Simple and efficient PRFs with tighter Security via All-Prefix Universal Hash Functions

Tibor Jager
Paderborn University

Rafael Kurek
Paderborn University

Jiaxin Pan
Karlsruhe Institute of Technology

This talk

- New notion for Hash Functions
  - All-Prefix Universality
  - Examples

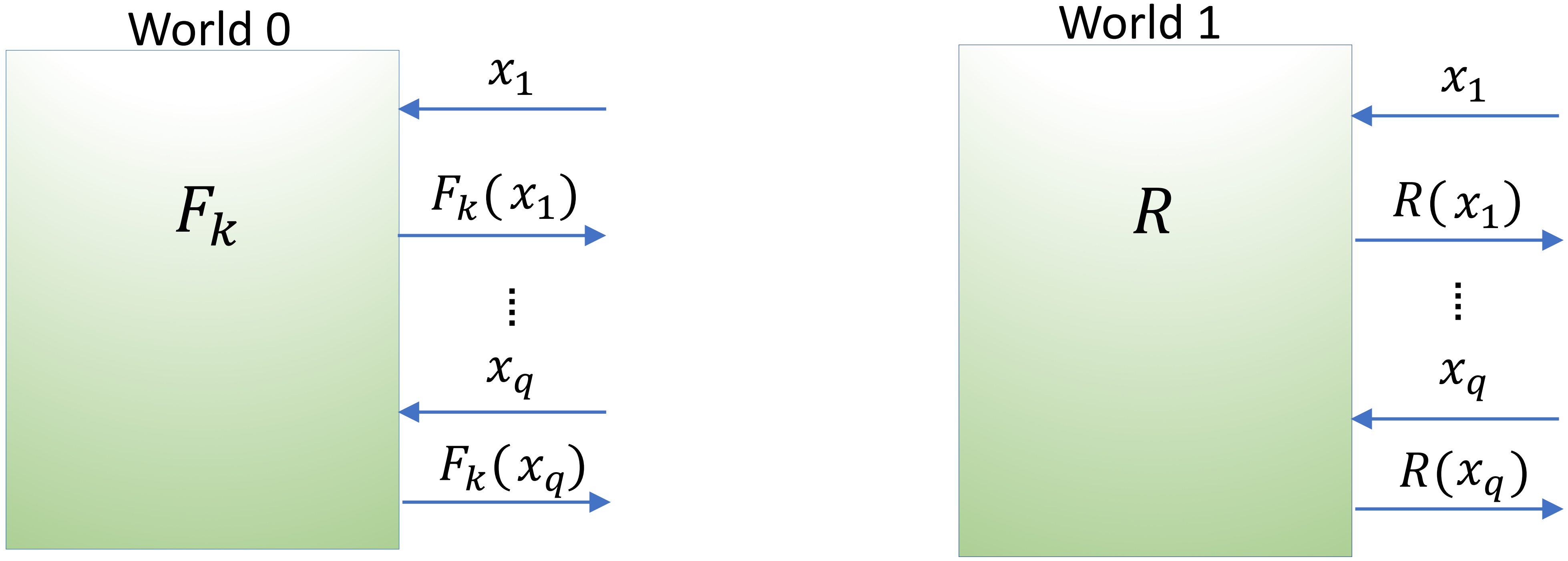
This talk

- New notion for Hash Functions
  - All-Prefix Universality
  - Examples
- New framework for tightly secure Pseudorandom Functions
  - very simple, small keys, efficient
  - covering Matrix-DDH (MDDH) and learning with errors (LWE)

