DWCDM: A Single-Keyed Nonce Based BBB Secure MAC

Mridul Nandi

Indian Statistical Institute, Kolkata

Indocrypt 2018, New Delhi

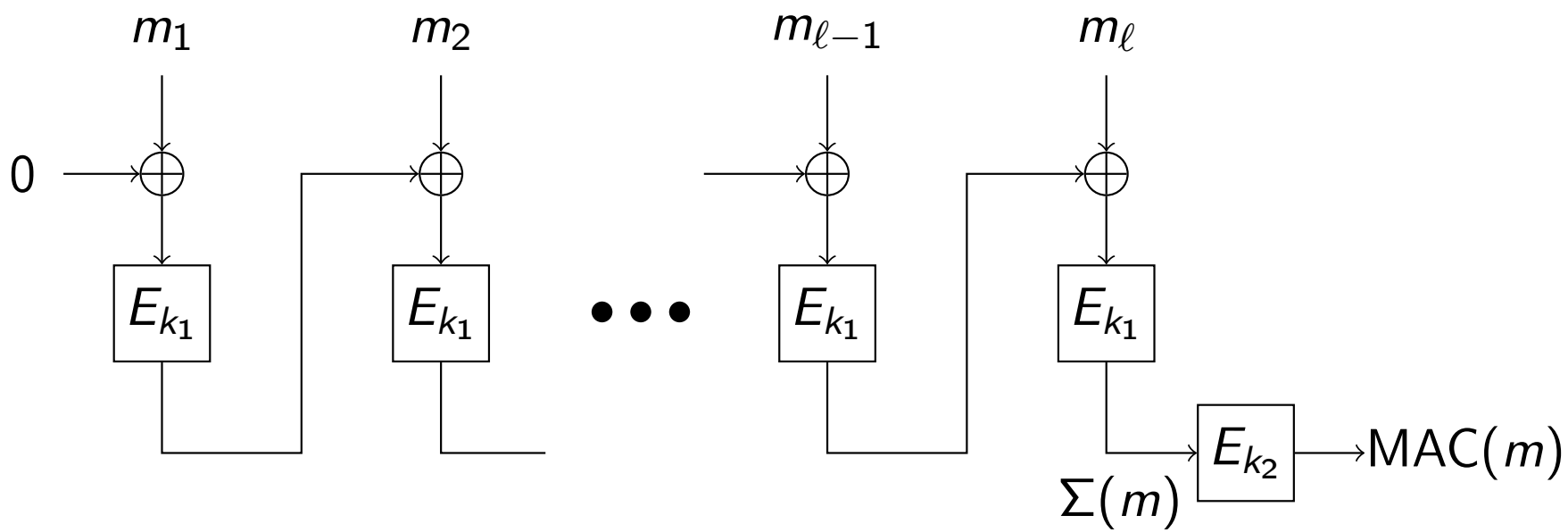
- Encrypt or Decrypt? To Make a Single-Key Beyond Birthday Secure Nonce-Based MAC – Nilanjan Datta, Avijit Dutta, Mridul Nandi and Kan Yasuda, CRYPTO 2018.




Introduction

- **Symmetric cryptography:** Alice and Bob share the same key.
- **Active attacker:** Eve might intercept and manipulate Alice's messages.
- **Authentication:** Alice computes and appends a keyed MAC or tag T... Bob recomputes tag and matches with T.

An Example of MAC: ECBC-MAC

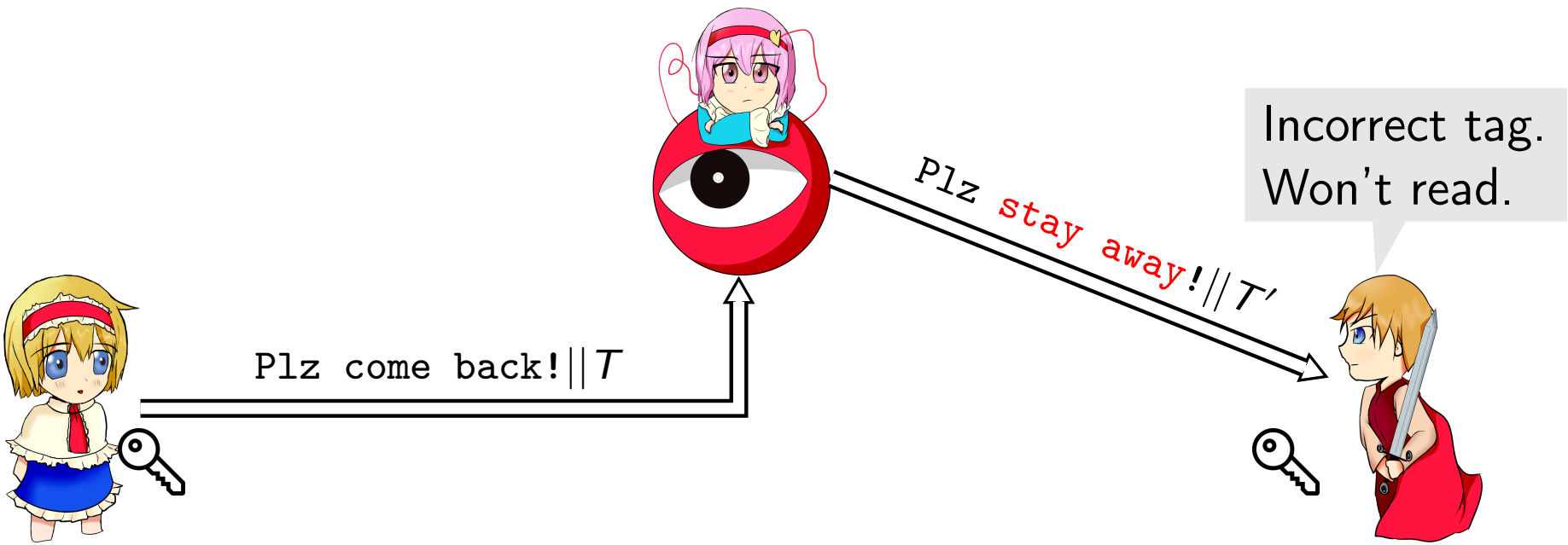


– $m_1||\cdots||m_\ell$: "`Plz come back || pad`", Tag : $T = \mathrm{MAC}(m)$.

– Alice sends T along with m to guarantee authenticity.

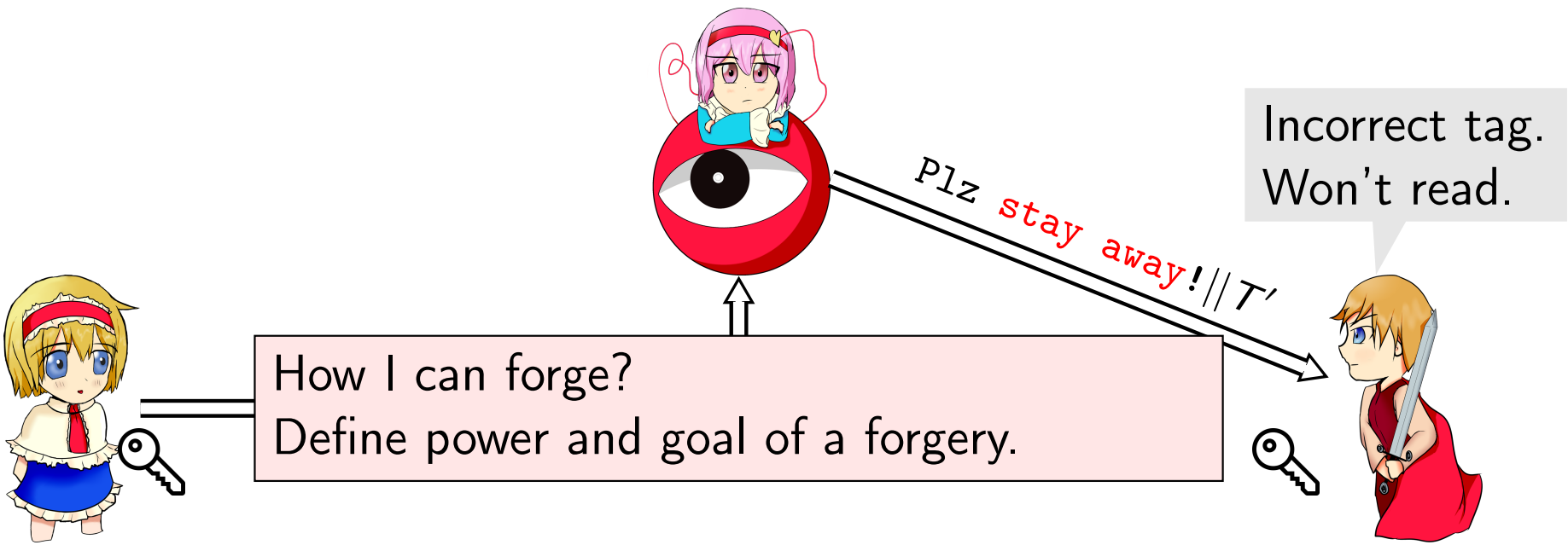
Introduction

- **Verifying:** Bob verifies the tag with the shared key and only reads the message if tags match.
- **Forgery:** Eve cannot modify the message without forging a new and correct tag.



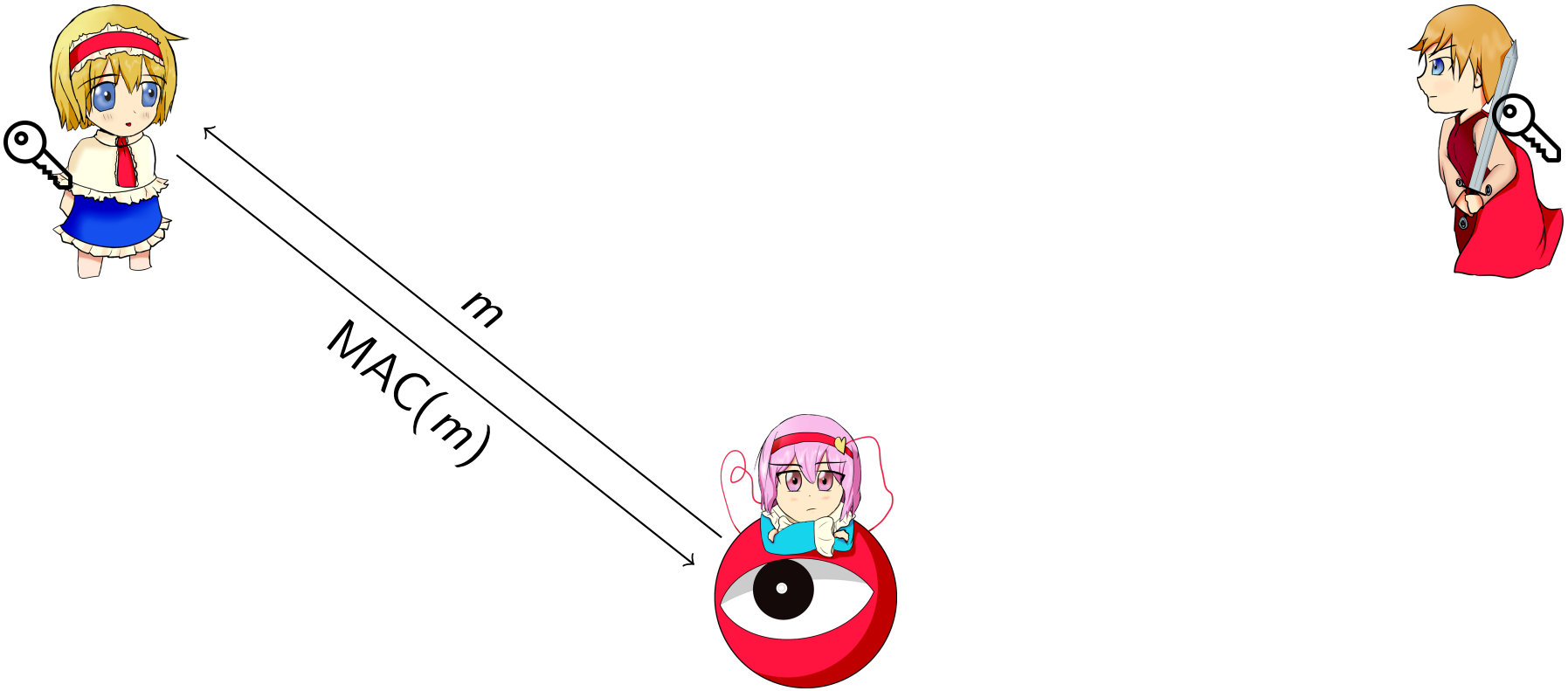
Introduction

- **Verifying:** Bob verifies the tag with the shared key and only reads the message if tags match.
- **Forgery:** Eve cannot modify the message without forging a new and correct tag.

