Reset-Sampling: Fine-tuning the Security of Standardized MACs

Ashwin Jha
CISPA Helmholtz Center for Information Security

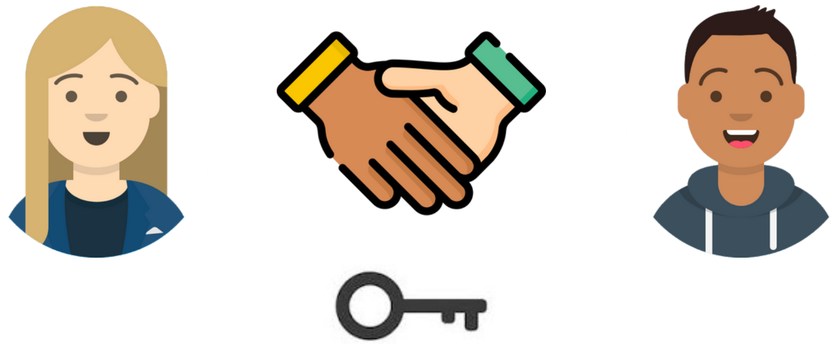
CRC Seminar Series, TII, Abu Dhabi
November 3rd, 2022

Reset-Sampling: Fine-tuning the Security of Standardized MACs

- MACs and their security
- LightMAC & OMAC
- Observations on the Security
- Some fine-tunings

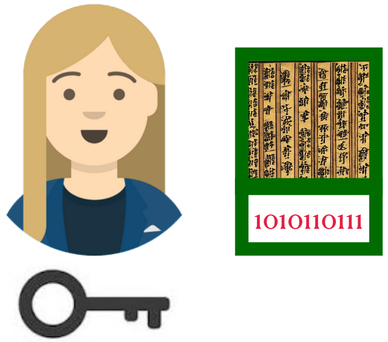
Message Authentication Codes (MAC)

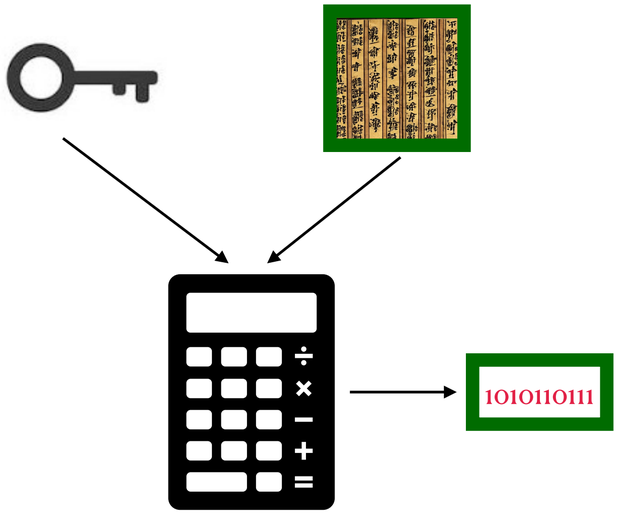
Message Authentication Codes (MAC)



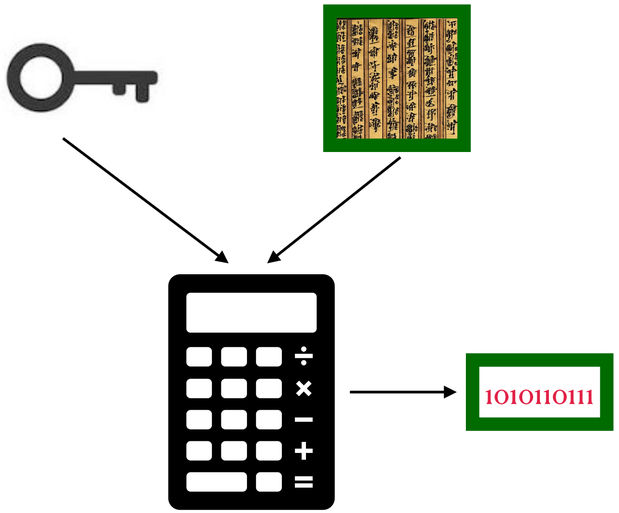
Message Authentication Codes (MAC)

Message Authentication Codes (MAC)

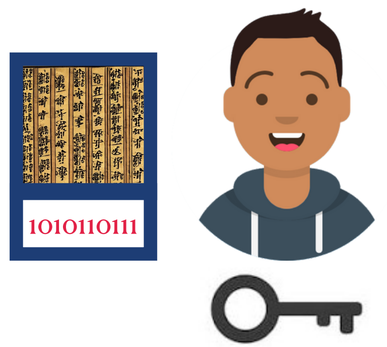


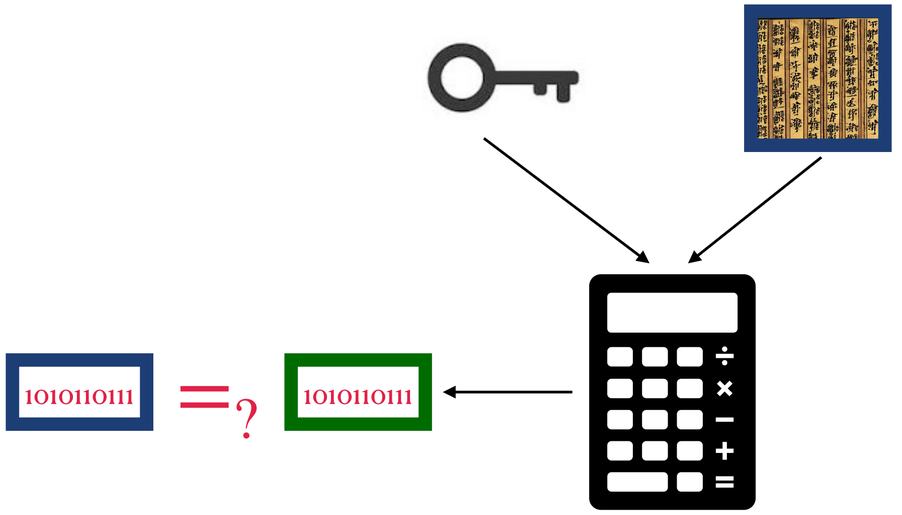


Message Authentication Codes (MAC)



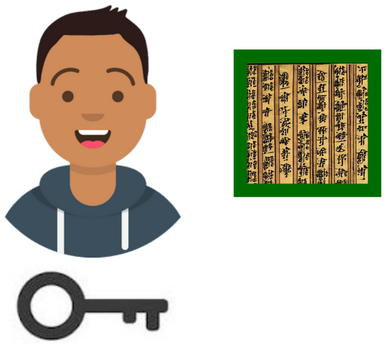
Message Authentication Codes (MAC)

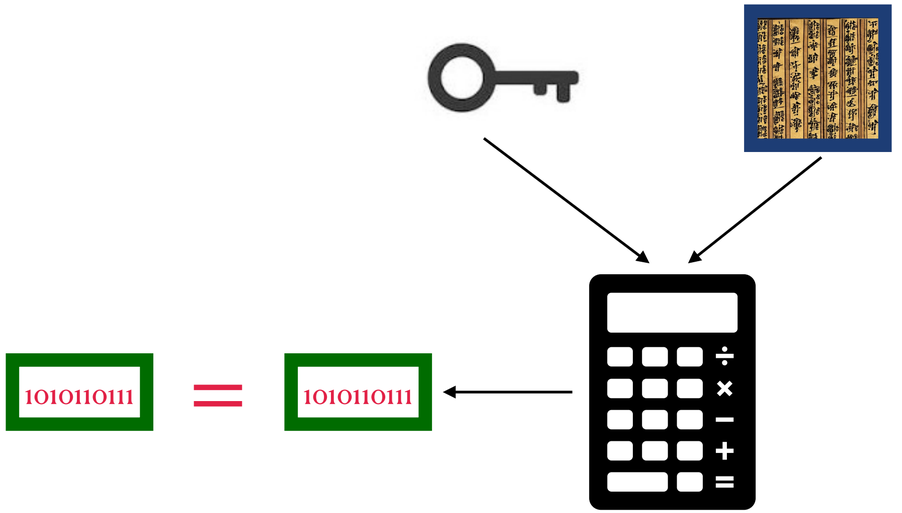




Message Authentication Codes (MAC)

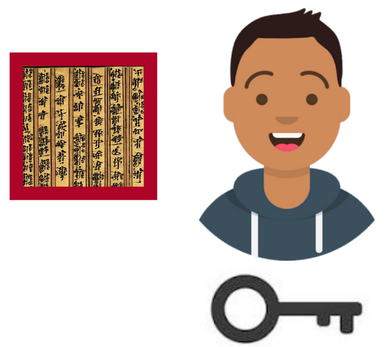
Authentication Succeeds

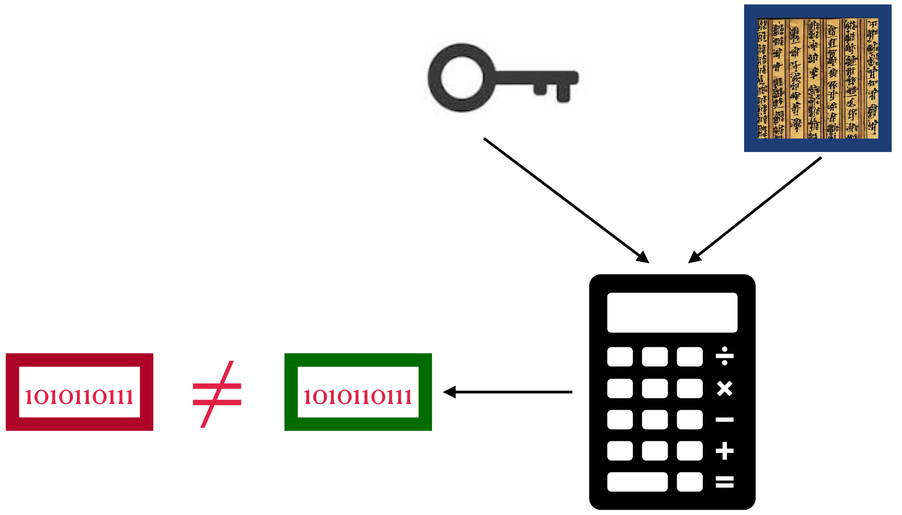




Message Authentication Codes (MAC)

