Domain extension for enhanced target collision-resistant hash functions

Ilya Mironov
Microsoft Research, Silicon Valley Campus

Outline

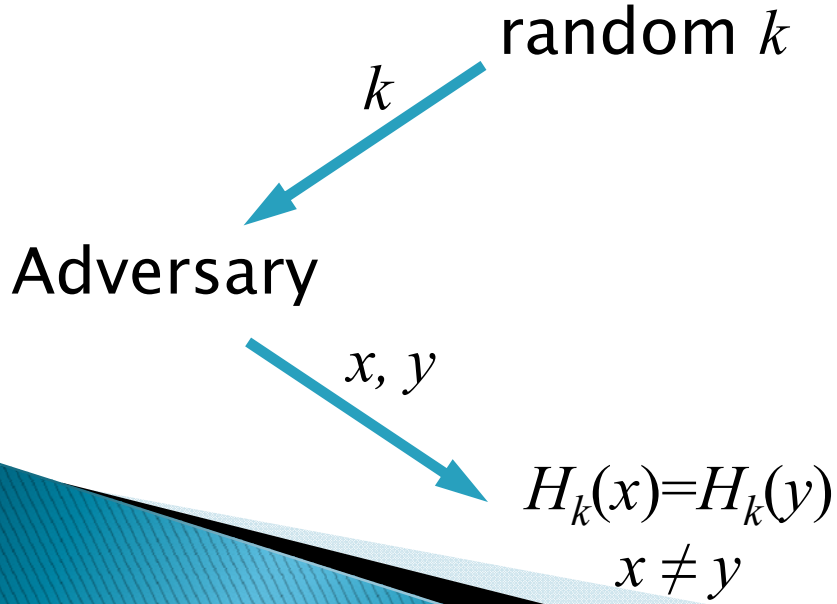
Domain extension for

enhanced target collision-resistant hash functions

Target Collision-Resistance (TCR)

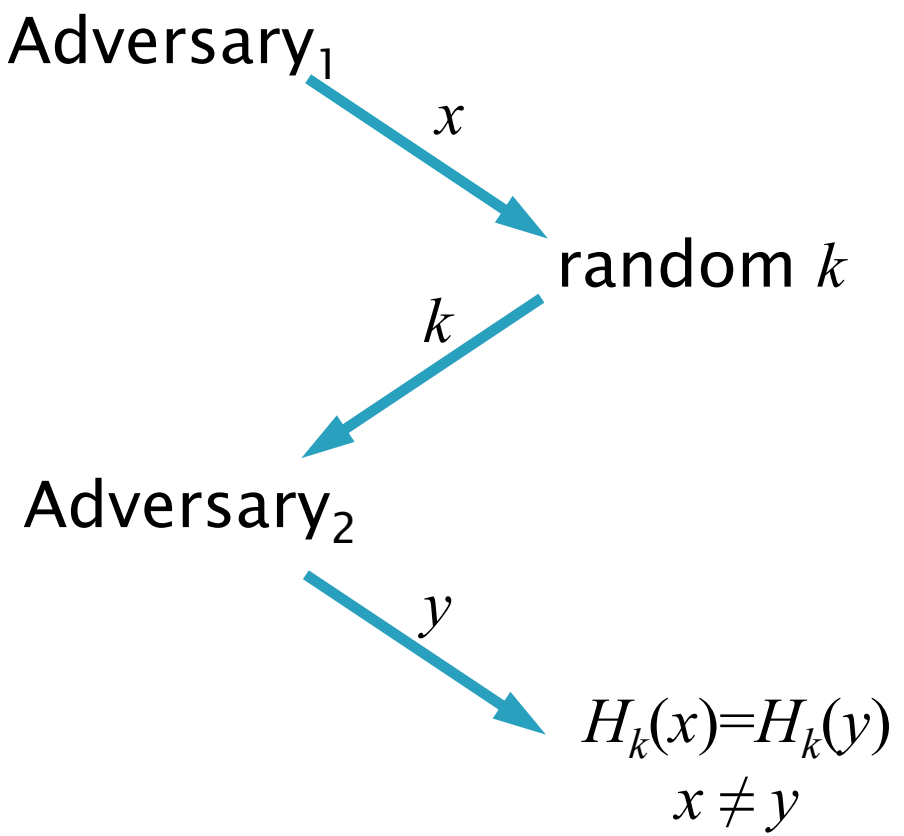
- Collision-resistance

  keyed $H_k: \{0,1\}^* \rightarrow \{0,1\}^n$



- **Target** collision-resistance

  keyed $H_k: \{0,1\}^* \rightarrow \{0,1\}^n$



[Naor-Yung'89]

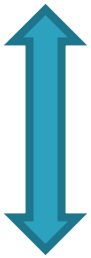
Hash-and-Sign Paradigm

Signature σ defined over fixed-length inputs
Public key PK, secret key SK

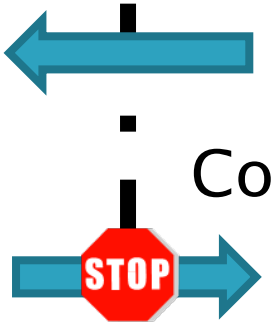
- Collision-resistance:
  - add random k to PK
  - $\sigma(H_k(M))$ is as secure as σ
- Target collision-resistance
  - generate random k for **each message**
  - $\sigma(k, H_k(M))$ is secure

