Cryptographic Primitives with Hinting Property

Sikhar Patranabis (IBM Research, India)

Joint work with Navid Alamati (VISA Research)

IACR ASIACRYPT 2022

December 06, 2022

Hints in real life

What is a good password hint?

A hint could be anything from **a single word that reminds you of your password to a full-fledged sentence, a string of characters, or anything else that helps you jump-start your associative memory**. The one thing that should not be in your password hint is your actual password, obviously.

wikiHow to do anything... UPGRADE

Question

If I forget my password, should I make my password hint the same as my password?

Community Answer

No, it's a very bad idea. This will make it very easy for someone to hack into your computer.

Helpful 36 Not Helpful 5

Password hint: “what is the sound of one hand clapping?”

Hints in cryptography

Pseudorandom Generator (PRG)

Assumption: The distinguisher is given no additional information about the seed $\mathbf{s}$

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

$$\text{PRG}: \{0,1\}^n \rightarrow \{0,1\}^{n^2}$$

$y_1 \quad y_2 \quad y_3 \quad \cdots \quad y_{n-1} \quad y_n$	n output strings of length n bits each
$\approx_c$	(computationally indistinguishable)
$z_1 \quad z_2 \quad z_3 \quad \cdots \quad z_{n-1} \quad z_n$	n **random** strings of length n bits each

Hints in cryptography

Hinting PRG [KW19]

The distinguisher is given some additional information or **"hint"** about the seed $\mathbf{s}$

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

$\text{HPRG}: \{0,1\}^n \rightarrow \{0,1\}^{n^2}$

$y_1 \quad y_2 \quad y_3 \quad \ldots \quad y_{n-1} \quad y_n$ — n output strings of length n bits each

Swap (y_i, z_i) if $s_i = 1$

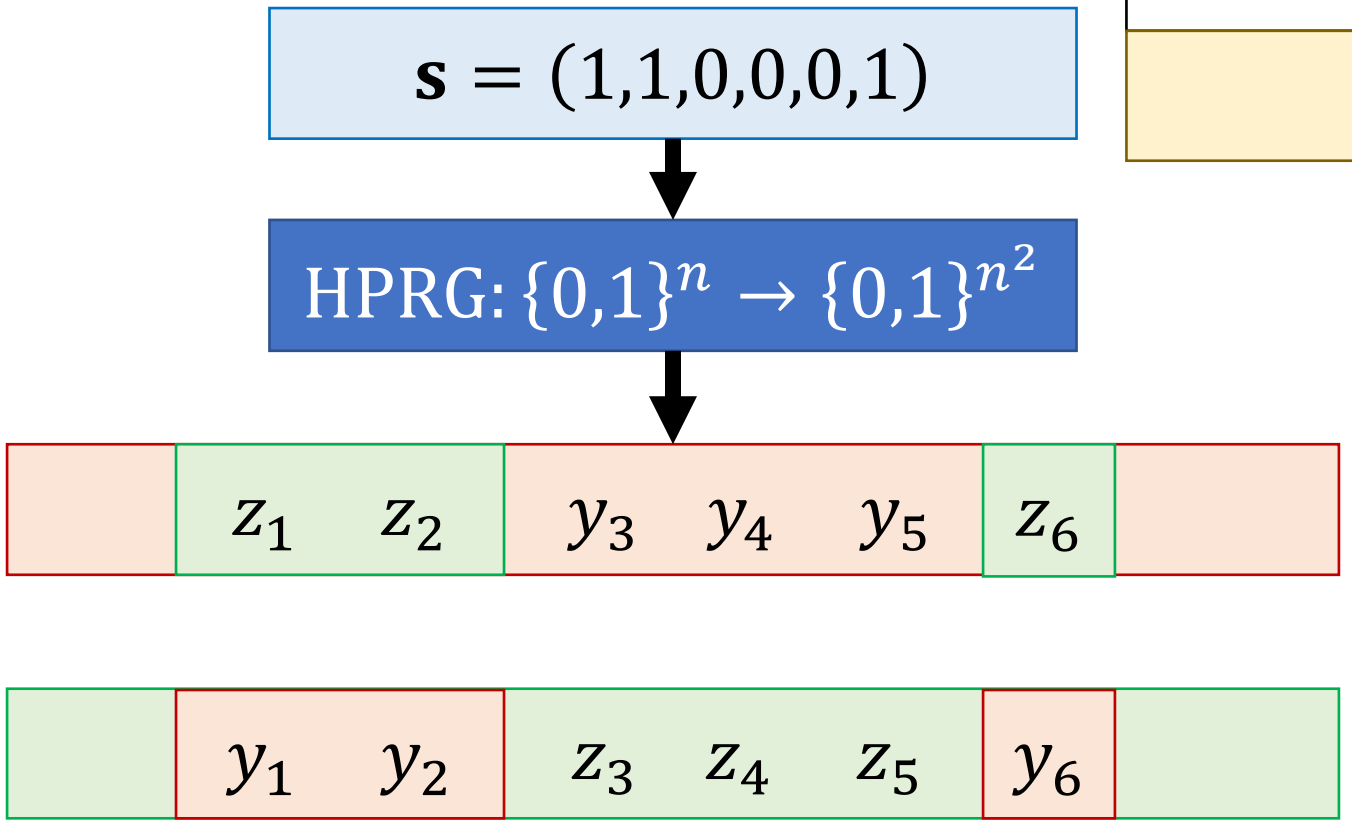
$z_1 \quad z_2 \quad z_3 \quad \ldots \quad z_{n-1} \quad z_n$ — n **random** strings of length n bits each

Hints in cryptography

Hinting PRG [KW19]

The distinguisher is given some additional information or **"hint"** about the seed $\mathbf{s}$

A toy example with $n = 6$



Hints in cryptography

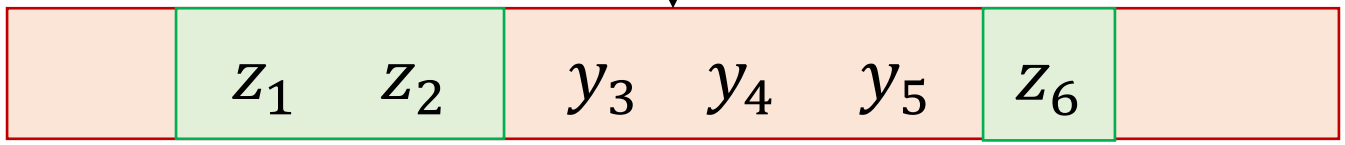
Hinting PRG [KW19]

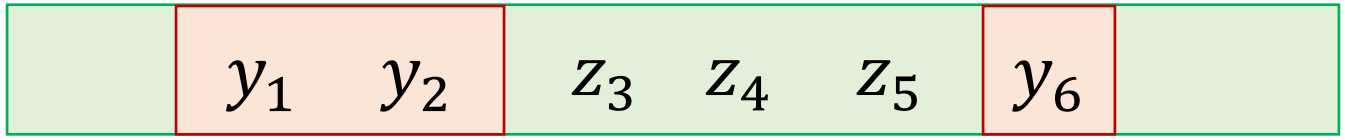
The distinguisher is given some additional information or **"hint"** about the seed **s**

A toy example with $n = 6$

$\mathbf{s} = (1,1,0,0,0,1)$

$\text{HPRG}: \{0,1\}^n \to \{0,1\}^{n^2}$





Embeds information about the seed **s**

But remains pseudorandom
(computationally indistinguishable from a $2 \times n$ matrix of random n-bit strings)

Hints in cryptography

Hinting PRG [KW19]

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

$\mathrm{HPRG}: \{0,1\}^n \to \{0,1\}^{n^2}$

$y_1 \quad y_2 \quad y_3 \quad \cdots \quad y_{n-1} \quad y_n$

$z_1 \quad z_2 \quad z_3 \quad \cdots \quad z_{n-1} \quad z_n$

The Hinting PRG game

Let $\mathrm{HPRG}(\mathbf{s} = (s_1, \ldots, s_n)) = (y_1, \ldots, y_n)$

$\mathbf{Z} = [z_{j,b}]_{b \in \{0,1\}, j \in [n]} \in (\{0,1\}^n)^{2 \times n}$

$z_{j,s_j} = y_j\,, \qquad z_{j,1-s_j} = z_j \leftarrow \{0,1\}^n$

$\mathbf{Z} \approx_c \mathbf{U} \leftarrow (\{0,1\}^n)^{2 \times n}$

$\mathbf{Z}$ is pseudorandom despite encoding additional "hints" about $\mathbf{s}$

Why study Hinting PRGs?

Cryptographic “booster” [KW19]

- Generic transformation from CPA to CCA security for public-key encryption (PKE)
- Transformation also works for attribute-based encryption (ABE) and predicate encryption (PE)

A myriad of other cryptographic applications

Key ingredient in new constructions of:

- Trapdoor one-way functions [KMT19,GHMO21]
- Designated-verifier NIZKs [LQRWW19]
- Black-box non-interactive non-malleable commitments [GKLW21]
- CCA-compatible public-key infrastructure [KW21]

Hinting Property vs Circular Security

Can view hinting property as a “deterministic” form of symmetric-key circular security

