Minicrypt Primitives with Algebraic Structure

Sikhar Patranabis (Applied Crypto Group, ETH Zürich)

Based on joint work(s) with:

Navid Alamati (University of Michigan)

Luca De Feo (IBM Zürich)

Hart Montgomery, Arnab Roy (Fujitsu Labs of America)

Disclaimers:

Disclaimers:

- This talk is *not* on practice-oriented cryptography

Disclaimers:

- This talk is *not* on practice-oriented cryptography
- This talk presents an *alternative* perspective to cryptography – through the lens of computational complexity theory

Disclaimers:

- This talk is *not* on practice-oriented cryptography
- This talk presents an *alternative* perspective to cryptography – through the lens of computational complexity theory
- This talk is *not* meant to intimidate

Disclaimers:

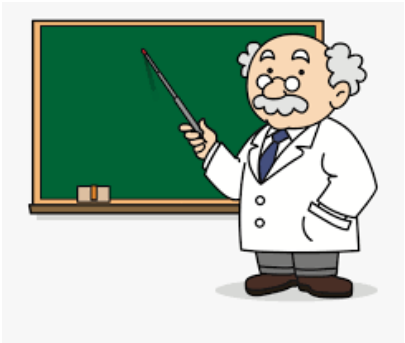
- This talk is *not* on practice-oriented cryptography
- This talk presents an *alternative* perspective to cryptography – through the lens of computational complexity theory
- This talk is *not* meant to intimidate

This is a Sunday afternoon and many of you are tired after a long week

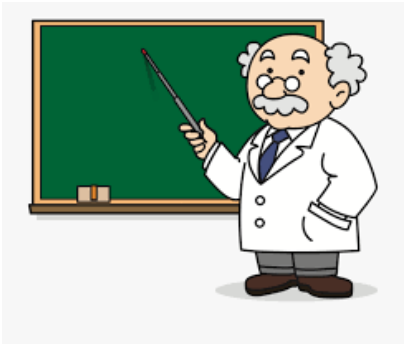
But if you are still here, thank you and let's have some fun….

A Tale of Five Worlds [Impagliazzo’95]

A Tale of Five Worlds [Impagliazzo’95]

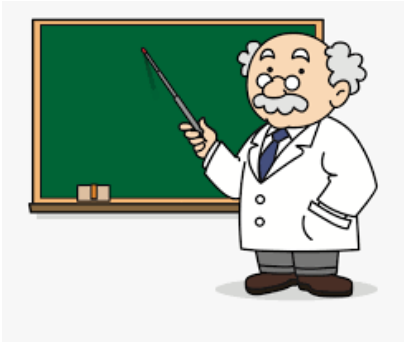


A Tale of Five Worlds [Impagliazzo'95]



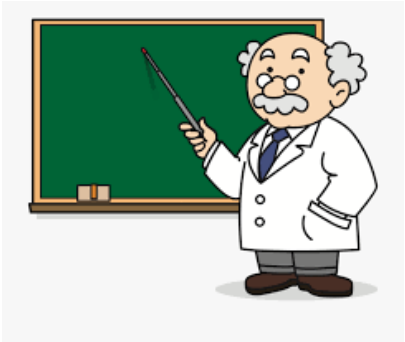
- *Algorithmica:* $\mathrm{P} = \mathrm{NP}$ (or something "morally equivalent " such as $\mathrm{NP} \subseteq \mathrm{BPP}$)

A Tale of Five Worlds [Impagliazzo'95]



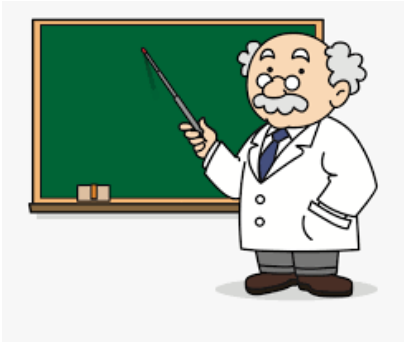
- *Algorithmica:* $\mathrm{P} = \mathrm{NP}$ (or something "morally equivalent " such as $\mathrm{NP} \subseteq \mathrm{BPP}$)
- *Heuristica:* NP problems are hard in the worst case but easy on average.

A Tale of Five Worlds [Impagliazzo'95]



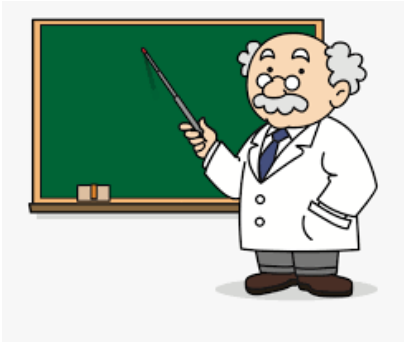
- *Algorithmica:* $\mathrm{P} = \mathrm{NP}$ (or something "morally equivalent " such as $\mathrm{NP} \subseteq \mathrm{BPP}$)
- *Heuristica:* NP problems are hard in the worst case but easy on average.
- *Pessiland:* NP problems are hard on average but no one-way functions

A Tale of Five Worlds [Impagliazzo'95]



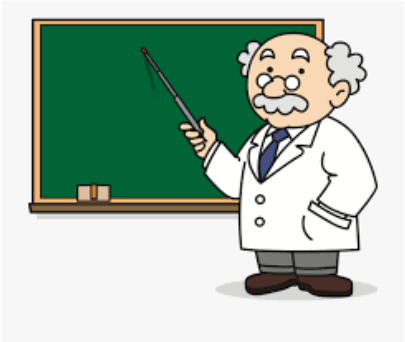
- *Algorithmica:* $\mathrm{P} = \mathrm{NP}$ (or something "morally equivalent " such as $\mathrm{NP} \subseteq \mathrm{BPP}$)
- *Heuristica:* NP problems are hard in the worst case but easy on average.
- *Pessiland:* NP problems are hard on average but no one-way functions
- *Minicrypt:* One-way functions exist but no public-key cryptography

A Tale of Five Worlds [Impagliazzo'95]



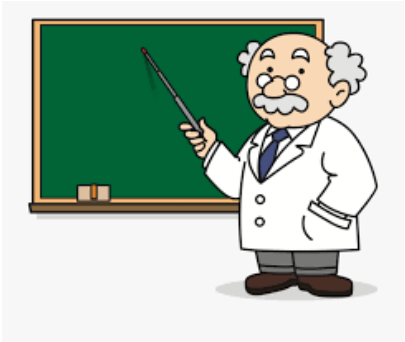
- *Algorithmica:* $\mathrm{P} = \mathrm{NP}$ (or something "morally equivalent " such as $\mathrm{NP} \subseteq \mathrm{BPP}$)
- *Heuristica:* NP problems are hard in the worst case but easy on average.
- *Pessiland:* NP problems are hard on average but no one-way functions
- *Minicrypt:* One-way functions exist but no public-key cryptography
- *Cryptomania:* Public-key cryptography is possible

A Tale of Five Worlds [Impagliazzo'95]



- *Algorithmica:* $\mathrm{P} = \mathrm{NP}$ (or something "morally equivalent " such as $\mathrm{NP} \subseteq \mathrm{BPP}$)
- *Heuristica:* NP problems are hard in the worst case but easy on average.
- *Pessiland:* NP problems are hard on average but no one-way functions
- *Minicrypt:* One-way functions exist but no public-key cryptography
- *Cryptomania:* Public-key cryptography is possible

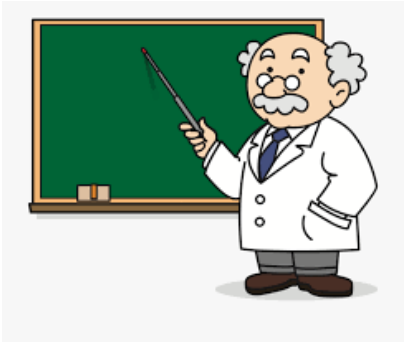
A Tale of Five Worlds [Impagliazzo'95]



Minicrypt + ? = Cryptomania

- *Minicrypt:* One-way functions exist but no public-key cryptography
- *Cryptomania:* Public-key cryptography is possible

A Tale of Five Worlds [Impagliazzo'95]



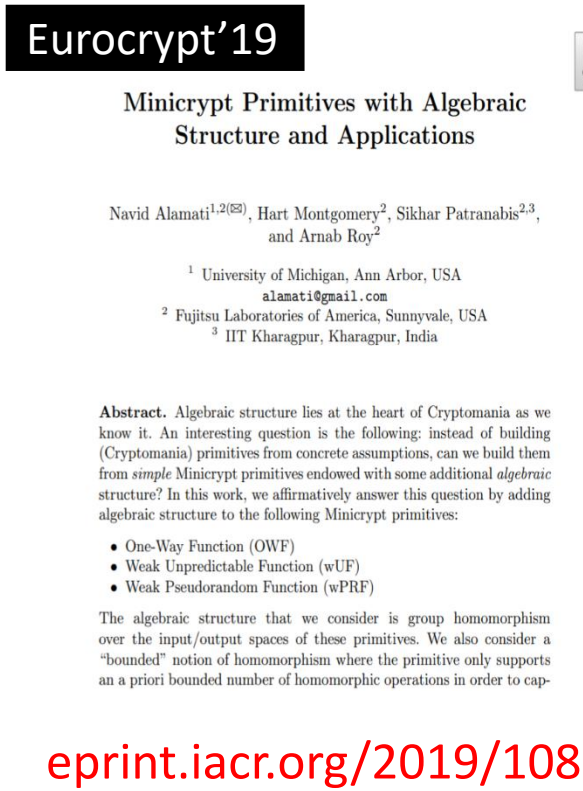
This Talk

Minicrypt + Algebraic Structure = Cryptomania

- *Minicrypt:* One-way functions exist but no public-key cryptography
- *Cryptomania:* Public-key cryptography is possible

Baby Steps….

Eurocrypt'19



Minicrypt Primitives with Algebraic Structure and Applications

Navid Alamati[1,2(✉)], Hart Montgomery[2], Sikhar Patranabis[2,3], and Arnab Roy[2]

[1] University of Michigan, Ann Arbor, USA
alamati@gmail.com
[2] Fujitsu Laboratories of America, Sunnyvale, USA
[3] IIT Kharagpur, Kharagpur, India

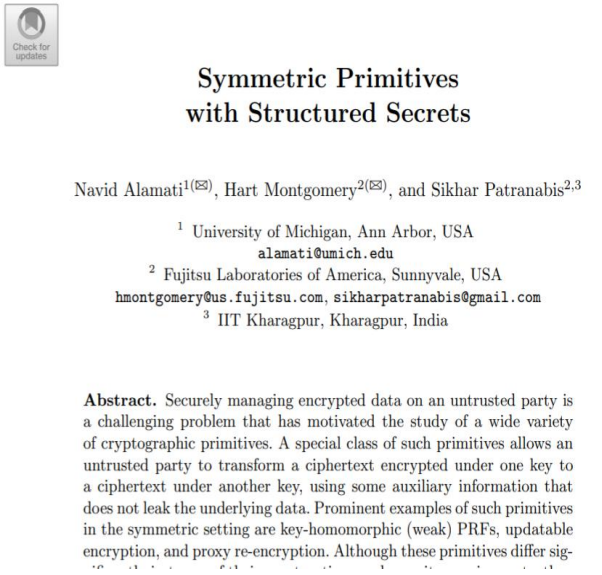
Abstract. Algebraic structure lies at the heart of Cryptomania as we know it. An interesting question is the following: instead of building (Cryptomania) primitives from concrete assumptions, can we build them from *simple* Minicrypt primitives endowed with some additional *algebraic* structure? In this work, we affirmatively answer this question by adding algebraic structure to the following Minicrypt primitives:

- One-Way Function (OWF)
- Weak Unpredictable Function (wUF)
- Weak Pseudorandom Function (wPRF)

The algebraic structure that we consider is group homomorphism over the input/output spaces of these primitives. We also consider a "bounded" notion of homomorphism where the primitive only supports an a priori bounded number of homomorphic operations in order to cap-

eprint.iacr.org/2019/108

Crypto'19



Symmetric Primitives with Structured Secrets

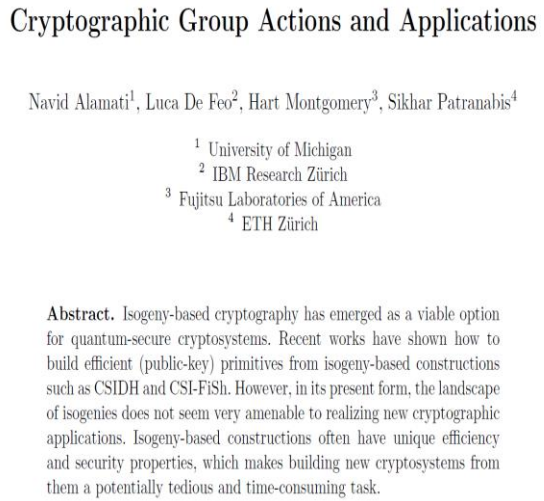
Navid Alamati[1(✉)], Hart Montgomery[2(✉)], and Sikhar Patranabis[2,3]

[1] University of Michigan, Ann Arbor, USA
alamati@umich.edu
[2] Fujitsu Laboratories of America, Sunnyvale, USA
hmontgomery@us.fujitsu.com, sikharpatranabis@gmail.com
[3] IIT Kharagpur, Kharagpur, India

Abstract. Securely managing encrypted data on an untrusted party is a challenging problem that has motivated the study of a wide variety of cryptographic primitives. A special class of such primitives allows an untrusted party to transform a ciphertext encrypted under one key to a ciphertext under another key, using some auxiliary information that does not leak the underlying data. Prominent examples of such primitives in the symmetric setting are key-homomorphic (weak) PRFs, updatable encryption, and proxy re-encryption. Although these primitives differ sig-

eprint.iacr.org/2019/608

Asiacrypt'20 (Conditionally accepted)



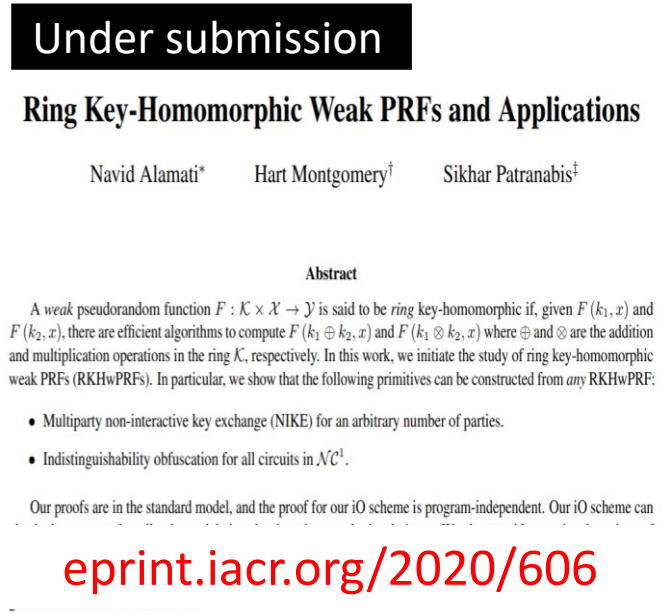
Cryptographic Group Actions and Applications

Navid Alamati[1], Luca De Feo[2], Hart Montgomery[3], Sikhar Patranabis[4]

[1] University of Michigan
[2] IBM Research Zürich
[3] Fujitsu Laboratories of America
[4] ETH Zürich

Abstract. Isogeny-based cryptography has emerged as a viable option for quantum-secure cryptosystems. Recent works have shown how to build efficient (public-key) primitives from isogeny-based constructions such as CSIDH and CSI-FiSh. However, in its present form, the landscape of isogenies does not seem very amenable to realizing new cryptographic applications. Isogeny-based constructions often have unique efficiency and security properties, which makes building new cryptosystems from them a potentially tedious and time-consuming task.

Under submission



Ring Key-Homomorphic Weak PRFs and Applications

Navid Alamati* Hart Montgomery† Sikhar Patranabis‡

Abstract

A *weak* pseudorandom function $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ is said to be *ring* key-homomorphic if, given $F(k_1, x)$ and $F(k_2, x)$, there are efficient algorithms to compute $F(k_1 \oplus k_2, x)$ and $F(k_1 \otimes k_2, x)$ where $\oplus$ and $\otimes$ are the addition and multiplication operations in the ring $\mathcal{K}$, respectively. In this work, we initiate the study of ring key-homomorphic weak PRFs (RKHwPRFs). In particular, we show that the following primitives can be constructed from *any* RKHwPRF:

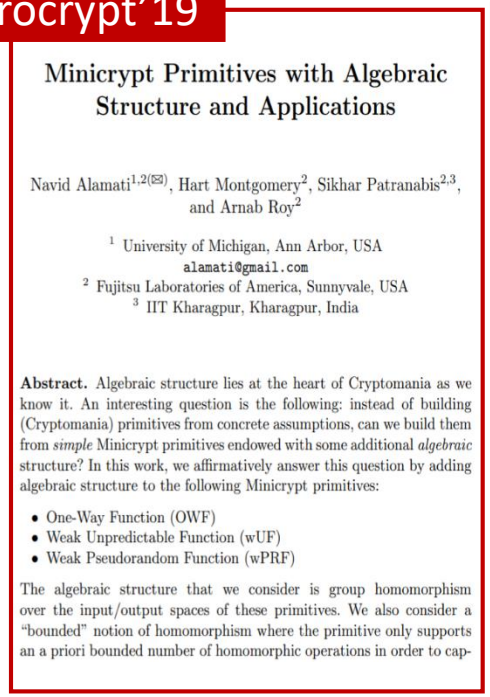
- Multiparty non-interactive key exchange (NIKE) for an arbitrary number of parties.
- Indistinguishability obfuscation for all circuits in $\mathcal{NC}^1$.

Our proofs are in the standard model, and the proof for our iO scheme is program-independent. Our iO scheme can

eprint.iacr.org/2020/606

Baby Steps….