This talk

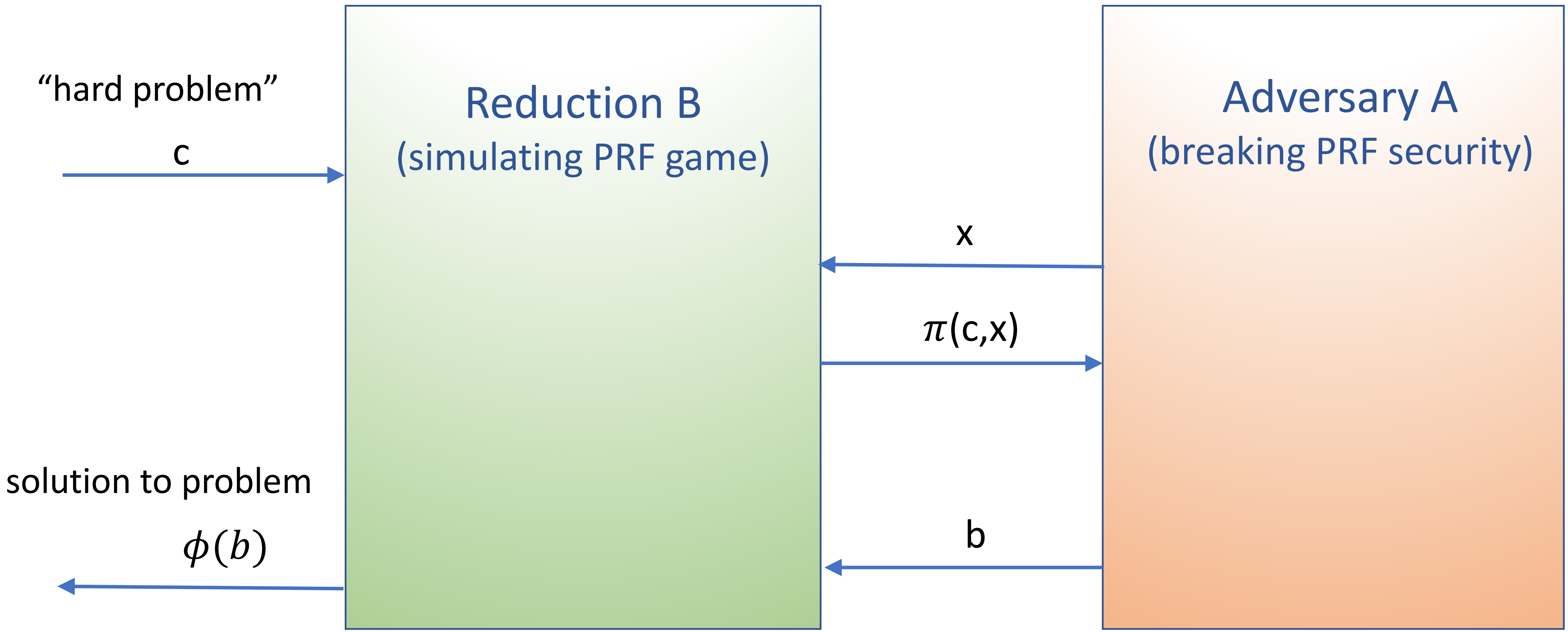
- New notion for Hash Functions
  - All-Prefix Universality
  - Examples
- New framework for tightly secure Pseudorandom Functions
  - very simple, small keys, efficient
  - covering Matrix-DDH (MDDH) and learning with errors (LWE)
- LWE-based PRF
  - Currently most efficient construction with weaker security assumption and super-poly modulus

Pseudorandom Functions (PRFs)



We call F a pseudorandom Function if both worlds are computationally indistinguishable.

Cryptographic Reduction



Tightness in reductions

We say that reduction B loses a factor L, if

$$\frac{t(B)}{e(B)} = L \, \frac{t(A)}{e(A)}$$

- t: running time
- e: advantage

We say the reduction is “tight“, if L is small (i.e. constant or logarithmic).

Tightness in reductions

We say that reduction B loses a factor L, if

$$\frac{t(B)}{e(B)} = L \, \frac{t(A)}{e(A)}$$

- t: running time
- e: advantage

We say the reduction is "tight", if L is small (i.e. constant or logarithmic).

Loss might depend on input length!

PRFs with loss depending on input length

- GGM PRF [FOCS84]
- Matrix-DDH-based PRFs [Escala et al. CRYPTO13]
  - Naor-Reingold PRF [FOCS97]
  - Lewko-Waters PRF [CCS09]
- LWE-based PRFs
  - BPR PRF [Banerjee et al. EUROCRYPT12]