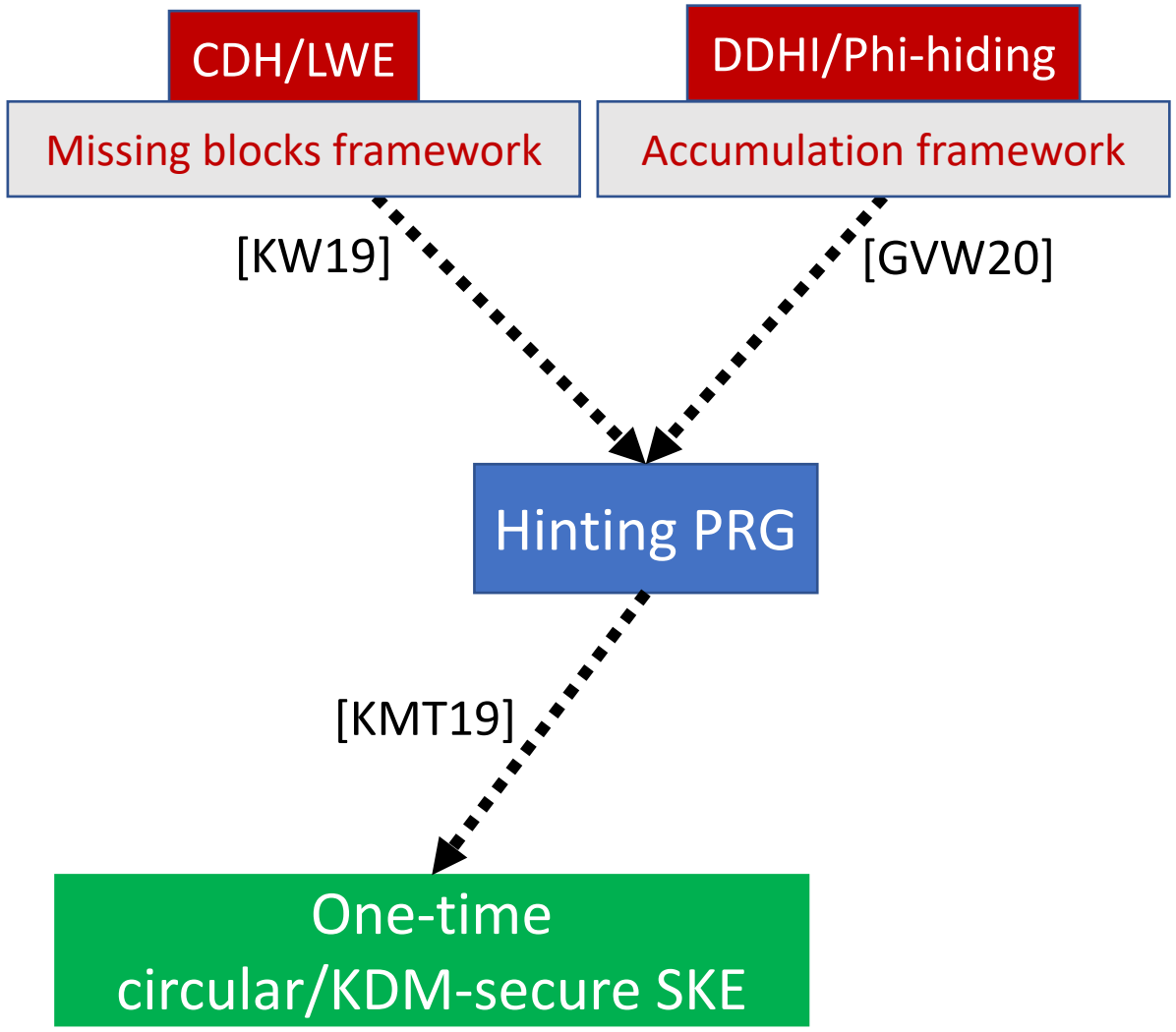
Hinting PRG	• Retains pseudorandomness of (deterministic) output even given some “hinting” information about the secret seed
Circular-Secure Symmetric-Key Encryption	• Retains semantic security of (randomized) encryption even when encrypting the bits of the secret key

Hinting Property vs Circular Security

Can view hinting property as a “deterministic” form of symmetric-key circular security

Hinting PRG	• Retains pseudorandomness of (deterministic) output even given some “hinting” information about the secret seed • Construction and proof techniques are complicated and inherently rooted in algebraic/ “public-key style” mathematical assumptions [KW19, GVW20] • Cryptographic complexity unclear (inherently requires public-key techniques?)
Circular-Secure Symmetric-Key Encryption	• Retains semantic security of (randomized) encryption even when encrypting the bits of the secret key • Simple construction and proof techniques from certain standard decisional assumptions (e.g., DDH [BHHO08]) • Weaker than public-key encryption (realizable from random oracles [BRS03])

Hinting PRGs: Current landscape vs what we ask



- **Simpler constructions and proofs** from standard decisional assumptions (e.g., DDH)?
- Realizations from a **wider class of assumptions** (e.g., isogeny-based assumptions)?

- Can we **extend** the hinting property to **other** symmetric-key primitives?
- What are the applications of such extensions? Can we realize them from standard assumptions?

- **Cryptographic complexity** of hinting PRGs?
- Are mathematically structured “public-key-style” assumptions **necessary**?

Our Contributions

Bold arrows denote results/implications from our paper

- New extensions of the hinting property to **pseudorandom functions (PRFs)**
  - PRF → Hinting PRF
  - weak PRF* → Hinting weak PRF
- New security definitions:
  - (Weak) pseudorandomness in the presence of **hints about the secret key**
  - **Multi-evaluation** security (as opposed to single-evaluation security for hinting PRG)

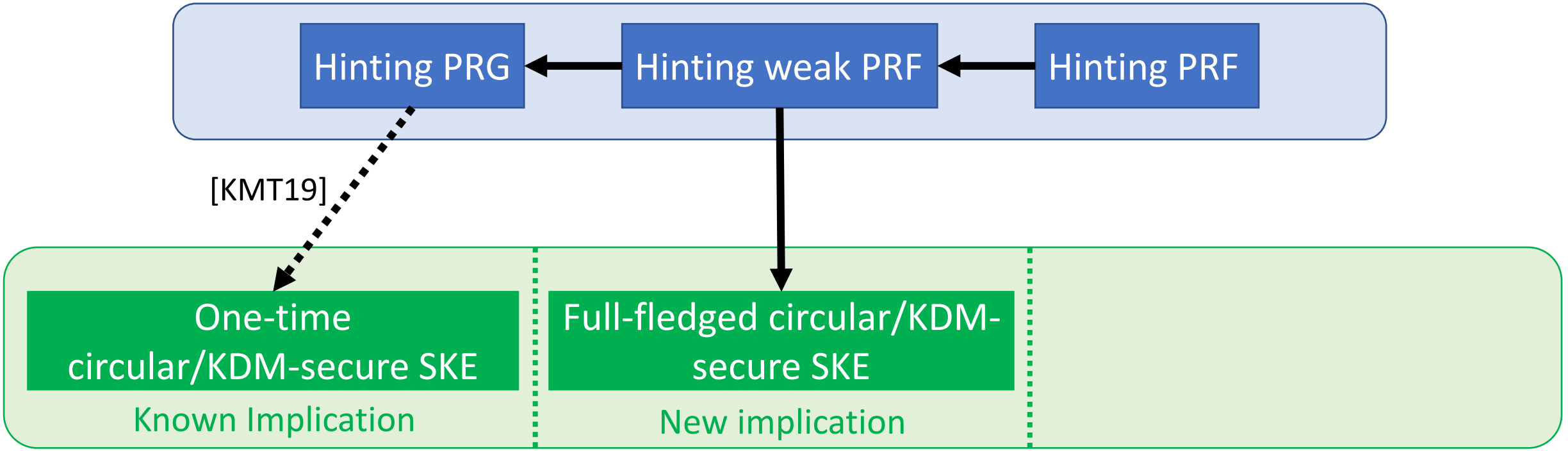
Cryptographic primitives with hinting property

* A weak PRF (informally) guarantees pseudorandomness on uniformly randomly sampled inputs

Our Contributions

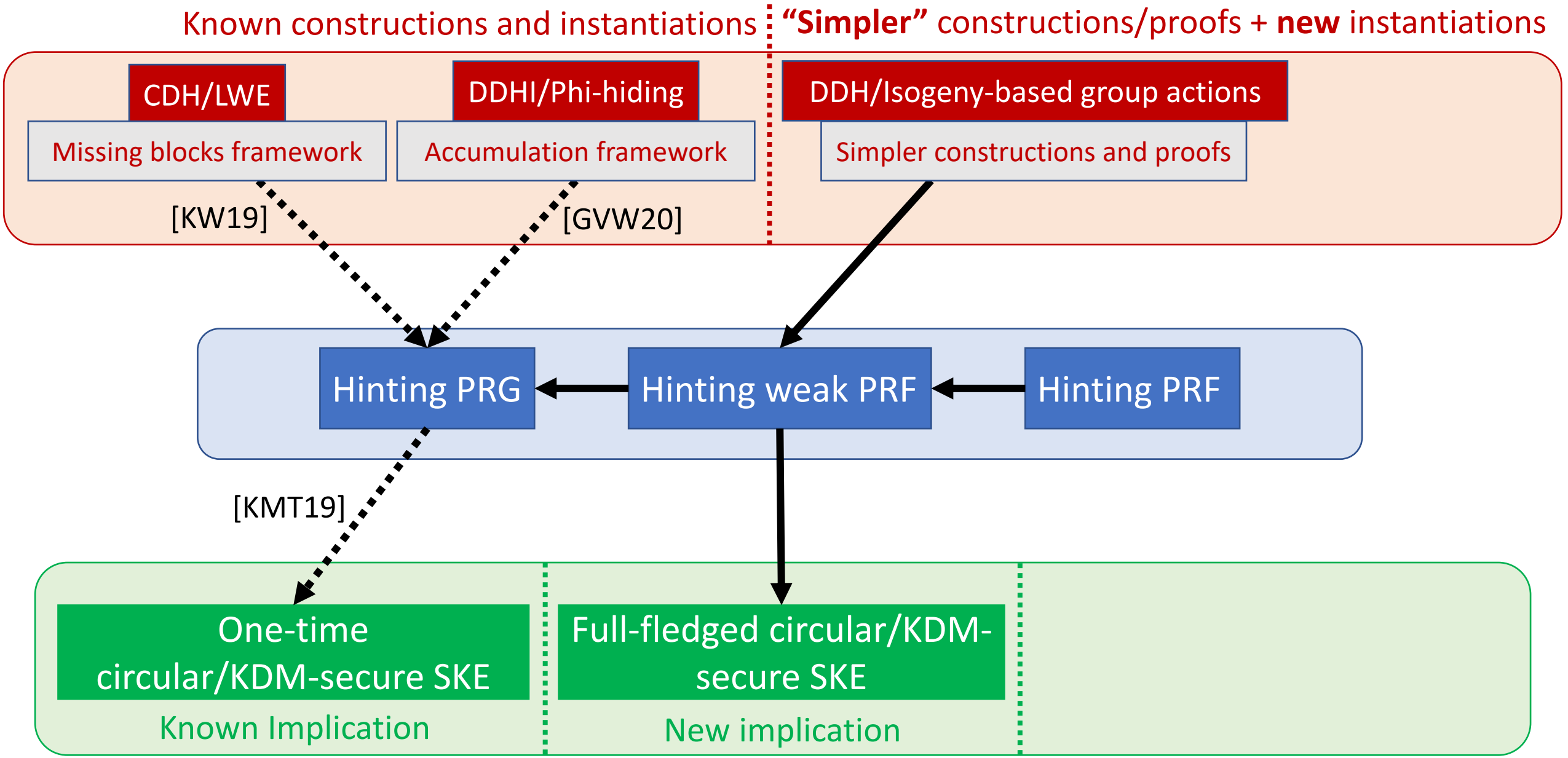
Bold arrows denote results/implications from our paper