Eurocrypt'19



Minicrypt Primitives with Algebraic Structure and Applications

Navid Alamati[1,2(✉)], Hart Montgomery[2], Sikhar Patranabis[2,3], and Arnab Roy[2]

[1] University of Michigan, Ann Arbor, USA
alamati@gmail.com
[2] Fujitsu Laboratories of America, Sunnyvale, USA
[3] IIT Kharagpur, Kharagpur, India

Abstract. Algebraic structure lies at the heart of Cryptomania as we know it. An interesting question is the following: instead of building (Cryptomania) primitives from concrete assumptions, can we build them from *simple* Minicrypt primitives endowed with some additional *algebraic* structure? In this work, we affirmatively answer this question by adding algebraic structure to the following Minicrypt primitives:

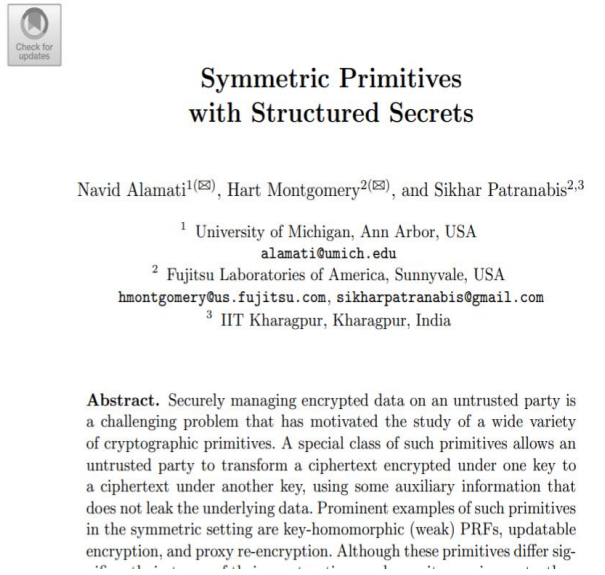
- One-Way Function (OWF)
- Weak Unpredictable Function (wUF)
- Weak Pseudorandom Function (wPRF)

The algebraic structure that we consider is group homomorphism over the input/output spaces of these primitives. We also consider a "bounded" notion of homomorphism where the primitive only supports an a priori bounded number of homomorphic operations in order to cap-

eprint.iacr.org/2019/108

This Talk

Crypto'19



Symmetric Primitives with Structured Secrets

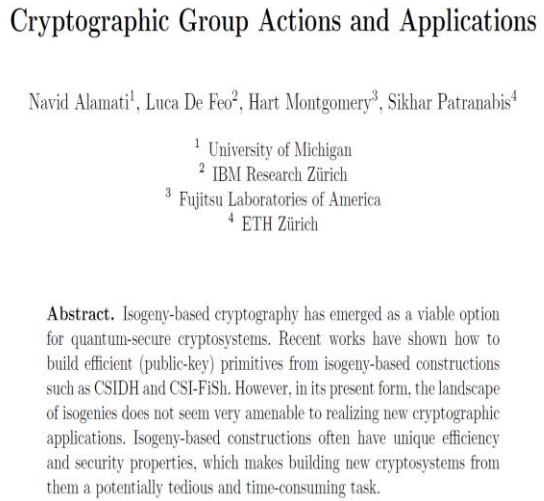
Navid Alamati[1(✉)], Hart Montgomery[2(✉)], and Sikhar Patranabis[2,3]

[1] University of Michigan, Ann Arbor, USA
alamati@umich.edu
[2] Fujitsu Laboratories of America, Sunnyvale, USA
hmontgomery@us.fujitsu.com, sikharpatranabis@gmail.com
[3] IIT Kharagpur, Kharagpur, India

Abstract. Securely managing encrypted data on an untrusted party is a challenging problem that has motivated the study of a wide variety of cryptographic primitives. A special class of such primitives allows an untrusted party to transform a ciphertext encrypted under one key to a ciphertext under another key, using some auxiliary information that does not leak the underlying data. Prominent examples of such primitives in the symmetric setting are key-homomorphic (weak) PRFs, updatable encryption, and proxy re-encryption. Although these primitives differ sig-

eprint.iacr.org/2019/608

Asiacrypt'20 (Conditionally accepted)



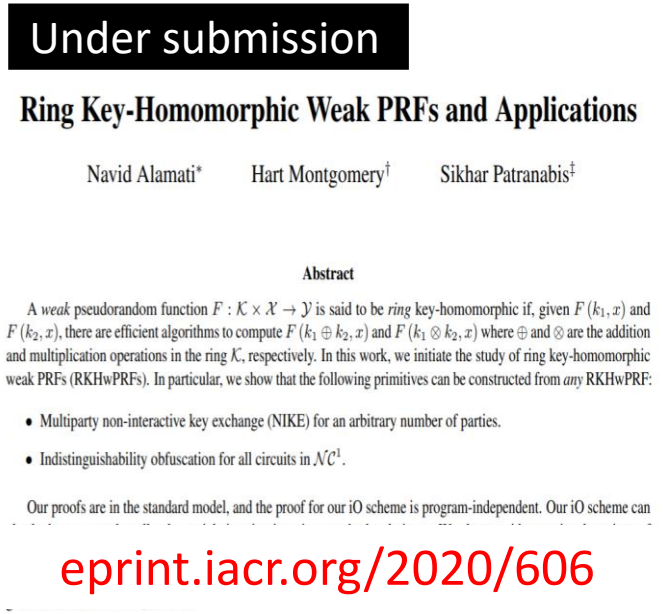
Cryptographic Group Actions and Applications

Navid Alamati[1], Luca De Feo[2], Hart Montgomery[3], Sikhar Patranabis[4]

[1] University of Michigan
[2] IBM Research Zürich
[3] Fujitsu Laboratories of America
[4] ETH Zürich

Abstract. Isogeny-based cryptography has emerged as a viable option for quantum-secure cryptosystems. Recent works have shown how to build efficient (public-key) primitives from isogeny-based constructions such as CSIDH and CSI-FiSh. However, in its present form, the landscape of isogenies does not seem very amenable to realizing new cryptographic applications. Isogeny-based constructions often have unique efficiency and security properties, which makes building new cryptosystems from them a potentially tedious and time-consuming task.

Under submission



Ring Key-Homomorphic Weak PRFs and Applications

Navid Alamati* Hart Montgomery† Sikhar Patranabis‡

Abstract

A *weak* pseudorandom function $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ is said to be *ring* key-homomorphic if, given $F(k_1, x)$ and $F(k_2, x)$, there are efficient algorithms to compute $F(k_1 \oplus k_2, x)$ and $F(k_1 \otimes k_2, x)$ where $\oplus$ and $\otimes$ are the addition and multiplication operations in the ring $\mathcal{K}$, respectively. In this work, we initiate the study of ring key-homomorphic weak PRFs (RKHwPRFs). In particular, we show that the following primitives can be constructed from *any* RKHwPRF:

- Multiparty non-interactive key exchange (NIKE) for an arbitrary number of parties.
- Indistinguishability obfuscation for all circuits in $\mathcal{NC}^1$.

Our proofs are in the standard model, and the proof for our iO scheme is program-independent. Our iO scheme can

eprint.iacr.org/2020/606

Building Blocks

- Minicrypt primitives
  - One-Way Functions (OWFs)
  - Weak Unpredictable Functions (wUFs)
  - Weak Pseudorandom Functions (wPRFs)

Building Blocks – This Talk

- Minicrypt primitives + Algebraic structure
  - One-Way Functions (OWFs)
  - Weak Unpredictable Functions (wUFs)
  - Weak Pseudorandom Functions (wPRFs)

Building Blocks – This Talk

Homomorphism between the input and output spaces

- Minicrypt primitives + Algebraic structure
  - One-Way Functions (OWFs)
  - Weak Unpredictable Functions (wUFs)
  - Weak Pseudorandom Functions (wPRFs)

Building Blocks – This Talk

Homomorphism between the input and output spaces

- Minicrypt primitives + Algebraic structure
  - Homomorphic One-Way Functions (HOWFs)
  - Input-Homomorphic Weak Unpredictable Functions (IHwUFs)
  - Input-Homomorphic Weak Pseudorandom Functions (IHwPRFs)

Definitions

Homomorphic One-Way Function

A one-way function $f : \mathcal{X} \to \mathcal{Y}$ such that:

- $(\mathcal{X}, \bigoplus)$ and $(\mathcal{Y}, \bigotimes)$ are efficiently samplable groups
- for all $x_1, x_2 \in \mathcal{X}$

$$f\,(x_1 \oplus x_2) = f(x_1) \otimes f(x_2)$$

Definitions

Input-Homomorphic weak Unpredictable Function

A weak unpredictable function $F : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{Y}$ such that:

- $(\mathcal{X}, \bigoplus)$ and $(\mathcal{Y}, \bigotimes)$ are efficiently samplable groups
- for all $k \in \mathcal{K}$ and for all $x_1, x_2 \in \mathcal{X}$

$$F\,(k, x_1 \bigoplus x_2) = F(k, x_1) \bigotimes F(k, x_2)$$

Definitions

Input-Homomorphic weak PRF

A weak PRF $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ such that:

- $(\mathcal{X}, \bigoplus)$ and $(\mathcal{Y}, \bigotimes)$ are efficiently samplable groups
- for all $k \in \mathcal{K}$ and for all $x_1, x_2 \in \mathcal{X}$

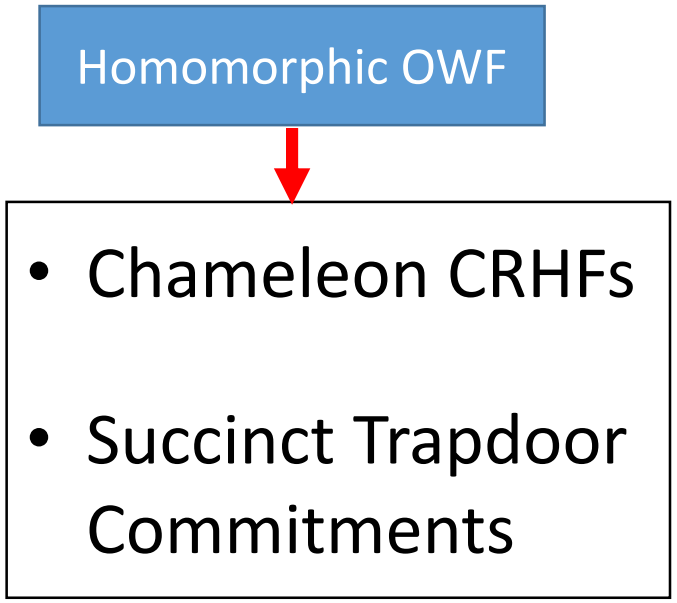
$$F\,(k, x_1 \bigoplus x_2) = F(k, x_1) \bigotimes F(k, x_2)$$

“Bounded” Homomorphism

- Minicrypt primitives + Algebraic Structure
  - (Bounded) Homomorphic One-Way Functions
  - (Bounded) Input-Homomorphic Weak Unpredictable Functions
  - (Bounded) Input-Homomorphic Weak Pseudorandom Functions

Outline

- **Our results**
- An alternative approach to designing primitives
- A cryptoplexity hierarchy in Cryptomania
- Technical overview
- Summary and open questions

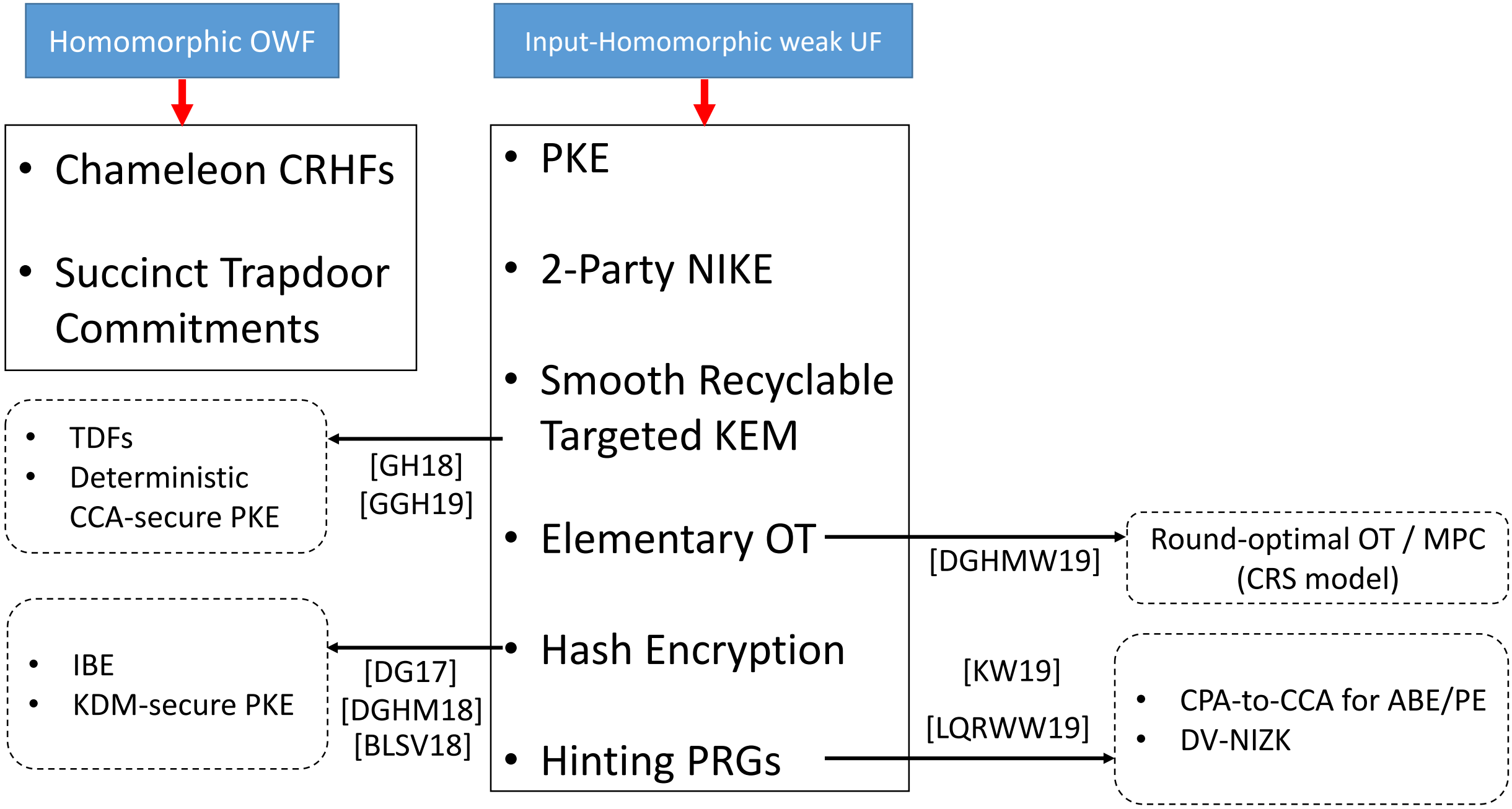

Homomorphic OWF
• Chameleon CRHFs
• Succinct Trapdoor Commitments

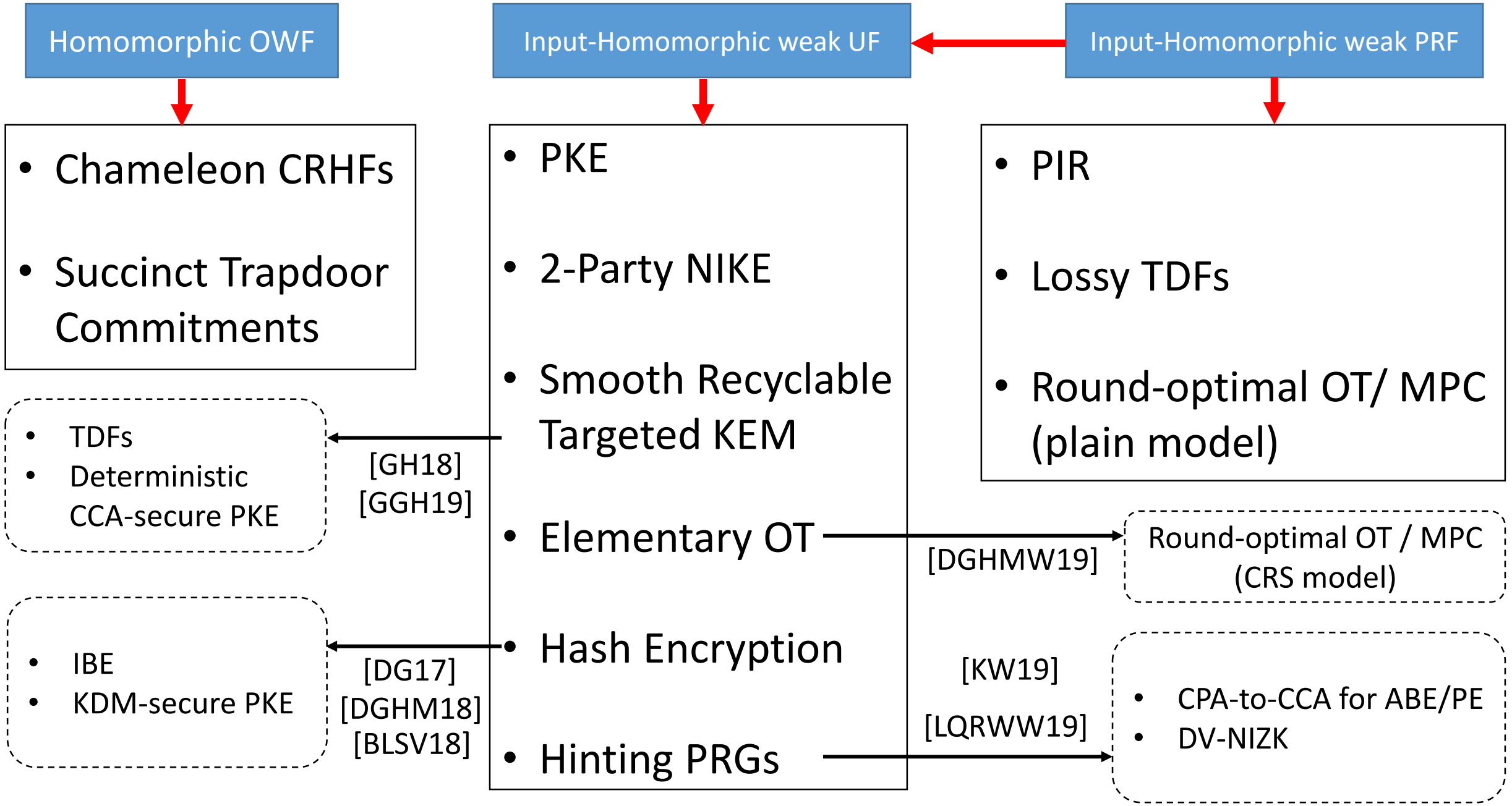
Homomorphic OWF

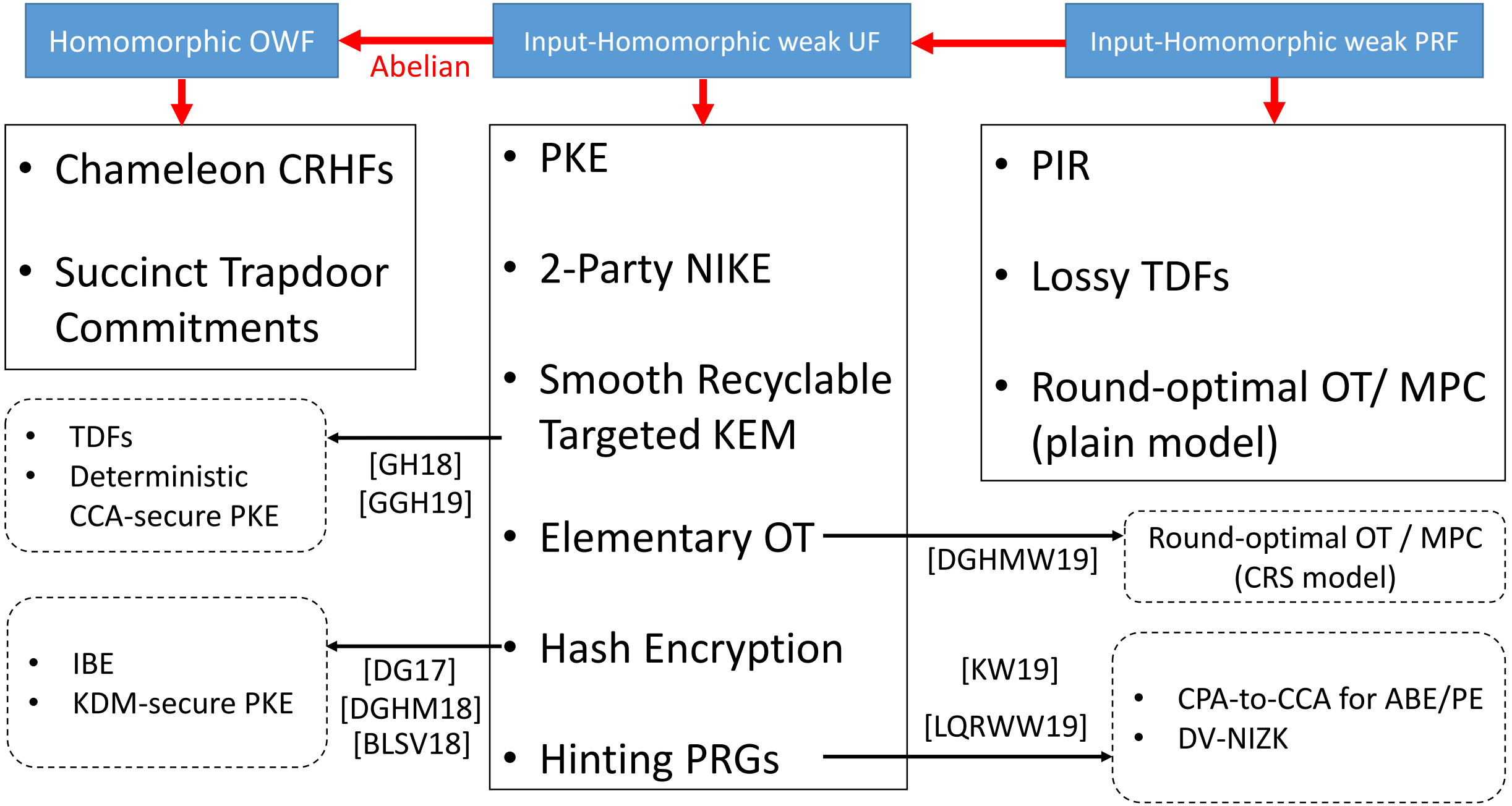
- Chameleon CRHFs
- Succinct Trapdoor Commitments

