Exploring Crypto Dark Matter:
New Simple PRF Candidates and Their Applications

Dan Boneh, Yuval Ishai, Alain Passelègue,
Amit Sahai, and David J. Wu

How Do We Design Cryptographic Primitives?

1. Introduce hardness assumption (e.g., RSA, discrete log, LWE)
2. Reduce security to breaking hardness assumption

Theory-Driven

Clean problems to analyze:
"n primitives $\leftrightarrow$ 1 assumption"

Algebraic structure can reduce concrete efficiency and can be exploited in attacks (e.g., sub-exponential-time attacks)

How Do We Design Cryptographic Primitives?

Schemes have good concrete efficiency and oftentimes tuned to application demands

Can be messy or more difficult to analyze "n primitives $\leftrightarrow$ n assumptions"

1. Design primitive (e.g., block ciphers, hash functions) with focus on concrete efficiency
2. Security relies on heuristics, cryptanalysis

Practice-Oriented

The Landscape of Cryptography

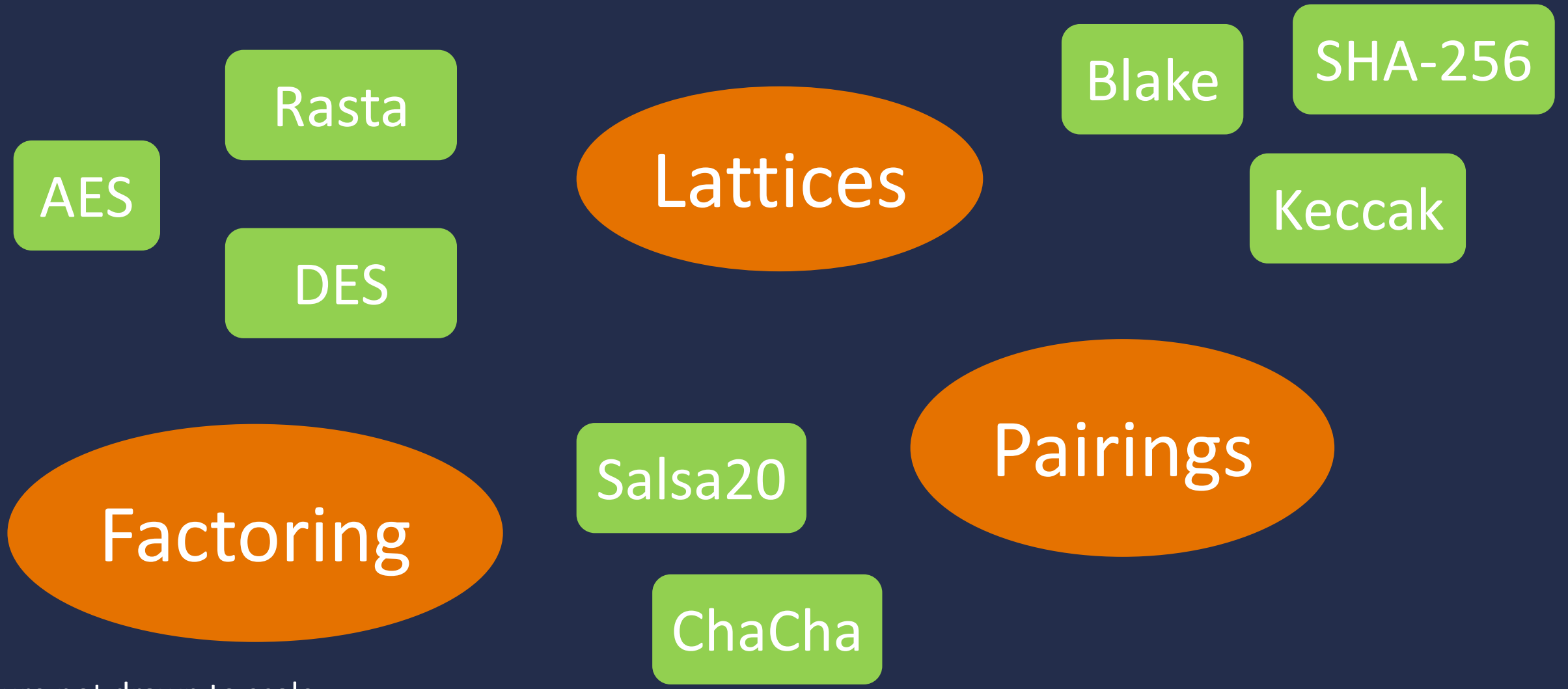


Figure not drawn to scale

The Landscape of Cryptography

Exploring Crypto Dark Matter

Goals:

- Explore simplest unexplored areas of cryptography
- New intractability conjectures such that:
  - Validity ⇒ Simple constructions of crypto primitives
    - **Theory:** minimize natural complexity measures
    - **Practice:** useful efficiency features for applications
  - Invalidity ⇒ Interesting positive results in other domains

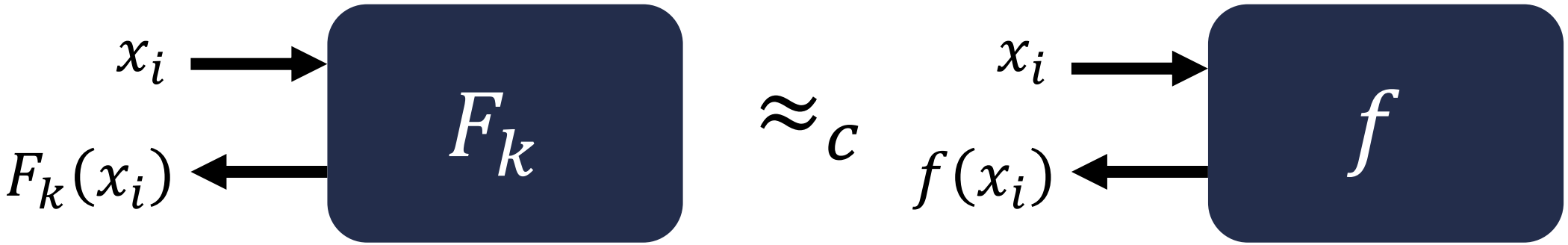
Earlier examples:

- Goldreich's one-way function based on expander graphs [Gol01]
- Miles and Viola [MV12] and Akavia et al. [ABGKR14] work on constructing low-complexity PRFs