- New **stronger** implications of the hinting property:
  - A hinting weak PRF implies (in a black-box manner) a full-fledged circular-secure symmetric-key encryption (SKE) scheme
    - Circular security guarantee holds with respect to multiple encryptions of the secret key
  - Non-black-box amplification to full-fledged KDM-secure SKE [App14]



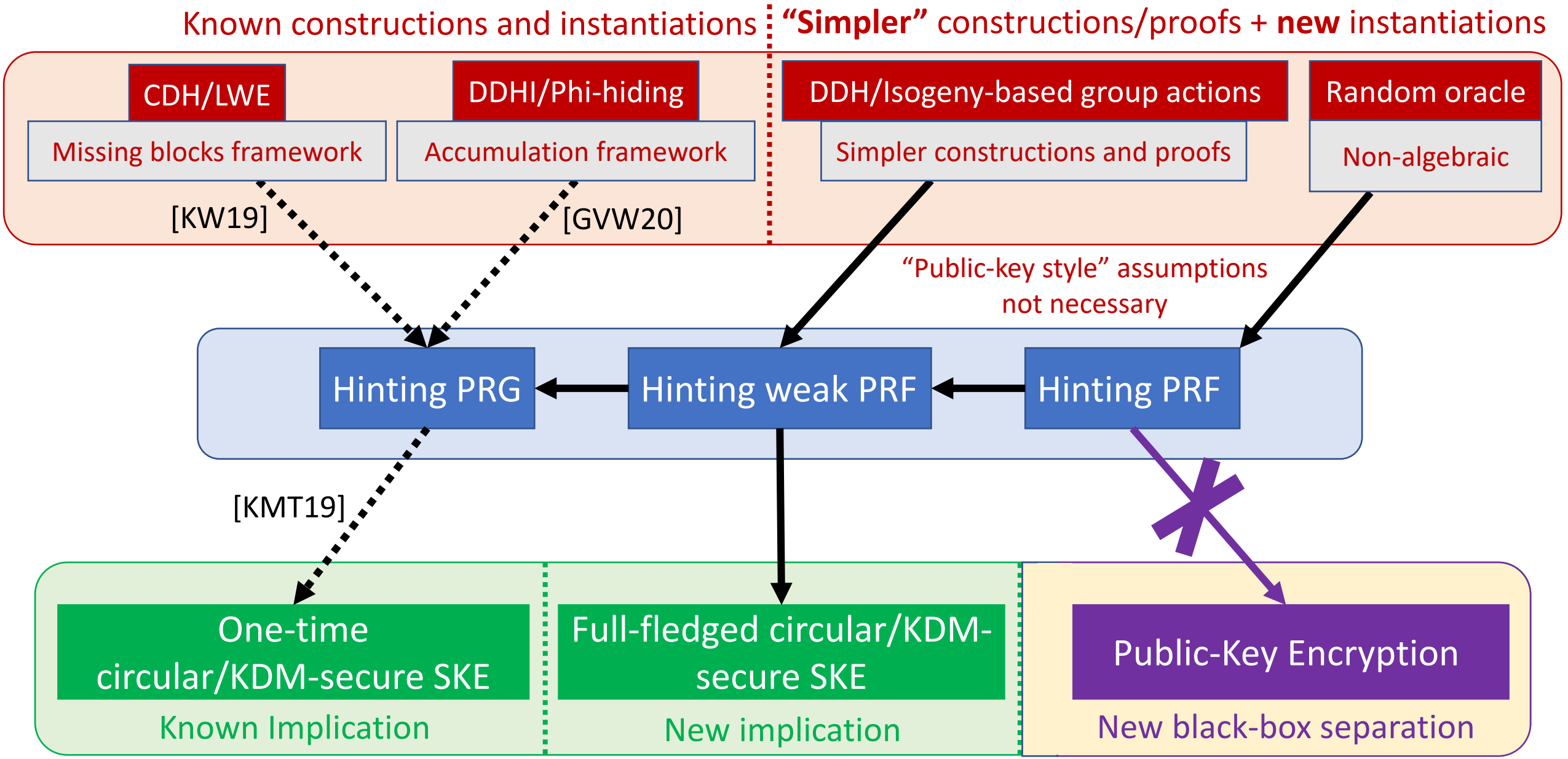
Our Contributions

Bold arrows denote results/implications from our paper



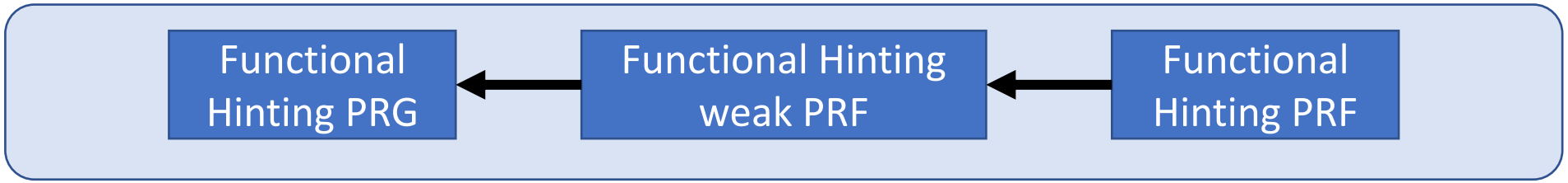
Our Contributions

Bold arrows denote results/implications from our paper



Our Contributions: Functional Hinting Property

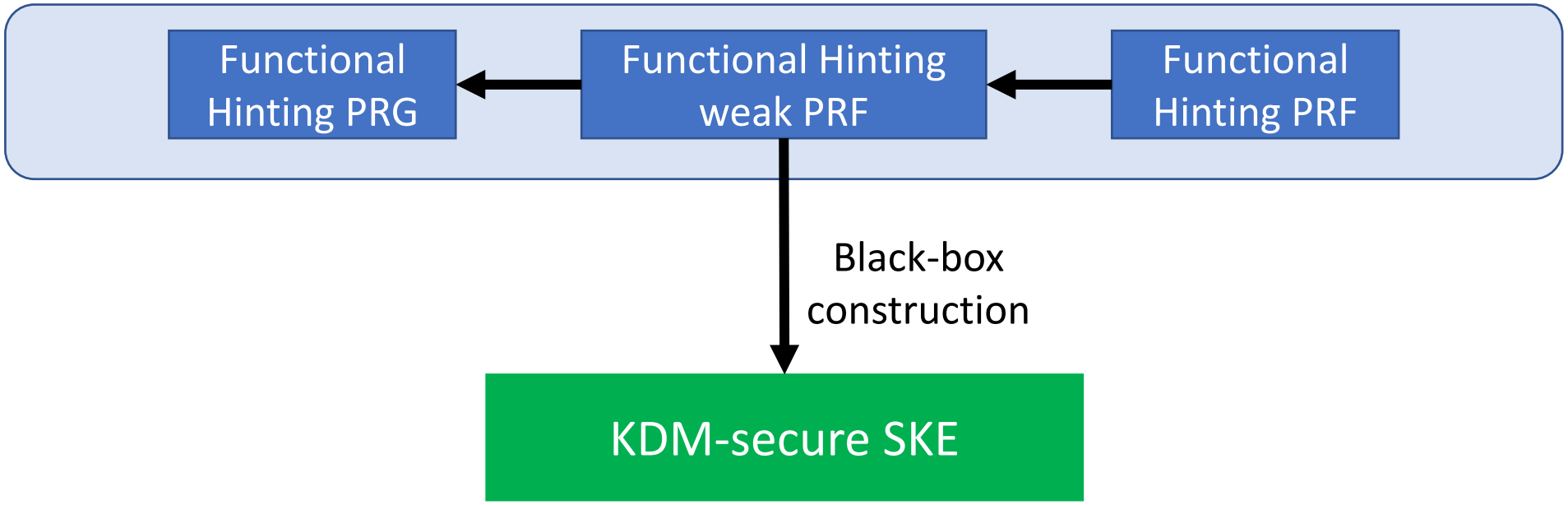
- New strengthening of the hinting property to **functional hinting property**
  - Functional hinting PRG: hints about each bit of **some function** of the seed
  - Functional hinting (weak) PRF: hints about each bit of **some function** of the secret key
  - The function may be chosen **adversarially** from a fixed function family
- Example:
  - Seed $\mathbf{s} = (s_1, \ldots, s_n) \in \{0,1\}^n$
  - Hints about each bit of the **quadratic** function $f(\mathbf{s}) = \{s_i . s_j\}_{i,j\in[n]} \in \{0,1\}^{n^2}$



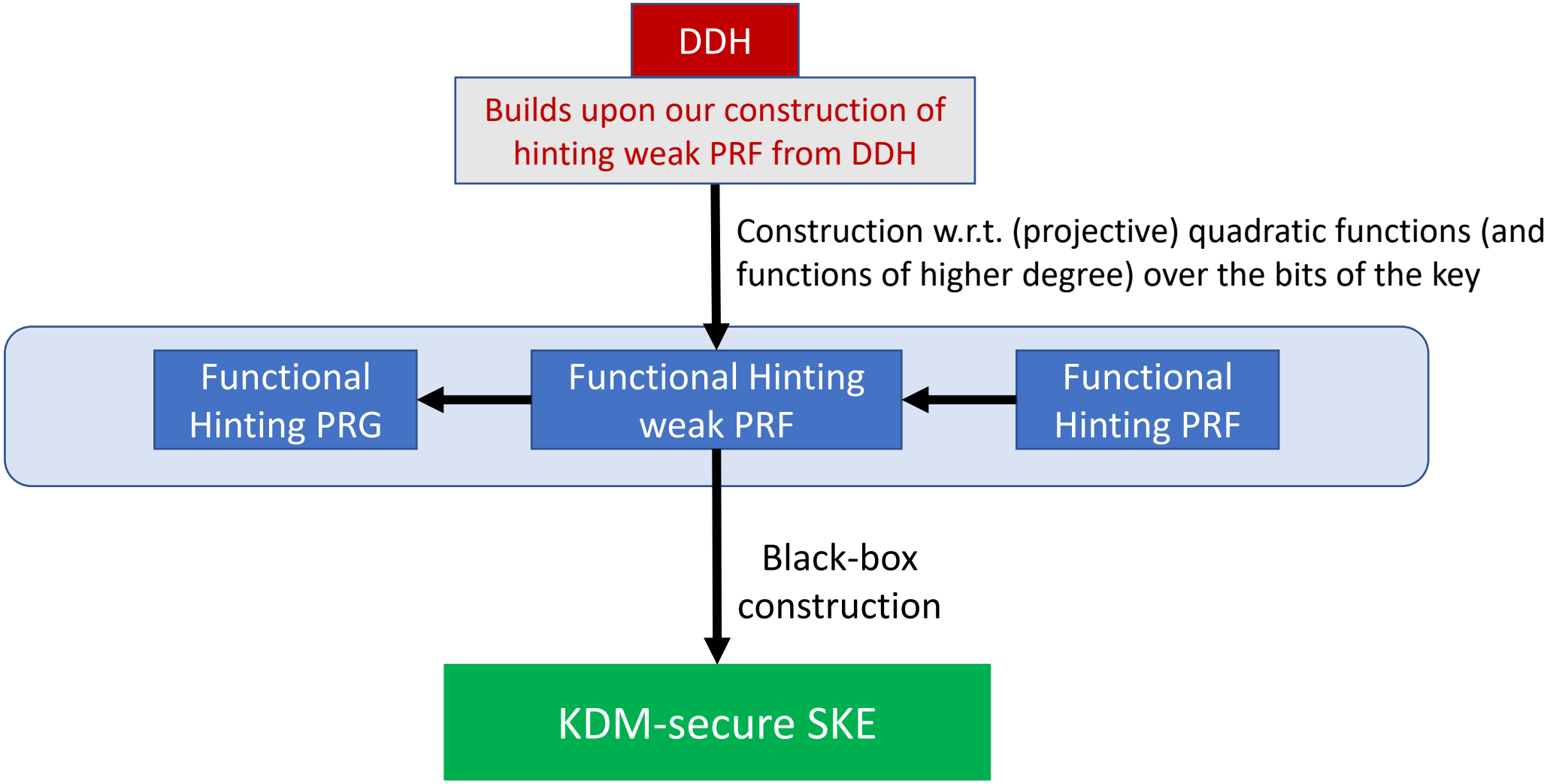
Cryptographic primitives with **functional** hinting property

