The Exact Security of PMAC

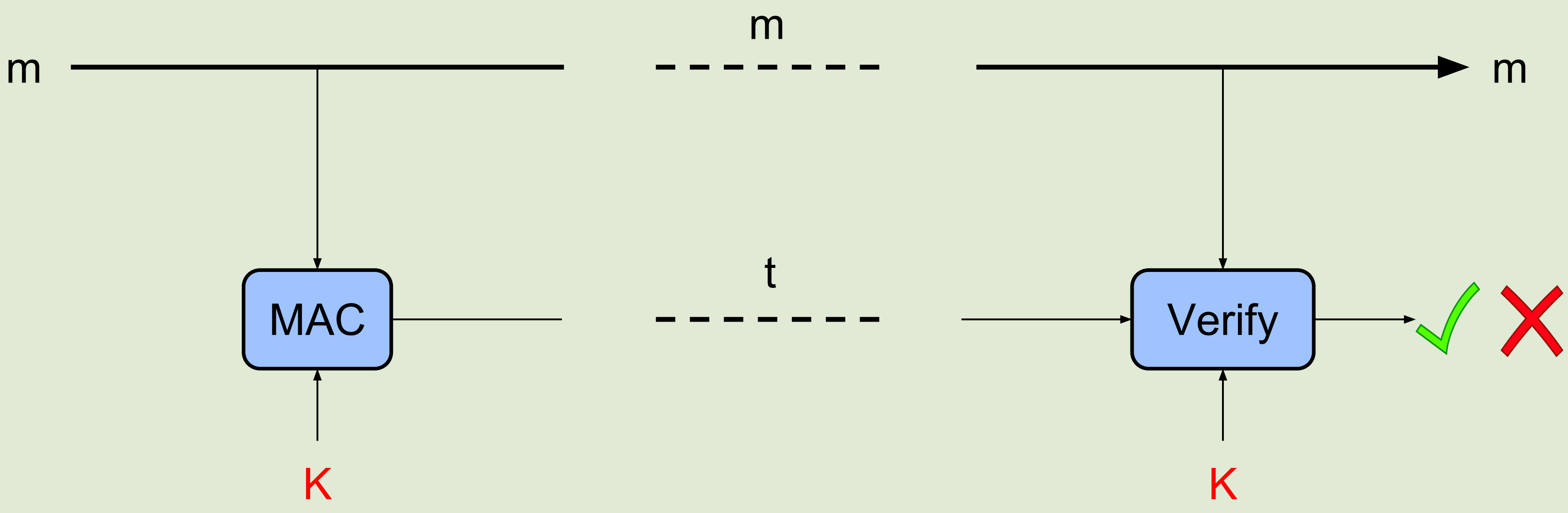
Peter Gaži **Krzysztof Pietrzak** **<u>Michal Rybár</u>**

IST Austria

Fast Software Encryption 2017

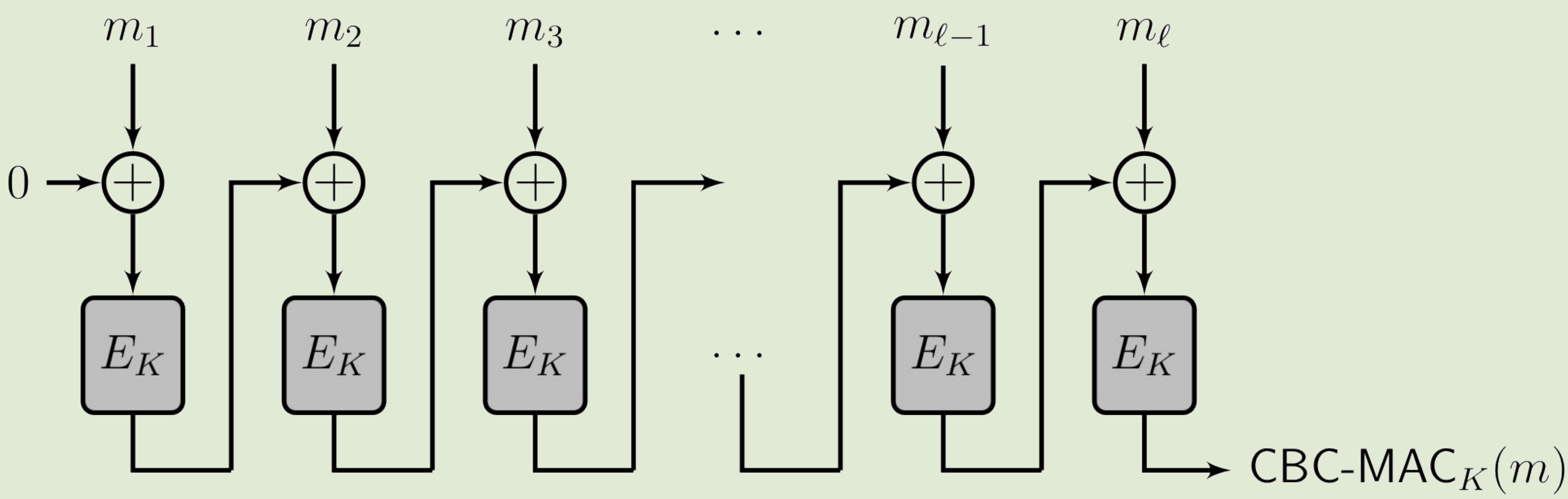
Message Authentication Codes

- Authenticating messages over an insecure channel



- Shared symmetric key K

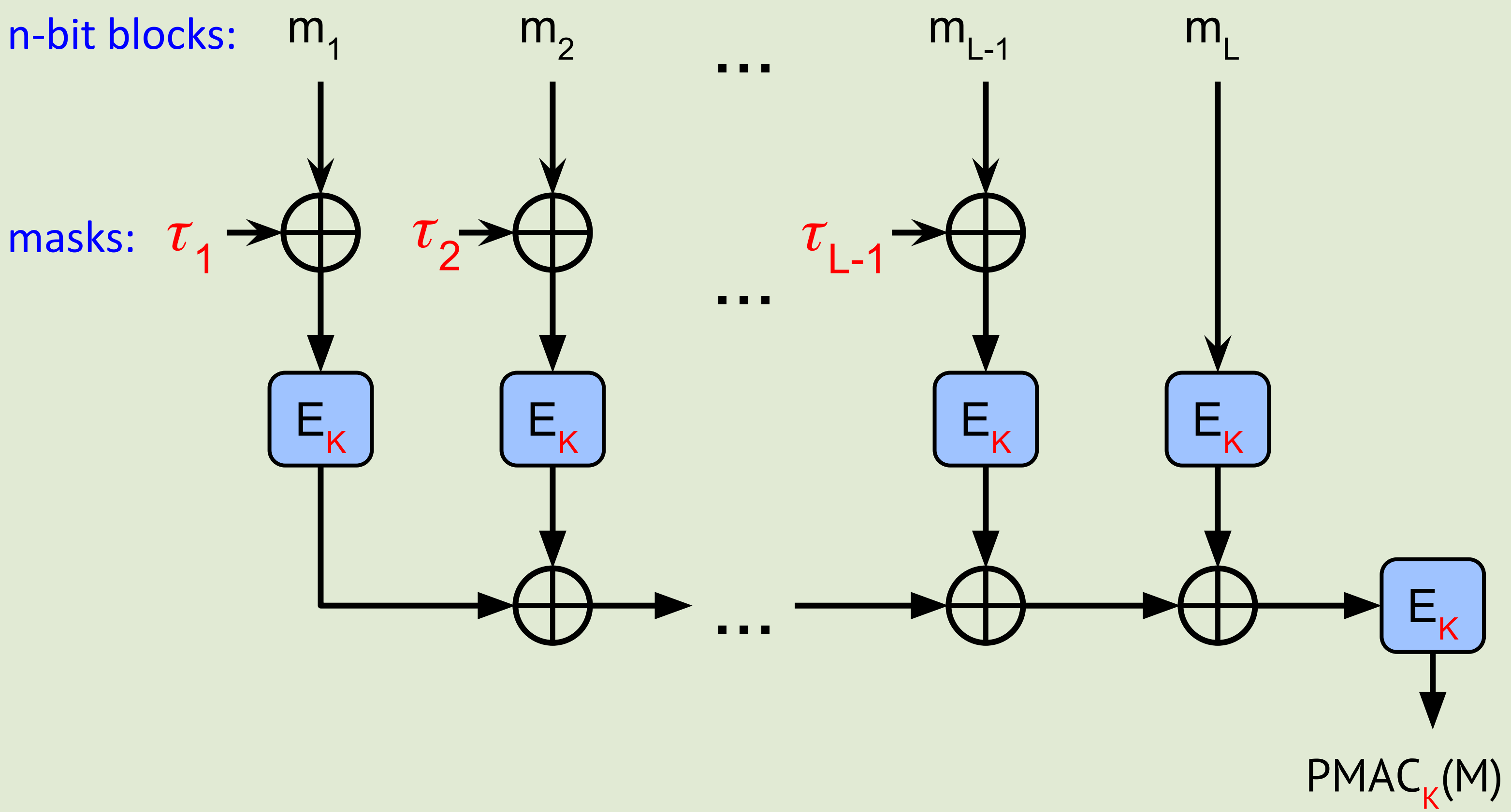
CBC-MAC [Bellare - Kilian - Rogaway '01]



- Encrypted-CBC additionally encrypts the output

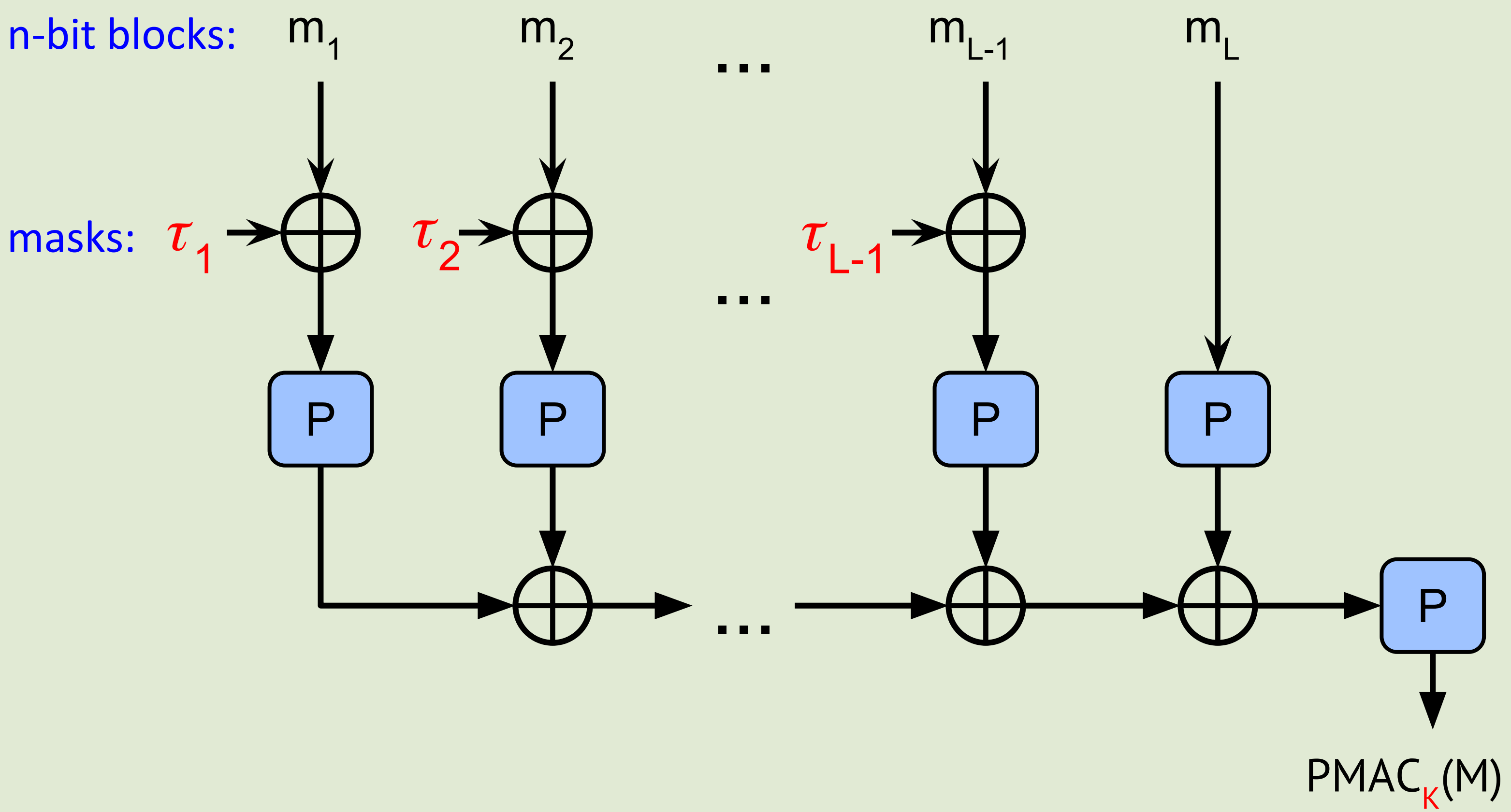
ParallelizableMAC [Black - Rogaway '02]