Naïve approach

1. Hash input x with cryptographic Hash Function

$$H: \{0,1\}^* \to \{0,1\}^n$$
$$\text{x} \longmapsto h(x)$$

2. Evaluate PRF on hash

$$F_k(h(x))$$

Naïve approach

1. Hash input x with cryptographic Hash Function

$$H : \{0,1\}^* \to \{0,1\}^n$$
$$\mathrm{x} \longmapsto h(x)$$

2. Evaluate PRF on hash

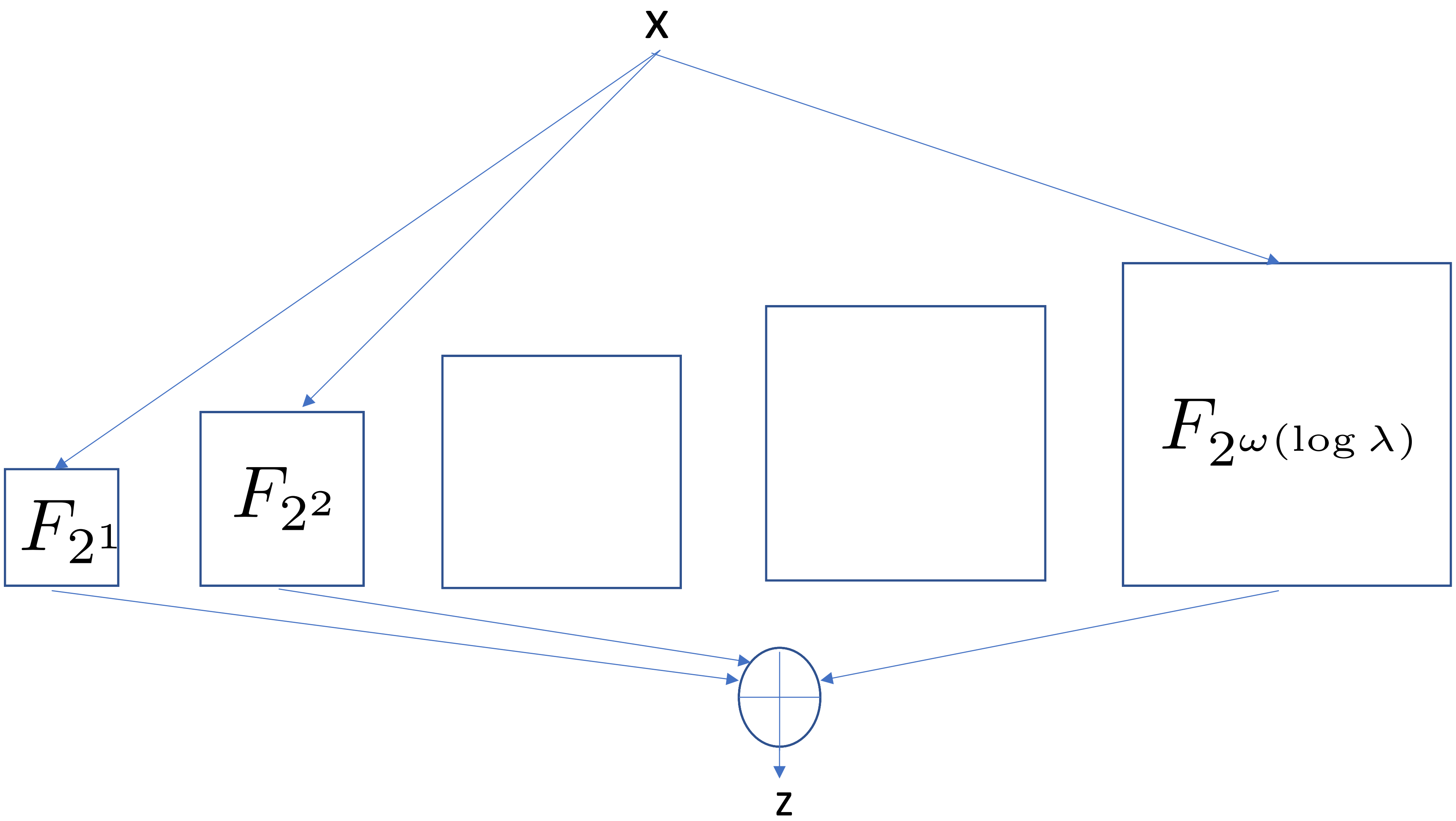
$$F_k(h(x))$$

n=2λ, where λ security parameter

$$\Longrightarrow Security\ Loss\ O(\lambda)\ and\ |sk| = O(\lambda)$$

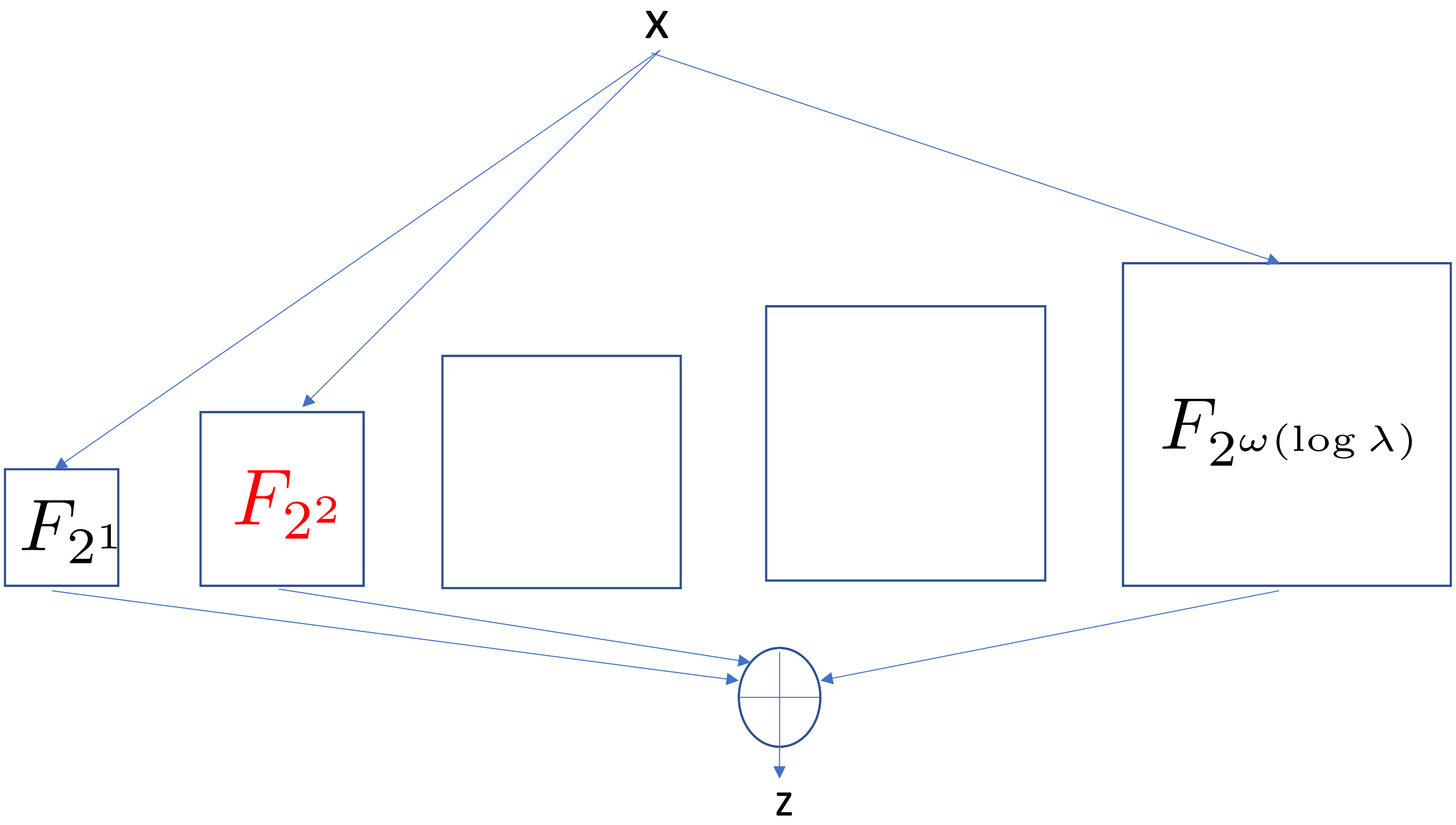
On-the-fly adaption

[Döttling and Schröder CRYPTO15]



