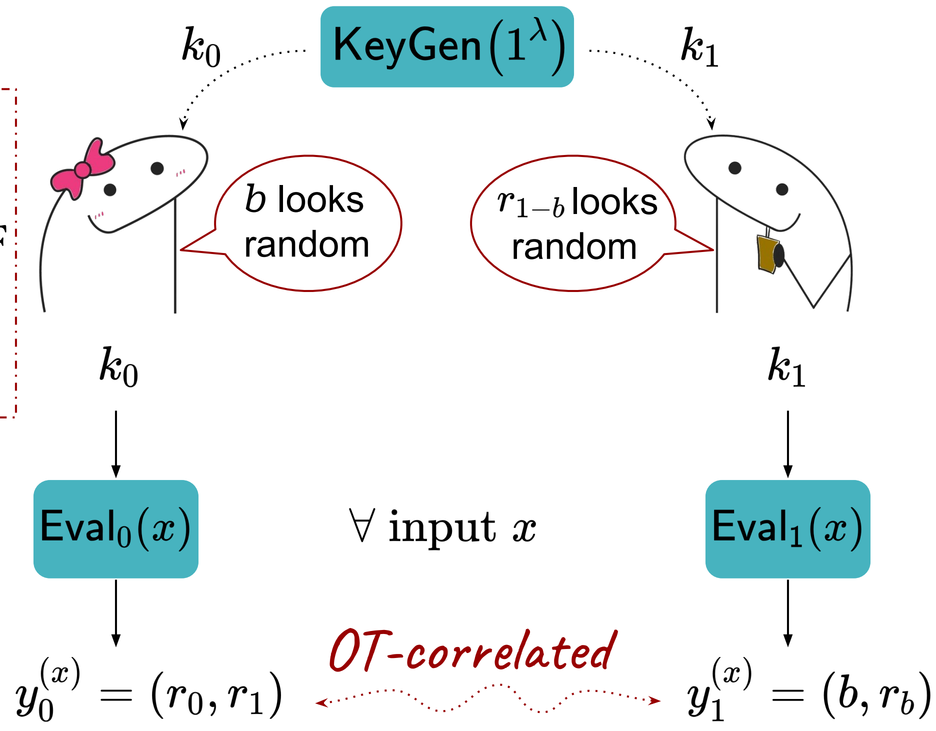
security:



Pseudorandom Correlation Functions (PCFs) [BCGIKS 20]

Our Contribution:

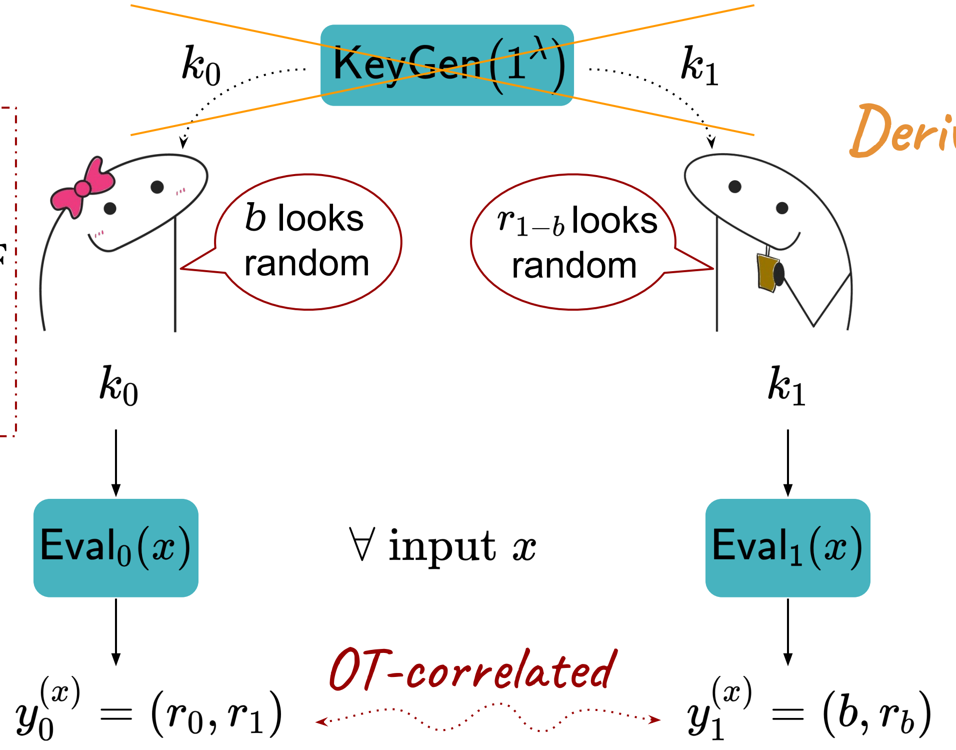
Efficient Public-Key PCF
for
OT Correlations



Pseudorandom Correlation Functions (PCFs) [BCGIKS 20]

Our Contribution:

Efficient Public-Key PCF
for
OT Correlations



Derive keys publicly

Our contributions

Efficient Public-Key PCF for OT Correlations
from
Naor-Reingold Constrained-PRF

Our contributions

Efficient Public-Key PCF for OT Correlations
from
Naor-Reingold Constrained-PRF

Tweaked
Naor-Reingold PRF

Our contributions

Efficient Public-Key PCF for OT Correlations
from
Naor-Reingold Constrained-PRF

Tweaked
Naor-Reingold PRF

Pseudorandomly-Constrained
PRF

Our contributions

Efficient Public-Key PCF for OT Correlations
from
Naor-Reingold Constrained-PRF

Tweaked Naor-Reingold PRF → Pseudorandomly-Constrained PRF → PCF for OT

Our contributions

Efficient Public-Key PCF for OT Correlations
from
Naor-Reingold Constrained-PRF

Tweaked Naor-Reingold PRF → Pseudorandomly-Constrained PRF → PCF for OT → PK-PCF for OT from Naor-Reingold

Our contributions

Efficient Public-Key PCF for OT Correlations
from
Naor-Reingold Constrained-PRF

Tweaked Naor-Reingold PRF → Pseudorandomly-Constrained PRF → PCF for OT → PK-PCF for OT from Naor-Reingold