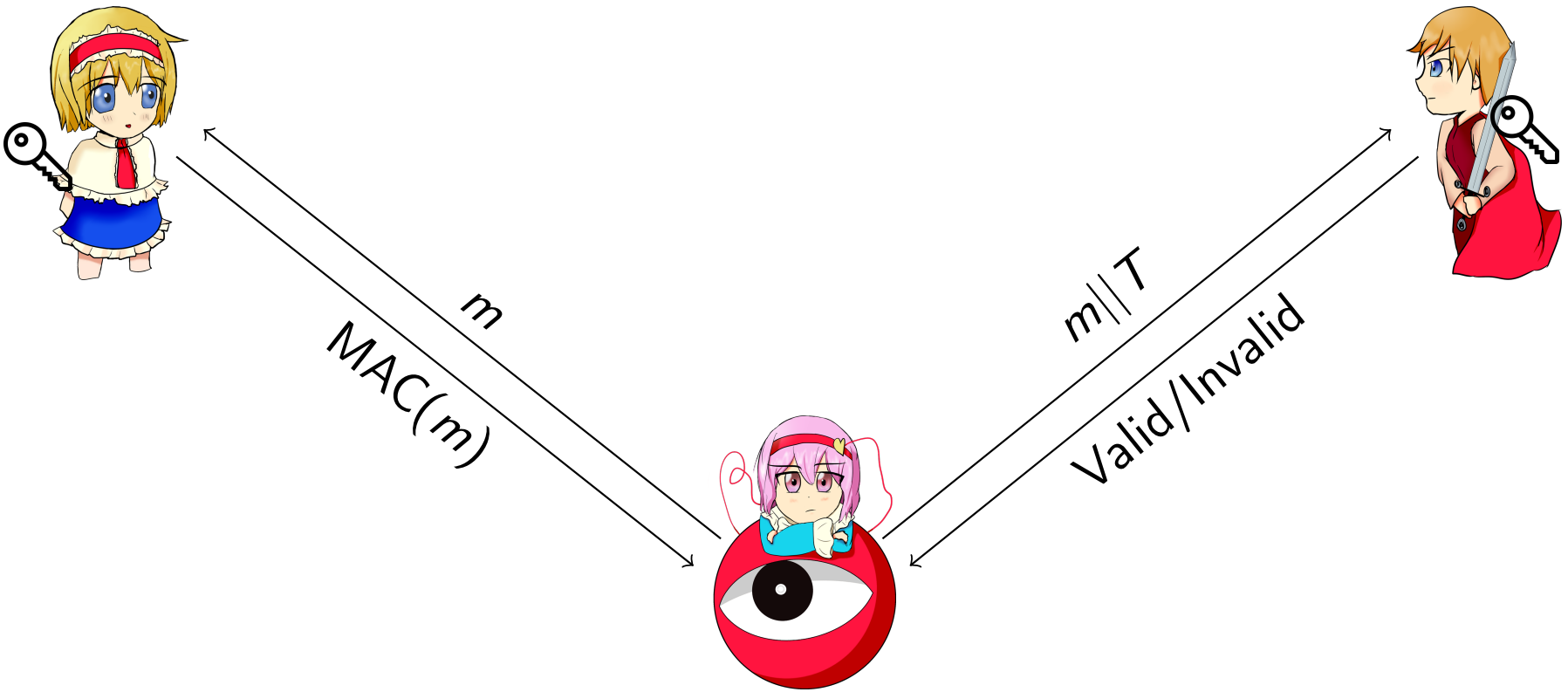


Forgery security game

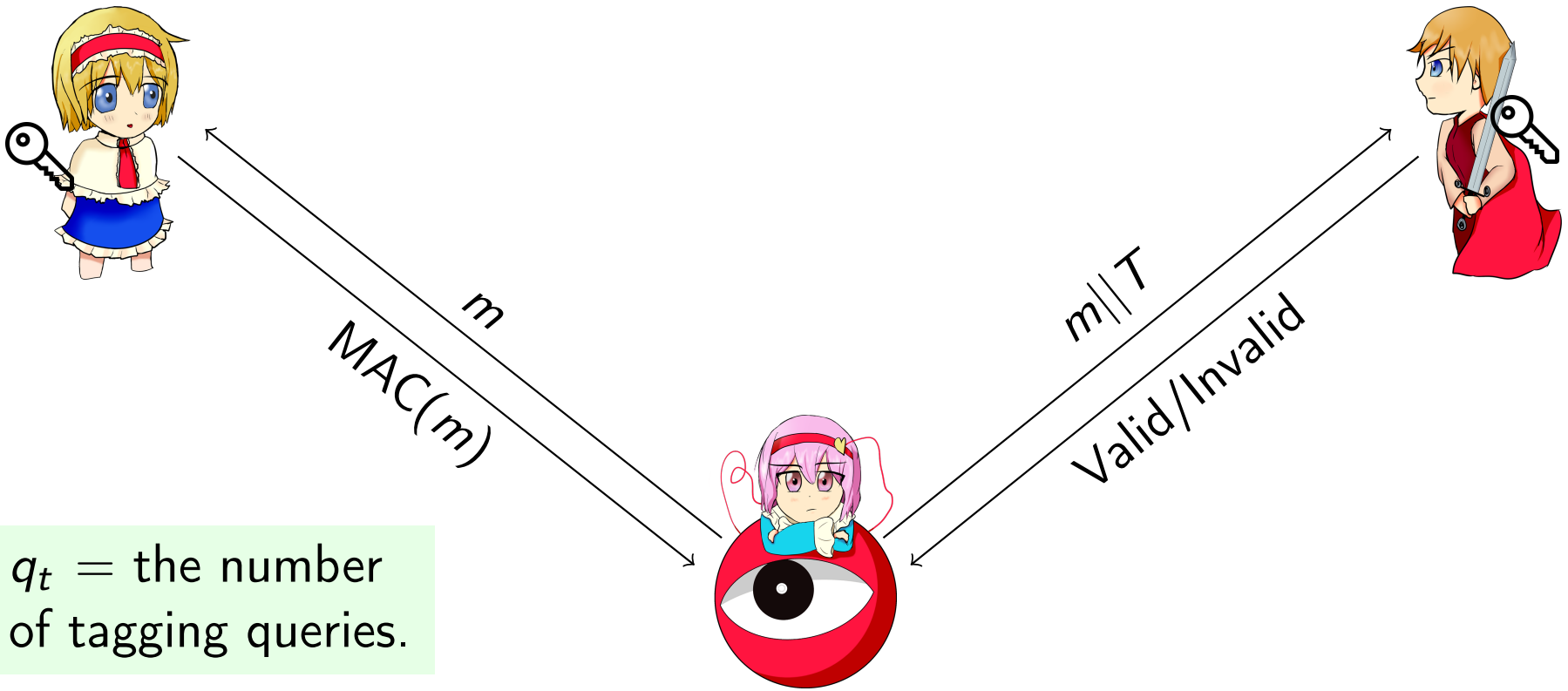
Forgery security game



Forgery security game

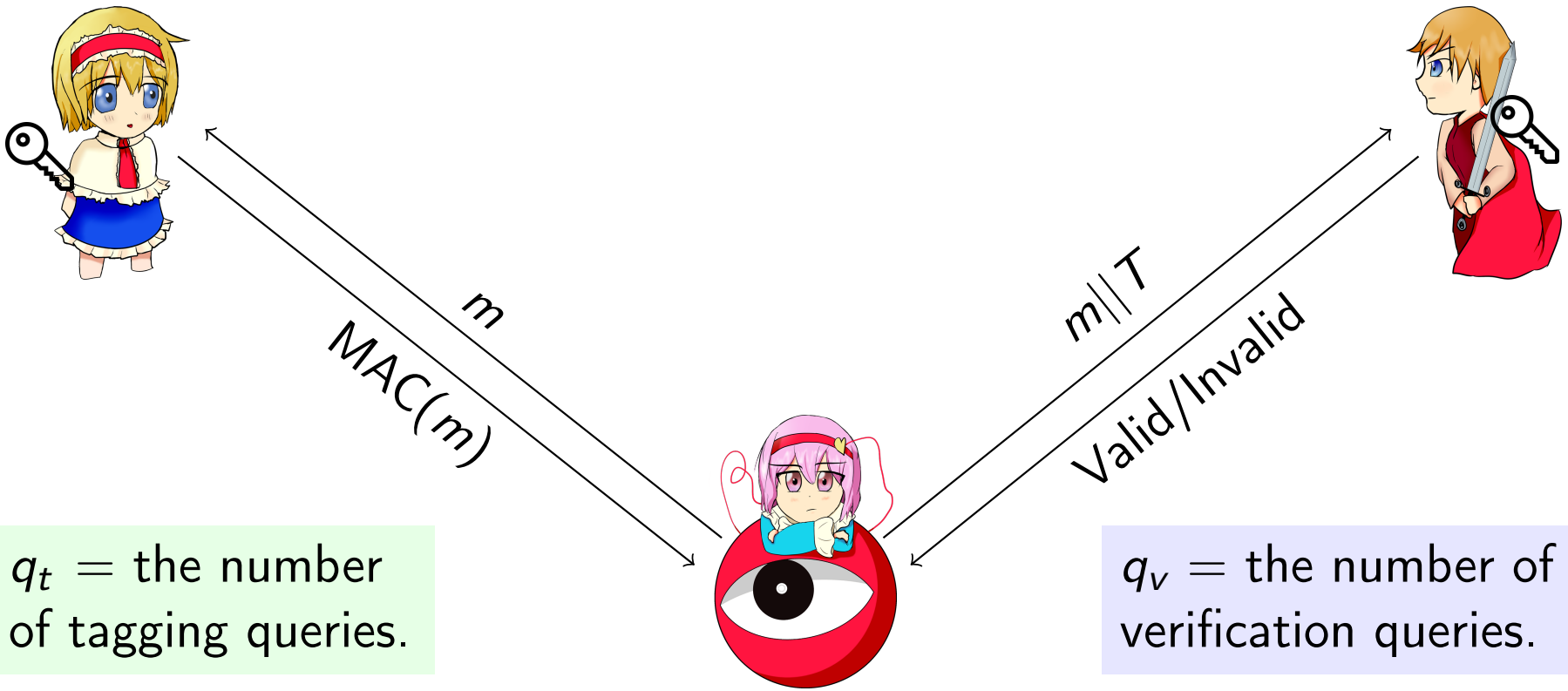


Forgery security game



q_t = the number of tagging queries.

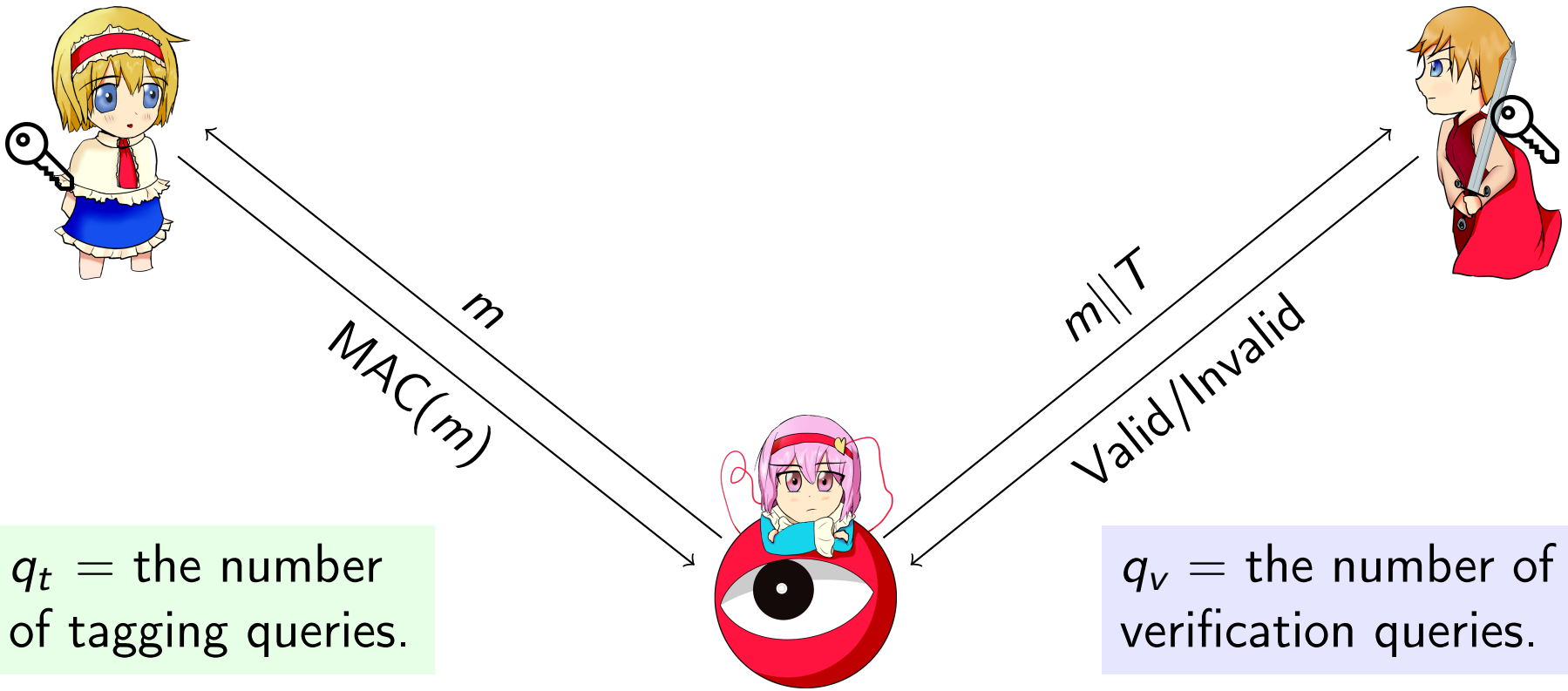
Forgery security game



q_t = the number of tagging queries.

q_v = the number of verification queries.