Our Contributions: Functional Hinting Property

- Even stronger implications of the functional hinting property:
  - A functional hinting weak PRF w.r.t. some function family $\mathcal{F}$ implies (in a black-box manner) a KDM-secure symmetric-key encryption (SKE) w.r.t. the same function family $\mathcal{F}$
  - New approach for achieving KDM-security in a black-box manner w.r.t. Boolean function families
  - Prior approaches [BGK11,KMT19] are designed specifically for arithmetic function families and inherently require some algebraic structure on the key space



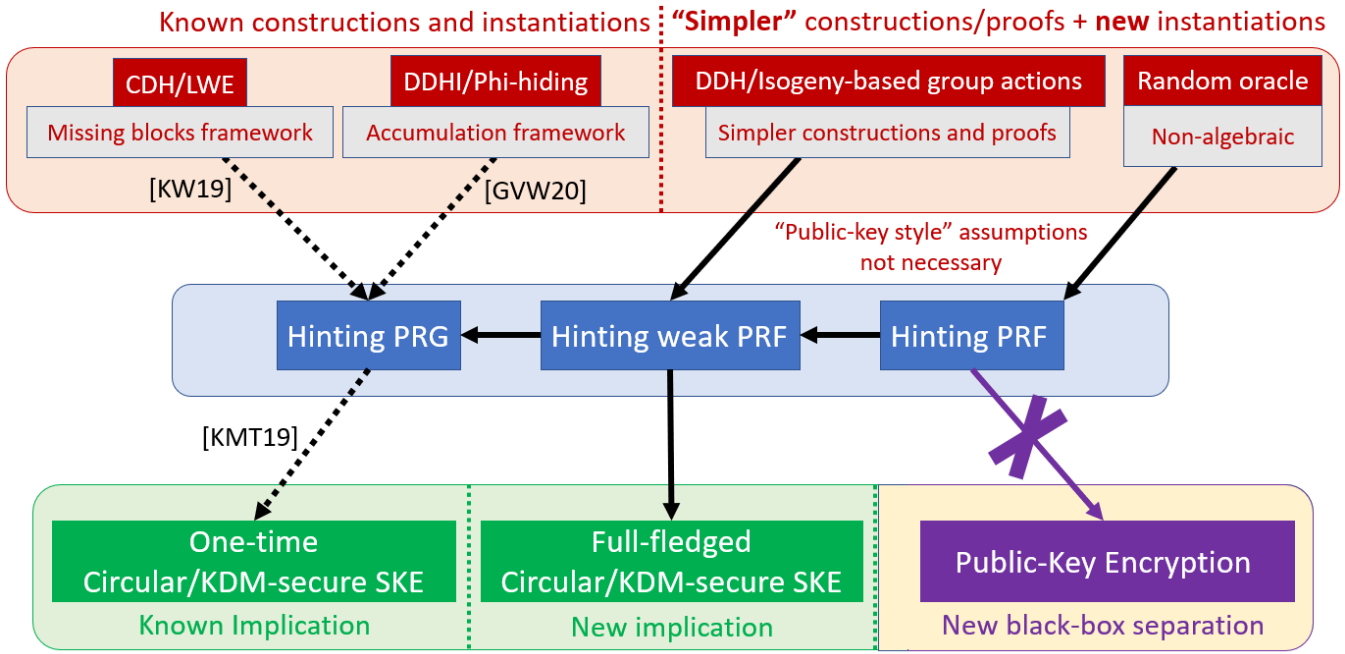
Our Contributions: Functional Hinting Property



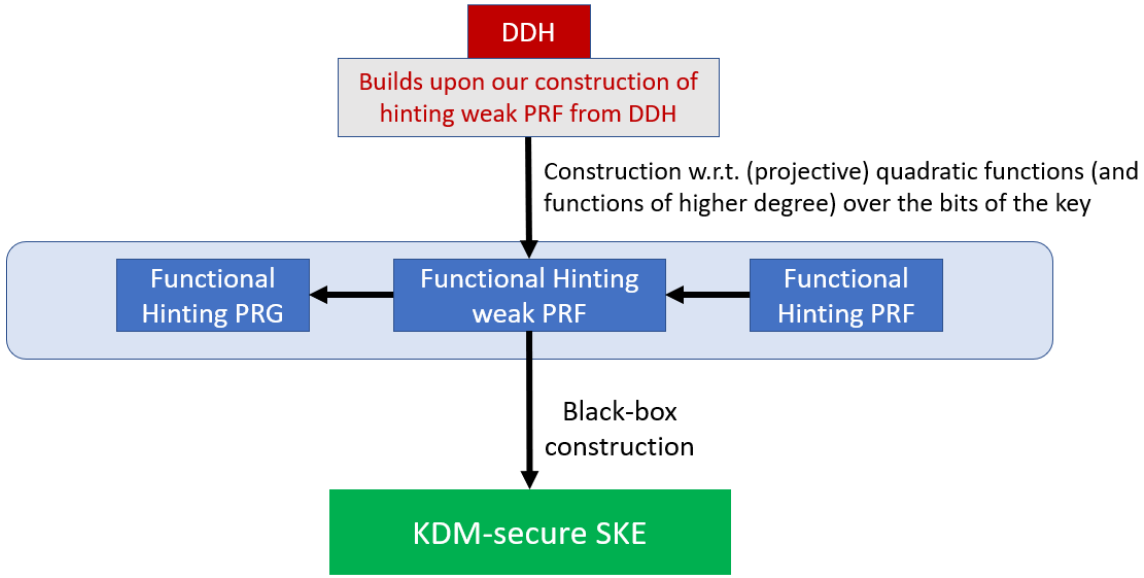
Our Contributions: Summary

Bold arrows denote results/implications from our paper

Primitives with hinting property



Primitives with functional hinting property



Talk Outline

- Simple Hinting PRG from DDH
- Hinting PRG from cryptographic group actions (brief overview)
- Hinting weak PRF (brief overview)
- Summary and open questions

Talk Outline

- Simple Hinting PRG from DDH
- Hinting PRG from cryptographic group actions (brief overview)
- Hinting weak PRF (brief overview)
- Summary and open questions

Simple Hinting PRG from DDH

- Let G be a DDH-hard group of prime order q with generator g, and let $n > \log|G| + \omega(\log \lambda)$
- Let $\mathrm{M} \leftarrow \mathbb{Z}_q^{n \times n}$ be a matrix with entries $m_{i,j}$ uniformly sampled from $\mathbb{Z}_q$
- Let $[\mathrm{M}]$ denote the matrix of group elements $g^{\mathrm{M}} \in G^{n \times n}$ (exponentiation applied component-wise)
- Define the function $H_{[\mathrm{M}]}: \{0,1\}^n \rightarrow G^n$ as:

$$H_{[\mathrm{M}]}(\mathrm{s} \in \{0,1\}^n) = [\mathrm{Ms}]$$

Simple Hinting PRG from DDH

- Let G be a DDH-hard group of prime order q with generator g, and let $n > \log|G| + \omega(\log\lambda)$
- Let $\mathrm{M} \leftarrow \mathbb{Z}_q^{n\times n}$ be a matrix with entries $m_{i,j}$ uniformly sampled from $\mathbb{Z}_q$
- Let $[\mathrm{M}]$ denote the matrix of group elements $g^{\mathrm{M}} \in G^{n\times n}$ (exponentiation applied component-wise)
- Define the function $H_{[\mathrm{M}]}: \{0,1\}^n \rightarrow G^n$ as:

$$H_{[\mathrm{M}]}(\mathrm{s} \in \{0,1\}^n) = [\mathrm{Ms}]$$

[PW08,FGK+10,AMP19]

H is a PRG assuming that G is DDH-hard

(Hint: apply the leftover hash lemma)

Simple Hinting PRG from DDH

- Let G be a DDH-hard group of prime order q with generator g, and let $n > \log|G| + \omega(\log\lambda)$
- Let $\mathrm{M} \leftarrow \mathbb{Z}_q^{n\times n}$ be a matrix with entries $m_{i,j}$ uniformly sampled from $\mathbb{Z}_q$
- Let $[\mathrm{M}]$ denote the matrix of group elements $g^{\mathrm{M}} \in G^{n\times n}$ (exponentiation applied component-wise)
- Define the function $H_{[\mathrm{M}]}: \{0,1\}^n \rightarrow G^n$ as:

$$H_{[\mathrm{M}]}(\mathrm{s} \in \{0,1\}^n) = [\mathrm{Ms}]$$

Our Result

H is a **hinting** PRG assuming that G is DDH-hard

(Hint: see the next few slides)

