Towards Tight Security Bounds for OMAC, XCBC and TMAC

Soumya Chattopadhyay Ashwin Jha Mridul Nandi

IACR Asiacrypt 2022
Taipei, Taiwan

December 7, 2022

https://ia.cr/2022/1234

Towards Tight Security Bounds for OMAC, XCBC and TMAC

Towards Tight Security Bounds for OMAC, XCBC and TMAC

- MACs and their security

Towards Tight Security Bounds for **OMAC, XCBC and TMAC**

- MACs and their security
- CBC-MACs: XCBC, TMAC, OMAC

Towards Tight **Security Bounds for OMAC, XCBC and TMAC**

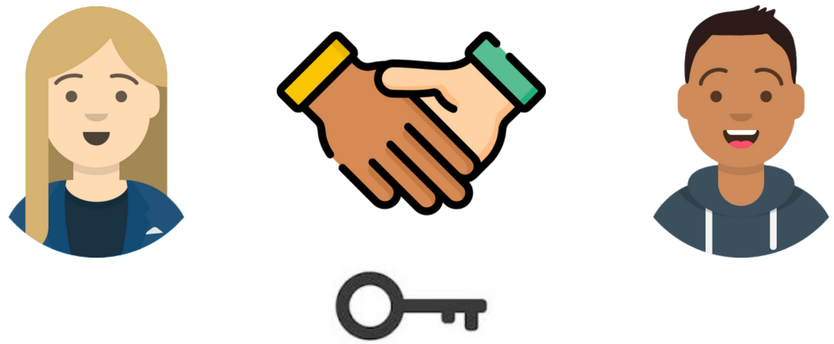
- MACs and their security
- CBC-MACs: XCBC, TMAC, OMAC
- Observations on their security

Towards Tight Security Bounds for OMAC, XCBC and TMAC

- MACs and their security
- CBC-MACs: XCBC, TMAC, OMAC
- Observations on their security
- A step towards tight security

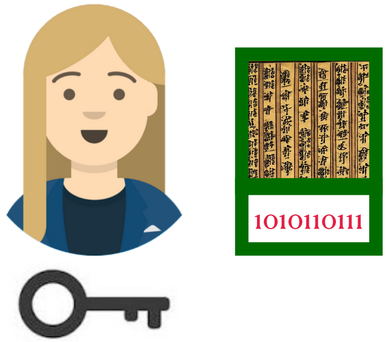
Message Authentication Codes (MAC)

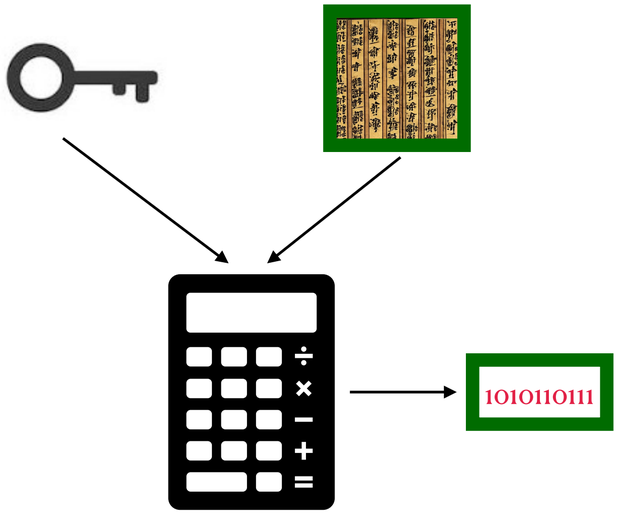
Message Authentication Codes (MAC)



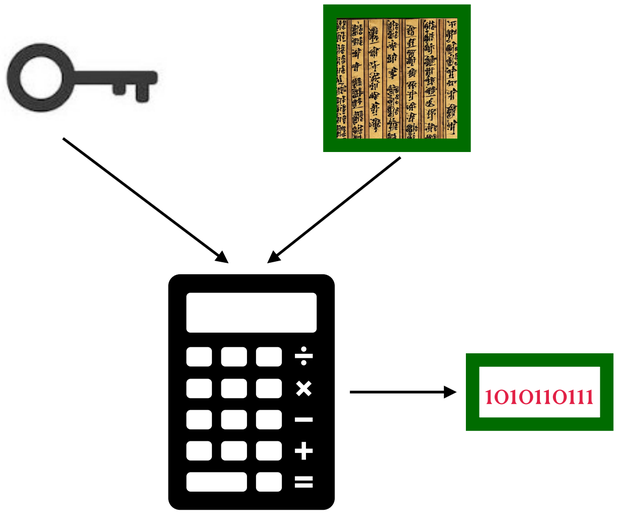
Message Authentication Codes (MAC)

Message Authentication Codes (MAC)

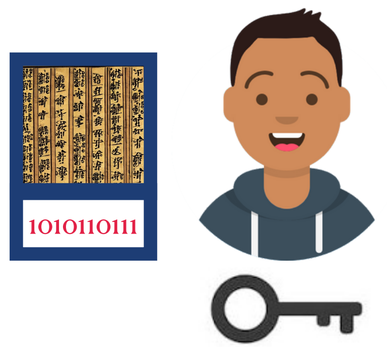


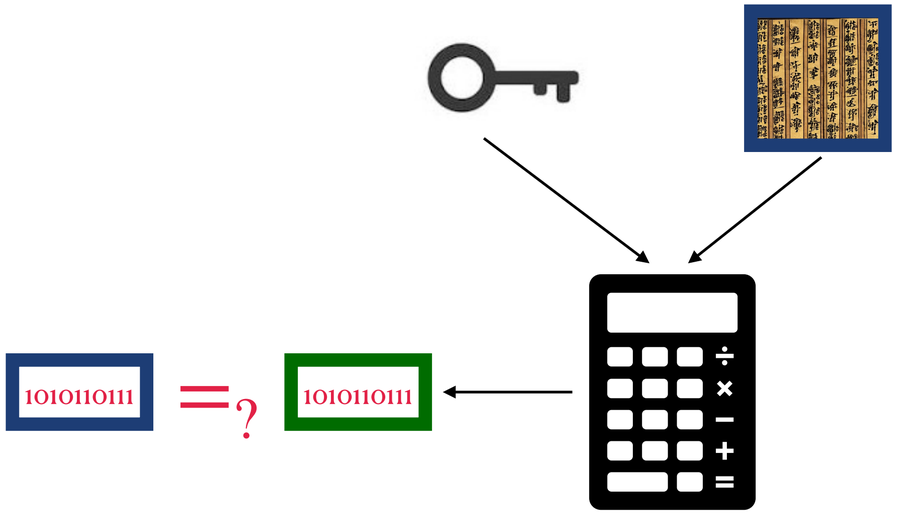


Message Authentication Codes (MAC)



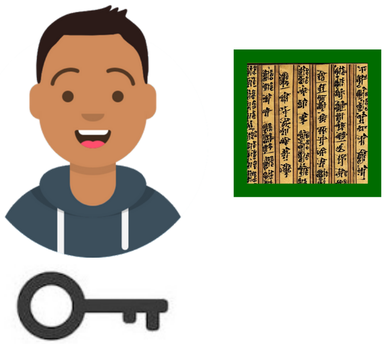
Message Authentication Codes (MAC)

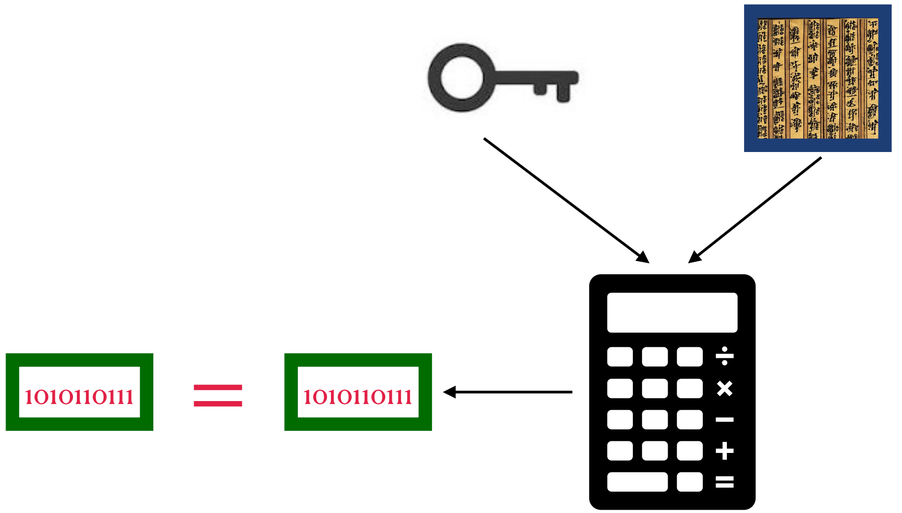




Message Authentication Codes (MAC)

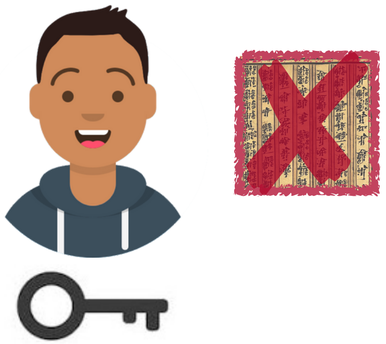
Authentication Succeeds

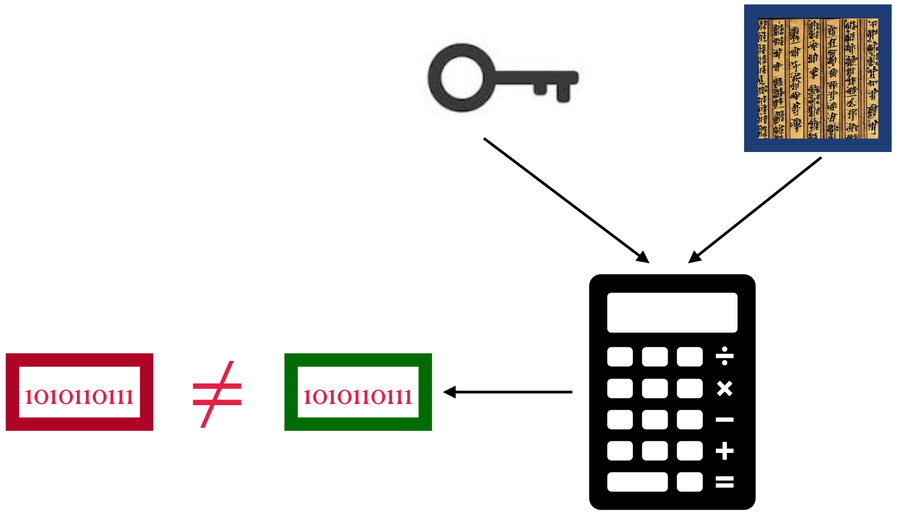




Message Authentication Codes (MAC)