Forgery security game



q_t = the number of tagging queries.

q_v = the number of verification queries.

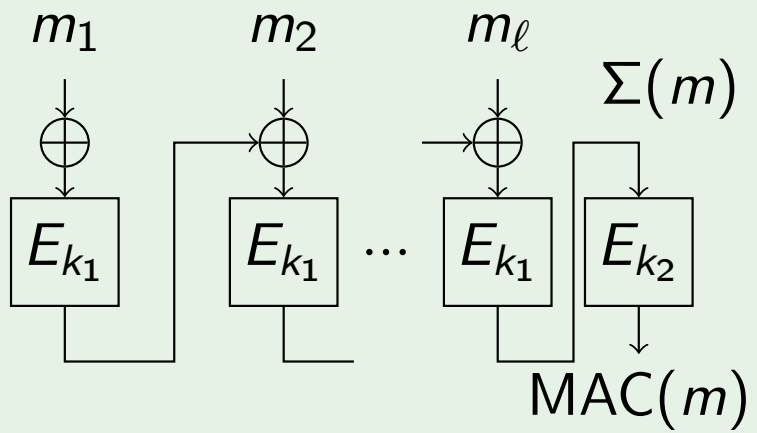
Can Eve forge a valid tag for a message that Alice never saw?

Case of ECBC

Properties of ECBC for all messages m, m', c:

$$
\begin{aligned}
& \mathrm{MAC}(m) = \mathrm{MAC}(m') \\
\iff \quad & E_{k_2}\big(\Sigma(m)\big) = E_{k_2}\big(\Sigma(m')\big) \\
\iff \quad & \Sigma(m) = \Sigma(m') \\
\iff \quad & \Sigma(m||c) = \Sigma(m'||c) \\
\iff \quad & \mathrm{MAC}(m||c) = \mathrm{MAC}(m'||c)
\end{aligned}
$$

ECBC mode

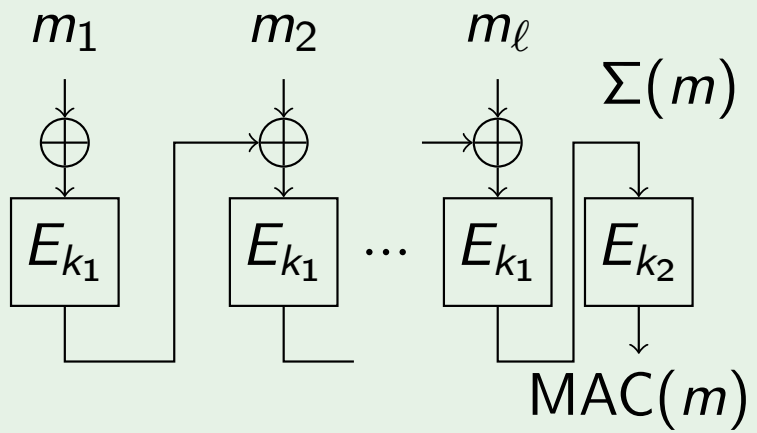


Case of ECBC

Properties of ECBC for all messages m, m', c:

$$\begin{aligned} & \mathrm{MAC}(m) = \mathrm{MAC}(m') \\ \iff \quad & E_{k_2}\big(\Sigma(m)\big) = E_{k_2}\big(\Sigma(m')\big) \\ \iff \quad & \Sigma(m) = \Sigma(m') \\ \iff \quad & \Sigma(m||c) = \Sigma(m'||c) \\ \iff \quad & \mathrm{MAC}(m||c) = \mathrm{MAC}(m'||c) \end{aligned}$$

ECBC mode

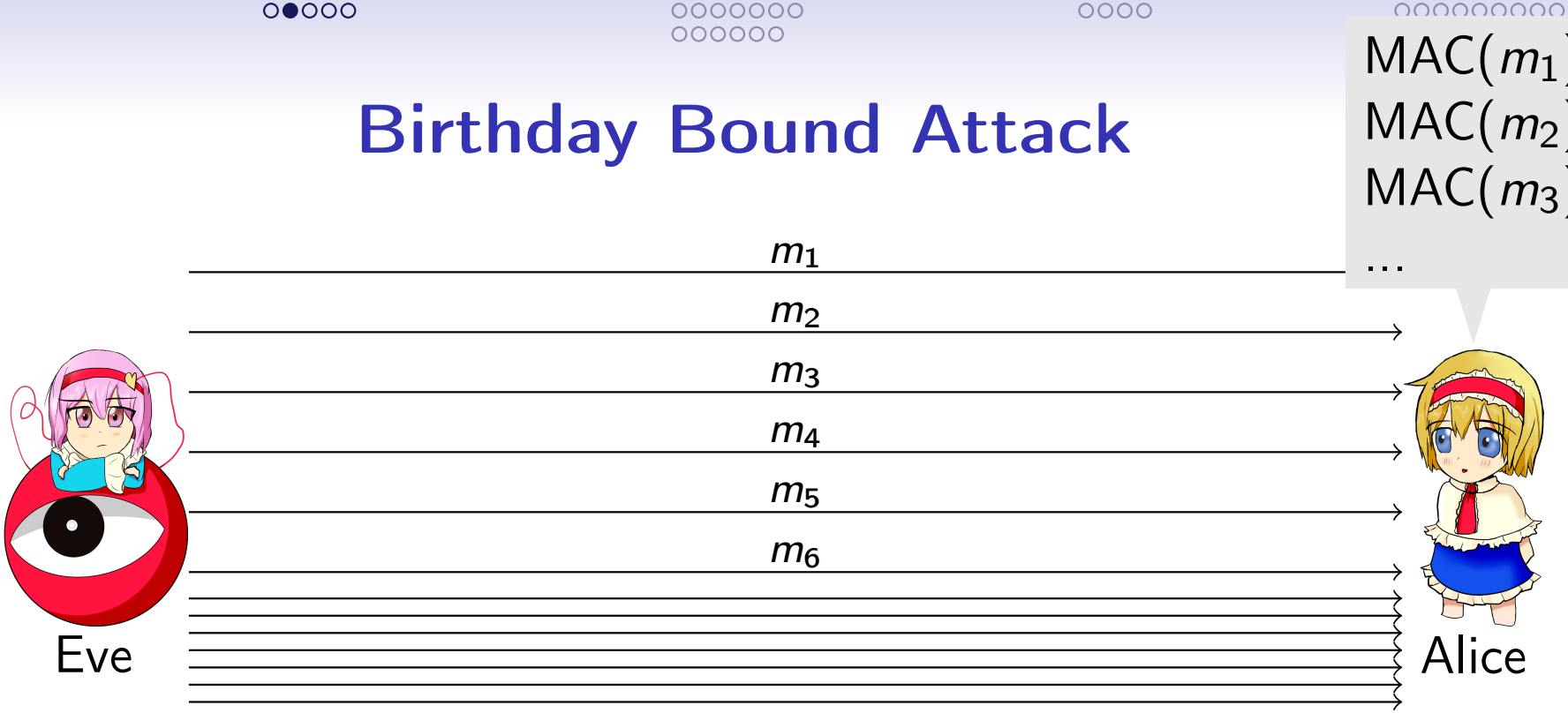


Expansion Property

Look for a pair of messages m, m' such that $\mathrm{MAC}(m) = \mathrm{MAC}(m')$. Then, for all c,

$$\mathrm{MAC}(m||c) = \mathrm{MAC}(m'||c)$$

Birthday Bound Attack



Looking for collisions

Eve looks for $\mathrm{MAC}(m_i) = \mathrm{MAC}(m_j)$ for some $i \neq j$.
She has $\simeq q_t^2$ pairs for an n-bit relationship so chances grow as:

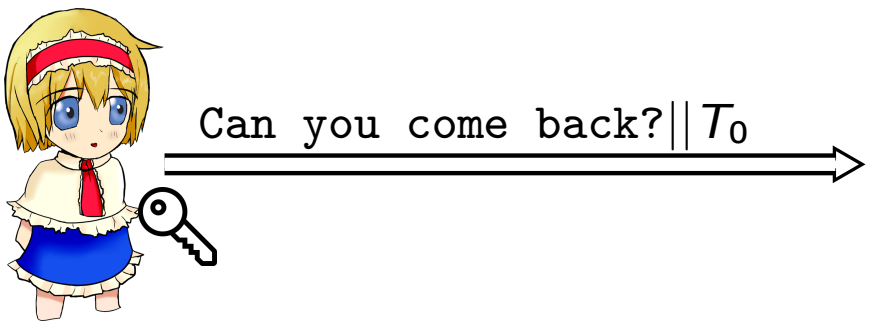
$$\mathbf{Adv}(\mathcal{A}) \simeq \frac{q_t^2}{2^n}$$

Forgery from collisions

Expansion property

$$\mathrm{MAC}(m) = \mathrm{MAC}(m') \implies \mathrm{MAC}(m||c) = \mathrm{MAC}(m'||c)\ \forall c$$

Collision found:
$\mathrm{MAC}(\texttt{You must}) =$
$\mathrm{MAC}(\texttt{No, don't})$



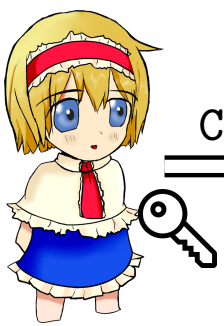
Forgery from collisions

Expansion property

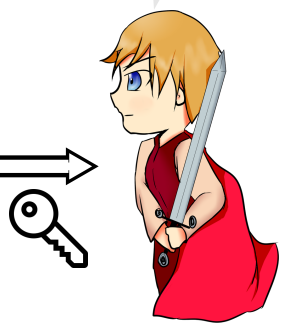
$\mathrm{MAC}(m) = \mathrm{MAC}(m') \implies \mathrm{MAC}(m||c) = \mathrm{MAC}(m'||c)\ \forall c$

Collision found:
$\mathrm{MAC}(\texttt{You must}) =$
$\mathrm{MAC}(\texttt{No, don't})$

Correct tag.
Will read.



$\texttt{Can you come back?}||T_0$



Forgery from collisions

Expansion property

$$\mathrm{MAC}(m) = \mathrm{MAC}(m') \implies \mathrm{MAC}(m||c) = \mathrm{MAC}(m'||c)\ \forall c$$

Tell Bob **he must** come back!

Collision found:
$\mathrm{MAC}(\texttt{You must}) =$
$\mathrm{MAC}(\texttt{No, don't})$

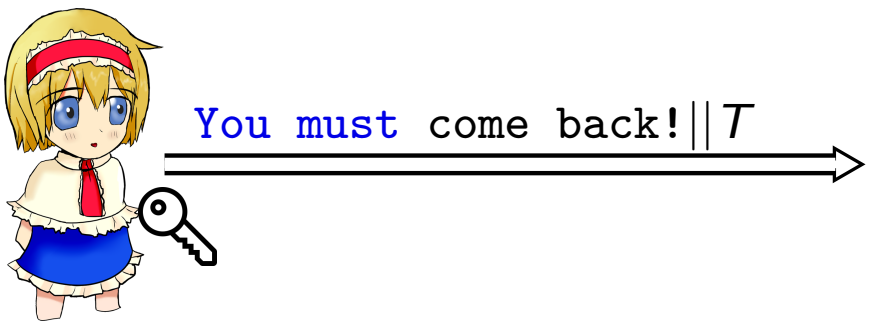
Oh you are right!