- Most prominent **parallel** MAC
- Some CAESAR candidates inspired by PMAC

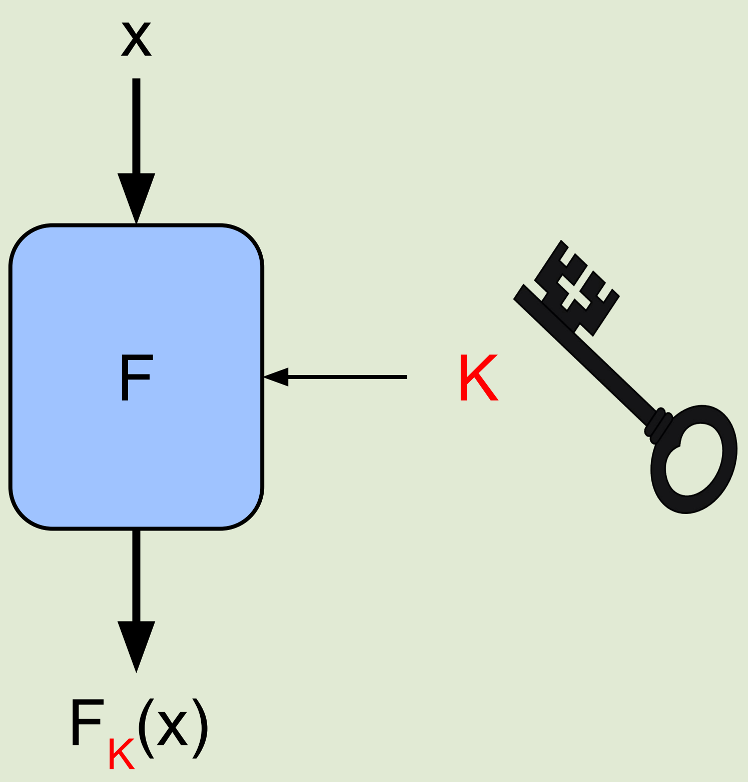


ParallelizableMAC [Black - Rogaway '02]

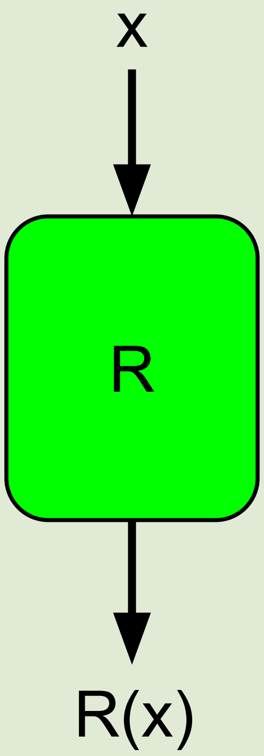
- We work with random permutations
- We focus on the **key-dependent masks** $\tau_1, \tau_2, \ldots, \tau_L$



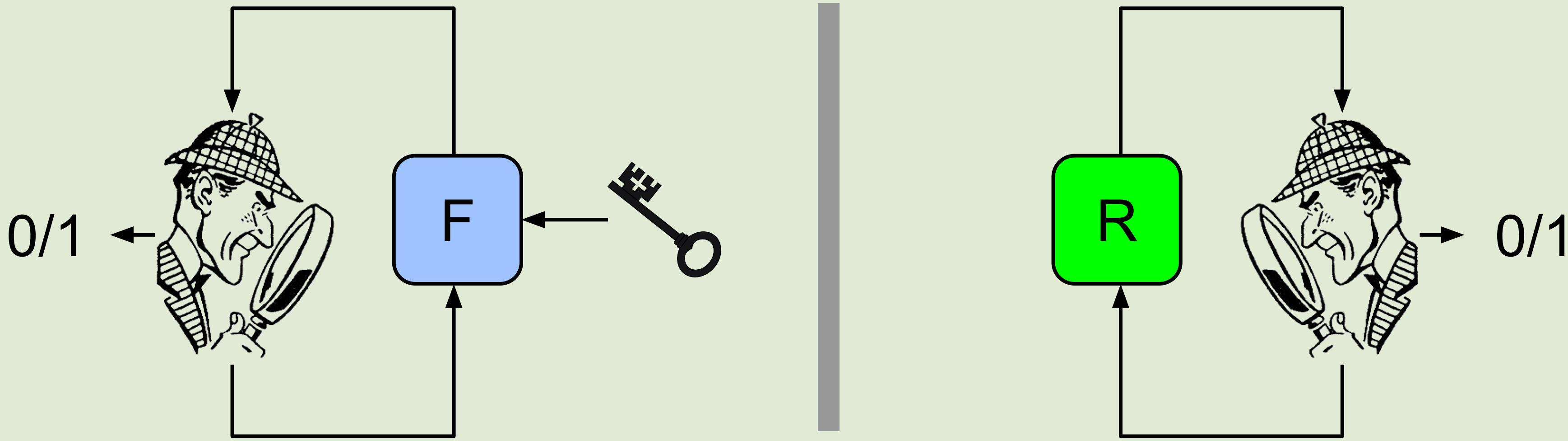
Pseudo-random Functions (PRFs)



Random Functions

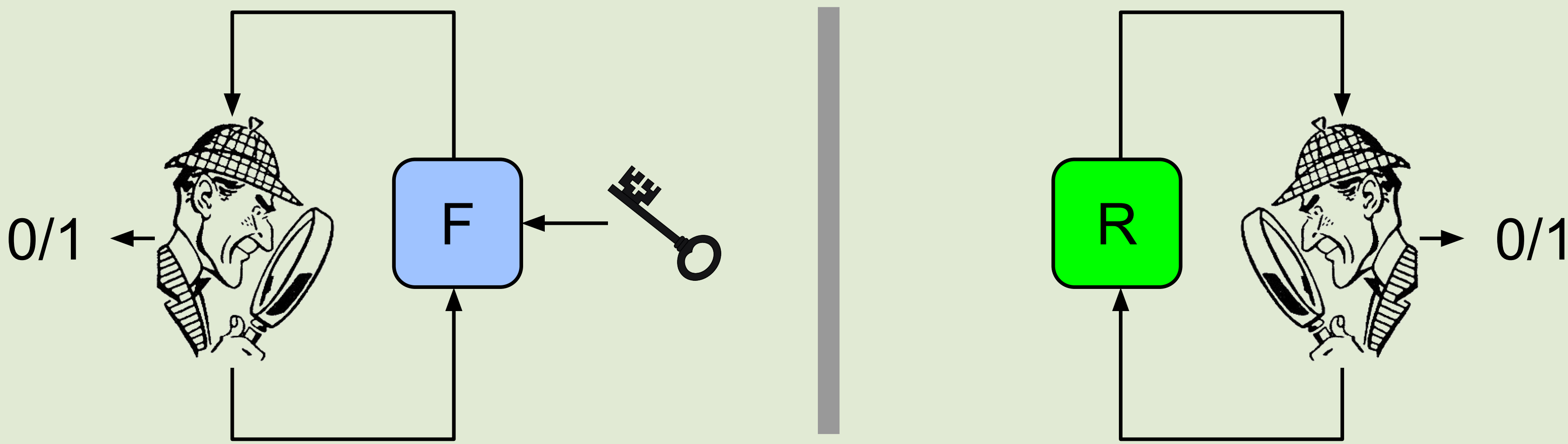


PRF advantage



PRF advantage: Pr[D($\mathbf{F}_K$) = 1] - Pr[D($\mathbf{R}$) = 1]

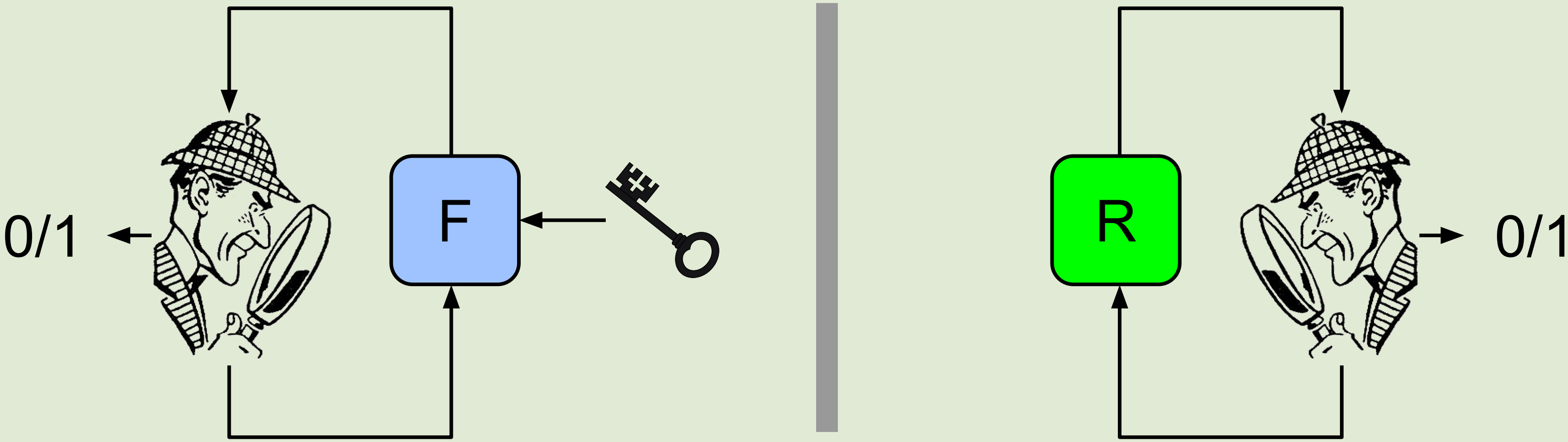
PRF advantage



PRF advantage: Pr[D($\mathbf{F}_K$) = 1] - Pr[D($\mathbf{R}$) = 1]

- Every PRF is a good MAC

PRF advantage

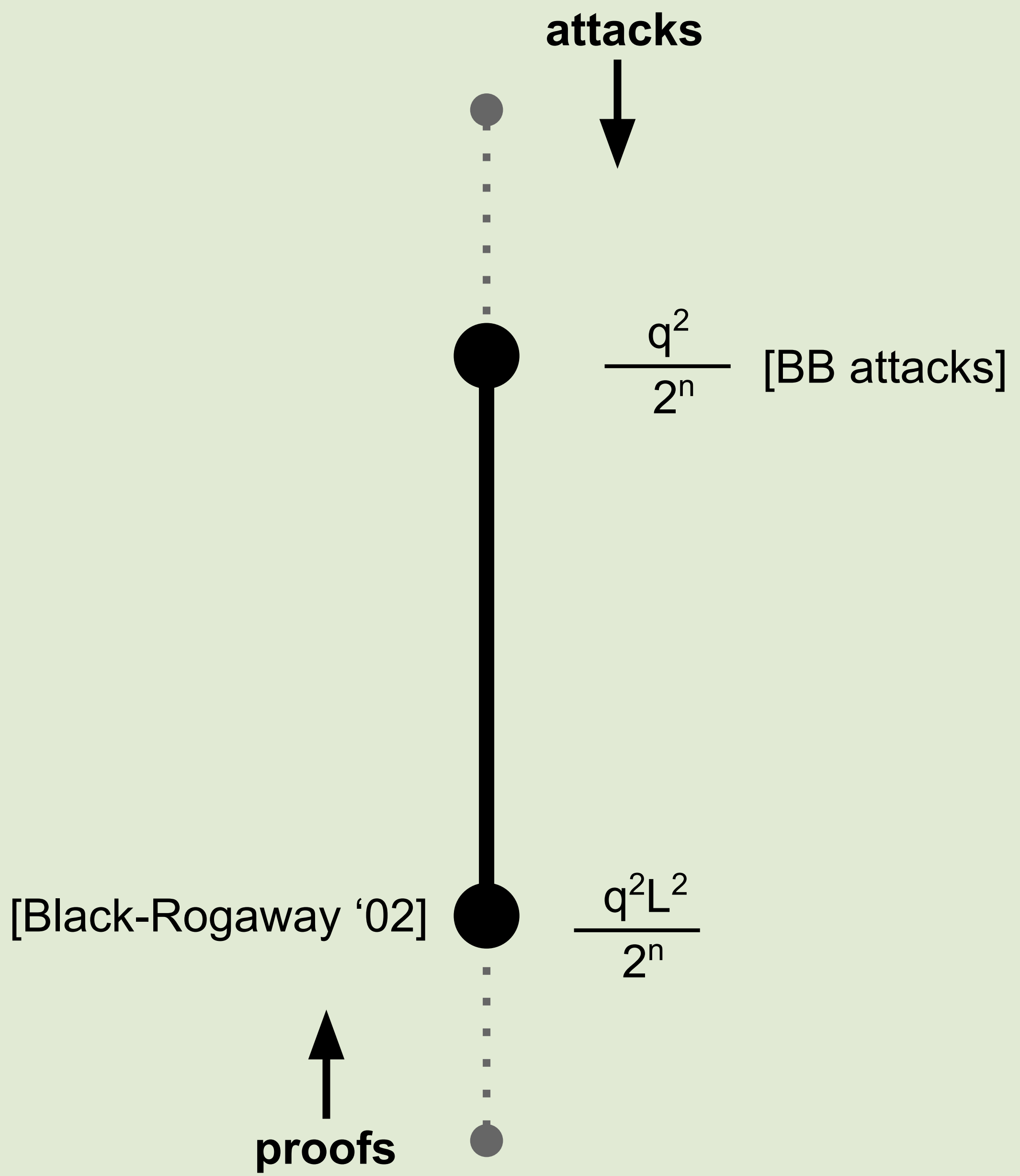


PRF advantage: Pr[D($\mathbf{F}_K$) = 1] - Pr[D($\mathbf{R}$) = 1]