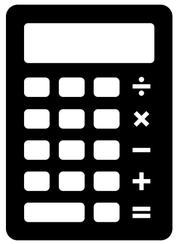
Authentication Fails





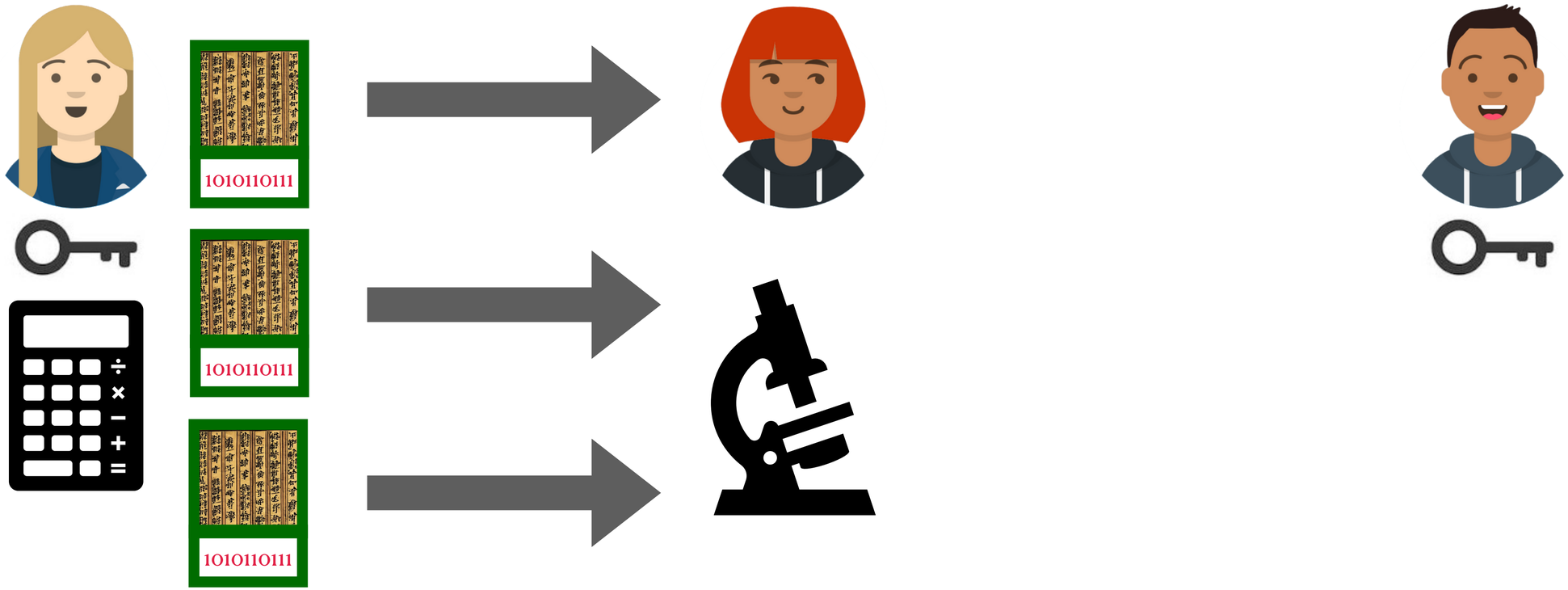
MAC Security

Unforgeability Game



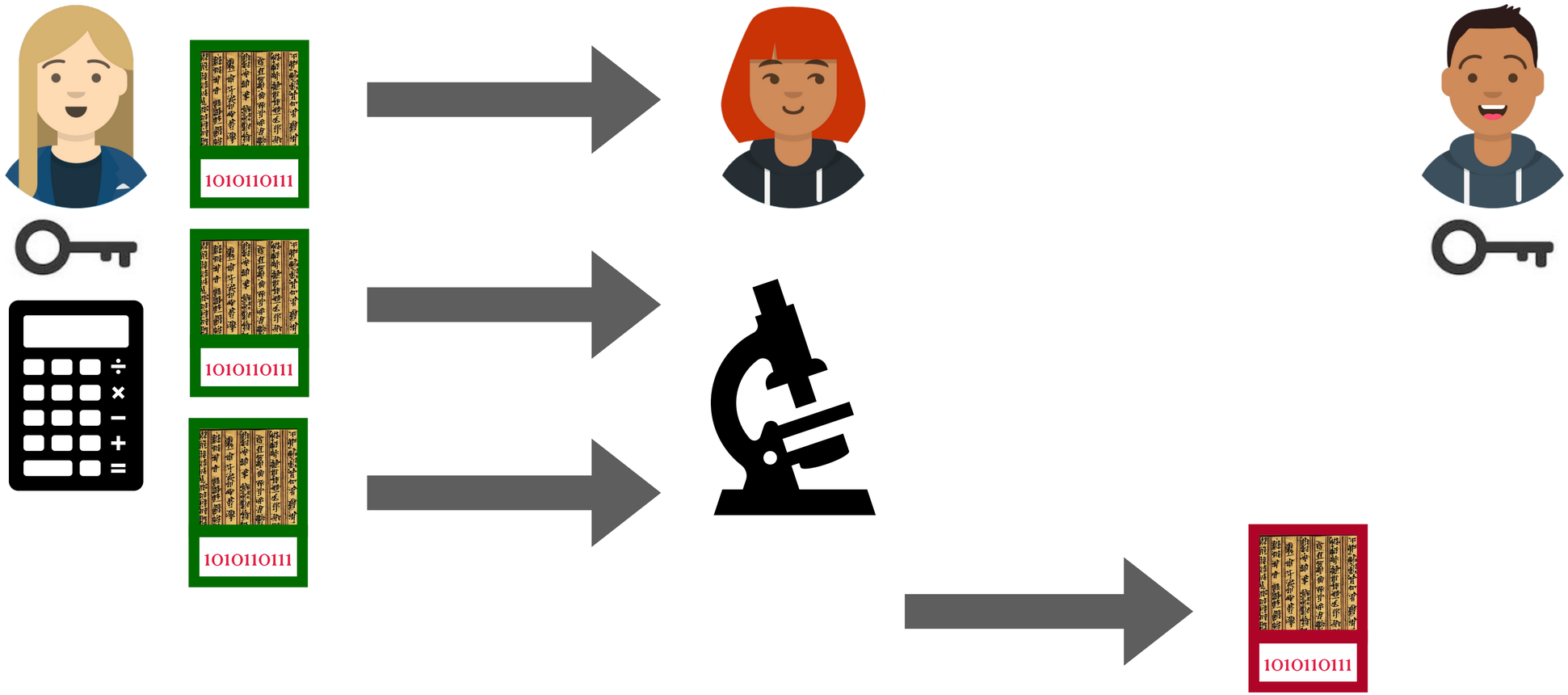
MAC Security

Unforgeability Game: Passive Adversary



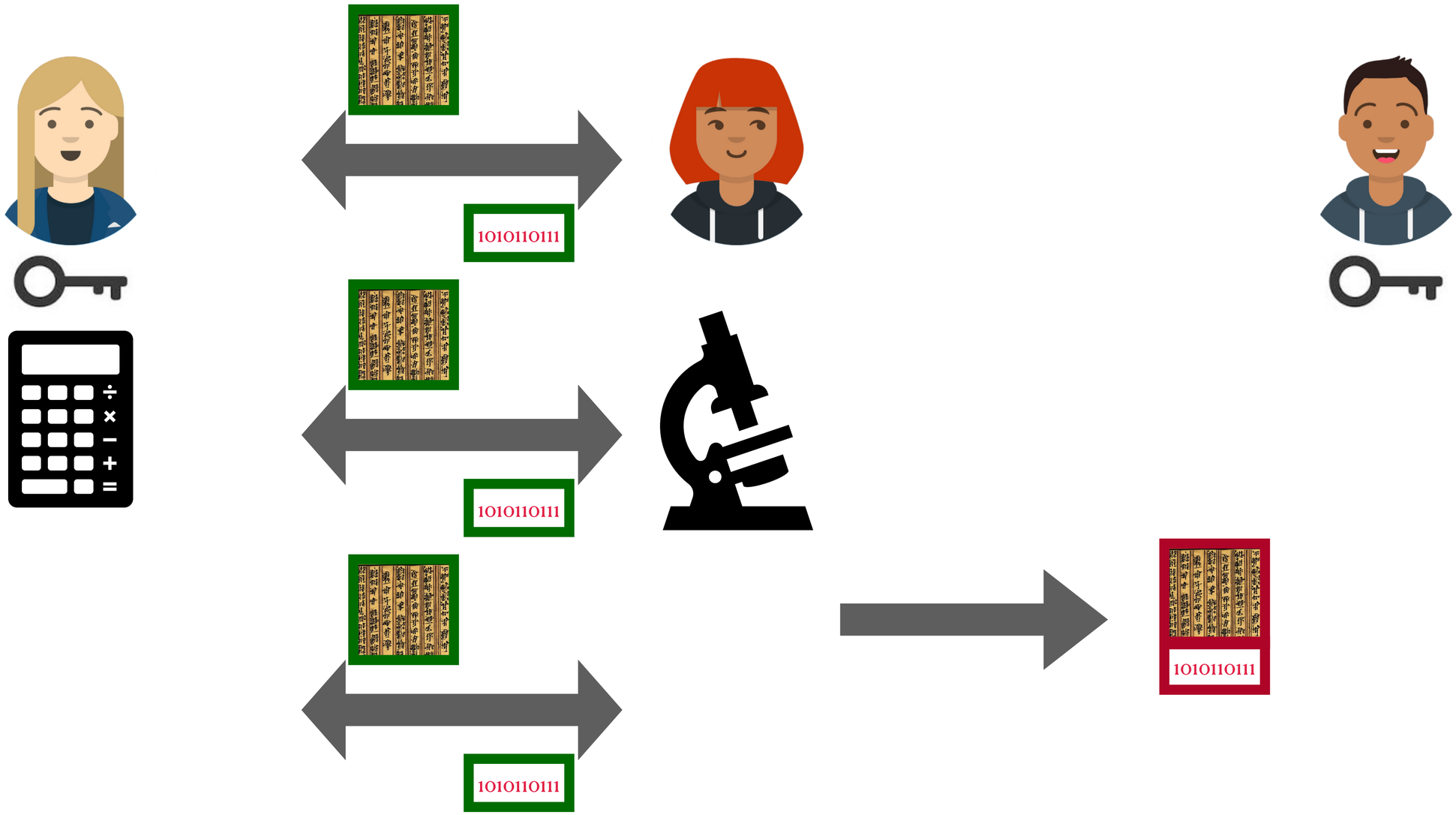
MAC Security

Unforgeability Game: Passive Adversary



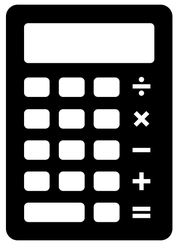
MAC Security

Unforgeability Game: Active Adversary



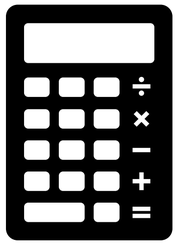
MAC Security

Unforgeability Game: Forgery Succeeds



MAC Security

Unforgeability Game: Forgery Succeeds



$$\text{MAC Security} \triangleq \Pr(\texttt{Forgery Succeeds})$$

MAC Security

Random Functions are Good MACs

MAC Security

Random Functions are Good MACs

$$\Pr\left(\texttt{Forgery Succeeds}\right) = \Pr\left(\texttt{Guessing}\right)$$

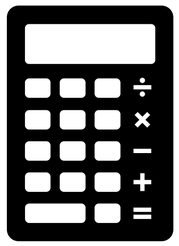
Pseudorandom Function Security

Ideal World (o)

Pseudorandom Function Security

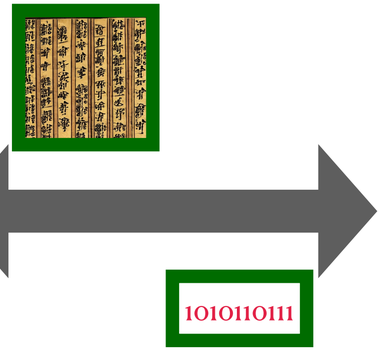
Ideal World (0)

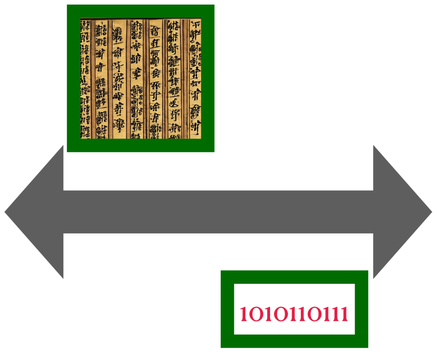
Real World (1)



Pseudorandom Function Security

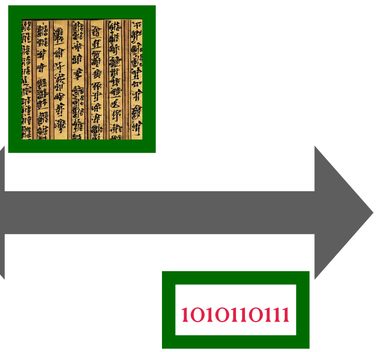
Ideal World (0)

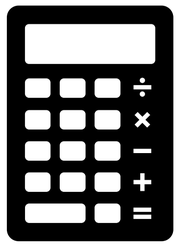


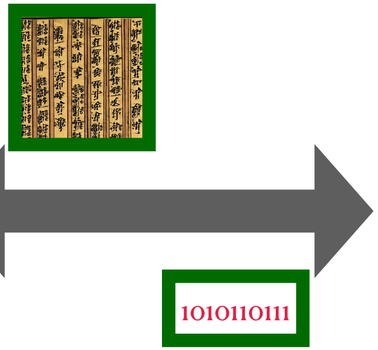


b

Real World (1)

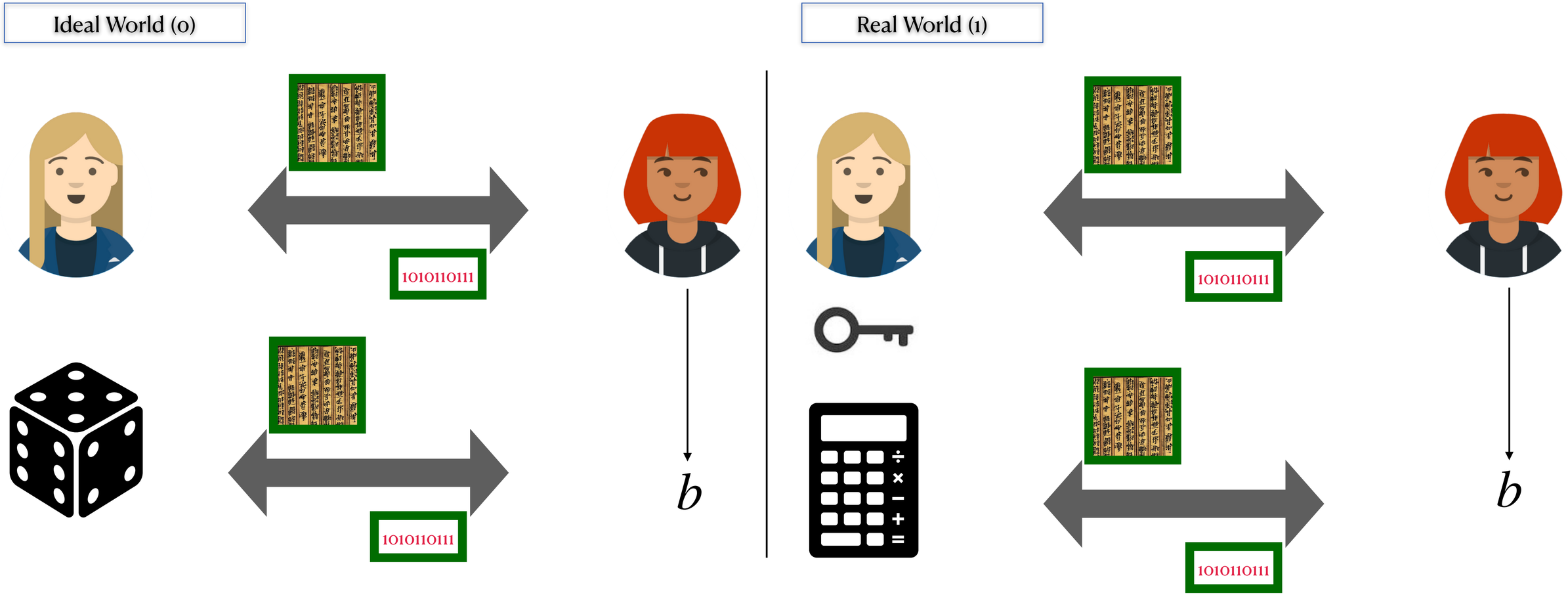






b

Pseudorandom Function Security



$$\mathbf{Adv}^{\mathrm{prf}}_{\mathbf{Alice}}(\mathbf{Eve}) := \left|\Pr\left(b = 1 \text{ in the real world}\right) - \Pr\left(b = 1 \text{ in the ideal world}\right)\right|$$

CBC-MAC

Ehrsam et al., US Patent 4074066

CBC-MAC

Ehrsam et al., US Patent 4074066

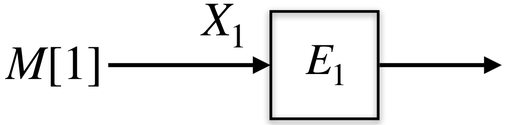
$$\left(M[1], \ldots, M[\ell]\right) \xleftarrow{n} M \in \left(\{0,1\}^n\right)^+$$

n: block size

CBC-MAC

Ehrsam et al., US Patent 4074066

$$\left(M[1], \ldots, M[\ell]\right) \xleftarrow{n} M \in \left(\{0,1\}^n\right)^+$$

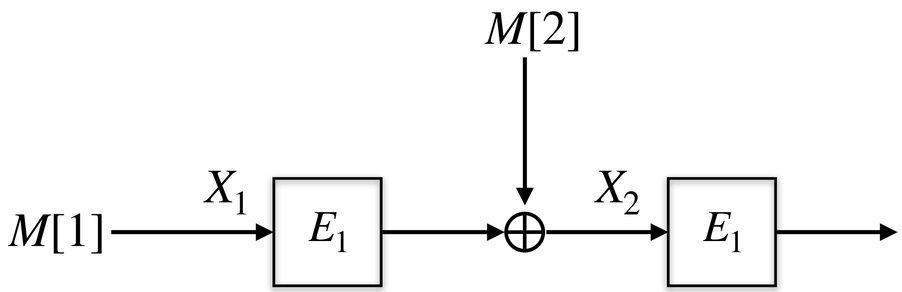


n: block size

CBC-MAC

Ehrsam et al., US Patent 4074066

$$\left(M[1], \ldots, M[\ell]\right) \xleftarrow{n} M \in \left(\{0,1\}^n\right)^+$$

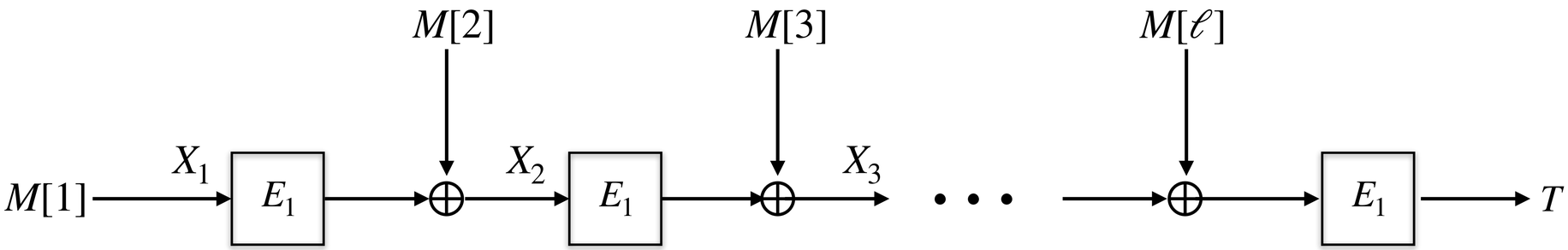


n: block size

CBC-MAC

Ehrsam et al., US Patent 4074066

$(M[1], \ldots, M[\ell]) \xleftarrow{n} M \in (\{0,1\}^n)^+$

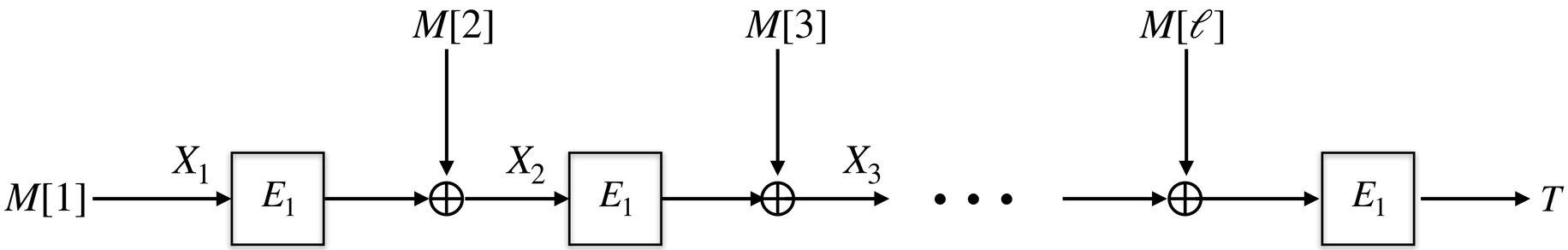


n: block size

CBC-MAC

Ehrsam et al., US Patent 4074066

$$\left(M[1], \ldots, M[\ell]\right) \xleftarrow{n} M \in \left(\{0,1\}^n\right)^+$$



- Susceptible to length extension* attacks.
- Input length must be a non-zero multiple of n.

n: block size

* $\text{CBC-MAC}\left(M \| X\right) = \text{CBC-MAC}\left(\text{CBC-MAC}\left(M\right) \| X\right)$

OMAC, XCBC, and TMAC

OMAC, XCBC, and TMAC

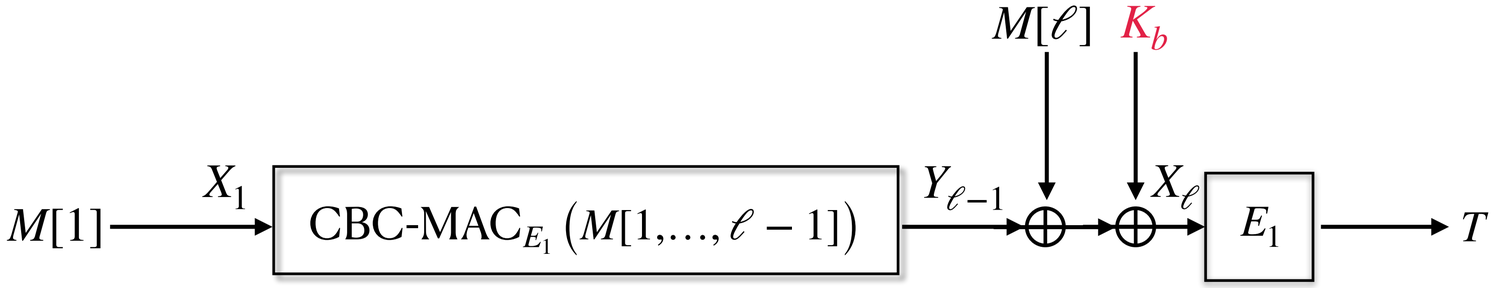
$\left(M[1], \ldots, M[\ell]\right) \xleftarrow{n} M \xleftarrow{\text{pad}} M' \in \{0,1\}^*$