Input-Homomorphic weak UF

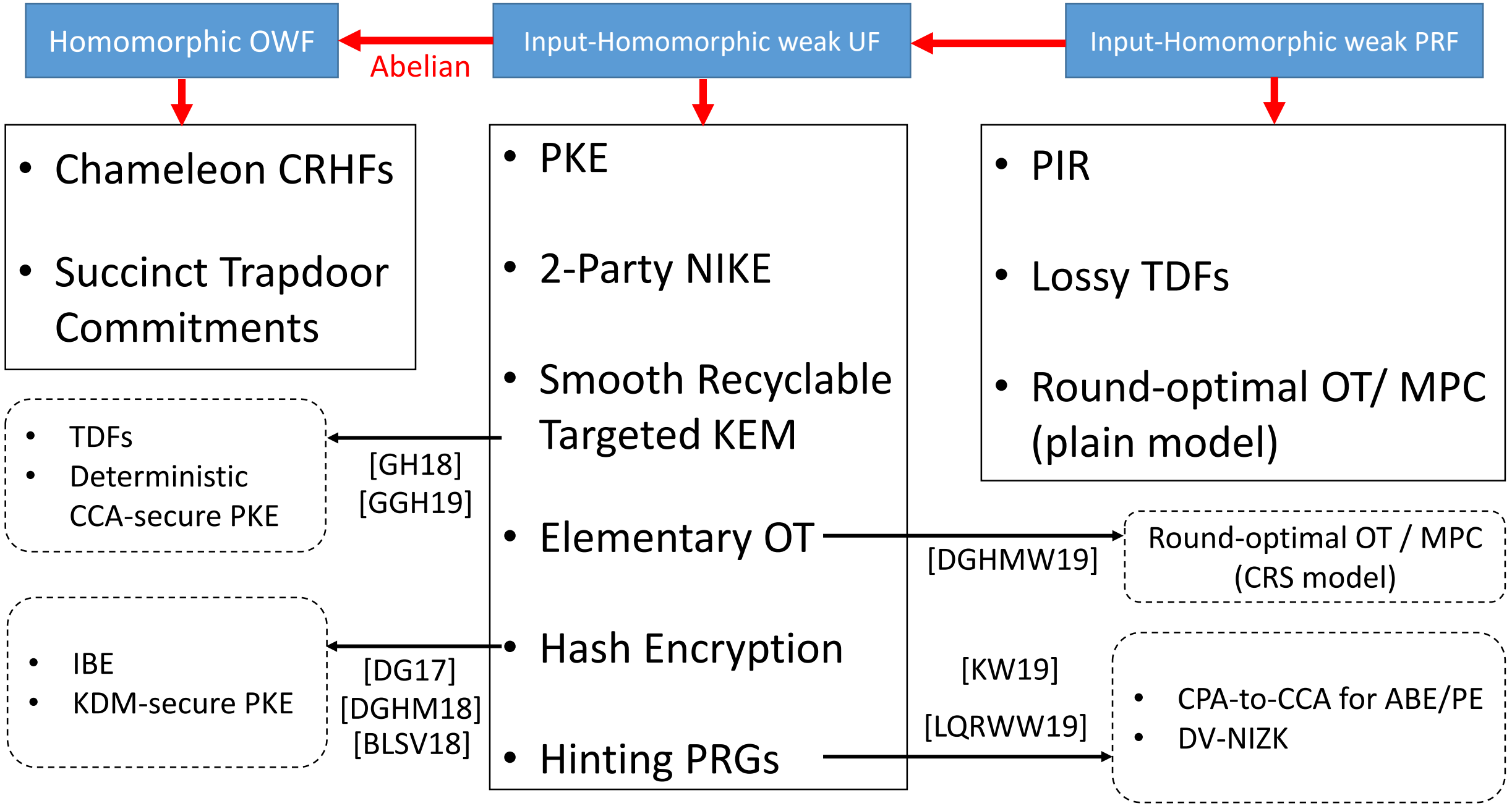
- PKE
- 2-Party NIKE
- Smooth Recyclable Targeted KEM
- Elementary OT
- Hash Encryption
- Hinting PRGs


Homomorphic OWF
Input-Homomorphic weak UF
• Chameleon CRHFs
• Succinct Trapdoor Commitments
• PKE
• 2-Party NIKE
• Smooth Recyclable Targeted KEM
• Elementary OT
• Hash Encryption
• Hinting PRGs
• TDFs
• Deterministic CCA-secure PKE
[GH18]
[GGH19]
• IBE
• KDM-secure PKE
[DG17]
[DGHM18]
[BLSV18]
[DGHMW19]
Round-optimal OT / MPC (CRS model)
[KW19]
[LQRWW19]
• CPA-to-CCA for ABE/PE
• DV-NIZK


Homomorphic OWF
Input-Homomorphic weak UF
Input-Homomorphic weak PRF
• Chameleon CRHFs
• Succinct Trapdoor Commitments
• PKE
• 2-Party NIKE
• Smooth Recyclable Targeted KEM
• Elementary OT
• Hash Encryption
• Hinting PRGs
• PIR
• Lossy TDFs
• Round-optimal OT/ MPC (plain model)
• TDFs
• Deterministic CCA-secure PKE
[GH18]
[GGH19]
• IBE
• KDM-secure PKE
[DG17]
[DGHM18]
[BLSV18]
[DGHMW19]
Round-optimal OT / MPC (CRS model)
[KW19]
[LQRWW19]
• CPA-to-CCA for ABE/PE
• DV-NIZK


Homomorphic OWF
Abelian
Input-Homomorphic weak UF
Input-Homomorphic weak PRF
• Chameleon CRHFs
• Succinct Trapdoor Commitments
• PKE
• 2-Party NIKE
• Smooth Recyclable Targeted KEM
• Elementary OT
• Hash Encryption
• Hinting PRGs
• PIR
• Lossy TDFs
• Round-optimal OT/ MPC (plain model)
• TDFs
• Deterministic CCA-secure PKE
[GH18]
[GGH19]
• IBE
• KDM-secure PKE
[DG17]
[DGHM18]
[BLSV18]
[DGHMW19]
Round-optimal OT / MPC (CRS model)
[KW19]
[LQRWW19]
• CPA-to-CCA for ABE/PE
• DV-NIZK

All implications hold for bounded homomorphism



Outline

- Our results
- **An alternative approach to designing primitives**
- A cryptoplexity hierarchy in Cryptomania
- Technical overview
- Summary and open questions

Traditional Approach to Cryptography

Assumptions
• Discrete log • Search LWE • Square-root finding
• CDH • RSA
• DDH/MDDH/D-Lin • Decision LWE • QR/DCR • Approx. GCD • Hidden number problem • Finite Field isomorphism

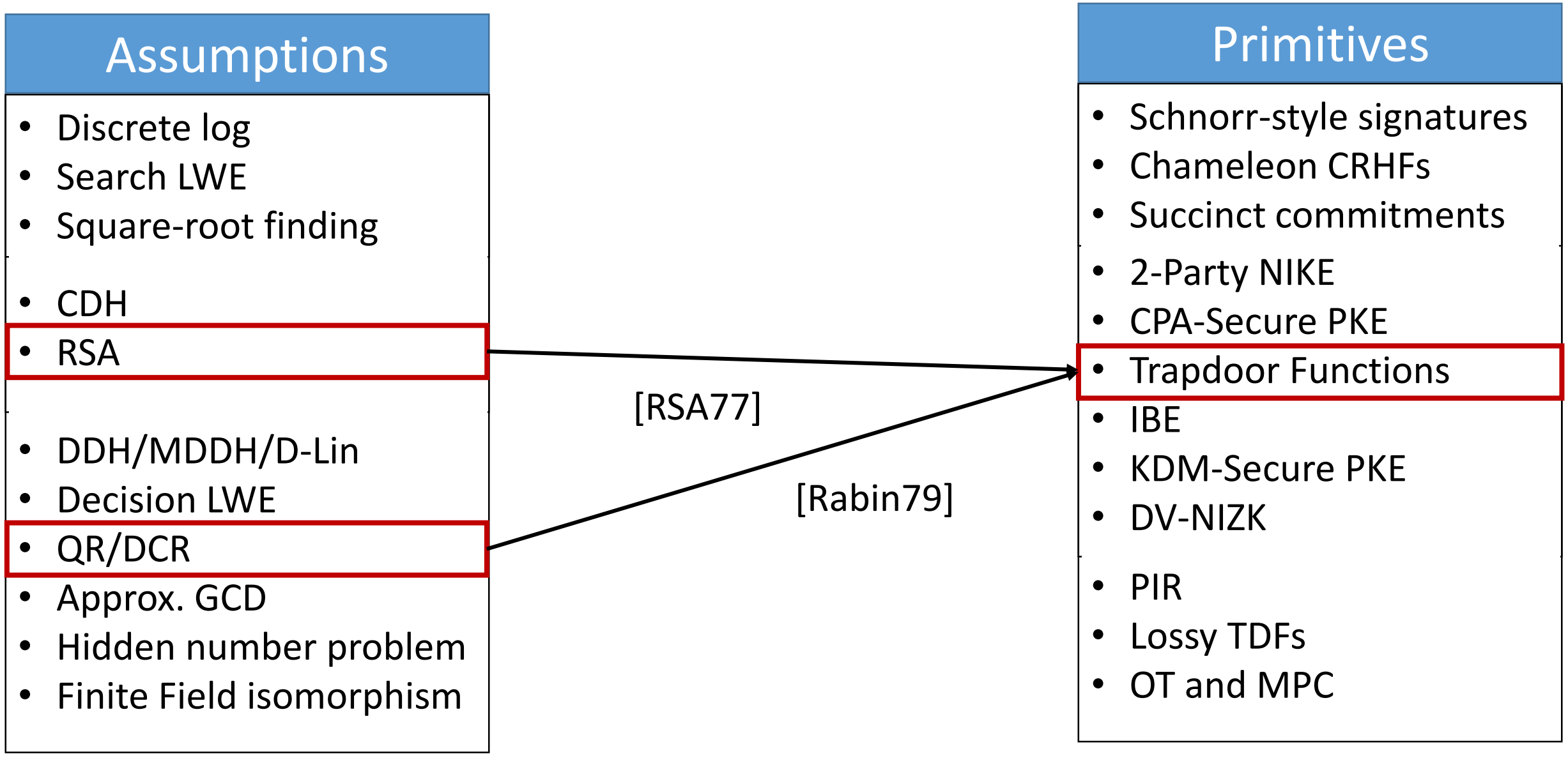
Primitives
• Schnorr-style signatures • Chameleon CRHFs • Succinct commitments
• 2-Party NIKE • CPA-Secure PKE • Trapdoor Functions • IBE • KDM-Secure PKE • DV-NIZK
• PIR • Lossy TDFs • OT and MPC

Traditional Approach to Cryptography

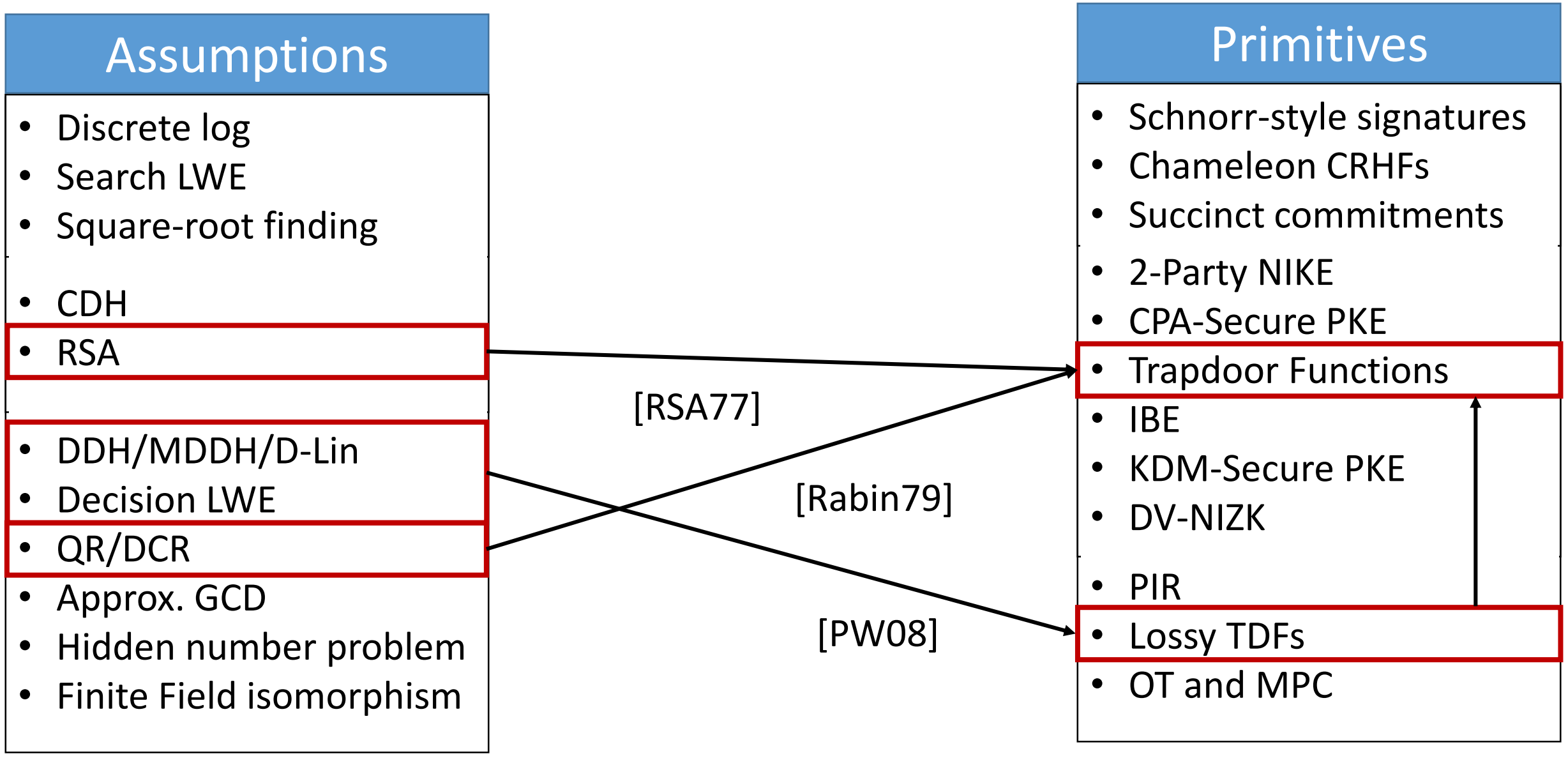
Assumptions
• Discrete log • Search LWE • Square-root finding
• CDH • RSA
• DDH/MDDH/D-Lin • Decision LWE • QR/DCR • Approx. GCD • Hidden number problem • Finite Field isomorphism

Primitives
• Schnorr-style signatures • Chameleon CRHFs • Succinct commitments
• 2-Party NIKE • CPA-Secure PKE
• Trapdoor Functions
• IBE • KDM-Secure PKE • DV-NIZK
• PIR • Lossy TDFs • OT and MPC