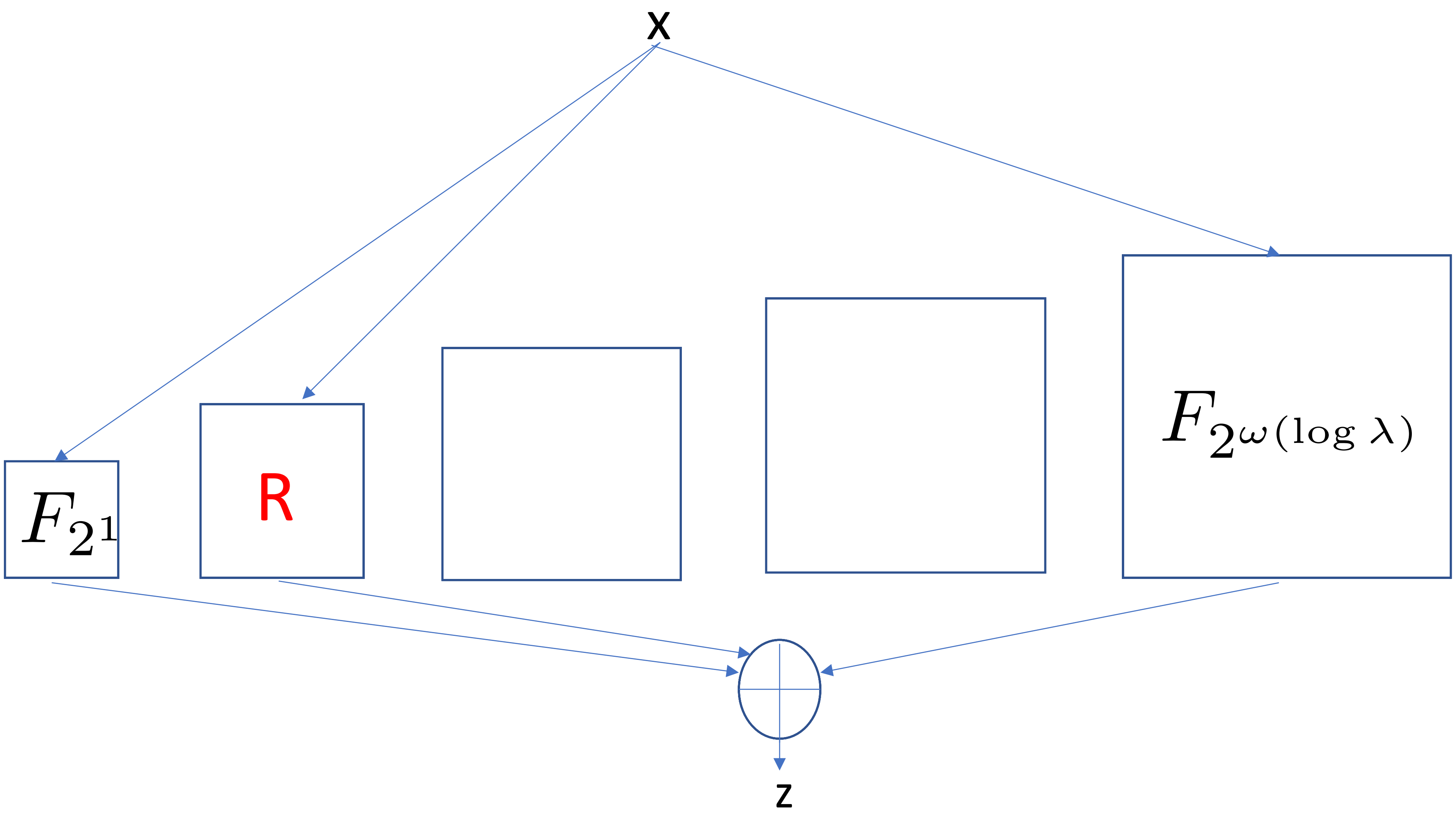
On-the-fly adaption

[Döttling and Schröder CRYPTO15]



On-the-fly adaption

[Döttling and Schröder CRYPTO15]



Döttling and Schröder [CRYPTO15]

- Works especially well for PRFs with loss in input length
- Tight security loss in framework
- Smaller keys
- $\lambda \cdot \omega(\log \lambda)$ invocations of underlying PRF (in the generic framework)

Döttling and Schröder [CRYPTO15]

- Works especially well for PRFs with loss in input length
- Tight security loss in framework
- Smaller keys
- $\lambda \cdot \omega(\log \lambda)$ invocations of underlying PRF (in the generic framework)

Can we do it with a single invocation?

Augmented cascade PRF

[Boneh at al. ACM CCS 2010]

Let $F: \underbrace{S \times K}_{\text{Key space}} \times \{0,1\} \to K$ be a PRF.

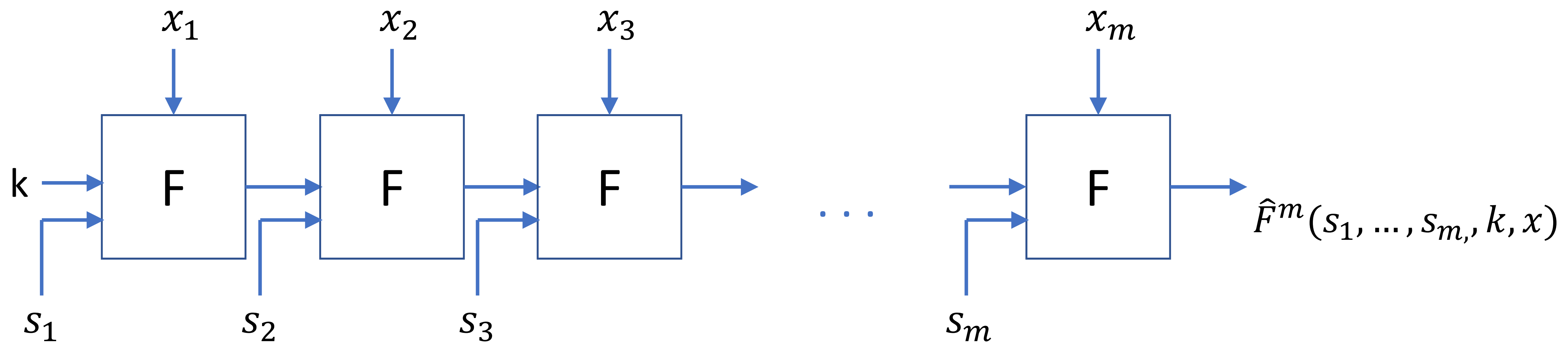
Augmented cascade PRF

[Boneh at al. ACM CCS 2010]

Let $F: S \times K \times \{0,1\} \rightarrow K$ be a PRF.