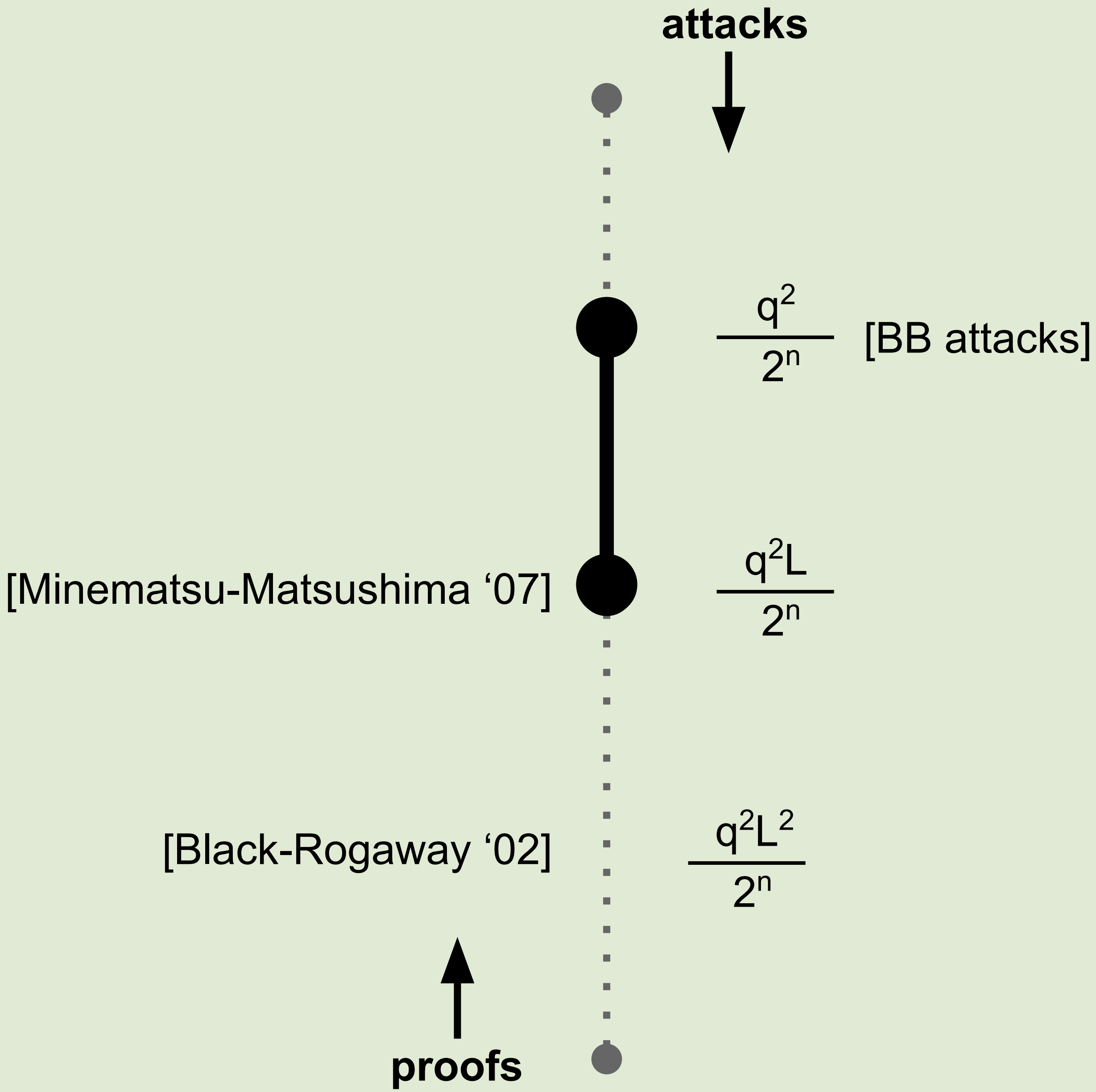
- Every PRF is a good MAC

- Security in terms of **Q messages** of length **L blocks** of size **N-bits**

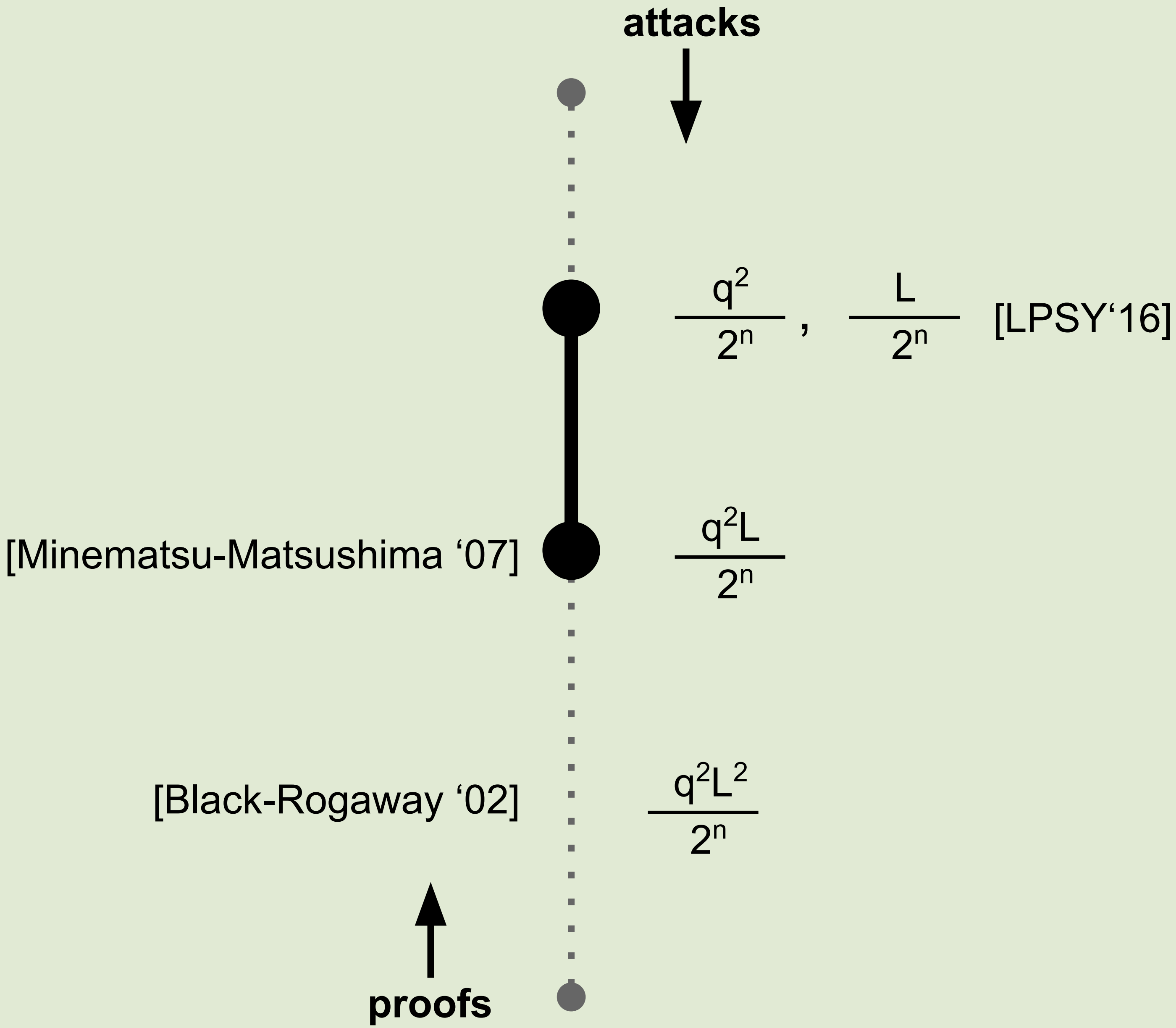
PRF security of PMAC - results



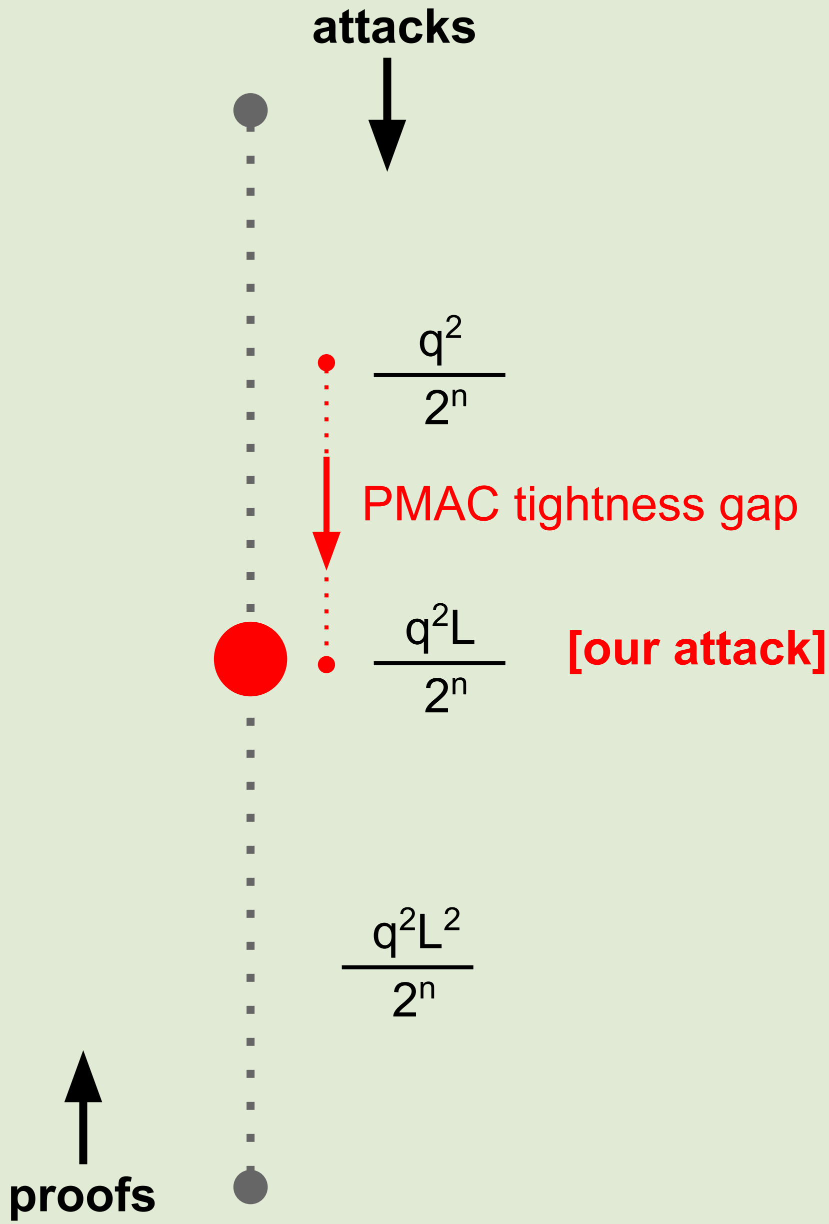
PRF security of PMAC - results



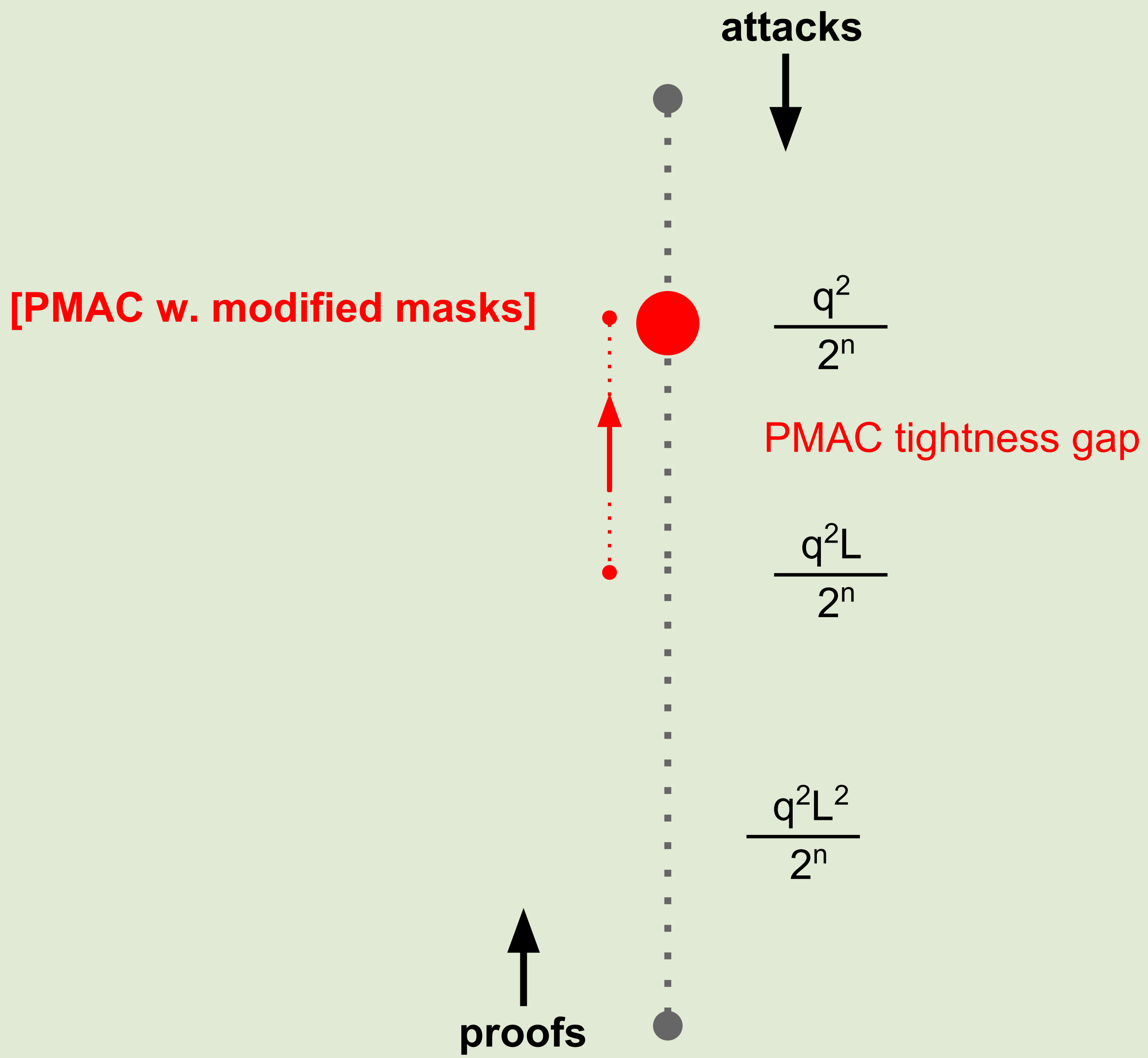
PRF security of PMAC - results



PRF security of PMAC - results