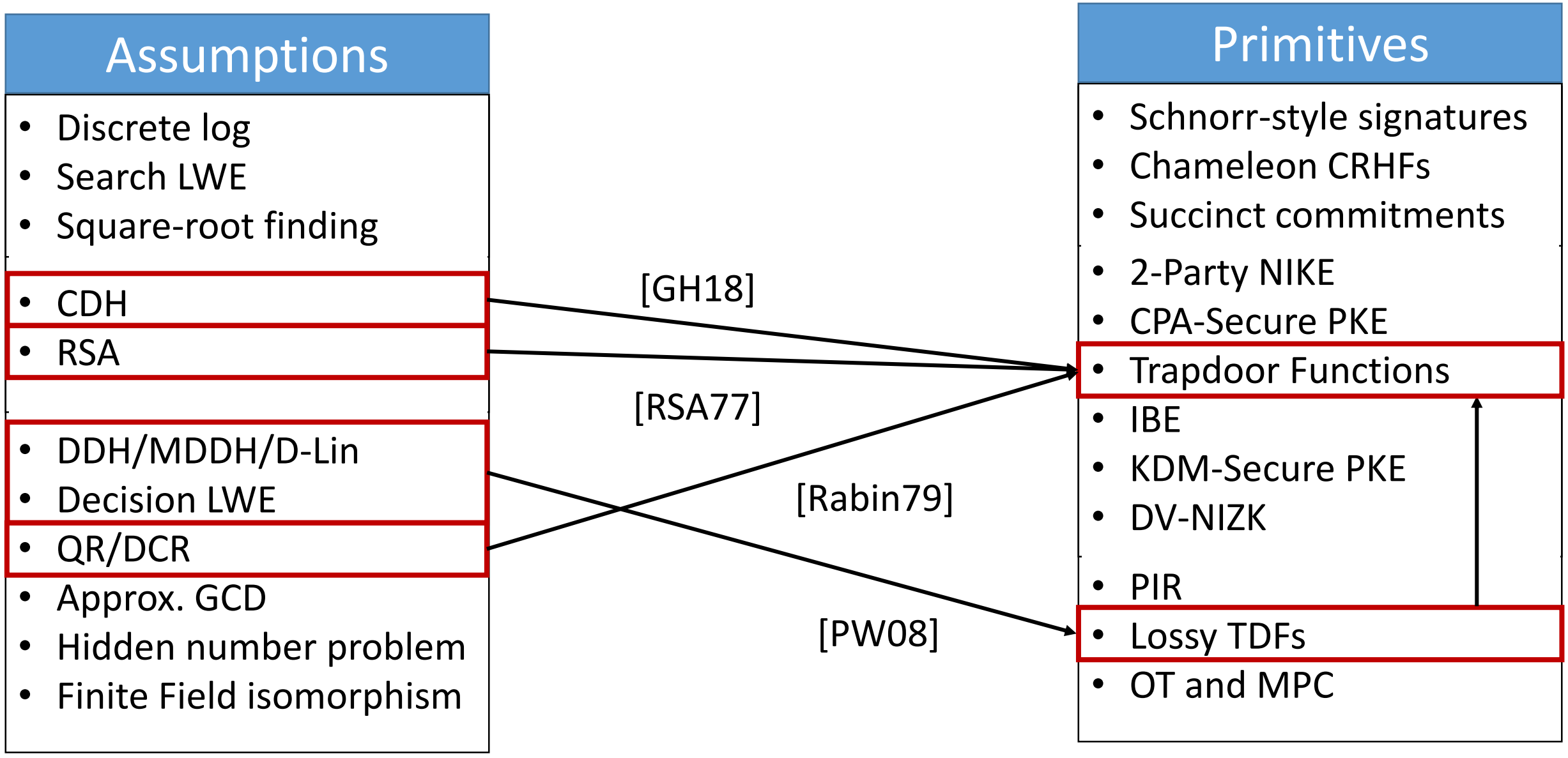
Traditional Approach to Cryptography



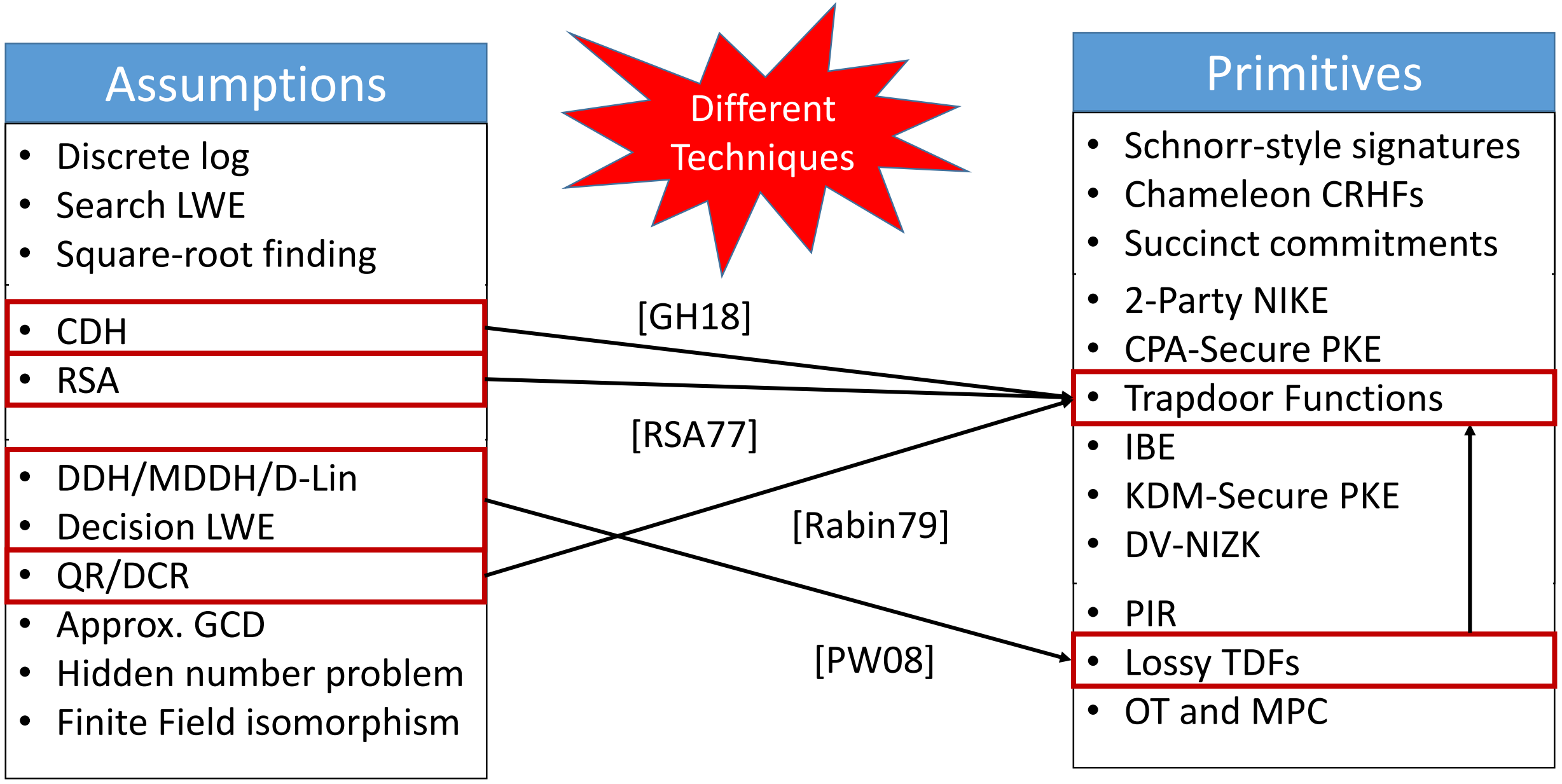
Traditional Approach to Cryptography



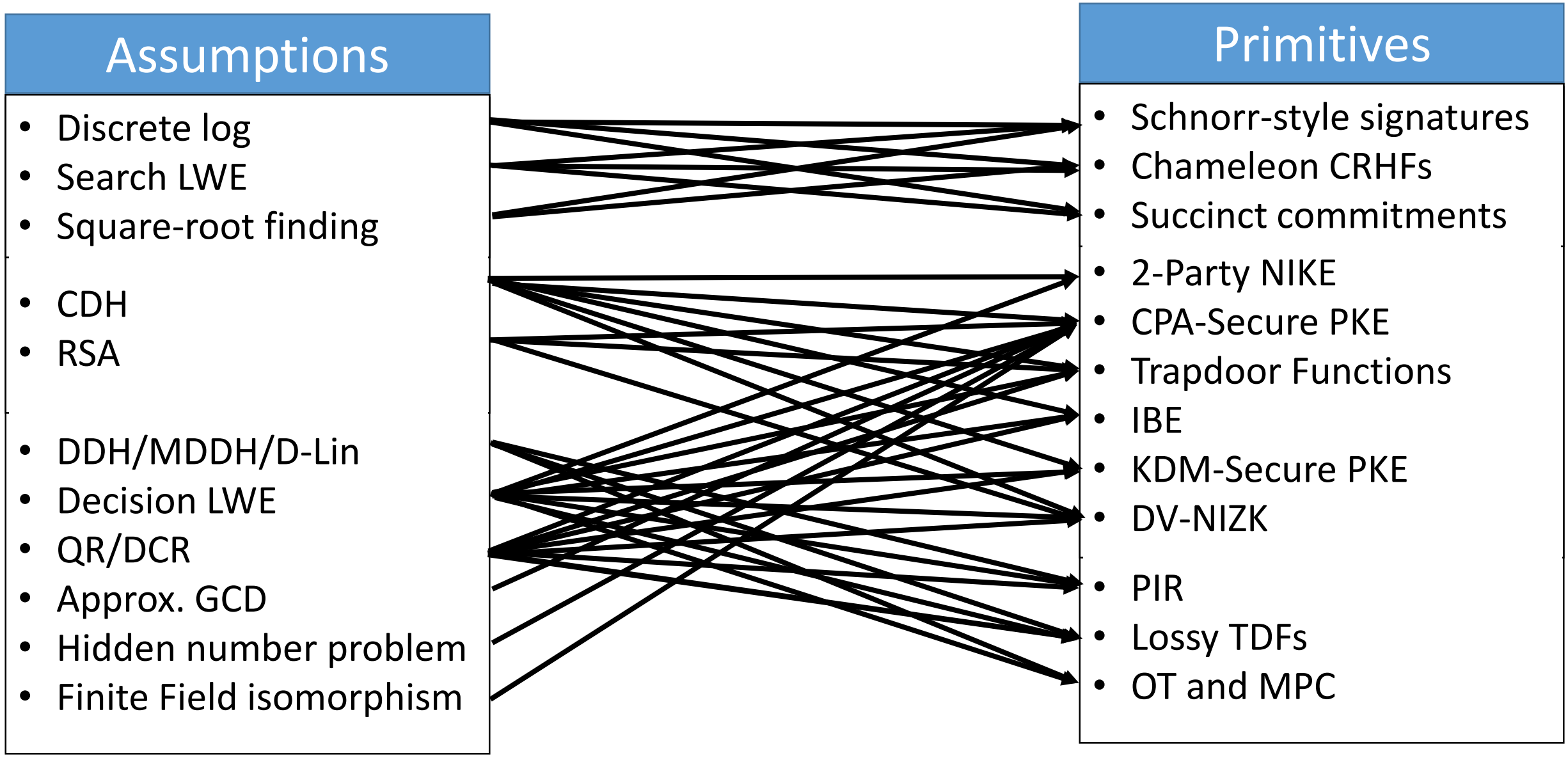
Traditional Approach to Cryptography



Traditional Approach to Cryptography

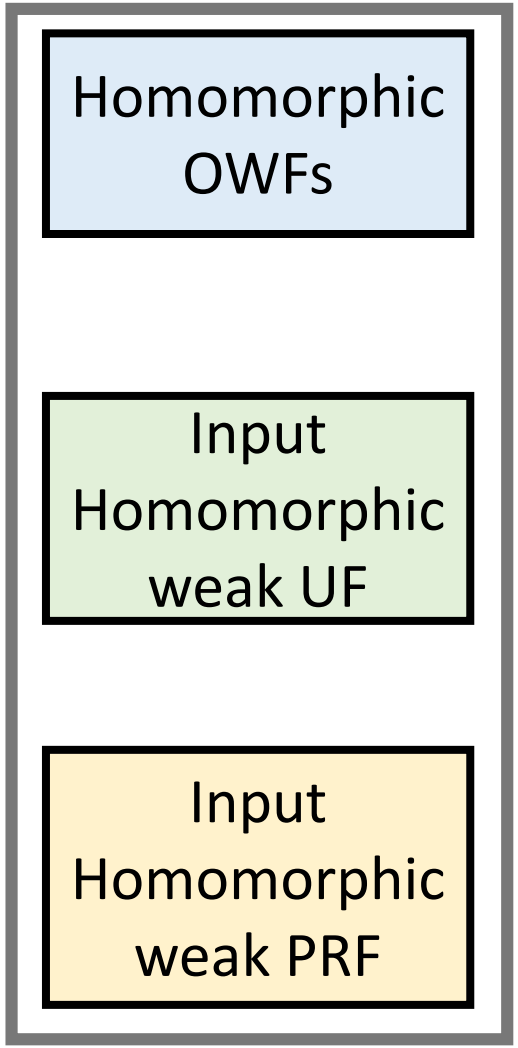


Traditional Approach to Cryptography



A “Narrow-Waist” Approach

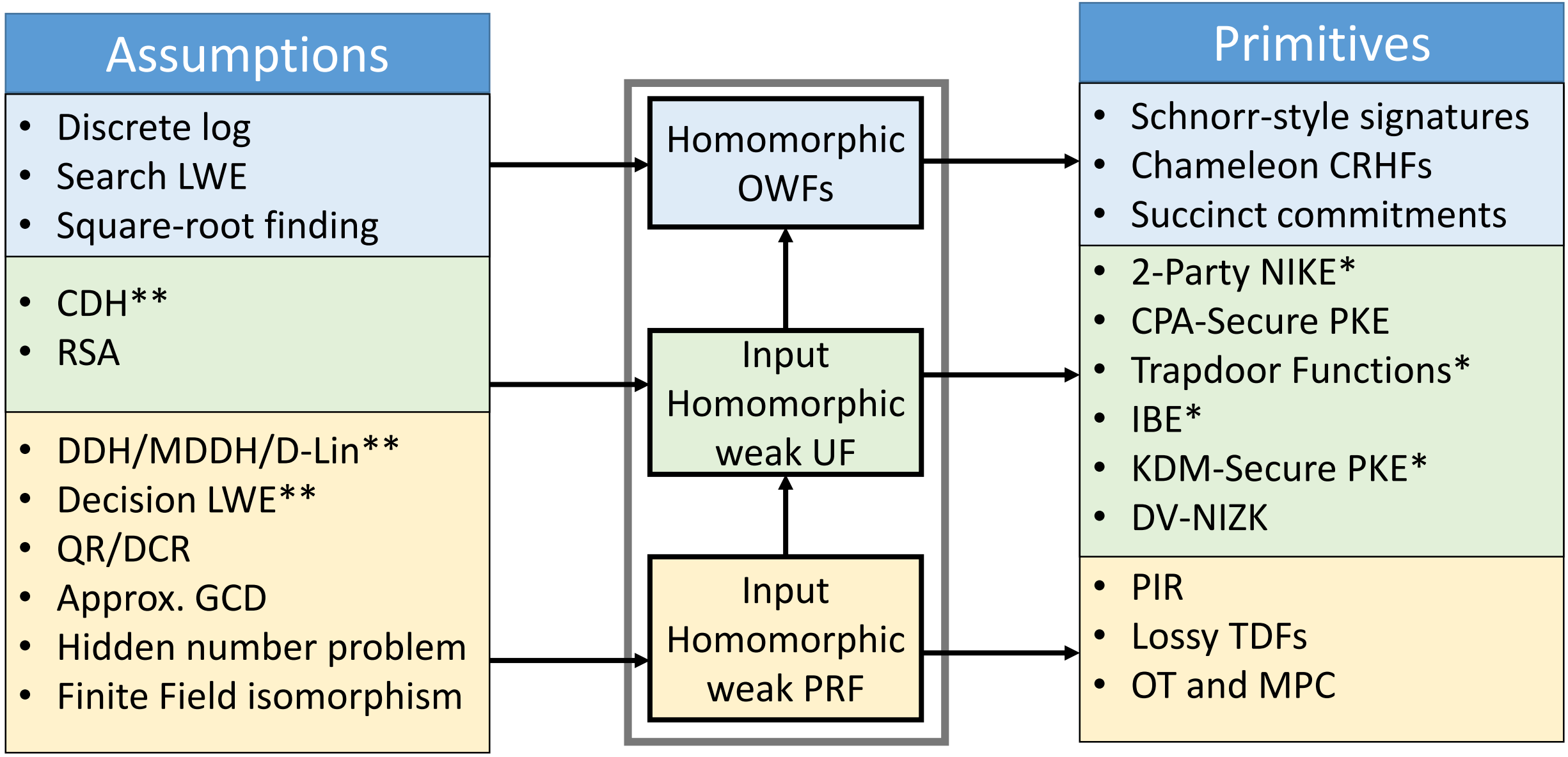
Assumptions
• Discrete log • Search LWE • Square-root finding
• CDH • RSA
• DDH/MDDH/D-Lin • Decision LWE • QR/DCR • Approx. GCD • Hidden number problem • Finite Field isomorphism



Primitives
• Schnorr-style signatures • Chameleon CRHFs • Succinct commitments
• 2-Party NIKE • CPA-Secure PKE • Trapdoor Functions • IBE • KDM-Secure PKE • DV-NIZK
• PIR • Lossy TDFs • OT and MPC