+ reusable DV-NIZKs

Our contributions

Efficient Public-Key PCF for OT Correlations
from
Naor-Reingold Constrained-PRF

In this talk

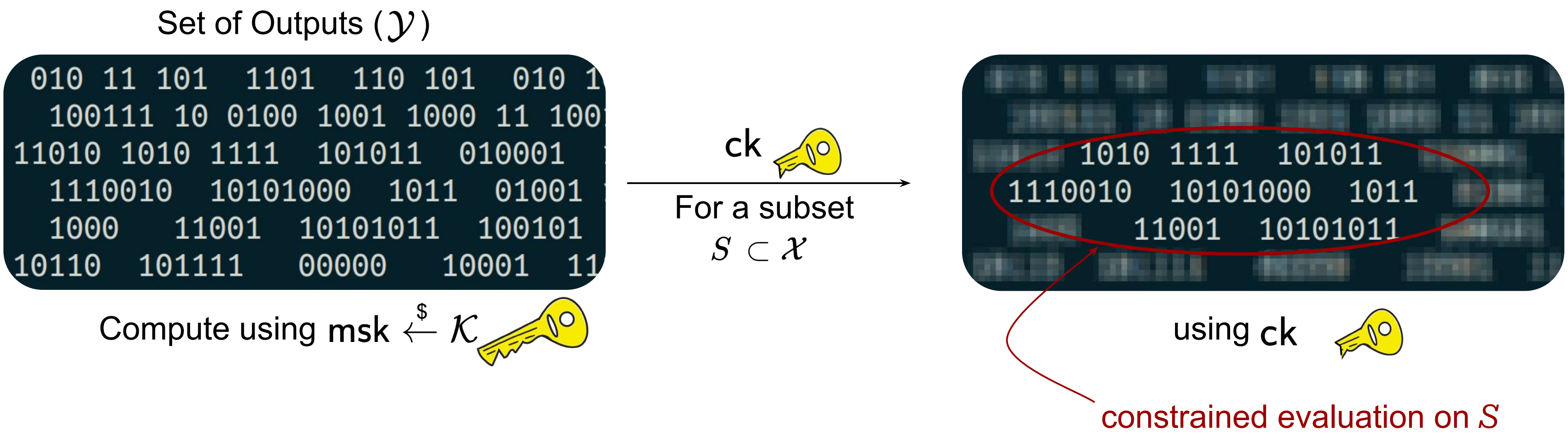
Tweaked Naor-Reingold PRF → Pseudorandomly-Constrained PRF → PCF for OT → PK-PCF for OT from Naor-Reingold

+ reusable DV-NIZKs

Constrained Pseudorandom Function

Constrained Pseudorandom Functions (**C**PRFs)

Pseudorandom Functions with constrained access to the evaluation.

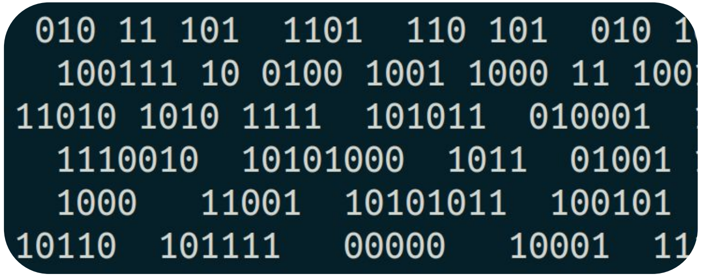


Constrained Pseudorandom Functions (**CPRFs**)

Pseudorandom Functions with constrained access to the evaluation.

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

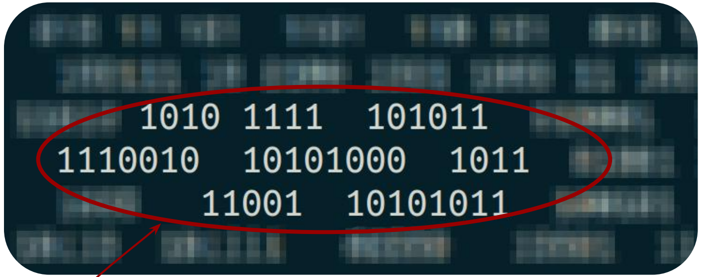
Set of Outputs ($\mathcal{Y}$)



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

ck 

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



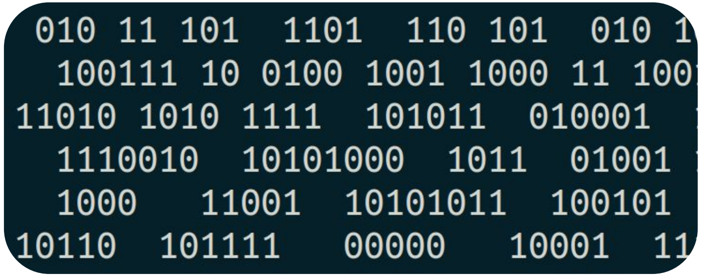
using ck 

constrained evaluation on S

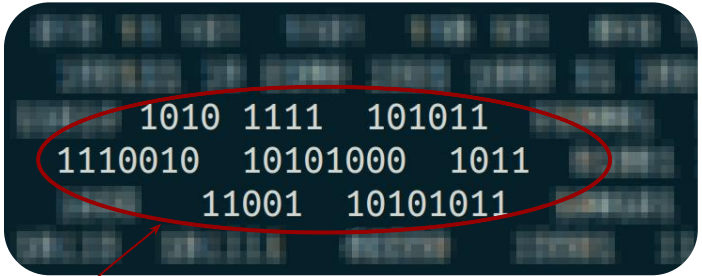
Constrained Pseudorandom Functions (**C**PRFs)

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

Set of Outputs ($\mathcal{Y}$)



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



using ck_F

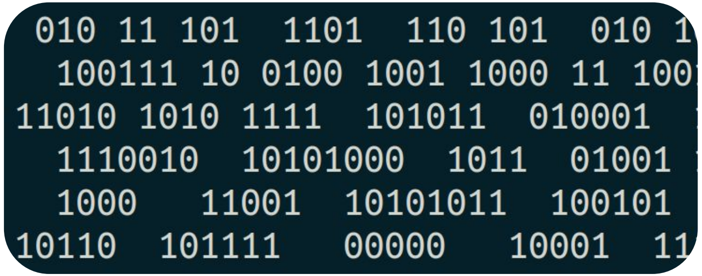
constrained evaluation on S_F

Constrained Pseudorandom Functions (**C**PRFs)

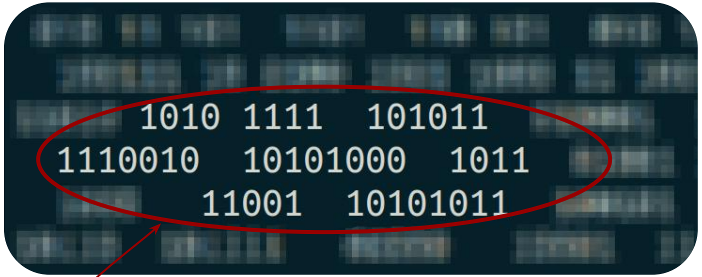
- Every predicate $\underbrace{F : \mathcal{X} \to \{0,1\}}$ defines a subset $S_F = \{x \in \mathcal{X} : F(x) = 0\}$