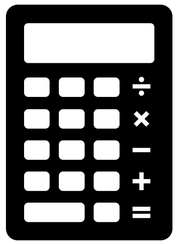
Authentication Fails





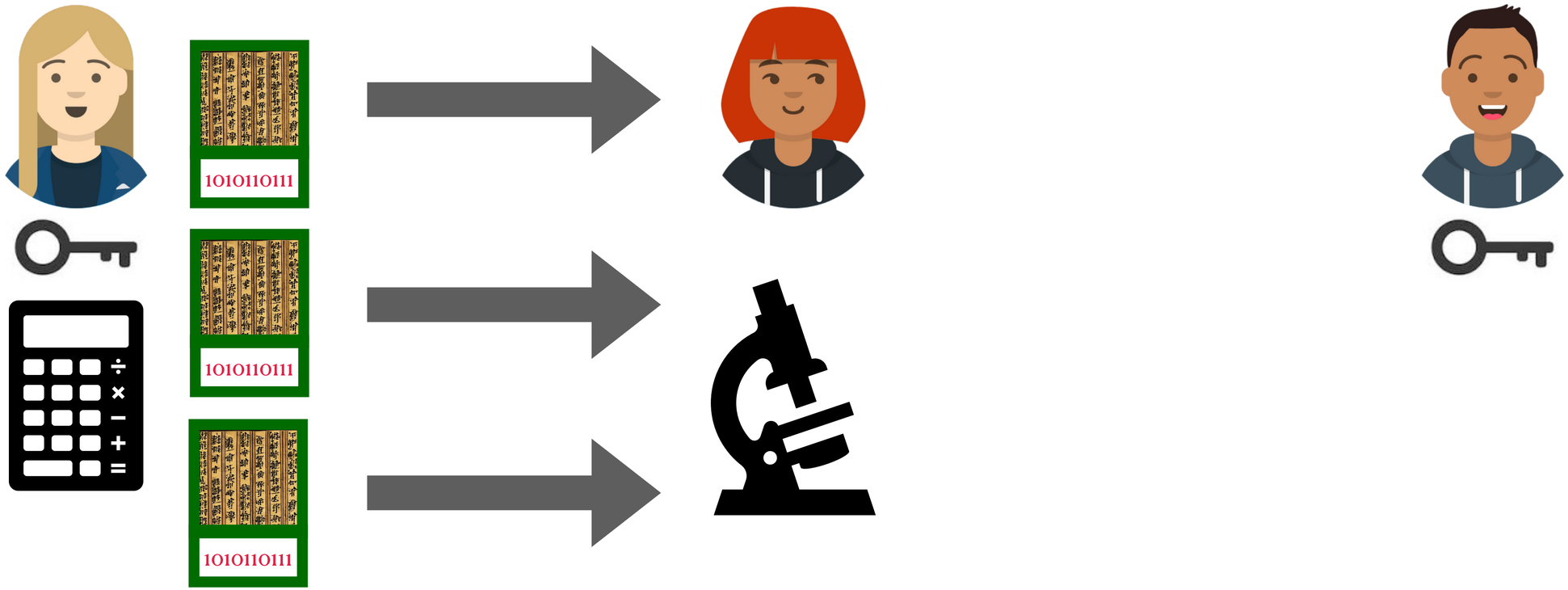
MAC Security

Unforgeability Game



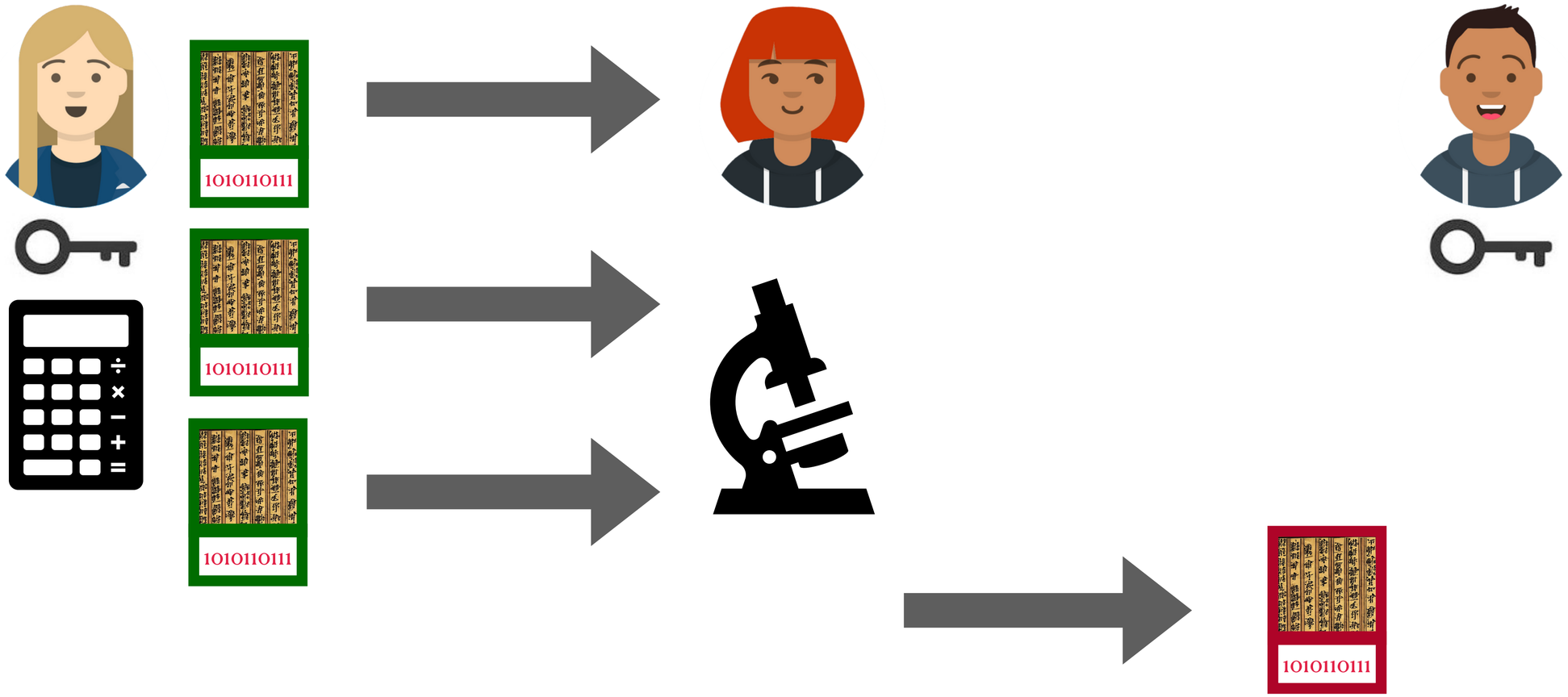
MAC Security

Unforgeability Game: Passive Adversary



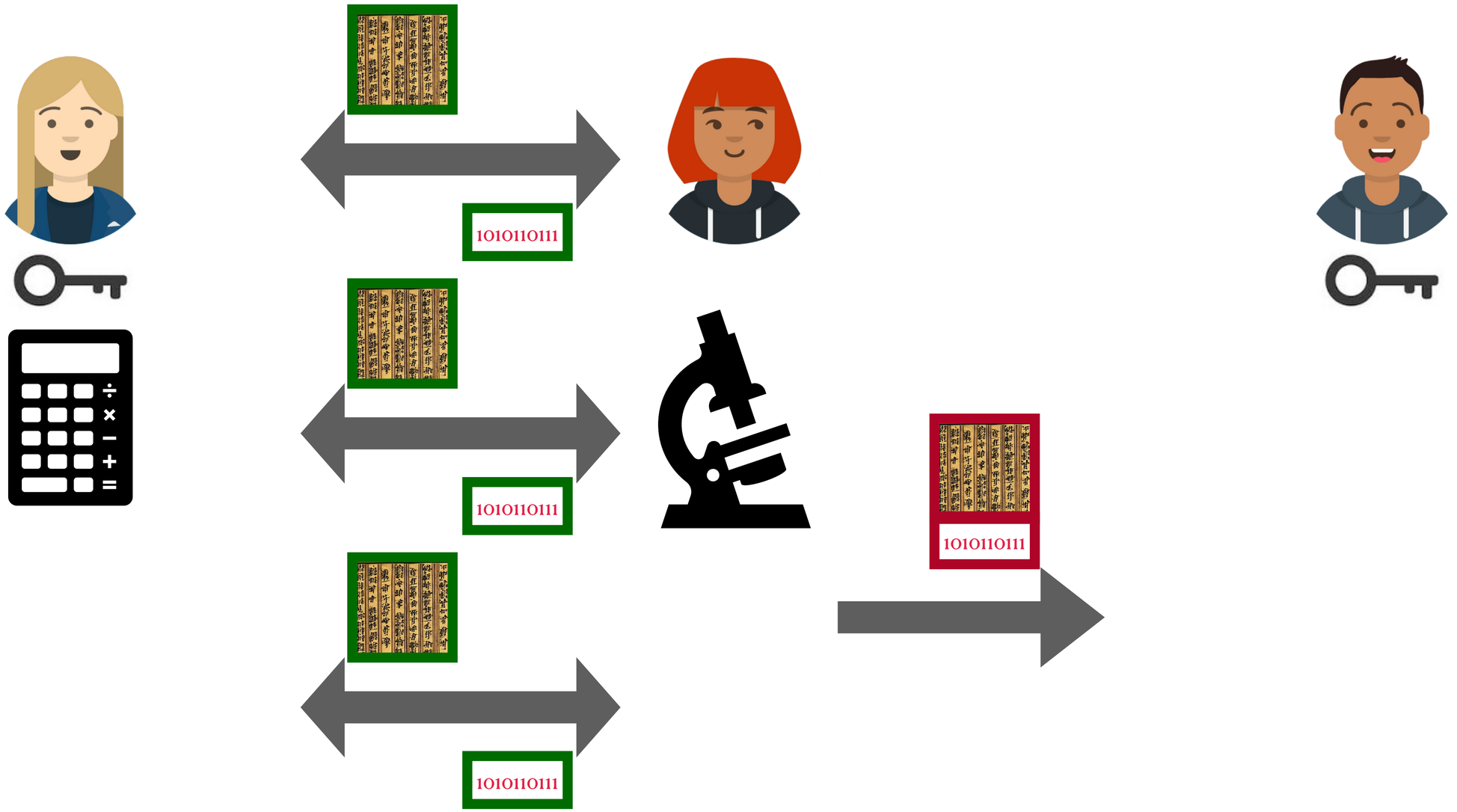
MAC Security

Unforgeability Game: Passive Adversary



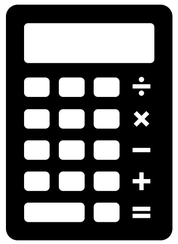
MAC Security

Unforgeability Game: Active Adversary



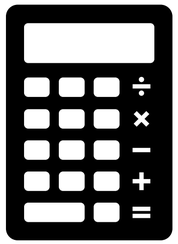
MAC Security

Unforgeability Game: Forgery Succeeds



MAC Security

Unforgeability Game: Forgery Succeeds



$$\Pr(\text{Forgery Succeeds})$$

MAC Security

Random Functions are Good MACs

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

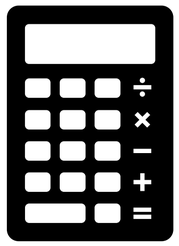
Pseudorandom Function Security

Ideal World (0)

Pseudorandom Function Security

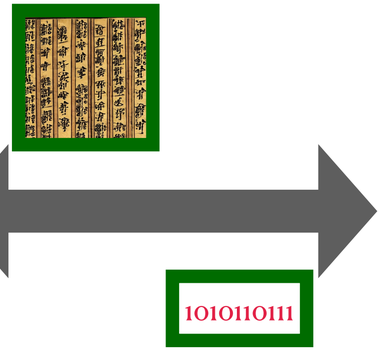
Ideal World (0)

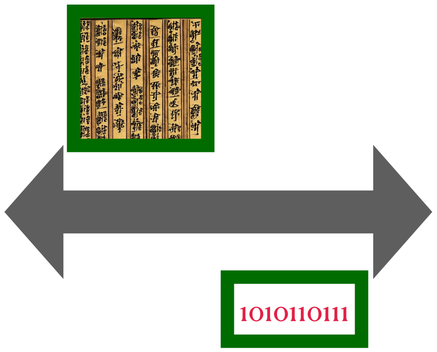
Real World (1)



Pseudorandom Function Security

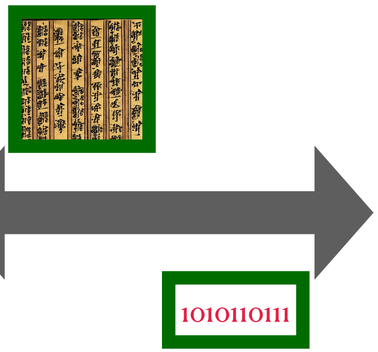
Ideal World (0)

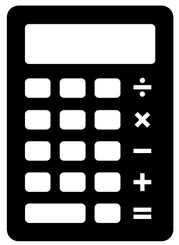


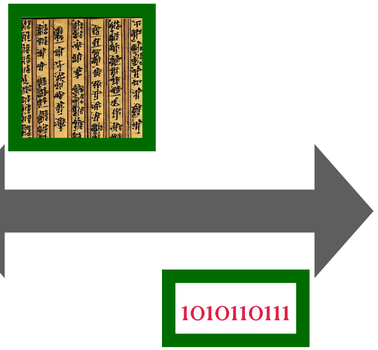


b

Real World (1)

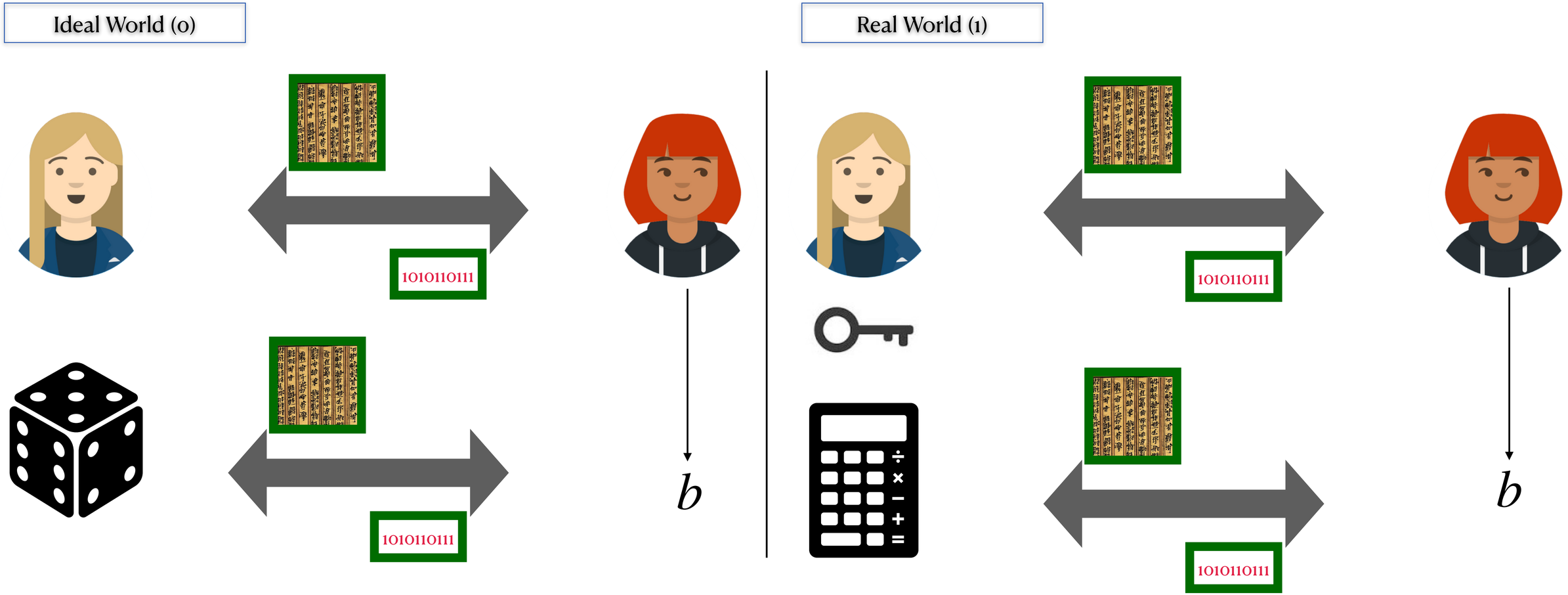






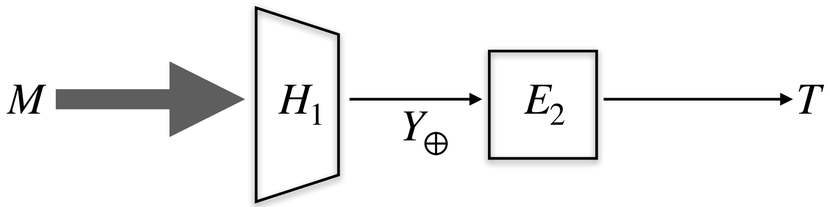
b

Pseudorandom Function Security



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

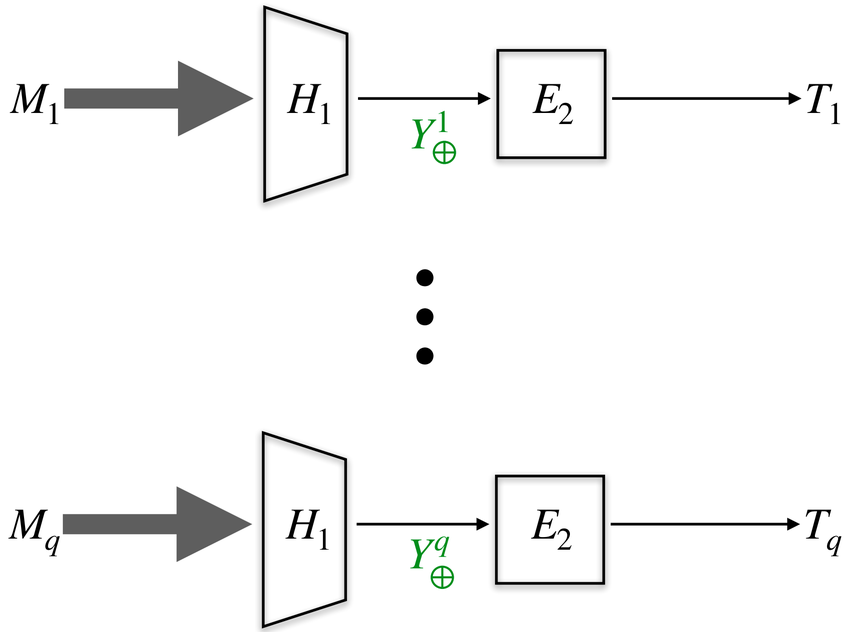
Hash then PRF



- $H_1 : \{0,1\}^* \rightarrow \{0,1\}^n$
- E_1 a permutation of $\{0,1\}^n$
- $H_1 \perp E_1$