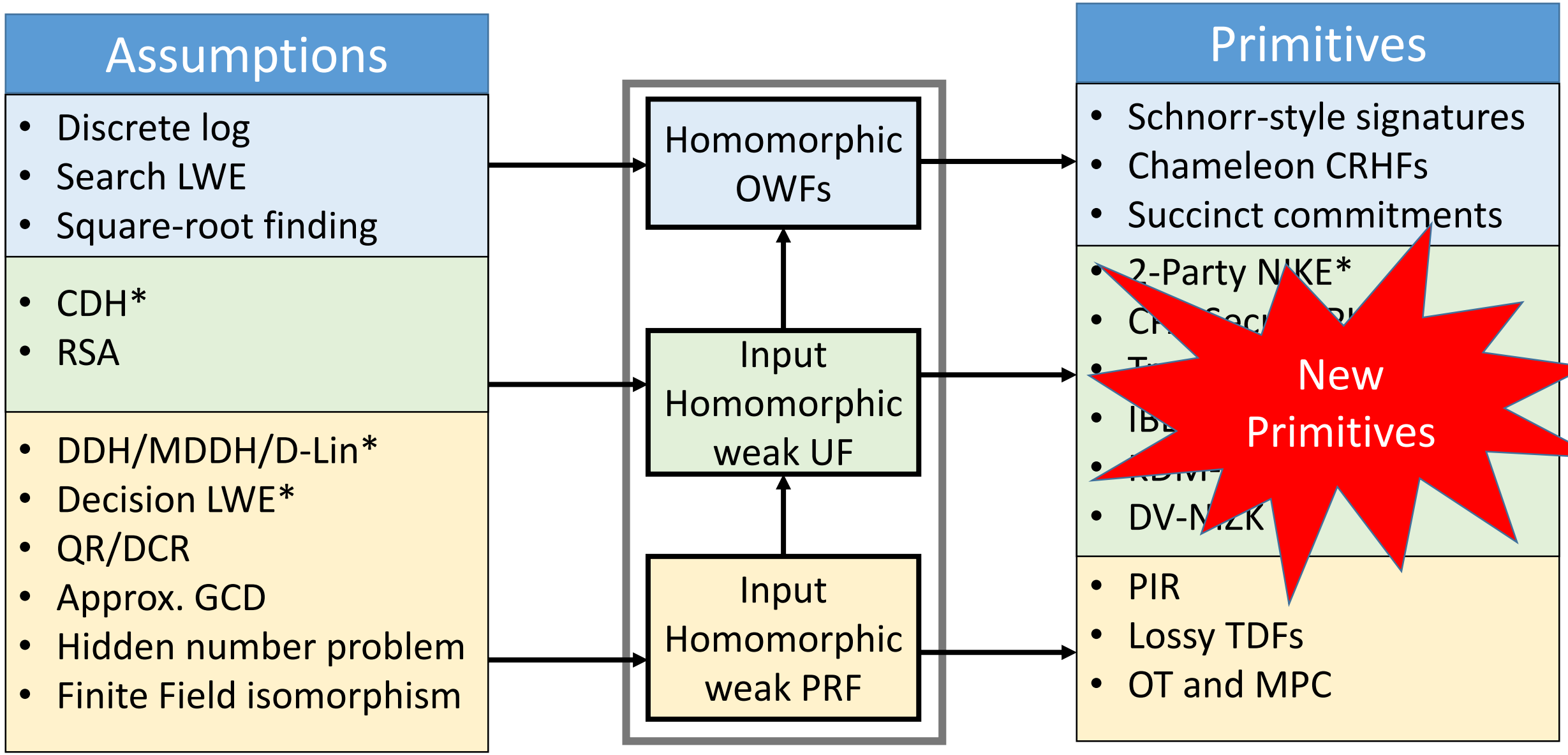
A “Narrow-Waist” Approach

* primitives need some additional structure from ** assumption



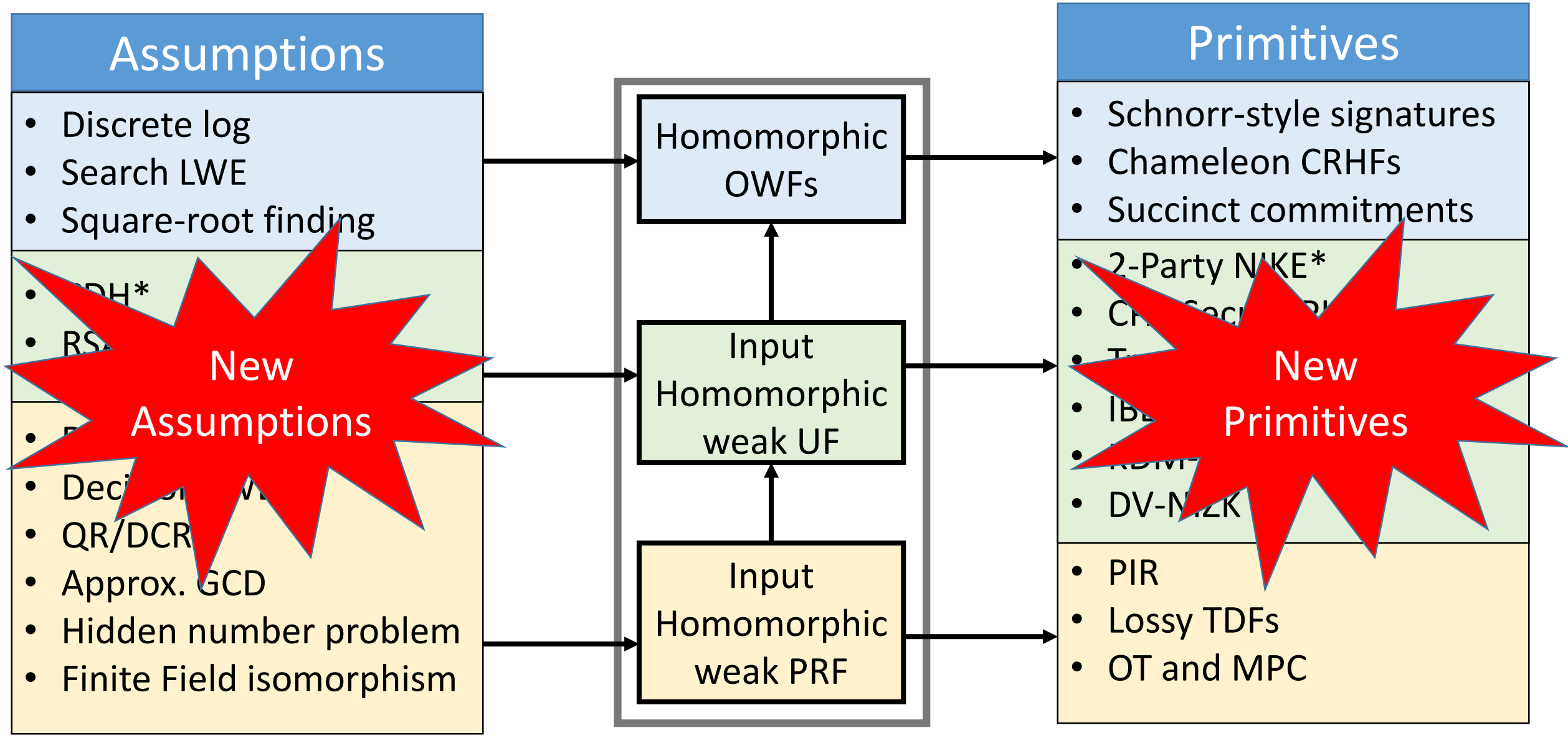
A “Narrow-Waist” Approach

* primitives need some additional structure from ** assumption



A “Narrow-Waist” Approach

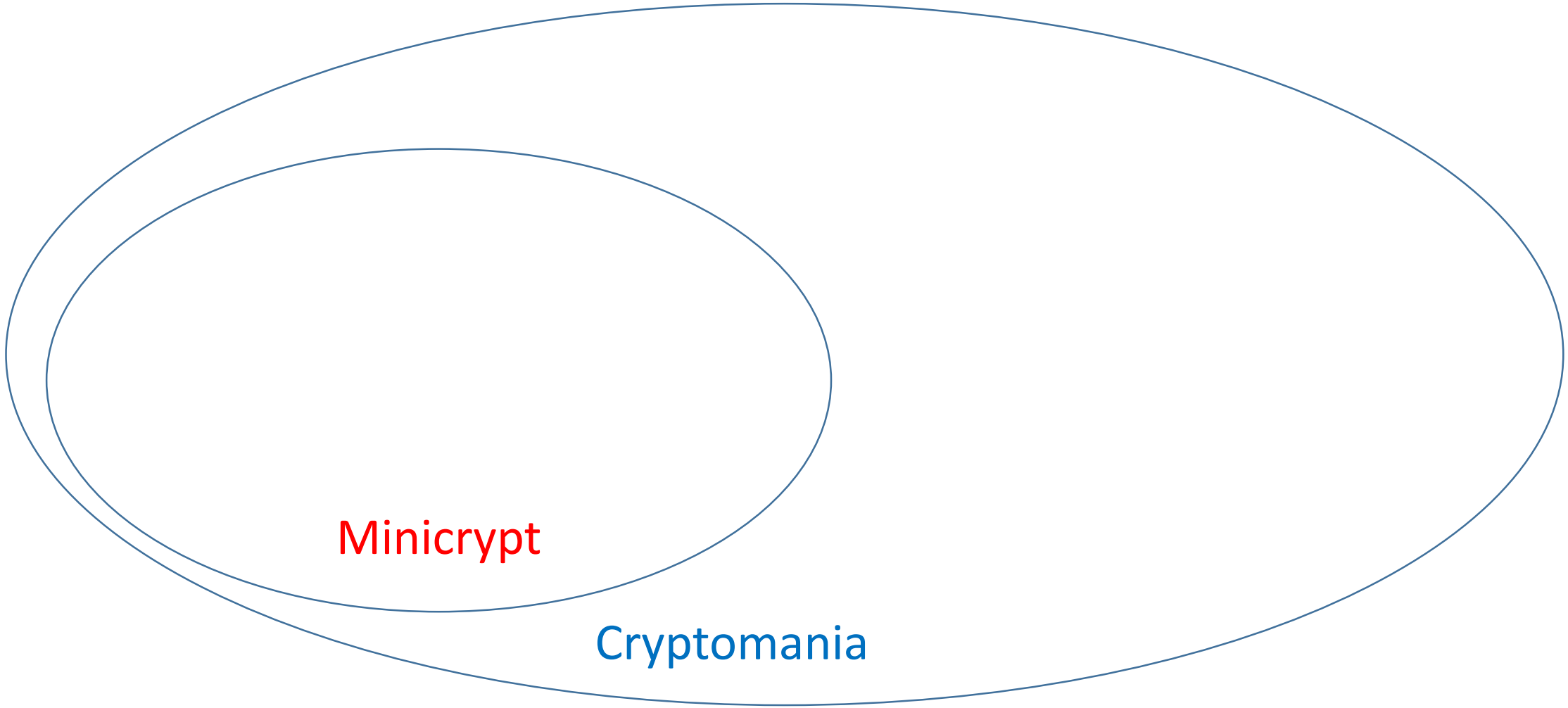
* primitives need some additional structure from ** assumption



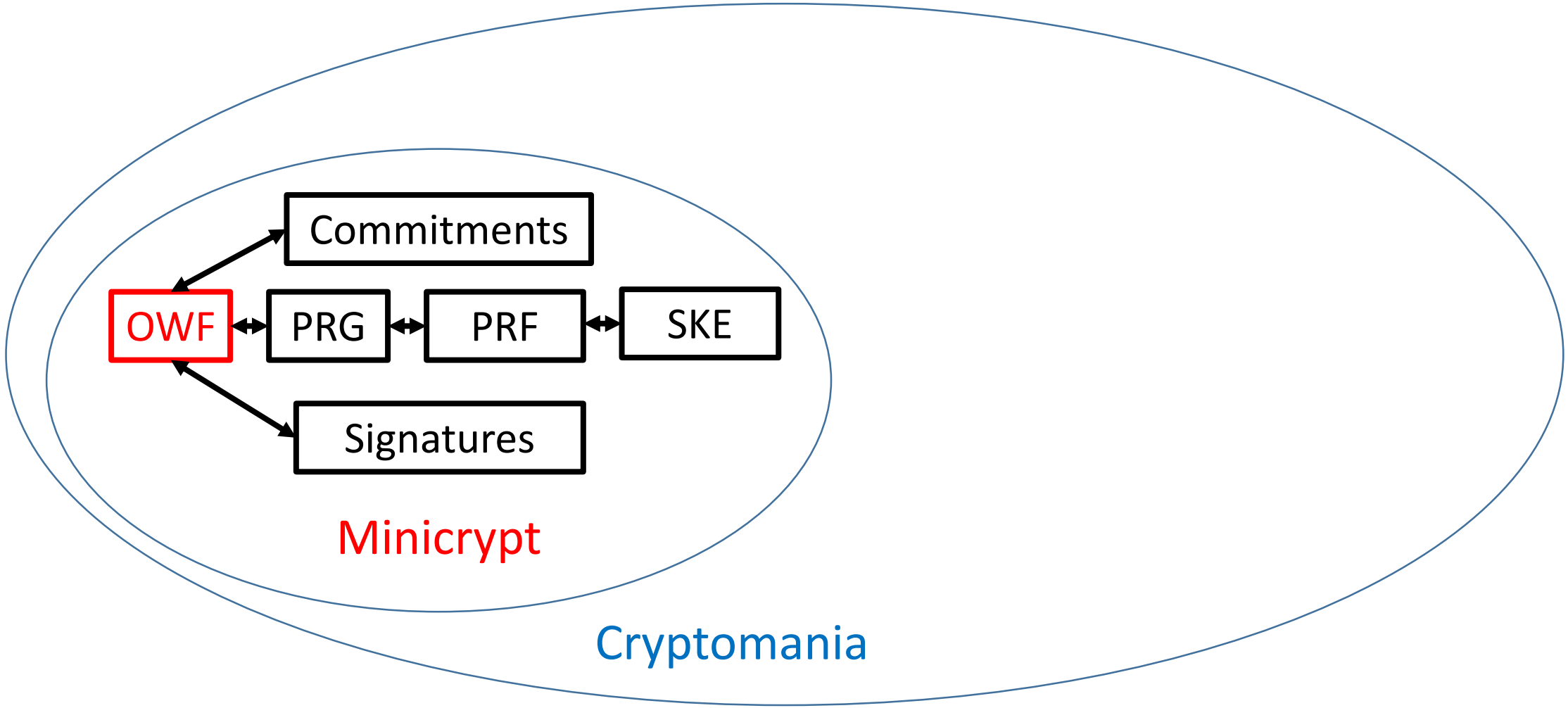
Outline

- Our results
- An alternative approach to designing primitives
- **A cryptoplexity hierarchy in Cryptomania**
- Technical overview
- Summary and open questions

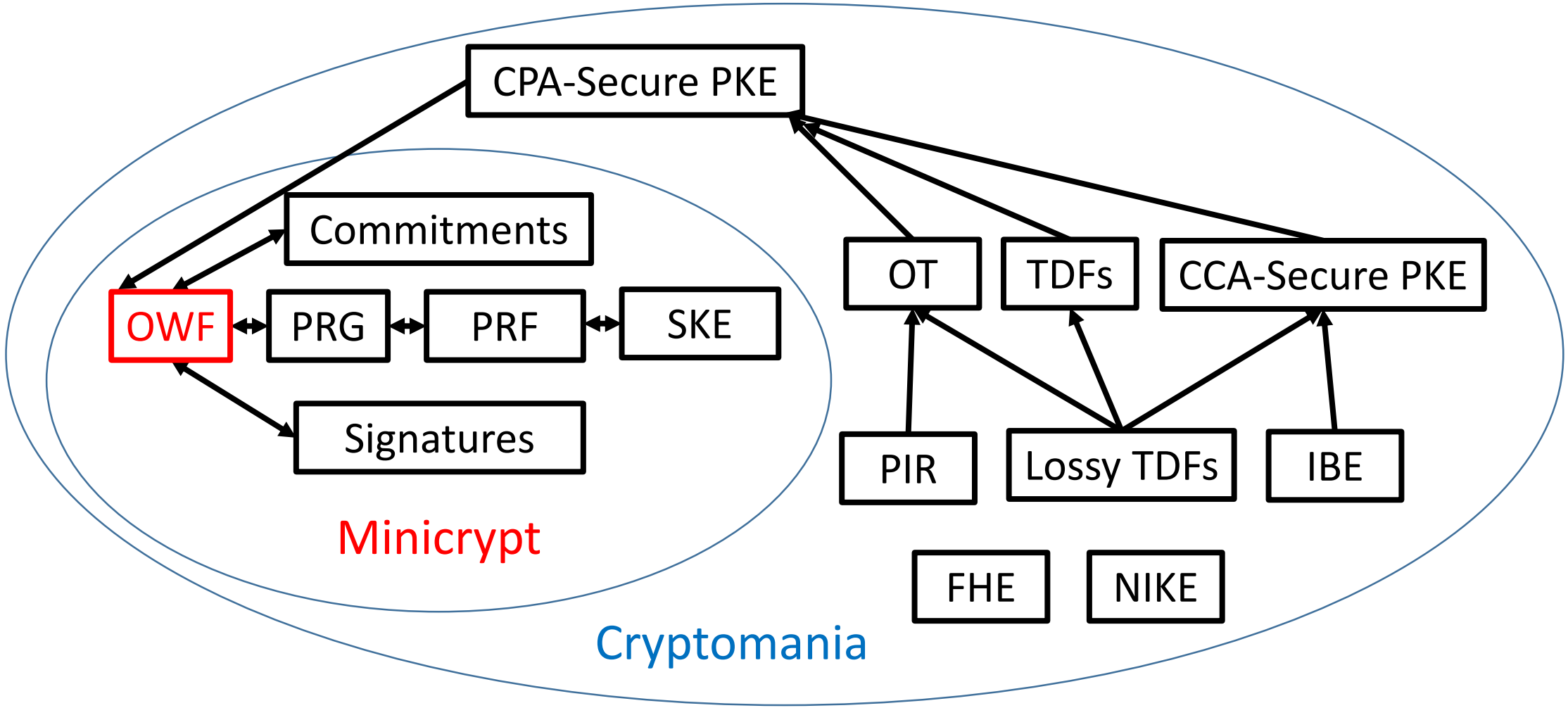
Cryptoplexity Perspective



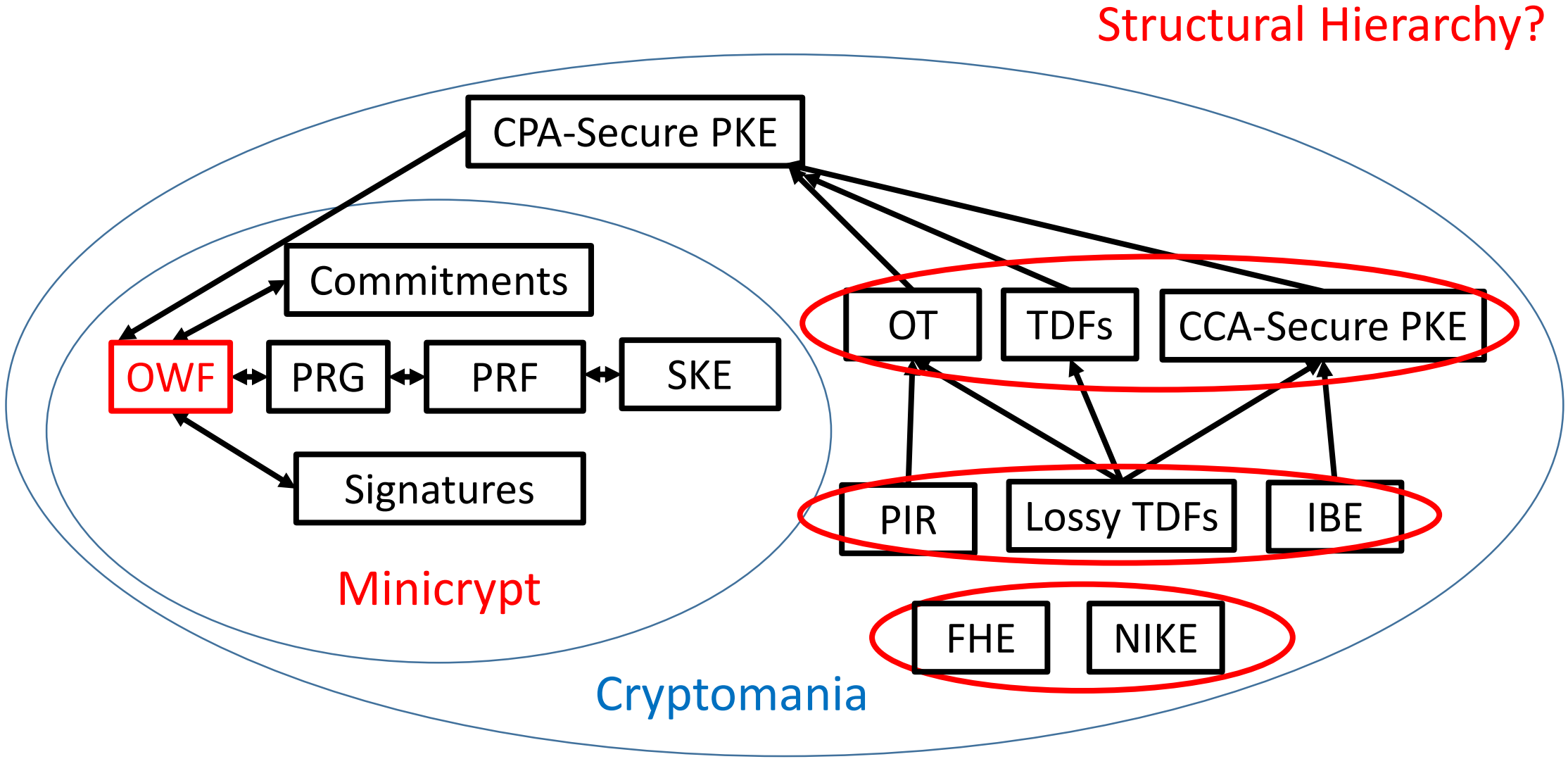
OWFs are “Minicrypt-Complete”



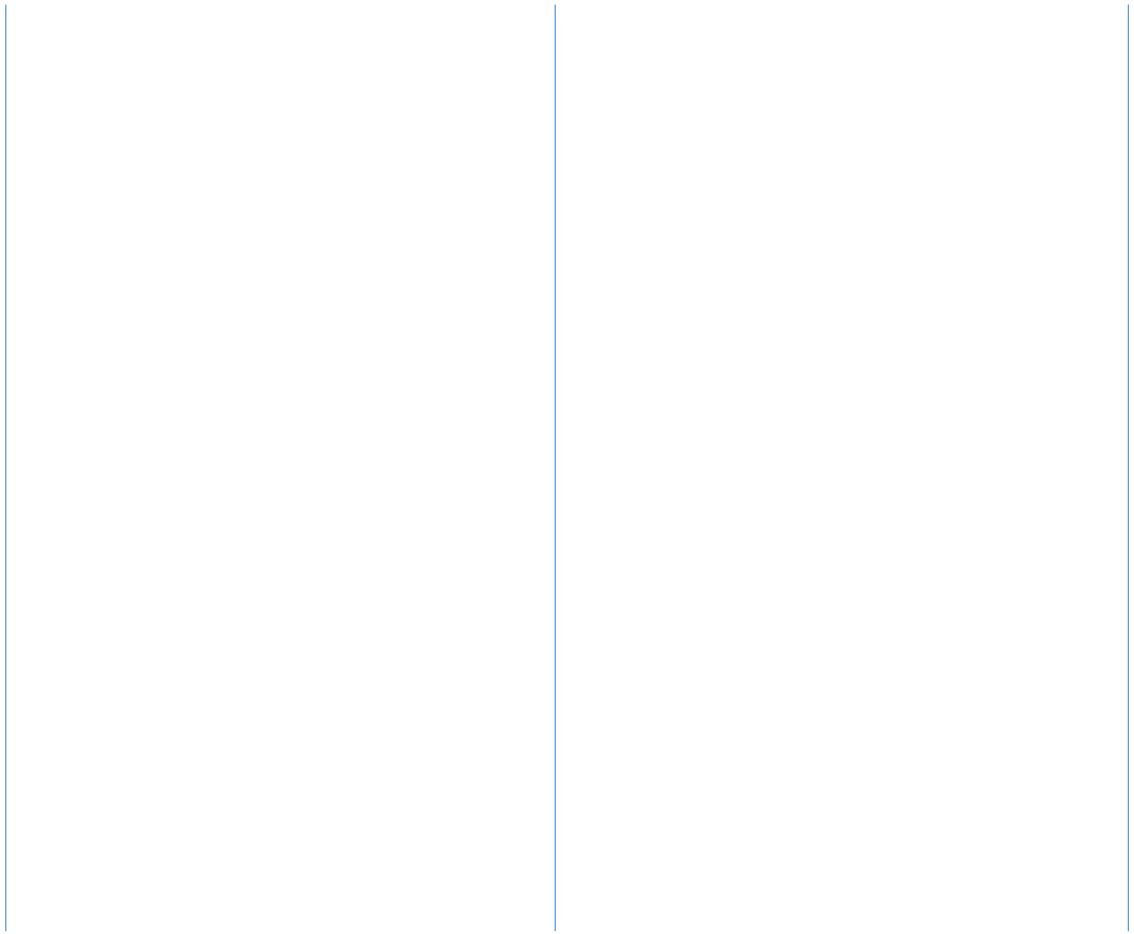
What about Cryptomania?