Black-box Constructions

One-way functions



TCR functions
PRF, MAC, signatures,
symmetric-key encryption

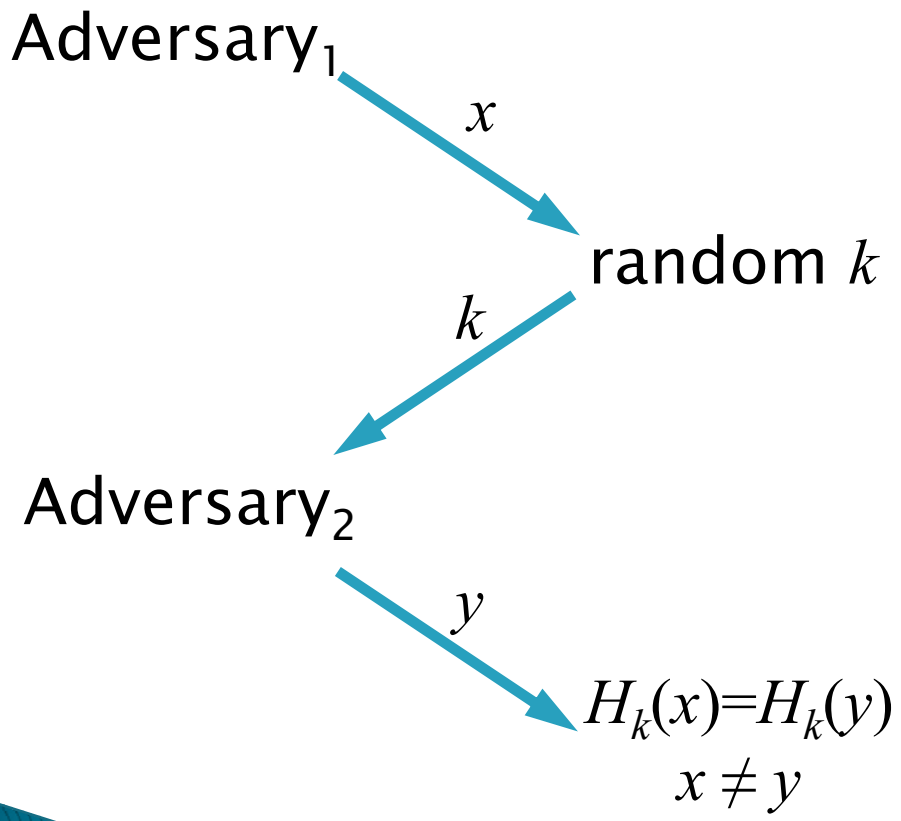


Collision-resistant functions

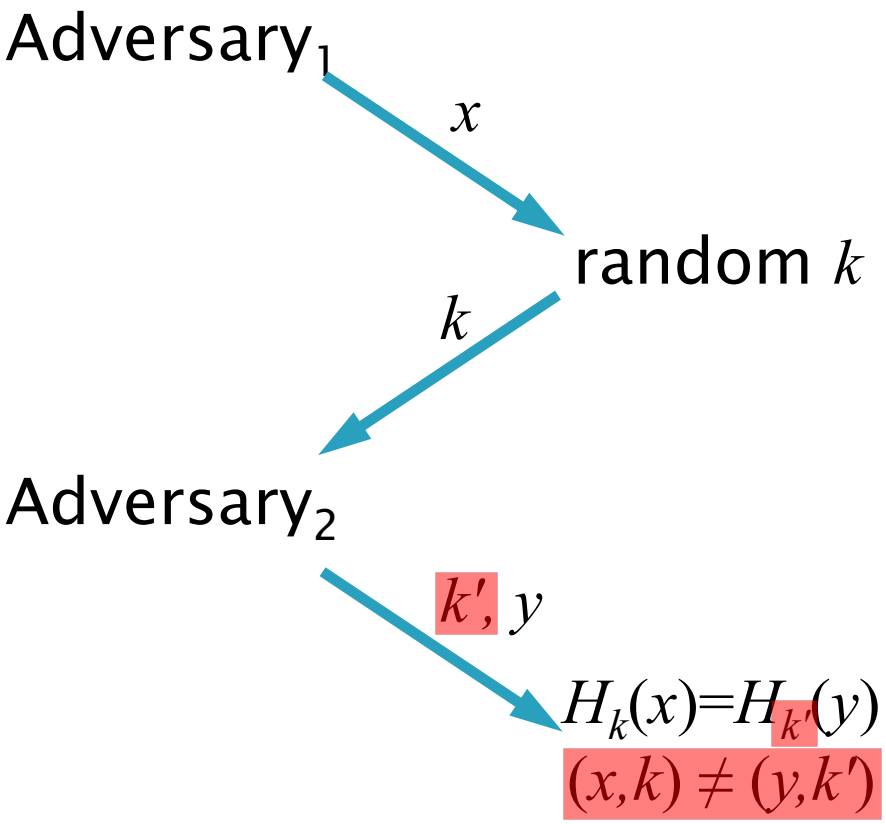
[Simon'98]

Enhanced Target Collision-Resistance

- (Plain) TCR



- **Enhanced** TCR



[Halevi-Krawczyk'06]