OMAC, XCBC, and TMAC

$$\left(M[1], \ldots, M[\ell]\right) \xleftarrow{n} M \xleftarrow{\text{pad}} M' \in \{0,1\}^*$$

$$\text{XCBC}_{E_1}(M') :=$$

Black and Rogaway, IACR CRYPTO 2000



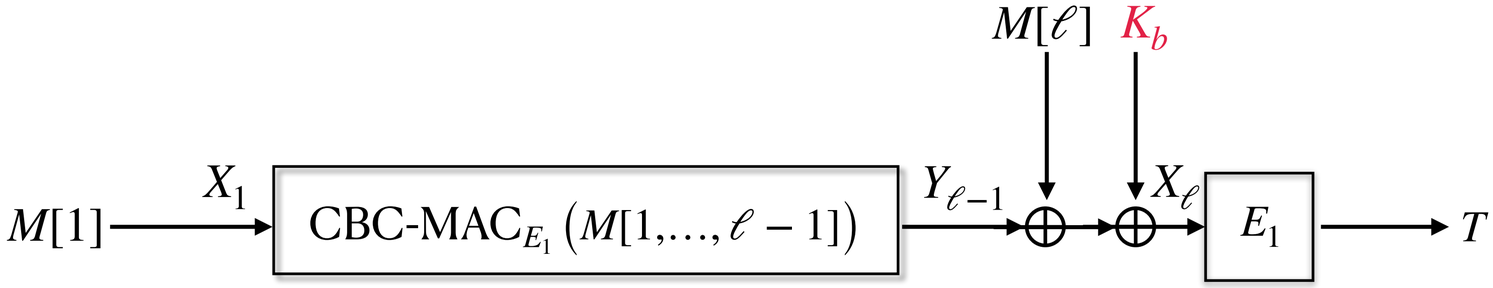
$b := (M =_? M')\ ?\ 0 : 1$

OMAC, XCBC, and TMAC

$\left(M[1], \ldots, M[\ell]\right) \xleftarrow{n} M \xleftarrow{\text{pad}} M' \in \{0,1\}^*$

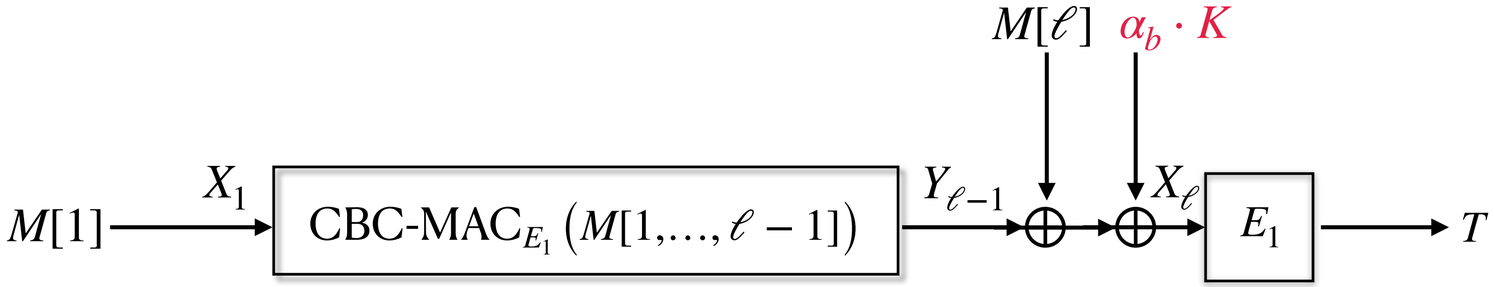
$\text{XCBC}_{E_1}(M') :=$

Black and Rogaway, IACR CRYPTO 2000



$\text{TMAC}_{E_1}(M') :=$

Kurosawa and Iwata, CT-RSA 2003



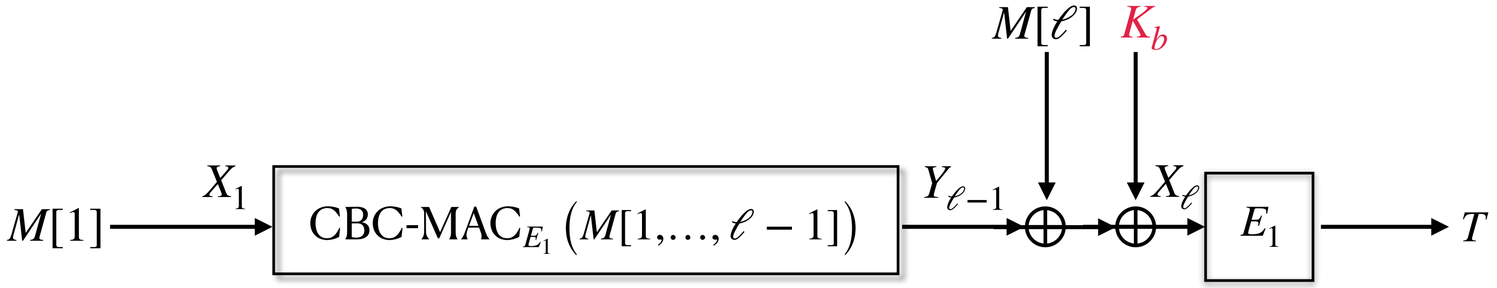
$b := (M =_? M')\ ?\ 0 : 1$

OMAC, XCBC, and TMAC

$(M[1], \ldots, M[\ell]) \xleftarrow{n} M \xleftarrow{\text{pad}} M' \in \{0,1\}^*$

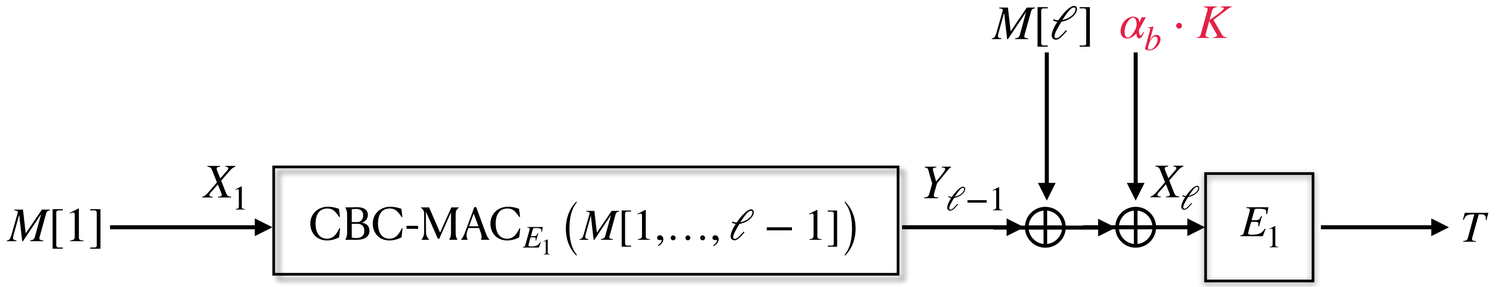
$\text{XCBC}_{E_1}(M') :=$

Black and Rogaway, IACR CRYPTO 2000



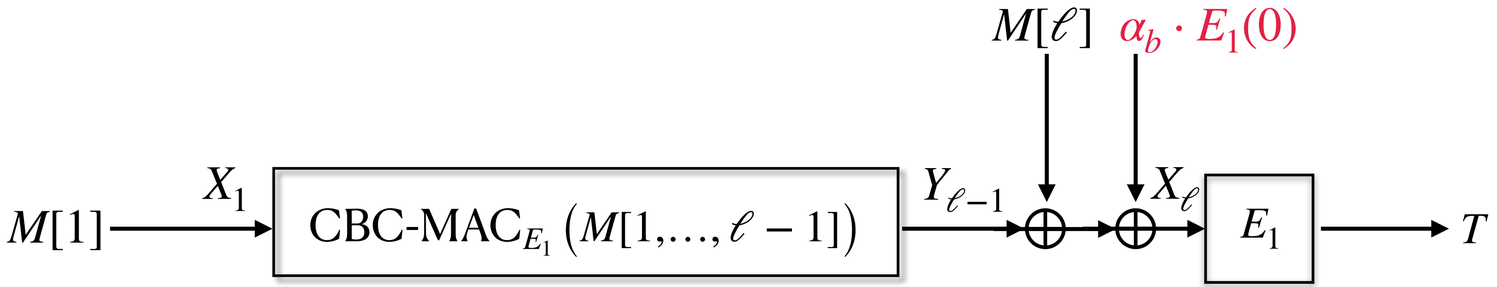
$\text{TMAC}_{E_1}(M') :=$

Kurosawa and Iwata, CT-RSA 2003



$\text{OMAC}_{E_1}(M') :=$

Iwata and Kurosawa, IACR FSE 2003;
NIST FIPS 800-38B;
ISO/IEC 29167-10:2017



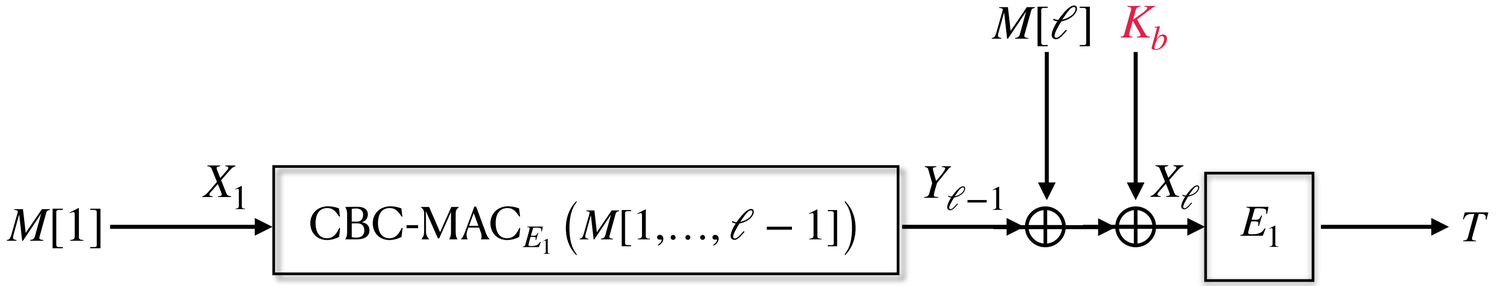
$b := (M =_? M')\ ?\ 0 : 1$

OMAC, XCBC, and TMAC

$\left(M[1], \ldots, M[\ell]\right) \xleftarrow{n} M \xleftarrow{\text{pad}} M' \in \{0,1\}^*$

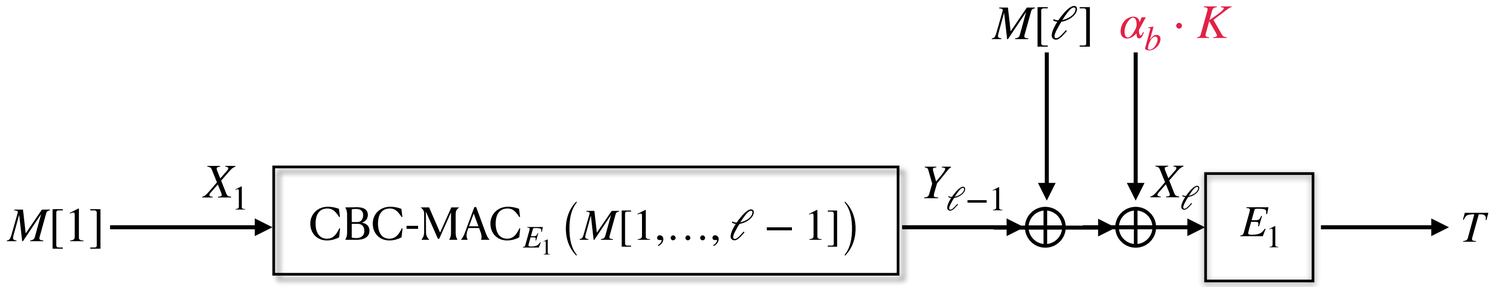
$\text{XCBC}_{E_1}(M') :=$

Black and Rogaway, IACR CRYPTO 2000



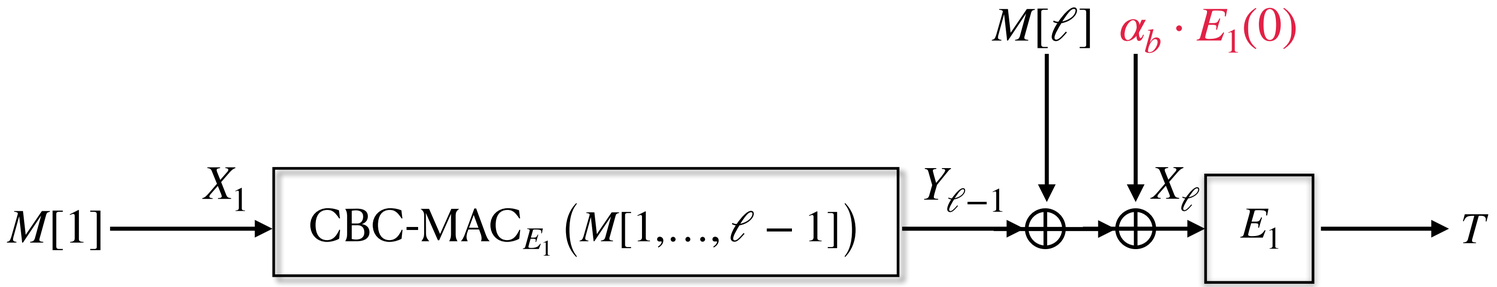
$\text{TMAC}_{E_1}(M') :=$

Kurosawa and Iwata, CT-RSA 2003



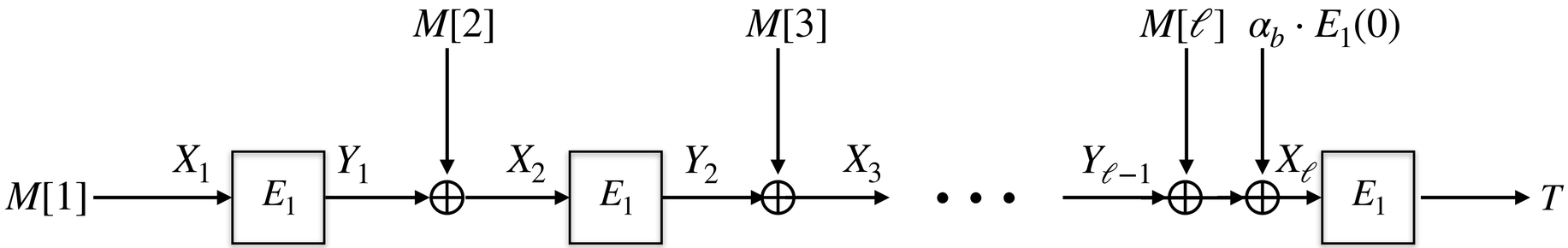
$\text{OMAC}_{E_1}(M') :=$

Iwata and Kurosawa, IACR FSE 2003;
NIST FIPS 800-38B;
ISO/IEC 29167-10:2017



$b := (M =_? M')\ ?\ 0 : 1$

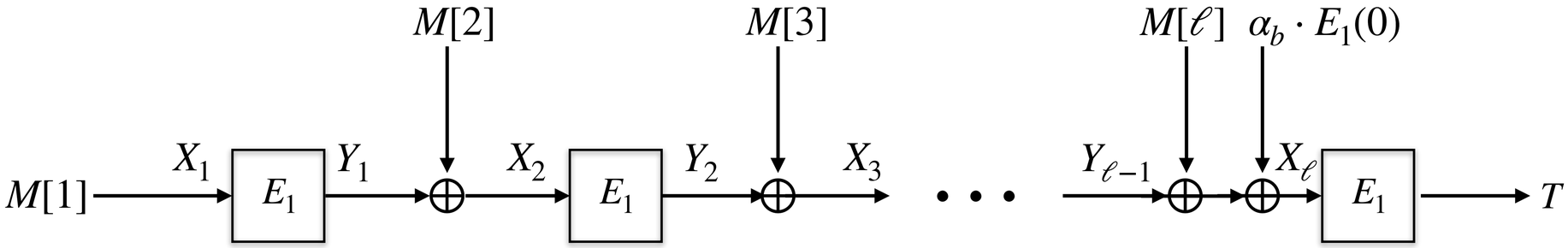
PRF Security of OMAC



- Best security bound:

$$\mathbf{Adv}^{\text{prf}}_{\text{CBC-MAC}}(\mathbf{Eve}) = O\left(\frac{q^2\ell}{2^n}\right)$$

