# Short Digital Signatures and ID-KEMs via Truncation Collision Resistance

Tibor Jager
Paderborn University

Rafael Kurek
Paderborn University

# Contributions

- New security notion for standard Hash Functions
  - Truncation-Collision Resistance
- New Digital Signature scheme and ID-KEM
  - From selective to full security in Standard Model
  - Solving open problem: single element in prime order group

# Random Oracle Model [BR93]

"Cryptographic Hash Function modelled as truly random function"

- (Simple) proofs ✅
- Strong security properties ✅
  - Short, full secure signatures [BLS01, BB04]
  - Short, full secure ID-KEMs [BF01, BB04]

# Random Oracle Model [BR93]

"Cryptographic Hash Function modelled as truly random function"

- (Simple) proofs ✅
- Strong security properties ✅
  - Short, full secure signatures [BLS01, BB04]
  - Short, full secure ID-KEMs [BF01, BB04]
- Unclear security guarantees for implementations [CGH02] ❌
- Unclear which security property required ❌

# Random Oracle Model [BR93]

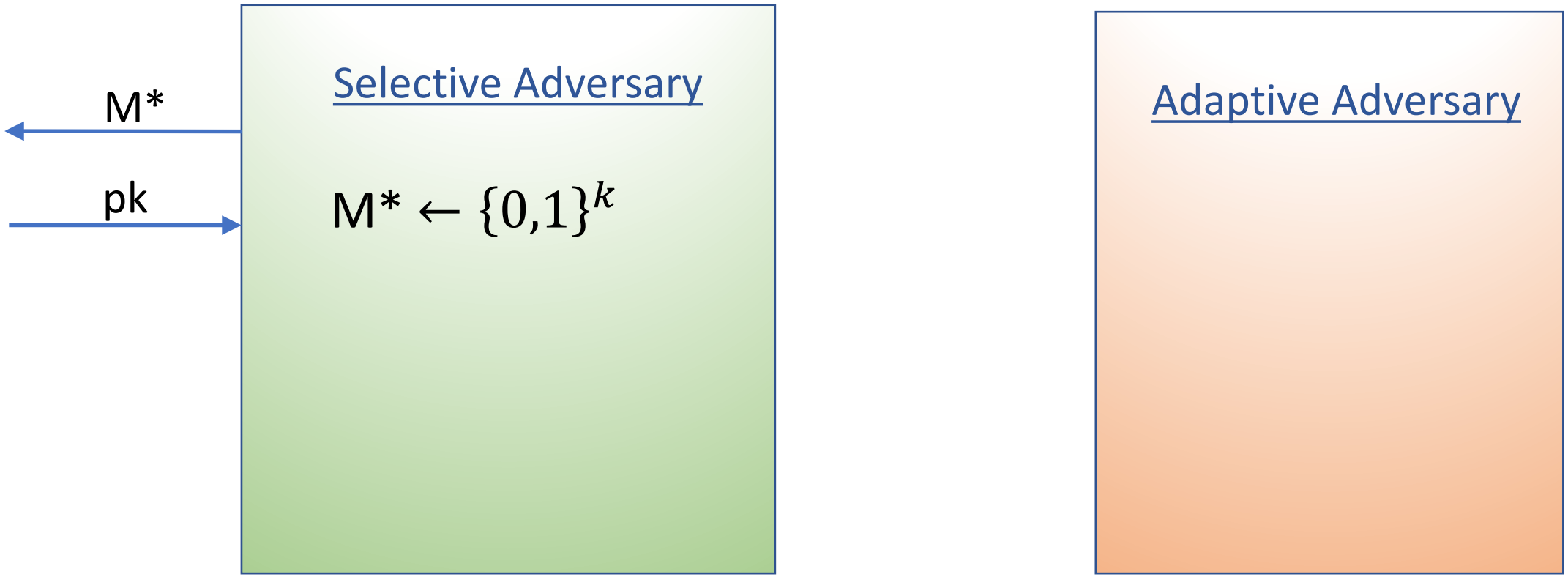
"Cryptographic Hash Function modelled as truly random function"

- (Simple) proofs ✅
- Strong security properties ✅
  - Short, full secure signatures [BLS01, BB04]
  - Short, full secure ID-KEMs [BF01, BB04]
- Unclear security guarantees for implementations [CGH02] ❌
- Unclear which security property required ❌