Forgery from collisions

Expansion property

$$\mathrm{MAC}(m) = \mathrm{MAC}(m') \implies \mathrm{MAC}(m||c) = \mathrm{MAC}(m'||c)\ \forall c$$

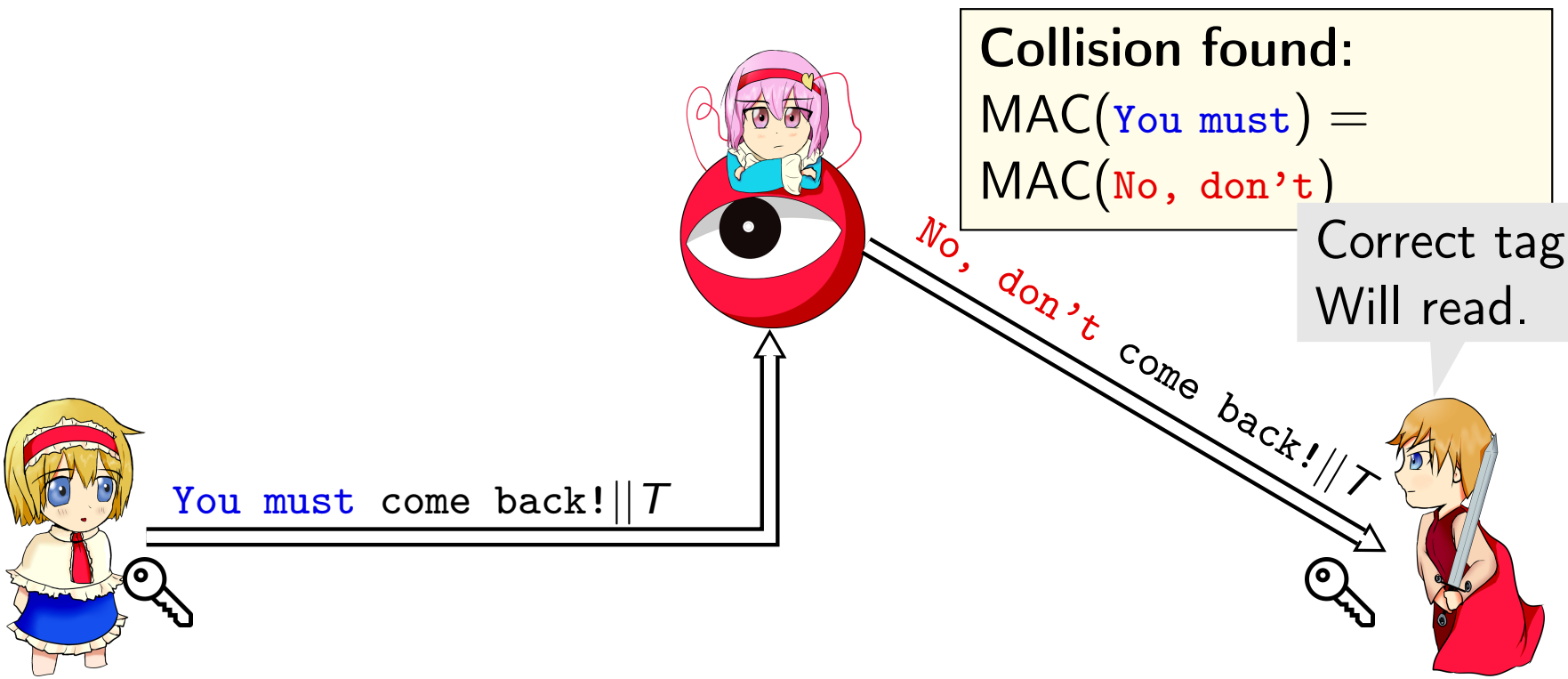
Collision found:
$\mathrm{MAC}(\texttt{You must}) =$
$\mathrm{MAC}(\texttt{No, don't})$



Forgery from collisions

Expansion property

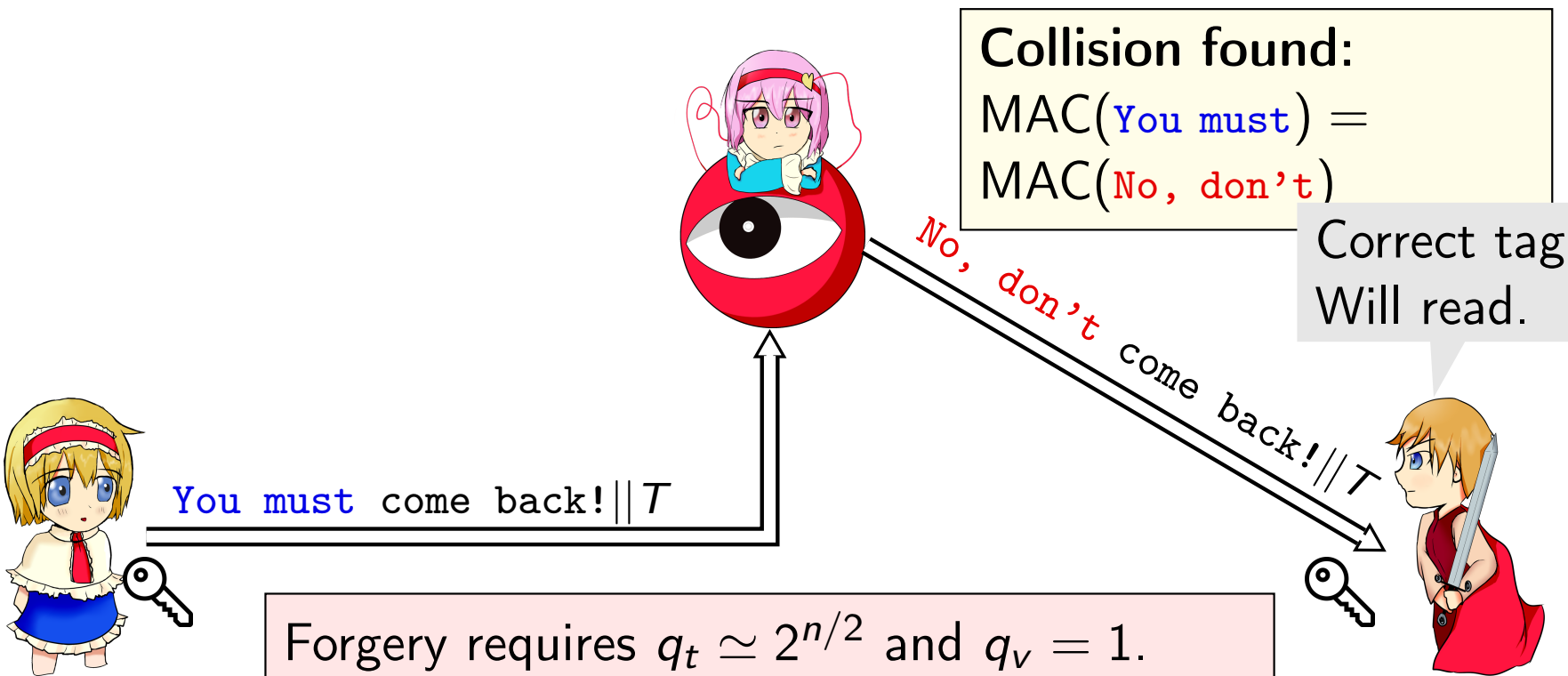
$$\mathrm{MAC}(m) = \mathrm{MAC}(m') \implies \mathrm{MAC}(m||c) = \mathrm{MAC}(m'||c)\ \forall c$$



Forgery from collisions

Expansion property

$\mathrm{MAC}(m) = \mathrm{MAC}(m') \implies \mathrm{MAC}(m||c) = \mathrm{MAC}(m'||c)\ \forall c$



Forgery requires $q_t \simeq 2^{n/2}$ and $q_v = 1$.
Not secure beyond birthday bound ($2^{n/2}$)

Why Beyond Birthday Security?

- BBB security is useful in lightweight cryptography
- Consider the security advantage $\epsilon = 2^{-10}$, $n = 64$ and $\ell = 2^{16}$ blocks.

Construction	Security	# of queries
ECBC	$16q_t^2/2^n$	$\approx 2^{25}$
PMAC	$5\ell q_t^2/2^n$	$\approx 2^{18}$

Table: Data limit of constructions achieving birthday bound security.

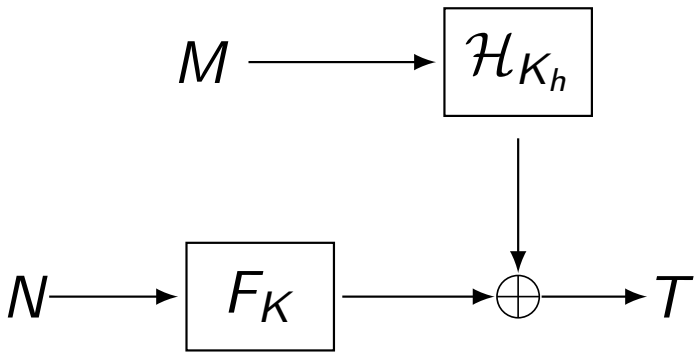
§ BBB security can allow to process larger number of blocks per session key.

Summary So Far

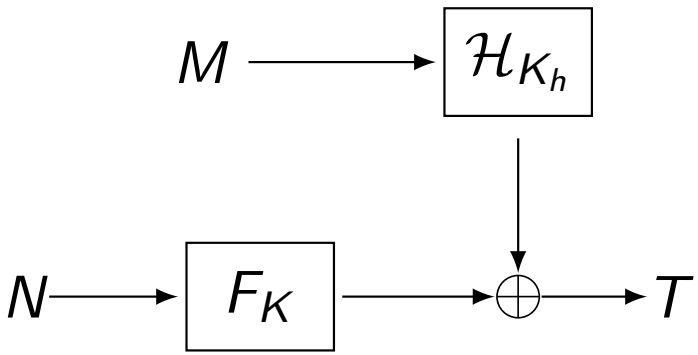
- Forgery Game of Message Authentication Code (MAC)
- Birthday Bound Forgery for ECBC MAC.
- Birthday Bound is not suitable for small block cipher based MAC

§ Coming up: How to get BBB secure MAC constructions.

Wegman Carter MAC [JCSS, 1981]

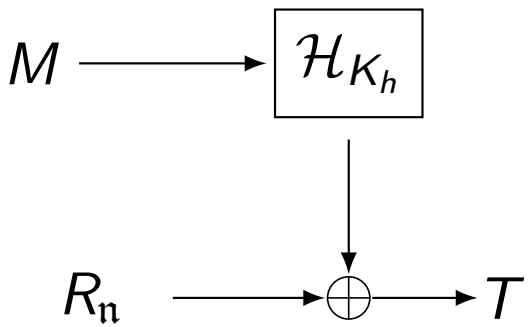


Wegman Carter MAC [JCSS, 1981]

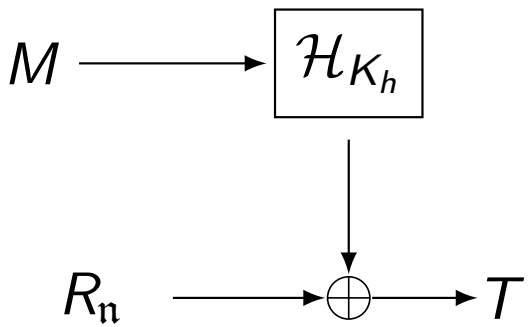


- Nonce based authenticator.
- Proposed by Wegman and Carter in 1981
  - based on a Code of Gilbert, MacWilliams and Sloane [GMS74] – a fresh key of size as large as message

Wegman Carter MAC



Wegman Carter MAC



- universal$_2$ is relaxed to a weaker hash AXU in [Kra94/Rog95]
  - $\Pr[H_k(M) \oplus H_k(M') = \delta]$ is small
- polynomial hashing over n bits:
  $\mathrm{Poly}_k(M) := m_d k \oplus \ldots \oplus m_1 k^d$ is $d/2^n$-AXU hash.

Getting rid of one time masking

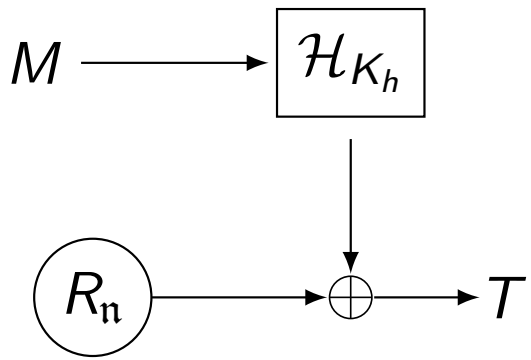
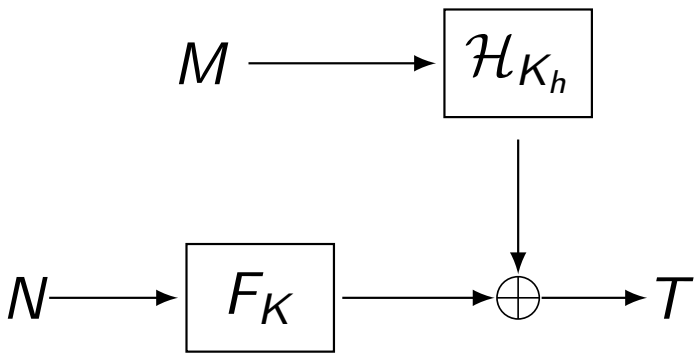


Figure: We can compute $R_{\mathfrak{n}}$ directly from $\mathfrak{n}$ and a secret key.