Simple Hinting PRG from DDH

$$H_{[\mathrm{M}]}(\mathrm{s} \in \{0,1\}^n) = [\mathrm{Ms}]$$

Our Result

H is a **hinting** PRG assuming that G is DDH-hard

Lemma

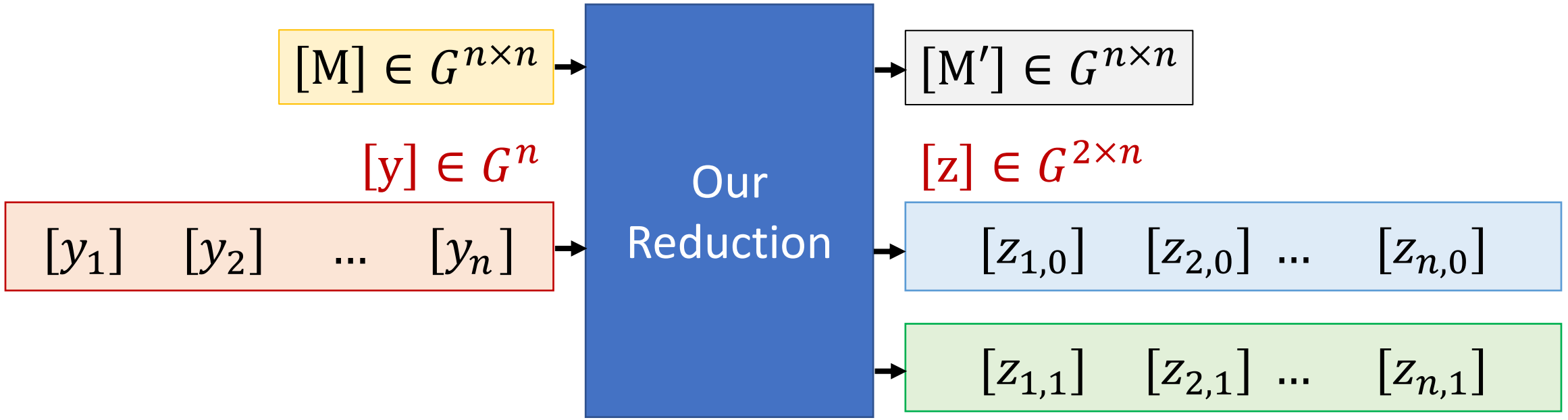
H is a **hinting** PRG assuming that it is a PRG

Simple Hinting PRG from DDH

$$H_{[\mathrm{M}]}(\mathrm{s} \in \{0,1\}^n) = [\mathrm{Ms}]$$

Lemma

H is a **hinting** PRG assuming that it is a PRG

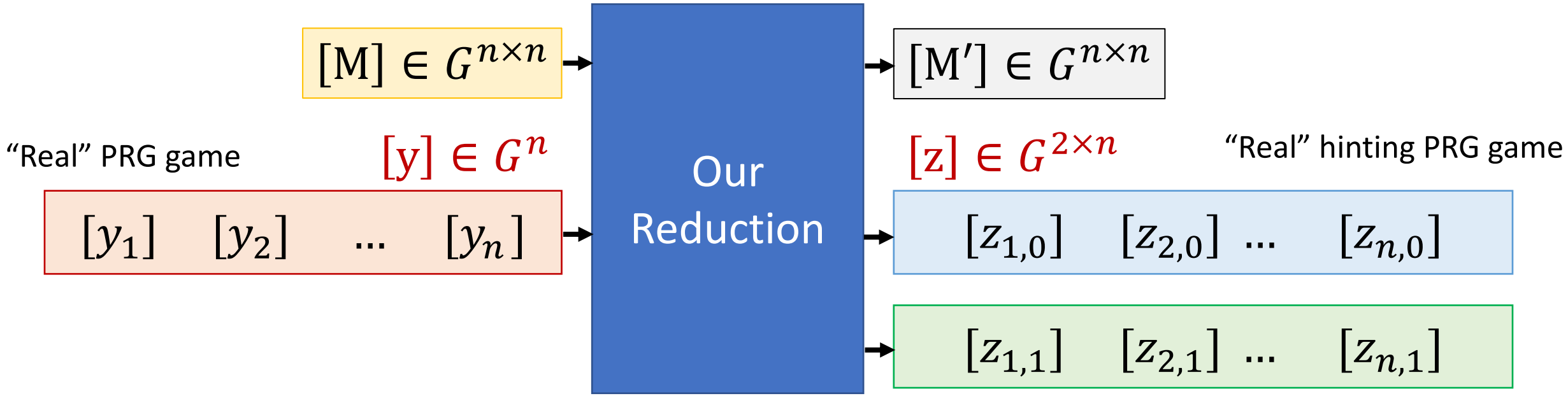


Simple Hinting PRG from DDH

$$H_{[\mathrm{M}]}(\mathrm{s} \in \{0,1\}^n) = [\mathrm{Ms}]$$

Lemma

H is a **hinting** PRG assuming that it is a PRG

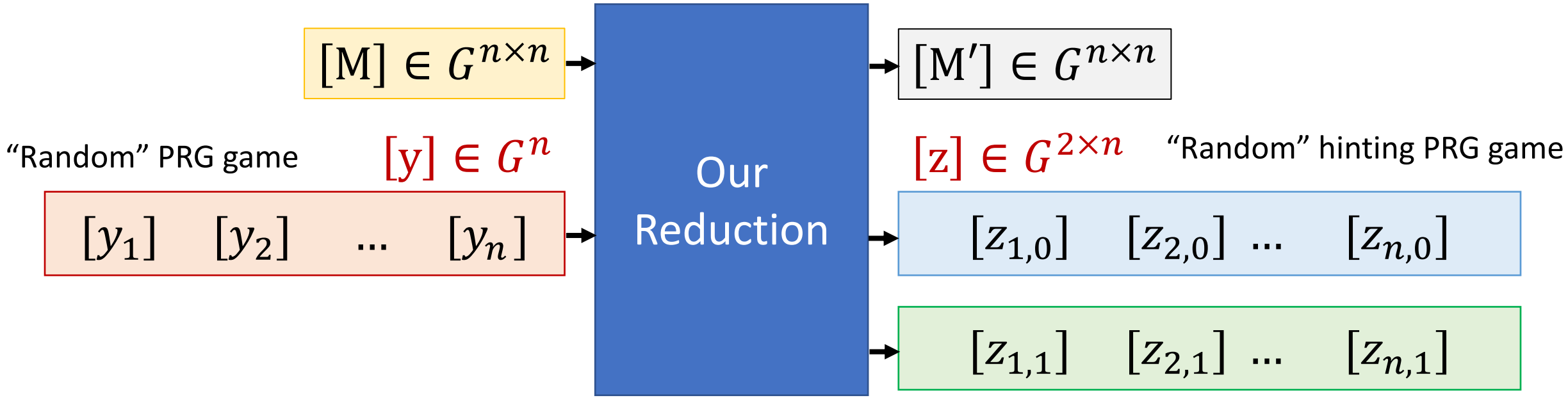


Simple Hinting PRG from DDH

$$H_{[\mathrm{M}]}(\mathrm{s} \in \{0,1\}^n) = [\mathrm{Ms}]$$

Lemma

H is a **hinting** PRG assuming that it is a PRG

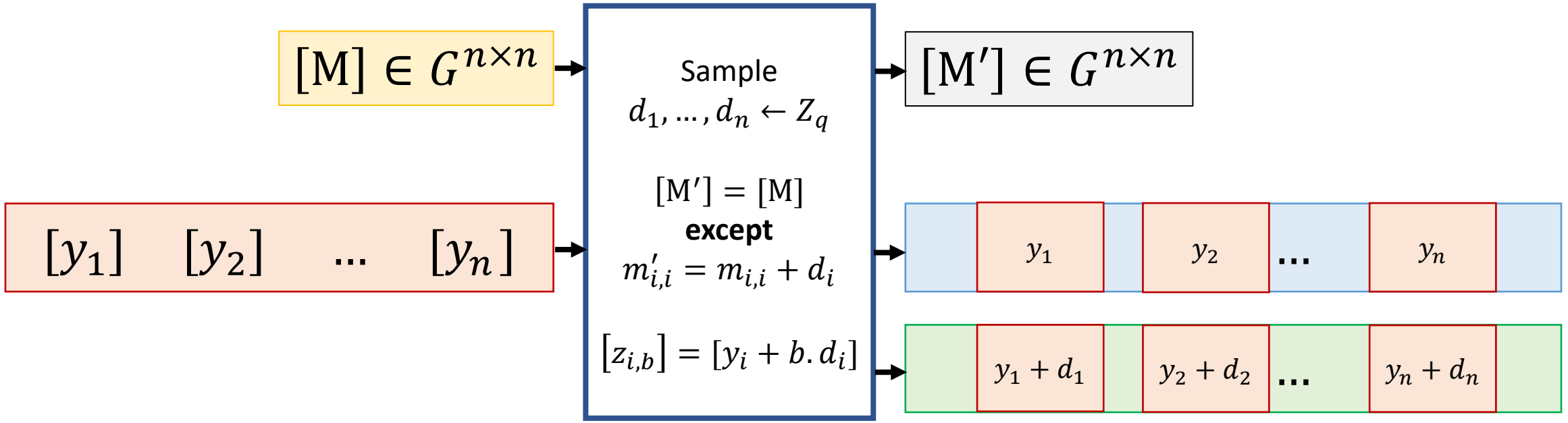


Simple Hinting PRG from DDH

$$H_{[\mathrm{M}]}(\mathrm{s} \in \{0,1\}^n) = [\mathrm{Ms}]$$

Lemma

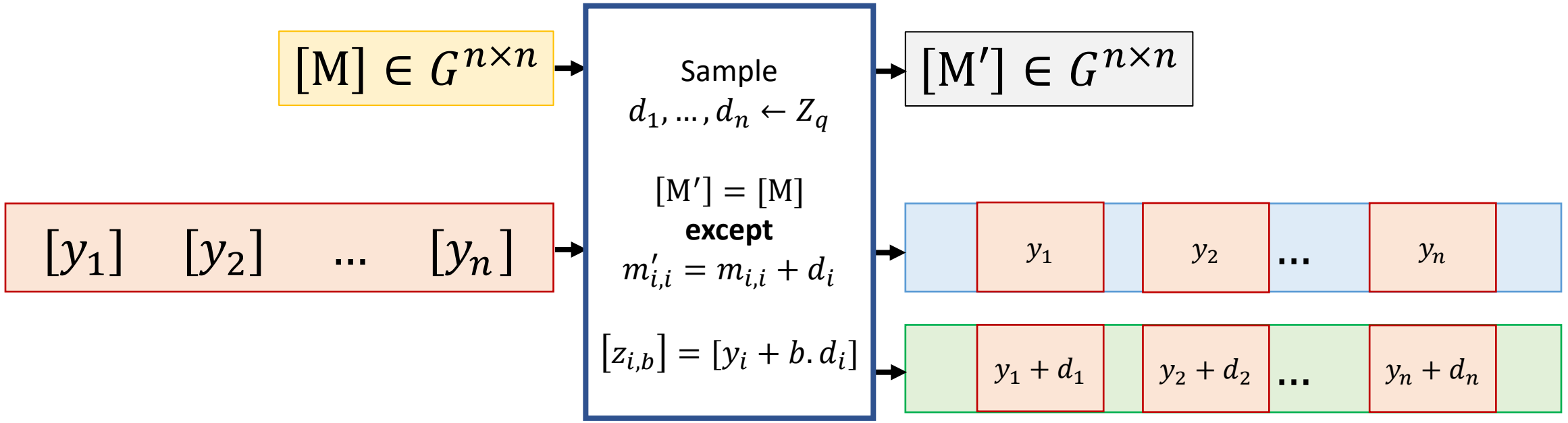
H is a **hinting** PRG assuming that it is a PRG