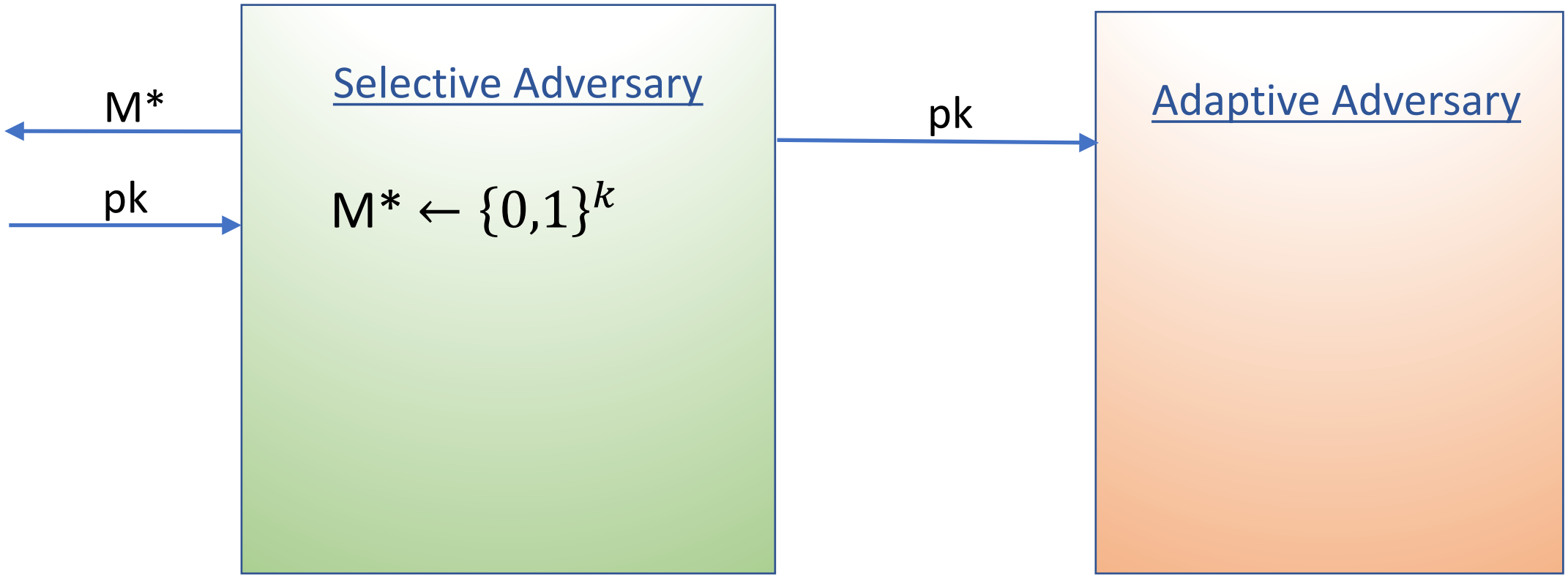
Looking for reasonable complexity assumption on standard Cryptographic Hash Functions to avoid ROM

# Problem of turning selective into adaptive security

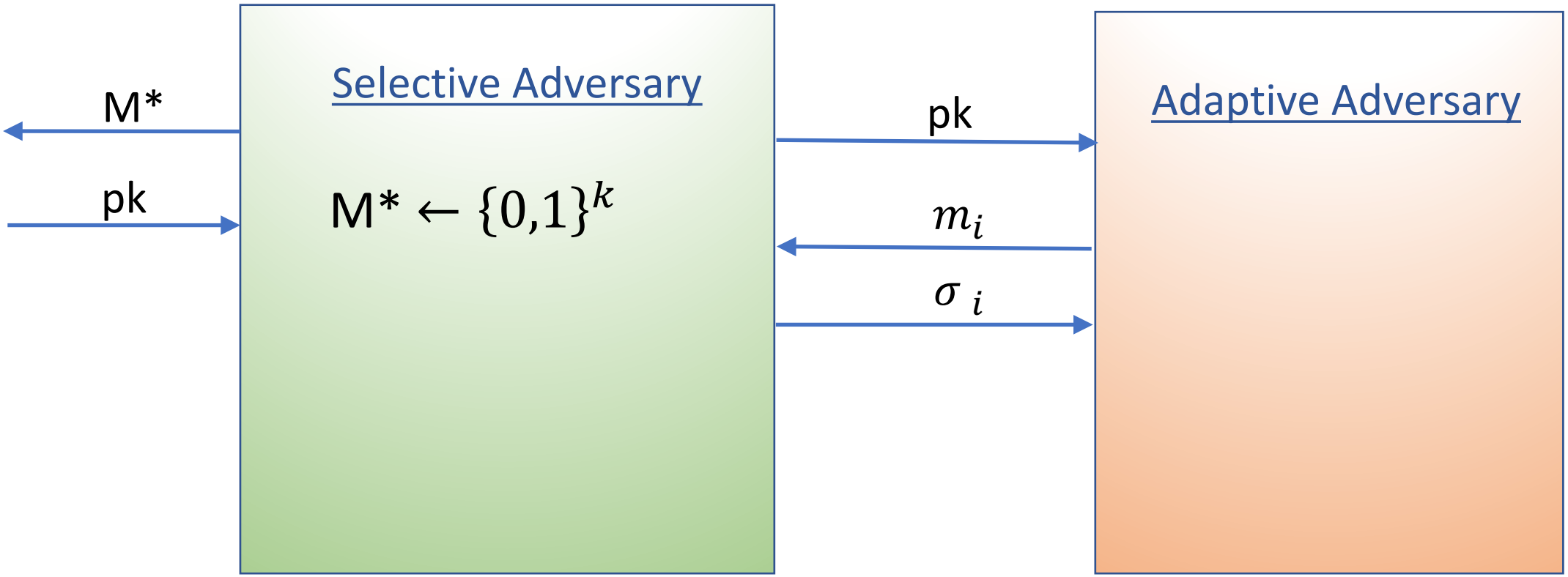
# Problem of turning selective into adaptive security