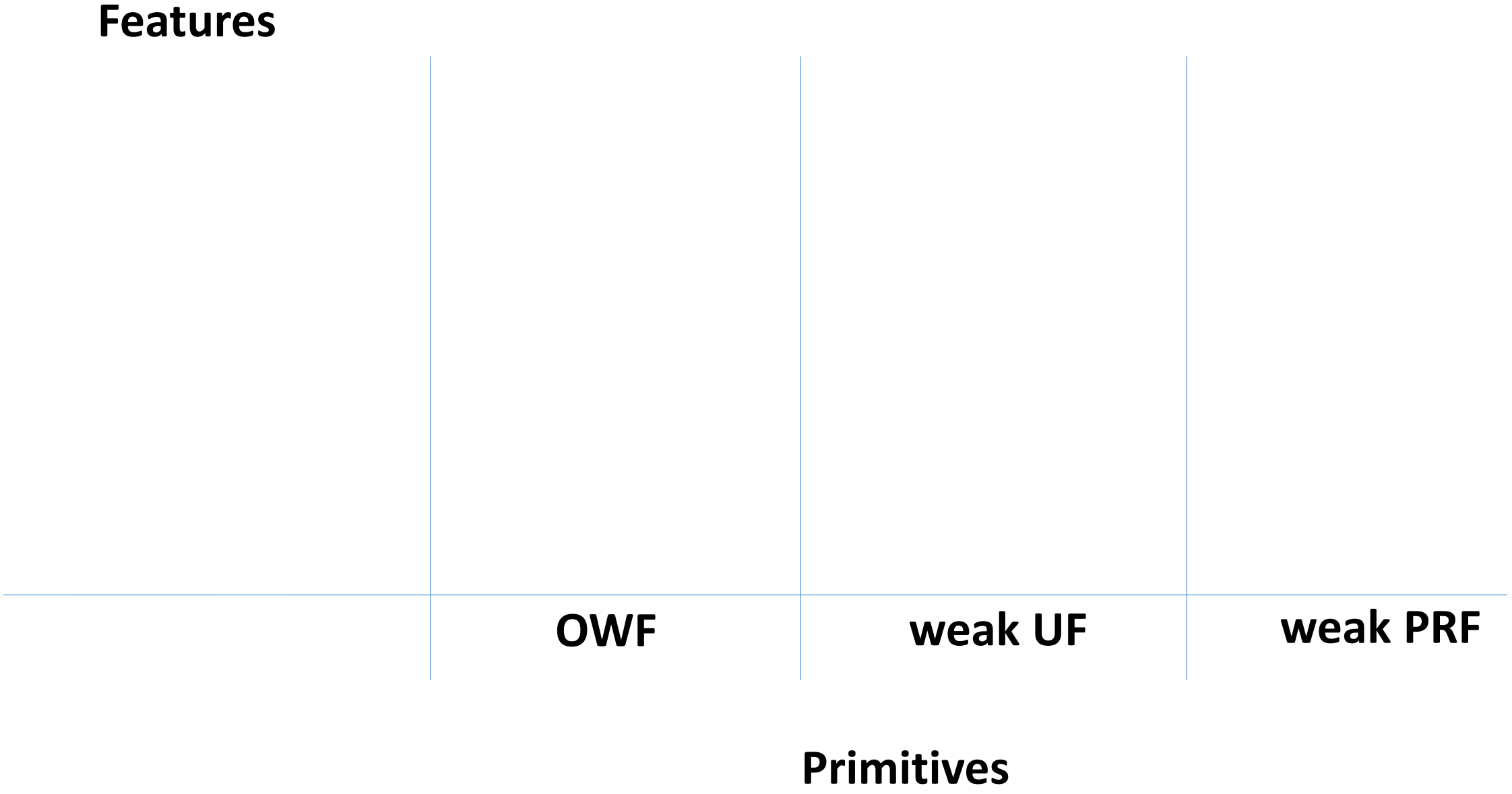
What about Cryptomania?



A Potential Cryptoplexity Hierarchy



A Potential Cryptoplexity Hierarchy



A Potential Cryptoplexity Hierarchy

Features

Dual-computability		2-party NIKE, PKE	
	OWF	**weak UF**	**weak PRF**

Primitives

A Potential Cryptoplexity Hierarchy

Features

Group Input-Homomorphism	Trapdoor CRHF, Succinct Commitments	TDF, IBE, DV-NIZK KDM-Secure PKE	PIR, Lossy TDF, OT, MPC
Dual-computability		2-party NIKE, PKE	
	OWF	**weak UF**	**weak PRF**

Primitives

A Potential Cryptoplexity Hierarchy

Features

Ring Input-Homomorphism			Fully-Homomorphic Encryption
Group Input-Homomorphism	Trapdoor CRHF, Succinct Commitments	TDF, IBE, DV-NIZK KDM-Secure PKE	PIR, Lossy TDF, OT, MPC
Dual-computability		2-party NIKE, PKE	
	OWF	**weak UF**	**weak PRF**

Primitives

A Potential Cryptoplexity Hierarchy

Features

Ring Input-Homomorphism			Fully-Homomorphic Encryption
Group Key-Homomorphism ↓ **Group Input-Homomorphism**	Trapdoor CRHF, Succinct Commitments	TDF, IBE, DV-NIZK KDM-Secure PKE	PIR, Lossy TDF, OT, MPC
Dual-computability		2-party NIKE, PKE	
	OWF	**weak UF**	**weak PRF**

Primitives

A Potential Cryptoplexity Hierarchy

Features			
Ring Key-Homomorphism			Multi-party NIKE, Indistinguishability Obfuscation
Ring Input-Homomorphism			Fully-Homomorphic Encryption
Group Key-Homomorphism ↓ **Group Input-Homomorphism**	Trapdoor CRHF, Succinct Commitments	TDF, IBE, DV-NIZK KDM-Secure PKE	PIR, Lossy TDF, OT, MPC
Dual-computability		2-party NIKE, PKE	
	OWF	**weak UF**	**weak PRF**
		Primitives	

A Potential Cryptoplexity Hierarchy

Features	Field key/input homomorphism is impossible!		
Ring Key-Homomorphism			Multi-party NIKE, Indistinguishability Obfuscation
Ring Input-Homomorphism			Fully-Homomorphic Encryption
Group Key-Homomorphism ↓ **Group Input-Homomorphism**	Trapdoor CRHF, Succinct Commitments	TDF, IBE, DV-NIZK KDM-Secure PKE	PIR, Lossy TDF, OT, MPC
Dual-computability		2-party NIKE, PKE	
	OWF	**weak UF**	**weak PRF**
		Primitives	

A Potential Cryptoplexity Hierarchy

Field key/input homomorphism is impossible!

More Structure

Features			
Ring Key-Homomorphism			Multi-party NIKE, Indistinguishability Obfuscation
Ring Input-Homomorphism			Fully-Homomorphic Encryption
Group Key-Homomorphism ↓ **Group Input-Homomorphism**	Trapdoor CRHF, Succinct Commitments	TDF, IBE, DV-NIZK KDM-Secure PKE	PIR, Lossy TDF, OT, MPC
Dual-computability		2-party NIKE, PKE	
	OWF	**weak UF**	**weak PRF**

Primitives

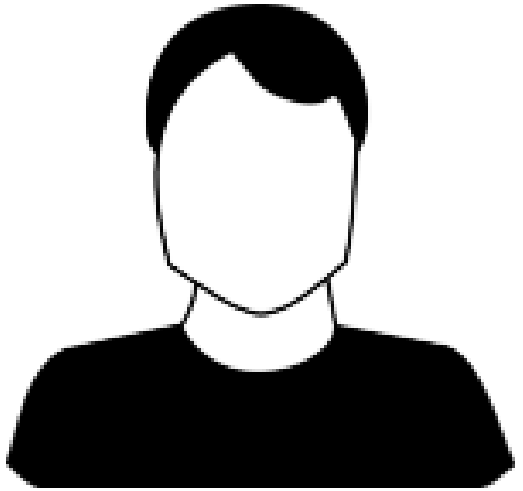
Outline

- Our results
- An alternative approach to designing primitives
- A cryptoplexity hierarchy in Cryptomania
- **Techniques**
- Summary and open questions

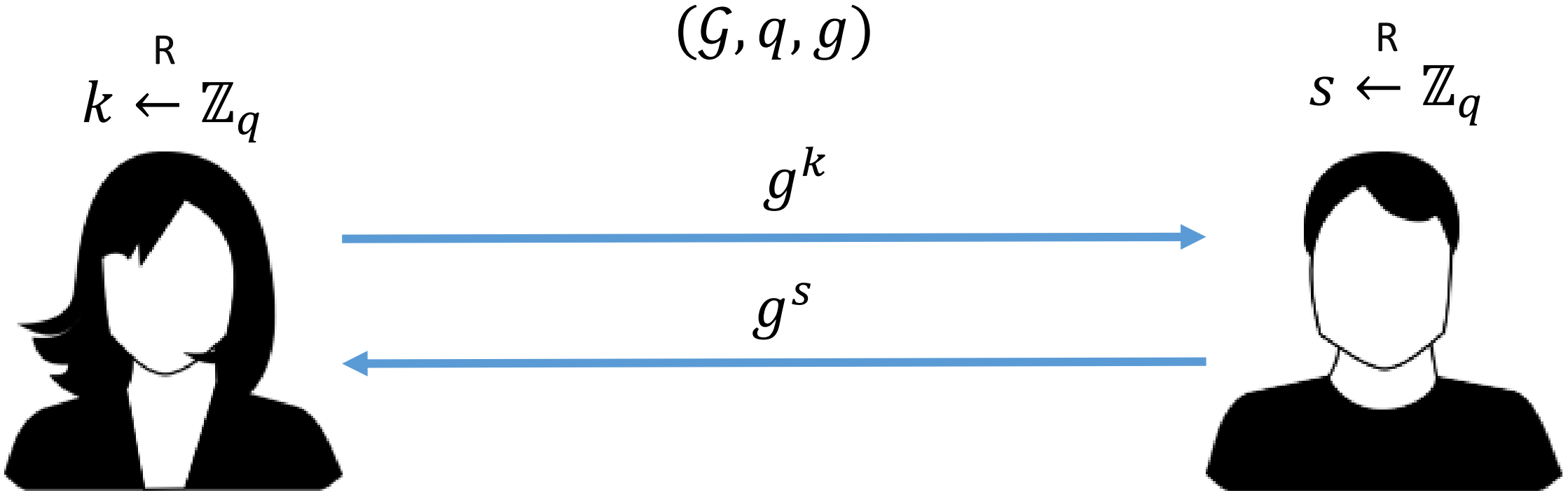
Two-party non-interactive key-exchange (NIKE) from Input-Homomorphic weak UF

Two-party NIKE from CDH (Computational Diffie-Hellman)

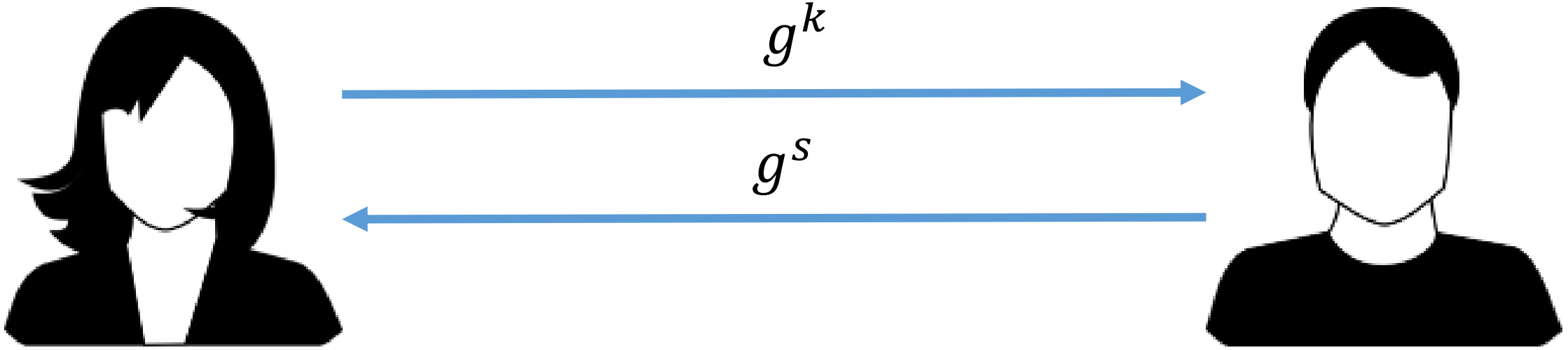
$$(\mathcal{G}, q, g)$$



Two-party NIKE from CDH (Computational Diffie-Hellman)



Two-party NIKE from CDH (Computational Diffie-Hellman)



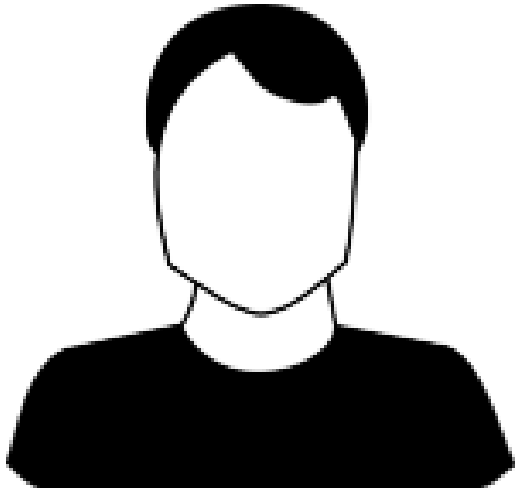
GL (g^{ks})

GL(): Goldreich-Levin Hardcore Predicate [GL89]

GL (g^{ks})

Two-party NIKE from CDH

$$\left(\mathcal{G}, q, \begin{matrix} g_{1,0} & \cdots & g_{n,0} \\ g_{1,1} & \cdots & g_{n,1} \end{matrix}\right) \qquad n > 3 \log |\mathcal{G}|$$

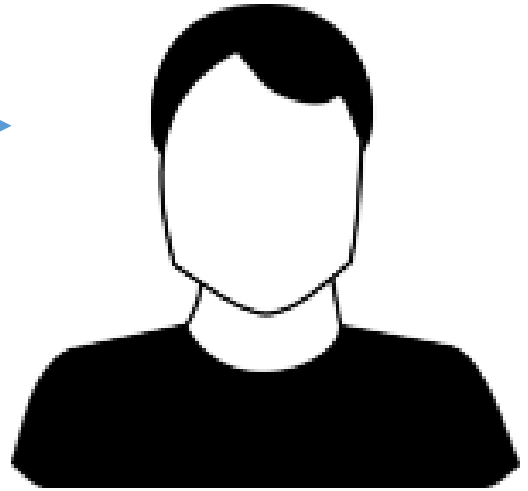


Two-party NIKE from CDH

$$\left(\mathcal{G}, q, \begin{matrix} g_{1,0} & \cdots & g_{n,0} \\ g_{1,1} & \cdots & g_{n,1} \end{matrix}\right) \qquad n > 3\log|\mathcal{G}|$$

$$k \xleftarrow{R} \mathbb{Z}_q$$

$$\begin{matrix} g_{1,0}^k & \cdots & g_{n,0}^k \\ g_{1,1}^k & \cdots & g_{n,1}^k \end{matrix}$$



Two-party NIKE from CDH

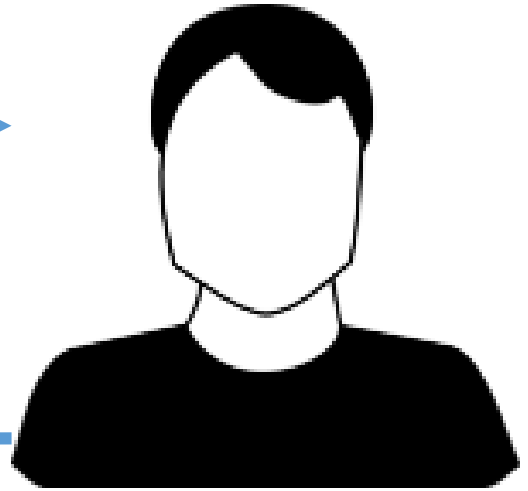
$$\left(\mathcal{G}, q, \begin{matrix} g_{1,0} & \cdots & g_{n,0} \\ g_{1,1} & \cdots & g_{n,1} \end{matrix}\right) \qquad n > 3\log|\mathcal{G}|$$

$k \xleftarrow{R} \mathbb{Z}_q$

$\mathbf{s} = (s_1, \ldots, s_n) \xleftarrow{R} \{0,1\}^n$

$$\begin{matrix} g_{1,0}^k & \cdots & g_{n,0}^k \\ g_{1,1}^k & \cdots & g_{n,1}^k \end{matrix}$$

$$\prod_{j=1}^{n} g_{j,s_j}$$



Two-party NIKE from CDH

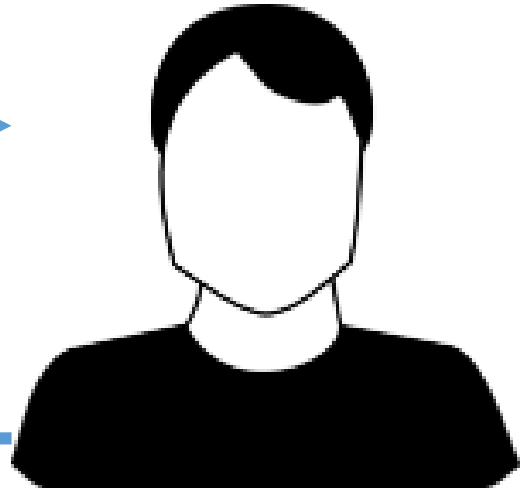
$$\left(\mathcal{G}, q, \begin{matrix} g_{1,0} & \cdots & g_{n,0} \\ g_{1,1} & \cdots & g_{n,1} \end{matrix}\right) \qquad n > 3\log|\mathcal{G}|$$