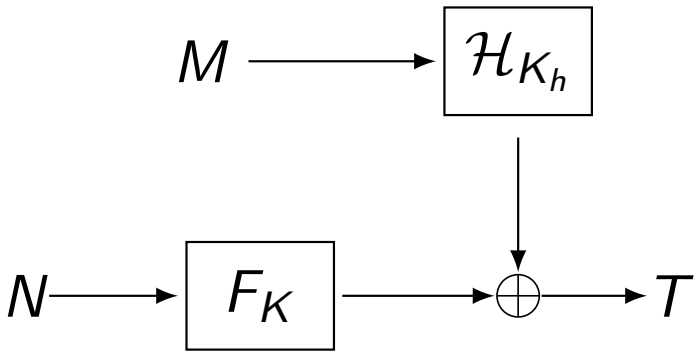
- Use PRBG (Brassard [Bra83]).
- Sequential in nature
  - Direct efficient computation of $R_{\mathfrak{n}}$ (Blum-Blum-Shub PRBG)
  - also modeled as pseudorandom function.

Getting rid of one time masking



- Use pseudorandom function on a unique value nonce.

Wegman Carter MAC [JCSS, 1981]

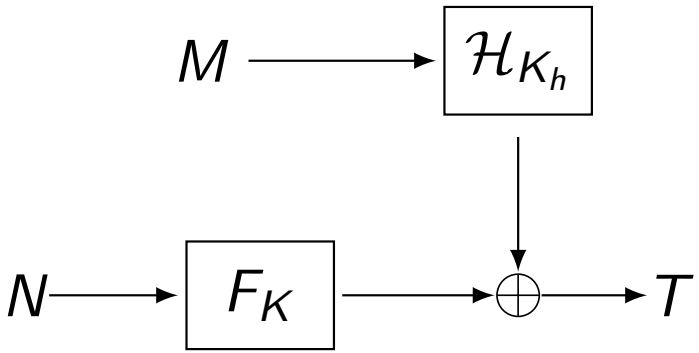


Construction	Security	# of queries
ECBC	$16q_t^2/2^n$	$\approx 2^{25}$
WC (Nonce Respecting)	$q_v\ell/2^n$	$\approx 2^{54}$

Table: The security advantage $\epsilon = 2^{-10}$, $n = 64$ and $\ell = 2^{16}$ blocks.

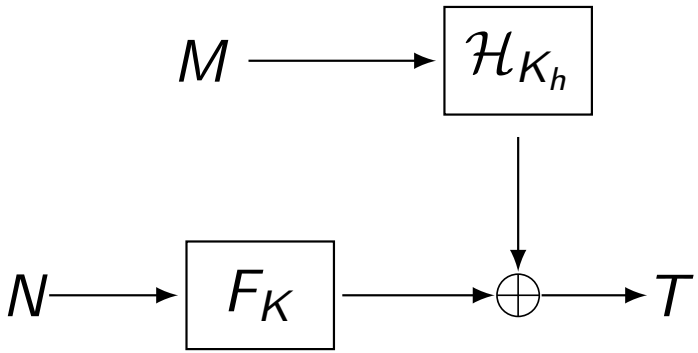
§ Security of WC relies on a crucial assumption: Nonce cannot repeat.

Nonce Misuse Attack of Wegman Carter MAC



- A makes two queries (N, M) and (N, M') and obtains reply T and T' respectively.
- A makes another query (N', M) and obtains reply T''.
- A forges with $(N', M', T \oplus T' \oplus T'')$.

Nonce Misuse Attack of Wegman Carter MAC



- A makes two queries (N, M) and (N, M') and obtains reply T and T' respectively.
- A makes another query (N', M) and obtains reply T''.
- A forges with $(N', M', T \oplus T' \oplus T'')$.

When $\mathcal{H}$ is Polyhash, then one can recover the hash key and mounts universal forgery.

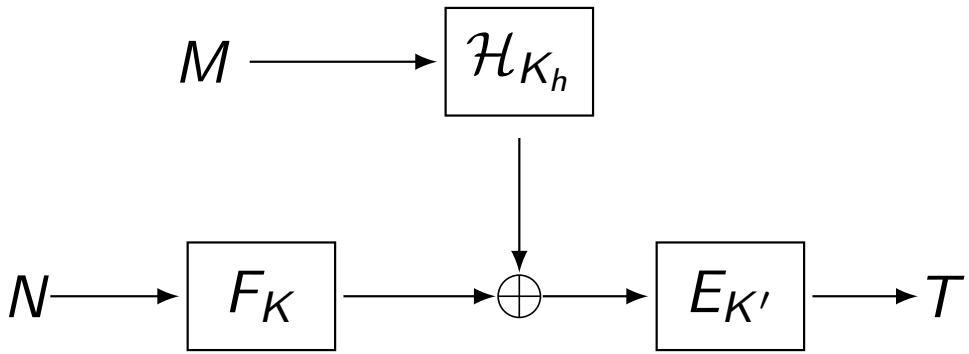
What We Want to Achieve ?

- Maintaining the uniqueness of nonce is difficult in certain applications

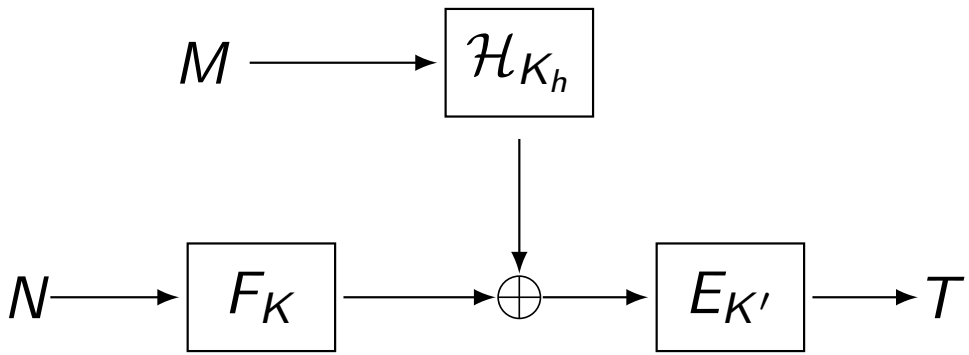
What We Want to Achieve ?

- Maintaining the uniqueness of nonce is difficult in certain applications
- Our Goal of this talk:
  § Constructions that give some security (birthday bound) in NM model but gives the beyond birthday bound security in NR model.

Encrypted Wegman Carter MAC [Cogliati and Seurin, CRYPTO 2016]



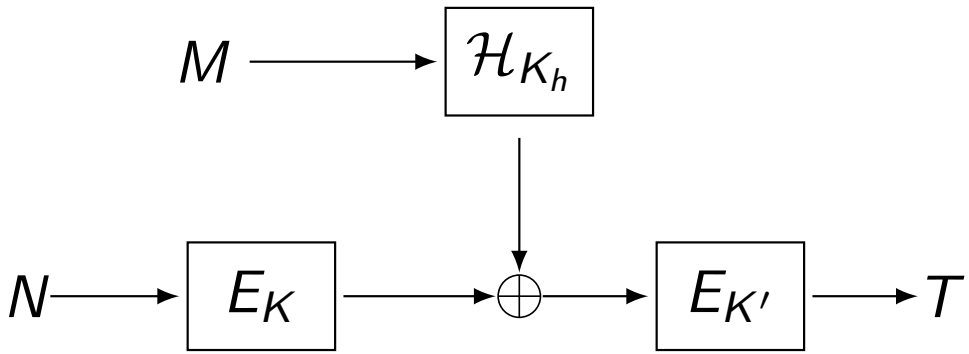
Encrypted Wegman Carter MAC [Cogliati and Seurin, CRYPTO 2016]



- Nonce Respecting (NR): Same security as Wegman Carter MAC in NR case
- Nonce Misuse (NM): Birthday Bound security

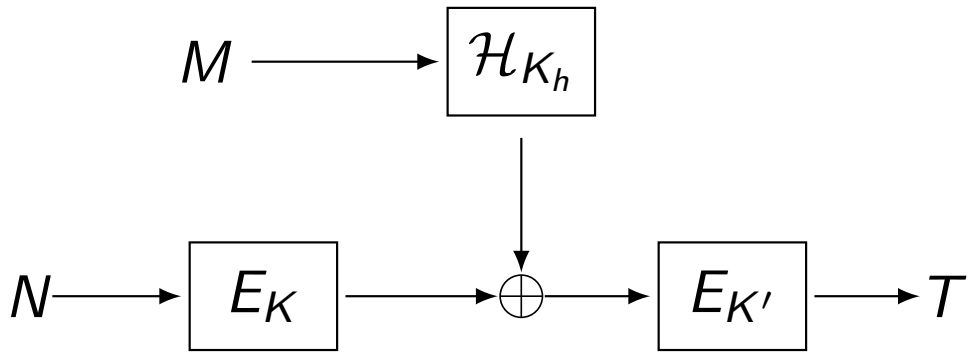
Instantiation of F_K

1. Encrypted Wegman-Carter-Shoup : $F_K \to E_K$



Instantiation of F_K

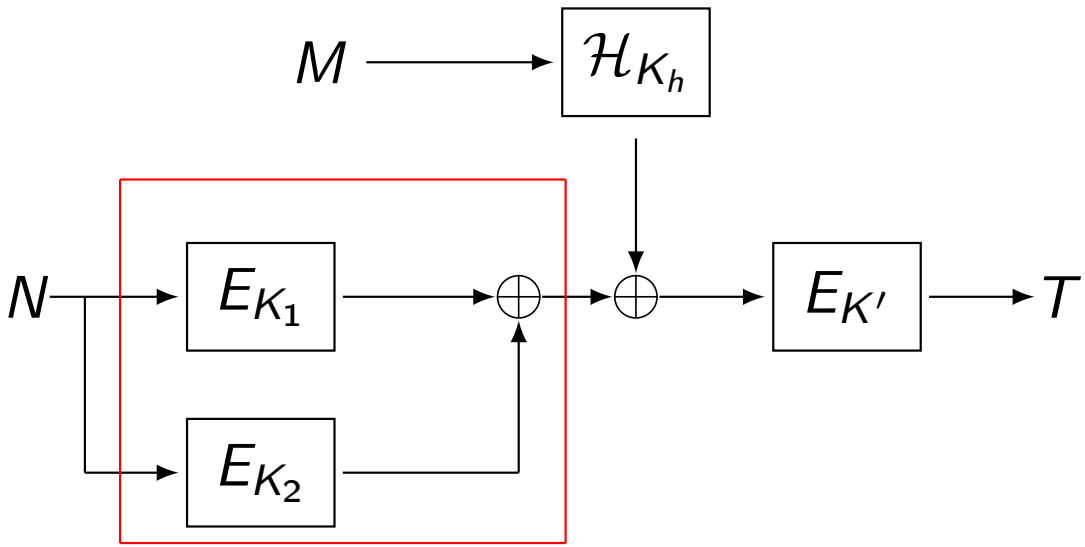
1. Encrypted Wegman-Carter-Shoup : $F_K \to E_K$



- Nonce Respecting (NR): Birthday Bound Security (distinguishing attack)
- Nonce Misuse (NM): Birthday Bound security
- Block cipher is more popular (can we use block cipher E_K as F_K?).

