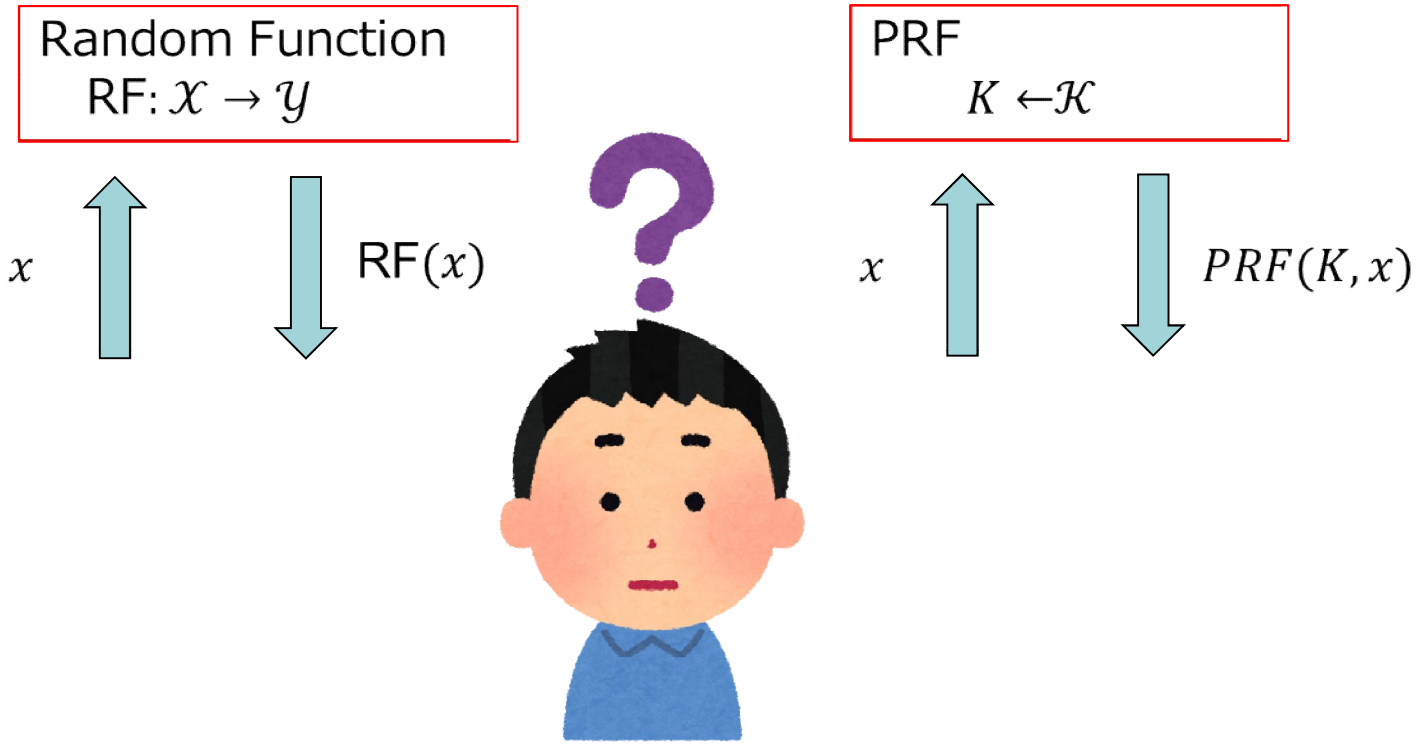
Constrained PRF for NC^1 in Traditional Group (a.k.a. Pairing-Free Group)

Nuttapong Attrapadung (AIST), Takahiro Matsuda (AIST),
Ryo Nishimaki (NTT), Shota Yamada (AIST), Takashi Yamakawa (NTT)