$k \xleftarrow{R} \mathbb{Z}_q$

$\mathbf{s} = (s_1, \ldots, s_n) \xleftarrow{R} \{0,1\}^n$

$$\begin{matrix} g_{1,0}^k & \cdots & g_{n,0}^k \\ g_{1,1}^k & \cdots & g_{n,1}^k \end{matrix}$$

$$\prod_{j=1}^{n} g_{j,s_j}$$



$\prod_{j=1}^{n} g_{j,s_j}^k$

$\prod_{j=1}^{n} g_{j,s_j}^k$

Two-party NIKE from CDH

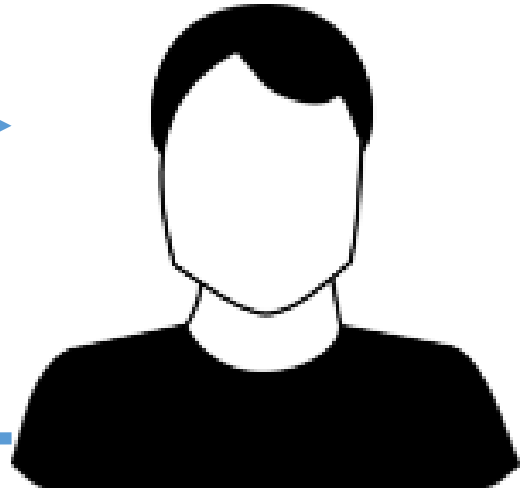
$$\left(\mathcal{G}, q, \begin{matrix} g_{1,0} & \cdots & g_{n,0} \\ g_{1,1} & \cdots & g_{n,1} \end{matrix}\right) \qquad n > 3\log|\mathcal{G}|$$

$k \xleftarrow{R} \mathbb{Z}_q$

$\mathbf{s} = (s_1, \ldots, s_n) \xleftarrow{R} \{0,1\}^n$

$$\begin{matrix} g_{1,0}^k & \cdots & g_{n,0}^k \\ g_{1,1}^k & \cdots & g_{n,1}^k \end{matrix}$$

$$\prod_{j=1}^{n} g_{j,s_j}$$



$\mathrm{GL}(\prod_{j=1}^{n} g_{j,s_j}^k)$

$\mathrm{GL}(\prod_{j=1}^{n} g_{j,s_j}^k)$

Two-party NIKE from CDH

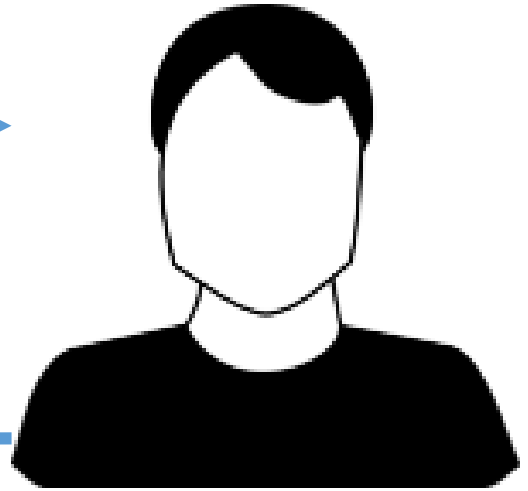
$$\left(\mathcal{G}, q, \begin{matrix} g_{1,0} & \cdots & g_{n,0} \\ g_{1,1} & \cdots & g_{n,1} \end{matrix}\right) \qquad n > 3\log|\mathcal{G}|$$

$k \xleftarrow{R} \mathbb{Z}_q$

$\mathbf{s} = (s_1, \ldots, s_n) \xleftarrow{R} \{0,1\}^n$

$$\begin{matrix} g_{1,0}^k & \cdots & g_{n,0}^k \\ g_{1,1}^k & \cdots & g_{n,1}^k \end{matrix}$$

$$\prod_{j=1}^{n} g_{j,s_j}$$



$\mathbf{s}$ is computationally hidden (by DLOG)

$\mathrm{GL}(\prod_{j=1}^{n} g_{j,s_j}^k)$

$\mathrm{GL}(\prod_{j=1}^{n} g_{j,s_j}^k)$

Two-party NIKE from CDH

$$\left(\mathcal{G}, q, \begin{matrix} g_{1,0} & \cdots & g_{n,0} \\ g_{1,1} & \cdots & g_{n,1} \end{matrix}\right) \qquad n > 3\log|\mathcal{G}|$$

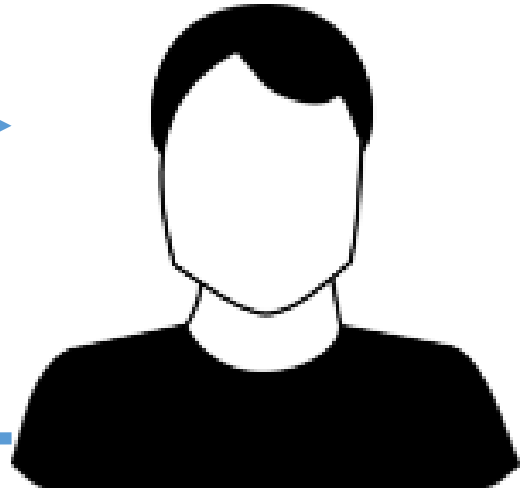
$k \xleftarrow{R} \mathbb{Z}_q$

$\mathbf{s} = (s_1, \ldots, s_n) \xleftarrow{R} \{0,1\}^n$

$$\begin{matrix} g_{1,0}^k & \cdots & g_{n,0}^k \\ g_{1,1}^k & \cdots & g_{n,1}^k \end{matrix}$$

By LHL

$$\prod_{j=1}^{n} g_{j,s_j} \approx_s g^*$$



$\mathrm{GL}(\prod_{j=1}^{n} g_{j,s_j}^k) \approx_s \mathrm{GL}(g^{*k})$

$\mathrm{GL}(g^{*k}) \approx_s \mathrm{GL}(\prod_{j=1}^{n} g_{j,s_j}^k)$

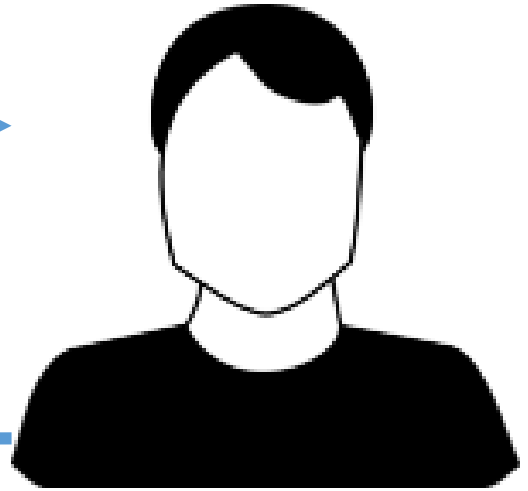
Two-party NIKE from CDH

$$\left(\mathcal{G}, q, \begin{matrix} g_{1,0} & \cdots & g_{n,0} \\ g_{1,1} & \cdots & g_{n,1} \end{matrix}\right) \qquad n > 3\log|\mathcal{G}|$$

$k \xleftarrow{R} \mathbb{Z}_q$

$$\begin{matrix} g_{1,0}^k & \cdots & g_{n,0}^k \\ g_{1,1}^k & \cdots & g_{n,1}^k \end{matrix}$$

$\mathbf{s} = (s_1, \ldots, s_n) \xleftarrow{R} \{0,1\}^n$



By LHL

$$\prod_{j=1}^{n} g_{j,s_j} \approx_s g^*$$

$$\mathrm{GL}\left(\prod_{j=1}^{n} g_{j,s_j}^k\right) \approx_s \boxed{\mathrm{GL}(g^{*k})} \approx_c b' \approx_c \boxed{\mathrm{GL}(g^{*k})} \approx_s \mathrm{GL}\left(\prod_{j=1}^{n} g_{j,s_j}^k\right)$$

By CDH

Translating to Input Homomorphic weak UF

CDH

IHwUF

Translating to Input Homomorphic weak UF

CDH

$$\left(\mathcal{G}, q, \begin{matrix} g_{1,0} & \cdots & g_{n,0} \\ g_{1,1} & \cdots & g_{n,1} \end{matrix}\right)$$

$$n > 3 \log |\mathcal{G}|$$

IHwUF

$$\left(F\colon \mathcal{K} \times \mathcal{X} \to \mathcal{Y} \quad \begin{matrix} x_{1,0} & \cdots & x_{n,0} \\ x_{1,1} & \cdots & x_{n,1} \end{matrix}\right)$$

$$n > 3 \log |\mathcal{X}|$$

Translating to Input Homomorphic weak UF

CDH

$$\left(\mathcal{G}, q, \begin{matrix} g_{1,0} & \cdots & g_{n,0} \\ g_{1,1} & \cdots & g_{n,1} \end{matrix}\right)$$

$$n > 3 \log |\mathcal{G}|$$

$$k \xleftarrow{R} \mathbb{Z}_q \qquad \begin{matrix} g_{1,0}^k & \cdots & g_{n,0}^k \\ g_{1,1}^k & \cdots & g_{n,1}^k \end{matrix}$$

IHwUF

$$\left(F\colon \mathcal{K} \times \mathcal{X} \to \mathcal{Y} \qquad \begin{matrix} x_{1,0} & \cdots & x_{n,0} \\ x_{1,1} & \cdots & x_{n,1} \end{matrix}\right)$$

$$n > 3 \log |\mathcal{X}|$$

$$k \xleftarrow{R} \mathcal{K} \qquad \begin{matrix} F(k, x_{1,0}) & \cdots & F(k, x_{n,0}) \\ F(k, x_{2,0}) & \cdots & F(k, x_{n,1}) \end{matrix}$$

Translating to Input Homomorphic weak UF

CDH

$$\left(\mathcal{G}, q, \begin{matrix} g_{1,0} & \cdots & g_{n,0} \\ g_{1,1} & \cdots & g_{n,1} \end{matrix}\right)$$

$$n > 3 \log |\mathcal{G}|$$

$$k \xleftarrow{R} \mathbb{Z}_q \qquad \begin{matrix} g_{1,0}^k & \cdots & g_{n,0}^k \\ g_{1,1}^k & \cdots & g_{n,1}^k \end{matrix}$$

$$\mathbf{s} = (s_1, \ldots, s_n) \xleftarrow{R} \{0,1\}^n \qquad \prod_{j=1}^{n} g_{j,s_j}$$

IHwUF

$$\left(F\colon \mathcal{K} \times \mathcal{X} \to \mathcal{Y} \quad \begin{matrix} x_{1,0} & \cdots & x_{n,0} \\ x_{1,1} & \cdots & x_{n,1} \end{matrix}\right)$$

$$n > 3 \log |\mathcal{X}|$$

$$k \xleftarrow{R} \mathcal{K} \qquad \begin{matrix} F(k, x_{1,0}) & \cdots & F(k, x_{n,0}) \\ F(k, x_{2,0}) & \cdots & F(k, x_{n,1}) \end{matrix}$$

$$\mathbf{s} = (s_1, \ldots, s_n) \xleftarrow{R} \{0,1\}^n \qquad \bigoplus_{j=1}^{n} x_{j,s_j}$$

Translating to Input Homomorphic weak UF

CDH

$$\left(\mathcal{G}, q, \begin{matrix} g_{1,0} & \cdots & g_{n,0} \\ g_{1,1} & \cdots & g_{n,1} \end{matrix}\right)$$

$$n > 3 \log |\mathcal{G}|$$

$$k \xleftarrow{R} \mathbb{Z}_q \qquad \begin{matrix} g_{1,0}^k & \cdots & g_{n,0}^k \\ g_{1,1}^k & \cdots & g_{n,1}^k \end{matrix}$$

One-way by DLOG

$$\mathbf{s} = (s_1, \ldots, s_n) \xleftarrow{R} \{0,1\}^n \qquad \prod_{j=1}^{n} g_{j,s_j}$$

IHwUF

$$\left(F\colon \mathcal{K} \times \mathcal{X} \to \mathcal{Y} \quad \begin{matrix} x_{1,0} & \cdots & x_{n,0} \\ x_{1,1} & \cdots & x_{n,1} \end{matrix}\right)$$

$$n > 3 \log |\mathcal{X}|$$

$$k \xleftarrow{R} \mathcal{K} \qquad \begin{matrix} F(k, x_{1,0}) & \cdots & F(k, x_{n,0}) \\ F(k, x_{2,0}) & \cdots & F(k, x_{n,1}) \end{matrix}$$

$$\mathbf{s} = (s_1, \ldots, s_n) \xleftarrow{R} \{0,1\}^n \qquad \bigoplus_{j=1}^{n} x_{j,s_j}$$

Translating to Input Homomorphic weak UF

CDH

$$\left(\mathcal{G}, q, \begin{matrix} g_{1,0} & \cdots & g_{n,0} \\ g_{1,1} & \cdots & g_{n,1} \end{matrix}\right)$$

$$n > 3 \log |\mathcal{G}|$$

$$k \xleftarrow{R} \mathbb{Z}_q \qquad \begin{matrix} g_{1,0}^k & \cdots & g_{n,0}^k \\ g_{1,1}^k & \cdots & g_{n,1}^k \end{matrix}$$

One-way by DLOG

$$\mathbf{s} = (s_1, \ldots, s_n) \xleftarrow{R} \{0,1\}^n \qquad \prod_{j=1}^{n} g_{j,s_j}$$

IHwUF

$$\left(F\colon \mathcal{K} \times \mathcal{X} \to \mathcal{Y}, \begin{matrix} x_{1,0} & \cdots & x_{n,0} \\ x_{1,1} & \cdots & x_{n,1} \end{matrix}\right)$$

$$n > 3 \log |\mathcal{X}|$$

$$k \xleftarrow{R} \mathcal{K} \qquad \begin{matrix} F(k, x_{1,0}) & \cdots & F(k, x_{n,0}) \\ F(k, x_{2,0}) & \cdots & F(k, x_{n,1}) \end{matrix}$$

Is this one-way in general?

$$\mathbf{s} = (s_1, \ldots, s_n) \xleftarrow{R} \{0,1\}^n \qquad \bigoplus_{j=1}^{n} x_{j,s_j}$$

One-Wayness of Subset Sums

Theorem:

If $\mathcal{X}$ is the input space of any input homomorphic weak UF

One-Wayness of Subset Sums

Theorem:

If $\mathcal{X}$ is the input space of any input homomorphic weak UF

then

the subset sum problem (with appropriate parameters) is average-case hard on $\mathcal{X}$

One-Wayness of Subset Sums

Theorem:

If $\mathcal{X}$ is the input space of any input homomorphic weak UF

then

the subset sum problem (with appropriate parameters) is average-case hard on $\mathcal{X}$

- CDH/DDH => DLOG
- LWE => SIS

One-Wayness of Subset Sums

Theorem:

If $\mathcal{X}$ is the input space of any input homomorphic weak UF

then

the subset sum problem (with appropriate parameters) is average-case hard on $\mathcal{X}$

- CDH/DDH => DLOG
- LWE => SIS

Explains the structural similarity underlying these assumptions

Theorem:

If $\mathcal{X}$ is the input space of any input homomorphic weak UF then the subset sum problem (with appropriate parameters) is average-case hard on $\mathcal{X}$

$$\begin{matrix} x_{1,0} & \dots & x_{n,0} \\ x_{1,1} & \dots & x_{n,1} \end{matrix}, \quad x^* \xleftarrow{R} \mathcal{X}$$

$$n > 3 \log |\mathcal{X}|$$

Theorem:

If $\mathcal{X}$ is the input space of any input homomorphic weak UF then the subset sum problem (with appropriate parameters) is average-case hard on $\mathcal{X}$

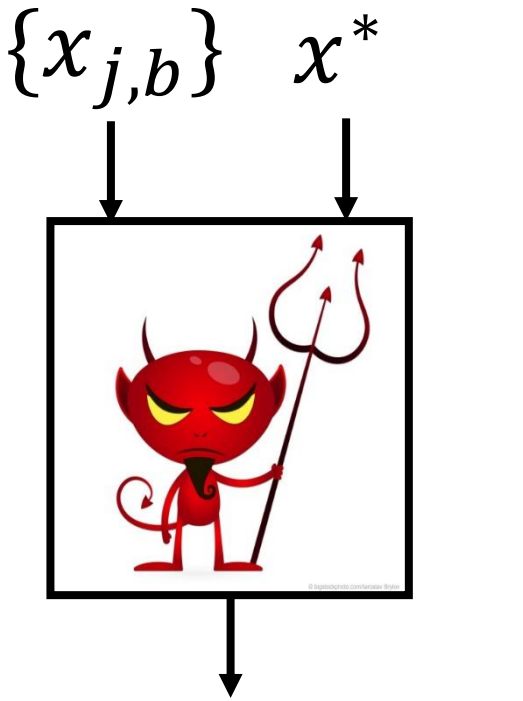
$$\begin{matrix} x_{1,0} & \cdots & x_{n,0} \\ x_{1,1} & \cdots & x_{n,1} \end{matrix}, \quad x^* \xleftarrow{R} \mathcal{X}$$

$$n > 3 \log |\mathcal{X}|$$

By LHL, any uniform x^* lies in the binary span of $\begin{matrix} x_{1,0} & \cdots & x_{n,0} \\ x_{1,1} & \cdots & x_{n,1} \end{matrix}$

Theorem:

If $\mathcal{X}$ is the input space of any input homomorphic weak UF then the subset sum problem (with appropriate parameters) is average-case hard on $\mathcal{X}$



$$\begin{matrix} x_{1,0} & \cdots & x_{n,0} \\ x_{1,1} & \cdots & x_{n,1} \end{matrix}, \; x^* \xleftarrow{R} \mathcal{X}$$

$$n > 3 \log |\mathcal{X}|$$

By LHL, any uniform x^* lies in the binary span of $\begin{matrix} x_{1,0} & \cdots & x_{n,0} \\ x_{1,1} & \cdots & x_{n,1} \end{matrix}$

Theorem:

If $\mathcal{X}$ is the input space of any input homomorphic weak UF then the subset sum problem (with appropriate parameters) is average-case hard on $\mathcal{X}$

$\{x_{j,b}\}$ x^*

$\mathbf{s} = (s_1, \ldots, s_n)$

$$\begin{matrix} x_{1,0} & \cdots & x_{n,0} \\ x_{1,1} & \cdots & x_{n,1} \end{matrix}, \; x^* \xleftarrow{R} \mathcal{X}$$

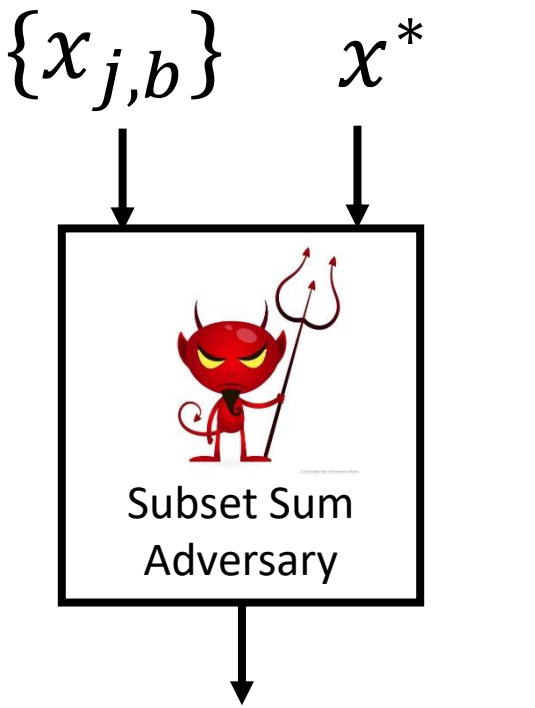
$$n > 3 \log |\mathcal{X}|$$

By LHL, any uniform x^* lies in the binary span of $\begin{matrix} x_{1,0} & \cdots & x_{n,0} \\ x_{1,1} & \cdots & x_{n,1} \end{matrix}$

$$\Pr\left[x^* = \bigoplus_{j=1}^{n} x_{j,s_j} \right] < \text{negl}(\lambda)$$

Suppose

$$\Pr\left[x^* = \bigoplus_{j=1}^{n} x_{j,\, s_j} \right] > \text{negl}\,(\lambda)$$