Hash then PRF

High Level Security Argument



$Y^1_\oplus \neq \cdots \neq Y^q_\oplus \implies T_1, \ldots, T_q$ are independent and uniform

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{HtPRF}}(\mathbf{Eve}) \leq \overbrace{\Pr\left(\exists i \neq j \ : \ Y^i_\oplus = Y^j_\oplus\right)}^{\text{Maximum Collision Probability of } H_1}$$

LightMAC

LuykxPTY, IACR FSE 2016; ISO/IEC 29192-6:2019

LightMAC

LuykxPTY, IACR FSE 2016; ISO/IEC 29192-6:2019

$(M[1], \ldots, M[\ell + 1]) \xleftarrow{n-s} M$

LightMAC

LuykxPTY, IACR FSE 2016; ISO/IEC 29192-6:2019

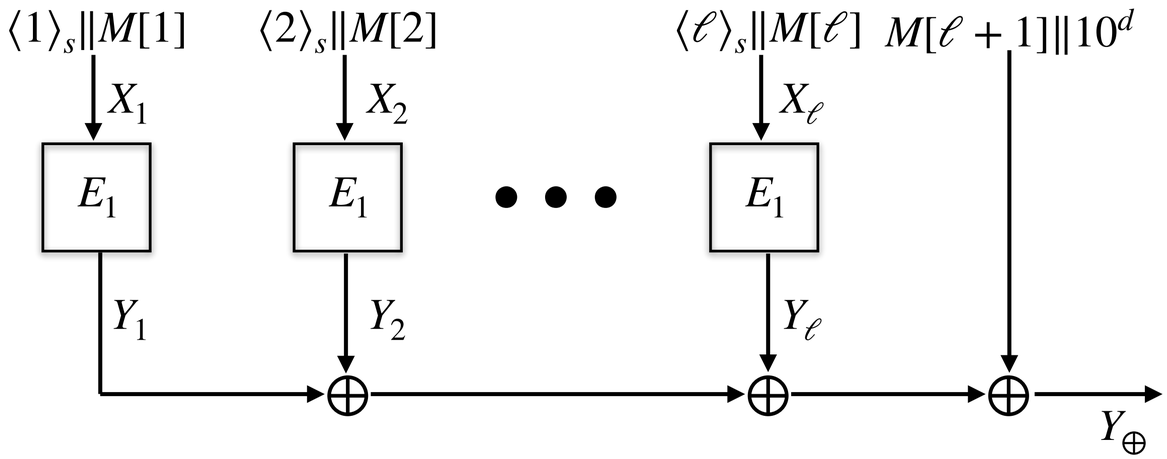
$(M[1], \ldots, M[\ell + 1]) \xleftarrow{n-s} M$

$\langle 1 \rangle_s \| M[1] \qquad \langle 2 \rangle_s \| M[2] \qquad \langle \ell \rangle_s \| M[\ell] \;\; M[\ell + 1] \| 10^d$

LightMAC

LuykxPTY, IACR FSE 2016; ISO/IEC 29192-6:2019

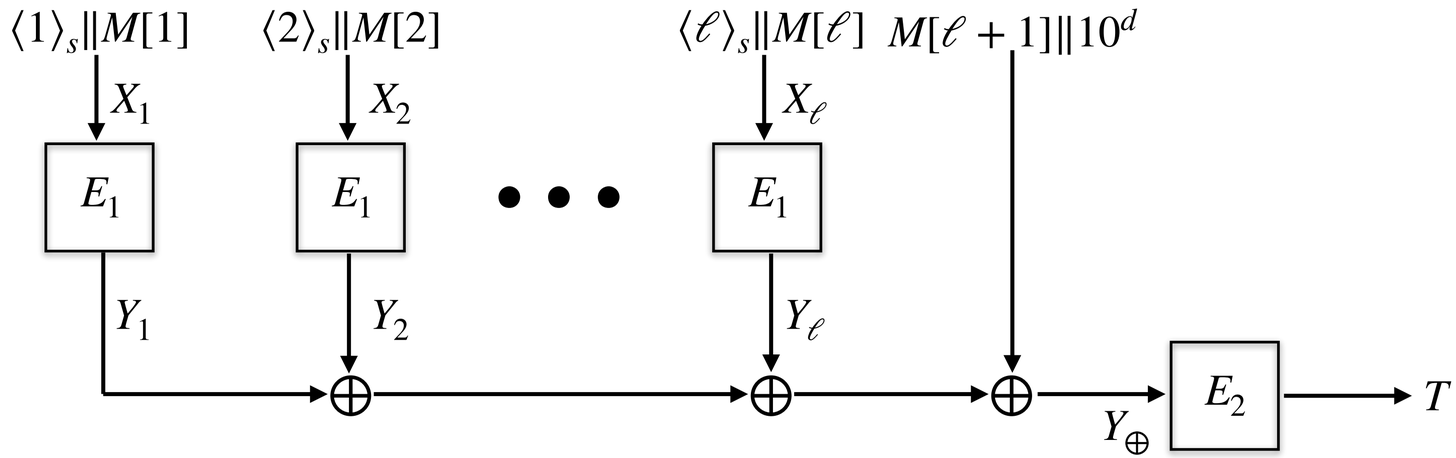
$(M[1], \ldots, M[\ell + 1]) \xleftarrow{n-s} M$



LightMAC

LuykxPTY, IACR FSE 2016; ISO/IEC 29192-6:2019

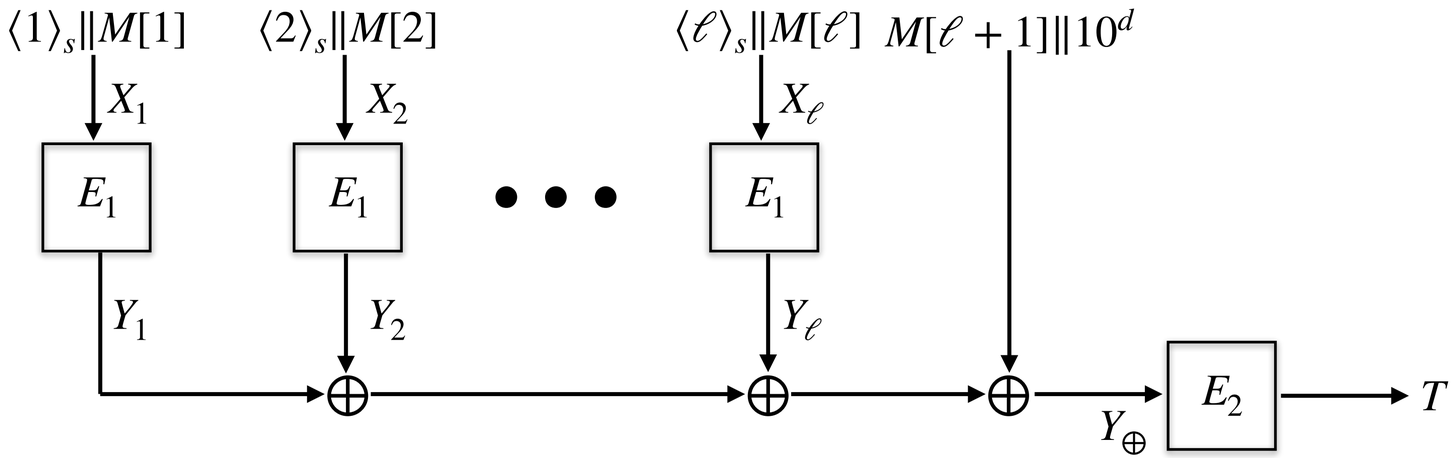
$(M[1], \ldots, M[\ell + 1]) \xleftarrow{n-s} M$



LightMAC

LuykxPTY, IACR FSE 2016; ISO/IEC 29192-6:2019

$(M[1], \ldots, M[\ell + 1]) \xleftarrow{n-s} M$

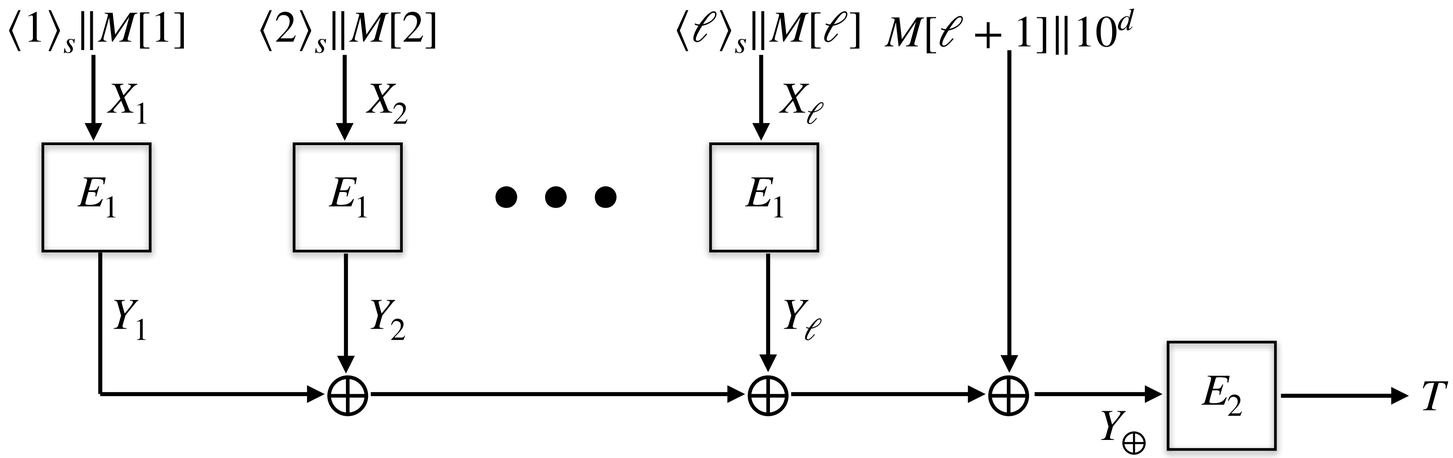


- Parallelizable yet compact.
- Birthday bound security: $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{LightMAC}}(\mathbf{Eve}) = O\left(\frac{q^2}{2^n}\right)$

LightMAC

LuykxPTY, IACR FSE 2016; ISO/IEC 29192-6:2019

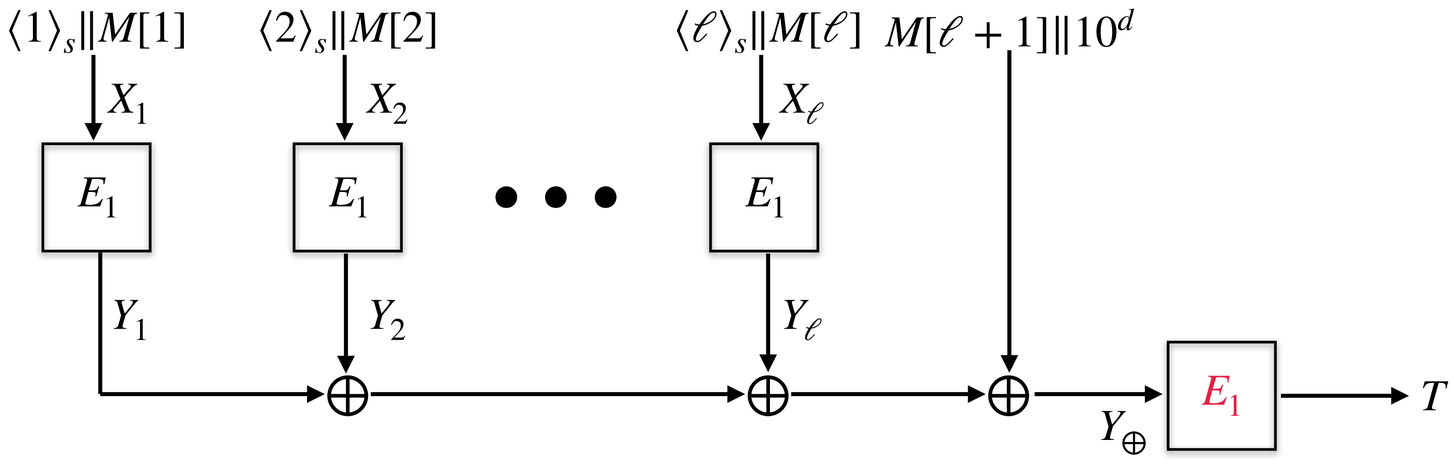
$(M[1], \ldots, M[\ell + 1]) \xleftarrow{n-s} M$



- Parallelizable yet compact.
- Birthday bound security: $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{LightMAC}}(\mathbf{Eve}) = O\left(\frac{q^2}{2^n}\right)$
- Two independent block cipher keys.