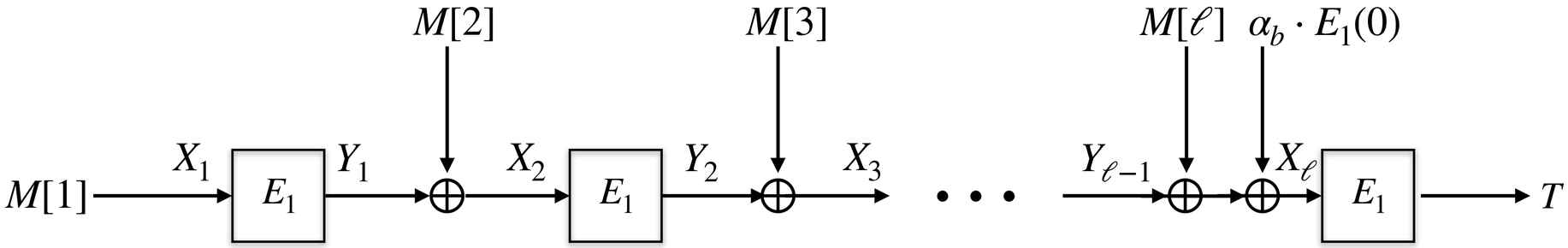
PRF Security of OMAC



- Best security bound:

$$\mathbf{Adv}^{\text{prf}}_{\text{CBC-MAC}}(\mathbf{Eve}) = O\left(\frac{q^2\ell}{2^n}\right) \qquad \text{i.e.} \qquad \mathbf{Eve} \text{ needs roughly } \sqrt{2^n/\ell} \text{ queries.}$$

PRF Security of OMAC



- Best security bound:

$$\mathbf{Adv}^{\text{prf}}_{\text{CBC-MAC}}(\mathbf{Eve}) = O\left(\frac{q^2\ell}{2^n}\right) \quad \text{i.e.} \quad \mathbf{Eve} \text{ needs roughly } \sqrt{2^n/\ell} \text{ queries.}$$

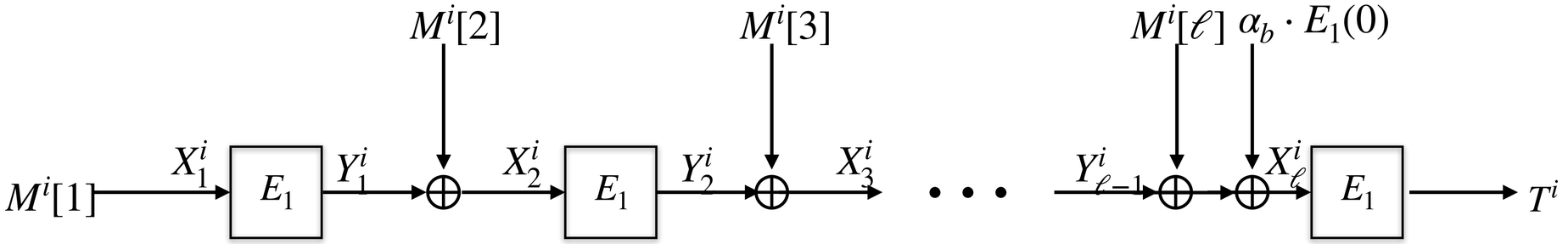
- No matching attack!
  - Folklore collision finding attack needs roughly $\sqrt{2^n}$ queries.

PRF Security of OMAC

Full Collision Event

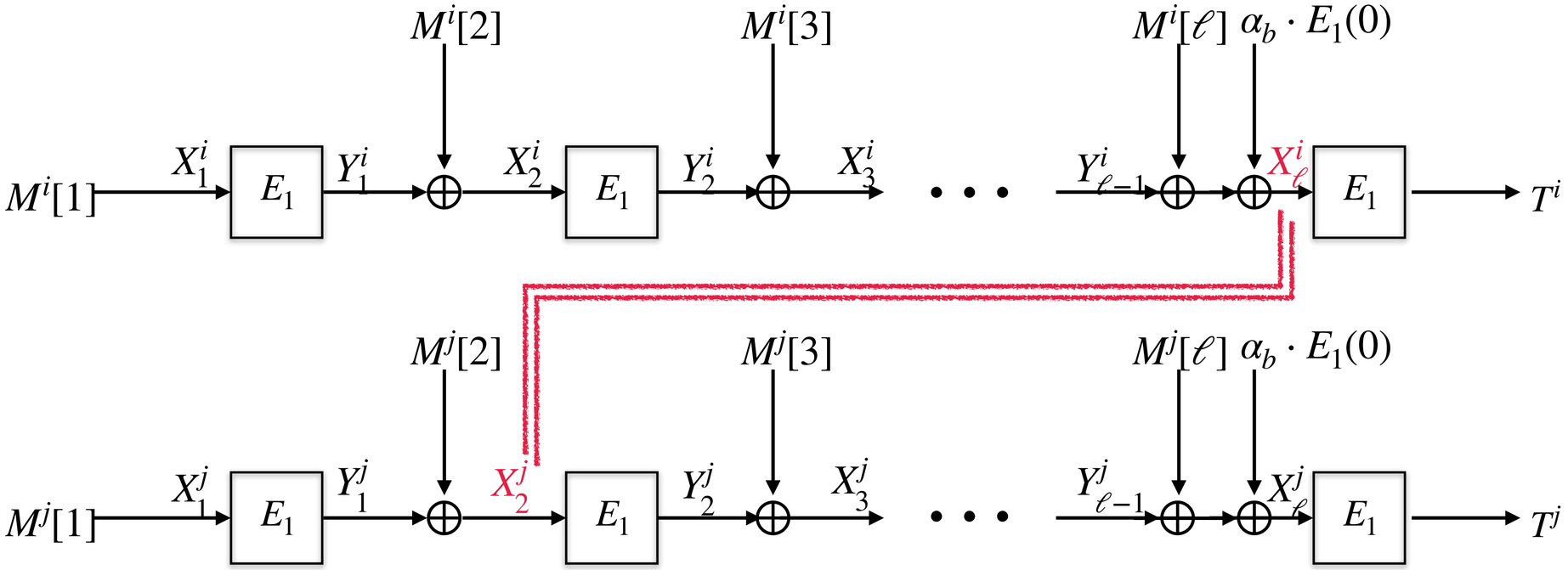
PRF Security of OMAC

Full Collision Event



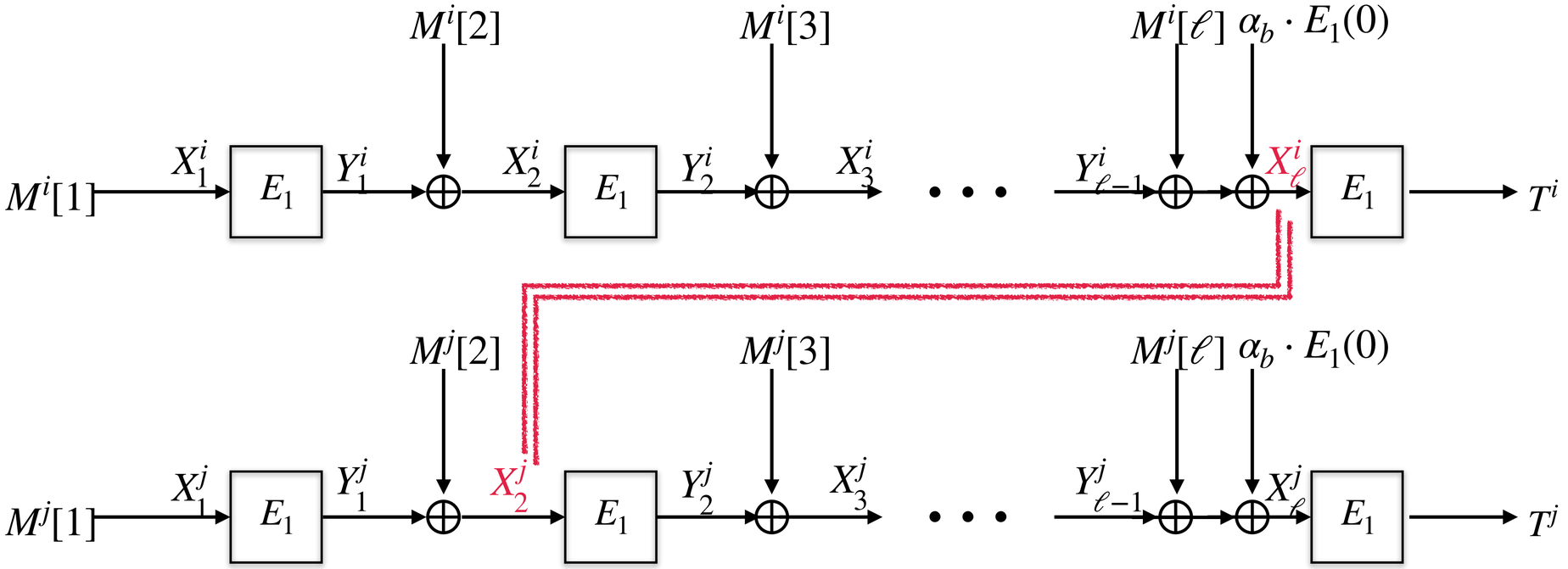
PRF Security of OMAC

Full Collision Event



PRF Security of OMAC

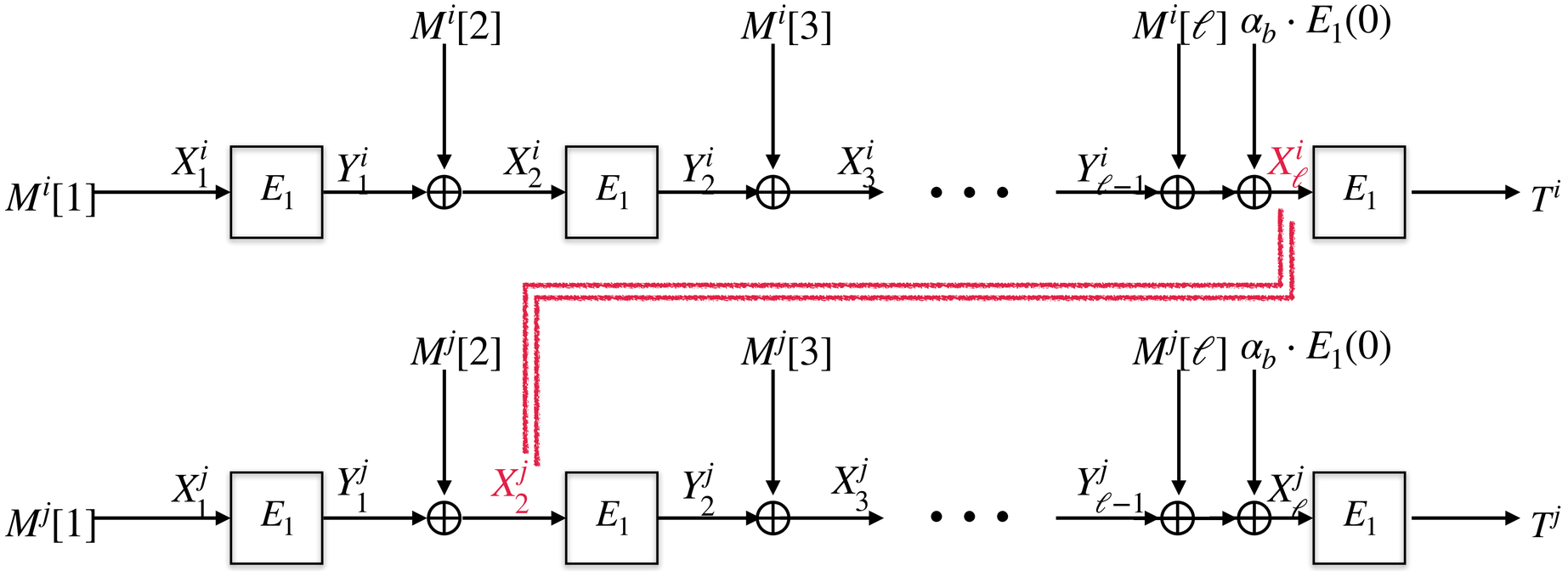
Full Collision Event



Full Collision : $\exists i, j, a$ such that $X_a^j = X_\ell^i$

PRF Security of OMAC

Full Collision Event



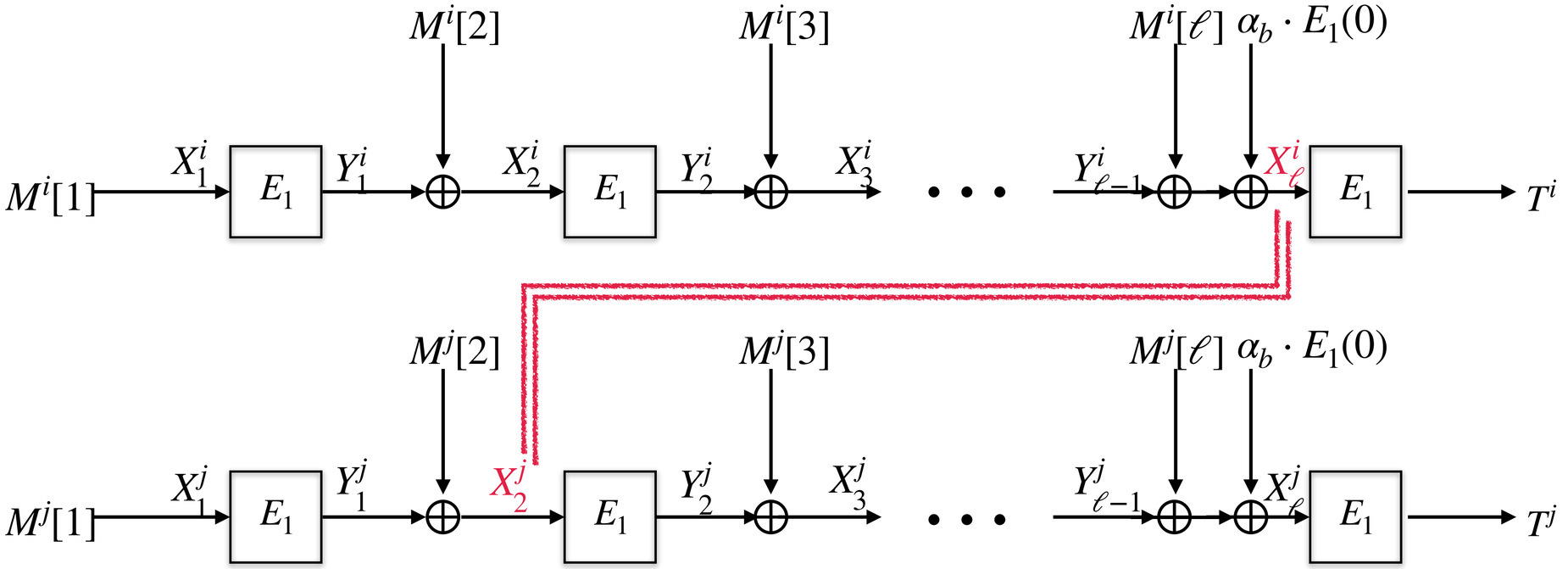
$$\Pr(\texttt{Full Collision}) = O\left(\frac{q^2\ell}{2^n}\right)$$

PRF Security of OMAC

Reset-Sampling Approach (CJN, IACR ASIACRYPT 2021)

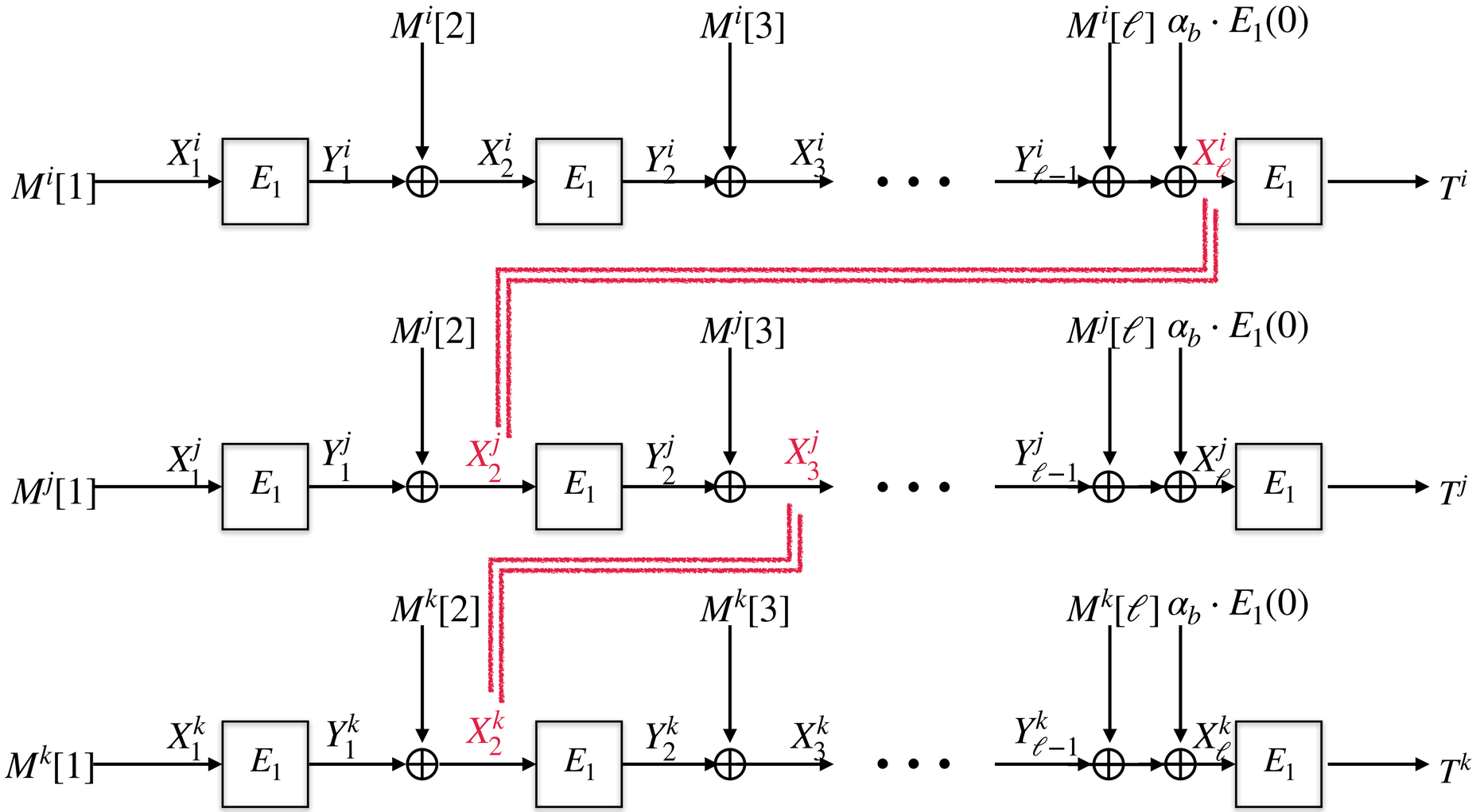
PRF Security of OMAC

Reset-Sampling Approach (CJN, IACR ASIACRYPT 2021)