Our Focus: (Weak) Pseudorandom Functions

Deterministic keyed function $F_k: \mathcal{X} \rightarrow \mathcal{Y}$

- Efficiently-computable
- Input-output behavior indistinguishable from truly random function $f: \mathcal{X} \rightarrow \mathcal{Y}$

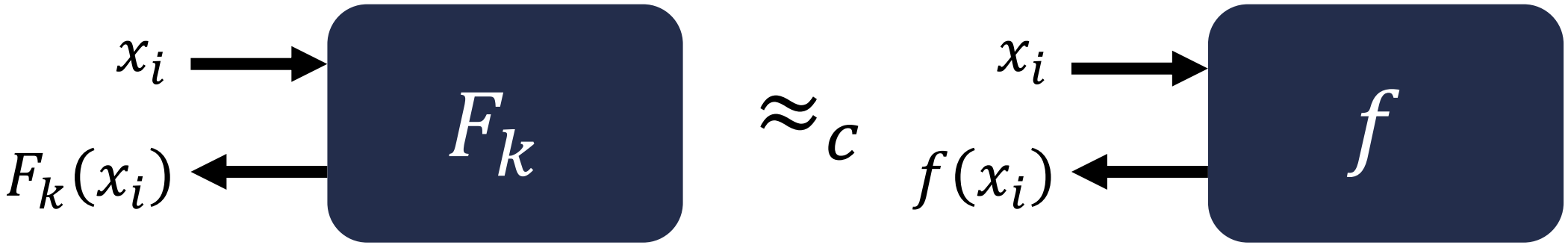


Our Focus: (Weak) Pseudorandom Functions

Deterministic keyed function $F_k: \mathcal{X} \rightarrow \mathcal{Y}$

- Effici
- Inpu truly random func

Weak PRF: Security is guaranteed as long as x_i's are uniformly random



What Do We Want to Optimize?

Traditionally:

- Primary goal: minimize key size
- Secondary goals: varies depending on application

This work:

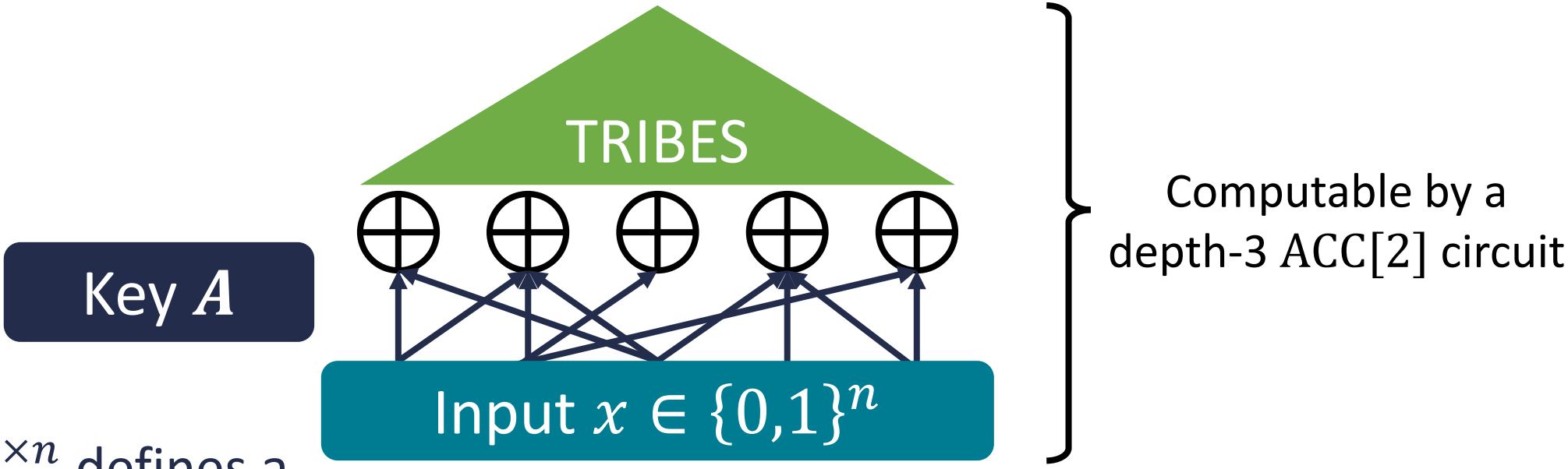
- Settle for “near-optimal” key size
- Focus on optimizing other standard measures
  - Circuit depth
  - Circuit size
  - Non-linear size and depth

} Useful for many MPC settings

A Simple Weak PRF Candidate

[ABGKR14]

Akavia-Bogdanov-Guo-Kamath-Rosen Construction



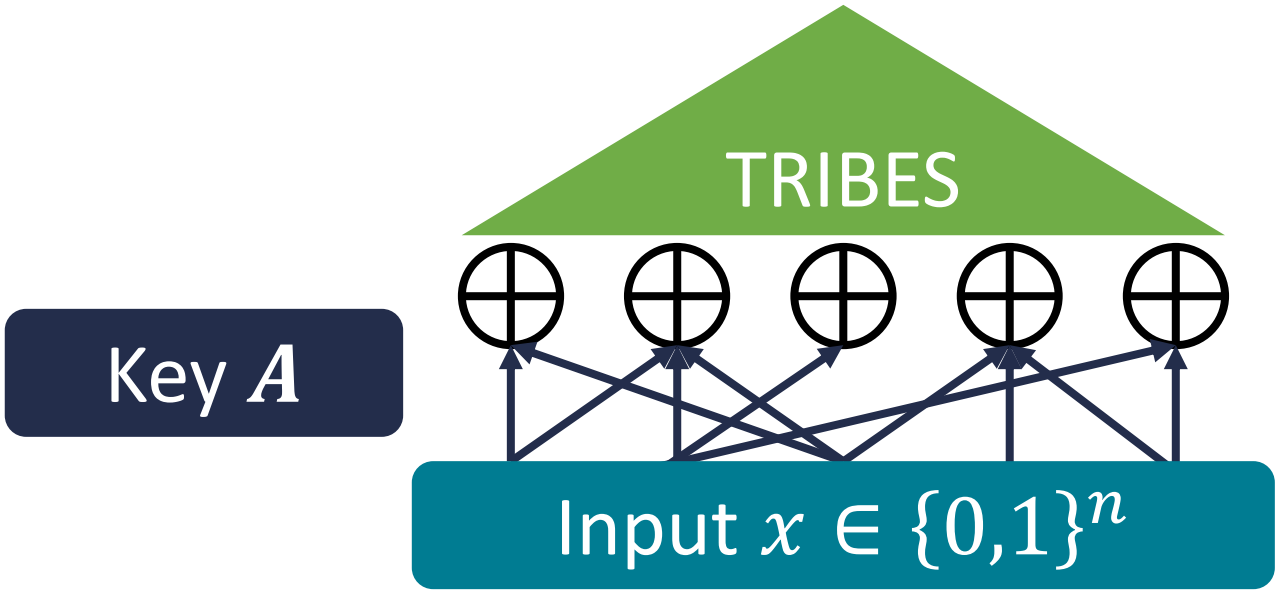
Key $A \in \mathbb{Z}_2^{n \times n}$ defines a mod-2 linear mapping

$$\mathrm{PRF}(A, x) := \mathrm{TRIBES}(Ax)$$

A Simple Weak PRF Candidate

[ABGKR14]