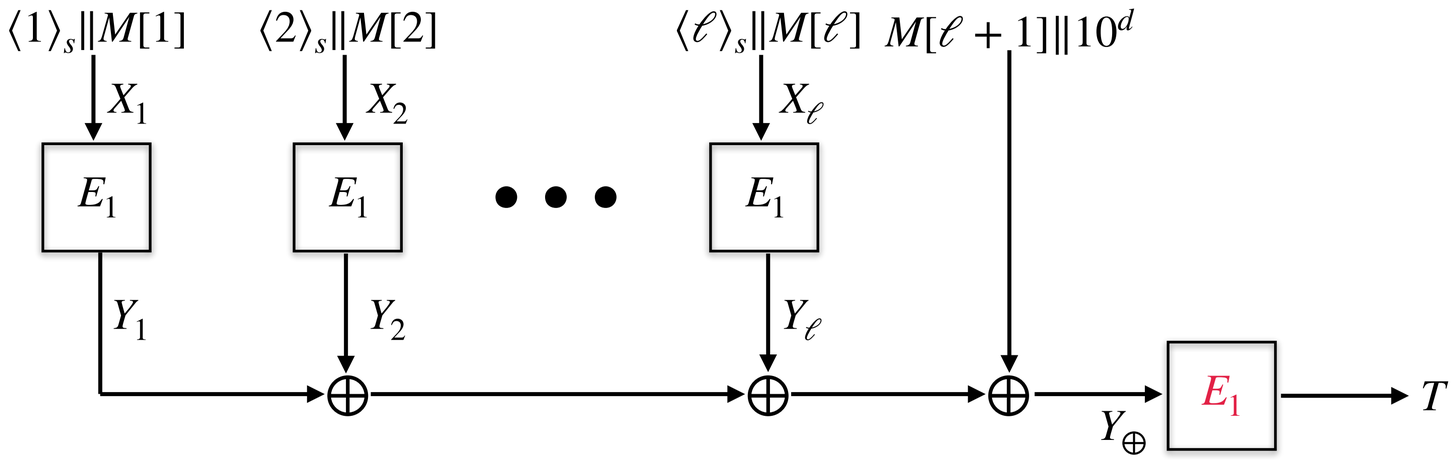
One-key LightMAC

ChattopadhyayJN, IACR ASIACRYPT 2021



One-key LightMAC

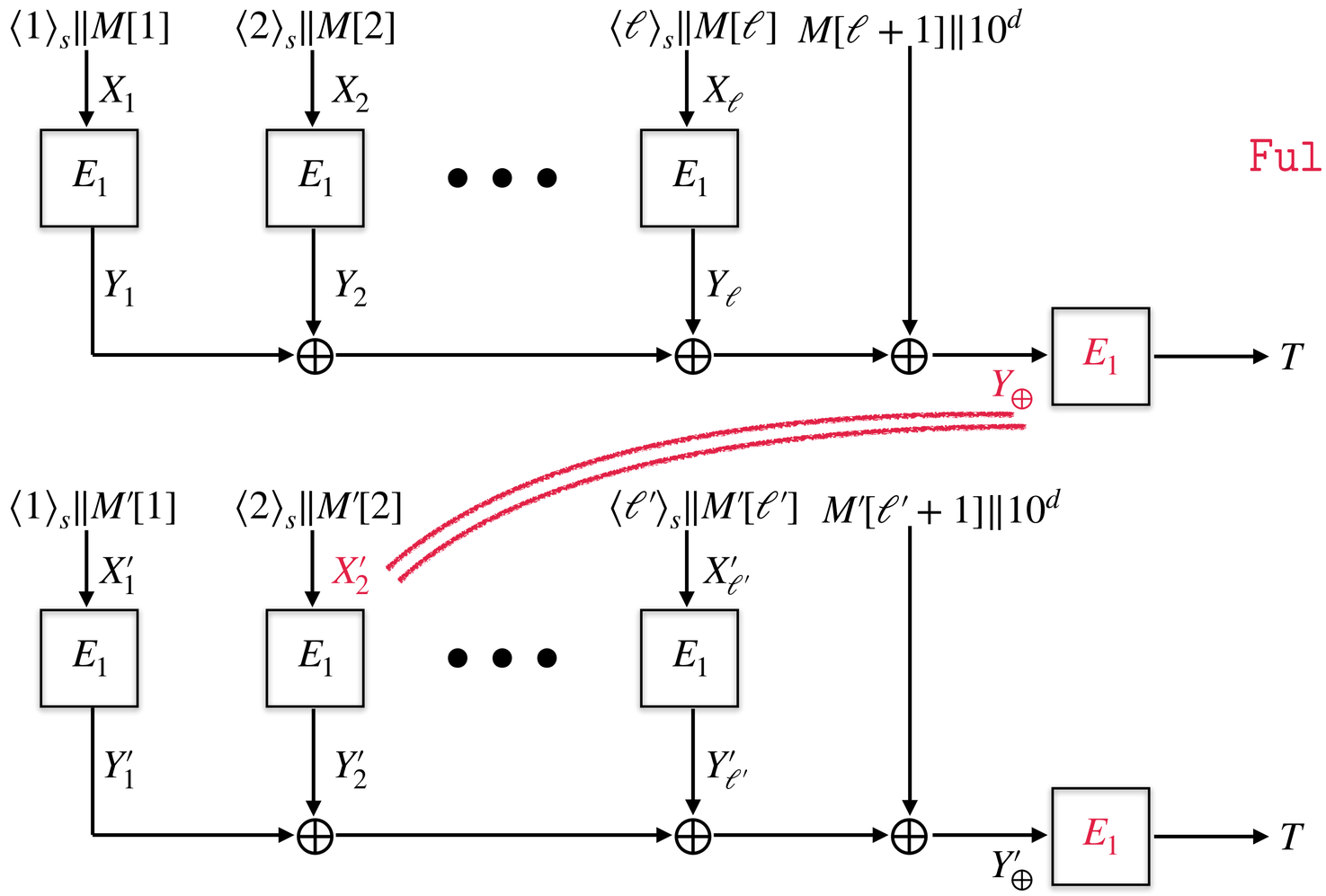
ChattopadhyayJN, IACR ASIACRYPT 2021



Is this secure?

One-key LightMAC

Full Collision Event

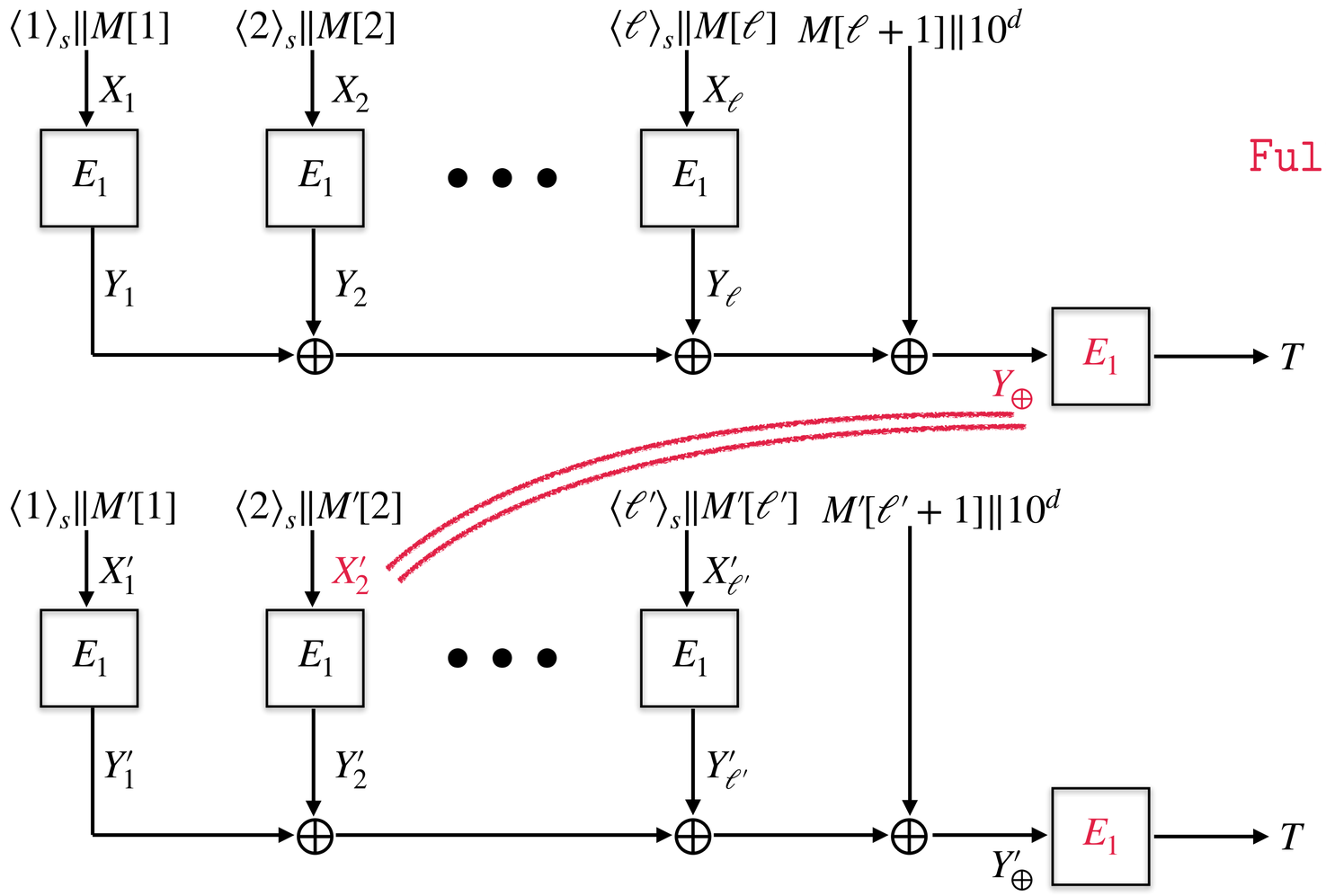


$$\texttt{Full Collision}: \quad \exists i, j, a, b \ : \ X_a^j = Y_\oplus^i$$

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

One-key LightMAC

Full Collision Event



$\texttt{Full Collision}: \quad \exists i, j, a, b \ : \ X_a^j = Y_\oplus^i$

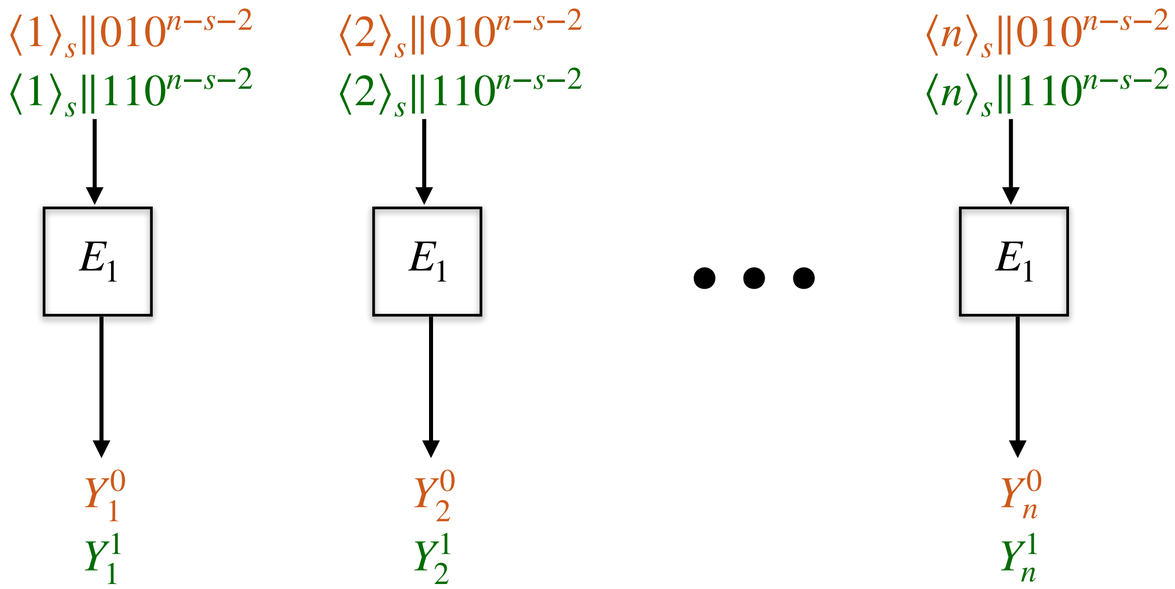
Is it even important?