Key space

Augmented cascade PRF $\hat{F}^m$



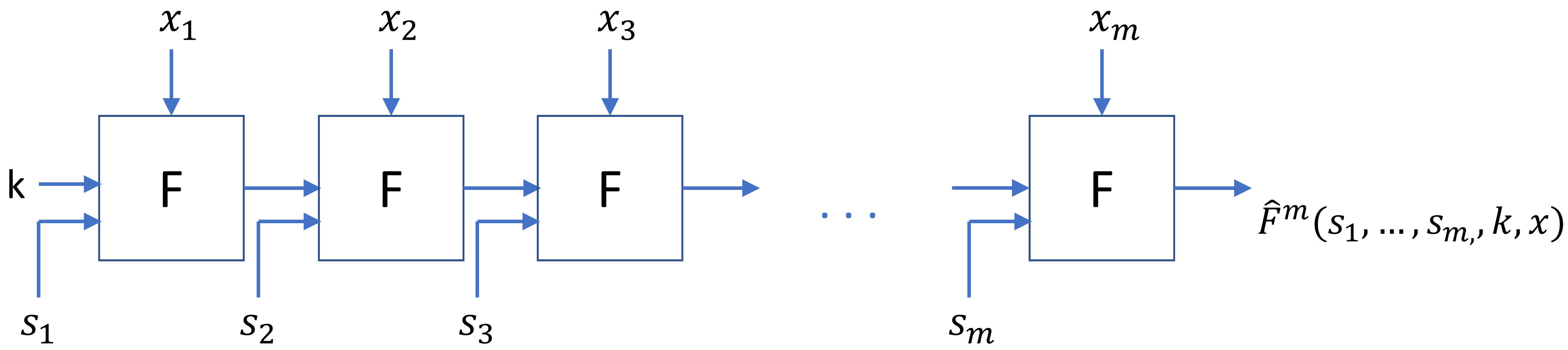
Augmented cascade PRF

[Boneh at al. ACM CCS 2010]

Let F: S × K × {0,1} → K be a PRF.

Key space

Augmented cascade PRF $\hat{F}^m$



Loss and $|sk|$ depend on input length!

=> shorter input => tighter proof and shorter keys

Universal Hash functions

Denote $H = \{h \mid h: \{0,1\}^n \to \{0,1\}^m\}$.

H is a family of universal hash functions, if

$$Pr_{h \leftarrow H}[h(x) = h(x')\ ] \leq \frac{1}{2^m}$$

$$\forall x \neq x'$$

All-Prefix Universal Hash Functions

Denote $H = \{h \mid h: \{0,1\}^n \to \{0,1\}^m\}$.

H is a family of all-prefix universal hash functions, if

$$Pr_{h \leftarrow H}[h(x)_i = h(x')_i] \leq \frac{1}{2^i}$$

$$\forall x \neq x' \ \ \forall i \in [m]$$

All-Prefix almost-Universal Hash Functions

Denote $H = \{h \mid h: \{0,1\}^n \to \{0,1\}^m\}$.

H is a family of all-prefix almost-universal hash functions, if

$$Pr_{h \leftarrow H}[h(x)_i = h(x')_i] \leq \frac{2}{2^i}$$

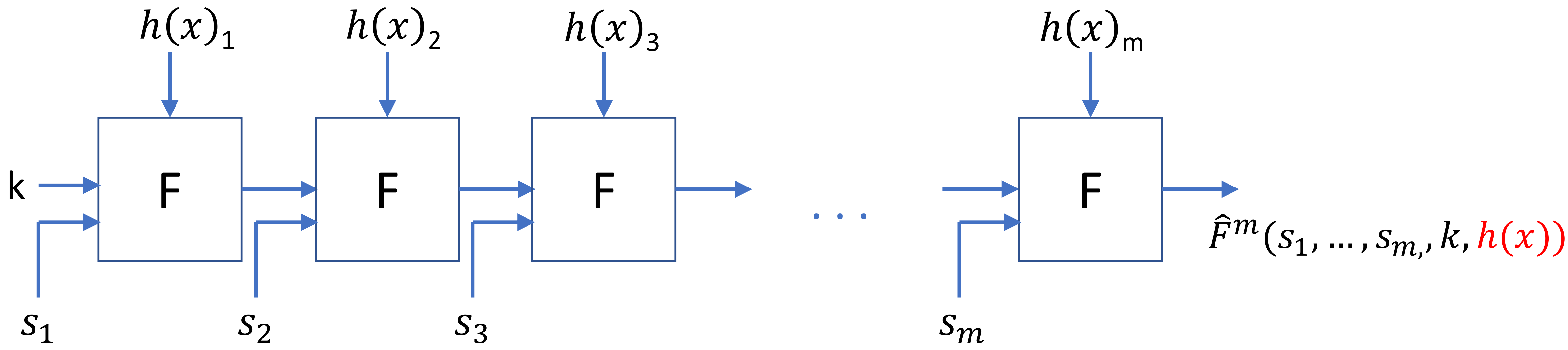
$$\forall x \neq x' \;\; \forall i \in [m]$$