Akavia-Bogdanov-Guo-Kamath-Rosen Construction



[BR17]: TRIBES function can be represented by a rational polynomial of degree $O(\log n)$, which yields a quasi-polynomial time distinguisher

Can we replace the TRIBES function with a different function to get a construction with better security (and similar complexity)?

Hardness from Modulus Mixing

Define the function $\mathrm{map}: \{0,1\}^n \to \mathbb{Z}_3$:

$$\mathrm{map}(x) := \sum_{i \in [n]} x_i \pmod 3$$

"mod-3 sum of binary vector"

Razborov-Smolensky: the map function *cannot*
be approximated by a low-degree polynomial over $\mathbb{Z}_2$

Our Main Weak PRF Candidate

$$F_A(x) := \mathrm{map}\left(A \times x \right)$$

PRF key

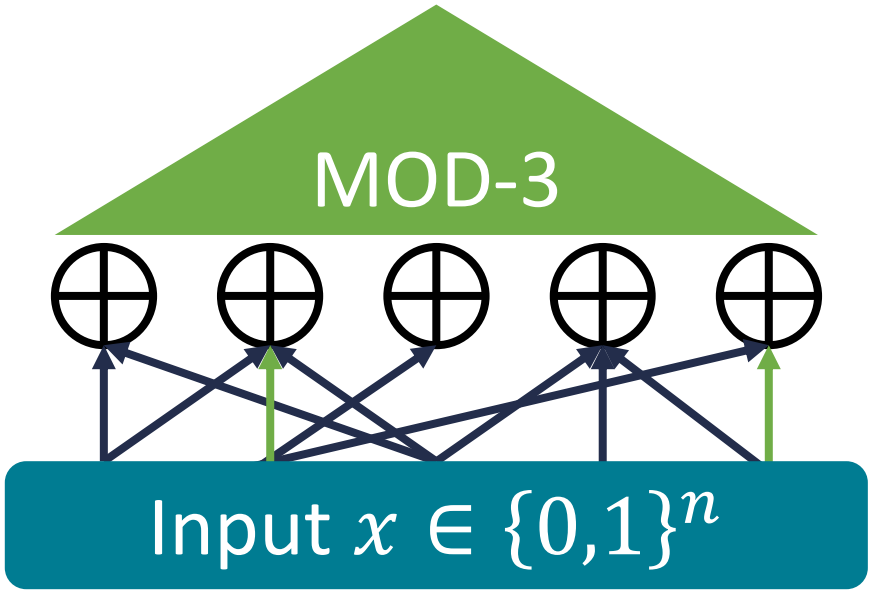
input

$A \in \mathbb{Z}_2^{n \times n}$ $x \in \mathbb{Z}_2^n$

"secret matrix-vector product over $\mathbb{Z}_2$, sum resulting values mod 3"

Our Main Weak PRF Candidate

Key A



Many variants:

- Replace mod-2/mod-3 with mod-p/mod-q
- **Multiple output bits:** replace "sum mod-3" with matrix-vector product mod-3
- **Compact keys:** take $\boldsymbol{A}$ to be a structured matrix

$$F_{\boldsymbol{A}}(x) \coloneqq \mathrm{map}(\boldsymbol{A}x) \text{ where } \boldsymbol{A} \in \mathbb{Z}_2^{n \times n}$$

Our Weak PRF Candidate

$$F_A(x) := \mathrm{map}(Ax) \text{ where } A \in \mathbb{Z}_2^{n \times n}$$

"secret matrix-vector product over $\mathbb{Z}_2$, sum resulting values mod 3"

Conjecture (Informal)**:** The above function family is a <u>weak</u> PRF family.

Basic conjecture: advantage of $\mathrm{poly}(\lambda)$-time adversary is $\mathrm{negl}(\lambda)$ when $n = \mathrm{poly}(\lambda)$

Stronger conjecture: advantage of 2^{λ}-time distinguishers is $2^{-\Omega(\lambda)}$ when $n = O(\lambda)$ – *exponential hardness*

Our Weak PRF Candidate

$$F_A(x) := \mathrm{map}(Ax) \text{ where } A \in \mathbb{Z}_2^{n \times n}$$

"secret matrix-vector product over $\mathbb{Z}_2$, sum resulting values mod 3"

Conjecture (Informal)**:** The above function family is a weak PRF family.

Candidate is not a strong PRF: can be expressed as a certain sparse polynomial over $\mathbb{Z}_3$ (which can be distinguished from random given non-adaptive queries)

Why Is This (Plausibly) Secure?

$$F_A(x) := \mathrm{map}(Ax) \text{ where } A \in \mathbb{Z}_2^{n \times n}$$

"secret matrix-vector product over $\mathbb{Z}_2$, sum resulting values mod 3"

- Cannot be approximated by low-degree polynomials
- Resilient to statistical learning algorithms (LMN-type)
- Highly nonlinear (BKW-style attacks do not seem to apply)

We invite further cryptanalysis of our candidates!

Is This Simple?