One-key LightMAC

A Short Message Attack

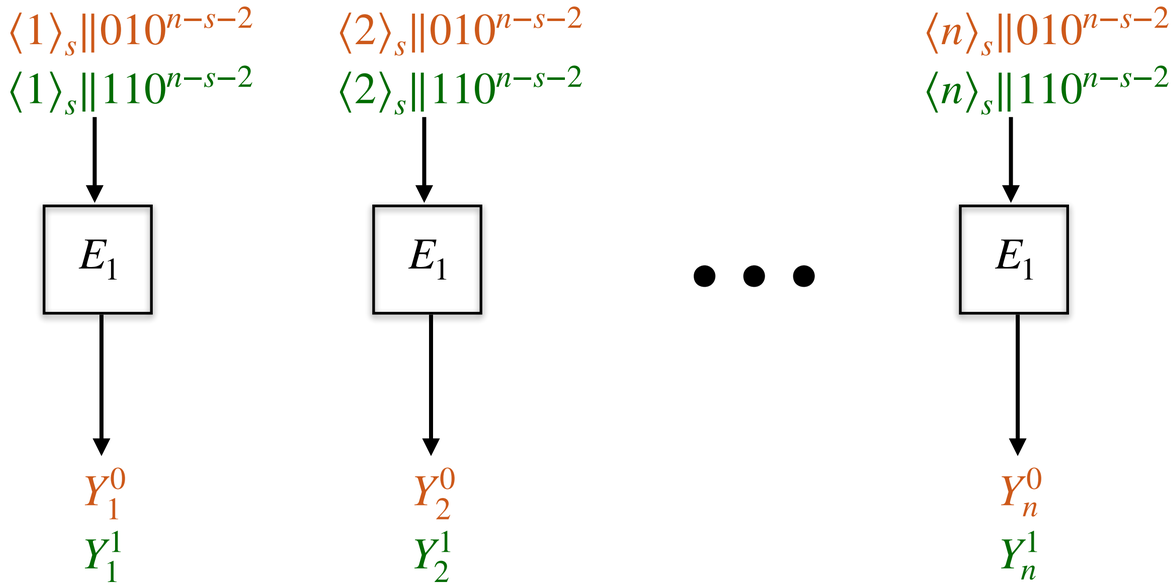
One-key LightMAC

A Short Message Attack



One-key LightMAC

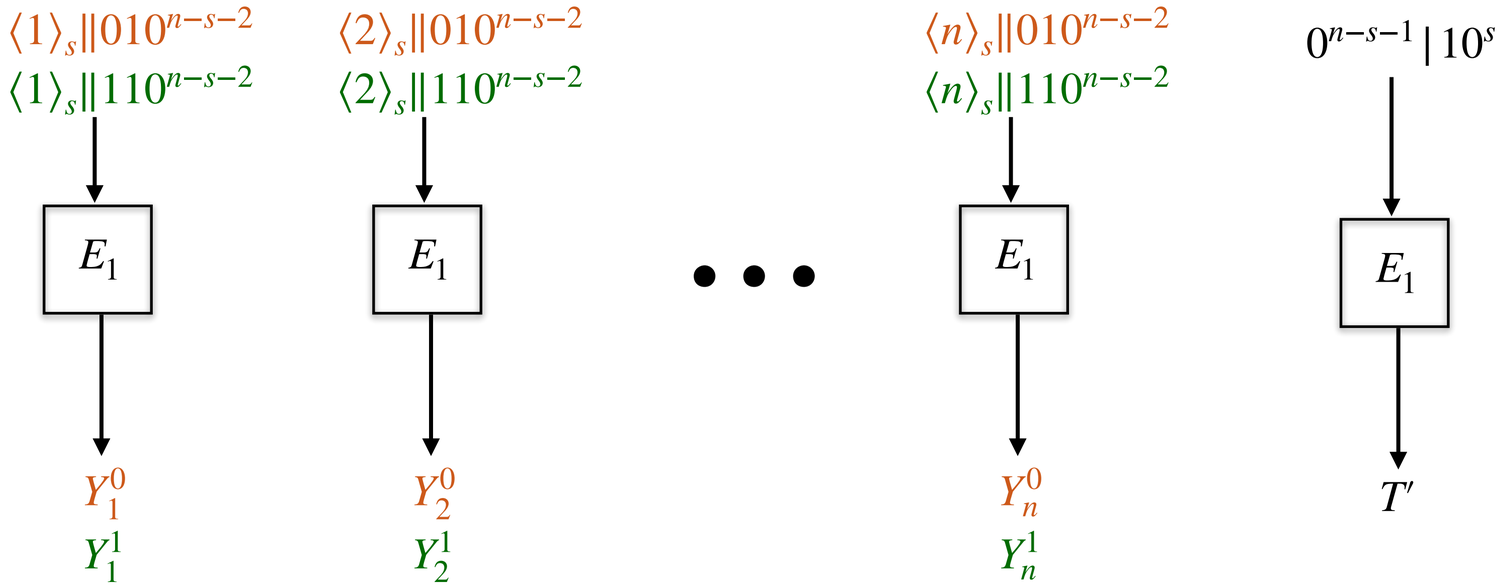
A Short Message Attack



- n lists each containing exactly 2 elements
- Using Generalized Birthday Problem: $\exists j_1, \ldots, j_n \in \{0,1\}$ such that $Y_1^{j_1} \oplus \cdots \oplus Y_n^{j_n} = 0^n$

One-key LightMAC

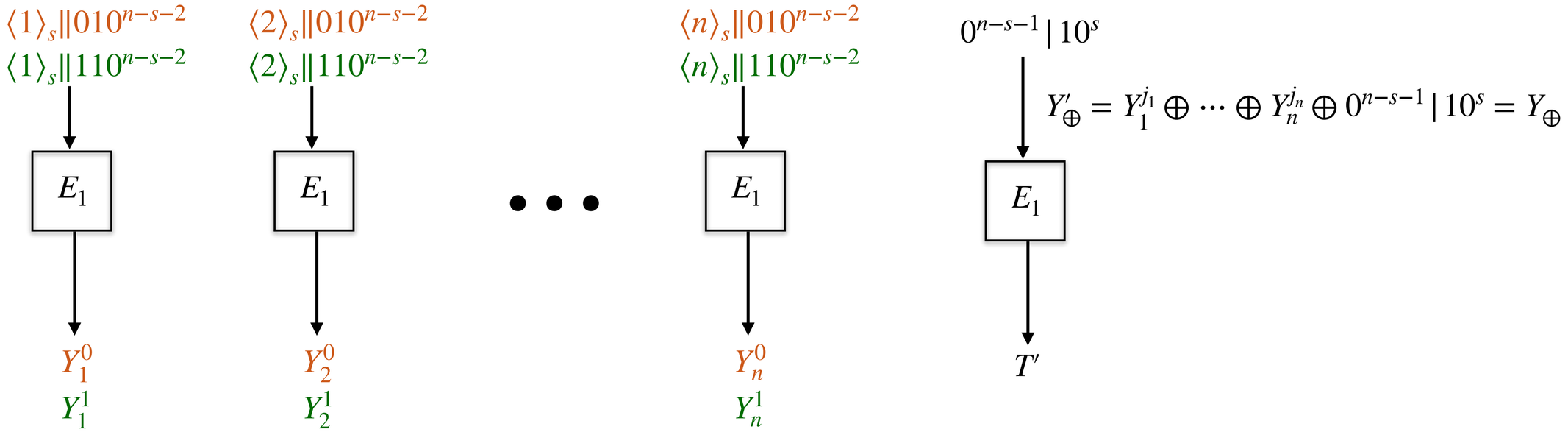
A Short Message Attack



- n lists each containing exactly 2 elements
- Using Generalized Birthday Problem: $\exists j_1, \ldots, j_n \in \{0,1\}$ such that $Y_1^{j_1} \oplus \cdots \oplus Y_n^{j_n} = 0^n$
- Construct $M = j_1 \| 10^{n-s-2} \| \cdots \| j_n \| 10^{n-s-2} \| 0^{n-s-1}$ and $M' = 0^{n-s-1}$

One-key LightMAC

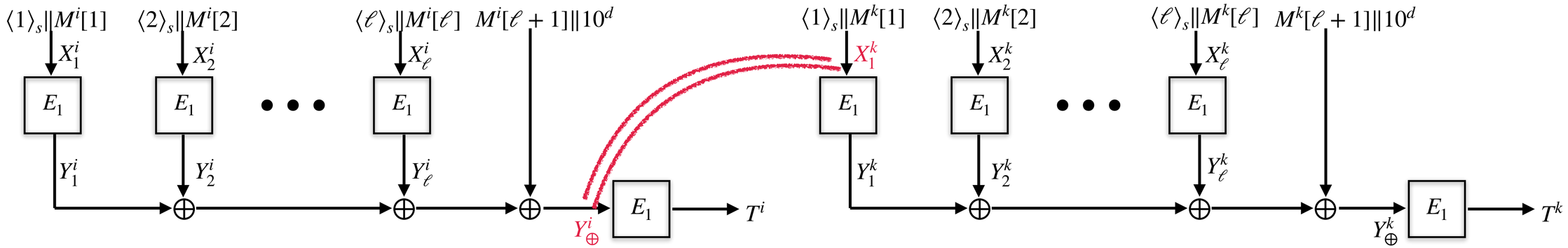
A Short Message Attack



- n lists each containing exactly 2 elements
- Using Generalized Birthday Problem: $\exists j_1, \ldots, j_n \in \{0,1\}$ such that $Y_1^{j_1} \oplus \cdots \oplus Y_n^{j_n} = 0^n$
- Construct $M = j_1 \| 10^{n-s-2} \| \cdots \| j_n \| 10^{n-s-2} \| 0^{n-s-1}$ and $M' = 0^{n-s-1}$
- $Y_\oplus = Y'_\oplus \implies T = T'$ (Collision on output leads to forgery)