(w)PRF ⇝ Pseudorandomly Constrained PRF

Set of Outputs ($\mathcal{Y}$)



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



using ck_F 

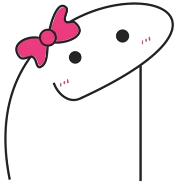
constrained evaluation on S_F

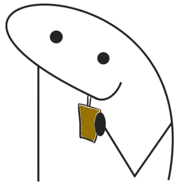
PCF for OT
from
Pseudorandomly-Constrained
PRFs

PCF for OT from CPRF

PCF for OT from CPRF

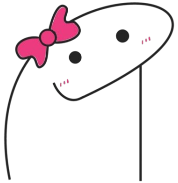
- wPRF $F_{\mathsf{k}} : \mathcal{X} \to \{0,1\}$

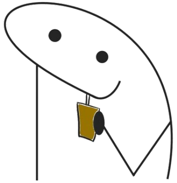




PCF for OT from CPRF

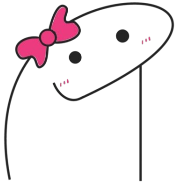
- wPRF $F_k : \mathcal{X} \to \{0,1\}$
- CPRF for F_k and $\overline{F_k}$

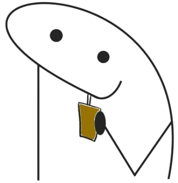




PCF for OT from CPRF

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





can generate a **ck** for either:

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

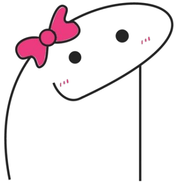
or

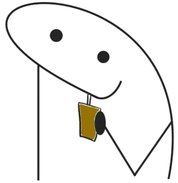
-all **x** s.t. $F_k(x)=1$

PCF for OT from CPRF

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

k_0 ← $\mathsf{KeyGen}(1^\lambda)$





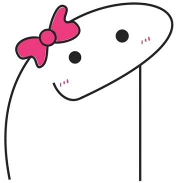
$$k_0 = \begin{cases} \mathsf{msk} \\ \mathsf{msk}' \end{cases}$$

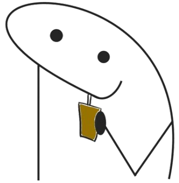
PCF for OT from CPRF

- 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

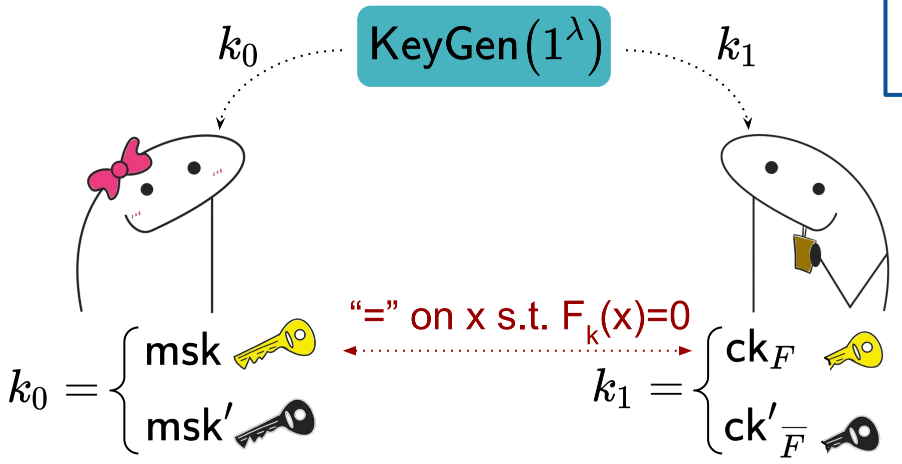




$$k_0 = \begin{cases} \mathsf{msk} \\ \mathsf{msk}' \end{cases} \qquad k_1 = \begin{cases} \mathsf{ck}_F \\ \mathsf{ck}'_{\overline{F}} \end{cases}, \mathsf{k}$$ (wPRF key)

PCF for OT from CPRF

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



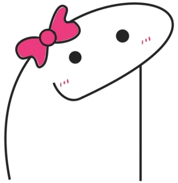
, k (wPRF key)

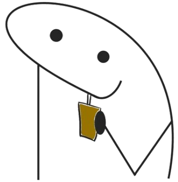
PCF for OT from CPRF

- 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





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

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

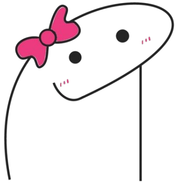
"=" on x s.t. $F_k(x)=1$

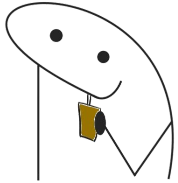
$k_1 = \begin{cases} \mathsf{ck}_F \\ \mathsf{ck}'_{\overline{F}} \end{cases}$, k (wPRF key)

PCF for OT from CPRF

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

$$k_0 \xleftarrow{} \mathsf{KeyGen}(1^\lambda) \xrightarrow{} k_1$$





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

$$\downarrow$$

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

$$\downarrow$$

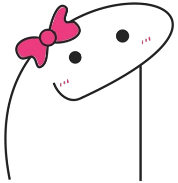
$$y_0^{(x)} = (\mathsf{CPRF}(\ , x), \mathsf{CPRF}(\ , x))$$

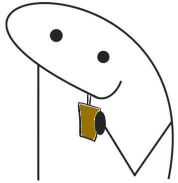
PCF for OT from CPRF

- 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





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

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

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

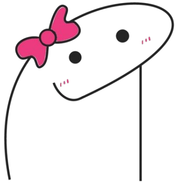
$$y_1^{(x)} = (F_{\mathsf{k}}(x) = {}^0/_1, \mathsf{CPRF}(\ /\ , x))$$

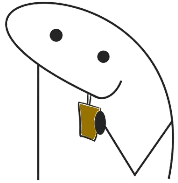
PCF for OT from CPRF

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

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

k_0 $\qquad$ 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)

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

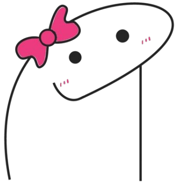
$$y_0^{(x)} = (\underbrace{\mathsf{CPRF}(\ ,x)}_{r_0}, \underbrace{\mathsf{CPRF}(\ ,x)}_{r_1})$$