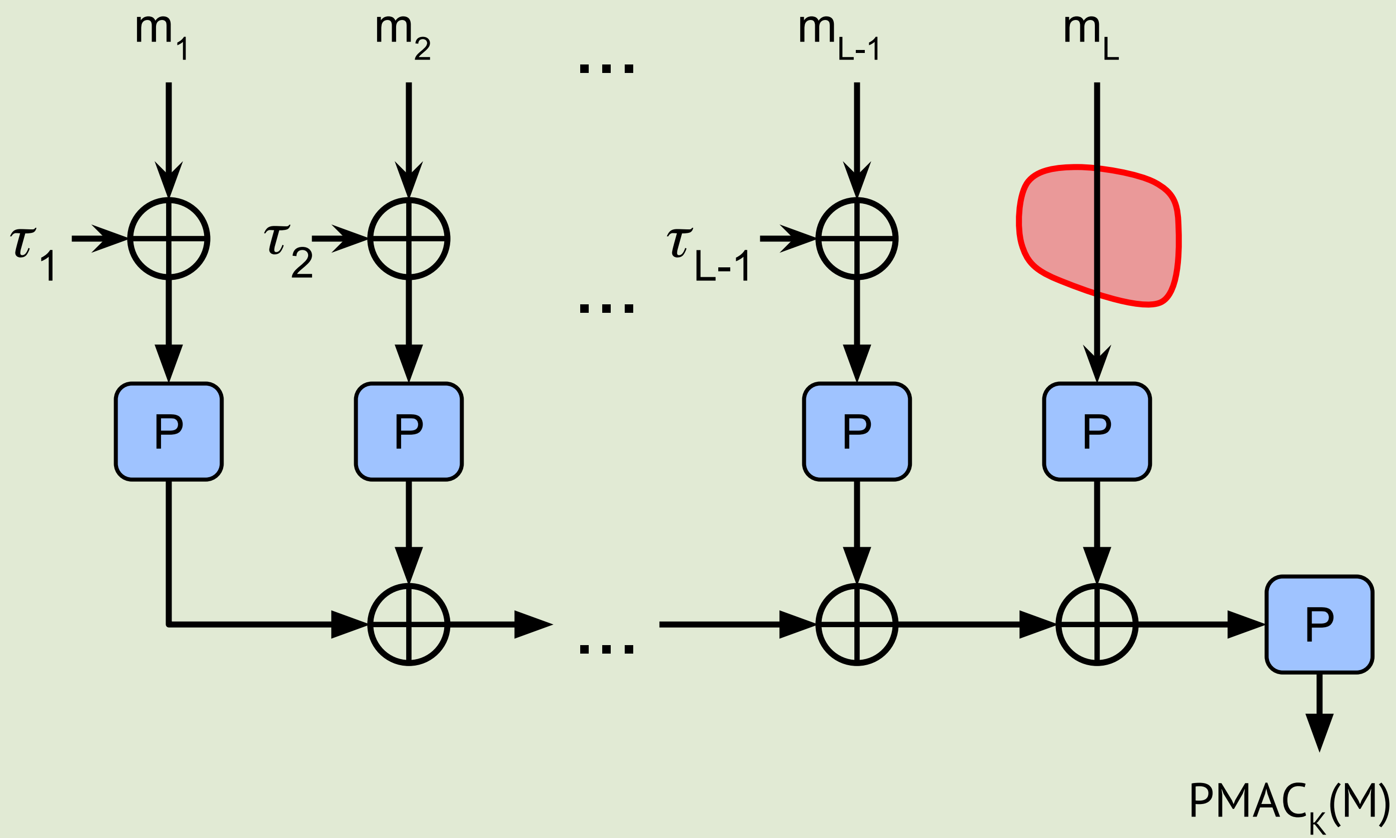


PRF security of PMAC - results



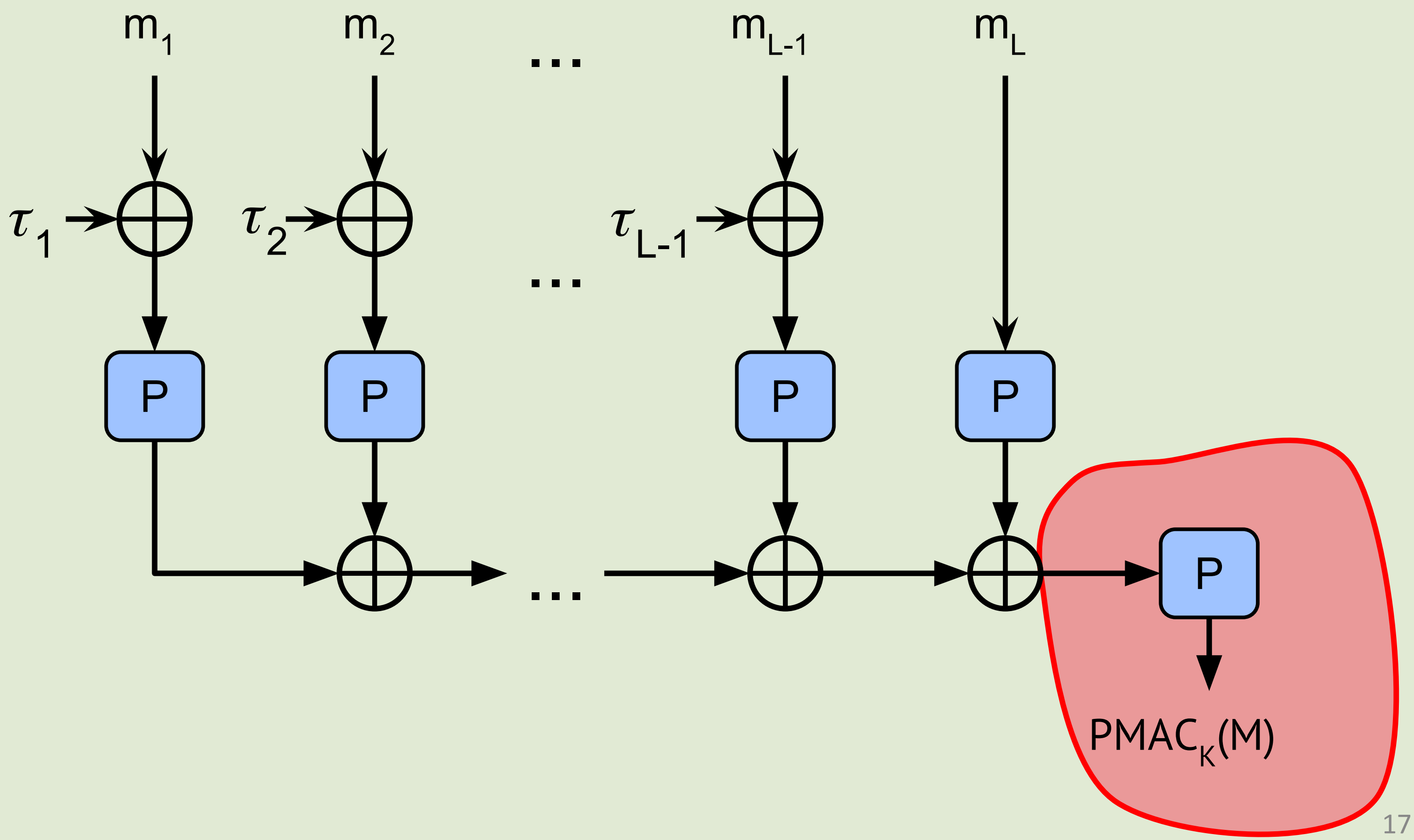
Reduction to simplified PMAC (sPMAC)

- We can ignore the last message block, **no mask**

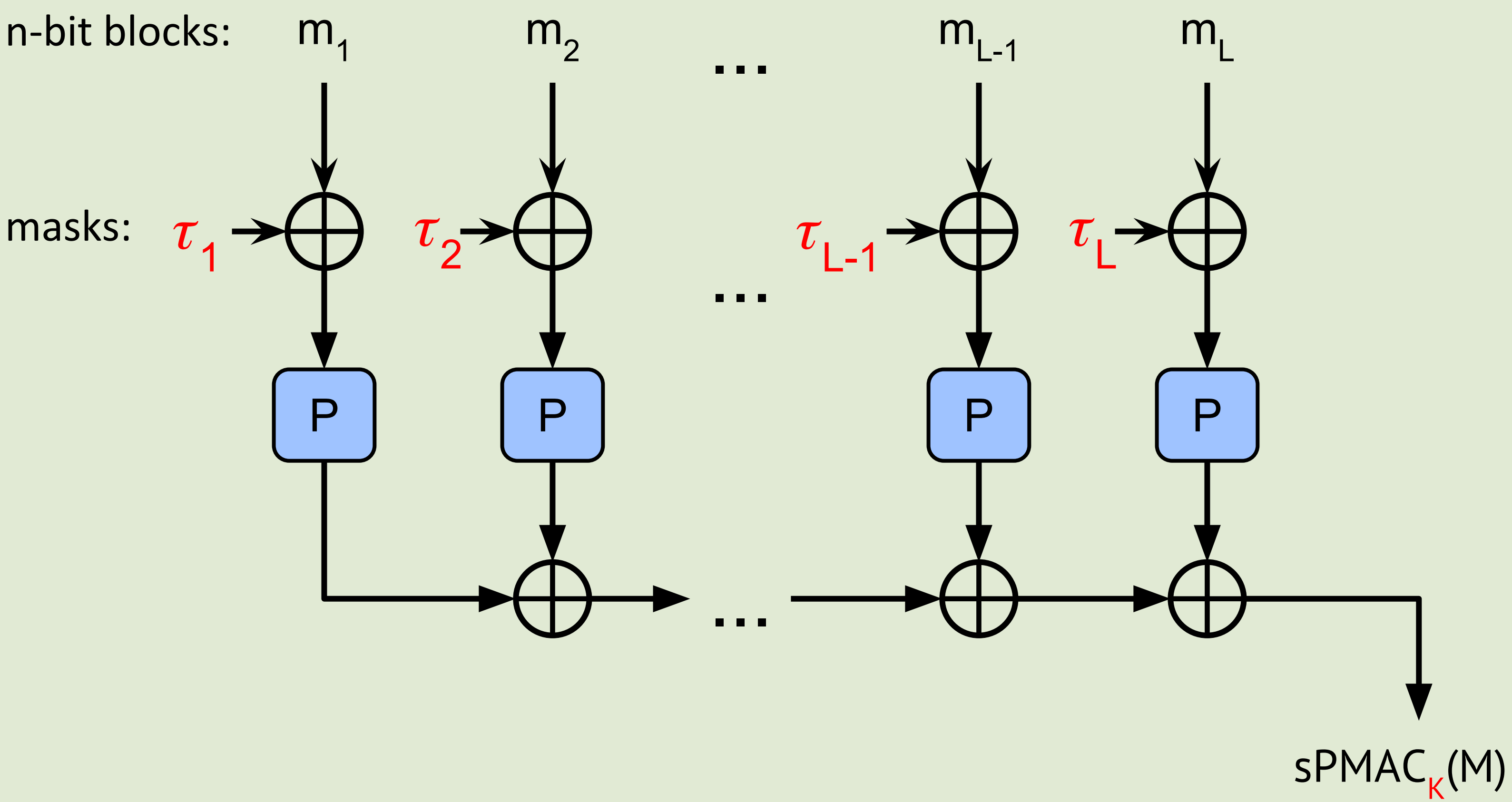


Reduction to sPMAC

- [Mau02]: **distinguishing** PMAC from a random function is equivalent to **non-adaptively triggering a collision** on the input to the outer permutation