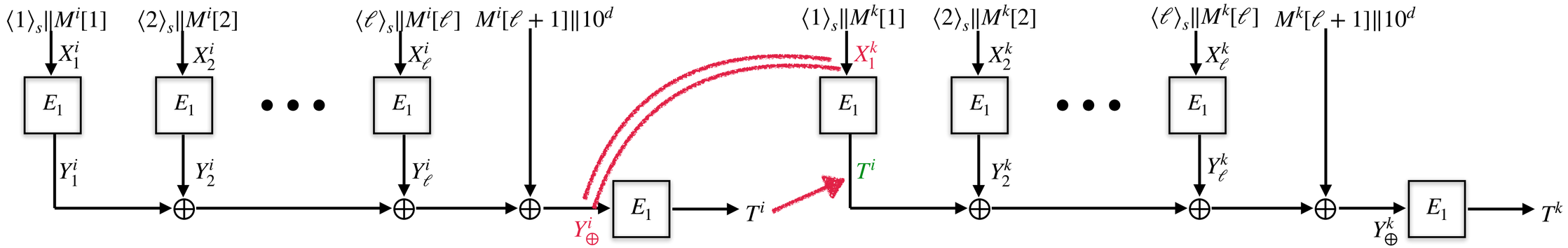
One-key LightMAC

Reset-Sampling



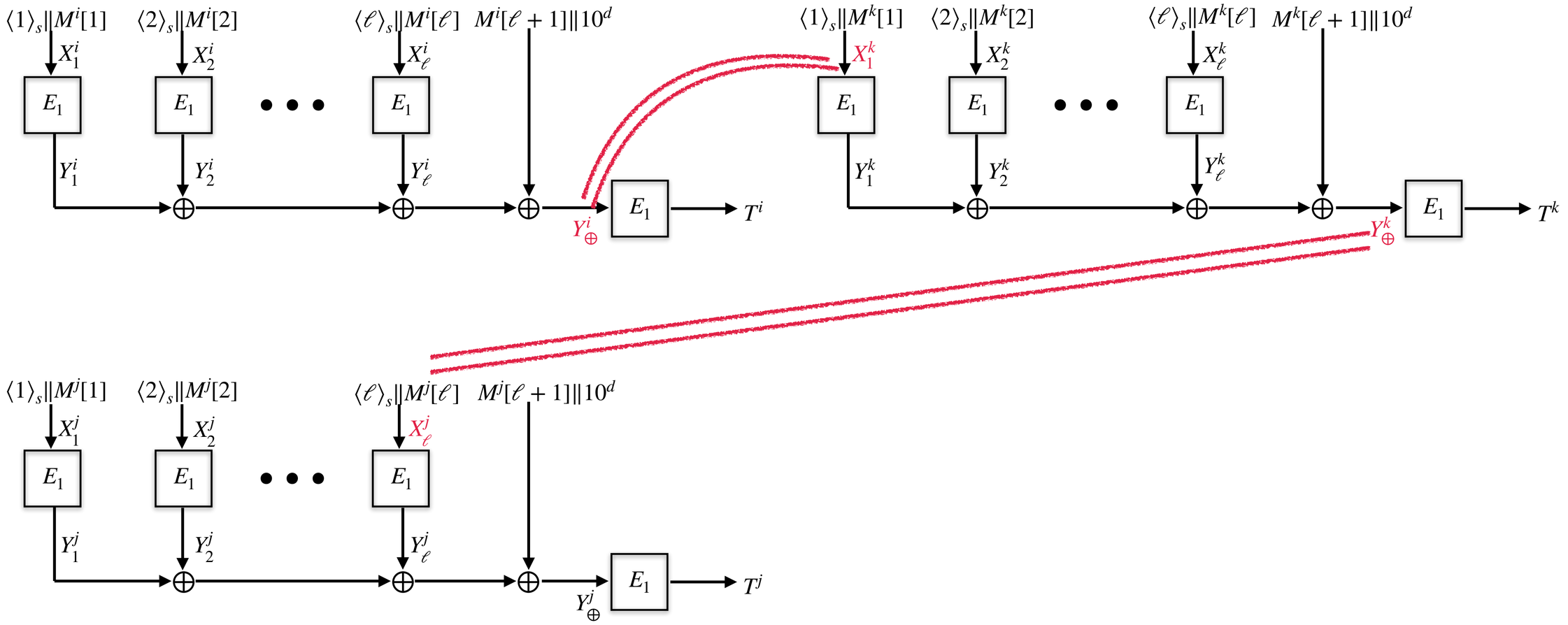
One-key LightMAC

Reset-Sampling



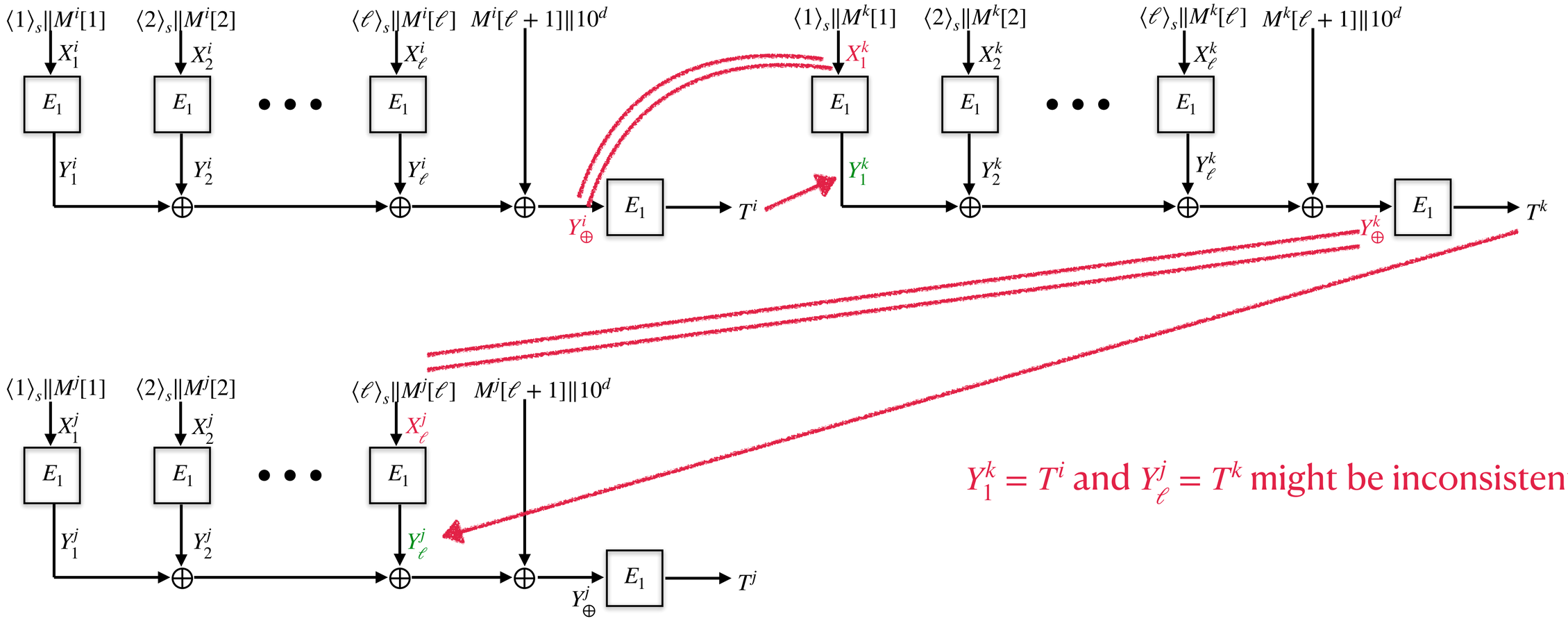
One-key LightMAC

Reset-Sampling



One-key LightMAC

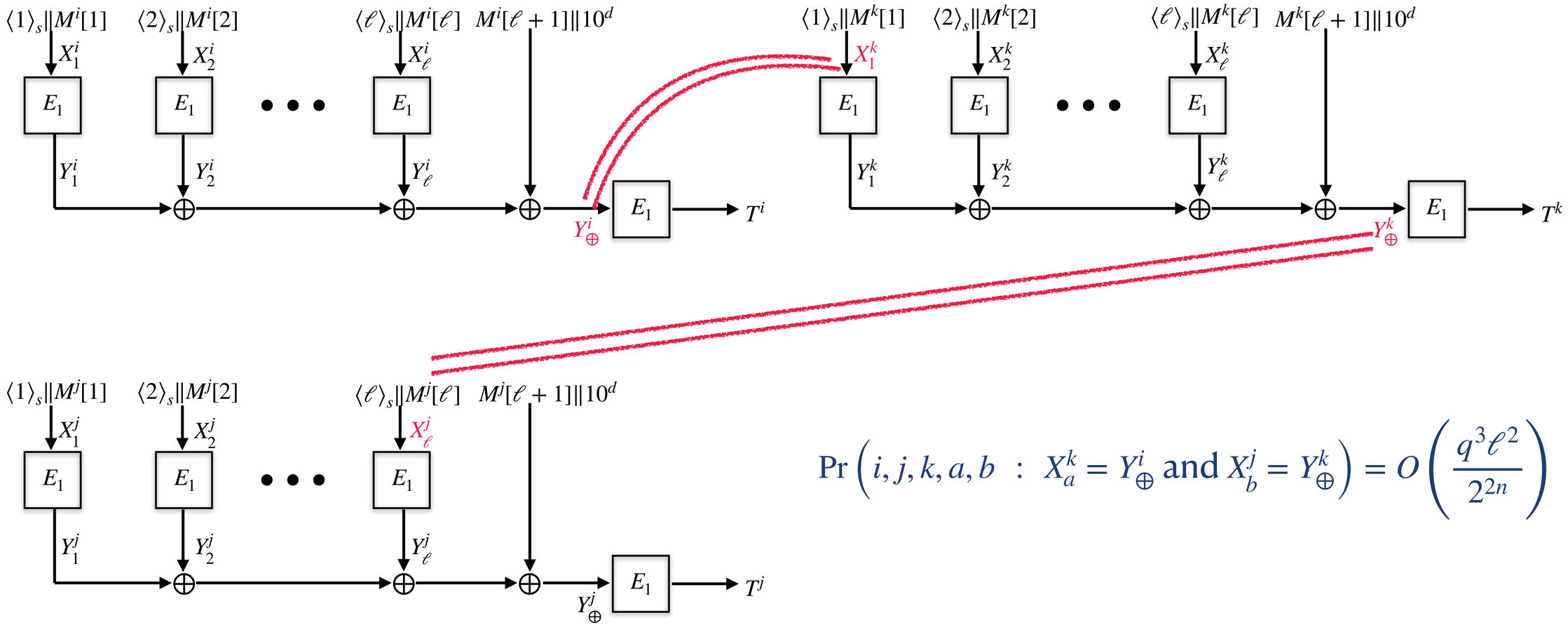
Reset-Sampling



$Y_1^k = T^i$ and $Y_\ell^j = T^k$ might be inconsistent

One-key LightMAC

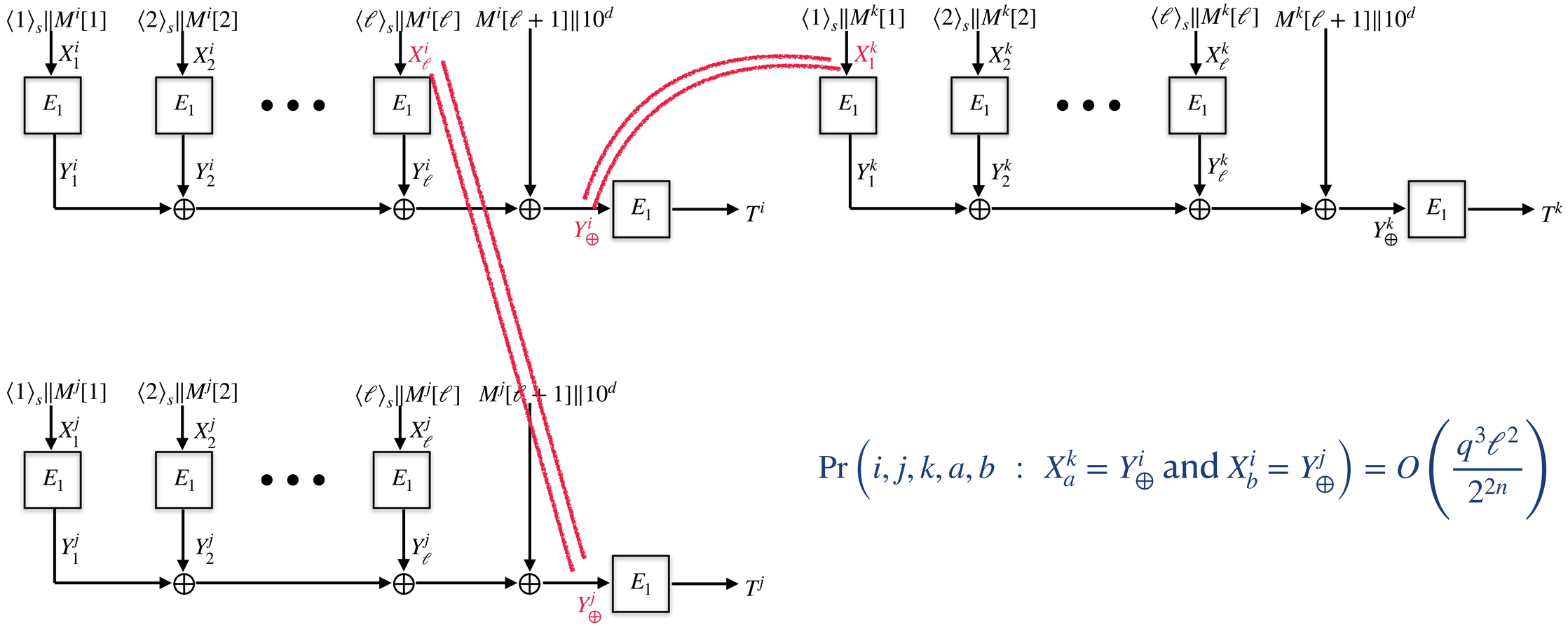
Reset-Sampling



$$\Pr\left(i,j,k,a,b \ : \ X_a^k = Y_\oplus^i \text{ and } X_b^j = Y_\oplus^k\right) = O\left(\frac{q^3\ell^2}{2^{2n}}\right)$$

One-key LightMAC

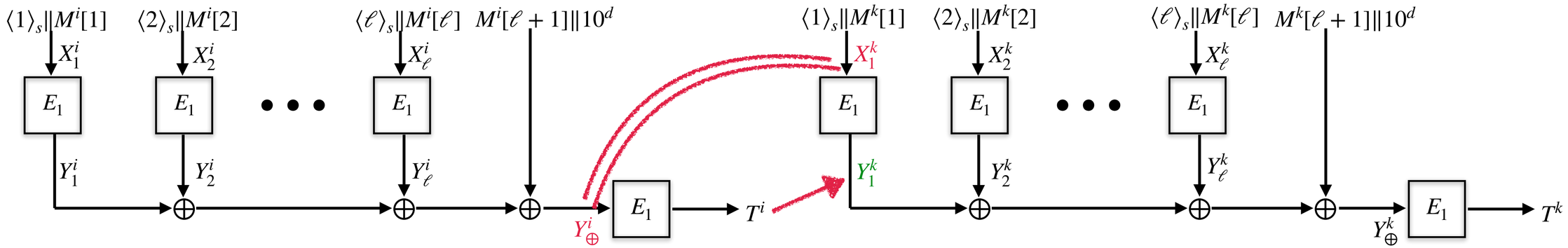
Reset-Sampling



$$\Pr\left(i,j,k,a,b \ : \ X_a^k = Y_\oplus^i \text{ and } X_b^i = Y_\oplus^j\right) = O\left(\frac{q^3\ell^2}{2^{2n}}\right)$$