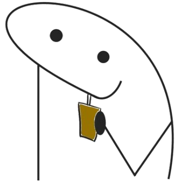
$$y_1^{(x)} = (\underbrace{F_{\mathsf{k}}(x) = {}^0/_1}_{b}, \underbrace{\mathsf{CPRF}(\ /\ ,x)}_{r_b})$$

PCF for OT from CPRF

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

$$k_0 \xleftarrow{} \mathsf{KeyGen}(1^\lambda) \xrightarrow{} k_1$$





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

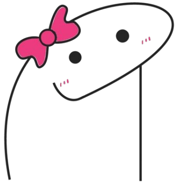
$$\mathsf{Eval}_0(x) \qquad\qquad \mathsf{Eval}_1(x)$$

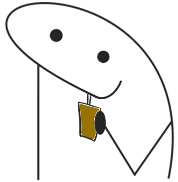
$$y_0^{(x)} = (\underbrace{\mathsf{CPRF}(\quad, x)}_{r_0}, \underbrace{\mathsf{CPRF}(\quad, x)}_{r_1}) \qquad y_1^{(x)} = (F_{\mathsf{k}}(x) = 0, \mathsf{CPRF}(\quad, x))$$

PCF for OT from CPRF

- 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_1





“=” on x s.t. $F_k(x)=0$

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

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

$\mathsf{Eval}_0(x)$

$\mathsf{Eval}_1(x)$

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

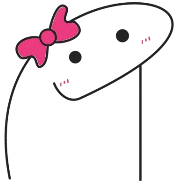
$$y_1^{(x)} = (F_{\mathsf{k}}(x) = 0, \mathsf{CPRF}(\;, x))$$

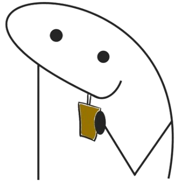
PCF for OT from CPRF

- 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





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

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

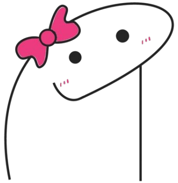
$$\mathsf{Eval}_0(x) \qquad \mathsf{Eval}_1(x)$$

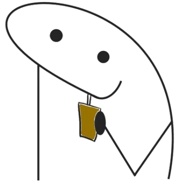
$$y_0^{(x)} = (\underbrace{\mathsf{CPRF}(\;, x)}_{r_0}, \underbrace{\mathsf{CPRF}(\;, x)}_{r_1}) \qquad y_1^{(x)} = (\underbrace{F_{\mathsf{k}}(x) = 0}_{0}, \underbrace{\mathsf{CPRF}(\;, x)}_{r_0})$$

PCF for OT from CPRF

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

$k_0 \xleftarrow{} \mathsf{KeyGen}(1^\lambda) \xrightarrow{} k_1$





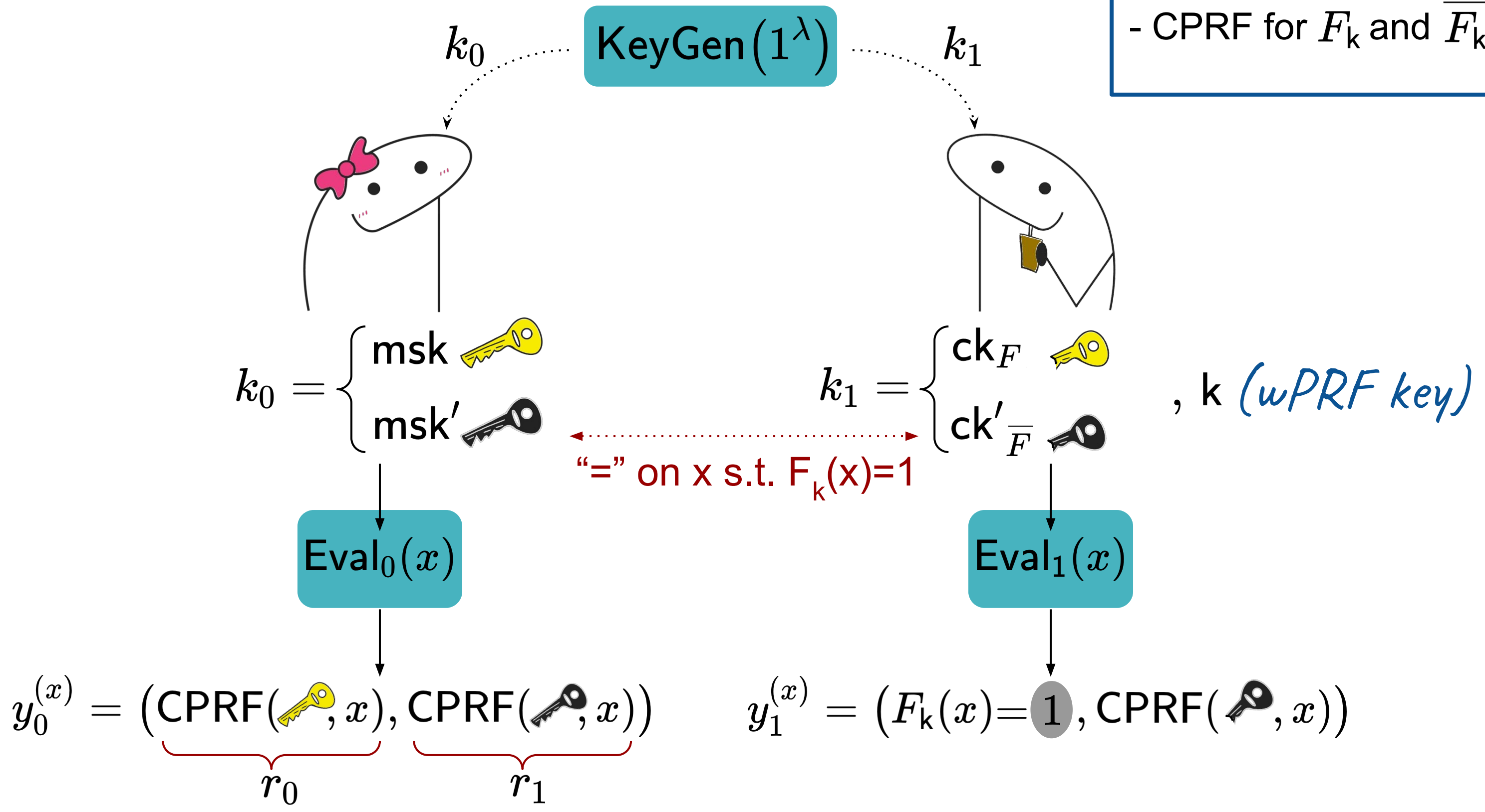
$$k_0 = \begin{cases} \mathsf{msk} \\ \mathsf{msk}' \end{cases} \qquad k_1 = \begin{cases} \mathsf{ck}_F \\ \mathsf{ck}'_{\overline{F}} \end{cases}, \ \mathsf{k} \ \text{(wPRF key)}$$