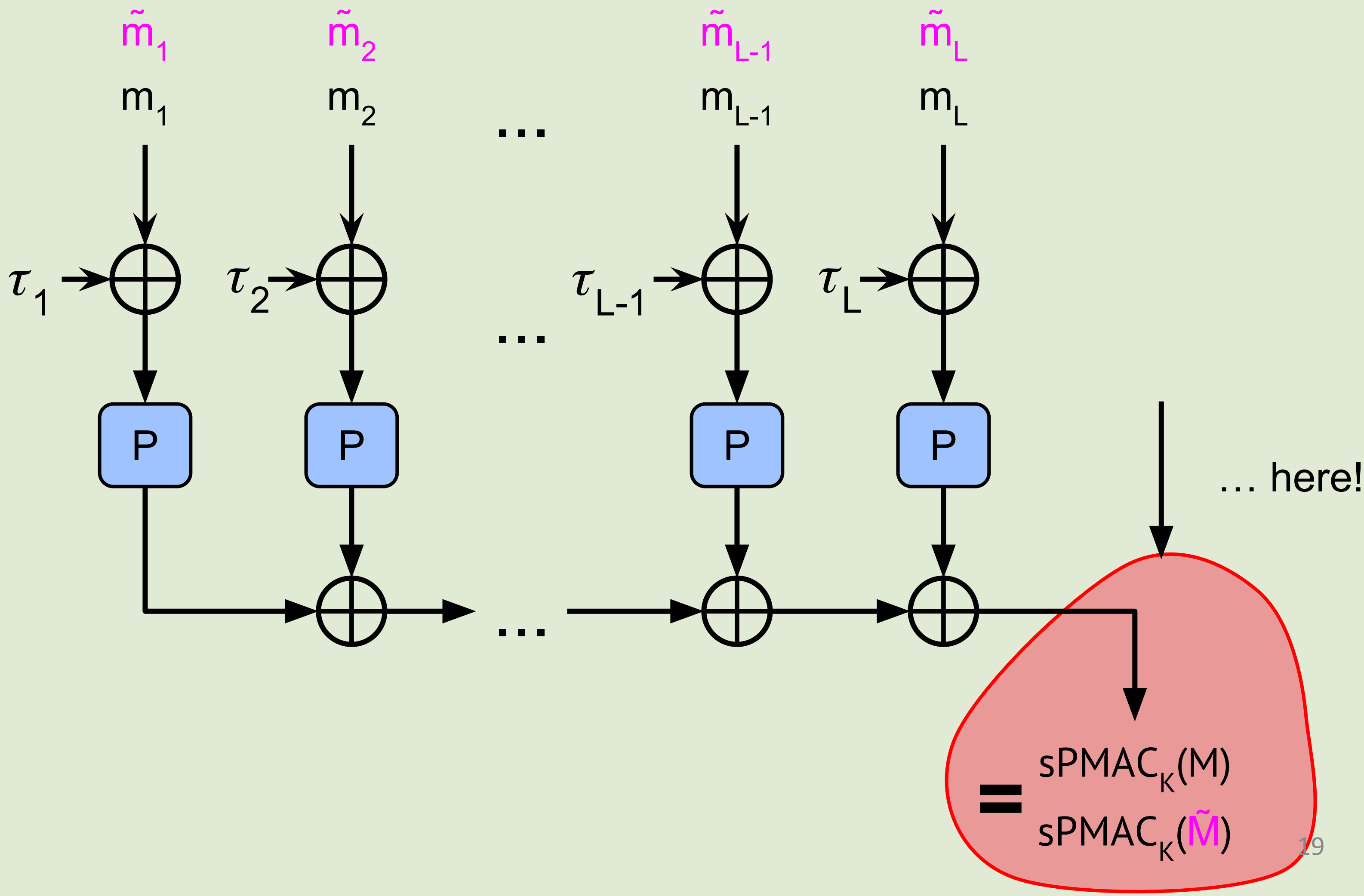


sPMAC



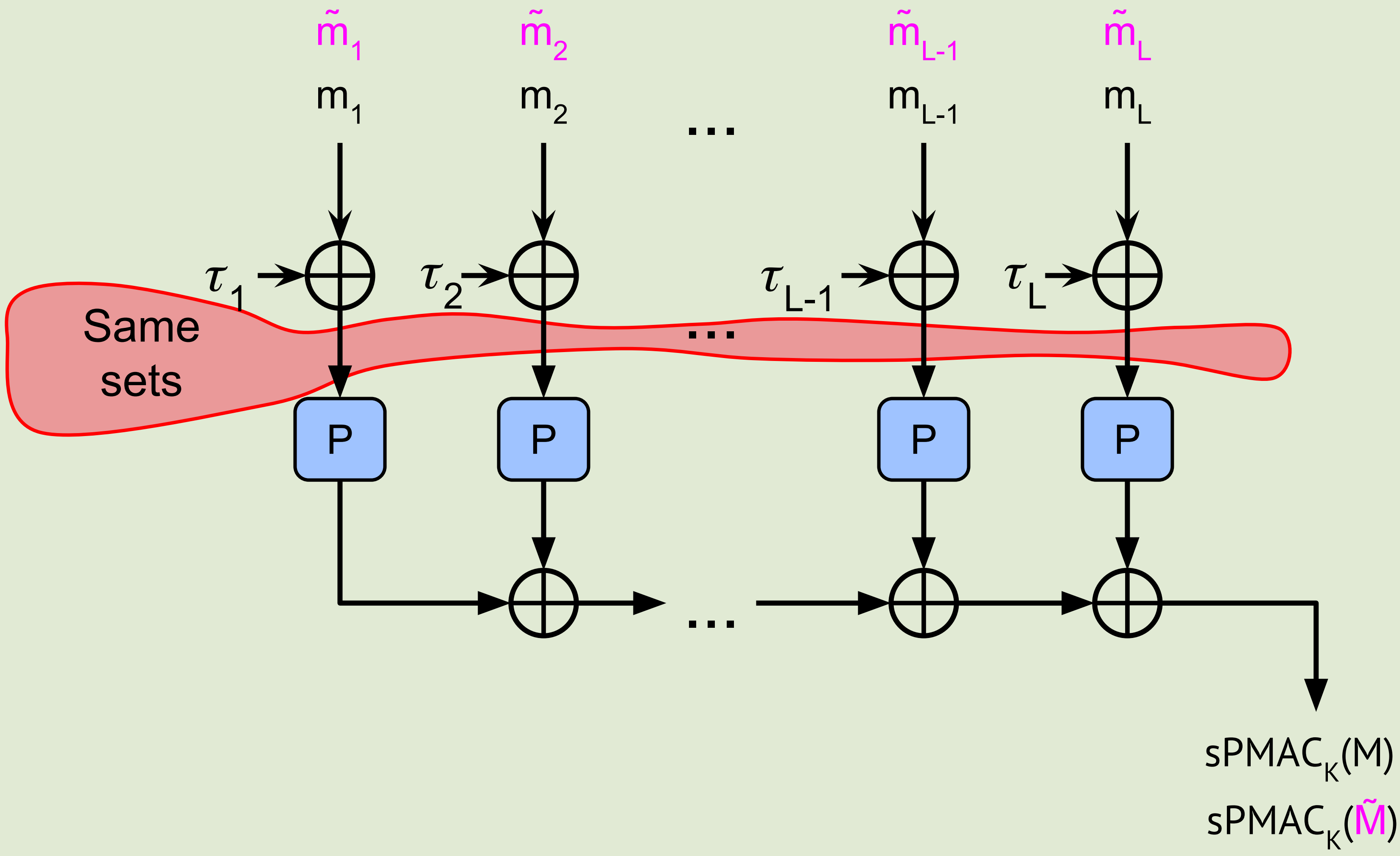
sPMAC - collisions

- Goal: collision of tags of M and $\tilde{M}$

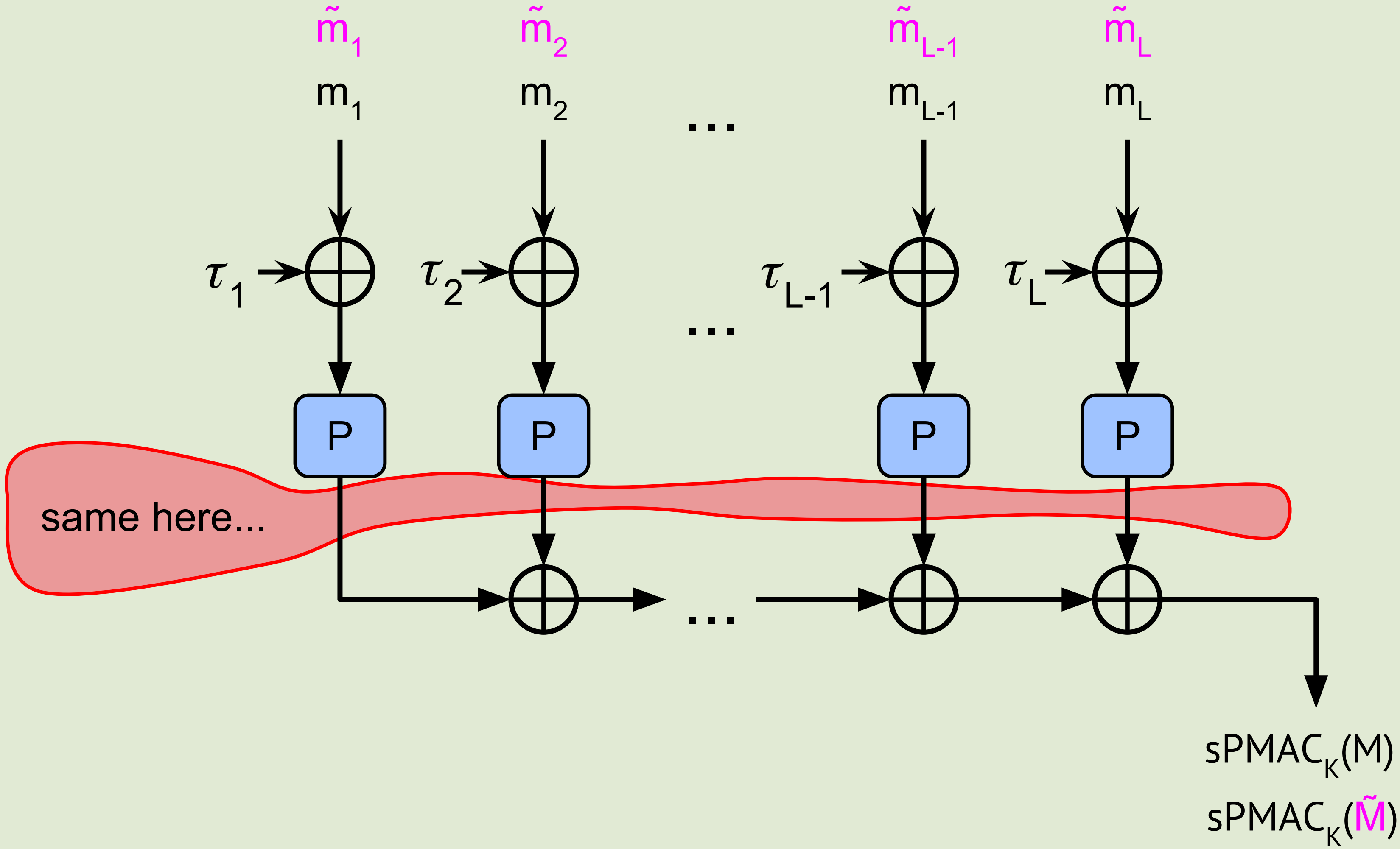


sPMAC - collisions

Collision: equality of sets of values

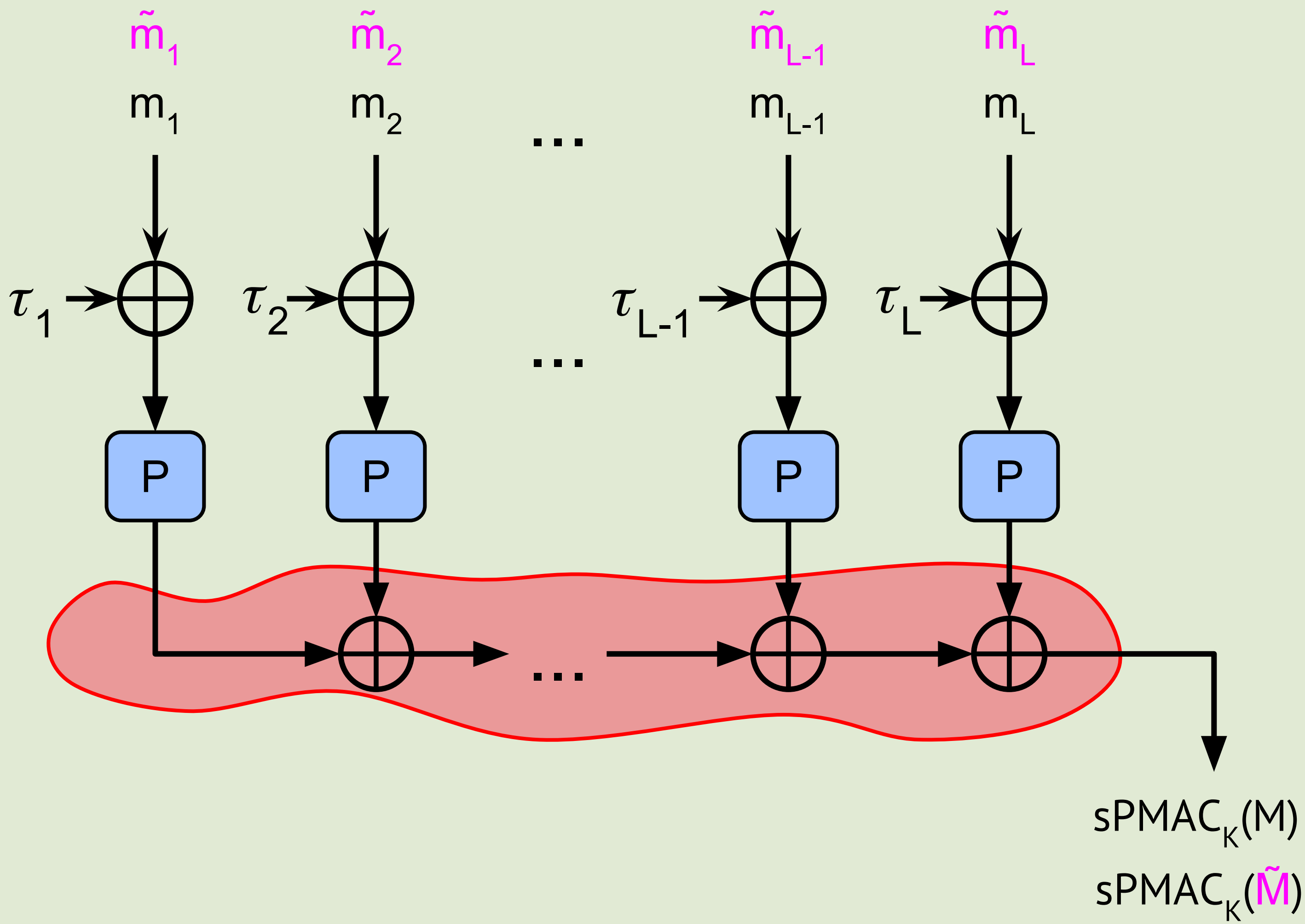