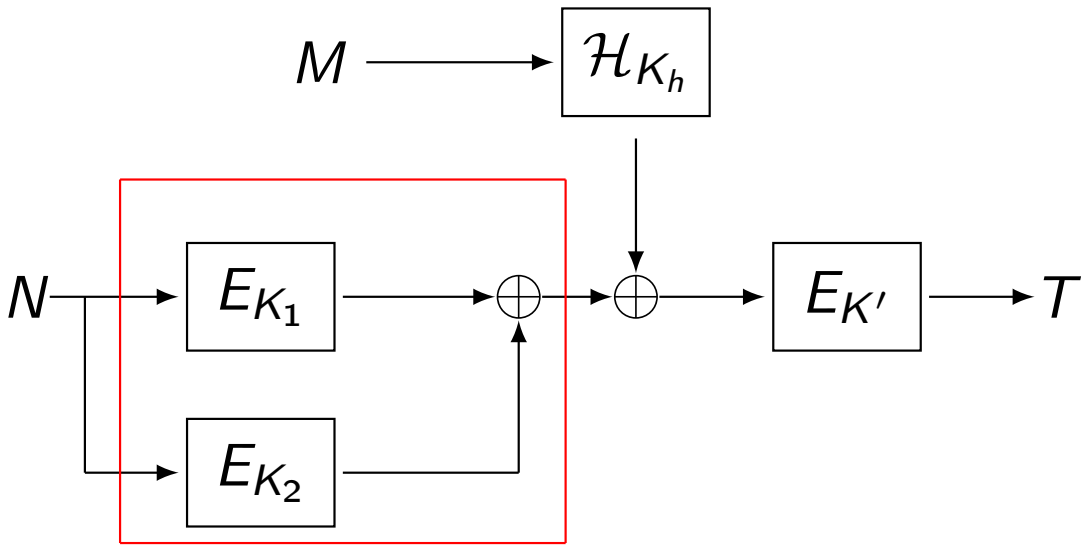
Instantiation of F_K

2. Encrypted Wegman-Carter with Sum of Permutation :
$F_K(N) \to E_{K_1}(N) + E_{K_2}(N)$



Instantiation of F_K

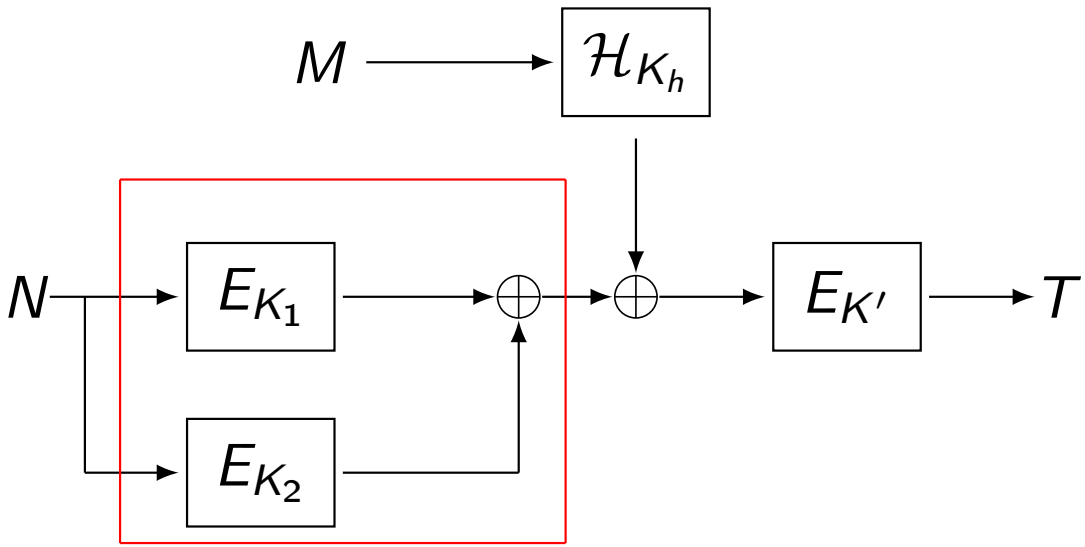
2. Encrypted Wegman-Carter with Sum of Permutation :
$F_K(N) \rightarrow E_{K_1}(N) + E_{K_2}(N)$



- Nonce Respecting (NR) : Beyond Birthday Bound Security.
- Nonce Misuse (NM) : Birthday Bound Security.

Instantiation of F_K

2. Encrypted Wegman-Carter with Sum of Permutation :
$F_K(N) \rightarrow E_{K_1}(N) + E_{K_2}(N)$

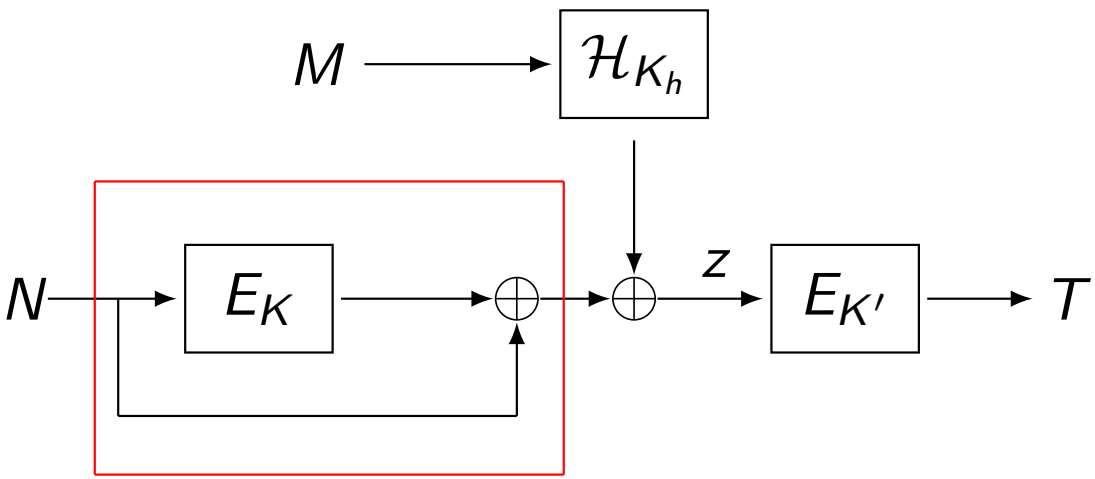


- Nonce Respecting (NR) : Beyond Birthday Bound Security.
- Nonce Misuse (NM) : Birthday Bound Security.

Can we reduce the number of BC calls?

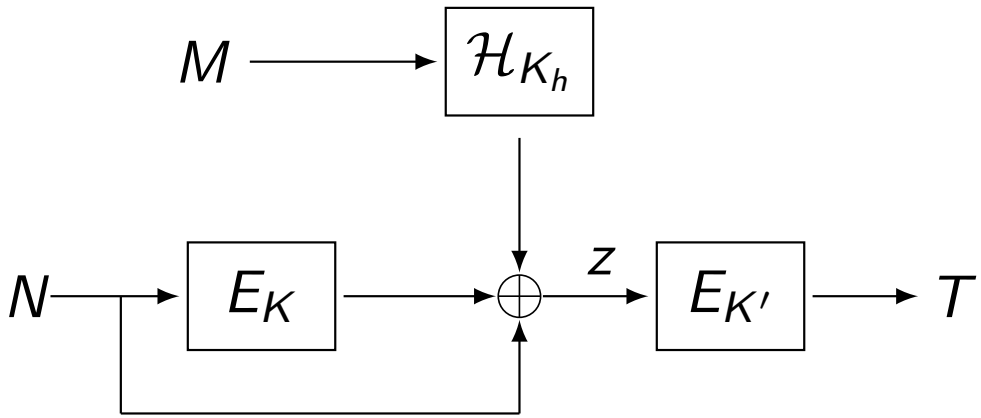
Instantiation of F_K

3. Encrypted Wegman-Carter with Davies-Meyer :
$F_K(N) \to E_K(N) + N$



Instantiation of F_K by Keyed Davies-Meyer Construction

EWCDM [Cogliati and Seurin, CRYPTO 2016]



Conjecture of Cogliati and Seurin

Single keyed EWCDM (i.e $K = K'$) is BBB Secure against NR adversaries.

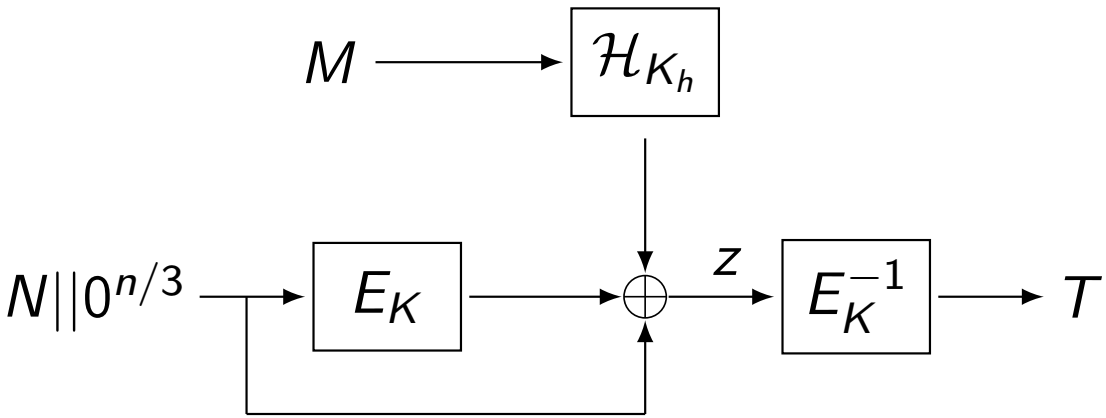
Summary So Far

- Birthday Bound Forgery for ECBC MAC.
- WC is completely broken for a single repetition of nonce.
- EWCDM has the following features:
  1. Based on block cipher (pseudorandom permutation)
  2. BBB security against NR adversaries
  3. Birthday bound security against NM adversaries
  4. But, it has three keys!!

§ Coming up: How to get Single Keyed BBB secure MAC.

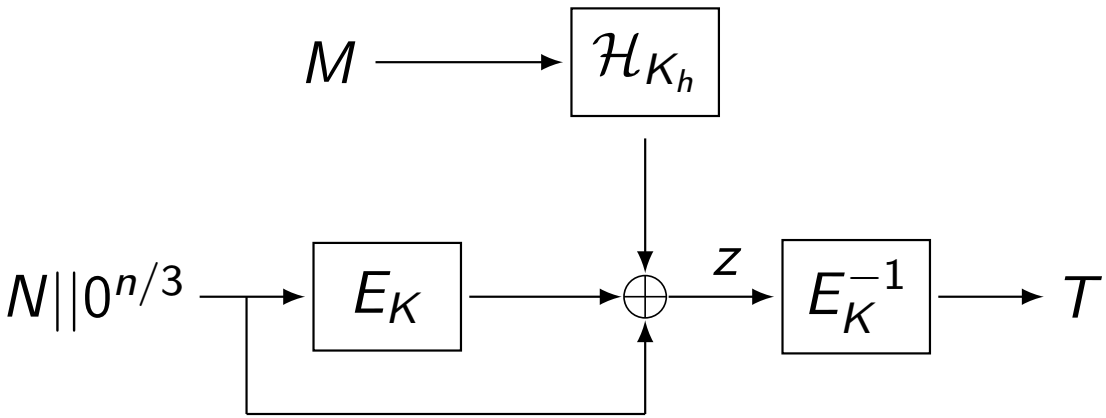
1. Decrypted Wegman-Carter with Davies-Meyer (DWCDM)

DWCDM



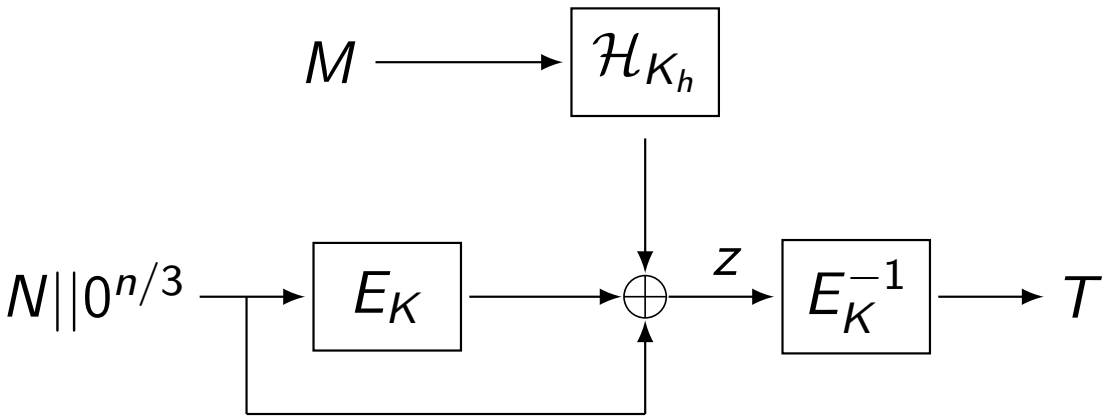
- Single Keyed Nonce Based MAC (Nonce Space: $2n/3$ bits)

DWCDM



- Single Keyed Nonce Based MAC (Nonce Space: $2n/3$ bits)
  why $2n/3$ bits ?