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

$$y_0^{(x)} = (\underbrace{\mathsf{CPRF}(\ , x)}_{r_0}, \underbrace{\mathsf{CPRF}(\ , x)}_{r_1}) \qquad y_1^{(x)} = (F_{\mathsf{k}}(x)=1, \mathsf{CPRF}(\ , x))$$

PCF for OT from CPRF

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

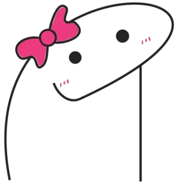


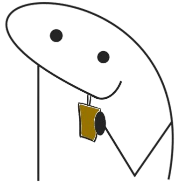
PCF for OT from CPRF

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

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

k_0 $\qquad$ k_1





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

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

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

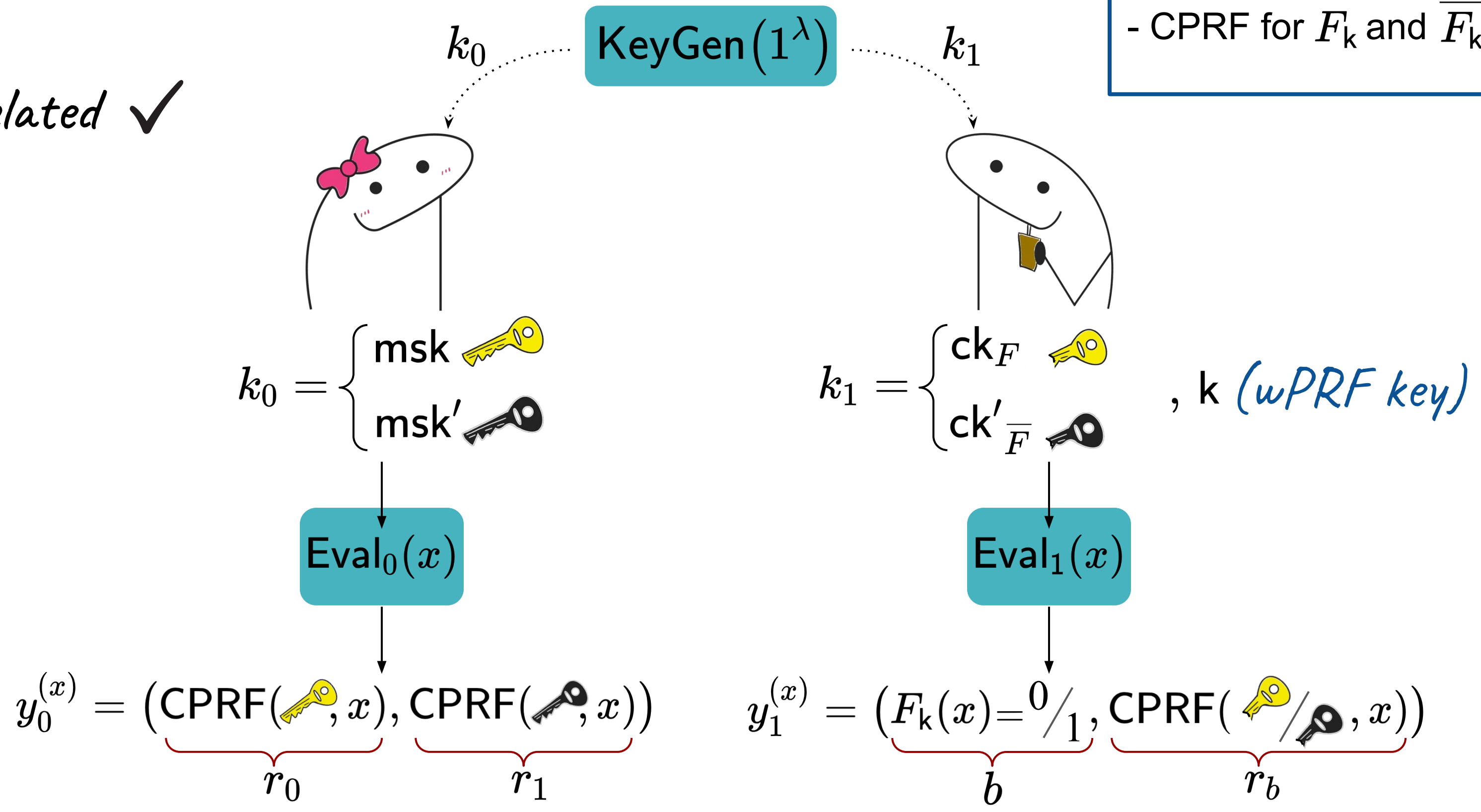
$$y_0^{(x)} = (\underbrace{\mathsf{CPRF}(\ ,x)}_{r_0}, \underbrace{\mathsf{CPRF}(\ ,x)}_{r_1})$$

$$y_1^{(x)} = (\underbrace{F_\mathsf{k}(x) = 1}_{1}, \underbrace{\mathsf{CPRF}(\ ,x)}_{r_1})$$

PCF for OT from CPRF

OT-correlated ✓

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



PCF for OT from CPRF

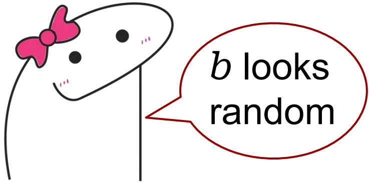
- wPRF $F_{\mathsf{k}} : \mathcal{X} \to \{0,1\}$
- CPRF for F_{k} and $\overline{F_{\mathsf{k}}}$