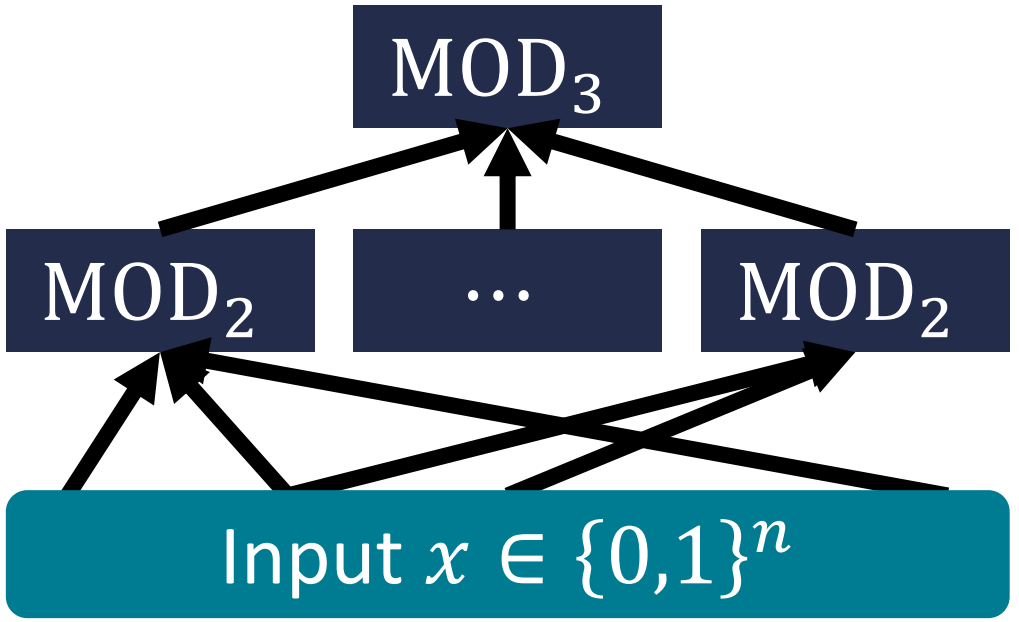
$$F_A(x) \coloneqq \mathrm{map}(Ax) \text{ where } A \in \mathbb{Z}_2^{n \times n}$$

"secret matrix-vector product over $\mathbb{Z}_2$, sum resulting values mod 3"

Conceptual simplicity: no mention of groups, S-boxes, …

Complexity-theoretic: candidate can be computed by:

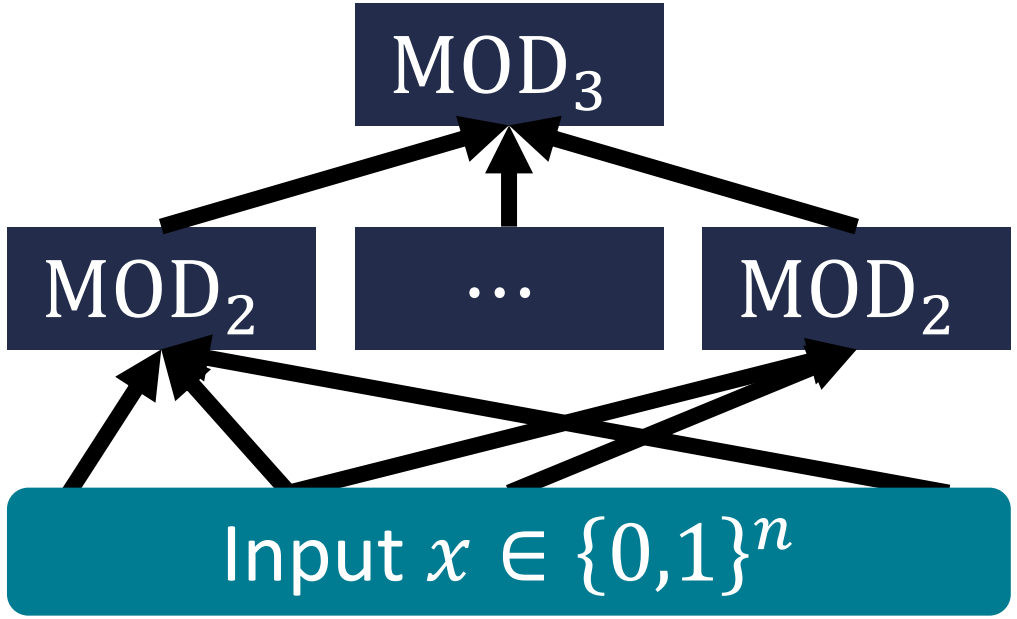
- Depth-2 ACC circuits
- Width-3 branching programs [Bar95]
- Sparse multilinear $\mathbb{Z}_3$-polynomials



Theoretical Implications

Complexity-theoretic: Candidate can be comparable by:

- Depth-2 ACC circuits
- Width-3 branching programs [Bar95]
- Sparse multilinear $\mathbb{Z}_3$-polynomials



Implications of our conjectures:

- Depth-2 $\mathrm{ACC}[6]$ is **not PAC-learnable** in sub-exponential time under the uniform distribution
- Width-3 branching programs are **not PAC-learnable** in sub-exponential time under the uniform distribution
- Sparse multivariate $\mathbb{Z}_3$-polynomials are **hard to interpolate** given only random evaluations on $\{-1,1\}^n$

Theoretical Implications

What is the "minimal" complexity class that contains (weak) PRFs (with exponential security)?

	AC^0	$\mathrm{ACC}^0[p]$	$\mathrm{ACC}^0[m]$
Depth 2			**This Work:** Weak PRF (exponential)
Depth 3	Weak PRF [AR16] (quasi-polynomial)	Weak PRF [ABGKR14] (quasi-polynomial)	**This Work:** Strong PRF (exponential)
Depth ≥ 3	Weak PRF [Kha93] (quasi-polynomial)	Strong PRF [Vio13] (quasi-polynomial)	

No strong PRFs for broad classes of depth-2 circuits [BV96]