Hash-and-Sign Paradigm

Signature σ defined over fixed-length inputs
Public key PK, secret key SK

- TCR:
  - generate random k for each message
  - $\sigma(k, H_k(M))$ is secure
- Enhanced TCR:
  - generate random k for each message
  - $k, \sigma(H_k(M))$ is secure
- Basis of RMX
  - message pre-processing
  - retrofits existing code

[Halevi-Krawczyk'06]

SHA-3 Criteria

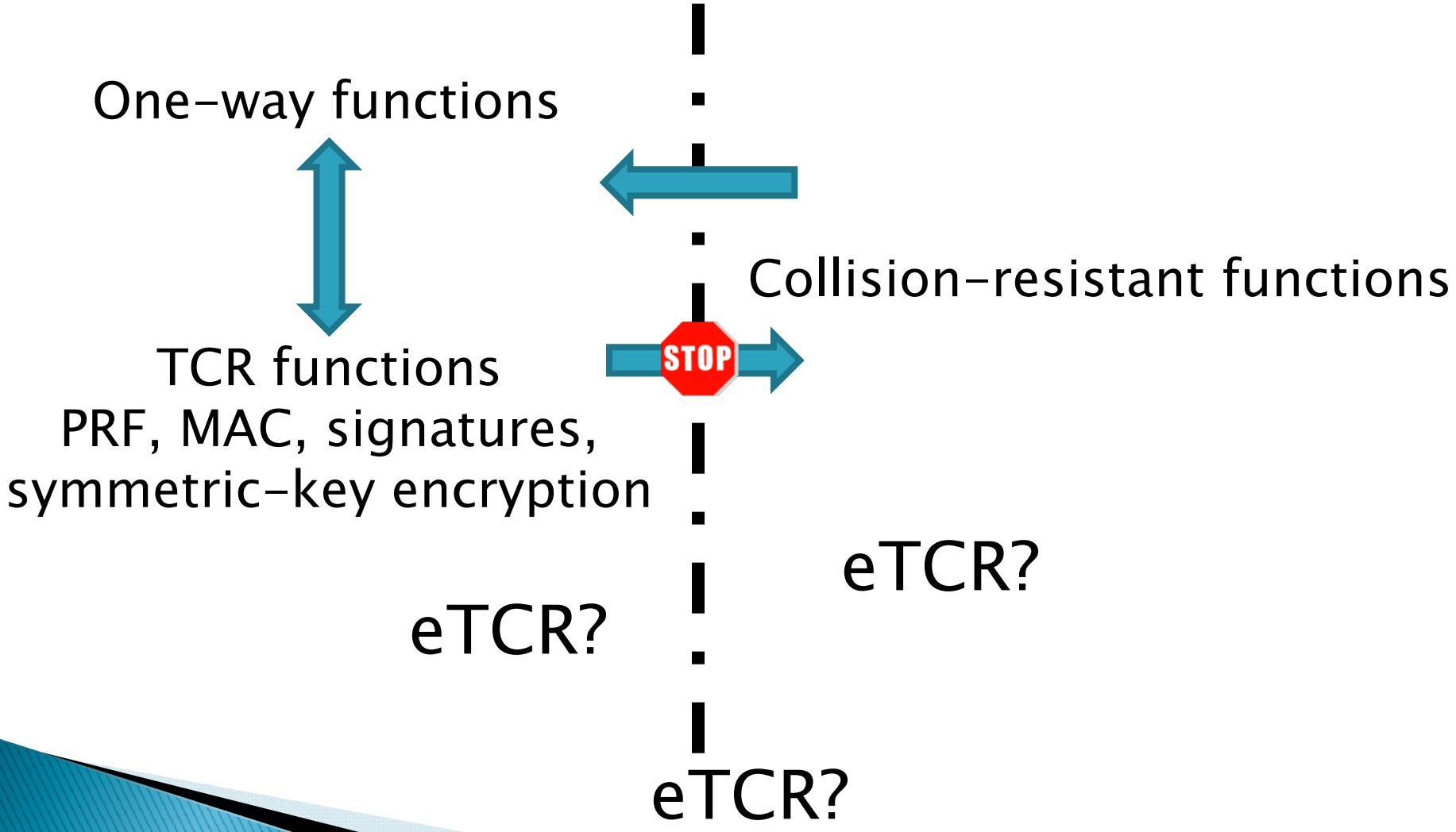
Federal Register /Vol. 72, No. 212:

- Support of HMAC, PRF
- If a construct is specified for the use of the candidate algorithm in a randomized hashing scheme, the construct must, with overwhelming probability, provide *n* bits of security against the following attack:
  - The attacker chooses a message, *M1*.
  - The specified construct is then used on *M1* with a randomization value *r1* that has been randomly chosen without the attacker's control after the attacker has supplied *M1*.
  - Given *r1*, the attacker then attempts to find a second message *M2* and randomization value *r2* that yield the same randomized hash value.