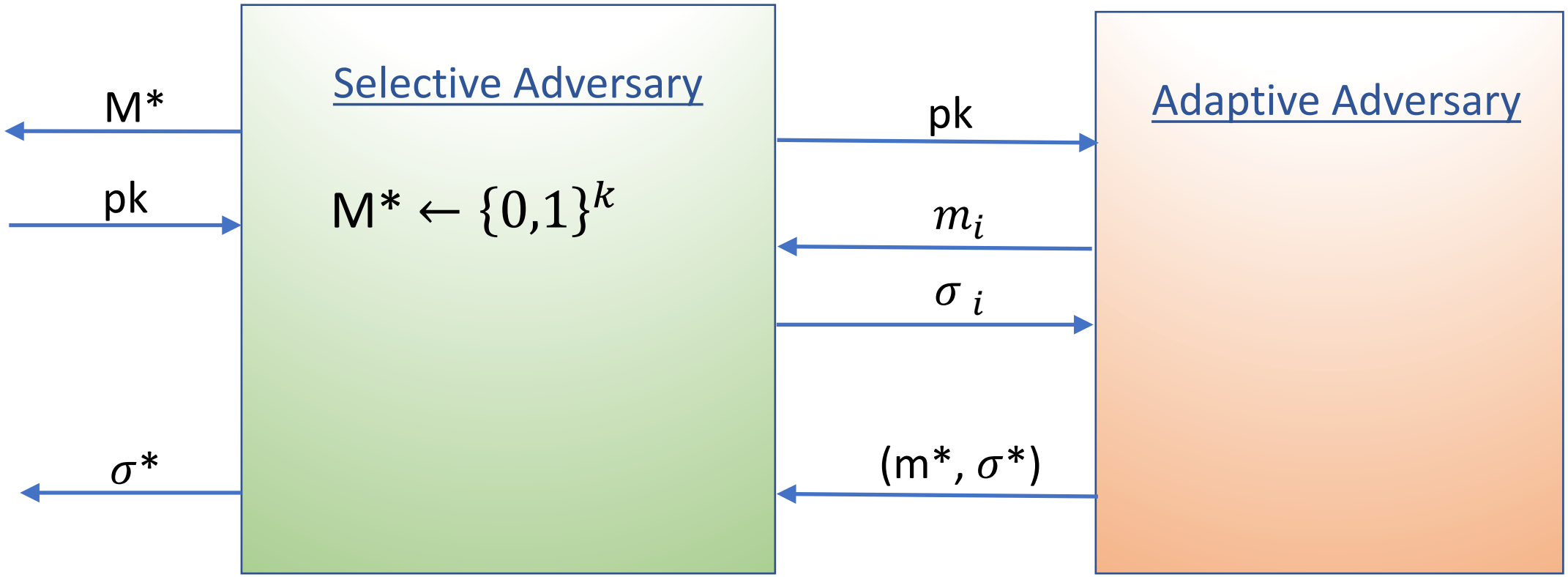
# Problem of turning selective into adaptive security



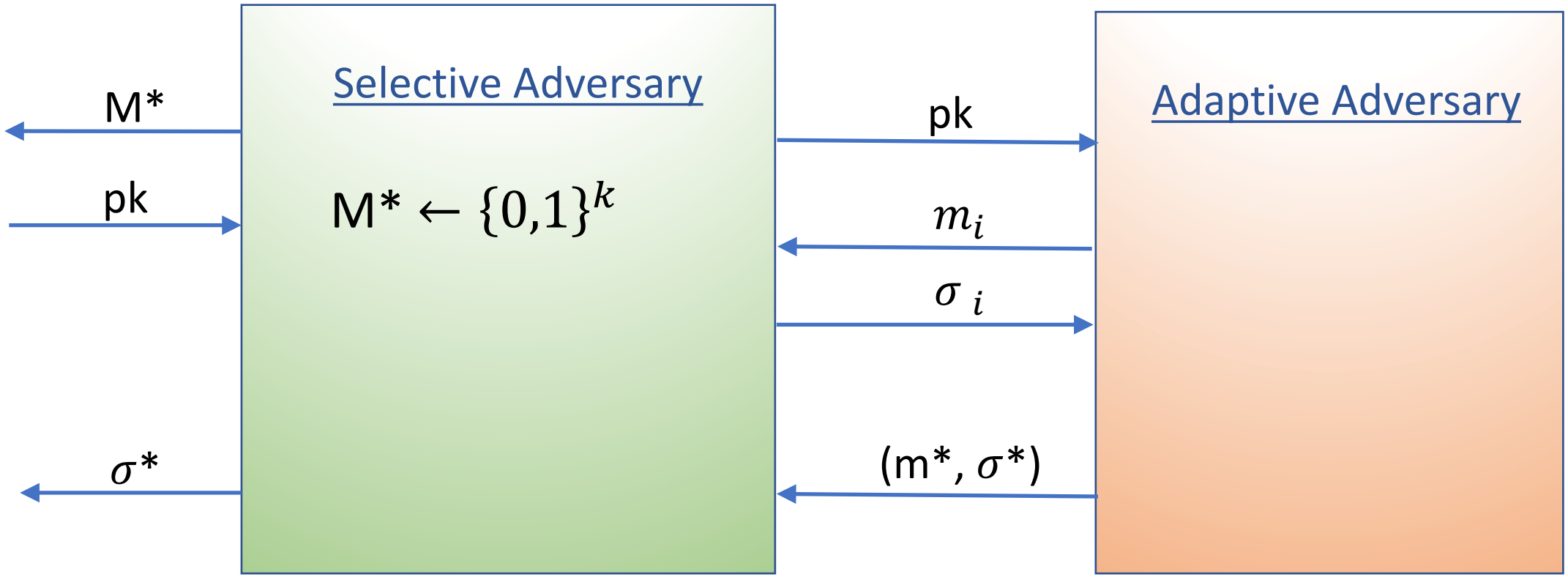
# Problem of turning selective into adaptive security