sPMAC - collisions



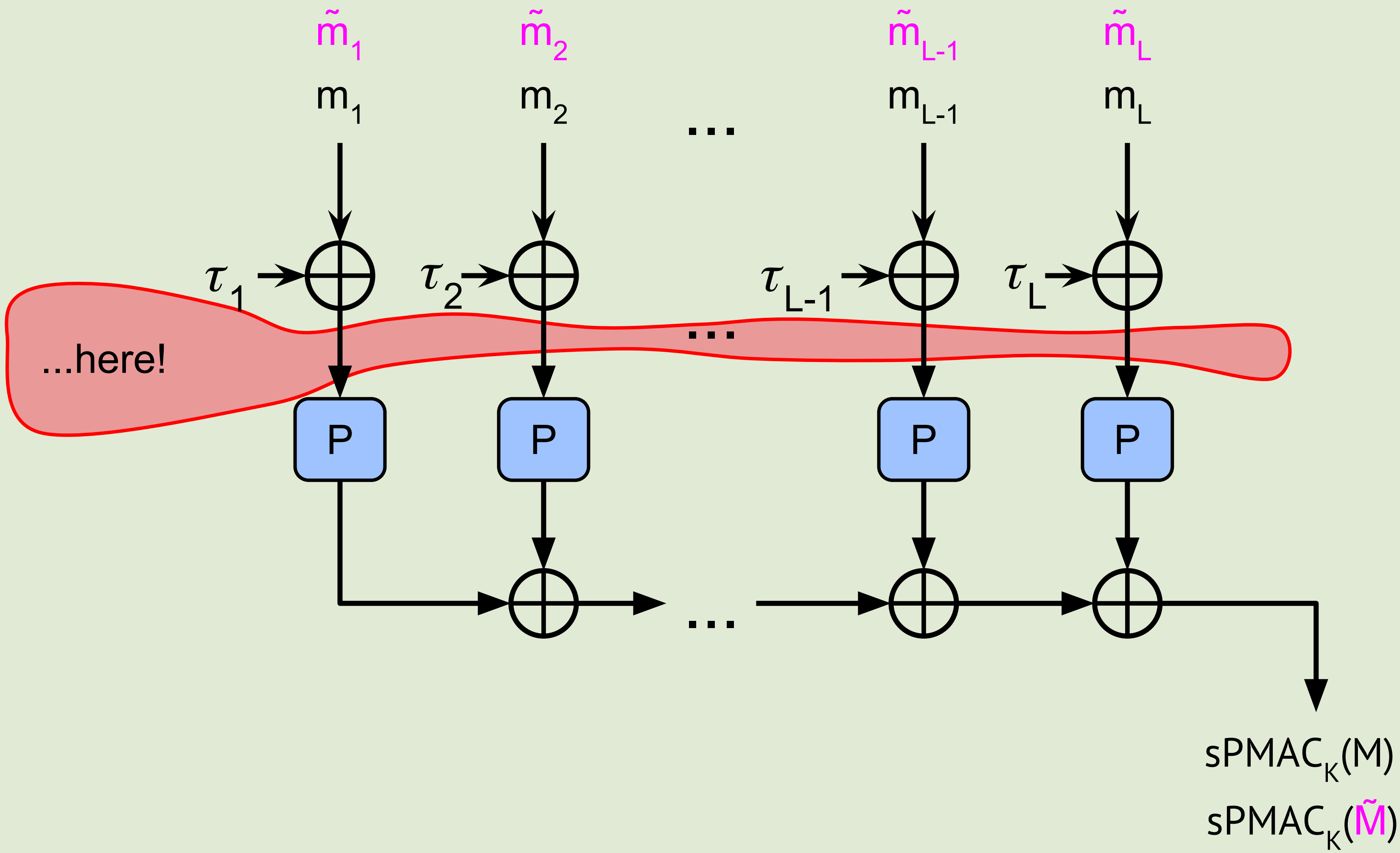
sPMAC - collisions

Collision happens here with very small probability 2^{-n+1}

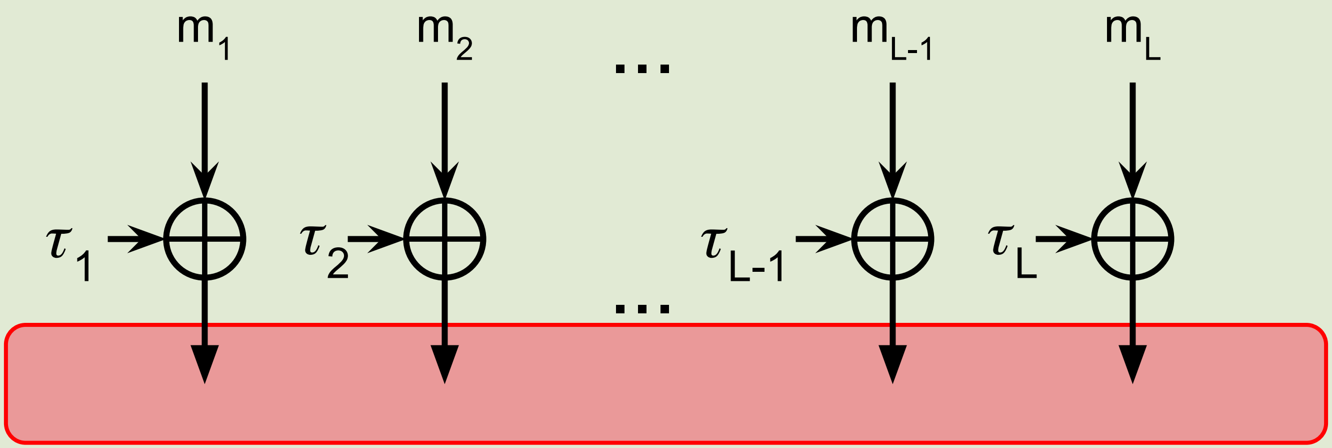


sPMAC - collisions

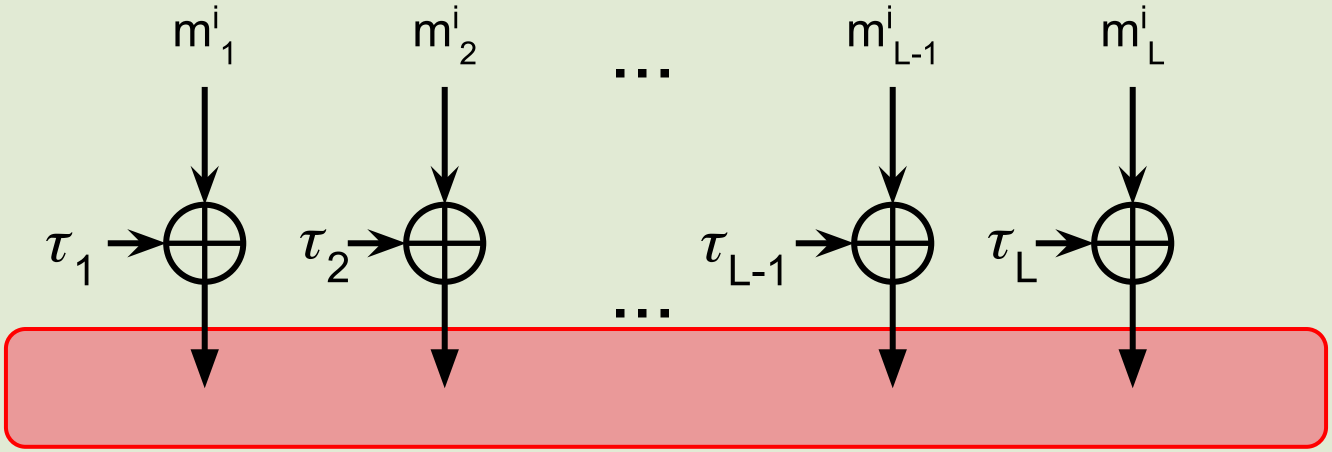
Our interest is ...