Enhanced Target Collision-Resistance


I WANT eTCR
FOR U.S. ARMY
NEAREST RECRUITING STATION

Black-box Constructions



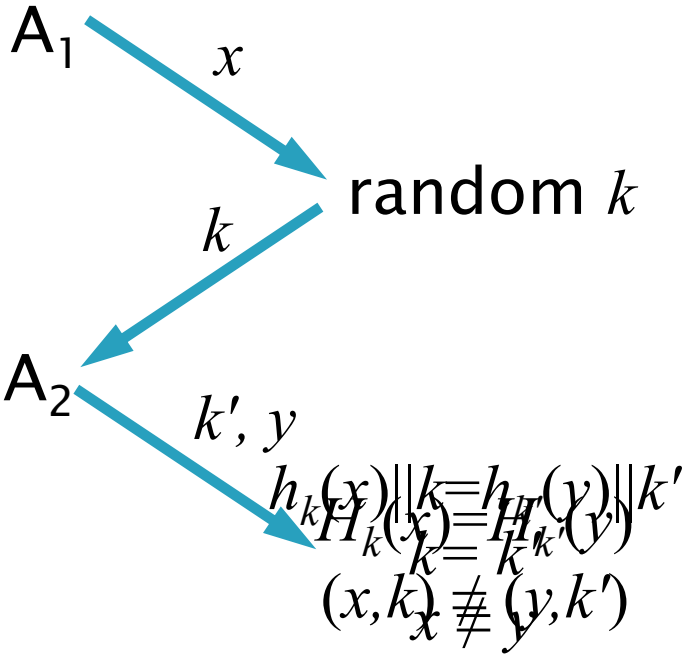
From TCR to eTCR

TCR ⟸ eTCR — by definition

TCR ⟹ eTCR

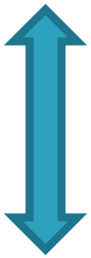
h_k—TCR

$H_k(x)=h_k(x)||k$—eTCR

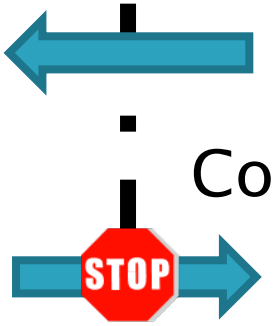


Black-box Constructions

One-way functions



TCR functions
PRF, MAC, signatures,
symmetric-key encryption
eTCR

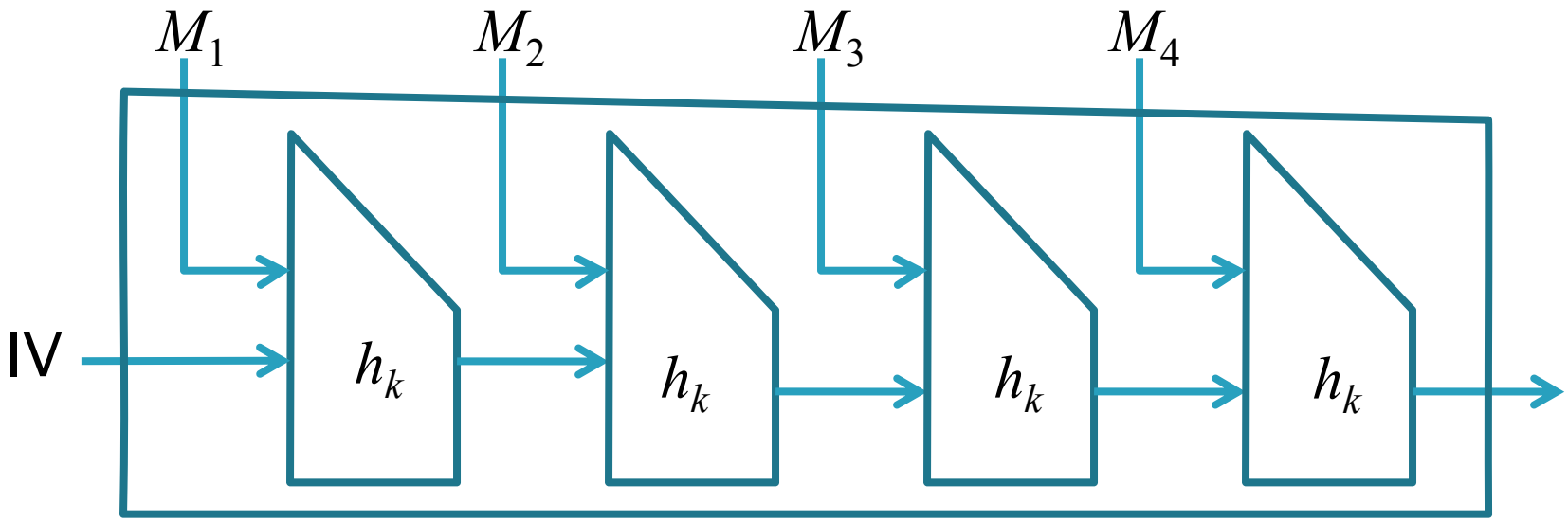


Collision-resistant functions

Domain Extension

Given $h_k: \{0,1\}^m \rightarrow \{0,1\}^n$ construct $H_K: \{0,1\}^* \rightarrow \{0,1\}^n$

Merkle-Damgård:

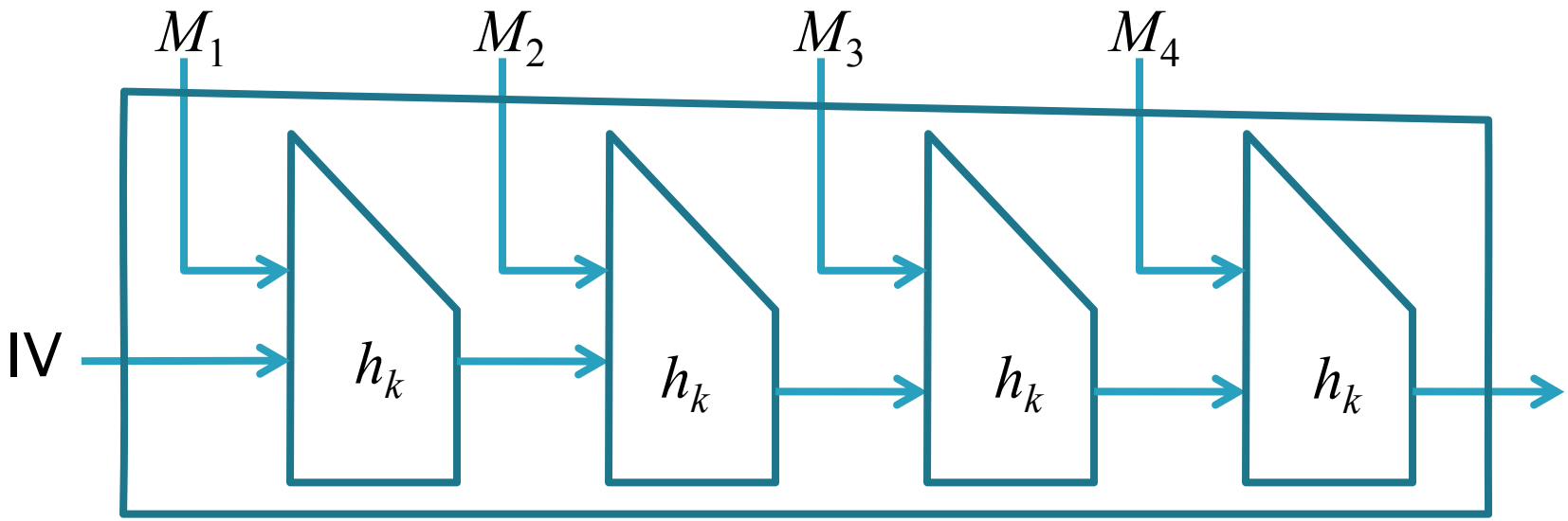


Collision-resistant

Domain Extension for TCR

Given $h_k: \{0,1\}^m \rightarrow \{0,1\}^n$ construct $H_K: \{0,1\}^* \rightarrow \{0,1\}^n$

Merkle-Damgård:



Target collision-resistant

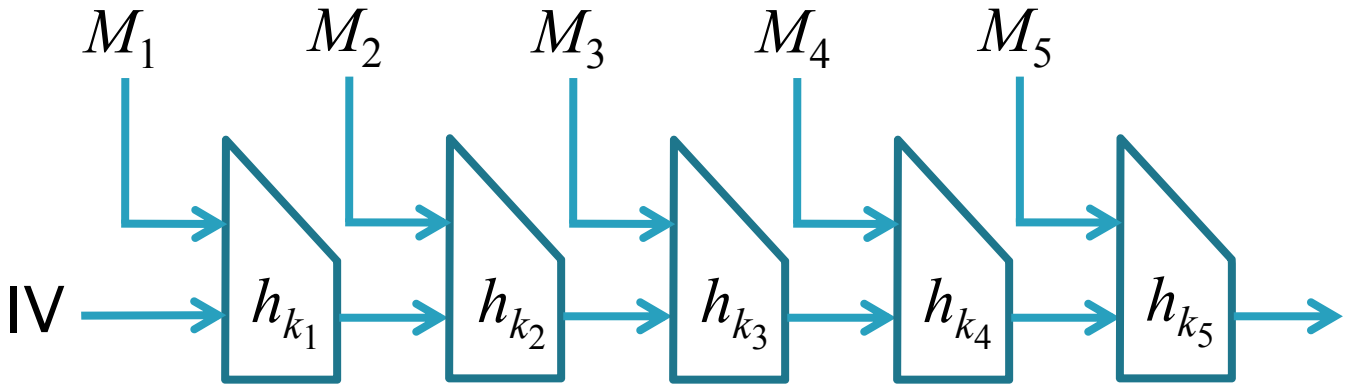
[Bellare-Rogaway'97]

Domain Extension for TCR

Linear hash:

Key: k_1, k_2, k_3, k_4, k_5

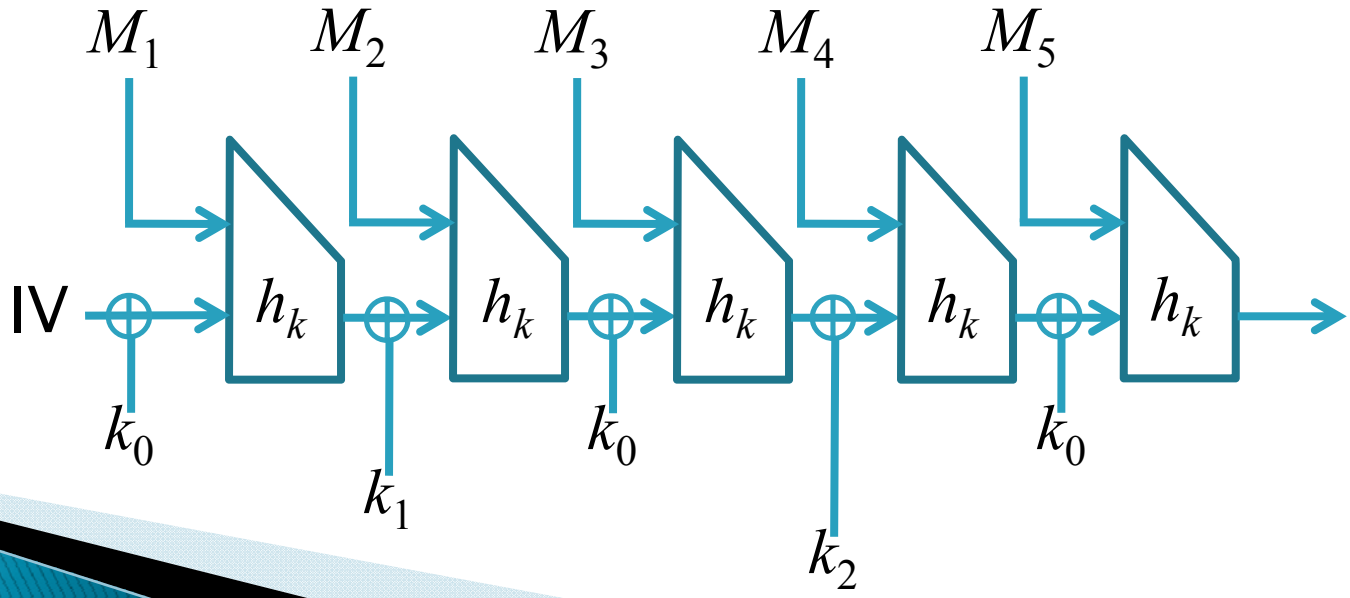
[NY89]



Shoup scheme:

Key: k, k_0, k_1, k_2

[Shoup'00]

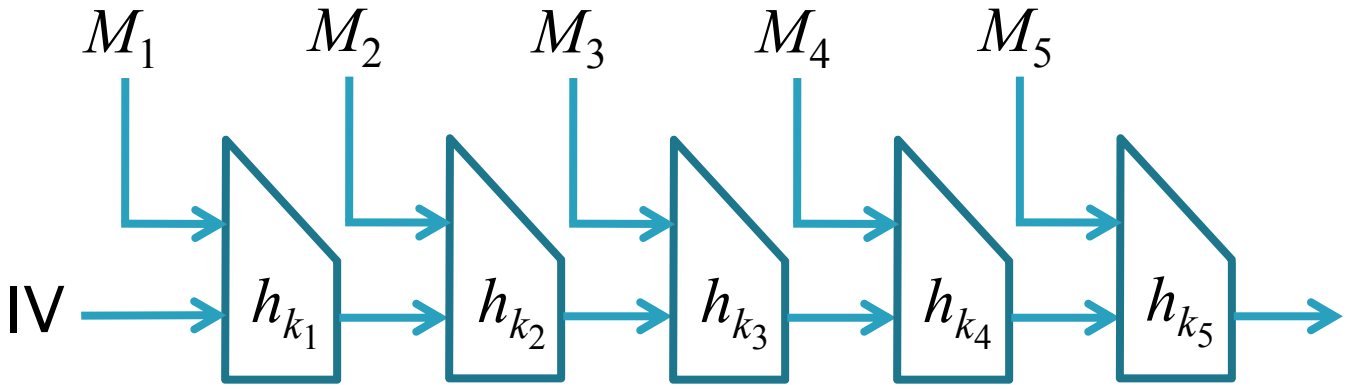


Domain Extension for eTCR

Linear hash:

Key: k_1, k_2, k_3, k_4, k_5

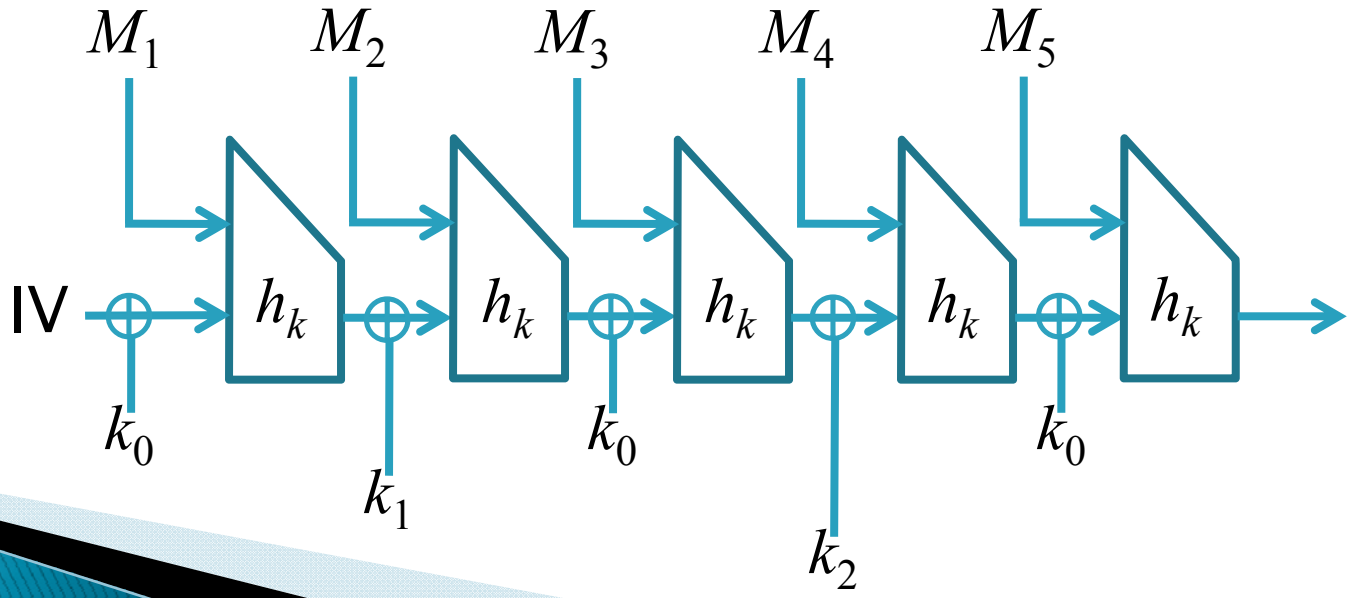
[NY89]