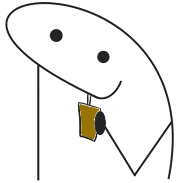
OT-correlated ✓

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

k_0 k_1

wPRF security





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

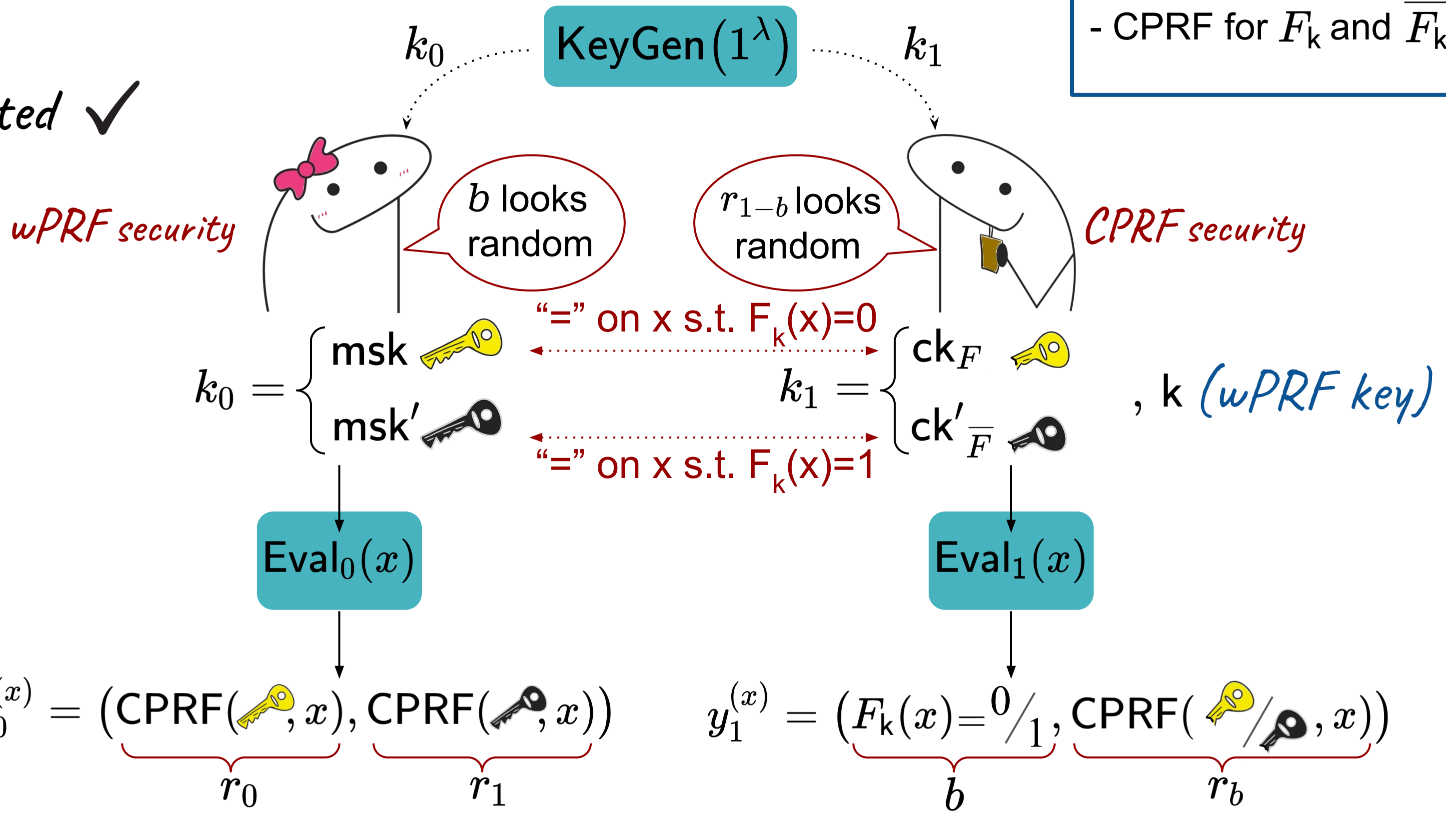
$$\mathsf{Eval}_0(x) \qquad \mathsf{Eval}_1(x)$$

$$y_0^{(x)} = (\underbrace{\mathsf{CPRF}(\ , x)}_{r_0}, \underbrace{\mathsf{CPRF}(\ , x)}_{r_1}) \qquad y_1^{(x)} = (\underbrace{F_{\mathsf{k}}(x) = {}^0\!/_1}_{b}, \underbrace{\mathsf{CPRF}(\ /\ , x)}_{r_b})$$

PCF for OT from CPRF

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

OT-correlated ✓



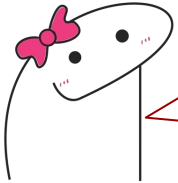
PCF for OT from CPRF

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

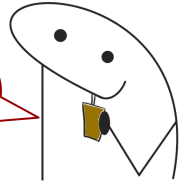
OT-correlated ✓

Secure ✓ *wPRF security* *CPRF security*

$$\text{KeyGen}(1^\lambda) \quad k_0, \; k_1$$



b looks random



r_{1-b} looks random

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

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

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

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

PCF for OT from CPRF

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

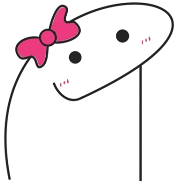
OT-correlated ✓

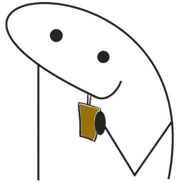
Secure ✓

Precomputable

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

k_0 $\qquad$ k_1





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

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

$$y_0^{(x)} = (\mathsf{CPRF}(\ , x), \mathsf{CPRF}(\ , x)) \qquad y_1^{(x)} = (F_{\mathsf{k}}(x) = {}^0/_1, \mathsf{CPRF}(\ /\ , x))$$

PCF for OT from CPRF

OT-correlated ✓

Secure ✓

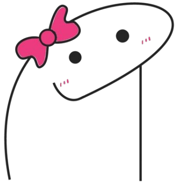
Precomputable

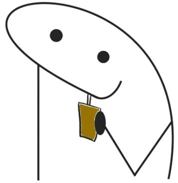
① ②

- 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





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

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

$\mathsf{Eval}_0(x)$

$\mathsf{Eval}_1(x)$

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

$y_1^{(x)} = (F_{\mathsf{k}}(x) = {}^{0}/_{1}, \mathsf{CPRF}(\ /\ , x))$

Our contributions

Efficient Public-Key PCF for OT Correlations
from
Naor-Reingold Constrained-PRF

Tweaked Naor-Reingold PRF → Pseudorandomly-Constrained PRF → PCF for OT → PK-PCF for OT from Naor-Reingold

CPRF for (w)PRFs and their complement

precomputable

Our contributions

Efficient Public-Key PCF for OT Correlations
from
Naor-Reingold Constrained-PRF

Tweaked Naor-Reingold PRF → Pseudorandomly-Constrained PRF → PCF for OT → PK-PCF for OT from Naor-Reingold

CPRF for (w)PRFs and their complement

precomputable

Our contributions

Efficient Public-Key PCF for OT Correlations
from
Naor-Reingold Constrained-PRF

Tweaked Naor-Reingold PRF	Pseudorandomly-Constrained PRF	PCF for OT	PK-PCF for OT from Naor-Reingold
CPRF for Inner-Product Membership	*CPRF for (w)PRFs and their complement*	*precomputable*	

Our contributions

Efficient Public-Key PCF for OT Correlations
from
Naor-Reingold Constrained-PRF

Tweaked
Naor-Reingold PRF

Pseudorandomly-Constrained
PRF

PCF for OT

PK-PCF for OT
from
Naor-Reingold

CPRF for
Inner-Product Membership

CPRF for
(w)PRFs and their complement

precomputable

wPRFs expressed as IPM

Naor-Reingold CPRF
for
Inner-Product Membership

Naor-Reingold PRF

($\mathbb{G}$ of prime order p)

Naor Reingold PRF

- **Master Secret Key :**

  $\mathsf{msk} := \left(g \xleftarrow{\$} \mathbb{G},\ (a_1, a_2, \ldots, a_n) \xleftarrow{\$} (\mathbb{Z}_p^*)^n\right)$

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

  $F_{\mathsf{msk}}(x) := g^{\prod_{i=1}^{n} a_i^{x_i}}$

$\boxed{\text{security: DDH assumption}}$

Naor-Reingold **C**PRF ($\mathbb{G}$ of prime order p)

$\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ s.t.