sPMAC target

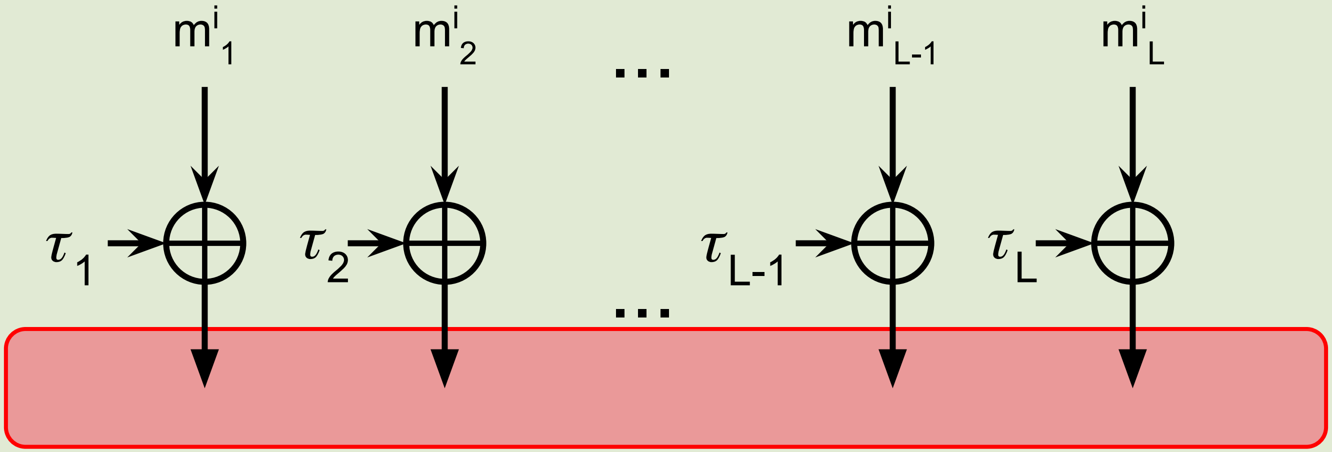


sPMAC target



- Assume q messages $M_i = (m^i_1, m^i_2, \ldots, m^i_L)$

sPMAC target



- Assume q messages $M_i = (m^i_1, m^i_2, \dots, m^i_L)$

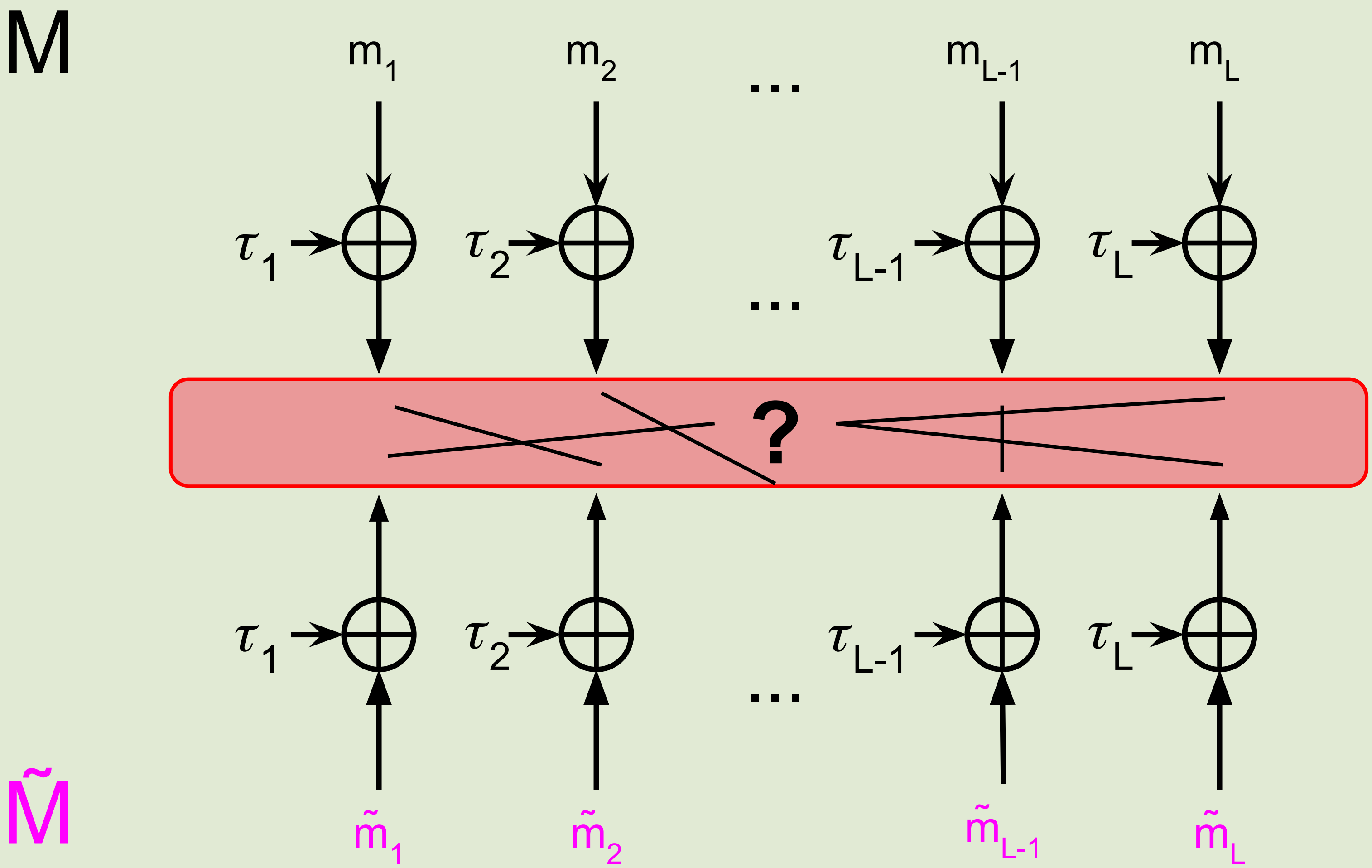
$$\max_{M_1,\dots,M_q} \Pr_{\tau_1,\dots,\tau_L}\left[\exists i < j \ : \ \left\{m^i_1 \oplus \tau_1, \dots, m^i_L \oplus \tau_L\right\} = \left\{m^j_1 \oplus \tau_1, \dots, m^j_L \oplus \tau_L\right\}\right]$$

Masks $\tau_1, \tau_2, \ldots$ in PMAC [BR'02]

$$\tau_i = \gamma_i \cdot \mathbf{R}$$

- **R uniformly random in $\{0,1\}^n$**
- $\gamma_1, \gamma_2, \gamma_3, \ldots$ are canonical **Gray code**
  - for any $k \leq n$, first 2^k elements form a group in $GF(2^n)$

sPMAC - 2 messages



$$\max_{M_1, M_2} \Pr_{\tau_1,\ldots,\tau_L} \left[\left\{ m_1 \oplus \tau_1, \ldots, m_L \oplus \tau_L \right\} = \left\{ \tilde{m}_1 \oplus \tau_1, \ldots, \tilde{m}_L \oplus \tau_L \right\} \right]$$

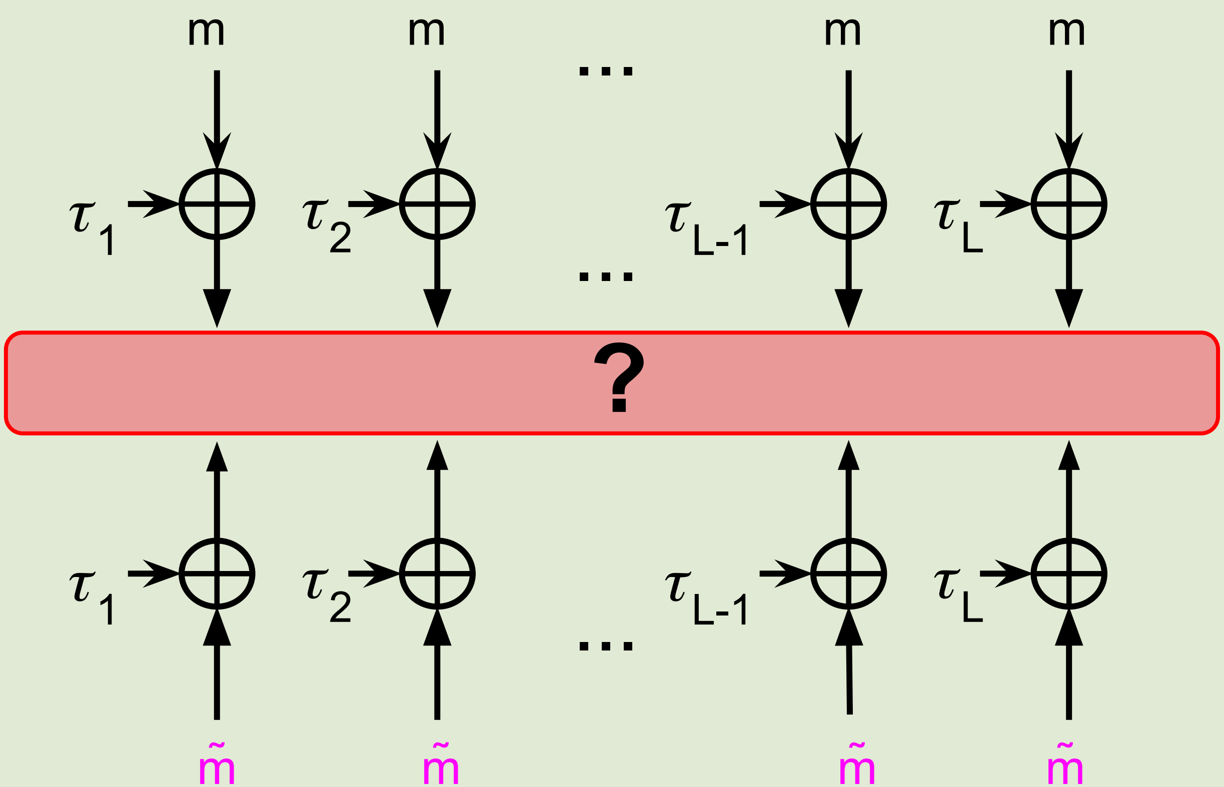
Outline

- Motivation
- PMAC
- Collisions and sPMAC

- Results
  - **New attack - exact upper bound on security of PMAC**
  - PMAC security bounds independent of query length L

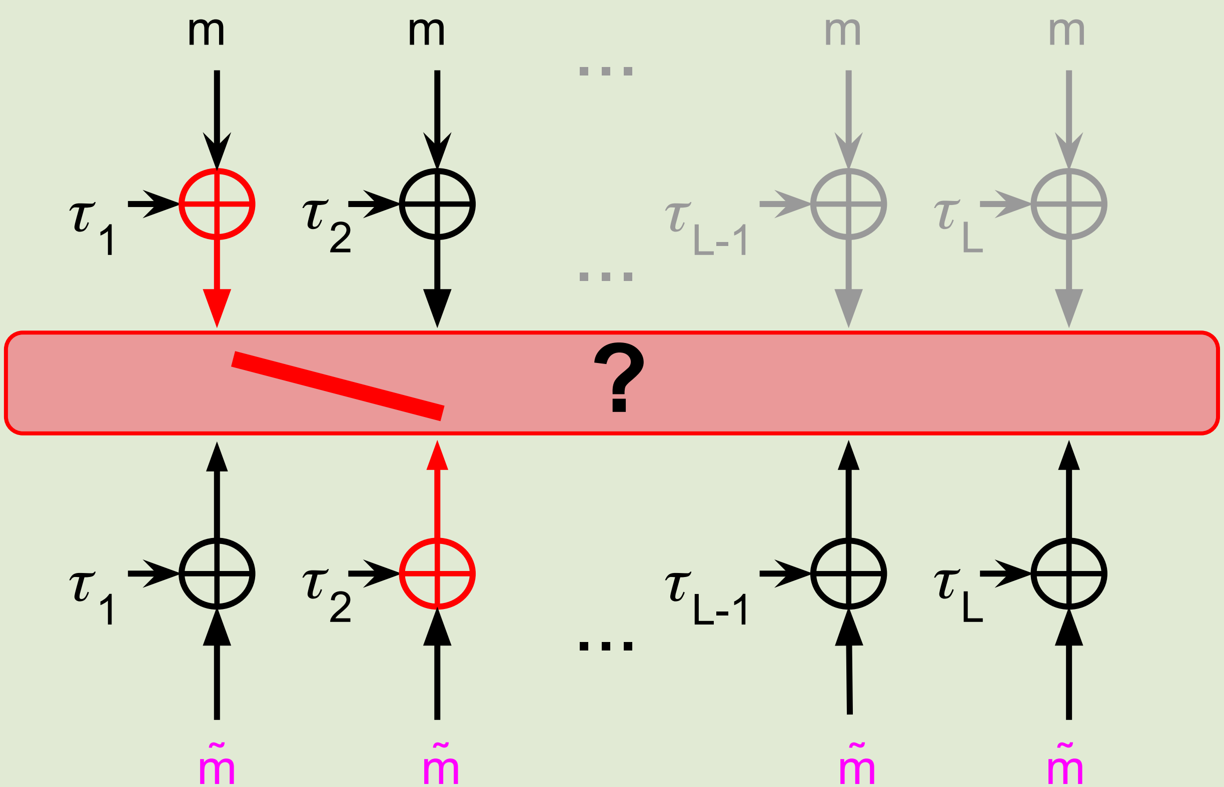
The Attack

- Pick random message blocks m, $\tilde{m}$
  - M = m || m || … || m
  - $\tilde{M}$ = $\tilde{m}$ || $\tilde{m}$ || … || $\tilde{m}$