Simple Hinting PRG from DDH

$[y_i]$-s are distributed as in the "real" PRG game w.r.t. the PRG parameter [M]

- $y_i = \sum_{j\in[n]} m_{i,j}s_j, \quad z_{i,0} = y_i, \quad z_{i,1} = y_i + d_i$

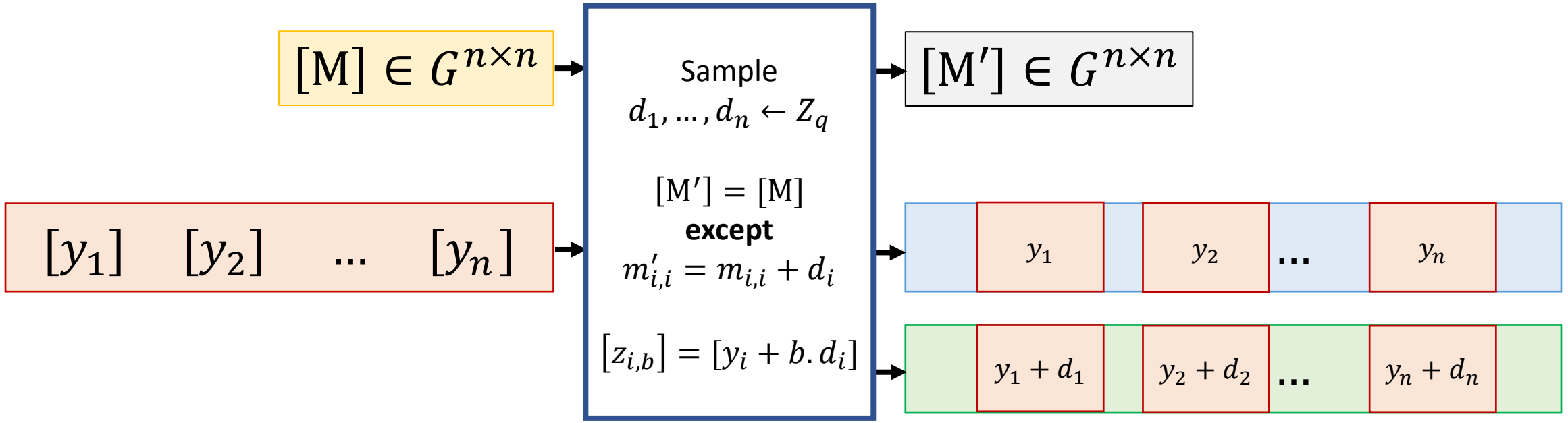


Simple Hinting PRG from DDH

$[y_i]$-s are distributed as in the "real" PRG game w.r.t. the PRG parameter [M]

- $y_i = \sum_{j\in[n]} m_{i,j}s_j, \quad z_{i,0} = y_i, \quad z_{i,1} = y_i + d_i$
- If $s_i = 0$, $z_{i,0} = \sum_{j\in[n]} m_{i,j}s_j = \sum_{j\in[n]} m'_{i,j}s_j$,

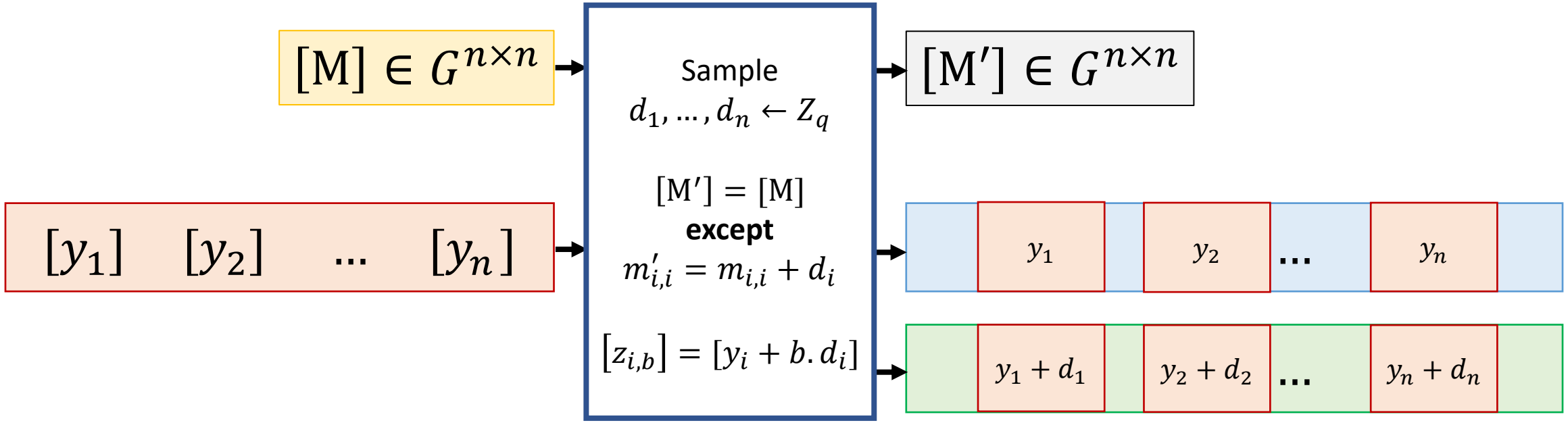
$z_{i,1}$ is distributed uniformly randomly in Z_q



Simple Hinting PRG from DDH

$[y_i]$-s are distributed as in the "real" PRG game w.r.t. the PRG parameter [M]

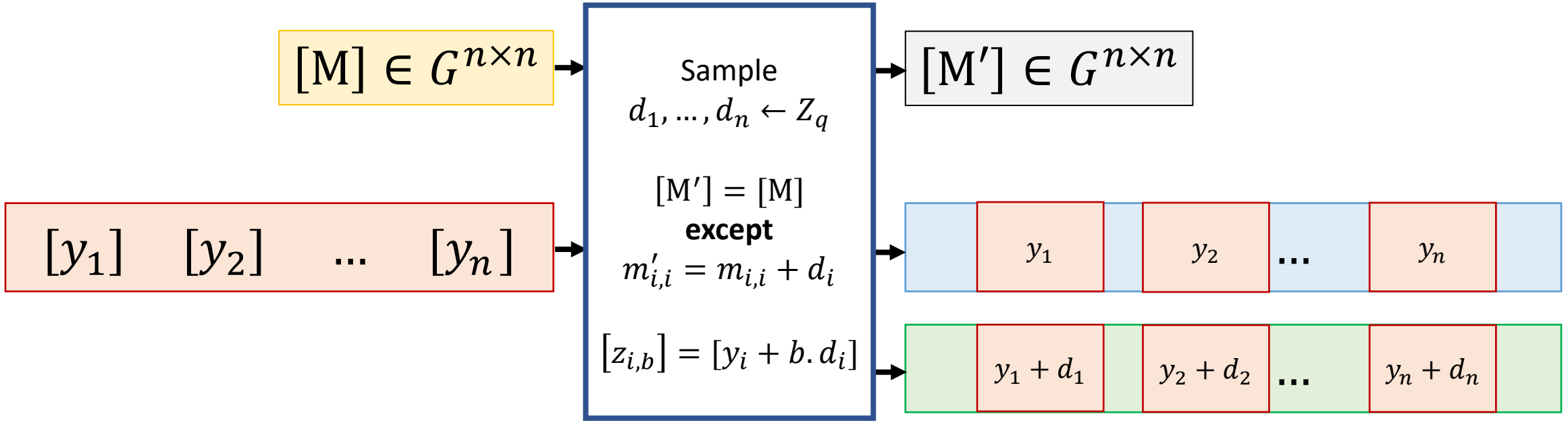
- $y_i = \sum_{j\in[n]} m_{i,j}s_j, \quad z_{i,0} = y_i, \quad z_{i,1} = y_i + d_i$
- If $s_i = 0$, $z_{i,0} = \sum_{j\in[n]} m_{i,j}s_j = \sum_{j\in[n]} m'_{i,j}s_j$, $z_{i,1}$ is distributed uniformly randomly in Z_q
- If $s_i = 1$, $z_{i,1} = \sum_{j\in[n]} m_{i,j}s_j + d_i = \sum_{j\in[n]} m'_{i,j}s_j$, $z_{i,0}$ is distributed uniformly randomly in Z_q



Simple Hinting PRG from DDH

$[y_i]$-s are distributed as in the "real" PRG game w.r.t. the PRG parameter [M] → $[z_{i,b}]$-s are distributed as in the "real" hinting PRG game w.r.t. the PRG parameter [M′]