2018.08.20
CRYPTO 2018

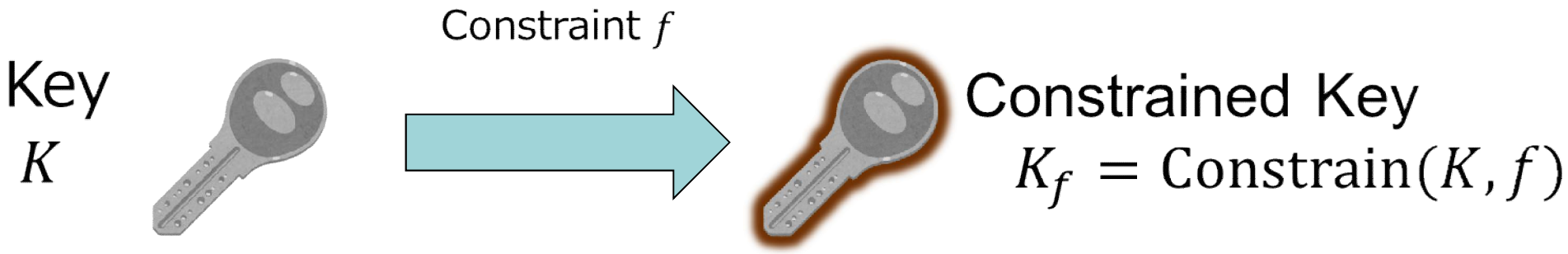
Pseudorandom Function (PRF)

- PRF is a keyed function that is indistinguishable from a random function via oracle accesses.
- There is a construction based on any OWF [GGM86].



Constrained PRF (CPRF) [BW13, KPTZ13, BGI14]

$$PRF(K, x) \rightarrow y$$



Correctness : If $f(x) = 0$

$PRF(K_f, x) = PRF(K, x)$

Security : If $f(x) = 1$

$PRF(K, x)$ is pseudorandom given K_f

Motivation 1: CPRF on Pairing-Free Group

- There are several known constructions of CPRFs.

Collusion-resistant setting:
- Multilinear-map-based [BW13]
- Obfuscation-based [BZ14]

Single-key setting:
- Lattice-based [BV15]

* We omit CPRFs for specific functionalities like puncturing.

Construction on Pairing-free group?

Motivation 2: Private CPRF [BLW17]

- CPRF is said to be **private** if K_f does not reveal f.

Collusion-resistant setting:
- Multilinear-map-based [BLW17]
- Obfuscation-based [BLW17]

Single-key setting:
- Lattice-based [BKM17,CC17,BTVW17]

Construction on Pairing-free group?

Our Results

- Result 1: **CPRF for NC^1** on pairing-free group
  - Selectively single-key secure
    under L-DDHI assumption on $\mathbb{QR}_q$ + DDH assumption

- Result 2: **Private CPRF for bit-fixing** on pairing-free group
  - Selectively single-key secure under DDH assumption

Core Technique:
Correlated-Input Secure Hash Function

Selective Single-key Security of CPRF

coin’

Key query $f \in \mathcal{F}$

$K_f = \mathrm{Constrain}(K, f)$

Evaluation query x

$\mathrm{PRF}($

Challenge query x^*

$\mathrm{PRF}(K, x^*)$ if coin=1

$y \leftarrow \mathcal{Y}$ if coin=0

$K \leftarrow \mathcal{K}$

coin← $\{0,1\}$

Adversary must follow the following rules:

1. $f(x^*) = 1$
2. x^* is not queried as an evaluation query

CPRF is selectively single-key secure if |Pr[coin’=coin]-1/2|=negl.

Roadmap

Selectively single-key secure CPRF for NC^1
against adversaries that make **no evaluation queries**

Correlated-input secure hash

Selectively secure single-key CPRF for NC^1
against adversaries that make **unbounded evaluation queries**

First Step: No-Evaluation-Secure CPRF

- Let U be a universal circuit for a function class $\mathcal{F}$.
  - i.e. we have $U((f_1, \dots, f_z), x) = f(x)$
- Assume the degree of U as a multivariate polynomial is at most $D = \mathrm{poly}(\lambda)$.
  - Such a universal circuit exists for NC^1 [CH85]
- Let G be a cyclic group of order p with a generator g.