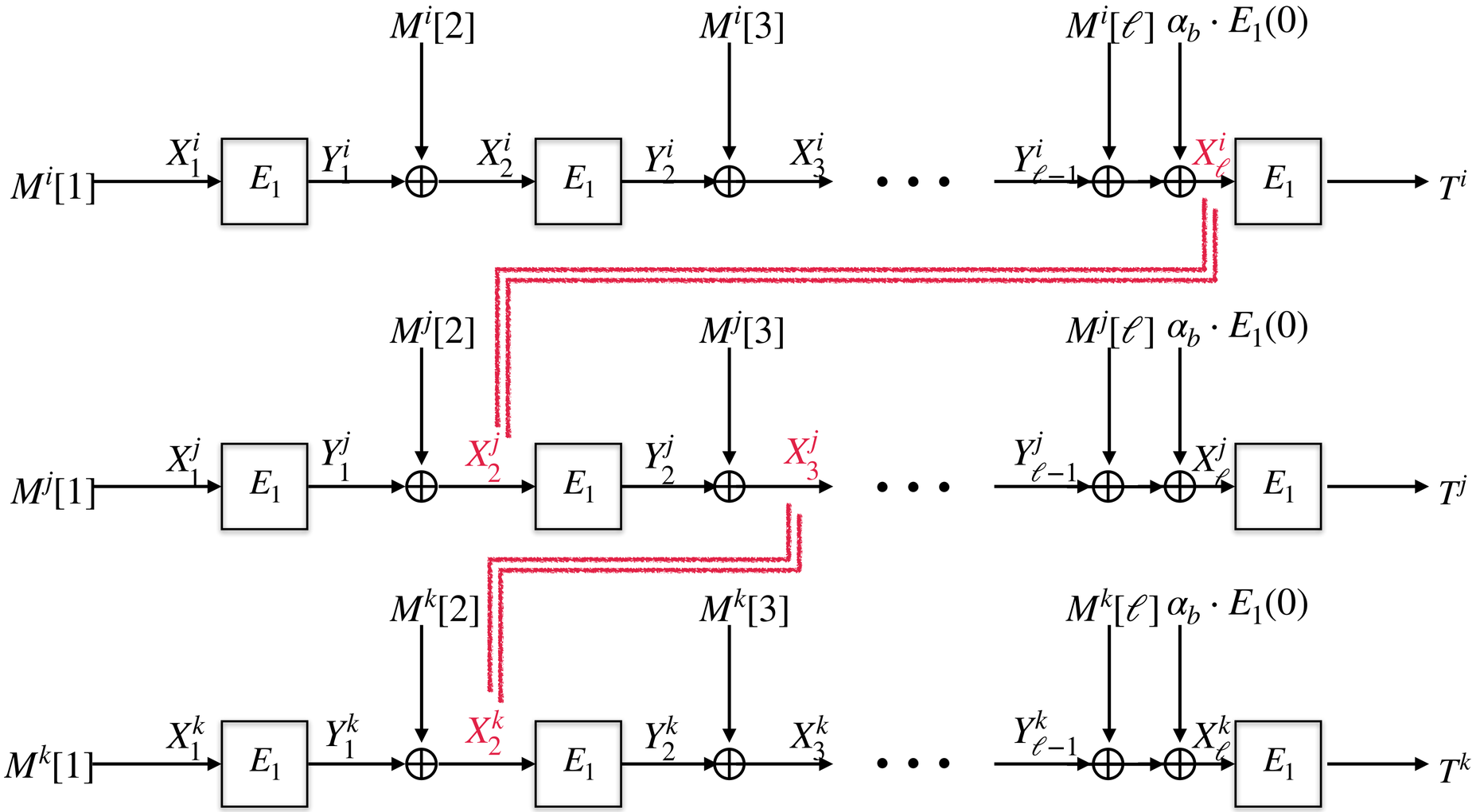
PRF Security of OMAC

Reset-Sampling Approach (CJN, IACR ASIACRYPT 2021)



PRF Security of OMAC

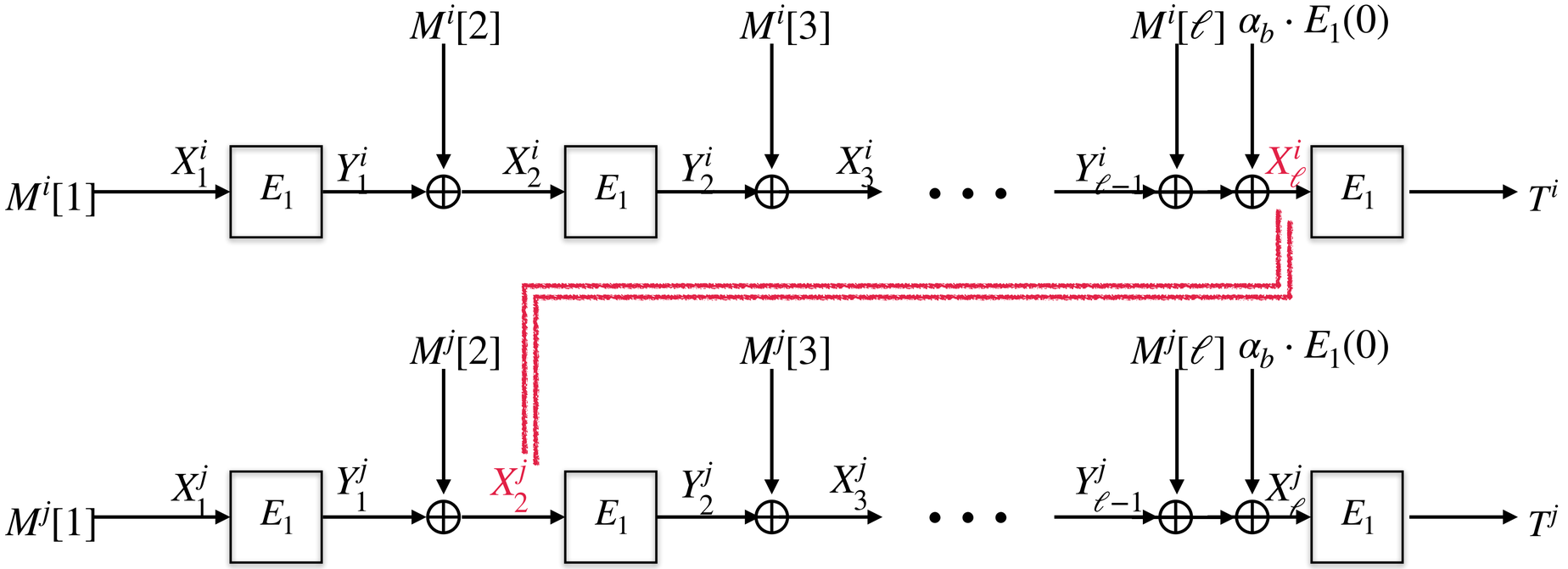
Reset-Sampling Approach (CJN, IACR ASIACRYPT 2021)



$$= O\left(\frac{q^3\ell^2}{2^{2n}}\right)$$

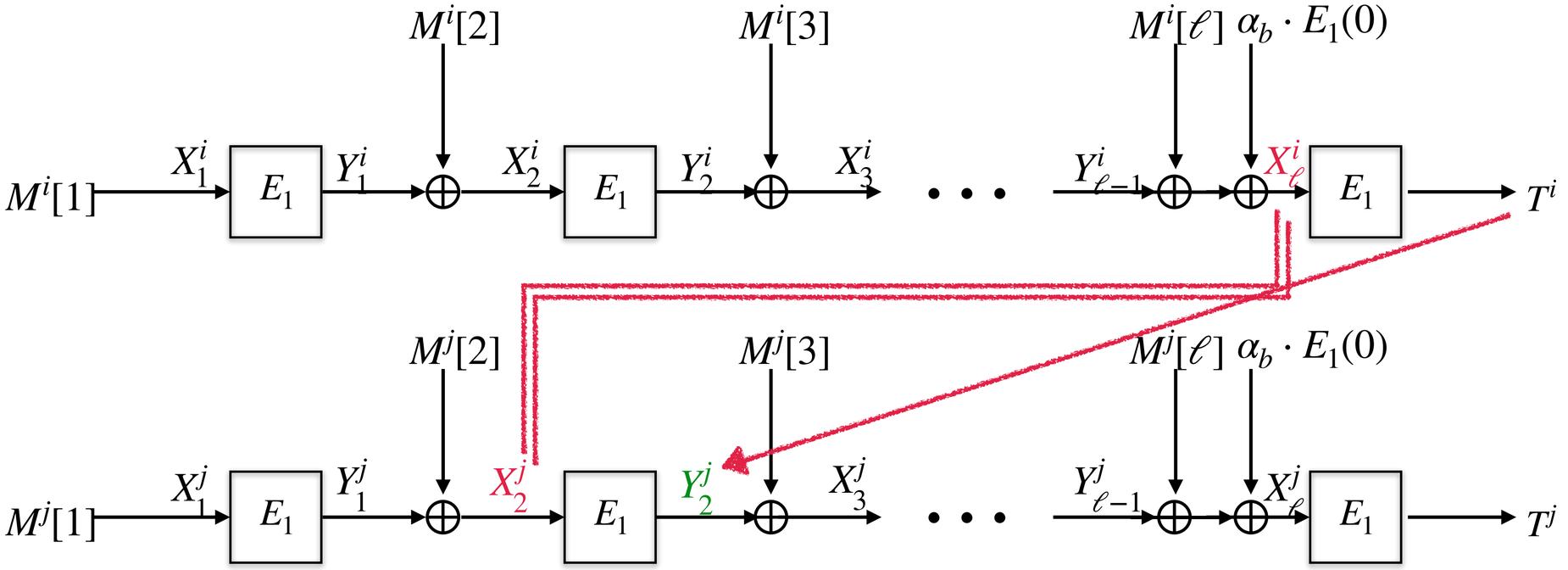
PRF Security of OMAC

Reset-Sampling Approach (CJN, IACR ASIACRYPT 2021)



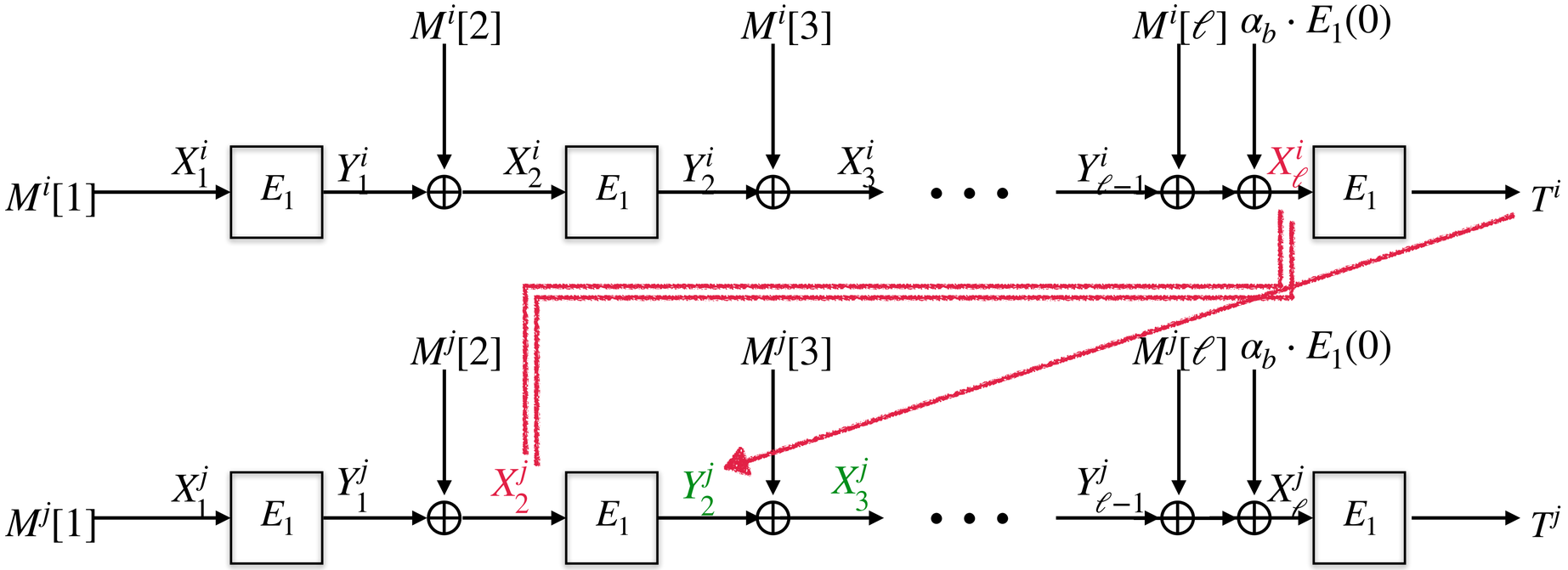
PRF Security of OMAC

Reset-Sampling Approach (CJN, IACR ASIACRYPT 2021)