# Problem of turning selective into adaptive security



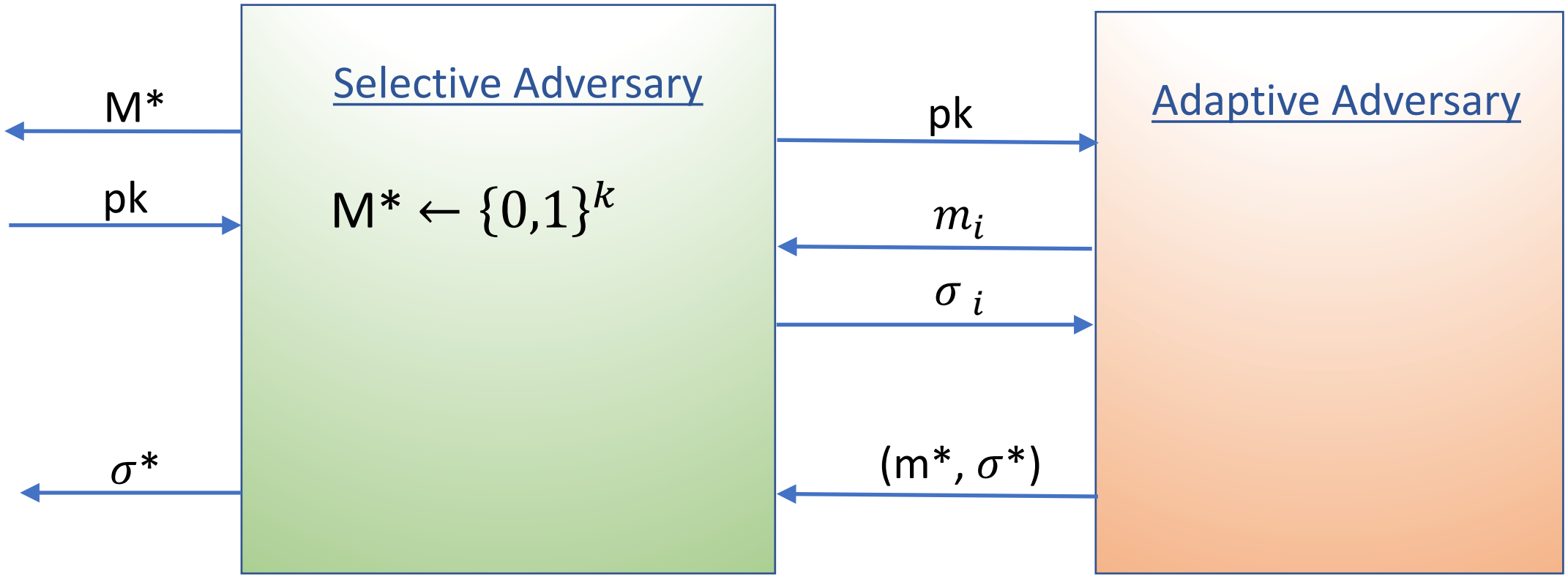
# Problem of turning selective into adaptive security




$$M^* = m^*$$

$$M^* \neq m_i \; \forall \; i$$

# Problem of turning selective into adaptive security




ROM:

$$\varepsilon_{Selective} \approx poly(k)^{-1} \cdot \varepsilon_{adaptive}$$

Standard:

$$\varepsilon_{selective} \approx 2^{-k} \cdot \varepsilon_{adaptive}$$

# Collision Resistance

# Collision Resistance

A Hash function H is Collision Resistant if

$$\Pr[\text{ A finds collision }] < \text{negl}(k)$$

for all ppt adversaries A.

# Truncation Collision Resistance

# Truncation Collision Resistance

A Hash function H is Truncation-Collision Resistant if

$$\Pr[\text{ A finds collision for prefix of length i }] < \frac{t(t-1)}{2^{i+1}}$$

for all probabilistic t-time adversaries A.

# Truncation Collision Resistance

A Hash function H is Truncation-Collision Resistant if

$$\Pr[\text{ A finds collision for prefix of length i }] < \frac{t(t-1)}{2^{i+1}}$$

for all probabilistic t-time adversaries A.

(Related to birthday bound)

# Main property

H(x)= 10100110001110001111011100110011011100010

# Main property

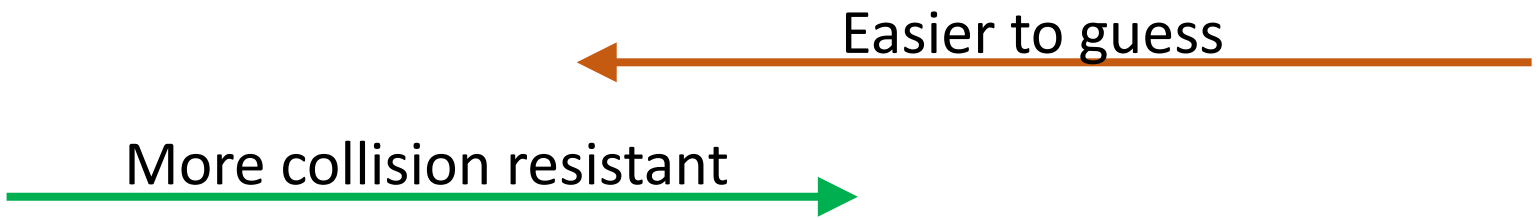
H(x)= 10100110001110001111011100110011011000 10