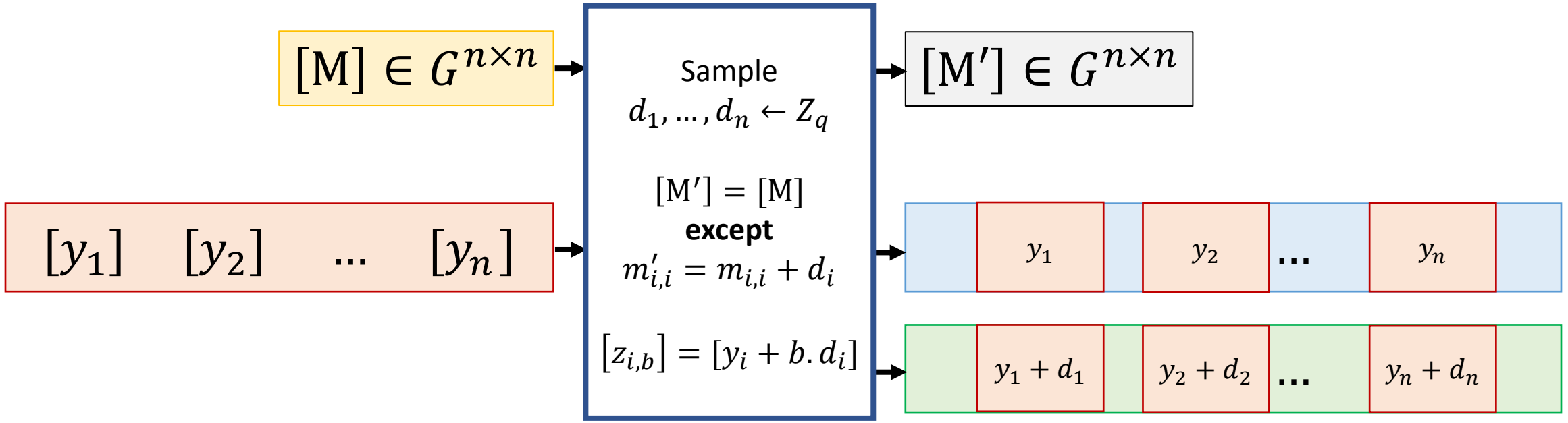
- $y_i = \sum_{j\in[n]} m_{i,j}s_j, \quad z_{i,0} = y_i, \quad z_{i,1} = y_i + d_i$
- If $s_i = 0$, $z_{i,0} = \sum_{j\in[n]} m_{i,j}s_j = \sum_{j\in[n]} m'_{i,j}s_j$, $z_{i,1}$ is distributed uniformly randomly in Z_q
- If $s_i = 1$, $z_{i,1} = \sum_{j\in[n]} m_{i,j}s_j + d_i = \sum_{j\in[n]} m'_{i,j}s_j$, $z_{i,0}$ is distributed uniformly randomly in Z_q



Simple Hinting PRG from DDH

$[y_i]$-s are distributed as in the "random" PRG game w.r.t. the PRG parameter [M] → $[z_{i,b}]$-s are distributed as in the "random" hinting PRG game w.r.t. the PRG parameter [M′]

- y_i is distributed uniformly randomly in Z_q, $z_{i,0} = y_i$, $z_{i,1} = y_i + d_i$
- Both $z_{i,0}$ and $z_{i,1}$ are distributed uniformly randomly in Z_q



Talk Outline

- Simple Hinting PRG from DDH
- Hinting PRG from cryptographic group actions (brief overview)
- Hinting weak PRF (brief overview)
- Summary and open questions

Hinting PRG from cryptographic group actions (brief overview)

Our simple approach for constructing hinting PRGs from DDH readily generalizes to cryptographic group actions (commutative and regular group actions)

Hinting PRG from cryptographic group actions (brief overview)

Our simple approach for constructing hinting PRGs from DDH readily generalizes to cryptographic group actions (commutative and regular group actions)

A group action of a group $(G,\cdot)$ on a set $\mathcal{X}$ is a function $\star\colon G \times \mathcal{X} \to \mathcal{X}$ such that:

- Letting e be the identity element in G, for every $x \in \mathcal{X}$ we have $e \star x = x$
- For every $g, h \in G$ and for every $x \in \mathcal{X}$ we have $(g \cdot h) \star x = g \star (h \star x)$
- G is a commutative/abelian group
- For any $x, x' \in \mathcal{X}$, there exists a **unique** $g \in G$ such that $g \star x = x'$

Plausibly **post-quantum secure** instantiations from the CSIDH family of isogenies [CLMPR18] and derivatives of CSIDH with known group structure (such as CSI-Fish [BKV19])

Definitions adopted from [ADMP20]

(Same as definitions in the previous talk)

Hinting PRG from cryptographic group actions (brief overview)

Our simple approach for constructing hinting PRGs from DDH readily generalizes to cryptographic group actions (commutative and regular group actions)

A group action of a group $(G,\cdot)$ on a set $\mathcal{X}$ is a function $\star\colon G \times \mathcal{X} \to \mathcal{X}$ such that:

- Letting e be the identity element in G, for every $x \in \mathcal{X}$ we have $e \star x = x$
- For every $g, h \in G$ and for every $x \in \mathcal{X}$ we have $(g \cdot h) \star x = g \star (h \star x)$
- G is a commutative/abelian group
- For any $x, x' \in \mathcal{X}$, there exists a **unique** $g \in G$ such that $g \star x = x'$

Plausibly **post-quantum secure** instantiations from the CSIDH family of isogenies [CLMPR18] and derivatives of CSIDH with known group structure (such as CSI-Fish [BKV19])

Definitions adopted from [ADM**P**20]

(Same as definitions in the previous talk)

Construction of hinting PRG from group action (generalizes construction from plain DDH)

- Let $\mathrm{M} = [\mathrm{m}_1\ \mathrm{m}_2\ \dots\ \mathrm{m}_n] \leftarrow G^{n\times n}$ and let $\mathrm{x} = [x_1\ x_2\ \dots\ x_n] \leftarrow \mathcal{X}^n$ for $n > \log|G| + \omega(\log\lambda)$
- Define the function $H_{\mathrm{M},\mathrm{x}}\colon \{0,1\}^n \to \mathcal{X}^n$ as:

$$H_{\mathrm{M},\mathrm{x}}(\mathrm{s} = (s_1, \dots, s_n)) = \mathrm{M}\mathrm{s} \star \mathrm{x} = (< \mathrm{m}_1, \mathrm{s} > \star\, x_1, < \mathrm{m}_2, \mathrm{s} > \star\, x_2, \dots, < \mathrm{m}_n, \mathrm{s} > \star\, x_n)$$

$$\text{where } < \mathrm{m}_\mathrm{i}, \mathrm{s} > = \prod_{j\in[n]} m_{i,j}^{s_j}$$

Hinting PRG from cryptographic group actions (brief overview)

Our simple approach for constructing hinting PRGs from DDH readily generalizes to cryptographic group actions (commutative and regular group actions)

A group action of a group $(G,\cdot)$ on a set $\mathcal{X}$ is a function $\star\colon G \times \mathcal{X} \to \mathcal{X}$ such that:

- Letting e be the identity element in G, for every $x \in \mathcal{X}$ we have $e \star x = x$
- For every $g, h \in G$ and for every $x \in \mathcal{X}$ we have $(g \cdot h) \star x = g \star (h \star x)$
- G is a commutative/abelian group
- For any $x, x' \in \mathcal{X}$, there exists a **unique** $g \in G$ such that $g \star x = x'$

Plausibly **post-quantum secure** instantiations from the CSIDH family of isogenies [CLMPR18] and derivatives of CSIDH with known group structure (such as CSI-Fish [BKV19])

Definitions adopted from [ADM**P**20]

(Same as definitions in the previous talk)

Construction of hinting PRG from group action (generalizes construction from plain DDH)

- Let $\mathrm{M} = [\mathrm{m}_1\ \mathrm{m}_2\ \dots\ \mathrm{m}_n] \leftarrow G^{n\times n}$ and let $\mathrm{x} = [x_1\ x_2\ \dots\ x_n] \leftarrow \mathcal{X}^n$ for $n > \log|G| + \omega(\log\lambda)$
- Define the function $H_{\mathrm{M},\mathrm{x}}\colon \{0,1\}^n \to \mathcal{X}^n$ as:

$$H_{\mathrm{M},\mathrm{x}}(\mathrm{s} = (s_1, \dots, s_n)) = \mathrm{M}\mathrm{s} \star \mathrm{x} = (< \mathrm{m}_1, \mathrm{s} > \star\, x_1, < \mathrm{m}_2, \mathrm{s} > \star\, x_2, \dots, < \mathrm{m}_n, \mathrm{s} > \star\, x_n)$$

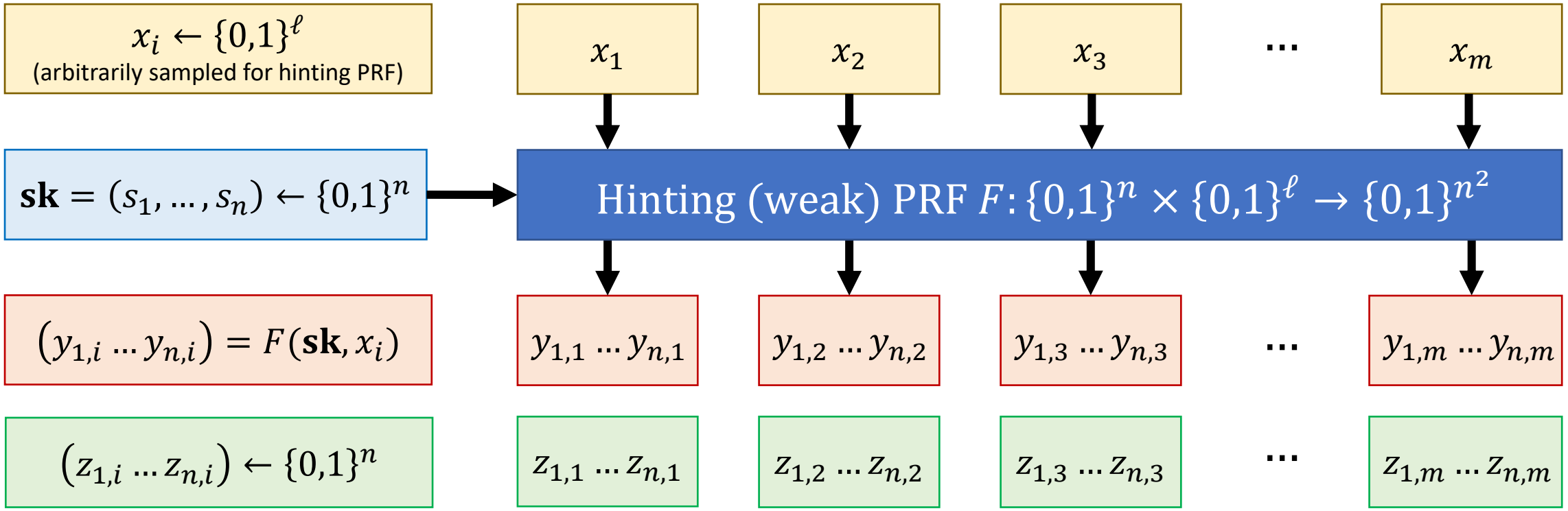
Our result (see paper for details)

H is a hinting PRG if the group action $\star\colon G \times \mathcal{X} \to \mathcal{X}$ satisfies the **linear hidden shift (LHS) assumption** [ADM**P**20]