Suppose

$$\Pr\left[x^* = \bigoplus_{j=1}^{n} x_{j,s_j}\right] > \text{negl}(\lambda)$$

→ Adversary against IHwUF $F: \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$

IHwUF Adversary

$\{x_{j,b}\}$ x^*

Subset Sum Adversary

$\mathbf{s} = (s_1, \ldots, s_n)$

$\{x_{j,b}, F(k, x_{j,b})\}$

$k \leftarrow \mathcal{K}$

x^*

y^*

$\Pr\left[y^* = F(k, x^*)\right] > \text{negl}(\lambda)$

IHwUF
Adversary

Subset Sum
Adversary

$\{x_{j,b}, F(k, x_{j,b})\}$

$k \leftarrow \mathcal{K}$

IHwUF
Adversary

$\{x_{j,b}\}$

Subset Sum
Adversary

$\{x_{j,b}, F(k, x_{j,b})\}$

$k \leftarrow \mathcal{K}$

IHwUF
Adversary

$\{x_{j,b}\}$

Subset Sum
Adversary

$\{x_{j,b}, F(k, x_{j,b})\}$

x^*

$k \leftarrow \mathcal{K}$

IHwUF
Adversary

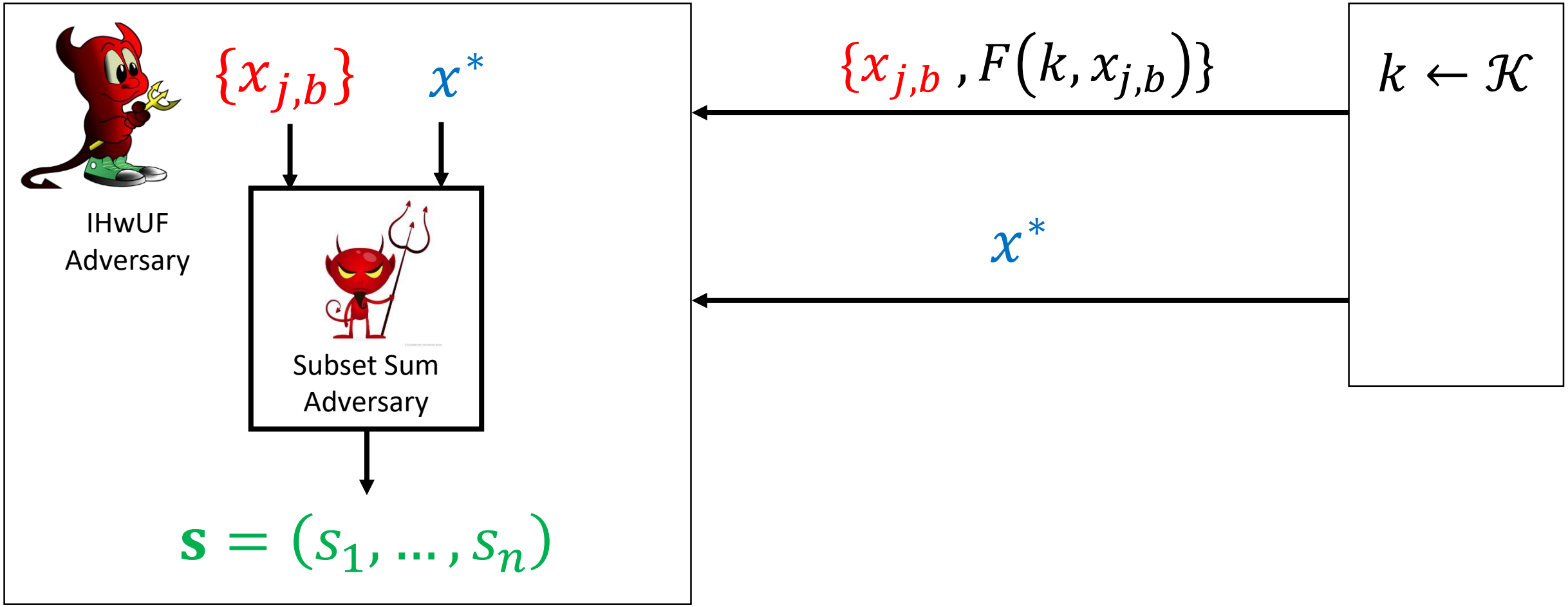
$\{x_{j,b}\}$ x^*

Subset Sum
Adversary

$\{x_{j,b}, F(k, x_{j,b})\}$

x^*

$k \leftarrow \mathcal{K}$


$\{x_{j,b}\}$
x^*
IHwUF
Adversary
Subset Sum
Adversary
$\mathbf{s} = (s_1, \ldots, s_n)$
$\{x_{j,b}, F(k, x_{j,b})\}$
x^*
$k \leftarrow \mathcal{K}$

IHwUF
Adversary

$\{x_{j,b}\}$ x^*

Subset Sum
Adversary

$\mathbf{s} = (s_1, \ldots, s_n)$

$\{x_{j,b}, F(k, x_{j,b})\}$

x^*

$y^* = \bigotimes_{j=1}^{n} F\left(k, x_{j,s_j}\right)$

$k \leftarrow \mathcal{K}$

IHwUF
Adversary

$\{x_{j,b}\}$ x^*

Subset Sum
Adversary

$\mathbf{s} = (s_1, \ldots, s_n)$

$\{x_{j,b}, F(k, x_{j,b})\}$

x^*

$y^* = F\left(k, \bigoplus_{j=1}^{n} x_{j,s_j}\right)$

$k \leftarrow \mathcal{K}$

Suppose

$$\Pr\left[x^* = \bigoplus_{j=1}^{n} x_{j,s_j}\right] > \text{negl}(\lambda)$$

IHwUF Adversary

$\{x_{j,b}\}$ x^*

Subset Sum Adversary

$\mathbf{s} = (s_1, \ldots, s_n)$

$\{x_{j,b}, F(k, x_{j,b})\}$

x^*

$y^* = F\left(k, \bigoplus_{j=1}^{n} x_{j,s_j}\right)$

$k \leftarrow \mathcal{K}$

Suppose

$$\Pr\left[x^* = \bigoplus_{j=1}^{n} x_{j,s_j}\right] > \text{negl}(\lambda)$$

IHwUF Adversary

$\{x_{j,b}\}$ x^*

Subset Sum Adversary

$\mathbf{s} = (s_1, \ldots, s_n)$

$\{x_{j,b}, F(k, x_{j,b})\}$

x^*

$y^* = F(k, x^*)$

$k \leftarrow \mathcal{K}$

Suppose

$$\Pr\left[x^* = \bigoplus_{j=1}^{n} x_{j,s_j}\right] > \text{negl}(\lambda)$$

→ Adversary against IHwUF $F: \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$

IHwUF Adversary

$\{x_{j,b}\}$ x^*

Subset Sum Adversary

$\mathbf{s} = (s_1, \ldots, s_n)$

$\{x_{j,b}, F(k, x_{j,b})\}$

$k \leftarrow \mathcal{K}$

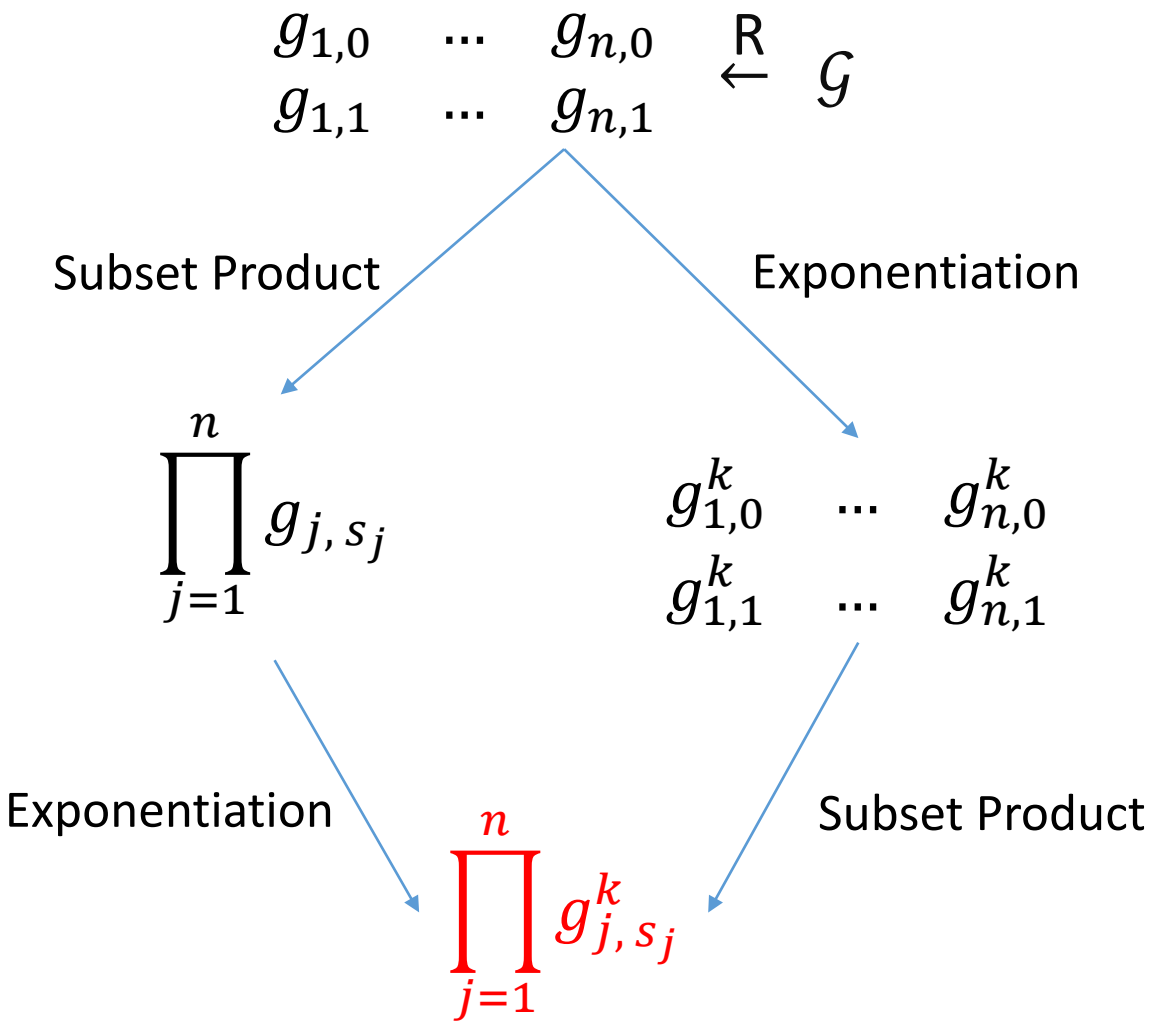
x^*

y^*

$\Pr\left[y^* = F(k, x^*)\right] > \text{negl}(\lambda)$

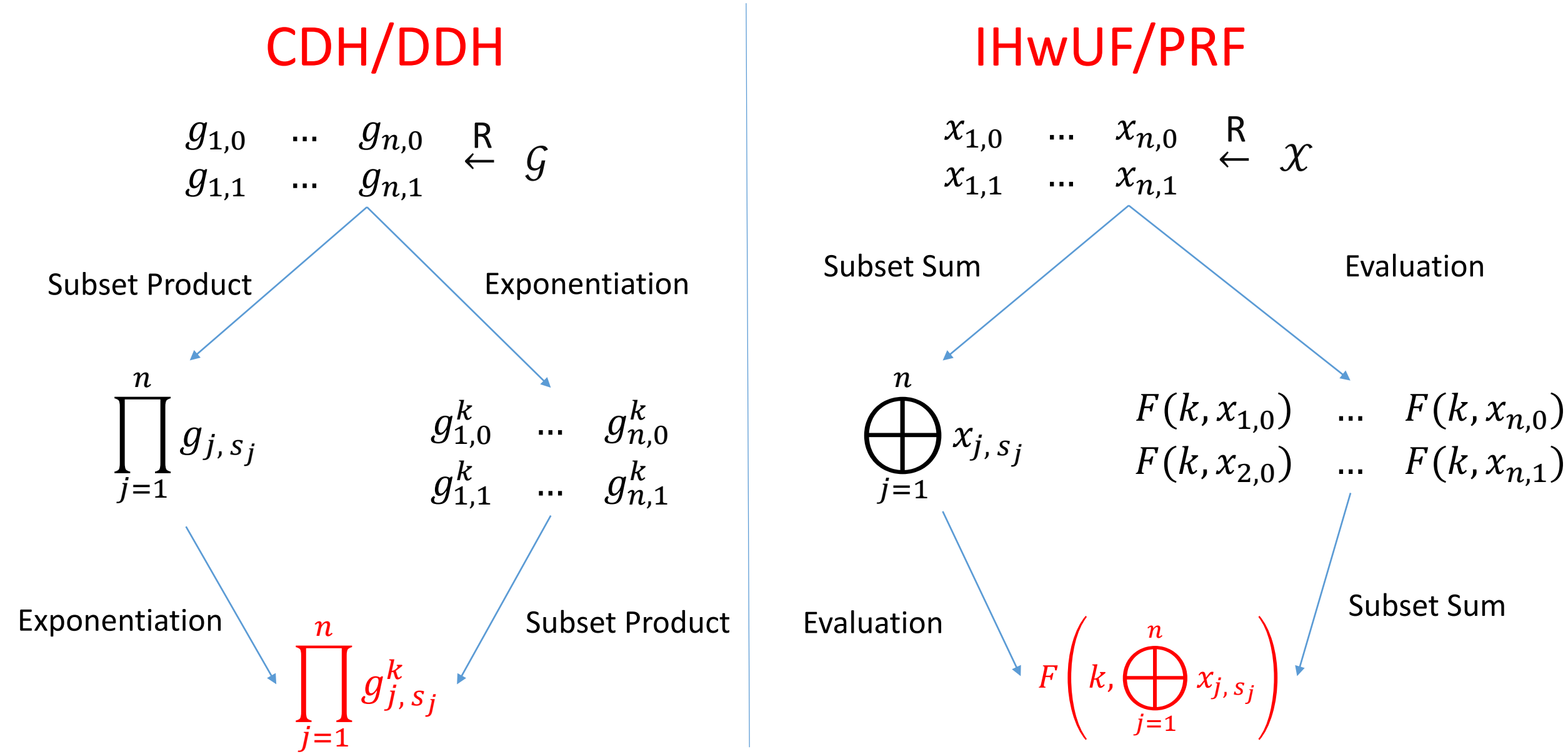
Abstracting a CDH/DDH-based protocol

CDH/DDH



IHwUF/PRF

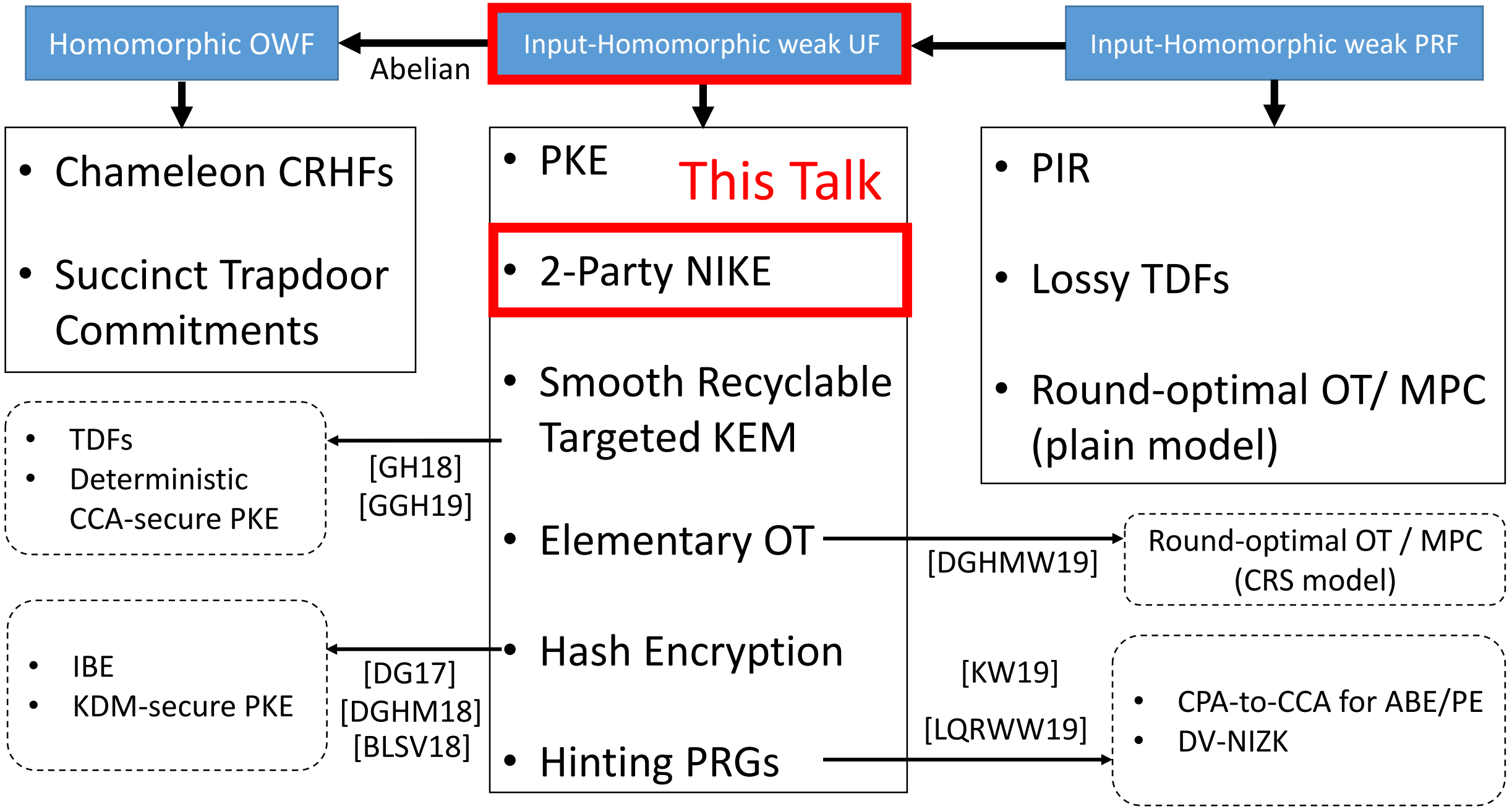
Abstracting a CDH/DDH-based protocol



Outline

- Our results
- An alternative approach to designing primitives
- A cryptoplexity hierarchy in Cryptomania
- Techniques
- **Summary and open questions**

All implications hold for bounded homomorphism



Open Questions

- More primitives from generic assumptions
  - NIZKs, VRFs, threshold signatures, ABE, PE?

- New (post-quantum) assumptions
  - Isogenies of elliptic curves?

- Black-box separations between generic primitives
  - HOWFs and IHwUFs?

Open Questions

- More primitives from generic assumptions
  - NIZKs, VRFs, threshold signatures, ABE, PE?

- New (post-quantum) assumptions
  - Isogenies of elliptic curves?

N. Alamati, L. De Feo, H. Montgomery, **S. Patranabis**.
Cryptographic Group Actions and Applications.
In ASIACRYPT 2020 (Conditionally accepted).

- Black-box separations between generic primitives
  - HOWFs and IHwUFs?

Thank you!

eprint.iacr.org/2019/108
eprint.iacr.org/2019/608
eprint.iacr.org/2020/606