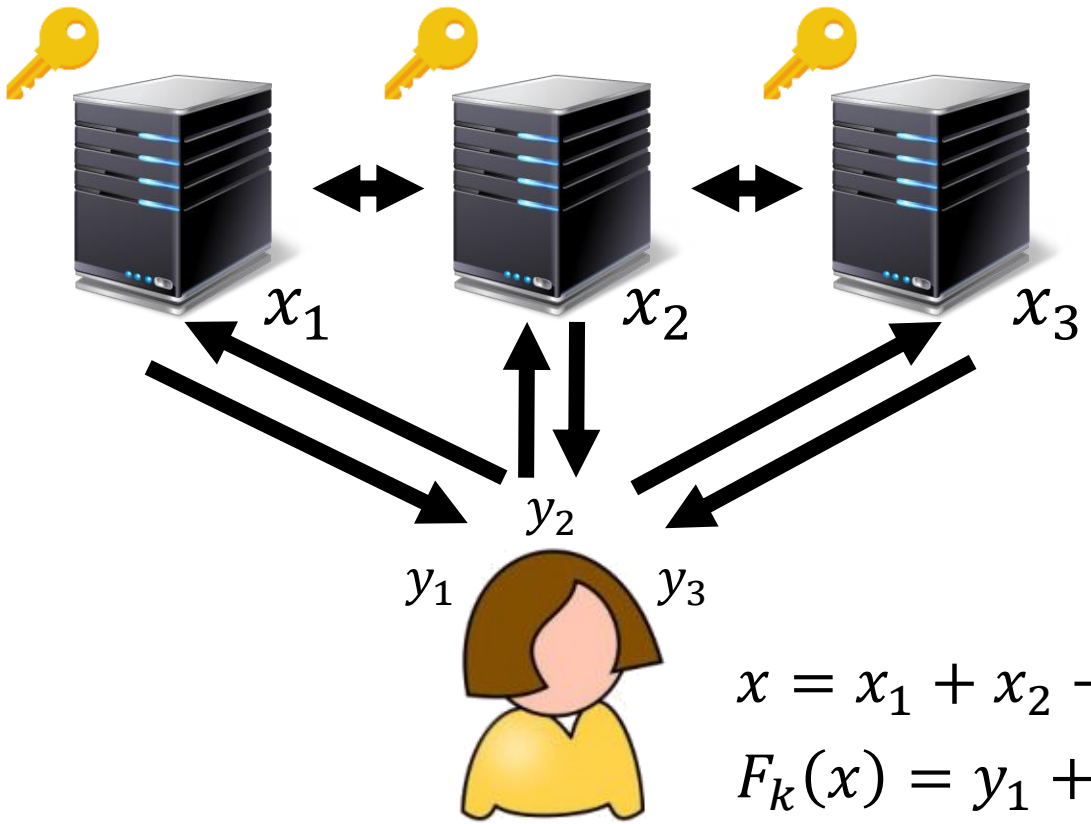
No weak PRFs with better than quasi-polynomial security [LMN89]

No strong PRFs with better than quasi-polynomial security [CIKK16]

Distributed PRF Evaluation

secret key is secret-shared across multiple parties

$$k = k_1 + k_2 + k_3 \pmod m$$



In typical MPC protocols, costs (e.g., communication, number of rounds, etc.) scale with the number of non-linear operations

$$x = x_1 + x_2 + x_3 \pmod m$$

$$F_k(x) = y_1 + y_2 + y_3 \pmod m$$

Distributed PRF Evaluation

Comparison for two-party distributed PRF evaluation with preprocessing

	Round Complexity	Online Communication (kb)	Preprocessing Size (kb)
Yao + AES	2	64.8	1491.2
Yao + LowMC	2	64.8	292.1
Our Candidate	**4**	**2.6**	**3.5**

Similar protocols for 2-round 3-party distributed evaluation protocol with similar communication via secret-sharing based MPC [BGW88, CCD88, AFLNO16]

Our Weak PRF Candidate

$$F_A(x) \coloneqq \mathrm{map}(Ax) \text{ where } A \in \mathbb{Z}_2^{n \times n}$$

"secret matrix-vector product over $\mathbb{Z}_2$, sum resulting values mod 3"

This is **not** a strong PRF!

Our Weak PRF Candidate

$$F_A(x) \coloneqq \mathrm{map}(Ax) \text{ where } A \in \mathbb{Z}_2^{n \times n}$$

"secret matrix-vector product over $\mathbb{Z}_2$, sum resulting values mod 3"

Attacks on strong PRF security:

- Non-adaptive distinguisher based on representation as sparse polynomial
- Adaptive distinguisher based on representation as a finite automaton with multiplicity [BV94]

All known attacks rely on seeing PRF evaluations on close inputs (in Hamming distance)

Our Weak PRF Candidate

$$F_A(x) \coloneqq \mathrm{map}(Ax) \text{ where } A \in \mathbb{Z}_2^{n \times n}$$

"secret matrix-vector product over $\mathbb{Z}_2$, sum resulting values mod 3"

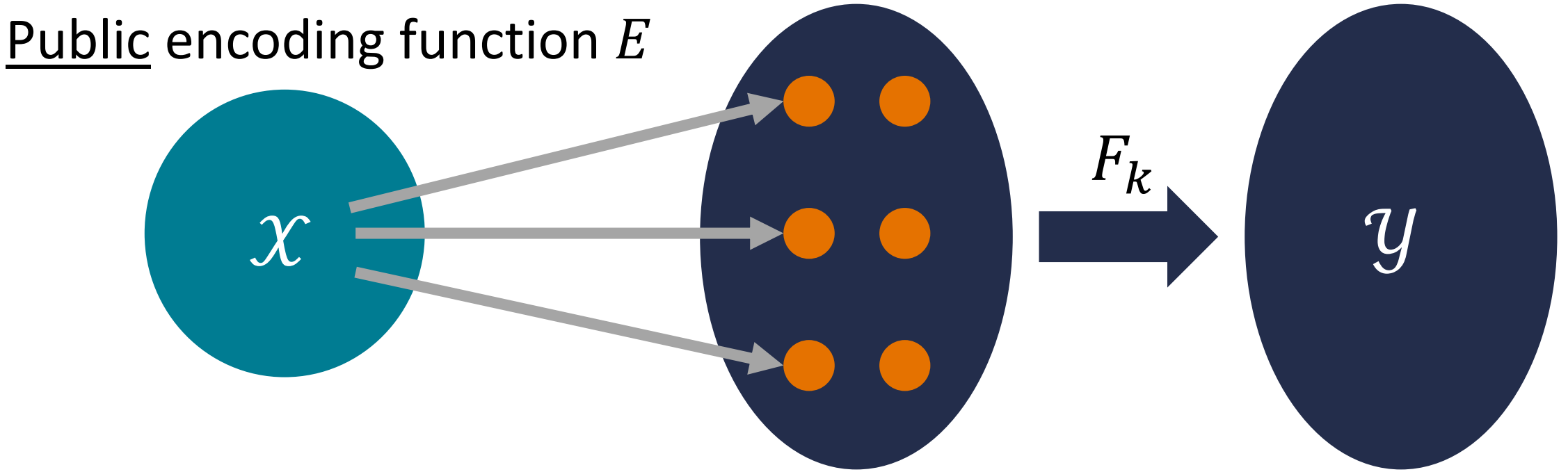
Attacks on strong PRF security:

- Non-adaptive distinguisher based on representation as sparse polynomial
- Adaptive distinguisher based on representation as a finite automaton with multiplicity [BV94]