$\langle \vec{x}, \vec{z} \rangle = 0$

Naor Reingold PRF

- **Master Secret Key :**

  $\mathsf{msk} := \left(g \xleftarrow{\$} \mathbb{G},\ (a_1, a_2, \ldots, a_n) \xleftarrow{\$} (\mathbb{Z}_p^*)^n\right)$

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

  $F_{\mathsf{msk}}(x) := g^{\prod_{i=1}^{n} a_i^{x_i}}$

Constraining Inner-Product

- **Constrained Key for** $\vec{z} = \overbrace{z_1, z_2, \ldots, z_n}^{\text{binary}}$ **:**

- **Constrained Evaluation:**

Naor-Reingold **C**PRF ($\mathbb{G}$ of prime order p)

$\mathsf{ck}_{\vec{z}}$ can evaluate on all $\vec{x}$ s.t.

$\langle \vec{x}, \vec{z} \rangle = 0$

Naor Reingold PRF

- **Master Secret Key :**

$$\mathsf{msk} := \left(g \xleftarrow{\$} \mathbb{G},\ (a_1, a_2, \ldots, a_n) \xleftarrow{\$} (\mathbb{Z}_p^*)^n\right)$$

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

$$F_{\mathsf{msk}}(x) := g^{\prod_{i=1}^{n} a_i^{x_i}}$$

Constraining Inner-Product

- **Constrained Key for** $\vec{z} = z_1, z_2, \ldots, z_n$ **:**

$$\mathsf{ck}_{\vec{z}} := \left(g, \left\{a_i \cdot r^{-z_i}\right\}_{i \in [n]}\right);\ r \xleftarrow{\$} \mathbb{Z}_p^*$$

- **Constrained Evaluation:**

Naor-Reingold **C**PRF ($\mathbb{G}$ of prime order p)

ck$_{\vec{z}}$ can evaluate on all $\vec{x}$ s.t.

$\langle \vec{x}, \vec{z} \rangle = 0$

Naor Reingold PRF

- **Master Secret Key :**

  $$\mathsf{msk} := \left(g \xleftarrow{\$} \mathbb{G},\ (a_1, a_2, \ldots, a_n) \xleftarrow{\$} (\mathbb{Z}_p^*)^n\right)$$

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

  $$F_{\mathsf{msk}}(x) := g^{\prod_{i=1}^n a_i^{x_i}}$$

Constraining Inner-Product

- **Constrained Key for** $\vec{z} = z_1, z_2, \ldots, z_n$ **:**

  $$\mathsf{ck}_{\vec{z}} := \left(g, \left\{a_i \cdot r^{-z_i}\right\}_{i \in [n]}\right);\ r \xleftarrow{\$} \mathbb{Z}_p^*$$

- **Constrained Evaluation:**

  $$F_{\mathsf{ck}_{\vec{z}}}(x) = g^{\prod_{i=1}^n (a_i \cdot r^{-z_i})^{x_i}}$$

  $$= \left(g^{\prod_{i=1}^n a_i^{x_i}}\right)^{r^{-\langle \vec{x}, \vec{z} \rangle}}$$

Naor-Reingold **C**PRF ($\mathbb{G}$ of prime order p)

ck$_{\vec{z}}$ can evaluate on all $\vec{x}$ s.t.

$\langle \vec{x}, \vec{z} \rangle = 0$

Naor Reingold PRF

- **Master Secret Key :**

  $$\mathsf{msk} := \left(g \xleftarrow{\$} \mathbb{G},\ (a_1, a_2, \ldots, a_n) \xleftarrow{\$} (\mathbb{Z}_p^*)^n\right)$$

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

  $$F_{\mathsf{msk}}(x) := g^{\prod_{i=1}^n a_i^{x_i}}$$

equal if

$\langle \vec{x}, \vec{z} \rangle = 0$

Constraining Inner-Product

- **Constrained Key for $\vec{z} = z_1, z_2, \ldots, z_n$:**

  $$\mathsf{ck}_{\vec{z}} := \left(g, \left\{a_i \cdot r^{-z_i}\right\}_{i \in [n]}\right);\ r \xleftarrow{\$} \mathbb{Z}_p^*$$

- **Constrained Evaluation:**

  $$F_{\mathsf{ck}_{\vec{z}}}(x) = g^{\prod_{i=1}^n (a_i \cdot r^{-z_i})^{x_i}}$$

  $$= \left(g^{\prod_{i=1}^n a_i^{x_i}}\right)^{r^{-\langle \vec{x}, \vec{z} \rangle}}$$

Naor-Reingold CPRF (𝔾 of prime order p)

ck$_{\vec{z}}$ can evaluate on all $\vec{x}$ s.t.

$\langle \vec{x}, \vec{z} \rangle = 0$

Naor Reingold PRF

- **Master Secret Key :**

  $$\mathsf{msk} := \left(g \xleftarrow{\$} \mathbb{G},\ (a_1, a_2, \ldots, a_n) \xleftarrow{\$} (\mathbb{Z}_p^*)^n\right)$$

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

  $$F_{\mathsf{msk}}(x) := g^{\prod_{i=1}^n a_i^{x_i}}$$

equal if

$\langle \vec{x}, \vec{z} \rangle = 0$

No-Evaluation Security

$g^{r^{\langle \vec{x}, \vec{z} \rangle}}$ looks random

(unconditional)

Constraining Inner-Product

- **Constrained Key for $\vec{z} = z_1, z_2, \ldots, z_n$:**

  $$\mathsf{ck}_{\vec{z}} := \left(g, \left\{a_i \cdot r^{-z_i}\right\}_{i \in [n]}\right);\ r \xleftarrow{\$} \mathbb{Z}_p^*$$