DWCDM

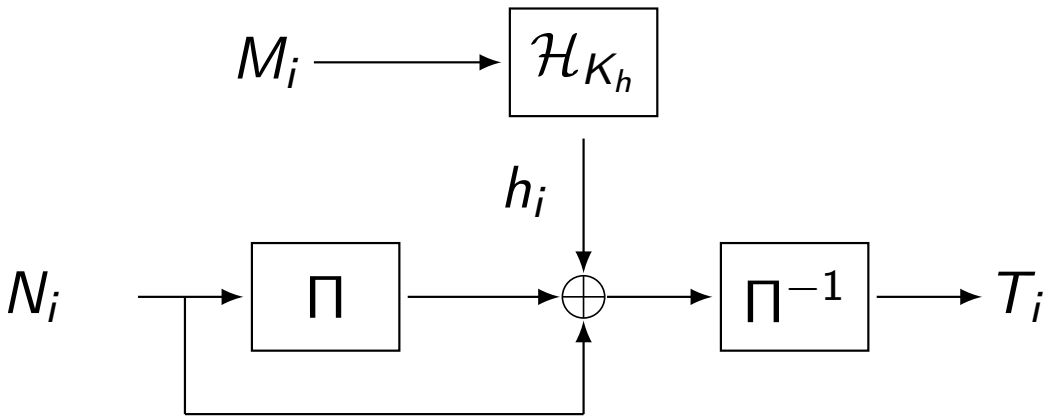


- Single Keyed Nonce Based MAC (Nonce Space: $2n/3$ bits) why $2n/3$ bits ?
- MAC security: $2n/3$-bit (NR setting), $n/2$-bit (NM setting)

A Glimpse of Pure Single Keyed DWCDM

- Derive the hash key as $K_h = \mathrm{E}_K(0^{n-1}1)$
- Polynomial hash applied on message
- Provides same level of security of DWCDM

Basic Idea of Proving Security



1. $\Pi(N_i) \oplus \Pi(T_i) = N_i \oplus h_i := \lambda_i$ for all i.
2. Sufficient to show high probability of above event for any fixed T_i and h_i (by fixing the hash key).
3. Want to estimate probability of $\Pi(N_i) \oplus \Pi(T_i) = \lambda_i$.

Analyzing the security of a MAC

1. The probability of $\Pi(n_i) \oplus \Pi(t_i) = n_i \oplus h_i := \lambda_i$ for all i is at least a value close to that of a random function.
2. In other words, want to find number of solutions of $P_{n_i} \oplus P_{t_i} = \lambda_i$ for all i, where $P_{n_i} = \Pi(n_i)$ and $P_{t_i} = Pi(t_i)$.
3. Group all n_i and t_i values depending on equalities. Let $x_1, \ldots, x_r$ denotes the distinct values.
4. Mirror Theory : Need to find number of solutions (P_x) of system of linear equations such that P_x's are distinct.

2. Mirror Theory

Mirror Theory

A system of q equations over $\mathcal{P} = \{P_1, \ldots, P_r\}$ variables.

$$
\begin{aligned}
P_{n_1} \oplus P_{t_1} &= \lambda_1 \\
P_{n_2} \oplus P_{t_2} &= \lambda_2 \\
&\vdots \\
P_{n_q} \oplus P_{t_q} &= \lambda_q
\end{aligned}
$$

Mirror Theory

A system of q equations over $\mathcal{P} = \{P_1, \ldots, P_r\}$ variables.

$$
\begin{aligned}
P_{n_1} \oplus P_{t_1} &= \lambda_1 \\
P_{n_2} \oplus P_{t_2} &= \lambda_2 \\
&\vdots \\
P_{n_q} \oplus P_{t_q} &= \lambda_q
\end{aligned}
$$

where n_i's and t_i's represent indices from 1 to r not necessarily distinct.

Mirror Theory

A system of q equations over $\mathcal{P} = \{P_1, \ldots, P_r\}$ variables.

$$\begin{aligned} P_{n_1} \oplus P_{t_1} &= \lambda_1 \\ P_{n_2} \oplus P_{t_2} &= \lambda_2 \\ &\vdots \\ P_{n_q} \oplus P_{t_q} &= \lambda_q \end{aligned}$$

where n_i's and t_i's represent indices from 1 to r not necessarily distinct.

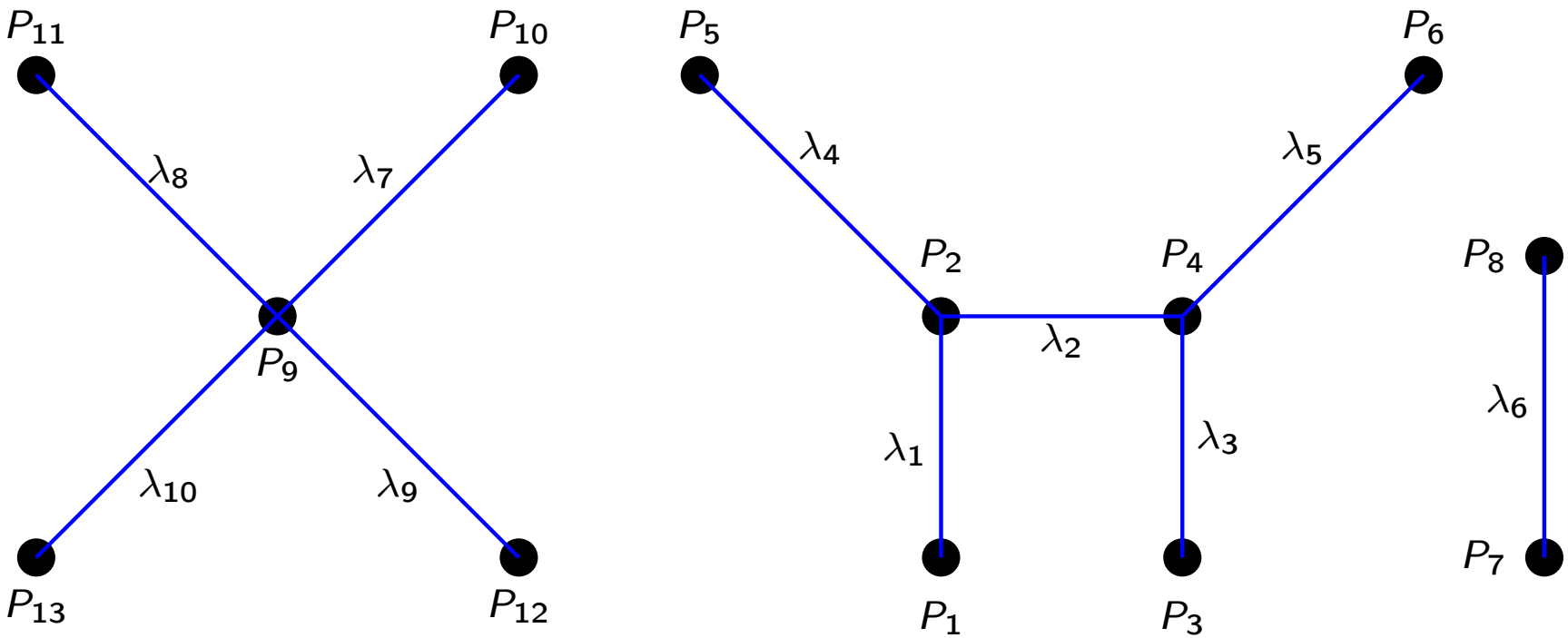
Goal of Mirror Theory

Count the number of solutions of $\mathcal{P}$ such that $P_a \neq P_b$ for $a \neq b \in \{1, \ldots, r\}$.

Current Status of Mirror Theory

- Optimal bound proved by Patarin.
- But the proof is not clear to the community.
- However, the proof is verifiable up to a certain security limit (e.g $3n/4$ in some cases).

Graphical view of Equations

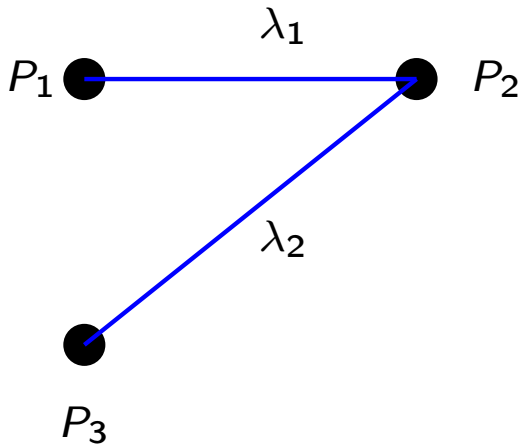


Cycle leads to dependency. So we assume acyclic graph.

Mirror Theory Example 1

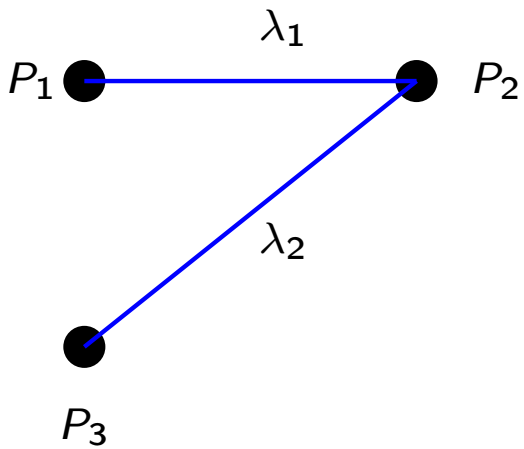
$$P_1 \oplus P_2 = \lambda_1$$

$$P_2 \oplus P_3 = \lambda_2$$



Mirror Theory Example 1

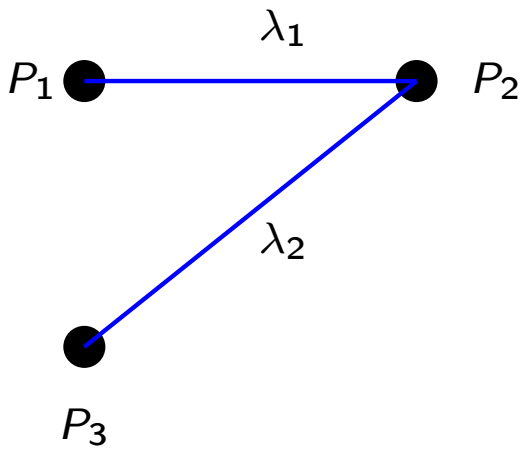
$$P_1 \oplus P_2 = \lambda_1$$
$$P_2 \oplus P_3 = \lambda_2$$



- Contradiction: $\lambda_1 = 0$ or $\lambda_2 = 0$ or $\lambda_1 = \lambda_2$. (Degeneracy)

Mirror Theory Example 1

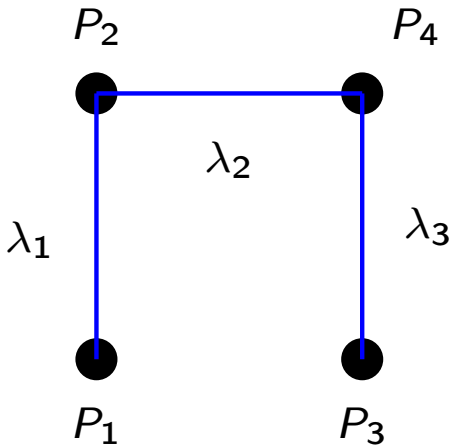
$$P_1 \oplus P_2 = \lambda_1$$
$$P_2 \oplus P_3 = \lambda_2$$



- Contradiction: $\lambda_1 = 0$ or $\lambda_2 = 0$ or $\lambda_1 = \lambda_2$. (Degeneracy)
- if $\lambda_1 \neq 0, \lambda_2 \neq 0, \lambda_1 \neq \lambda_2$, then the # of soln. is 2^n.

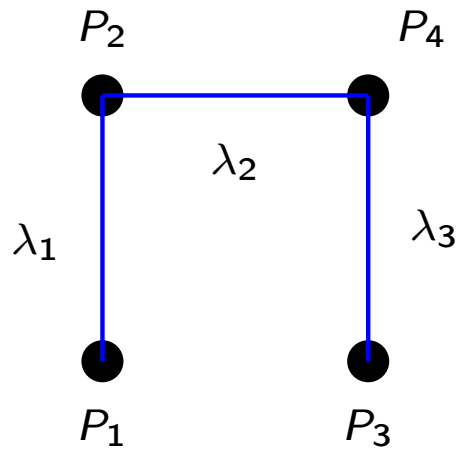
Mirror Theory Example 2

$$P_1 \oplus P_2 = \lambda_1$$
$$P_2 \oplus P_4 = \lambda_2$$
$$P_3 \oplus P_4 = \lambda_3$$



Mirror Theory Example 2

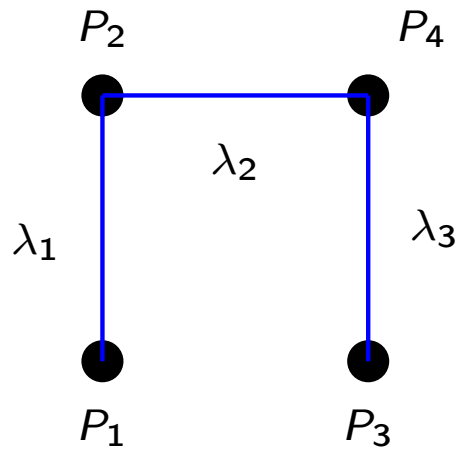
$$P_1 \oplus P_2 = \lambda_1$$
$$P_2 \oplus P_4 = \lambda_2$$
$$P_3 \oplus P_4 = \lambda_3$$



- Contradiction: $\lambda_1 \oplus \lambda_2 \oplus \lambda_3 = 0$ or λ_1 or $\lambda_2 = 0$ or $\lambda_3 = 0$ or $\lambda_1 = \lambda_2$ or $\lambda_1 = \lambda_3$ or $\lambda_2 = \lambda_3$. (Degeneracy)

Mirror Theory Example 2

$$P_1 \oplus P_2 = \lambda_1$$
$$P_2 \oplus P_4 = \lambda_2$$
$$P_3 \oplus P_4 = \lambda_3$$



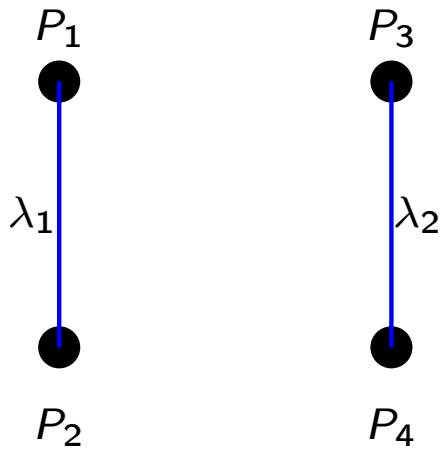
- Contradiction: $\lambda_1 \oplus \lambda_2 \oplus \lambda_3 = 0$ or λ_1 or $\lambda_2 = 0$ or $\lambda_3 = 0$ or $\lambda_1 = \lambda_2$ or $\lambda_1 = \lambda_3$ or $\lambda_2 = \lambda_3$. (Degeneracy)
- if no contradiction, then the # of solution is 2^n.