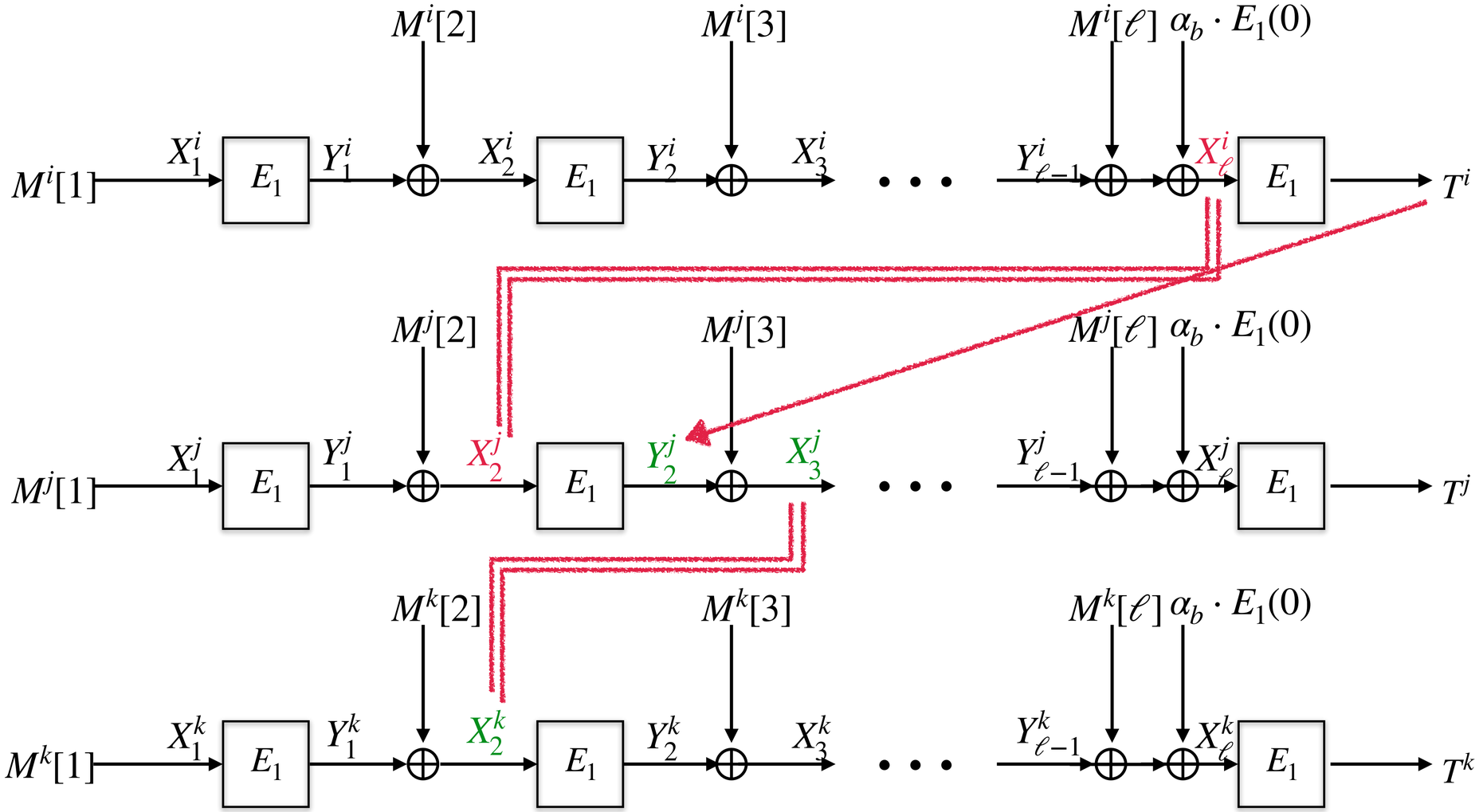
PRF Security of OMAC

Initial Resetting



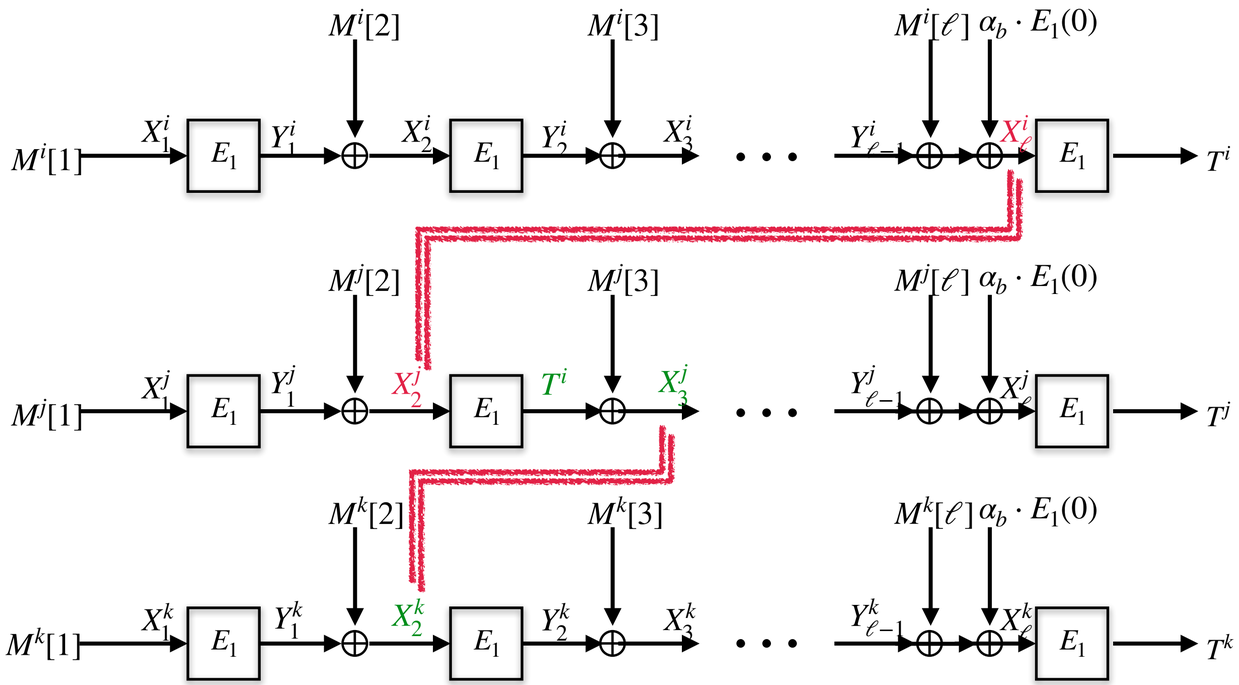
PRF Security of OMAC

Initial Resetting



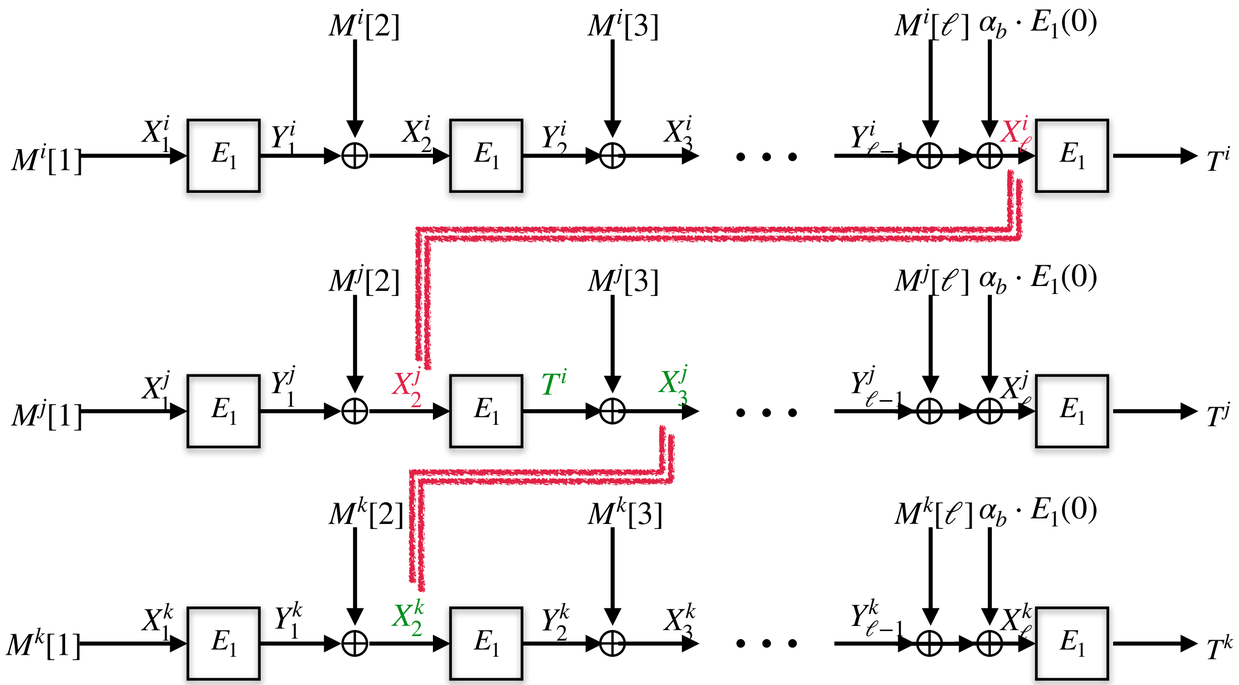
PRF Security of OMAC

Induced Resetting



PRF Security of OMAC

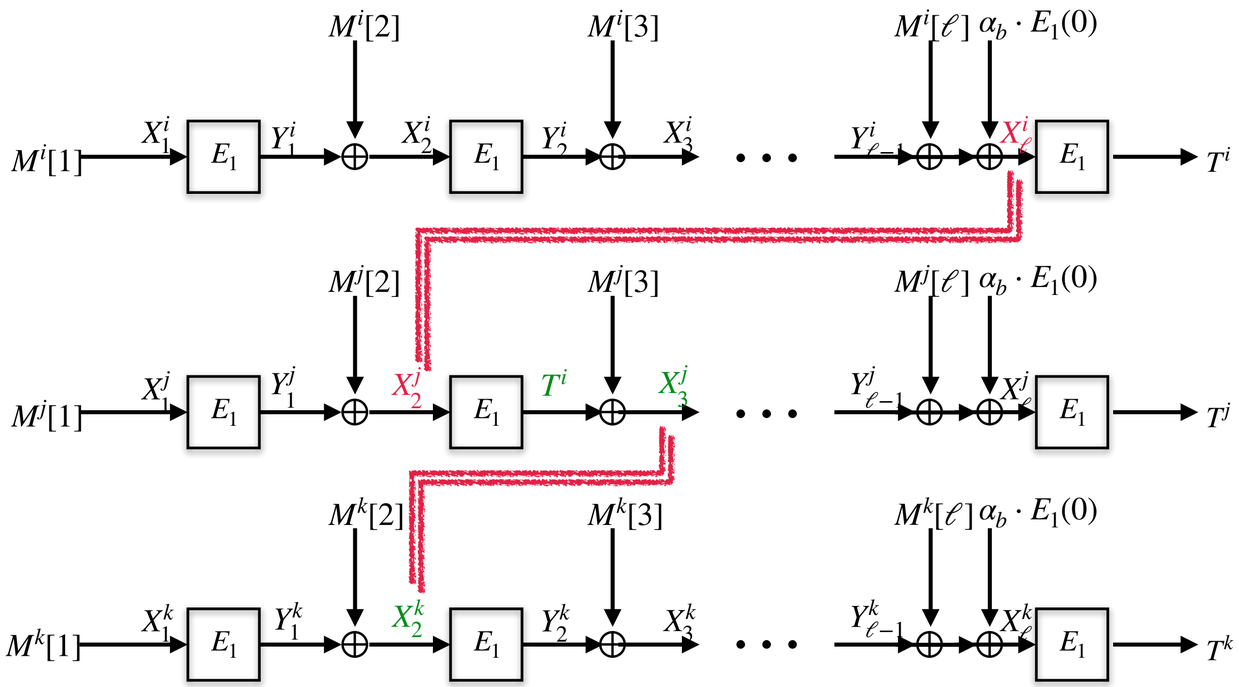
Induced Resetting

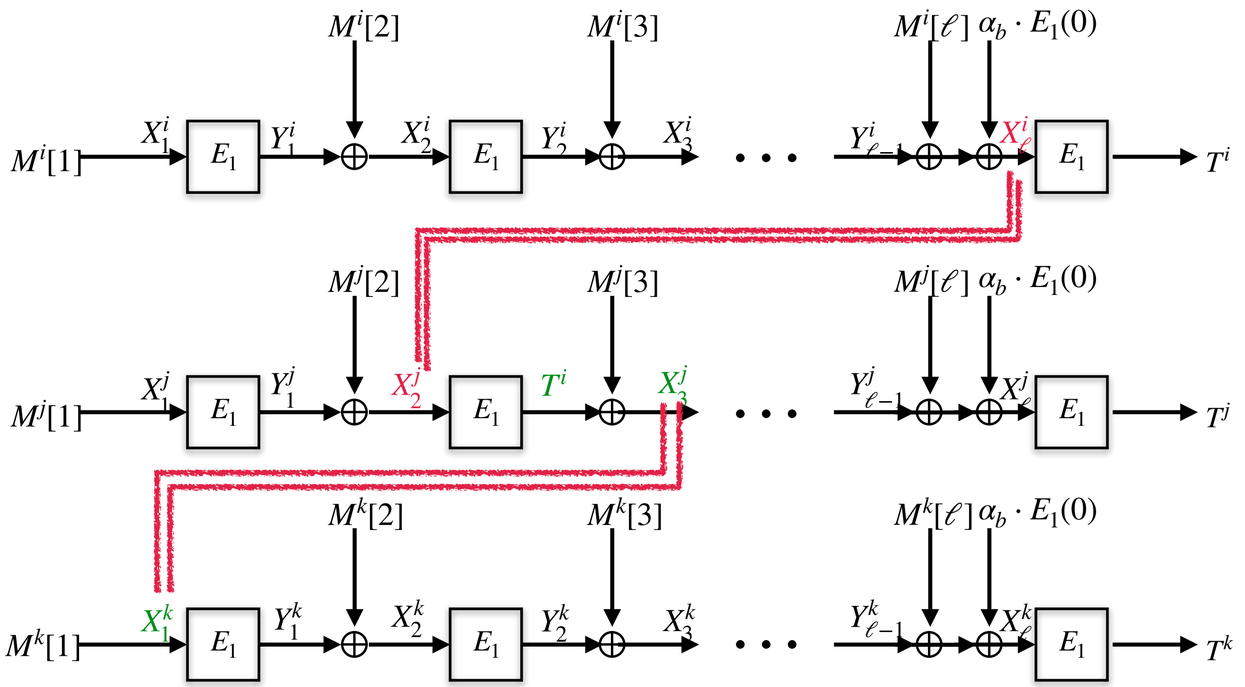


$$= O\left(\frac{q^3\ell^2}{2^{2n}}\right)$$

PRF Security of OMAC

Induced Resetting



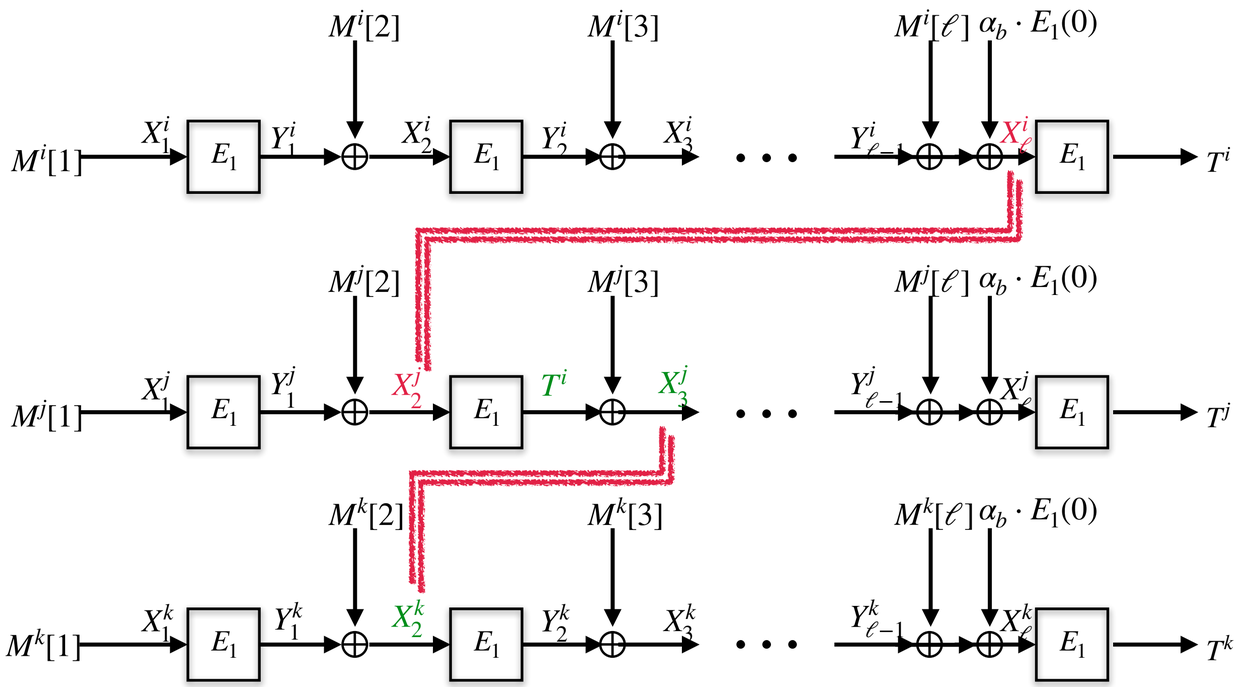


$$= O\left(\frac{q^3\ell^2}{2^{2n}}\right)$$

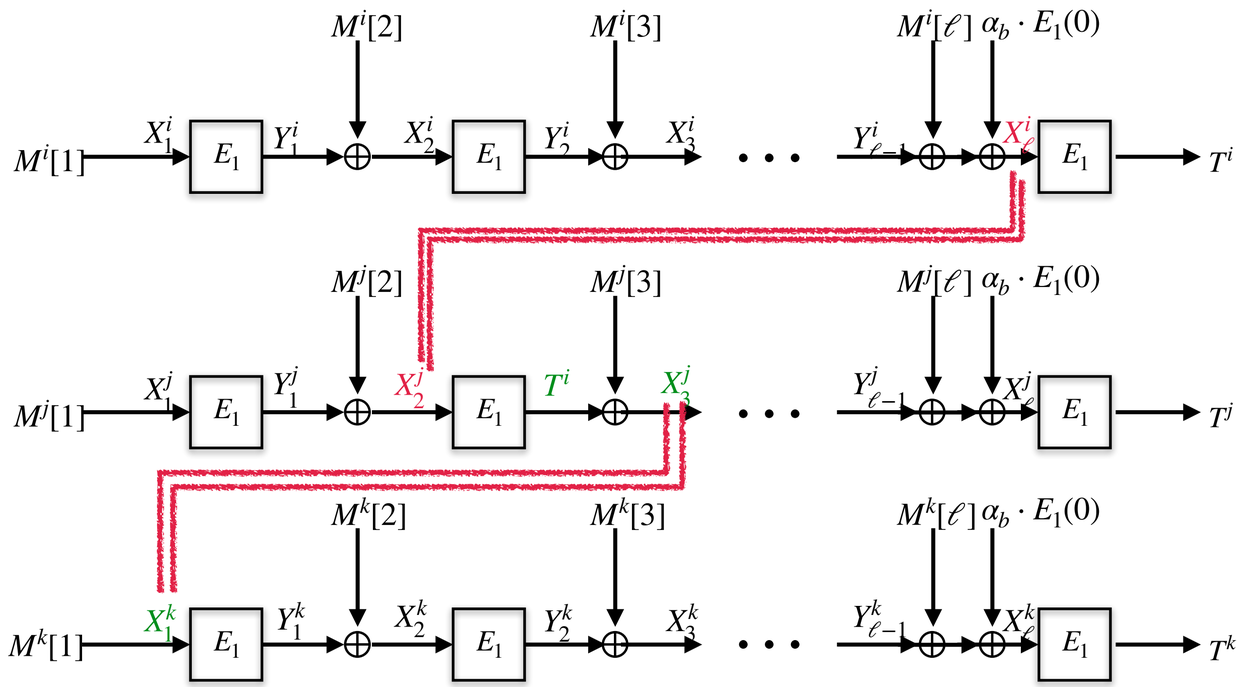
$$M^k[1] = T^i \oplus M^j[3]$$

PRF Security of OMAC

Induced Resetting



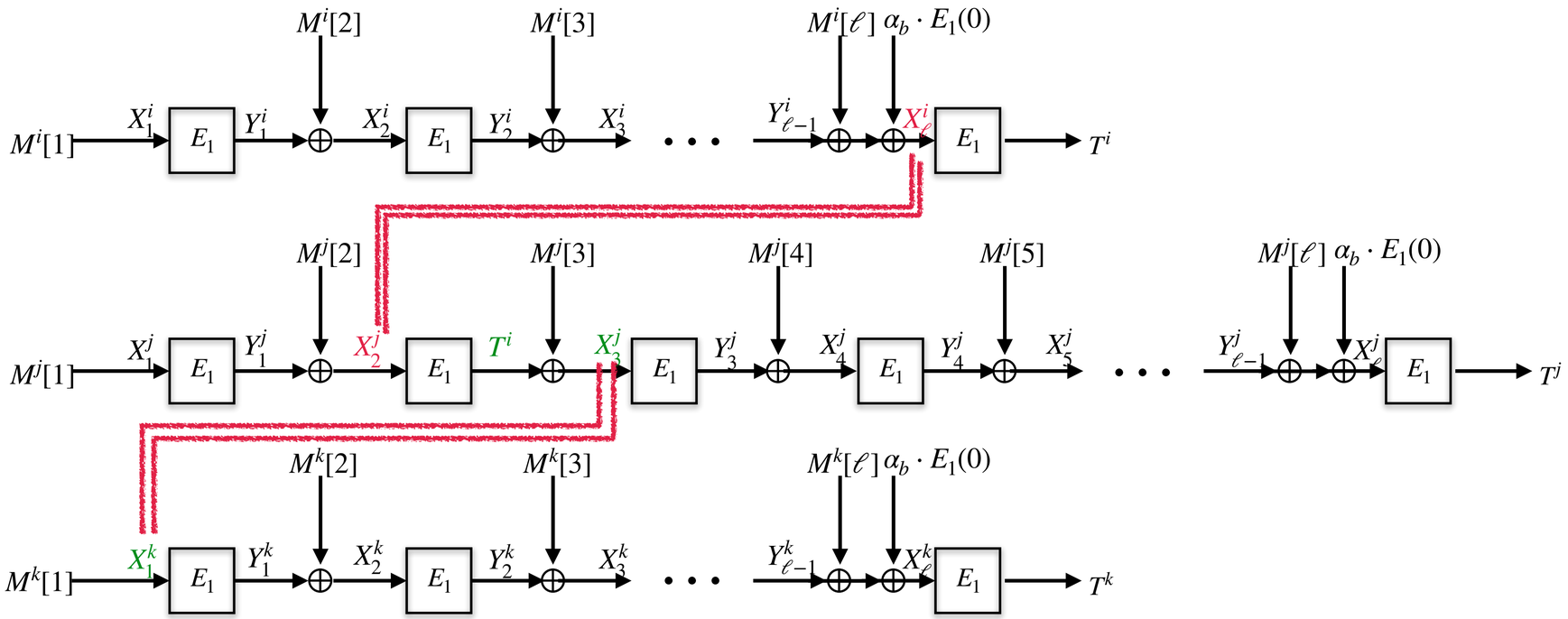
$$= O\left(\frac{q^3\ell^2}{2^{2n}}\right)$$



?