- **Constrained Evaluation:**

  $$F_{\mathsf{ck}_{\vec{z}}}(x) = g^{\prod_{i=1}^n (a_i \cdot r^{-z_i})^{x_i}}$$

  $$= \left(g^{\prod_{i=1}^n a_i^{x_i}}\right)^{r^{-\langle \vec{x}, \vec{z} \rangle}}$$

Full security via random oracle

Naor-Reingold **C**PRF ($\mathbb{G}$ of prime order p)

Naor Reingold PRF

- **Master Secret Key :**

  $\mathsf{msk} := \left(g \xleftarrow{\$} \mathbb{G},\ (a_1, a_2, \ldots, a_n) \xleftarrow{\$} (\mathbb{Z}_p^*)^n\right)$

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

  $F_{\mathsf{msk}}(x) := g^{\prod_{i=1}^{n} a_i^{x_i}}$

Constraining Inner-Product **Membership**

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

- **Constrained Evaluation:**

Naor-Reingold **C**PRF ($\mathbb{G}$ of prime order p)

$\mathsf{ck}_{(\vec{z},S)}$ can evaluate on all $\vec{x}$ s.t.

$\langle \vec{x}, \vec{z} \rangle \in S$

Naor Reingold PRF

- **Master Secret Key :**

  $\mathsf{msk} := \left(g \xleftarrow{\$} \mathbb{G},\ (a_1, a_2, \ldots, a_n) \xleftarrow{\$} (\mathbb{Z}_p^*)^n\right)$

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

  $F_{\mathsf{msk}}(x) := g^{\prod_{i=1}^{n} a_i^{x_i}}$

Constraining Inner-Product **Membership**

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

- **Constrained Evaluation:**

Naor-Reingold **C**PRF ($\mathbb{G}$ of prime order p)

ck$_{(\vec{z},S)}$ can evaluate on all $\vec{x}$ s.t. $\langle \vec{x}, \vec{z} \rangle \in S$

Naor Reingold PRF

- **Master Secret Key :**

  $\mathsf{msk} := \left(g \xleftarrow{\$} \mathbb{G},\ (a_1, a_2, \ldots, a_n) \xleftarrow{\$} (\mathbb{Z}_p^*)^n\right)$

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

  $F_{\mathsf{msk}}(x) := g^{\prod_{i=1}^n a_i^{x_i}}$

Constraining Inner-Product **Membership**

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

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

  $(r \xleftarrow{\$} \mathbb{Z}_p^*)$

- **Constrained Evaluation:**

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

  $= \left(g^{\prod_{i=1}^n a_i^{x_i}}\right)^{r^s \cdot r^{-\langle \vec{x}, \vec{z} \rangle}}$

Naor-Reingold **C**PRF ($\mathbb{G}$ of prime order p)

ck$_{(\vec{z},S)}$ can evaluate on all $\vec{x}$ s.t.

$\langle \vec{x}, \vec{z} \rangle \in S$

Naor Reingold PRF

- **Master Secret Key :**

  msk : $= \left(g \xleftarrow{\$} \mathbb{G},\ (a_1, a_2, \ldots, a_n) \xleftarrow{\$} (\mathbb{Z}_p^*)^n\right)$

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

  $$F_{\mathsf{msk}}(x) := g^{\prod_{i=1}^n a_i^{x_i}}$$

equal if

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

Constraining Inner-Product **Membership**

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

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

  $(r \xleftarrow{\$} \mathbb{Z}_p^*)$

- **Constrained Evaluation:**

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

  $$= \left(g^{\prod_{i=1}^n a_i^{x_i}}\right)^{r^s \cdot r^{-\langle \vec{x}, \vec{z} \rangle}}$$

Naor-Reingold **C**PRF ($\mathbb{G}$ of prime order p)

$\mathsf{ck}_{(\vec{z},S)}$ can evaluate on all $\vec{x}$ s.t. $\langle \vec{x}, \vec{z} \rangle \in S$

Naor Reingold PRF

- **Master Secret Key :**

  $\mathsf{msk} := \left(g \xleftarrow{\$} \mathbb{G},\ (a_1, a_2, \ldots, a_n) \xleftarrow{\$} (\mathbb{Z}_p^*)^n\right)$

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

  $F_{\mathsf{msk}}(x) := g^{\prod_{i=1}^n a_i^{x_i}}$

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

No-Evaluation Security

$g^{r^{\langle \vec{x}, \vec{z} \rangle}}$ *looks random given* $\left(g^{r^s}\right)_{s \in S}$

(sparse power-DDH)

Constraining Inner-Product **Membership**

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

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

  $(r \xleftarrow{\$} \mathbb{Z}_p^*)$

- **Constrained Evaluation:**

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

  $$= \left(g^{\prod_{i=1}^n a_i^{x_i}}\right)^{r^s \cdot r^{-\langle \vec{x}, \vec{z} \rangle}}$$

Full security via random oracle

Inner-Product Membership Predicates

IPM Predicates

- Inner-Product Equality & Inequality
- Puncturing
  - Puncturing a Hamming ball
  - **Puncturable PRF in NC[1]**
- **weak PRFs**
  - LWR [BPR12],[BIPSW18]
  - XOR-MAJ (GAR) [Gol00,AR16]

[BPR12] weak PRF:

$$F_{\vec{k}}(\vec{x}) = \lfloor \langle \vec{k}, \vec{x} \rangle \rceil_2$$

$$\vec{k}, \vec{x} \in \mathbb{Z}_q^n$$

$$F_{\vec{k}}(\vec{x}) = 0 \iff \langle \vec{k}, \vec{x} \rangle \in S$$

$$S = \{ s \in \mathbb{Z}_{n \cdot q^2} \mid \lfloor s \rceil_2 = 0 \}$$

Conclusion

Efficient Public-Key PCF for OT Correlations
from
Naor-Reingold Constrained-PRF

Tweaked Naor-Reingold PRF → Pseudorandomly-Constrained PRF → PCF for OT → PK-PCF for OT from Naor-Reingold

CPRF for Inner-Product Membership

CPRF for (w)PRFs and their complement

wPRFs expressed as IPM

precomputable

+ reusable DV-NIZKs

+ lots of optimizations

Conclusion

Efficient Public-Key PCF for OT Correlations
from
Naor-Reingold Constrained-PRF

Tweaked Naor-Reingold PRF → Pseudorandomly-Constrained PRF → PCF for OT → PK-PCF for OT from Naor-Reingold

CPRF for Inner-Product Membership

CPRF for (w)PRFs and their complement

precomputable

+ reusable DV-NIZKs

+ lots of optimizations

wPRFs expressed as IPM

Thank You!

ia.cr/2024/178