Idea: require inputs to the PRF to be far apart

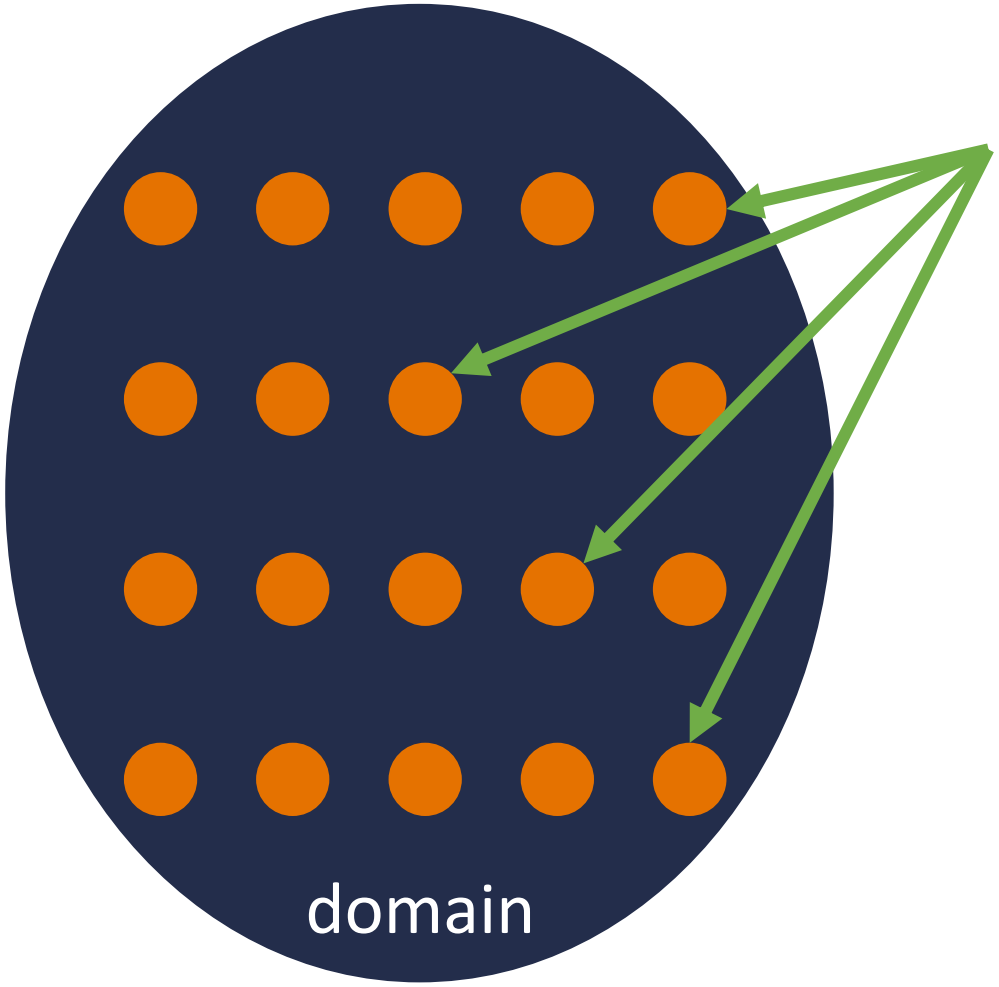
Encoded-Input PRFs

Idea: require inputs to the PRF to be far apart



Pushing the complexity of the PRF into the public encoding function E while leaving security in the simple evaluation of F_k

Encoded-Input PRFs

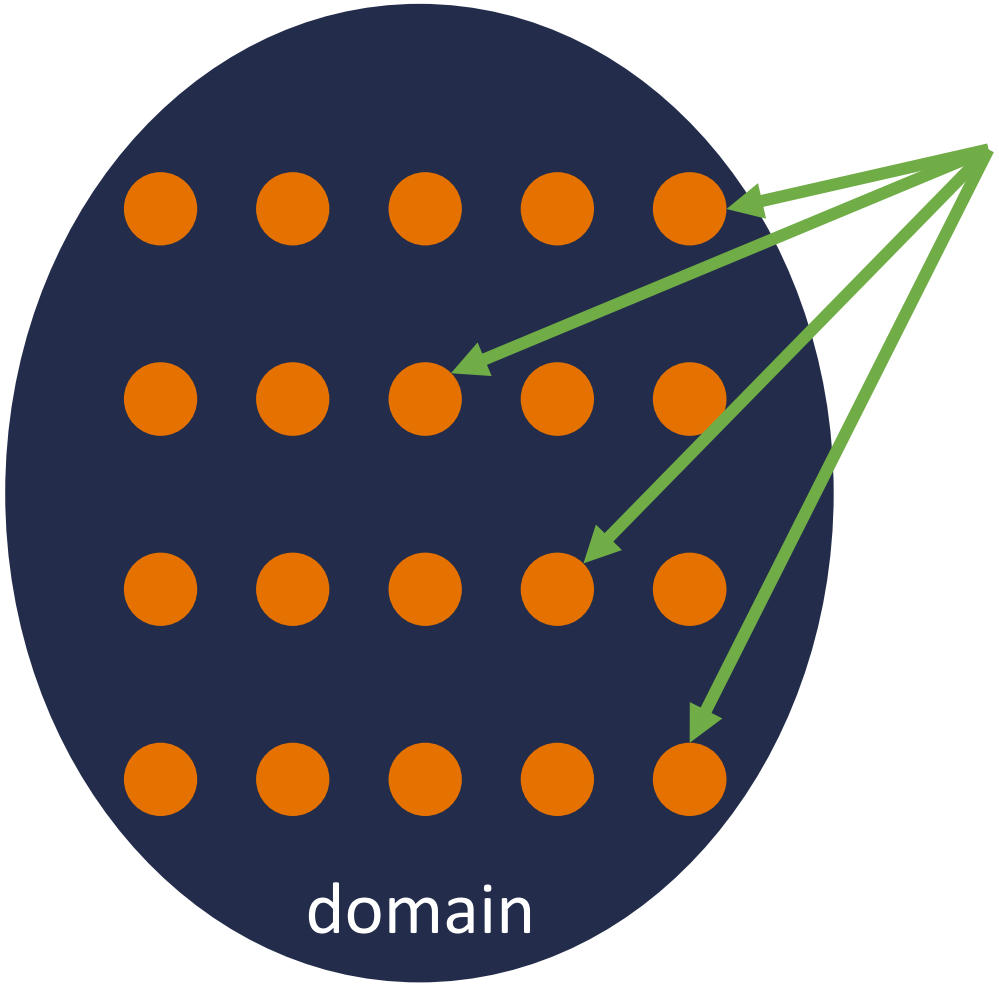


Encoded-input PRF: function whose behavior is pseudorandom on a sparse subset of the domain