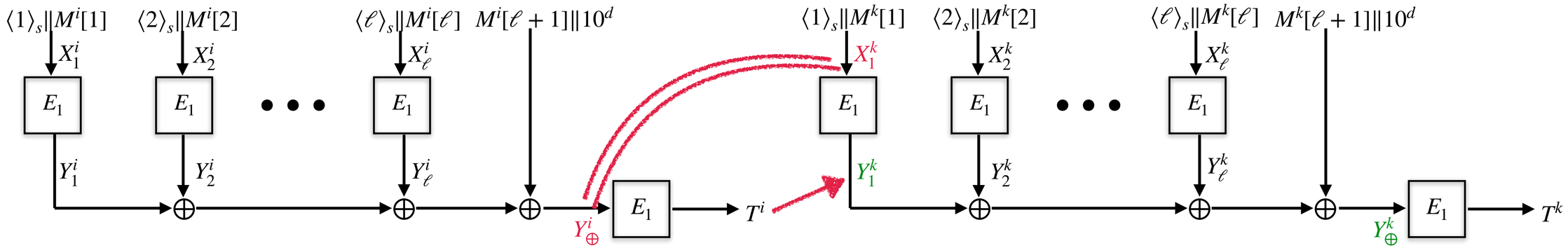
One-key LightMAC

Reset-Sampling



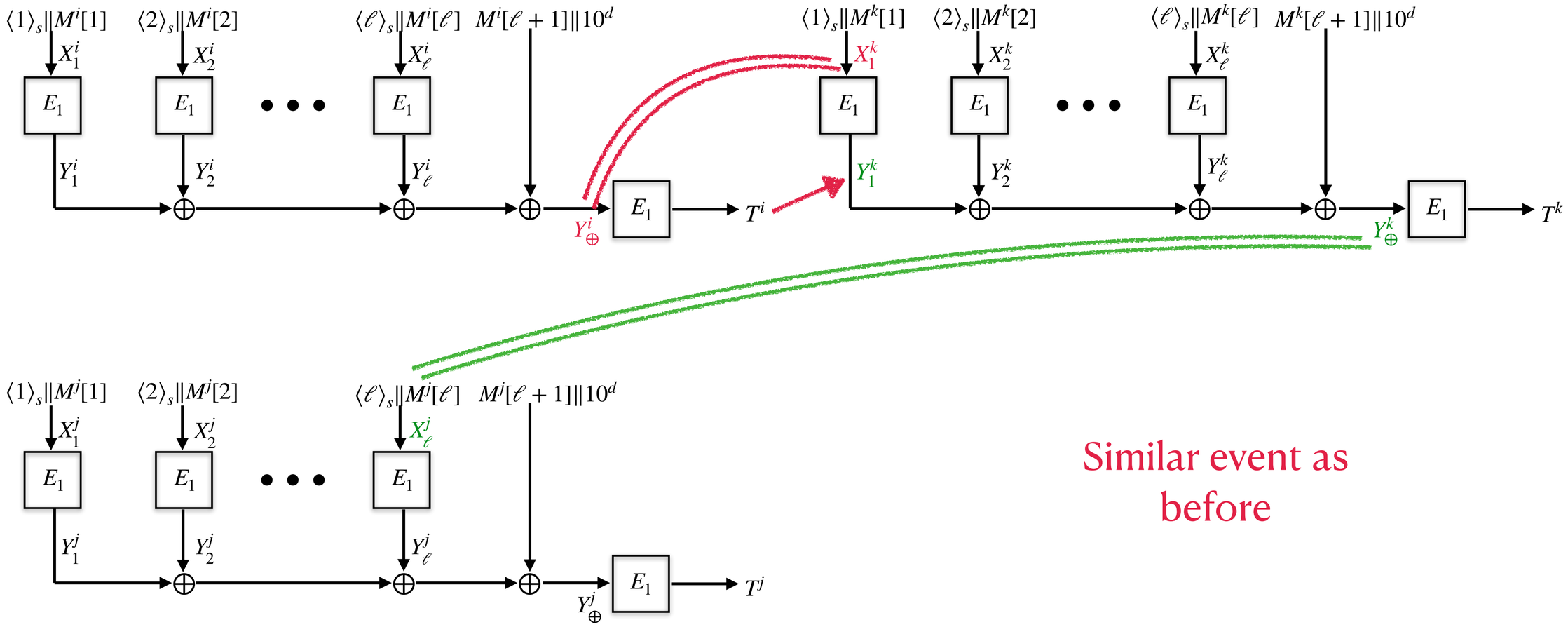
One-key LightMAC

Reset-Sampling



One-key LightMAC

Reset-Sampling



Similar event as before

One-key LightMAC

ChattopadhyayJN, IACR ASIACRYPT 2021

$$\mathbf{Adv}^{\mathrm{prf}}_{\text{1k-LightMAC}}(\mathbf{Eve}) = O\left(\frac{q^2}{2^n}\right), \qquad \text{while } \ell \ll 2^{n/4}$$

One-key LightMAC is identical in security up to acceptable restrictions on message length

OMAC

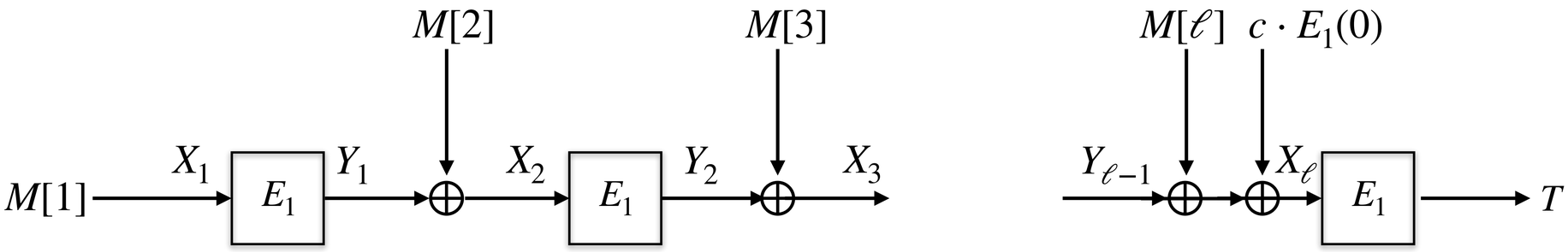
Iwata and Kurosawa, IACR FSE 2003; NIST FIPS 800-38B; ISO/IEC 29167-10:2017

$(M[1], \ldots, M[\ell]) \xleftarrow{n} M$

OMAC

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

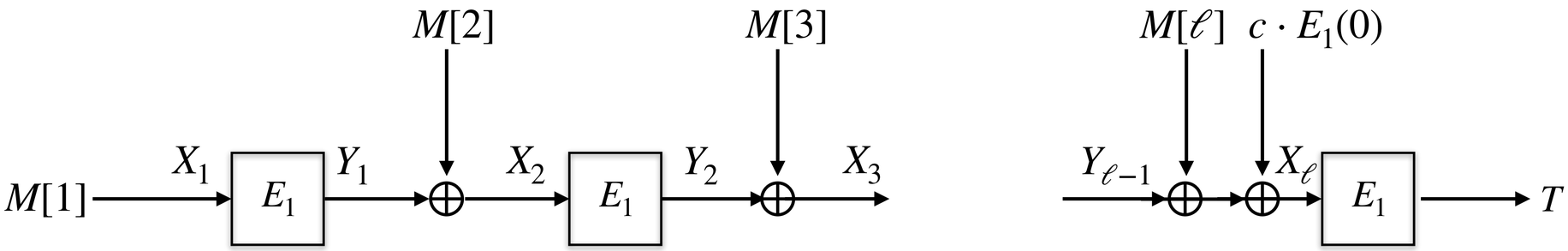
$(M[1], \ldots, M[\ell]) \xleftarrow{n} M$



OMAC

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

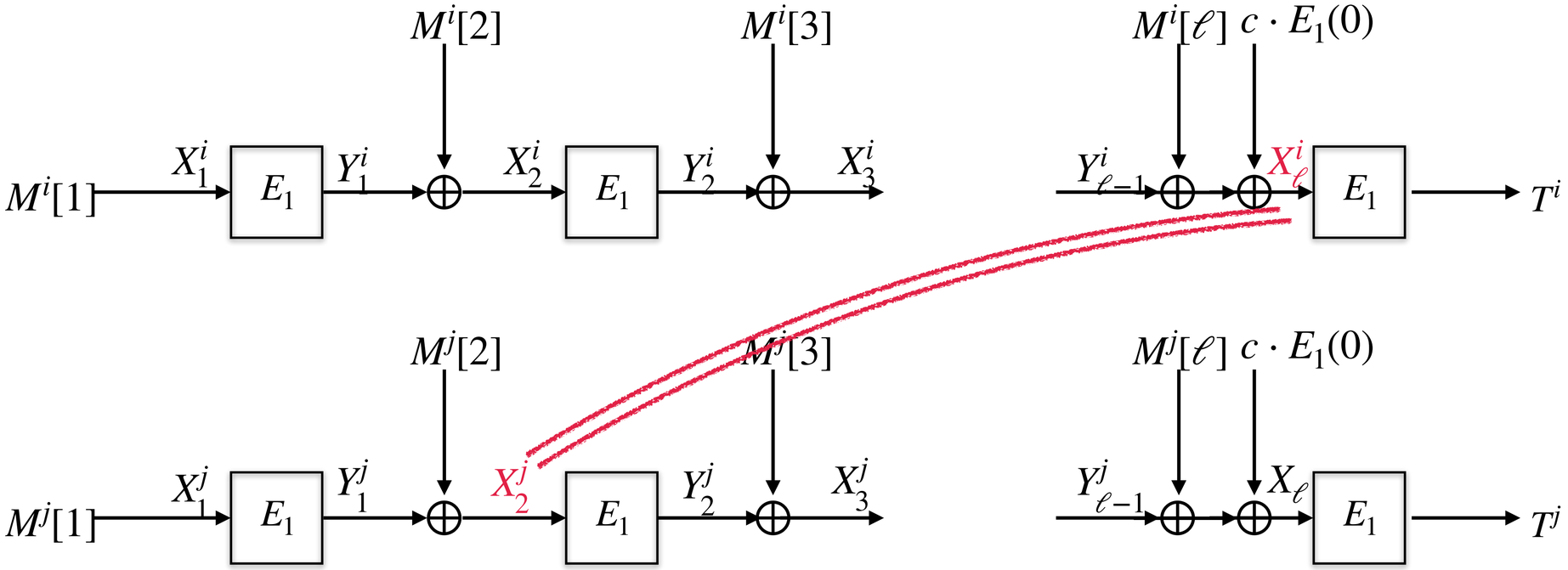
$(M[1], \ldots, M[\ell]) \xleftarrow{n} M$



- Sequential and single-key CBC-MAC.
- Best security bound: $\mathbf{Adv}^{\text{prf}}_{\text{CBC-MAC}}(\mathbf{Eve}) = O\left(\frac{q^2\ell}{2^n}\right)$
- No matching attack.