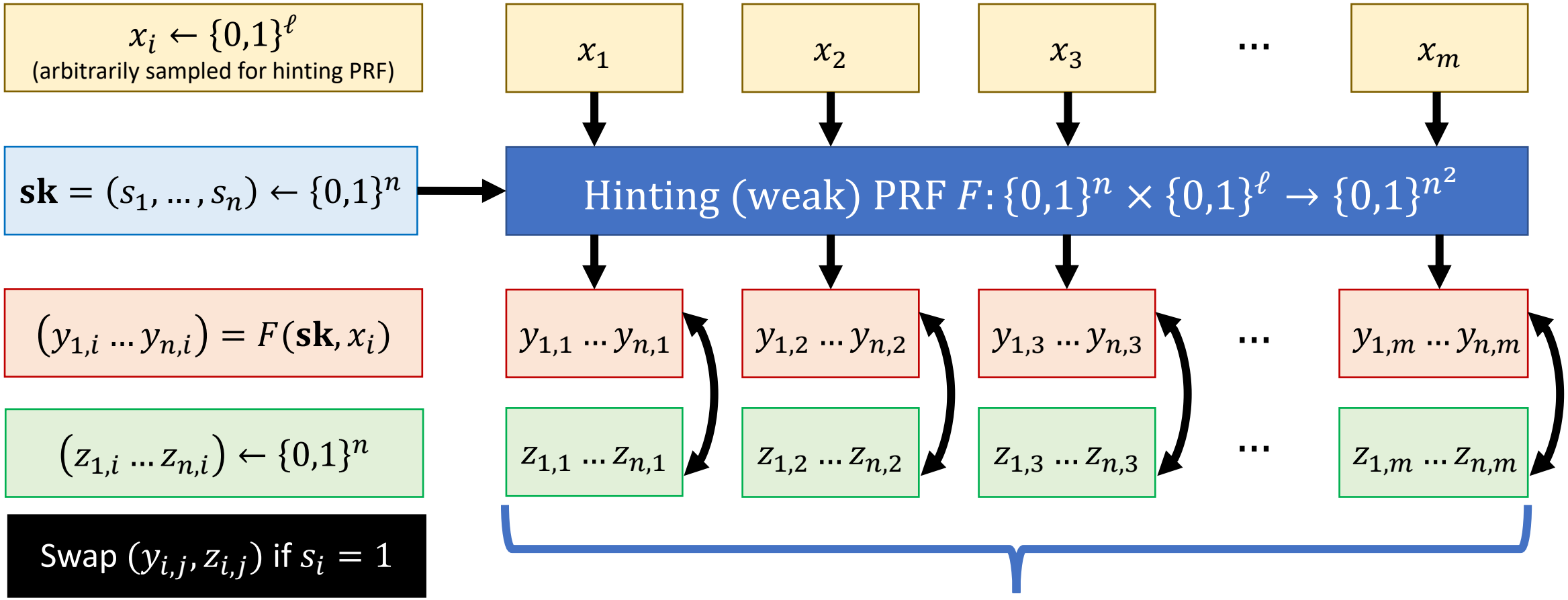
Talk Outline

- Simple Hinting PRG from DDH
- Hinting PRG from cryptographic group actions (brief overview)
- Hinting weak PRF (brief overview)
- Summary and open questions

Hinting (weak) PRF (brief overview)



Hinting (weak) PRF (informal definition)



Multi-evaluation hinting property (each wPRF evaluation leaks info about the secret key **sk**)

Remains pseudorandom across multiple evaluations
(computationally indistinguishable from a set of m matrices of dimension $2 \times n$, where each matrix consisting of random n-bit strings)

Hinting weak PRF (construction outlines)

Our simple approaches for constructing hinting PRGs from DDH/group actions naturally extend to hinting weak PRFs from the same assumptions

Hinting weak PRF from DDH (informal outline)

- Let G be a DDH-hard group of prime order q with generator g, and let $n > \log|G| + \omega(\log\lambda)$
- Define the function $F: \{0,1\}^n \times G^{n\times n} \rightarrow G^n$ as:

$$F(\mathrm{s} \in \{0,1\}^n, [\mathrm{M}]) = [\mathrm{Ms}]$$

Our Result-1

F is a **hinting** weak PRF assuming that G is a DDH-hard group

Hinting weak PRF from Group Actions (informal outline)

- Let $(G, \mathcal{X}, \star)$ be an LHS-hard cryptographic group action, and let $n > \log|G| + \omega(\log\lambda)$, and let $\mathrm{x} = [x_1\ x_2\ \ldots x_n] \leftarrow \mathcal{X}^n$
- Define the function $F'_{\mathrm{x}}: \{0,1\}^n \times G^{n\times n} \rightarrow \mathcal{X}^n$ as:

$$F'_{\mathrm{x}}(\mathrm{s} \in \{0,1\}^n, [\mathrm{M}]) = [\mathrm{Ms}] \star \mathrm{x}$$

Our Result-2

F' is a **hinting** weak PRF assuming that $(G, \mathcal{X}, \star)$ is an LHS-hard group action

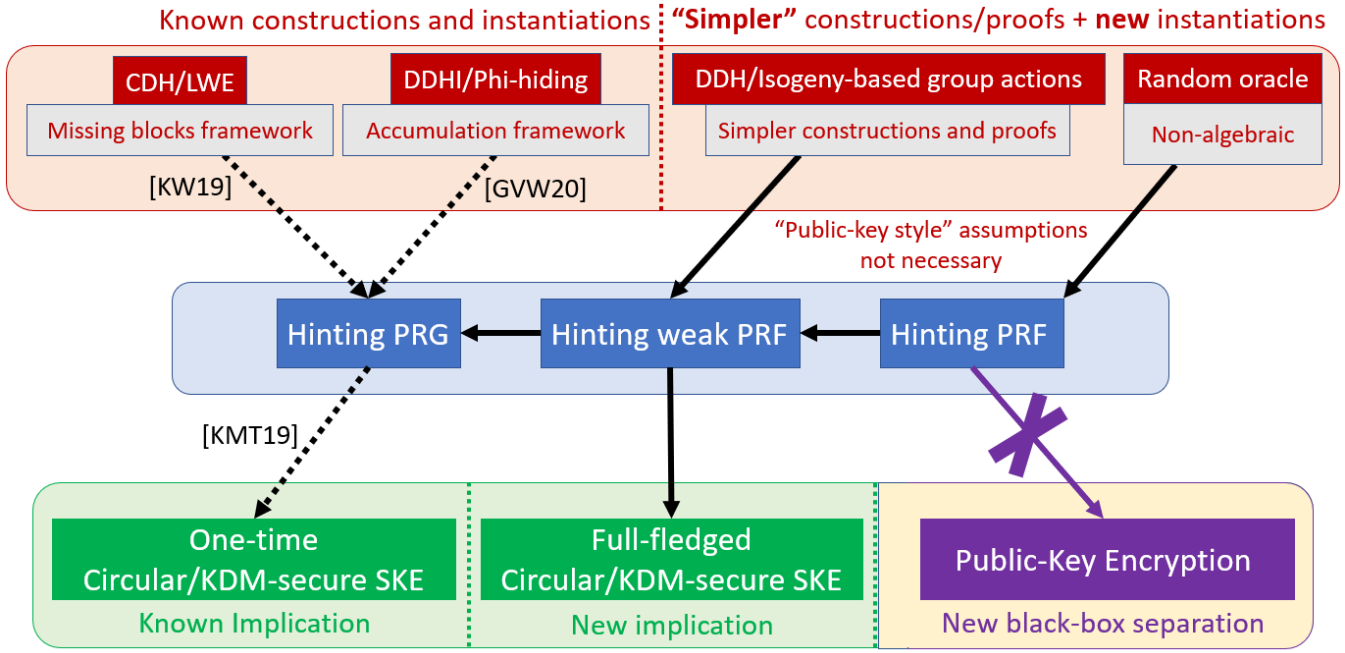
See paper for detailed constructions and proofs

Talk Outline

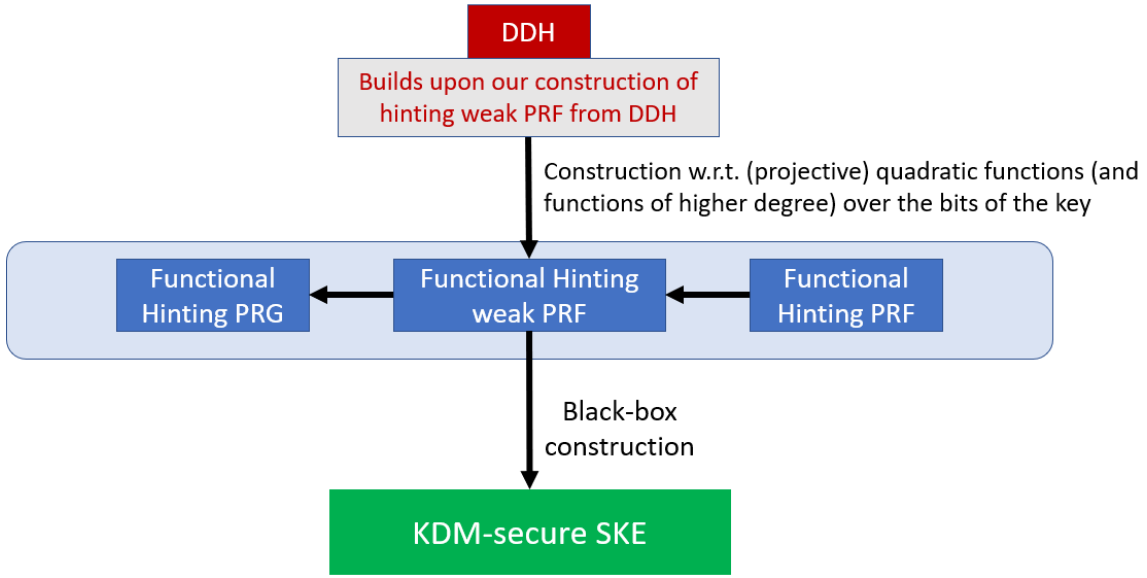
- Simple Hinting PRG from DDH
- Hinting PRG from cryptographic group actions (brief overview)
- Hinting weak PRF (brief overview)
- Summary and open questions

Summary and Open Questions

Primitives with hinting property



Primitives with functional hinting property



- Construct (functional) hinting PRFs from standard mathematical assumptions
- Realize primitives with the functional hinting property from a wider set of (quantum-safe) assumptions
- Investigate additional applications of primitives with the (functional) hinting property

Full version coming on ePrint soon

Thank You! Questions?