# Main property

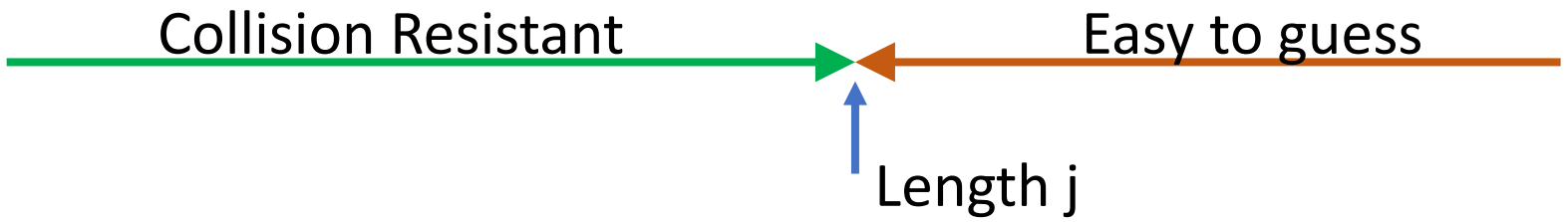
H(x)= 10100110001110001111011100110011011100010


# Main property

H(x)= 10100110001110001111011100110011011000 10




For every adversary A there exists a prefix length j s.t.