$$K = ((b_1, \dots, b_z) \leftarrow \mathbb{Z}_p^z, \alpha \leftarrow \mathbb{Z}_p^*)$$

$$PRF(K, x) := g^{\frac{U((b_1,\dots,b_z),x)}{\alpha}}$$

Evaluation by Constrained Key

$$PRF(K,x) := g^{\frac{U((b_1,\ldots,b_Z),x)}{\alpha}}$$

$\mathrm{Constrain}(K,f)$: For $i \in [z]$, compute $\boldsymbol{b_i' := \frac{(b_i - f_i)}{\alpha} \bmod p}$

Output $K_f := (f, b_1', \ldots, b_Z', g, g^{\alpha}, g^{\alpha^2}, \ldots, g^{\alpha^{D-1}})$

$\mathrm{CEval}\left(K_f := (f, b_1', \ldots, b_Z', g, g^{\alpha}, g^{\alpha^2}, \ldots, g^{\alpha^{D-1}}), x\right)$:

By the definition of b_i', we have $\boldsymbol{b_i = \alpha b_i' + f_i \bmod p}$

By using this equation, we can expand

$$U\big((b_1,\ldots,b_z),x\big) = \underbrace{U\big((f_1,\ldots,f_z),x\big)}_{= f(x) = 0} + \sum_{i\in[D]} c_i \alpha^i$$

$$PRF(K,x) = g^{\sum_{i\in[D]} c_i \alpha^{i-1}}$$

L-decisional Diffie-Hellman Inversion Assumption (L-DDHI Assumption)

L-DDHI Assumption

$$g \leftarrow G, \alpha \leftarrow \mathbb{Z}_p^*$$

Given $(g, g^{\alpha}, g^{\alpha^2}, \ldots, g^{\alpha^L})$

$$g^{\frac{1}{\alpha}} \approx R \leftarrow G$$

Theorem: The scheme is selectively single-key secure against adversary that makes **no evaluation queries** under the (D-1)-DDHI assumption

Proof of Single-key No-evaluation Security

- We prove that given $K_f := (f, b'_1, \ldots, b'_Z, g, g^{\alpha}, g^{\alpha^2}, \ldots, g^{\alpha^{D-1}})$, **if $f(x) = 1$**, then ***PRF(K, x) is pseudorandom***.
- Recall that we have $U((b_1, \ldots, b_z), x) = f(x) + \sum_{i \in [D]} c_i \alpha^i$
- If $f(x) = 1$, we have

$$PRF(K, x) = g^{\sum_{i \in [D]} c_i \alpha^{i-1}} \cdot g^{\frac{1}{\alpha}}$$

Computable from K

Pseudorandom under the (D-1)-DDHI assumption

$PRF(K, x)$ *is pseudorandom*

Roadmap

Selectively secure single-key CPRF for NC^1
against adversaries that make **no evaluation queries**

Correlated-input secure hash

Selectively secure single-key CPRF for NC^1
against adversaries that make **unbounded evaluation queries**

Why Only No-Evaluation Security?

- If the evaluation oracle is given, then **there exists an attack**.
- Suppose that an adversary is given K_f and $PRF(K,x)$ for x s.t. $f(x)=1$.

$$PRF(K,x) = g^{\sum_{i\in[D]} c_i \alpha^{i-1}} \cdot g^{\frac{1}{\alpha}}$$

- For $x' \neq x$ s.t. $f(x')=1$, we have

$$PRF(K,x') = g^{\sum_{i\in[D]} c'_i \alpha^{i-1}} \cdot g^{\frac{1}{\alpha}}$$
$$= PRF(K,x) \cdot \left(g^{\sum_{i\in[D]} c_i \alpha^{i-1}}\right)^{-1} \cdot g^{\sum_{i\in[D]} c'_i \alpha^{i-1}}$$