(F, E) is an encoded-input PRF if $F'(k, x) := F\big(k, E(x)\big)$ is a strong PRF

Advantage: checking that an input is properly encoded is simple (depth-2 circuit); this is useful for many applications

Encoded-Input PRFs

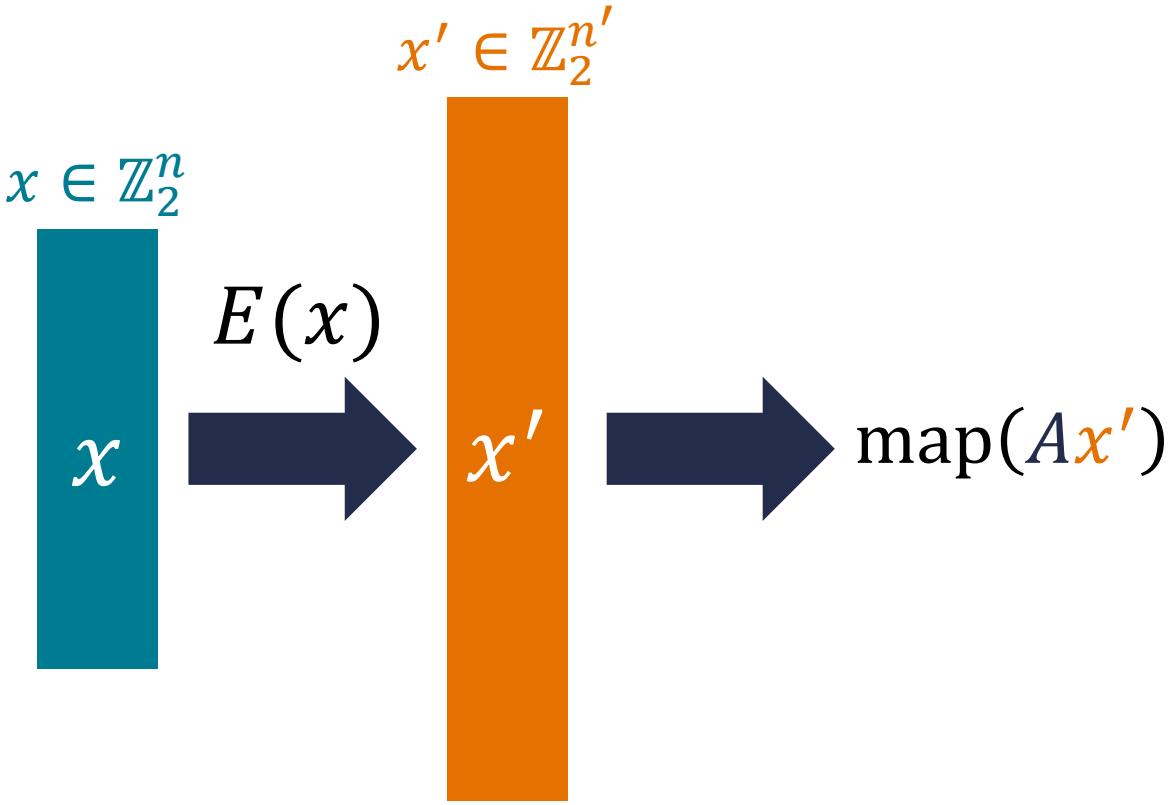


Encoded-input PRF: function whose behavior is pseudorandom on a sparse subset of the domain

(F, E) is an encoded-input PRF if $F'(k, x) \coloneqq F\big(k, E(x)\big)$ is a strong PRF

Concrete proposal: take encoding function to be encoding algorithm of a linear error-correcting code

Encoded-Input PRFs



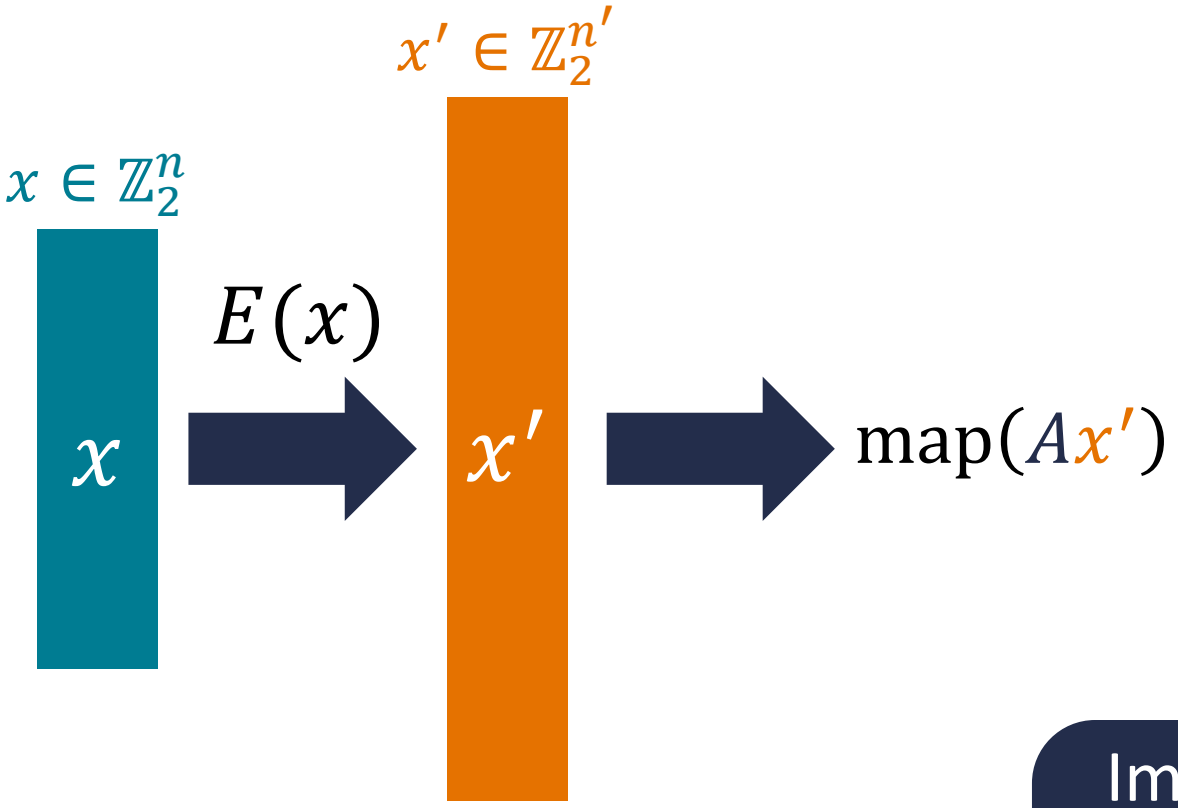
Encoding is done using a linear ECC over $\mathbb{Z}_3$ and taking the binary decomposition