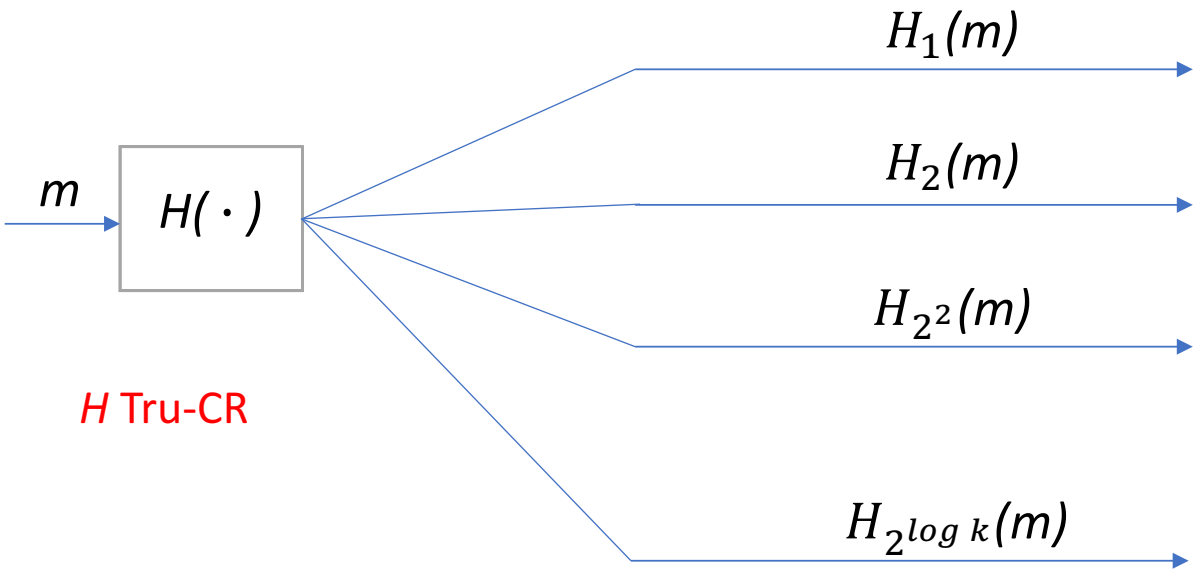


# Generic construction

## from selective to adaptive secure signatures without ROM

# Generic construction

## from selective to adaptive secure signatures without ROM

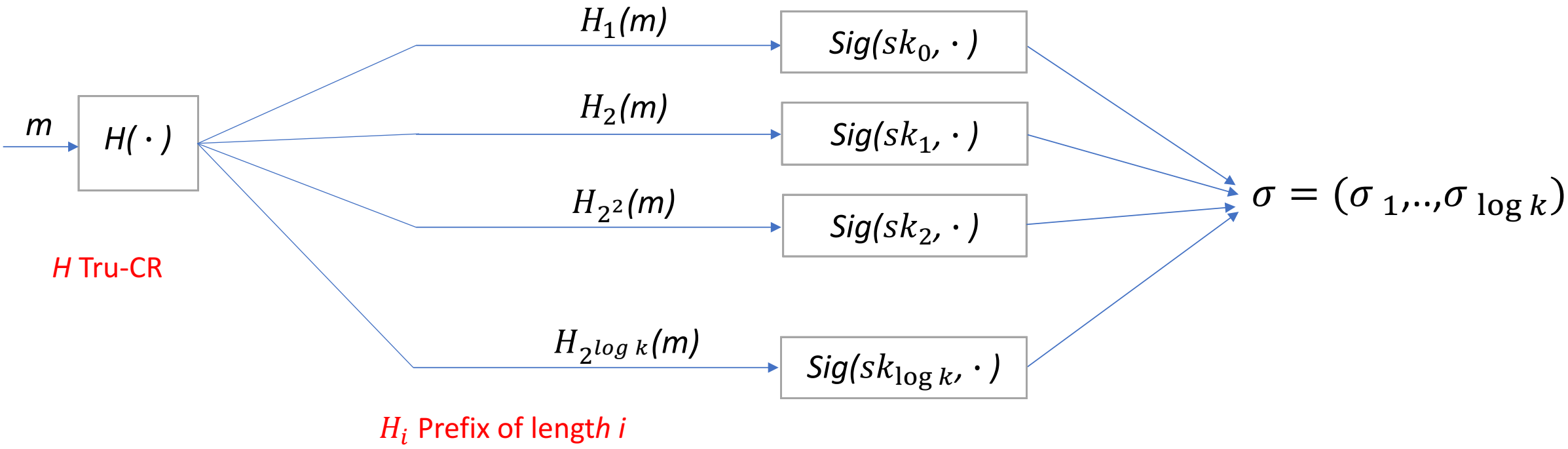



*H* Tru-CR

$H_i$ Prefix of length *i*

# Generic construction

## from selective to adaptive secure signatures without ROM




*H* Tru-CR

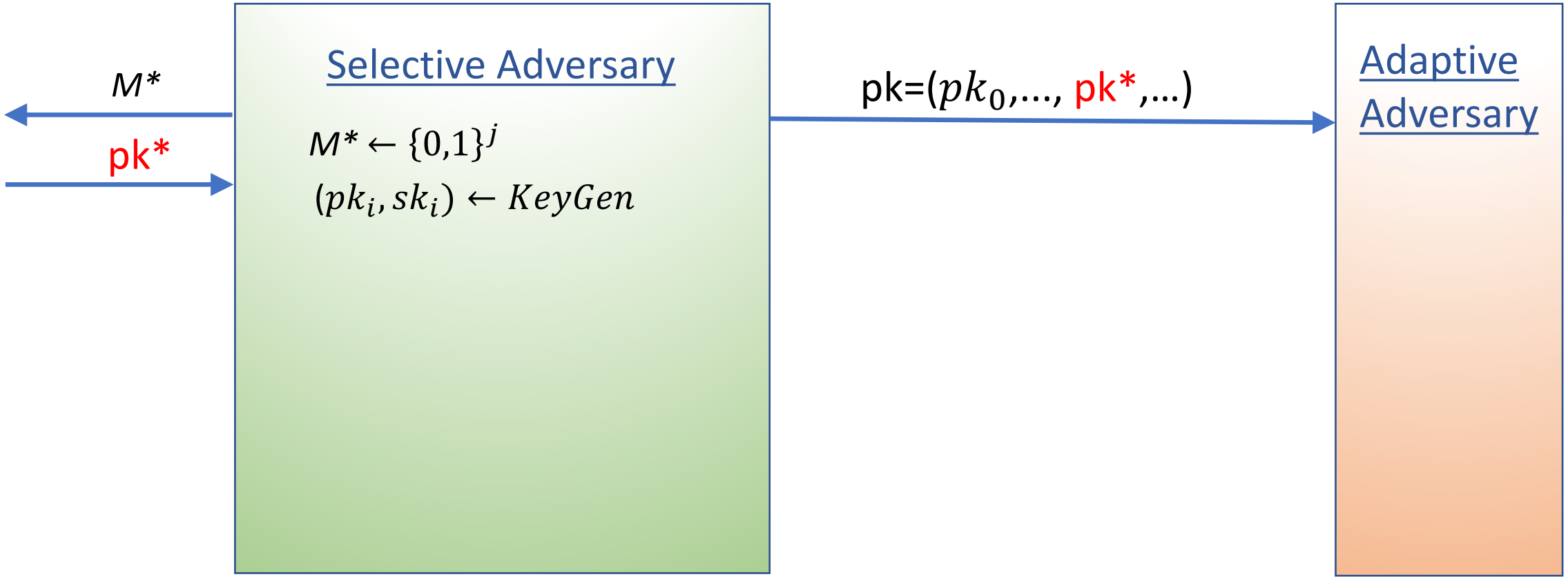
$H_i$ Prefix of length *i*

*Sig selective* secure

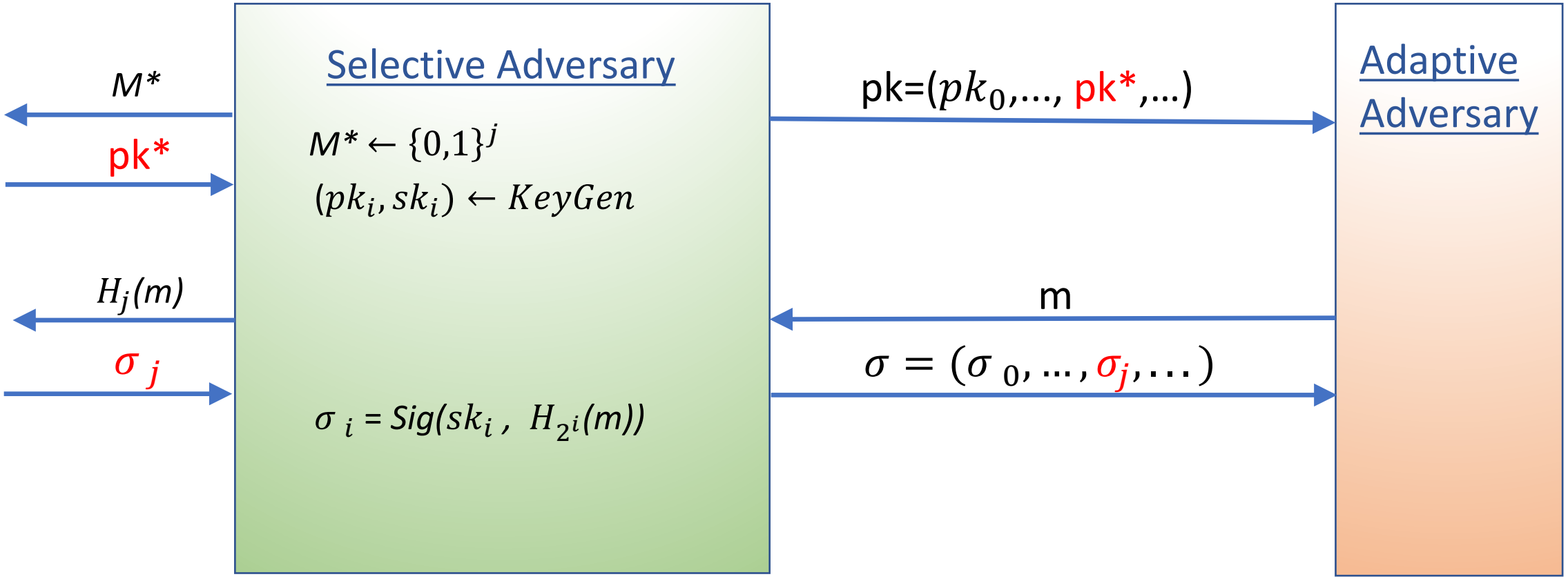
# Proof sketch

# Proof sketch

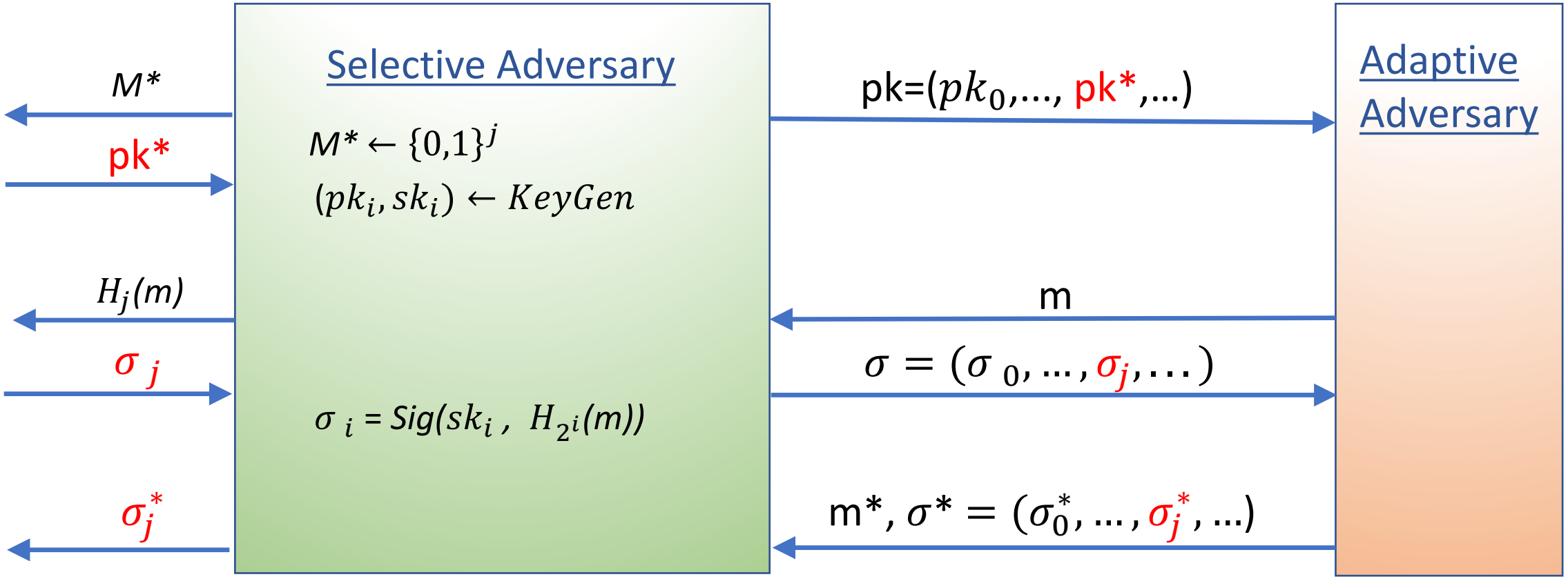
# Proof sketch



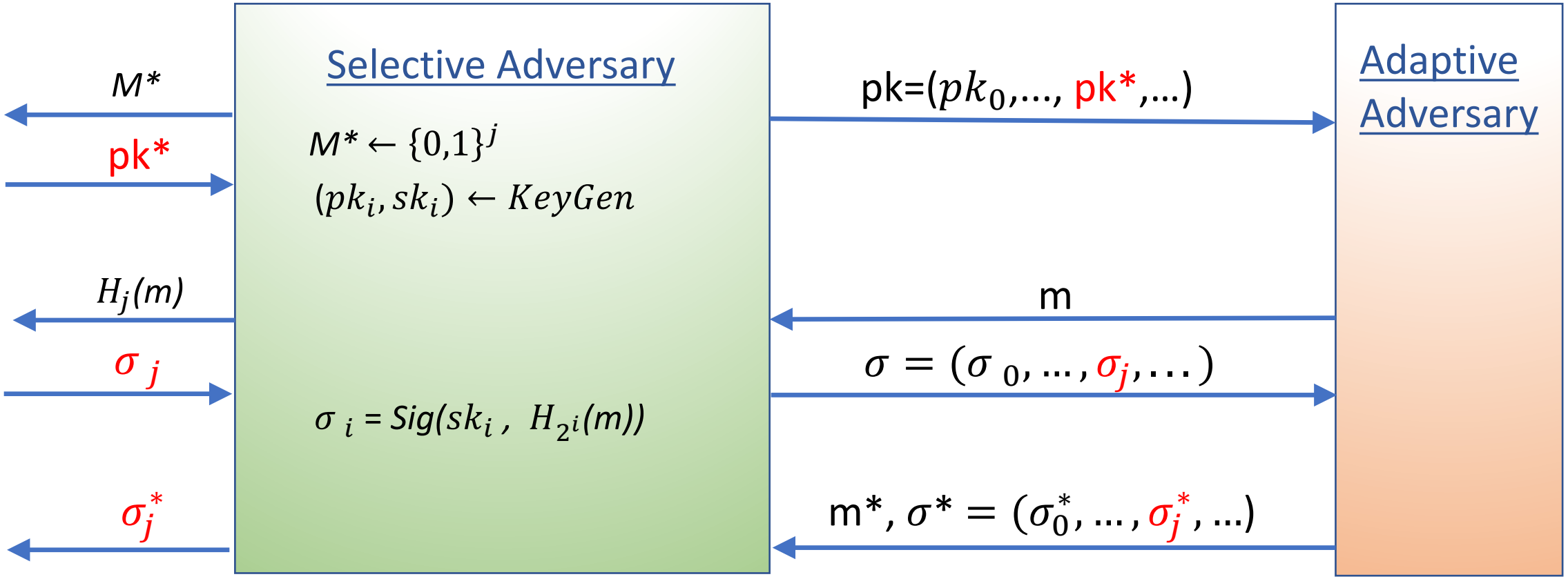
# Proof sketch



# Proof sketch



# Proof sketch




Truncation-CR: Guess of $H_j(m^*)$? ✅
No collision? ✅