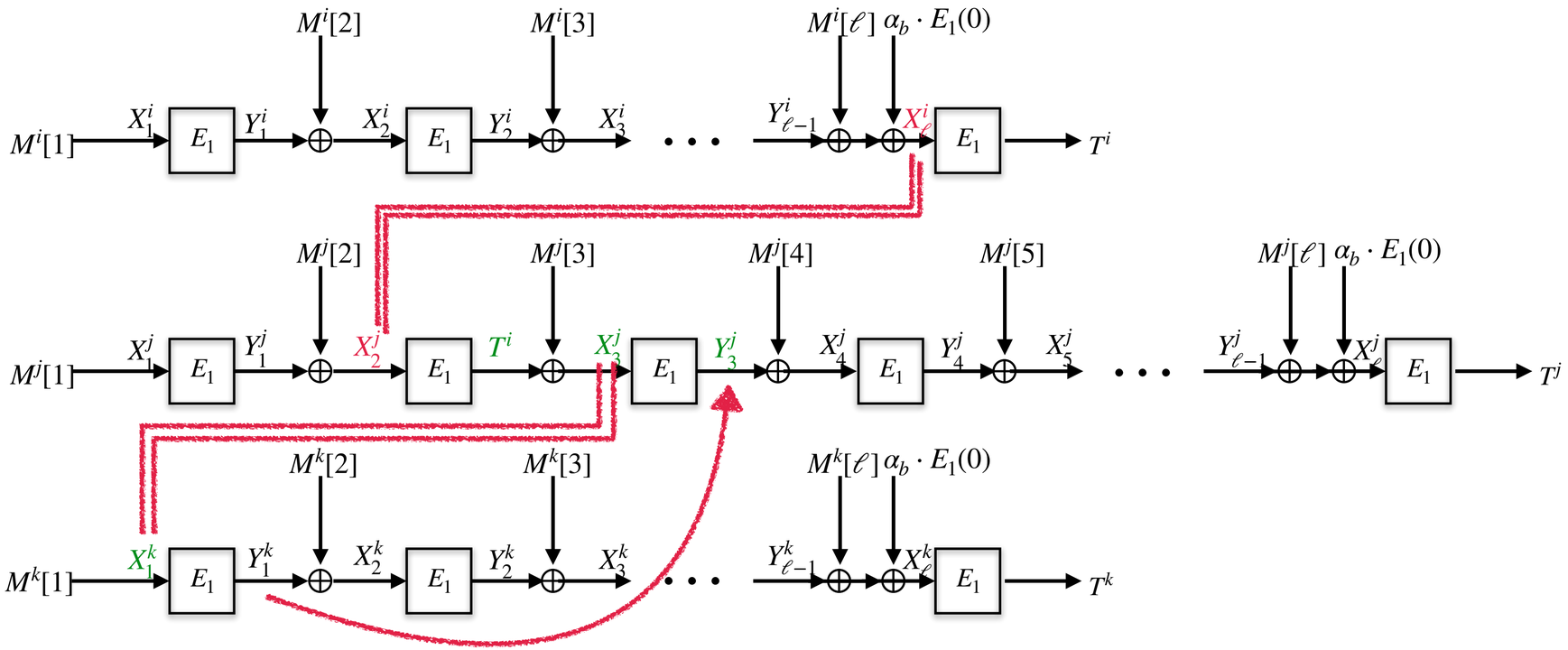
PRF Security of OMAC

Induced Resetting



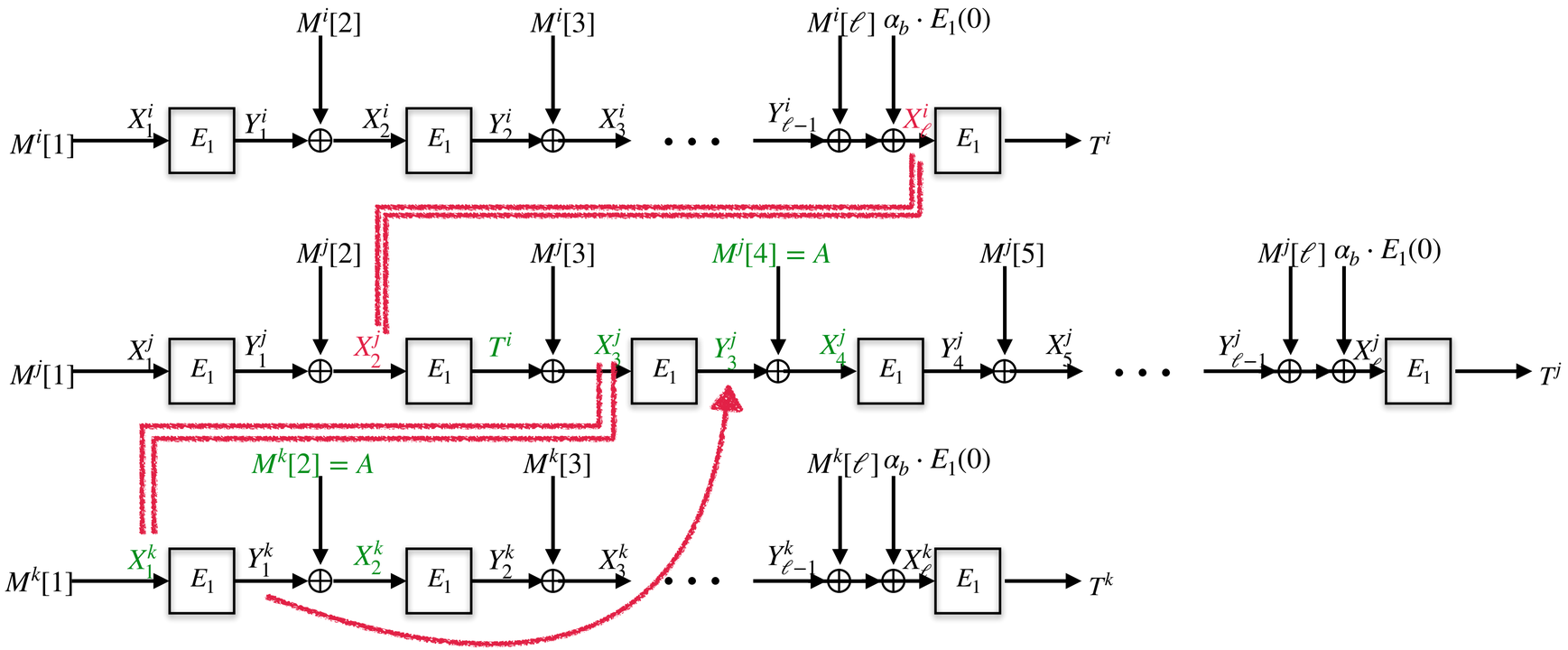
PRF Security of OMAC

Induced Resetting



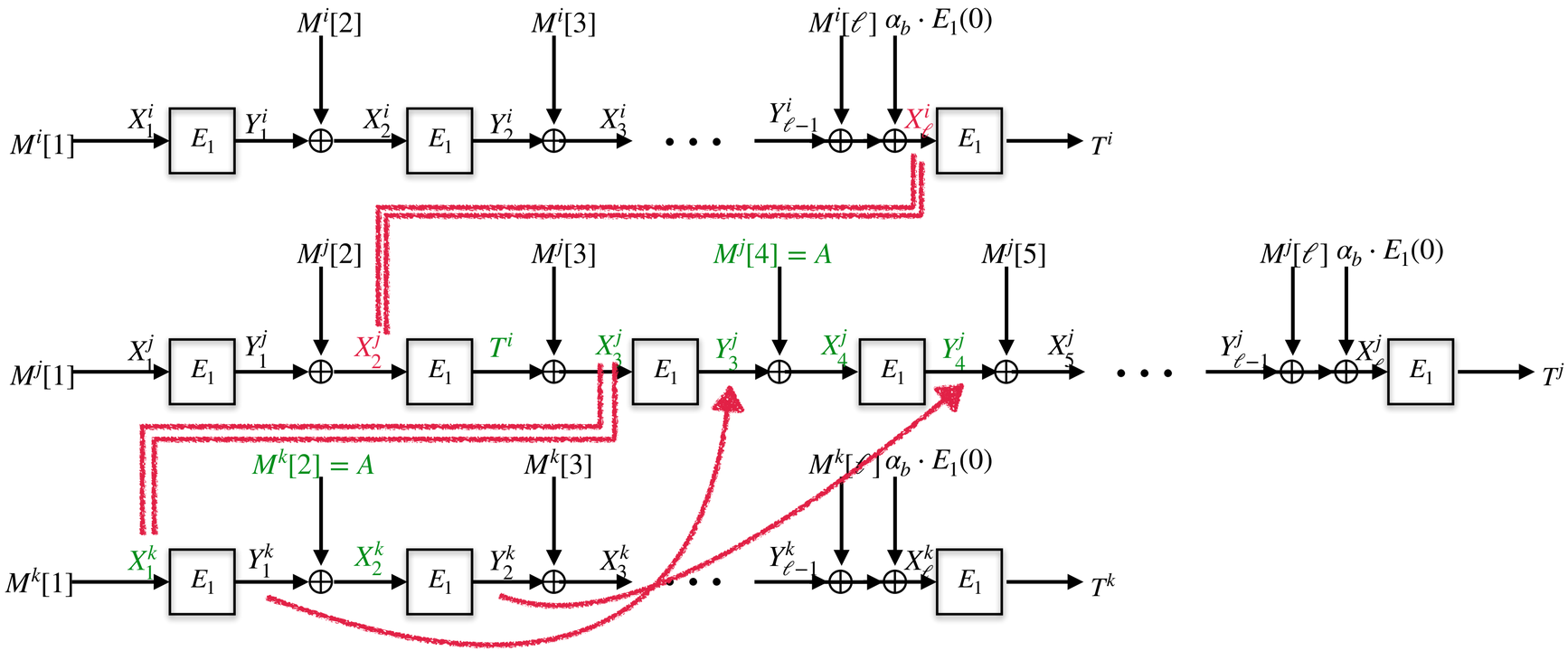
PRF Security of OMAC

Induced Resetting



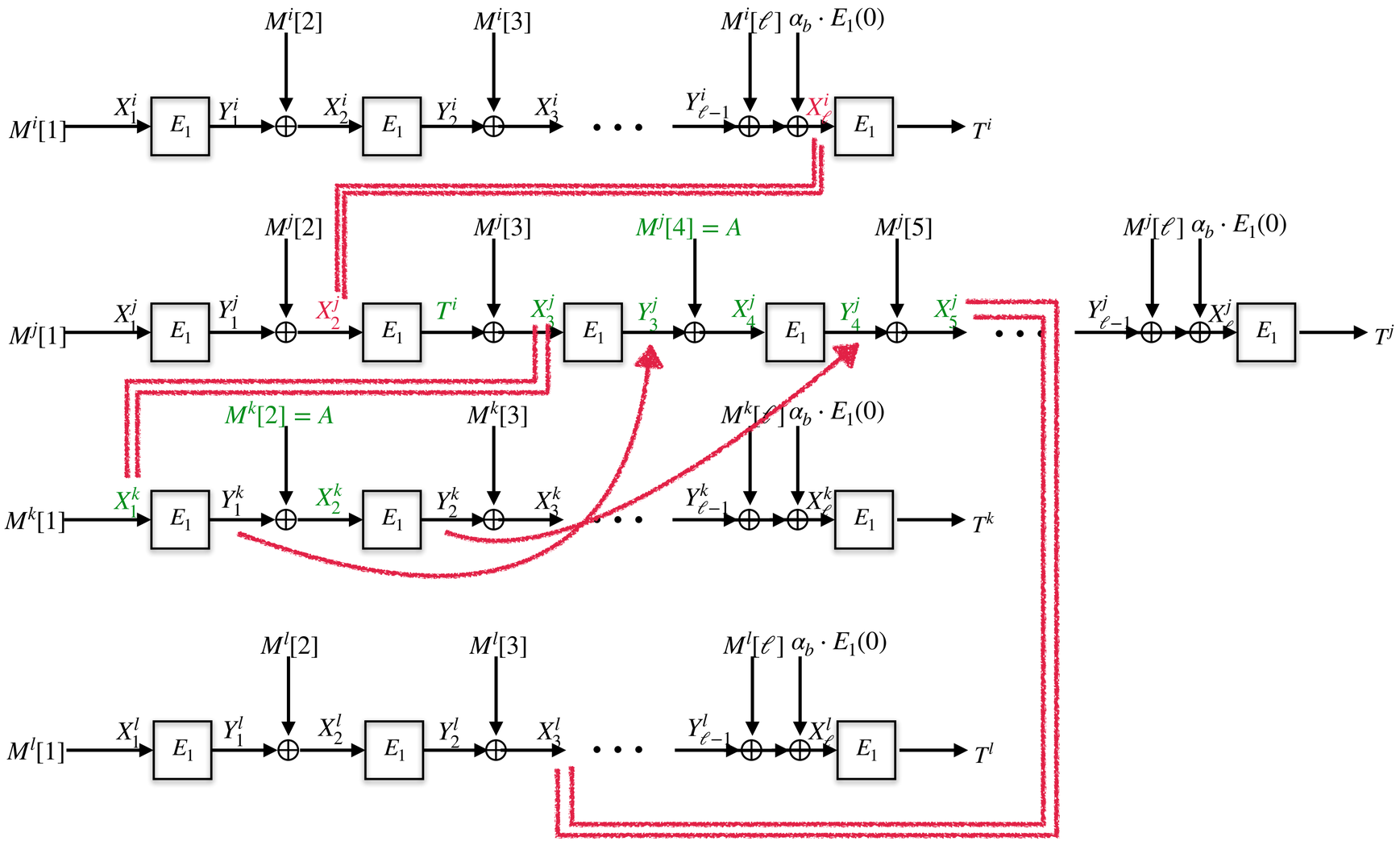
PRF Security of OMAC

Induced Resetting



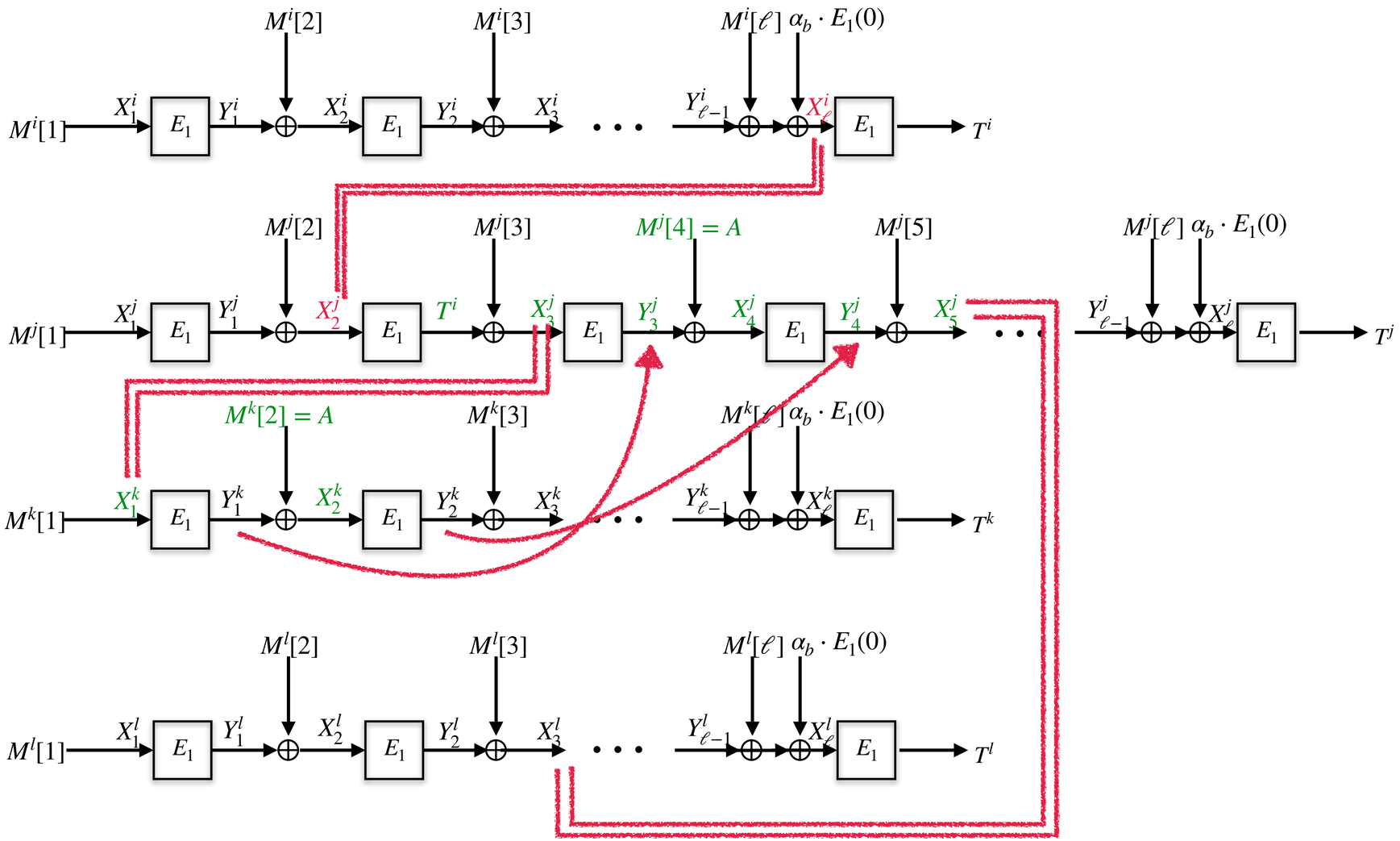
PRF Security of OMAC

Induced Resetting



PRF Security of OMAC

Induced Resetting



$$= O\left(\frac{q^3\ell^2}{2^{2n}}\right)$$

PRF Security of OMAC

Main Result

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{OMAC}}(\mathbf{Eve}) = O\left(\frac{q^2}{2^n} + \frac{q\ell^2}{2^n}\right)$$

PRF Security of OMAC

Main Result

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{OMAC}}(\mathbf{Eve}) = O\left(\frac{q^2}{2^n} + \frac{q\ell^2}{2^n}\right) \text{ i.e. } \mathbf{Eve} \text{ needs } \min\left\{\sqrt{2^n}, 2^n/\ell^2\right\} \text{ queries}$$

PRF Security of OMAC

Main Result

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{OMAC}}(\mathbf{Eve}) = O\left(\frac{q^2}{2^n} + \frac{q\ell^2}{2^n}\right) \text{ i.e. } \mathbf{Eve} \text{ needs } \min\left\{\sqrt{2^n}, 2^n/\ell^2\right\} \text{ queries}$$

$\left(\text{Existing: } \sqrt{2^n/\ell} \text{ queries}\right)$

$\left(\text{Folklore: } \sqrt{2^n} \text{ queries}\right)$

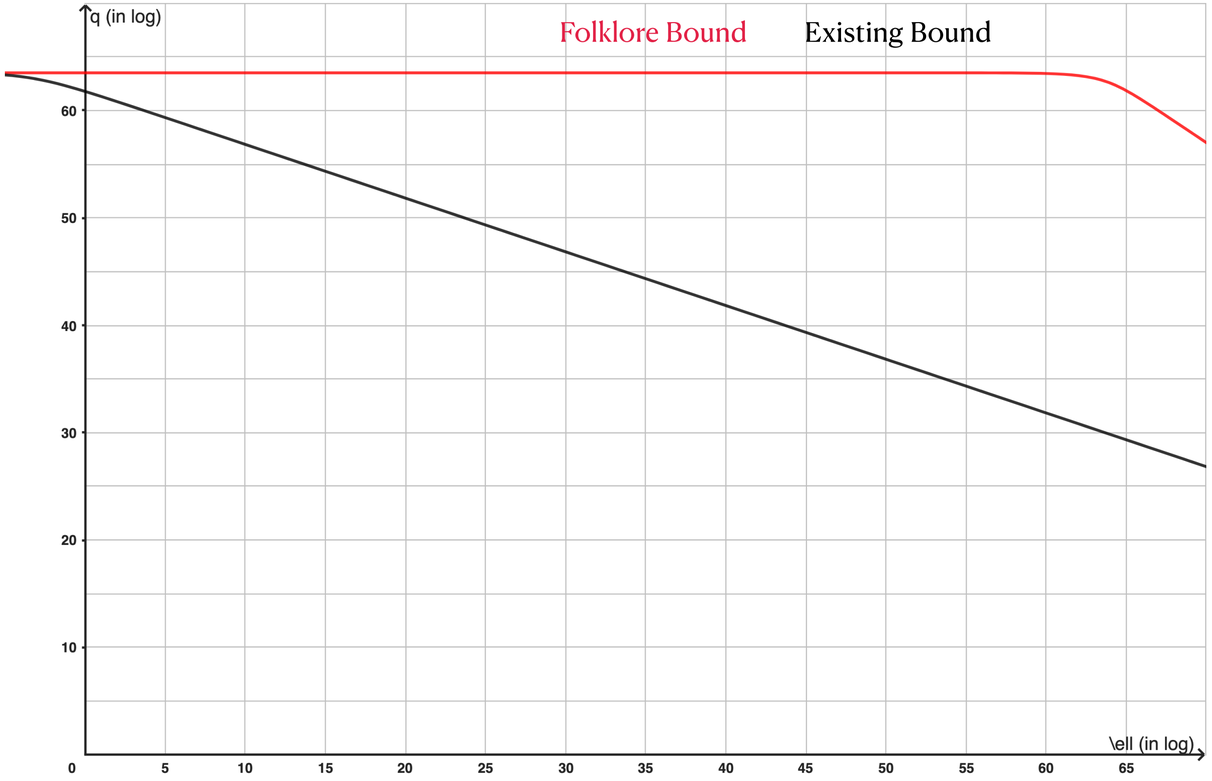
PRF Security of OMAC

Main Result

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{OMAC}}(\mathbf{Eve}) = O\left(\frac{q^2}{2^n} + \frac{q\ell^2}{2^n}\right) \text{ i.e. } \mathbf{Eve} \text{ needs } \min\left\{\sqrt{2^n}, 2^n/\ell^2\right\} \text{ queries}$$