The Augmented Cascade with Encoded Input

1. Hash input x with All-Prefix Universal Hash Function with output length m=ω(log λ)

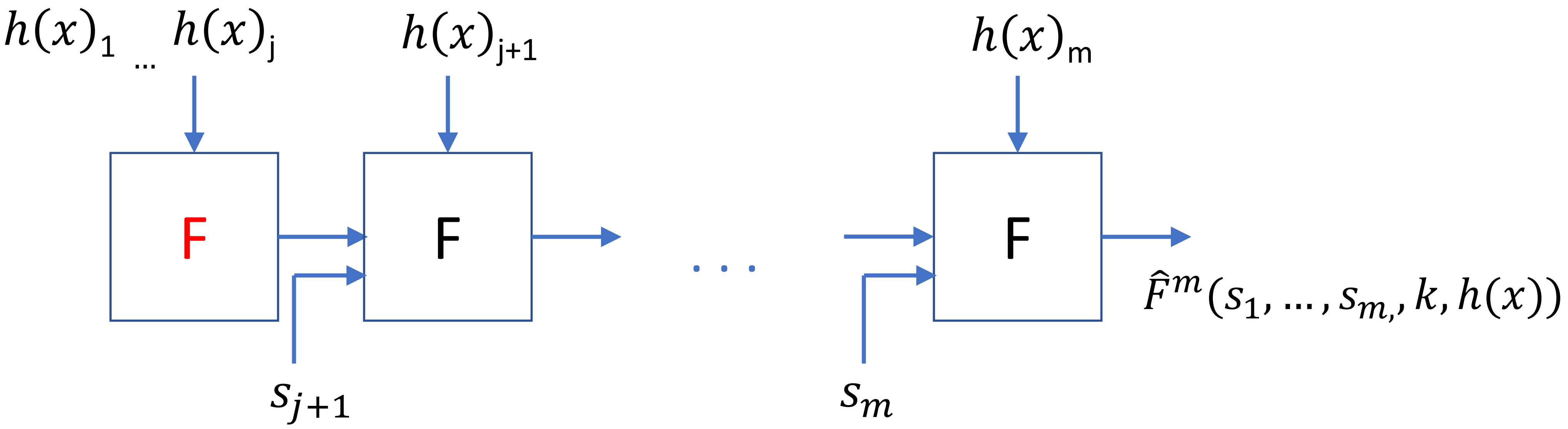
The Augmented Cascade with Encoded Input

1. Hash input x with All-Prefix Universal Hash Function with output length m=$\omega(\log \lambda)$
2. Evaluate Augmented Cascade PRF on h(x)



Proof sketch

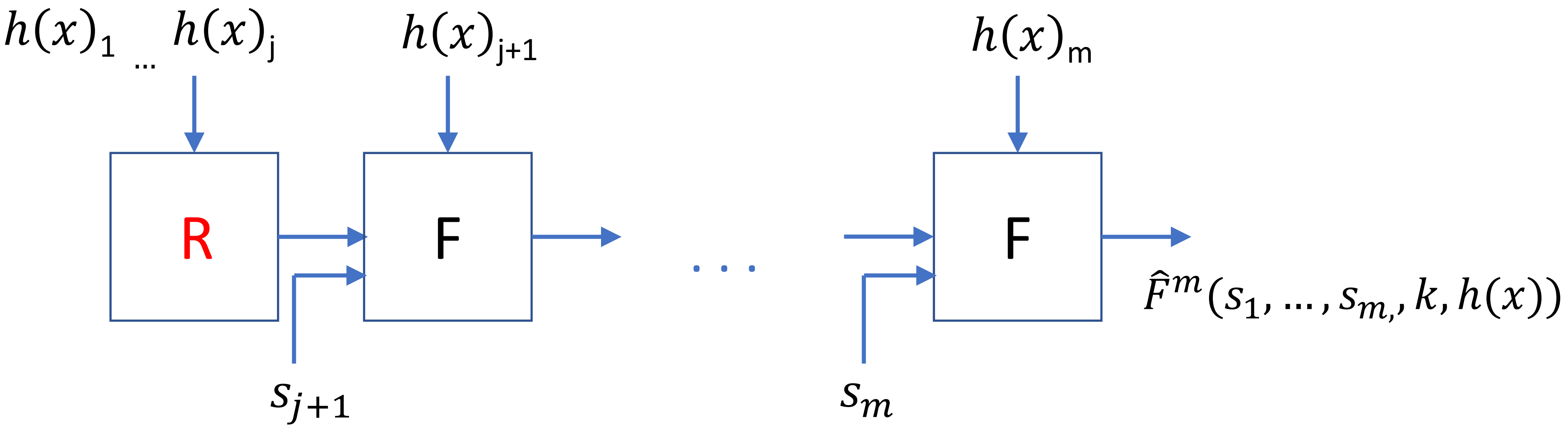
- B breaks AC-PRF with length j, where j depends on adversary A
- Simulates security game for A, breaking AC-PRF with encoded input



j=O(log k), m=ω(log λ)

Proof sketch

- B breaks AC-PRF with length j, where j depends on adversary A
- Simulates security game for A, breaking AC-PRF with encoded input