## In this talk

- Turning weak secure Digital Signature scheme into full secure without ROM

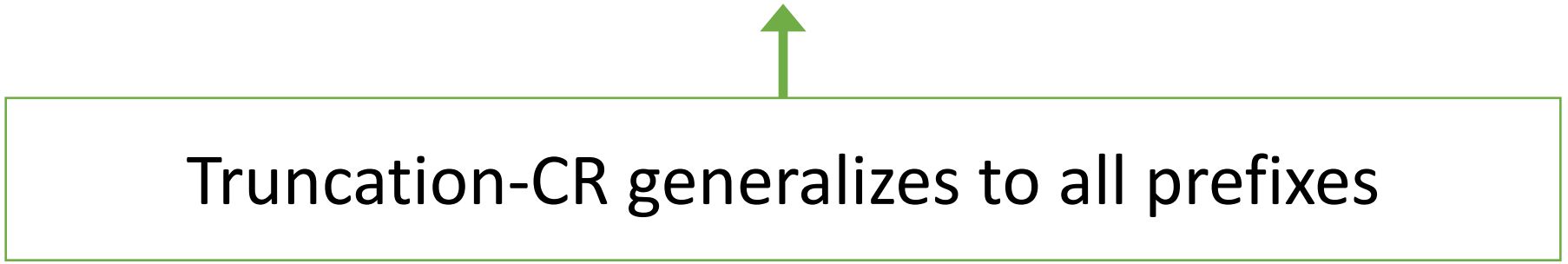
## In the paper

- From “selective and non-adaptive” to full adaptive security
- Same approach for ID-KEM
- Single element constructions due to aggregation of Boneh and Boyen signature scheme (ID-KEM resp.):

$$\sigma = \left( g^{\frac{1}{x_0 + H_1(m)}} \right)^{\prod_{i=1}^{\log k} \frac{1}{x_i + H_{2^i}(m)}}$$

# Truncation-CR assumption

- Truncated versions of SHA-256 and SHA-512 have been standardized by NIST (224 or 384 bits)
- SHA-3 standard defines extendable-output-functions (XOFs), where output length can be adapted to any desired length
- Standard way to choose hash function with “k-bit security”: 2k-bit output length.
  - essentially assuming: no significantly better collision attack than generic birthday algorithm exists



# Contributions

- New security notion for standard Hash Functions
  - Truncation-Collision Resistance
- New Digital Signature scheme and ID-KEM
  - From selective to full security in Standard Model
  - Solving open problem: single element in prime order group

# Future work

- Construction of Tru-CR Hash Function (sketch in full version)
- Further useful applications

# Thank you for your attention!

eprint.iacr.org/2017/061

# Related work

- Oracle Hashing [Canetti, CRYPTO 1997]
- Programmable HF [Hofheinz and Kiltz, CRYPTO 2008]
- UCE [Bellare et al., CRYPTO 2013]
- ICE [Farshim and Mittelbach, FSE 2016]
- ELF [Zhandry, CRYPTO 2016]