Degeneracy

1. To have a solution the sum of all labels of any path (can be an edge) should be nonzero.
2. If so, the number of solutions for a single component is 2^n.

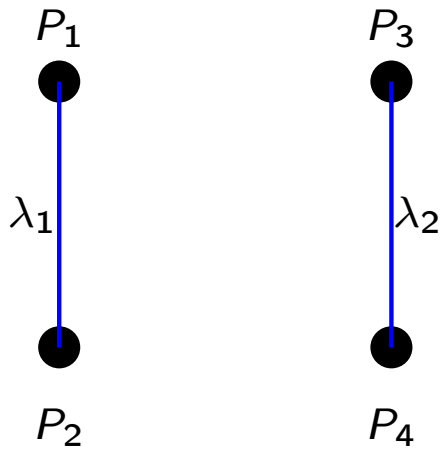
Mirror Theory Example 3

$$P_1 \oplus P_2 = \lambda_1$$
$$P_3 \oplus P_4 = \lambda_2$$



Mirror Theory Example 3

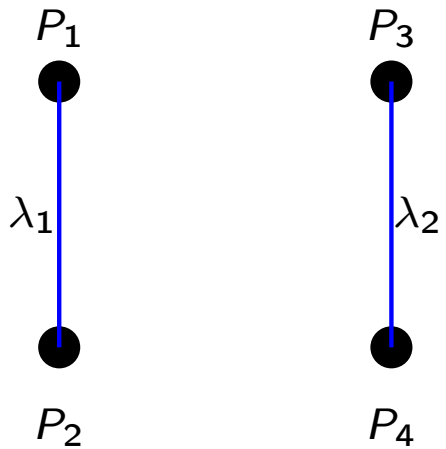
$$P_1 \oplus P_2 = \lambda_1$$
$$P_3 \oplus P_4 = \lambda_2$$



- Contradiction: $\lambda_1 = 0$ or $\lambda_2 = 0$. (Degeneracy)

Mirror Theory Example 3

$$P_1 \oplus P_2 = \lambda_1$$
$$P_3 \oplus P_4 = \lambda_2$$



- Contradiction: $\lambda_1 = 0$ or $\lambda_2 = 0$. (Degeneracy)
- if $\lambda_1 \neq 0, \lambda_2 \neq 0$, then the # of soln. is at least $2^n(2^n - 4)$ (why?).

Mirror Theory

In summary, Graph G is bad if

- (P.1) G contains a cycle
- (P.2) There is a path P in G, the sum of label of P is zero.

Mirror Theory

In summary, Graph G is bad if

- (P.1) G contains a cycle
- (P.2) There is a path P in G, the sum of label of P is zero.

Good Graph

G is good if G does not satisfy above.

Mirror Theory

In summary, Graph G is bad if

- (P.1) G contains a cycle
- (P.2) There is a path P in G, the sum of label of P is zero.

Good Graph

G is good if G does not satisfy above.

Main result (Mirror Theory by Patarin)

If $G = (\mathcal{V}, \mathcal{E})$ is a good graph, where $|\mathcal{V}| = r, |\mathcal{E}| = q$, then the distinct number of solutions is at least

$$\frac{(2^n)_r}{2^{nq}},$$

provided $(\xi_{\max} - 1)^2 \cdot r \leq 2^n/67$.

Mirror Theory

In summary, Graph G is bad if

- (P.1) G contains a cycle
- (P.2) There is a path P in G, the sum of label of P is zero.

Good Graph

G is good if G does not satisfy above.

Main result (Verifiable)

If $G = (\mathcal{V}, \mathcal{E})$ is a good graph, where $|\mathcal{V}| = r, |\mathcal{E}| = q$, then the distinct number of solutions is at least

$$\frac{(2^n)_r}{2^{nq}}(1 - \frac{q^3}{2^{2n}}).$$

MAC and Verification Eqn

MAC Eqn.

$$\Pi(N_1) \oplus \Pi(T_1) = \lambda_1$$
$$\Pi(N_2) \oplus \Pi(T_2) = \lambda_2$$
$$\vdots$$
$$\Pi(N_{q_m}) \oplus \Pi(T_{q_m}) = \lambda_{q_m}$$

MAC and Verification Eqn

MAC Eqn.

$$\Pi(N_1) \oplus \Pi(T_1) = \lambda_1$$
$$\Pi(N_2) \oplus \Pi(T_2) = \lambda_2$$
$$\vdots$$
$$\Pi(N_{q_m}) \oplus \Pi(T_{q_m}) = \lambda_{q_m}$$

Verification Non-Eqn

$$\Pi(N'_1) \oplus \Pi(T'_1) \neq \lambda'_1$$
$$\Pi(N'_2) \oplus \Pi(T'_2) \neq \lambda'_2$$
$$\vdots$$
$$\Pi(N'_{q_v}) \oplus \Pi(T'_{q_v}) \neq \lambda'_{q_v}$$

$$\boxed{\lambda_i = N_i \oplus H_k(M_i), \quad \lambda'_i = N'_i \oplus H_k(M'_i)}$$

Mirror theory can be extended for non-equations also.

Summary

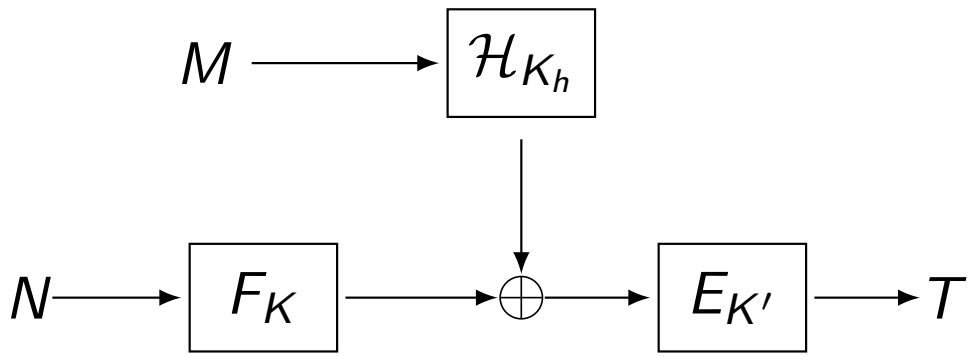
1. Classical constructions are birthday bound secure.
2. Wegman-Carter MAC and its different variants can provide BBB security in NR model.
3. DWCDM: A simple variant of EWCDM (Decryption instead of encryption) is single-keyed.
4. Security analysis relies on Mirror Theory.
5. Better understanding of Mirror Theory and its variants is important for many PRF and MAC Constructions.

Summary

1. Classical constructions are birthday bound secure.
2. Wegman-Carter MAC and its different variants can provide BBB security in NR model.
3. DWCDM: A simple variant of EWCDM (Decryption instead of encryption) is single-keyed.
4. Security analysis relies on Mirror Theory.
5. Better understanding of Mirror Theory and its variants is important for many PRF and MAC Constructions.

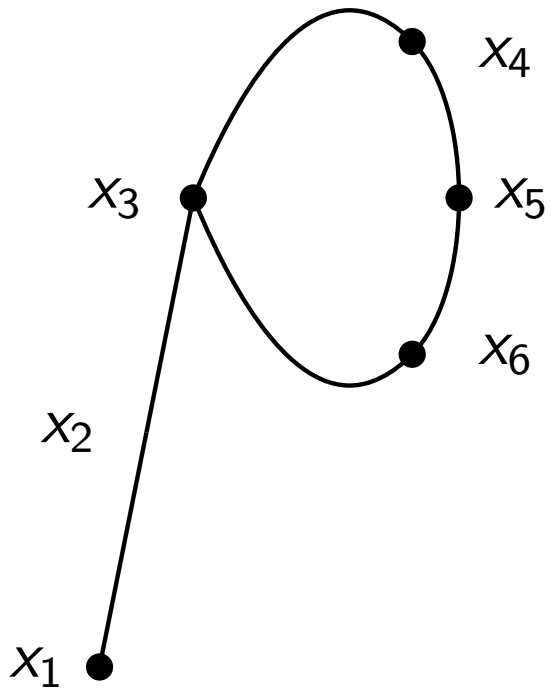
Thank You For Your Attention.

Nonce Misuse Attack on Encrypted Wegman Carter MAC



- A makes $2^{n/2}$ queries (N_i, M) with distinct nonces N_i.
- W.h.p A finds a collision in the tag $(T_i = T_j)$.
- A makes another queries (N_i, M') and obtains reply T
- A forges with (N_j, M', T).

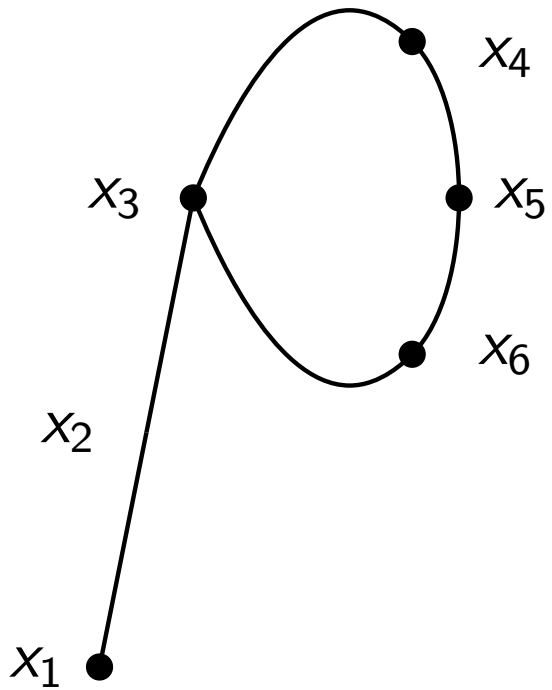
What if Nonce has n bits? (Nonce feedback attack)



$$
\begin{aligned}
\Pi(x_1) \oplus \Pi(x_2) &= H_k(m) + x_1 \\
\Pi(x_2) \oplus \Pi(x_3) &= H_k(m) + x_2 \\
\Pi(x_3) \oplus \Pi(x_4) &= H_k(m) + x_3 \\
\Pi(x_4) \oplus \Pi(x_5) &= H_k(m) + x_4 \\
\Pi(x_5) \oplus \Pi(x_6) &= H_k(m) + x_5 \\
\Pi(x_6) \oplus \Pi(x_3) &= H_k(m) + x_6
\end{aligned}
$$

$$x_3 + x_4 + x_5 + x_6 = 0$$

What if Nonce has n bits? (Nonce feedback attack)



$$
\begin{aligned}
\Pi(x_1) \oplus \Pi(x_2) &= H_k(m) + x_1 \\
\Pi(x_2) \oplus \Pi(x_3) &= H_k(m) + x_2 \\
\Pi(x_3) \oplus \Pi(x_4) &= H_k(m) + x_3 \\
\Pi(x_4) \oplus \Pi(x_5) &= H_k(m) + x_4 \\
\Pi(x_5) \oplus \Pi(x_6) &= H_k(m) + x_5 \\
\Pi(x_6) \oplus \Pi(x_3) &= H_k(m) + x_6
\end{aligned}
$$

$$x_3 + x_4 + x_5 + x_6 = 0$$

Forging Event

$(x_i + x_{i+1} + \cdots + x_j = 0) \Rightarrow (x_j, m, x_i)$ is a valid forgery.