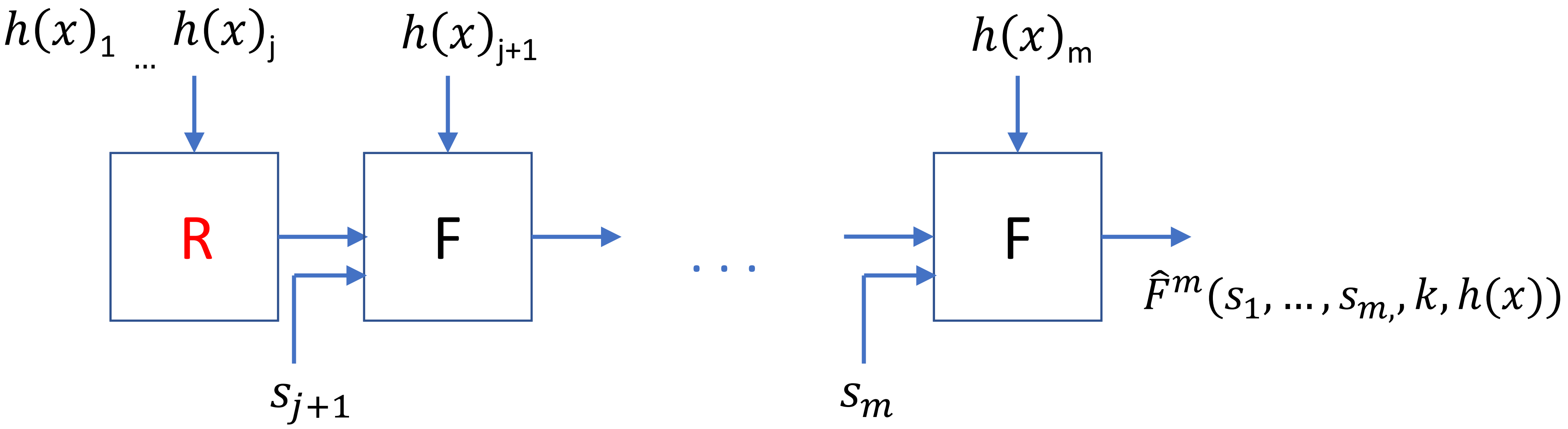


j=O(log k), m=ω(log λ)

Proof sketch

<u>APUHF</u>:

- R($h(\cdot)_j$) uniformly random ⇒ A gains no information about h ⇒ information-theoretically hard to find collision
- no collision on $h(\cdot)_j$ ⇒ R($h(\cdot)_j$) uniformly random for all queries



j=O(log k), m=ω(log λ)

One additional property required!

Perfect one-time security

$$\Pr_{k \leftarrow K}[\hat{F}(s, k, x) = k'] = \frac{1}{|K|}$$

for all $(s, k', x) \in S \times K \times \{0, 1\}$

Comparison MDDH-PRFs

	Key Size	Loss	Invocations	
MDDH PRFs	n	n	1	$n >> m$
DötSch15 PRF	$m = \omega(\log \lambda)$	$\mathcal{O}(\log \lambda)$	1	domain $\mathbb{Z}_q$
Our PRF	$m = \omega(\log \lambda)$	$\mathcal{O}(\log \lambda)$	1	

Comparison LWE

	Key Size	Loss	Invocations	Modulus
BPR PRFs	n	$Q \cdot N \cdot n$	1	exp in λ
DötSch15 PRF	$m = \omega(\log \lambda)$	$Q \cdot N \cdot \mathcal{O}(\log \lambda)$	$\lambda \cdot \omega(\log \lambda)$	super-poly in λ
Our PRF	$m = \omega(\log \lambda)$	$Q \cdot N \cdot \mathcal{O}(\log \lambda)$	1	super-poly in λ

Example: All-Prefix Universal HF

- Pairwise-independent hash functions mapping to bits

$$h_{a,b} : GF(2^n) \to GF(2^n)$$
$$x \mapsto ax + b$$

$$H = \{h_{a,b} : a, b \in \{0,1\}^n\}$$

Example: All-Prefix almost-Universal HF

- Dietzfelbinger et al. [DHKP, J ALG97]

$$h_a : \{0,1\}^m \rightarrow \{0,1\}^n$$

$$x \mapsto (ax \mod 2^n)\mathrm{div}^{n-m}$$

$$H_{n,m} = \{h_a : a \in [2^n - 1] \text{ and } a \text{ is odd}\}$$

Comparison to Truncation Collision Resistance

Both

- Similar technical properties
- Chosen prefix length depends on adversary

APUHF

- Security based on secret key
- Known Construction

Tru-CR HF

- Security not based on secret key
- Additional complexity assumption for standard HF

Conclusion

- New notion for Hash Functions
  - All-Prefix Universality
  - Examples
- New framework for tightly secure Pseudorandom Functions
  - very simple, small keys, efficient
  - covering Matrix-DDH (MDDH) and learning with errors (LWE)
- LWE-based PRF
  - Currently most efficient construction with weak security assumption

Thank you for your attention!

This talk: iacr.org/2018/826   Tuesday: iacr.org/2017/061

34