$\left(\text{Existing: } \sqrt{2^n/\ell} \text{ queries}\right)$

$\left(\text{Folklore: } \sqrt{2^n} \text{ queries}\right)$



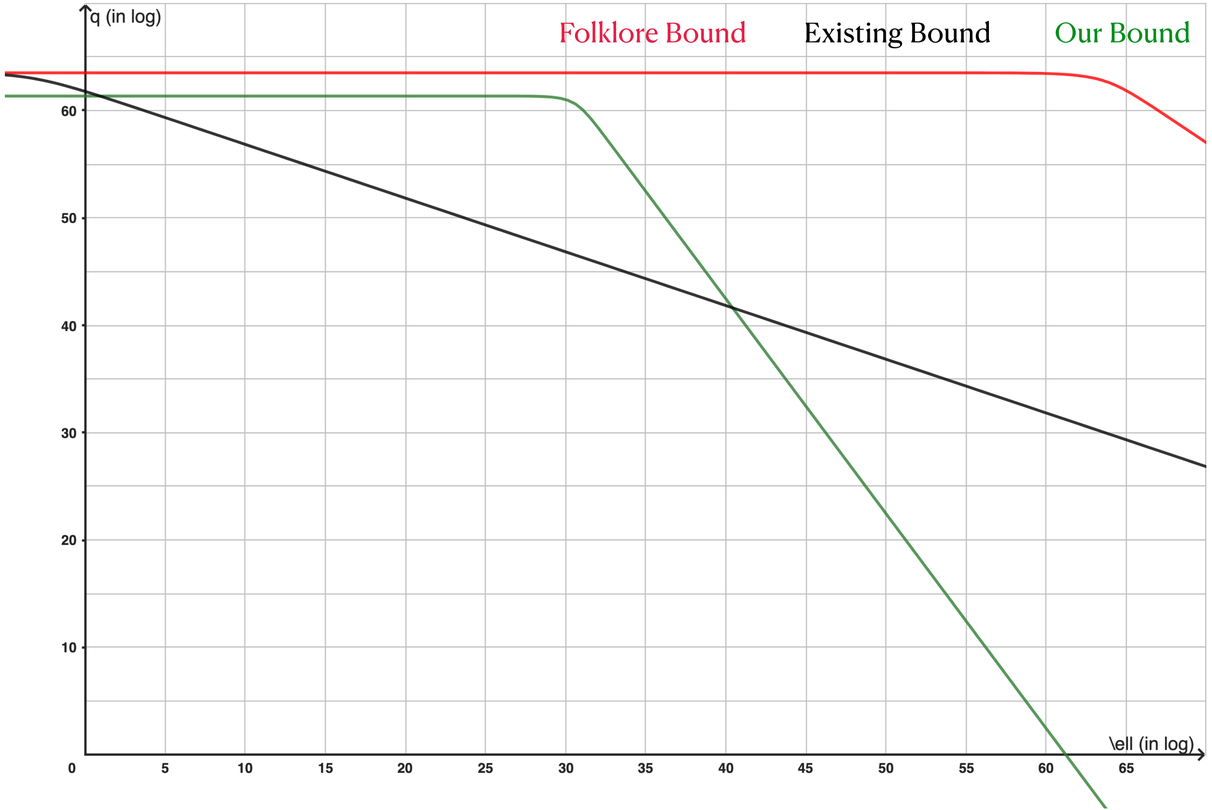
PRF Security of OMAC

Main Result

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{OMAC}}(\mathbf{Eve}) = O\left(\frac{q^2}{2^n} + \frac{q\ell^2}{2^n}\right) \text{ i.e. } \mathbf{Eve} \text{ needs } \min\left\{\sqrt{2^n}, 2^n/\ell^2\right\} \text{ queries}$$

$\left(\text{Existing: } \sqrt{2^n/\ell} \text{ queries}\right)$

$\left(\text{Folklore: } \sqrt{2^n} \text{ queries}\right)$



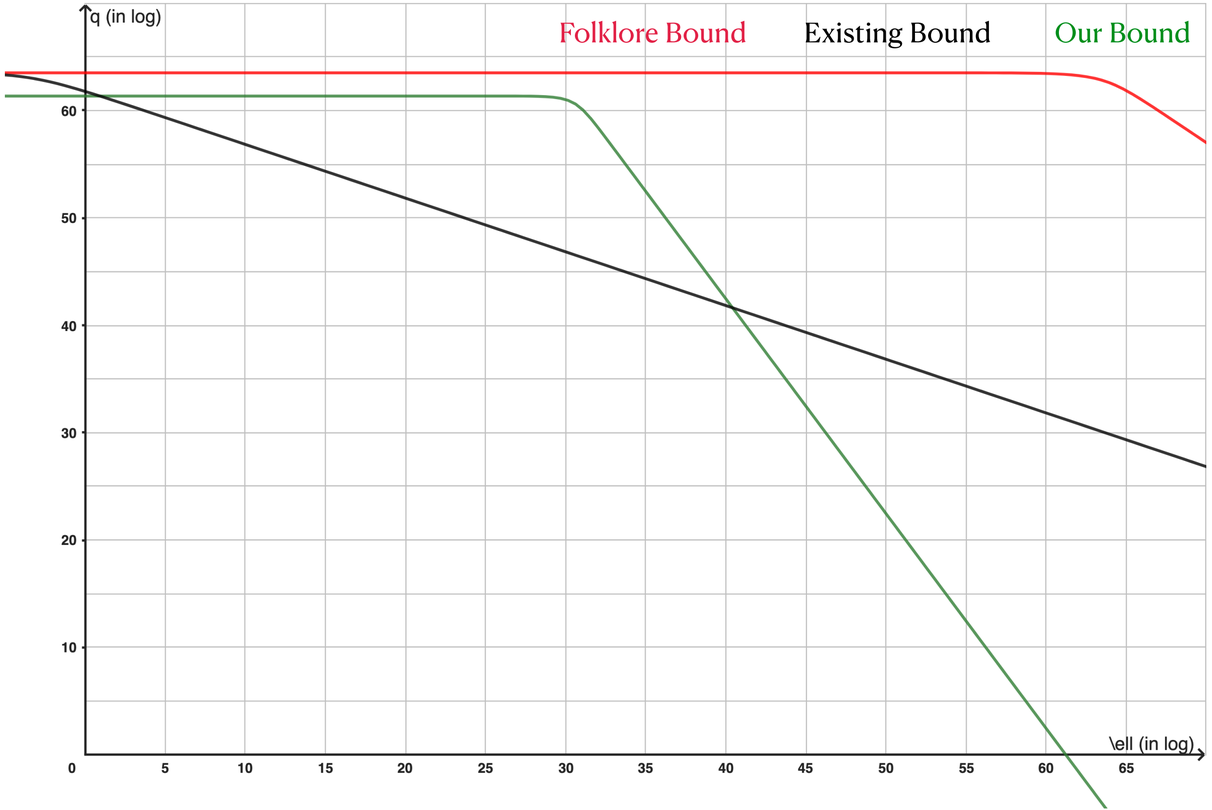
PRF Security of OMAC

Main Result

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{OMAC}}(\mathbf{Eve}) = O\left(\frac{q^2}{2^n} + \frac{q\ell^2}{2^n}\right) \text{ i.e. } \mathbf{Eve} \text{ needs } \min\left\{\sqrt{2^n}, 2^n/\ell^2\right\} \text{ queries}$$

$$\left(\text{Existing: } \sqrt{2^n/\ell} \text{ queries}\right)$$

$$\left(\text{Folklore: } \sqrt{2^n} \text{ queries}\right)$$



OMAC* is (almost) birthday bound secure.

* see full paper for similar results on XCBC and TMAC

Future Directions

- New applications of reset-sampling.
- Relaxation in the restriction on message lengths.
- An abstract formalization of the reset-sampling philosophy.

Future Directions

- New applications of reset-sampling.
- Relaxation in the restriction on message lengths.
- An abstract formalization of the reset-sampling philosophy.

Thank you