Computable from k

⇒ **$PRF(K,x')$ is predictable**

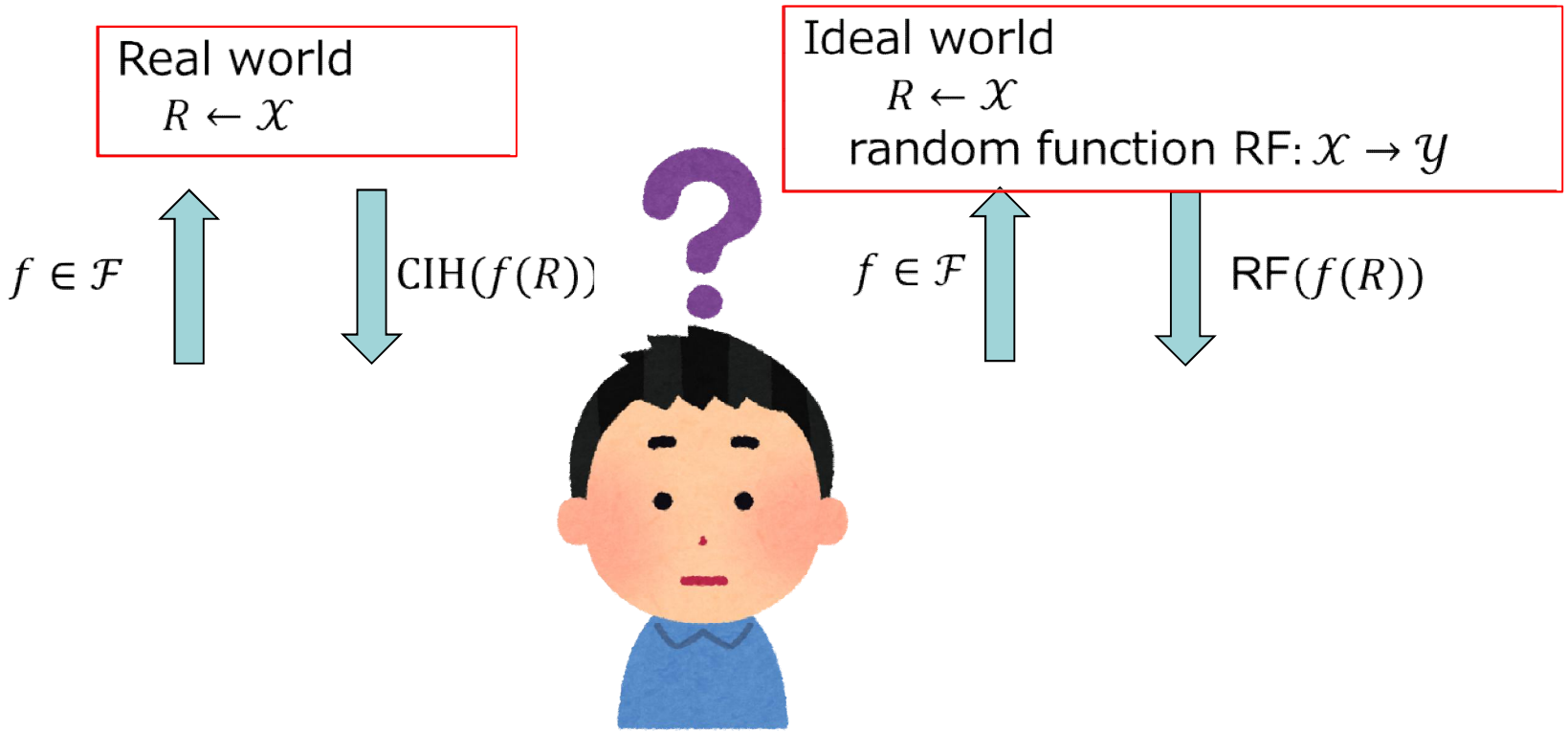
Toward Protecting the Attack

- The problem was that $PRF(K, x)$ and $PRF(K, x')$ have an **algebraic correlation.**
  - $PRF(K, x') = PRF(K, x) \cdot$ (Known Term)
- We want to break the correlation.

- Use **correlated-input secure hash function**!