Shoup scheme:

Key: k, k_0, k_1, k_2

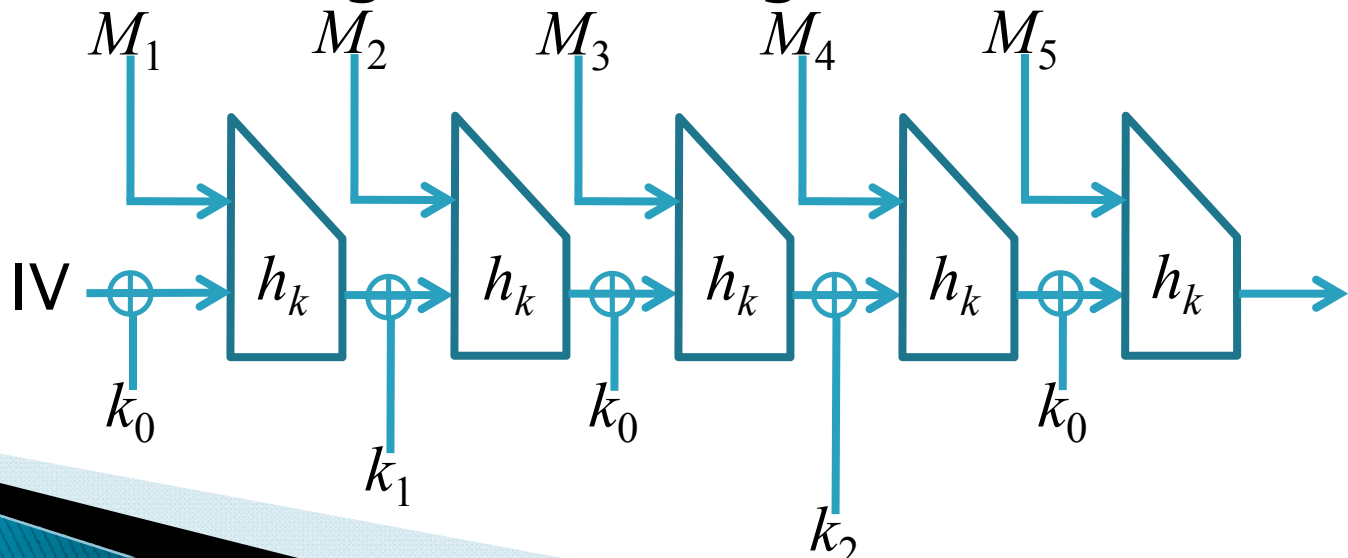
[Shoup'00]



Domain Extension for eTCR?

[RSM09] from FSE'09:

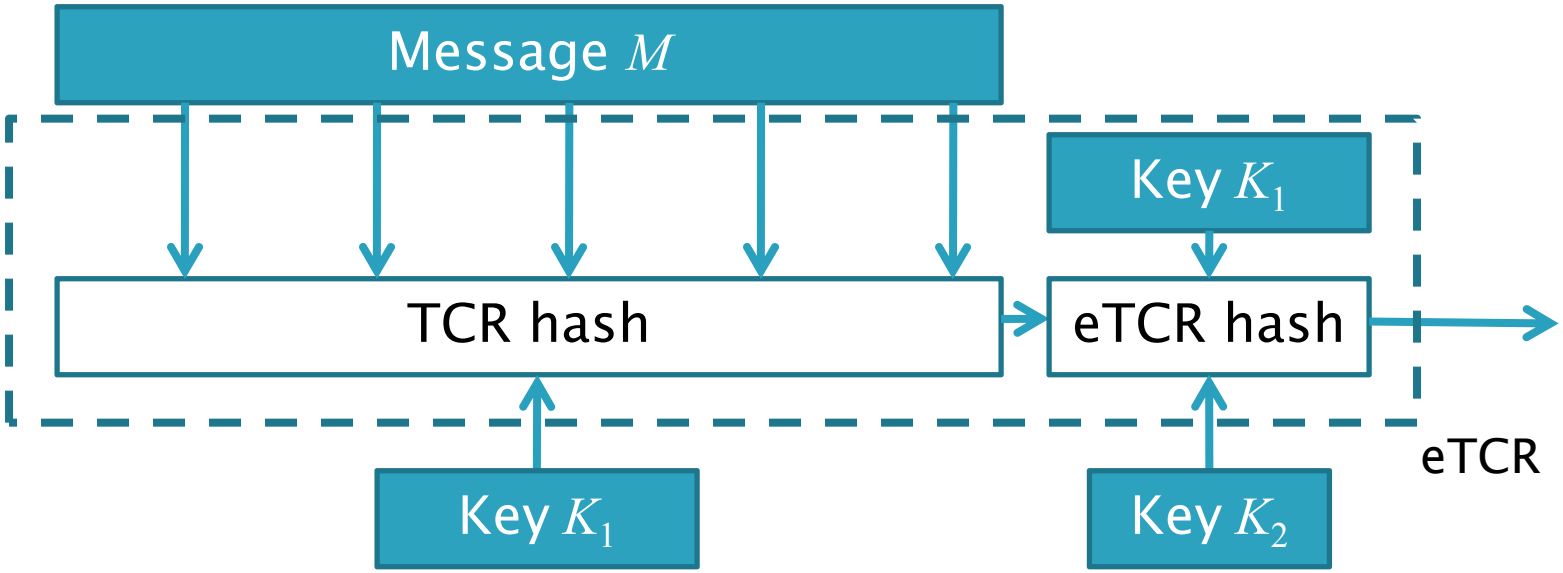
- ~~Merkle–Damgård~~
- ~~RMX~~
- ~~XOR Linear Hash~~
- ~~Shoup~~
- Linear hash (with length encoding)



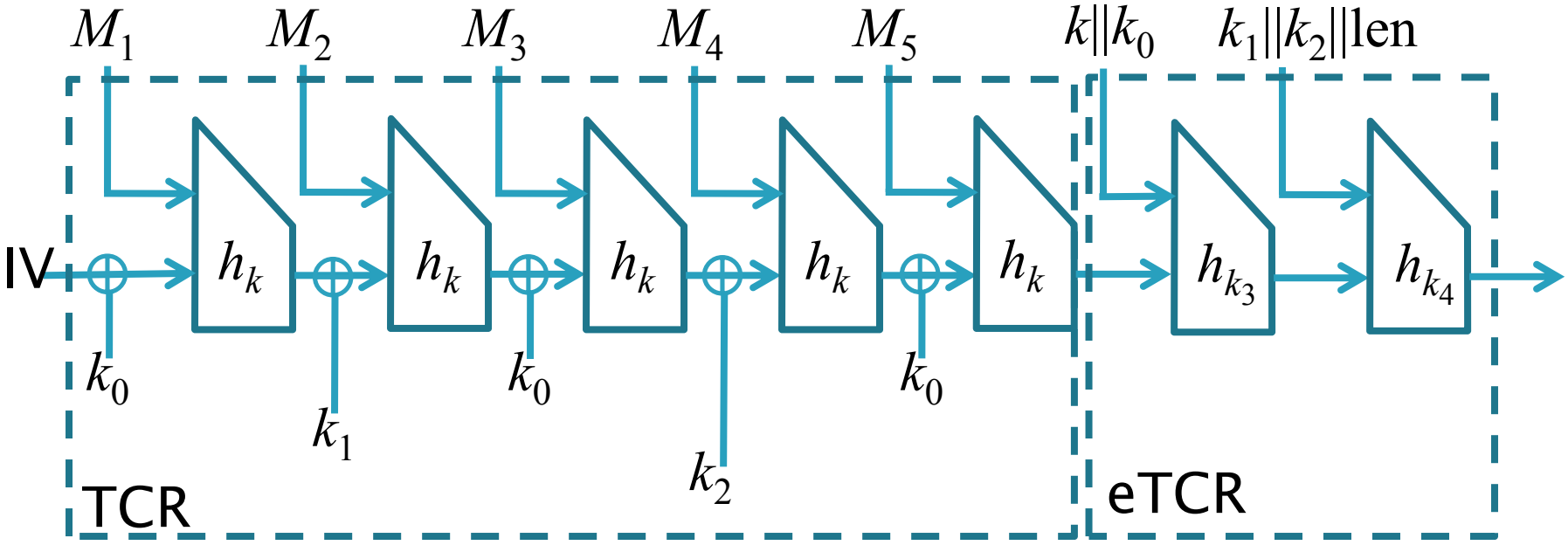
Efficient Domain Extender for eTCR?

- Linear Hash:
  - linear key expansion
  - extends eTCR
- Shoup scheme:
  - logarithmic key expansion
  - extends TCR
- If $h_k(x)$ is TCR, then $h_k(x)||k$ is eTCR…

Main Construction



Instantiation



Subtleties:

- Length encoding
- IV

Outline

Domain extension for

enhanced target collision-resistant hash functions

Summary

- eTCR is interesting and appealing property
- Domain extension scheme with logarithmic key blowup
- Open questions:
  - More efficient domain extension?
  - Impossibility results
  - Attacks on the eTCR property of SHA-3 candidates