Encoded-input PRF: function whose behavior is pseudorandom on a sparse subset of the domain

(F, E) is an encoded-input PRF if $F'(k, x) \coloneqq F\big(k, E(x)\big)$ is a strong PRF

Concrete proposal: take encoding function to be encoding algorithm of a linear error-correcting code

Encoded-Input PRFs



Encoded-input PRF: function whose behavior is pseudorandom on a sparse subset of the domain

(F, E) is an encoded-input PRF if $F'(k, x) := F\big(k, E(x)\big)$ is a strong PRF

Encoding is done using a linear ECC over $\mathbb{Z}_3$ and taking the binary decomposition

Important to consider ECC over $\mathbb{Z}_3$ and not $\mathbb{Z}_2$ since otherwise, encoding and multiplication by secret key A can be combined (again relies on modulus mixing!)

Encoded-Input PRFs and Strong PRFs

$A \in \mathbb{Z}_2^{m \times m}$ $G \in \mathbb{Z}_3^{m \times n}$ $x \in \{0,1\}^n$

$$F_A(x) := \text{map}\left(A \times \text{BinaryDec}\left(G \; x\right)\right)$$

Secret linear mapping

Public encoding procedure

Conjecture: F_A is a strong PRF (when considering the composition of encoding with weak PRF)

Encoded-Input PRFs and Strong PRFs

$A \in \mathbb{Z}_2^{m \times m}$ $G \in \mathbb{Z}_3^{m \times n}$ $x \in \{0,1\}^n$

$$F_A(x) := \text{map}\left(A \times \text{BinaryDec}\left(G\,x\right)\right)$$

First candidate strong PRF in depth-3 ACC^0
(and even has plausible exponential security)

Conjecture: F_A is a strong PRF (when considering the composition of encoding with weak PRF)

Asymptotically-Optimal Strong PRFs

Does there exist strong PRFs with <u>exponential security</u> that can be computed by <u>linear-size</u> circuits?

$$F_A(x) := \mathrm{map}\left(A \times \mathrm{BinaryDec}\left(G\,x\right)\right)$$

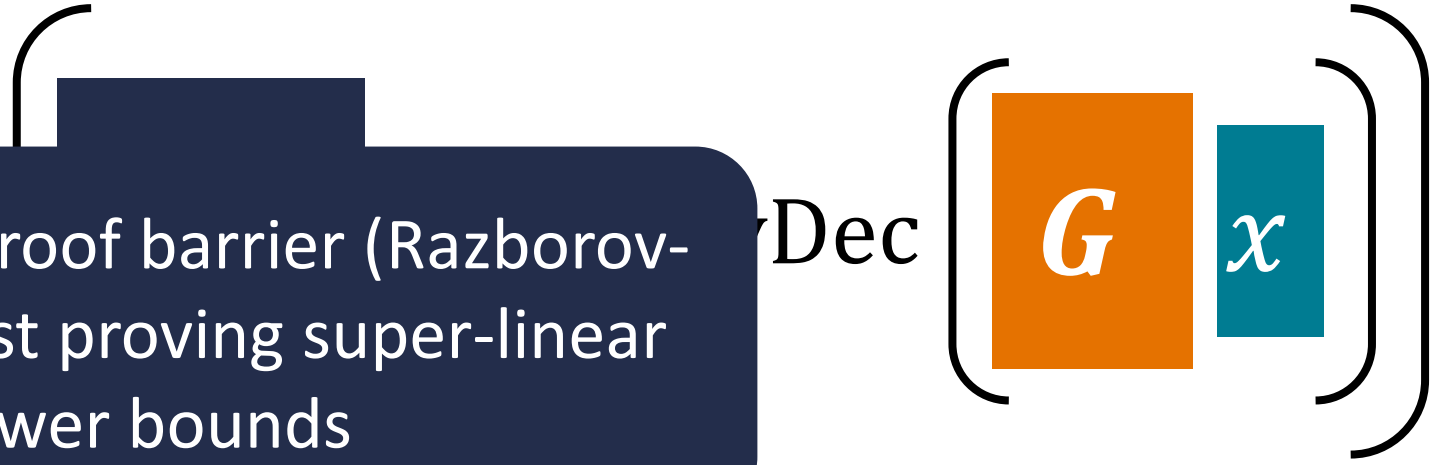
Resulting construction can be implemented by a *<u>linear-size</u>* circuit

Can instantiate with linear-time encodable codes [IKOS08, DI14]

Asymptotically-Optimal Strong PRFs

Does there exist strong PRFs with <u>exponential security</u> that can be computed by <u>linear-size</u> circuits?

Gives new natural proof barrier (Razborov-Rudich style) against proving super-linear circuit lower bounds



Resulting construction can be implemented by a *<u>linear-size</u>* circuit

Can instantiate with linear-time encodable codes [IKOS08, DI14]

Conclusions

$$F_A(x) \coloneqq \mathrm{map}(Ax) \text{ where } A \in \mathbb{Z}_2^{n \times n}$$

"secret matrix-vector product over $\mathbb{Z}_2$, sum resulting values mod 3"

Modulus mixing is a relatively unexplored source of hardness:

- Enables new and simple cryptographic primitives (e.g., weak PRF candidate in depth-2 ACC, strong PRF candidate in depth-3 ACC)
- Assumptions have numerous connections to problems in complexity theory, learning theory, mathematics

Open Questions and Future Directions

Building other cryptographic primitives (e.g., hash functions, signatures, etc.) from modulus mixing assumptions

- MPC-friendly primitives give natural candidate for *post-quantum* signatures [IKOS07]

Further cryptanalysis + applications of new PRF candidates

More crypto dark matter out there to be explored!

Thank you!

https://eprint.iacr.org/2018/1218