Correlated-Input Secure Hash Function (CIH) [GOR11]

- A hash function $\mathrm{CIH}: \mathcal{X} \to \mathcal{R}$ is a correlated-input hash function (CIH) for a function class $\mathcal{F}$ if the following two oracles are indistinguishable:

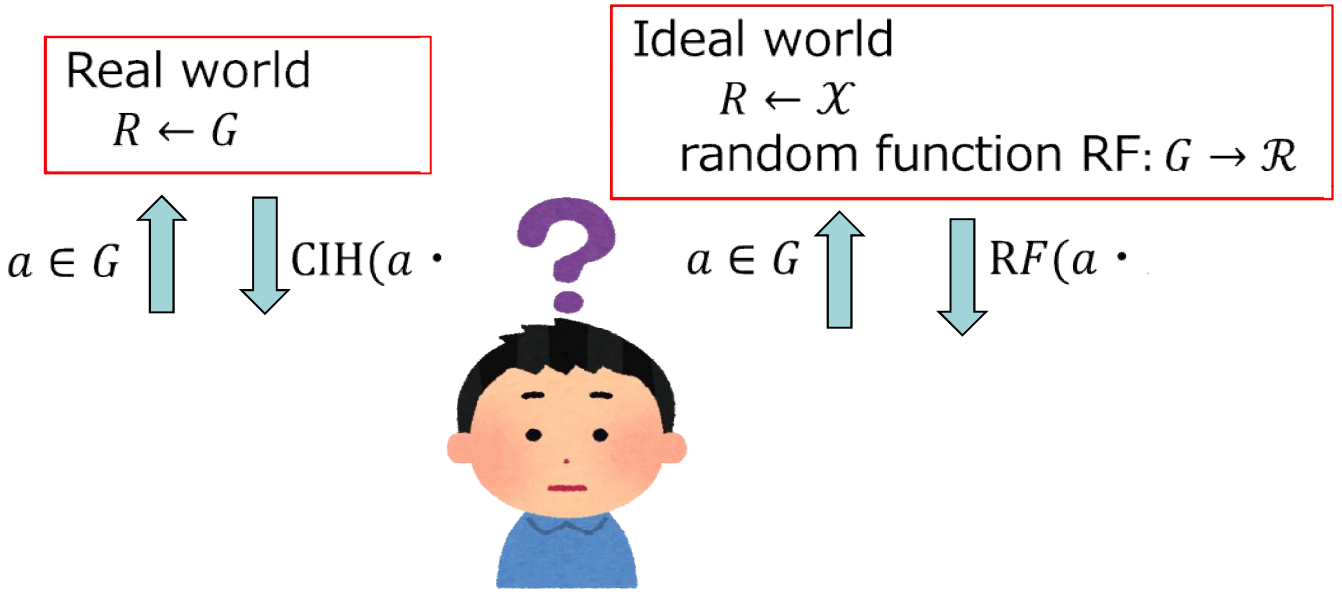


Group-compatible CIH

- We want to break algebraic correlations between group elements.

➡ We need a CIH for **group-compatible function class**.

- $\mathrm{CIH}: G \to \mathcal{R}$ is **G-compatible** CIH if it is a CIH for the class of all **non-zero constant multiplication functions** on G.



From No-Evaluation to Unbounded-Evaluation Security

- Let PRF_{NE} be our no-evaluation secure CPRF, and CIH be a G-compatible CIH.
- We define $PRF(K, x) \coloneqq CIH(PRF_{NE}(K, x))$.
- Constrained key of PRF is the same as that of PRF_{NE}.
- PRF is selectively single-key secure against adversaries that make **unbounded number of evaluation queries**.

Proof Sketch

- If $f(x) = 1$

$$PRF(K, x) = CIH(g^{\sum_{i \in [D]} c_i \alpha^{i-1}} \cdot g^{\frac{1}{\alpha}})$$

Proof Sketch

- If $f(x) = 1$

$$PRF(K, x) = CIH(g^{\sum_{i\in[D]} c_i \alpha^{i-1}} \cdot g^{\frac{1}{\alpha}})$$

D-DDHI assumption

$$PRF(K, x) = CIH(g^{\sum_{i\in[D]} c_i \alpha^{i-1}} \cdot R)$$

Proof Sketch

- If $f(x) = 1$

$$PRF(K, x) = CIH(g^{\sum_{i\in[D]} c_i \alpha^{i-1}} \cdot g^{\frac{1}{\alpha}})$$