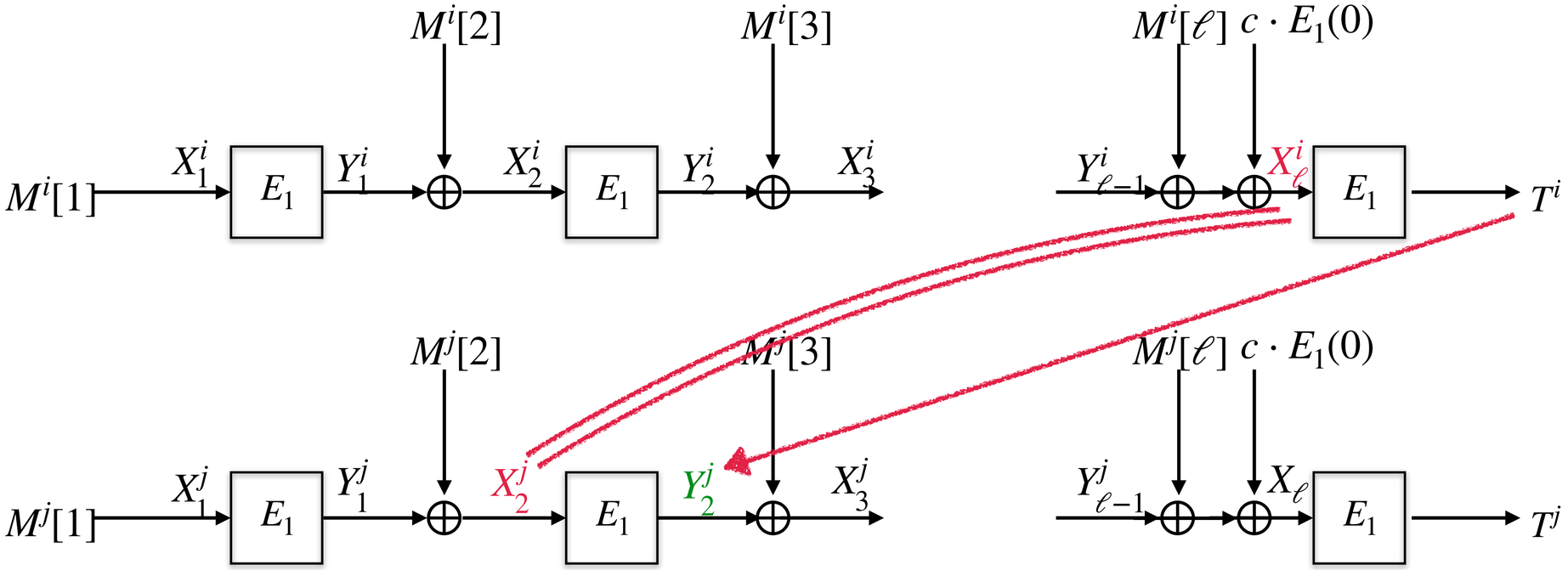
OMAC

Full Collision Event



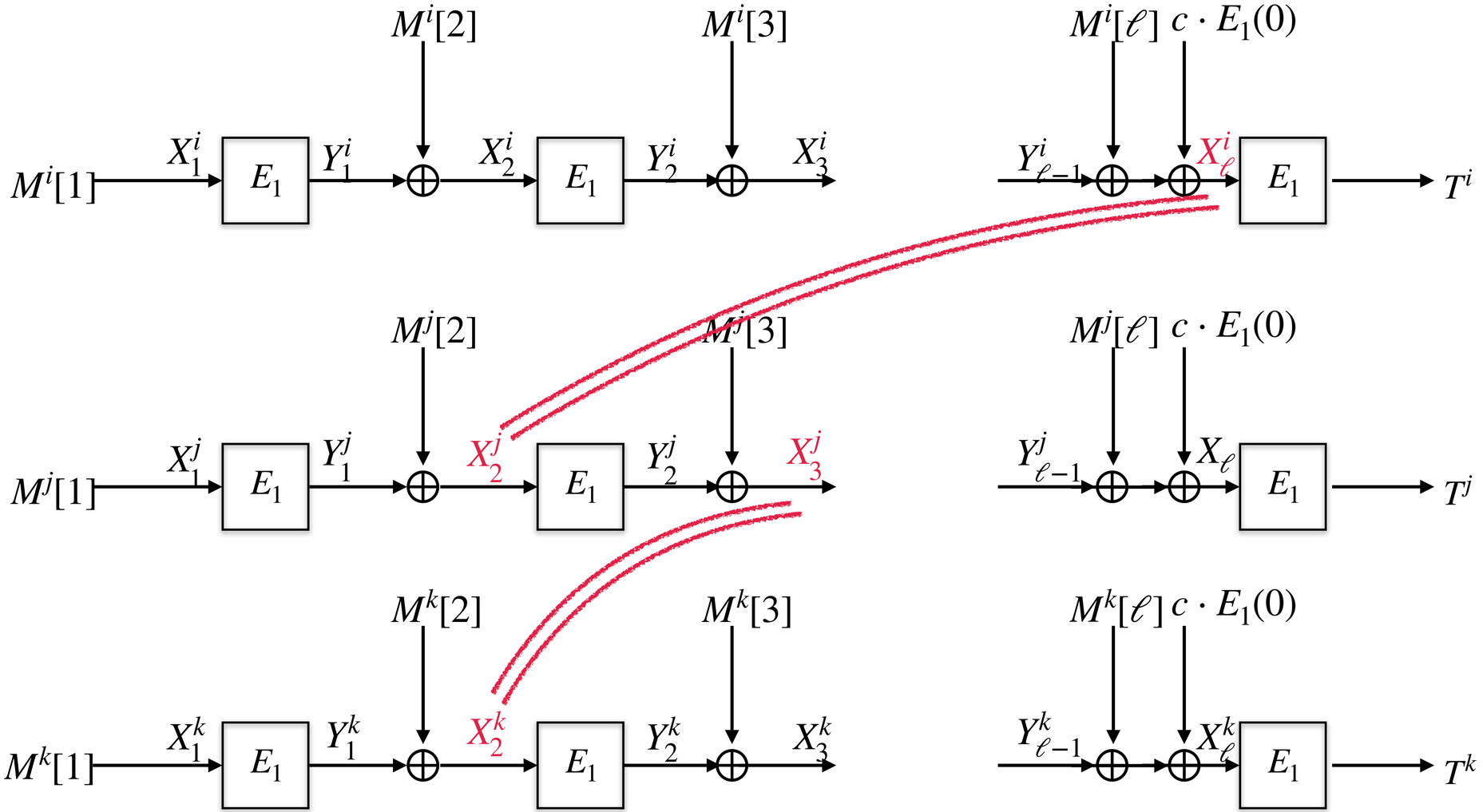
OMAC

Reset-Sampling



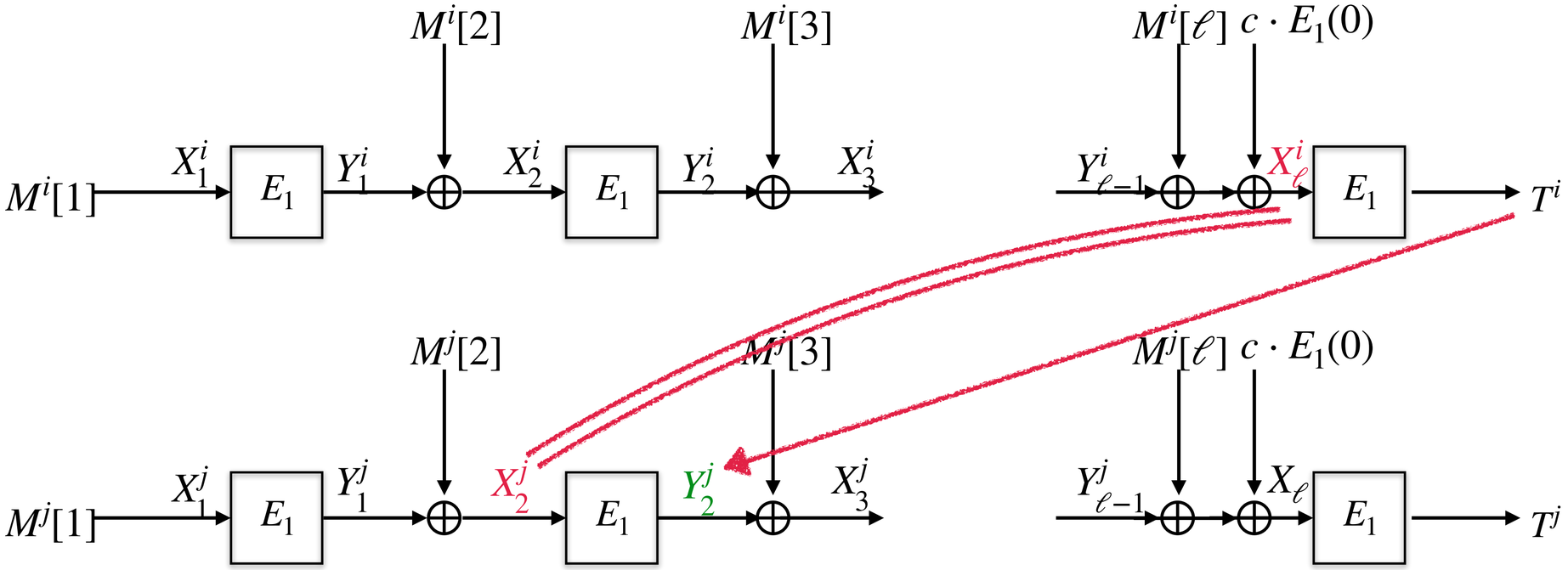
OMAC

Reset-Sampling



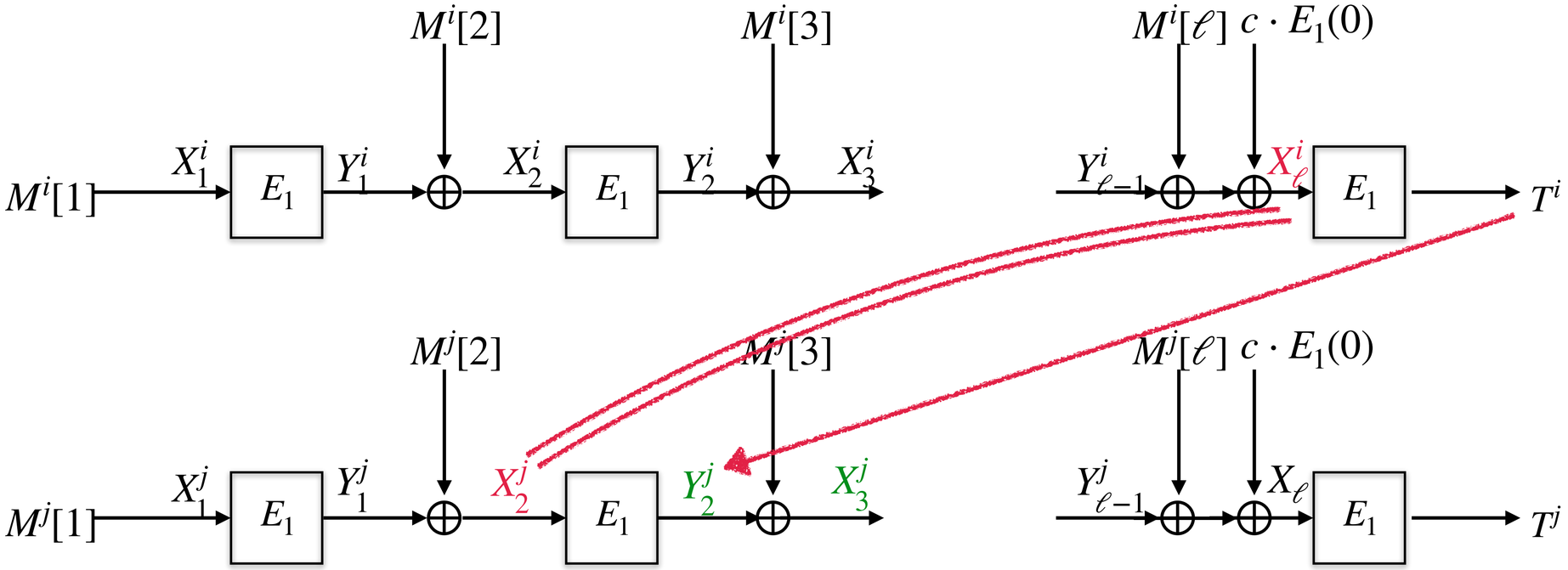
OMAC

Reset-Sampling



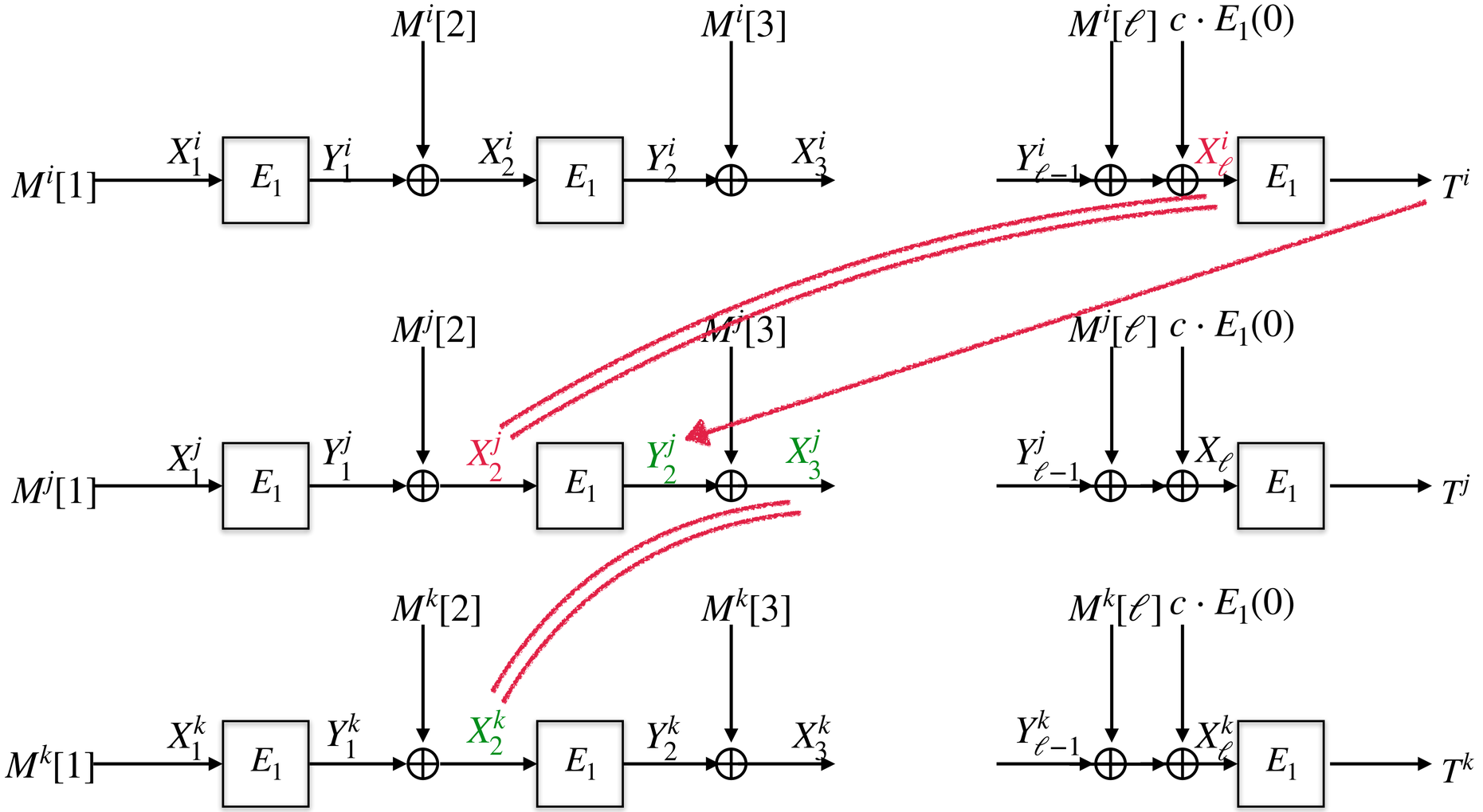
OMAC

Reset-Sampling



OMAC

Reset-Sampling



OMAC

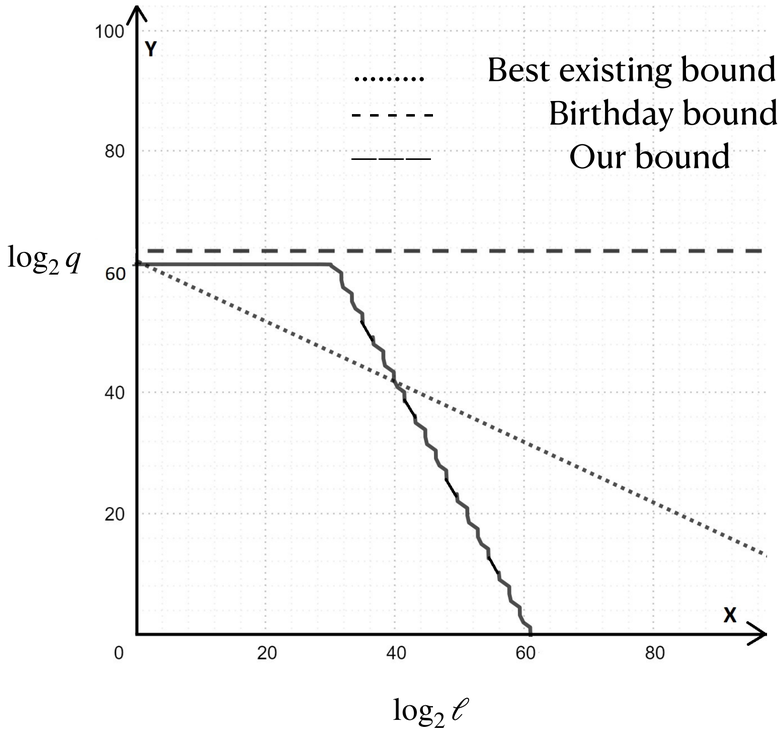
ChattopadhyayJN, IACR ASIACRYPT 2022

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

OMAC

ChattopadhyayJN, IACR ASIACRYPT 2022

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



OMAC is (almost) birthday bound secure.

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