D-DDHI assumption

$$PRF(K, x) = CIH(g^{\sum_{i\in[D]} c_i \alpha^{i-1}} \cdot R)$$

Security of CIH

$$PRF(K, x) = RF(g^{\sum_{i\in[D]} c_i \alpha^{i-1}} \cdot R)$$

Proof Sketch

- If $f(x) = 1$

$$PRF(K, x) = CIH(g^{\sum_{i\in[D]} c_i \alpha^{i-1}} \cdot g^{\frac{1}{\alpha}})$$

D-DDHI assumption

$$PRF(K, x) = CIH(g^{\sum_{i\in[D]} c_i \alpha^{i-1}} \cdot R)$$

Security of CIH

$$PRF(K, x) = RF(g^{\sum_{i\in[D]} c_i \alpha^{i-1}} \cdot R)$$

$RF(g^{\sum_{i\in[D]} c_i \alpha^{i-1}} \cdot R)$ is independent independently random for each x.
Now, evaluation queries are meaningless.
→**The security is reduced to the no-evaluation security of PRF_{NE}.**

Instantiations?

- We obtain selectively single-key secure CPRF for NC^1 assuming
  - **D-DDHI assumption** holds on G
  - There exists a **G-compatible CIH**
- What group G to use?
  - Unfortunately, there is **no known instantiation**!
- We further modify the construction.

Toward Actual Instantiation

- The only known construction of a group-compatible CIH is the one proposed by Bellare and Cash [BC10].
- Their CIH supports **component-wise multiplications over $(\mathbb{Z}_q^*)^m$** under the DDH assumption on another group G'.
- First attempt: Set **$G := \mathbb{Z}_q^*$** and define
  $PRF(K, x) := CIH(PRF_{NE}(K_1, x), \ldots, PRF_{NE}(K_m, x))$
- If (D-1)-DDHI assumption holds on $\mathbb{Z}_q^*$, then this construction works.
- However, **the (D-1)-DDHI assumption does not hold on $\mathbb{Z}_q^*$!**
  - Broken by computing Jacobi Symbol
- We set **$G := \mathbb{QR}_q$**, which is a quadratic residue subgroup of $\mathbb{Z}_q^*$
  - The attack by Jacobi Symbol does not work on $\mathbb{QR}_q$.

Our Actual Construction

- Our actual construction is described below.

  $PRF(K, x) := CIH\left(PRF_{NE}(K_1, x), \ldots, PRF_{NE}(K_m, x)\right)$

  where PRF_{NE} is instantiated on $G := \mathbb{QR}_q$, and CIH is Bellare-Cash CIH instantiated on G'.
- The above scheme is selectively single-key secure if
  1. The **(D-1)-DDHI assumption** holds on $\mathbb{QR}_q$.
  2. The **DDH assumption** holds on G'

Comparison among CPRFs

	Function class	Keys	Eval	Assumption
[BW13],[KPTZ13] [BGI14]	Puncturing	1	N/A	OWF
[BW13]	left/right	poly	poly	DBDH(RO)
[BW13]	P/poly	poly	poly	MDDH
[BZ14]	P/poly	poly	poly	iO
[BV15]	P/poly	1	poly	LWE+1D-SIS
[Bit17]	sub-match	1	0	DDH
[GHKW17]	sub-match	1	0	L-PDDH
[GHKW17]	sub-match	1	0	Φ-hiding
Ours		1	poly	DDH+L-DDHI

Comparison among Private CPRFs

	Function class	Keys	Eval	Assumption
[BLW17]	Puncturing	1	N/A	MLM
[BLW17]	Bit-fixing	poly	poly	MLM
[BLW17]	P/poly	poly	poly	iO
[BKM17]	Puncturing	1	N/A	LWE+1D-SIS
[CC17]		1	poly	LWE
[BTVW17]	P/poly	1	poly	LWE
[Ours]	Bit-fixing	1	poly	DDH

Summary

- We gave new constructions of CPRFs on pairing-free groups
  - Single-key CPRF for NC^1 from DDH and L-DDHI on $\mathbb{QR}_q$
  - Single-key private CPRF for bit-fixing from DDH
- Open problems
  - Collusion resistant and/or adaptive construction.
  - Instantiate our first construction based on general groups (instead of on a specific group $\mathbb{QR}_q$).
  - (Private) CPRF for wider function class on pairing-free groups.