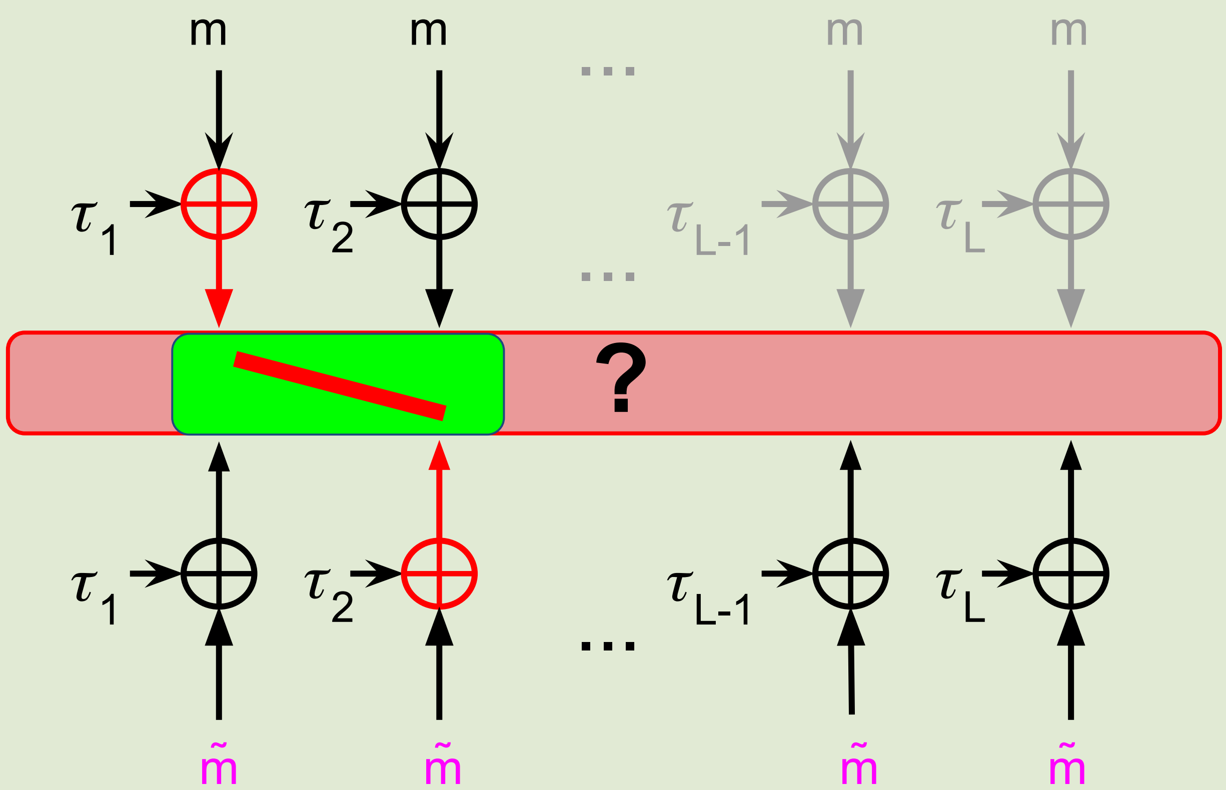
The Attack

- $\Pr[m \oplus \tau_1 = \tilde{m} \oplus \tau_2] = ?$



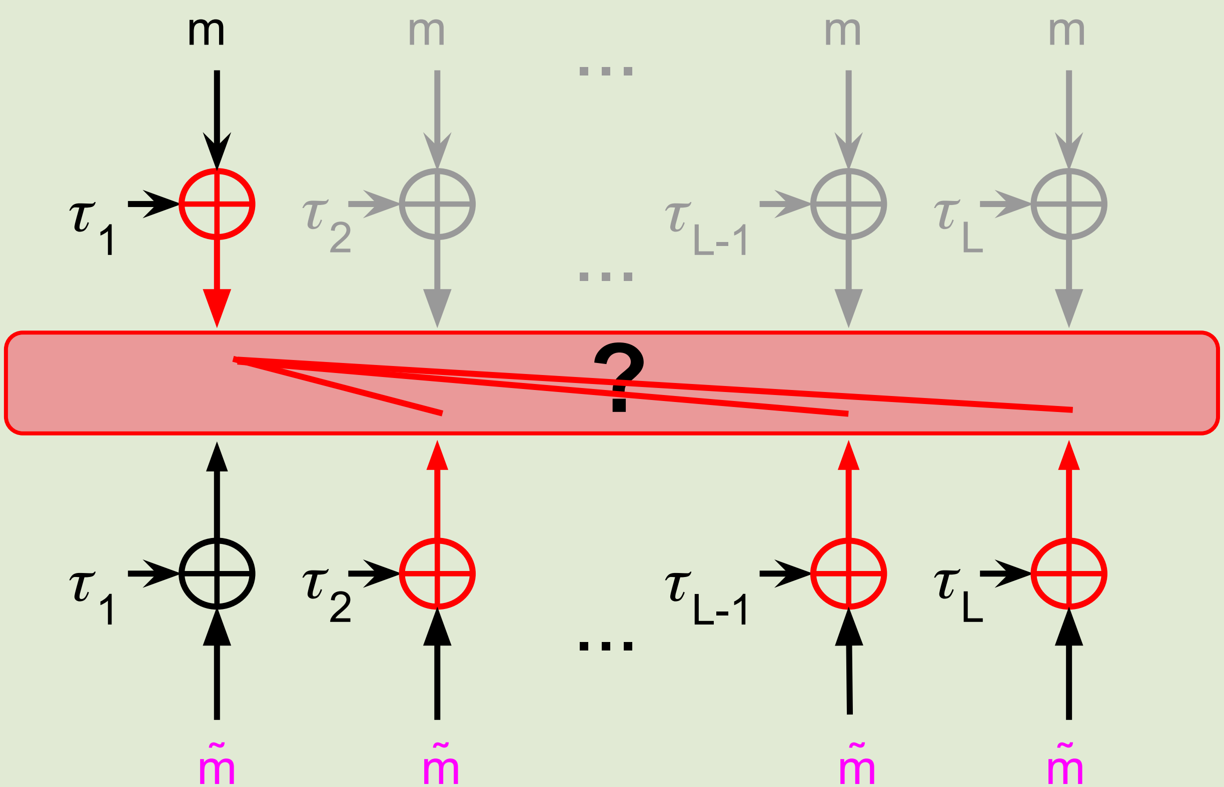
The Attack

- $R = (\tilde{m} \oplus m) / (\gamma_1 \oplus \gamma_2)$
- $\Pr[m \oplus \tau_1 = \tilde{m} \oplus \tau_2] = 1/2^n$



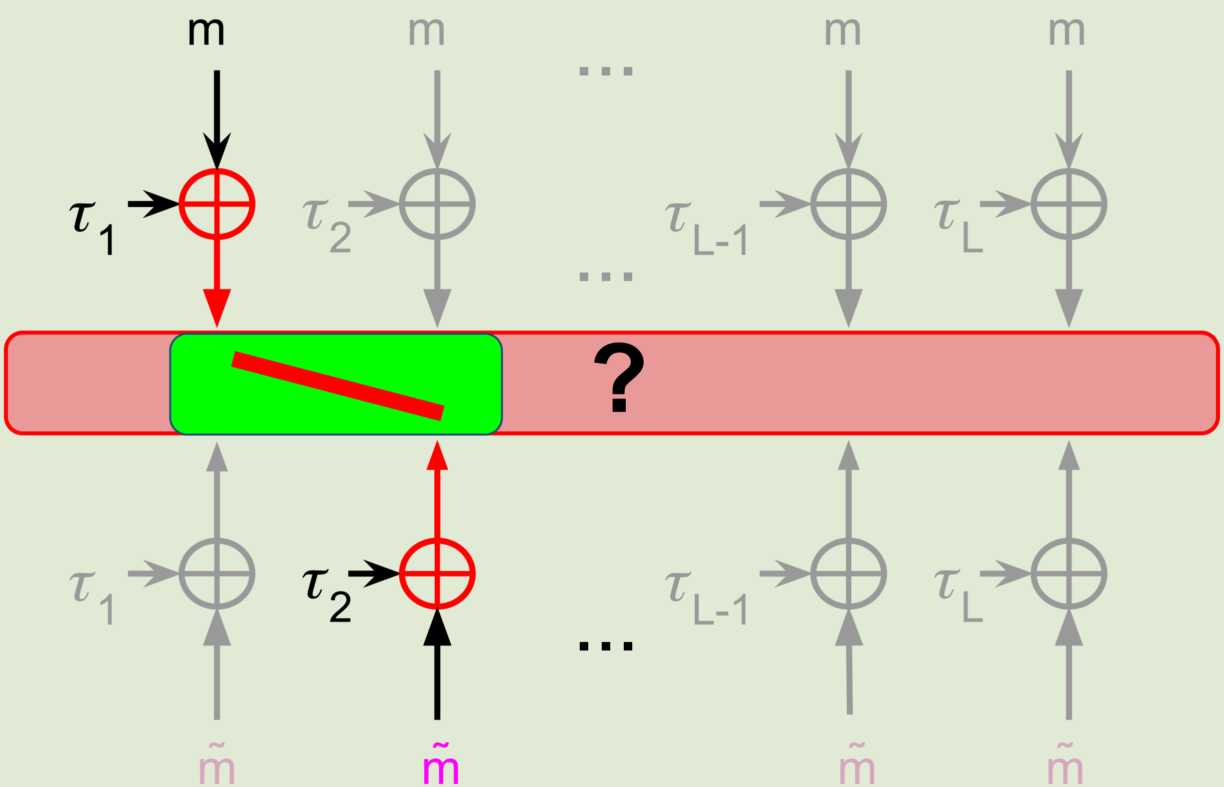
The Attack

$$\Pr[\exists\ i: m \oplus \tau_1 = \tilde{m} \oplus \tau_i] = L\text{-}1 / 2^n$$



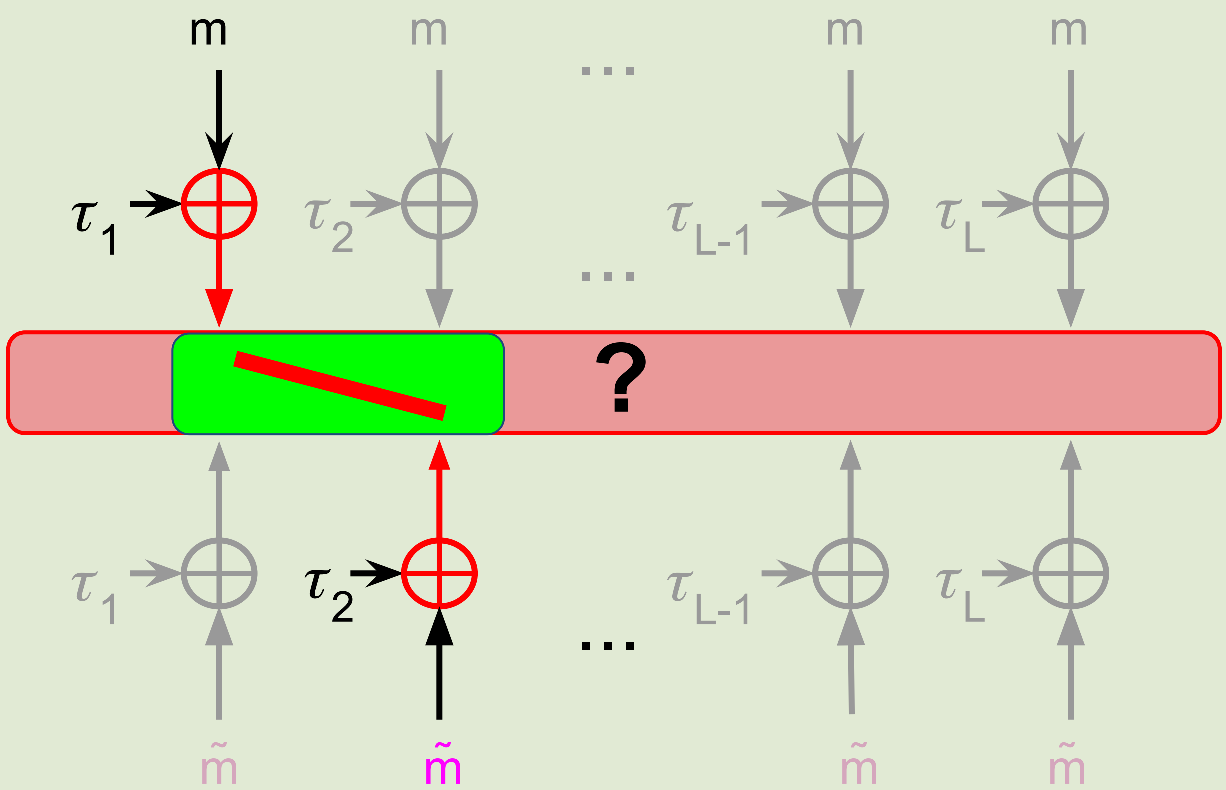
The Attack

- Have a single pairing

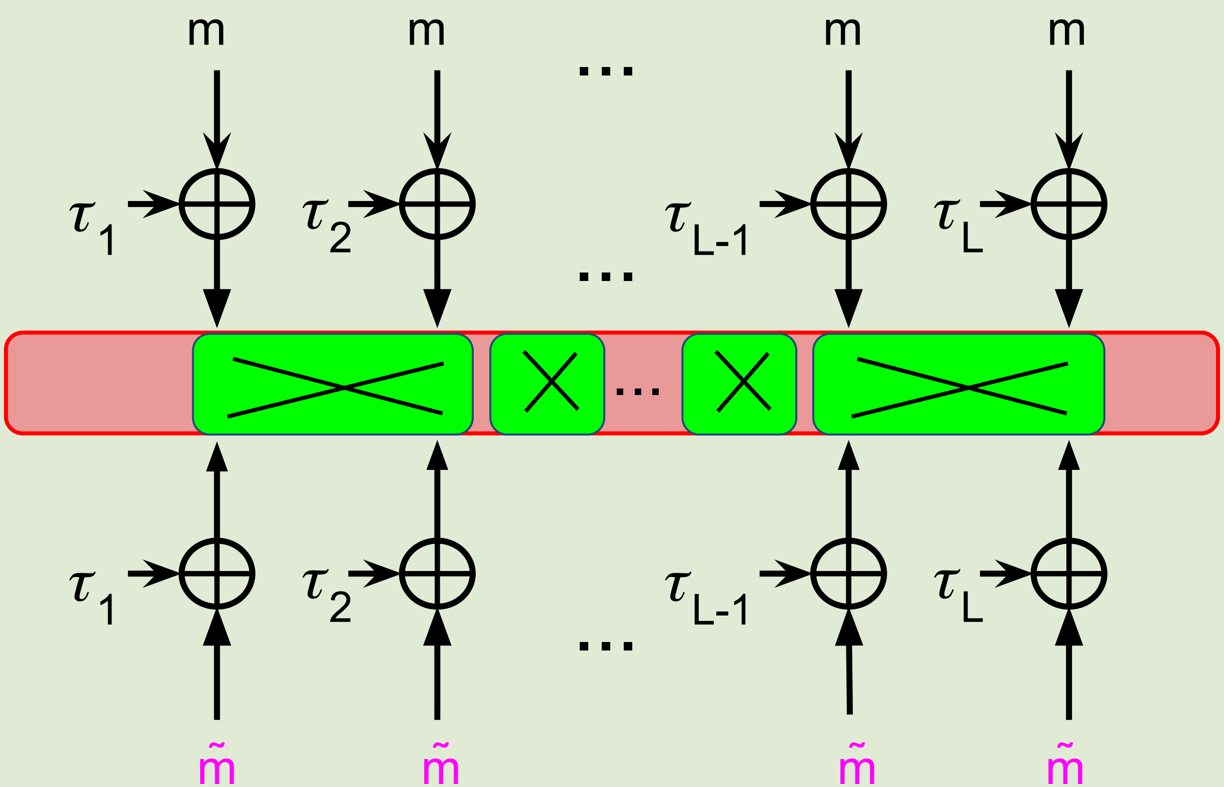


The Attack

- We need to match everything, not just one block
- $\gamma_1, \gamma_2, \ldots, \gamma_{L-1}, \gamma_L$ are a **group** (remember $\tau_i = \gamma_i \cdot R$)

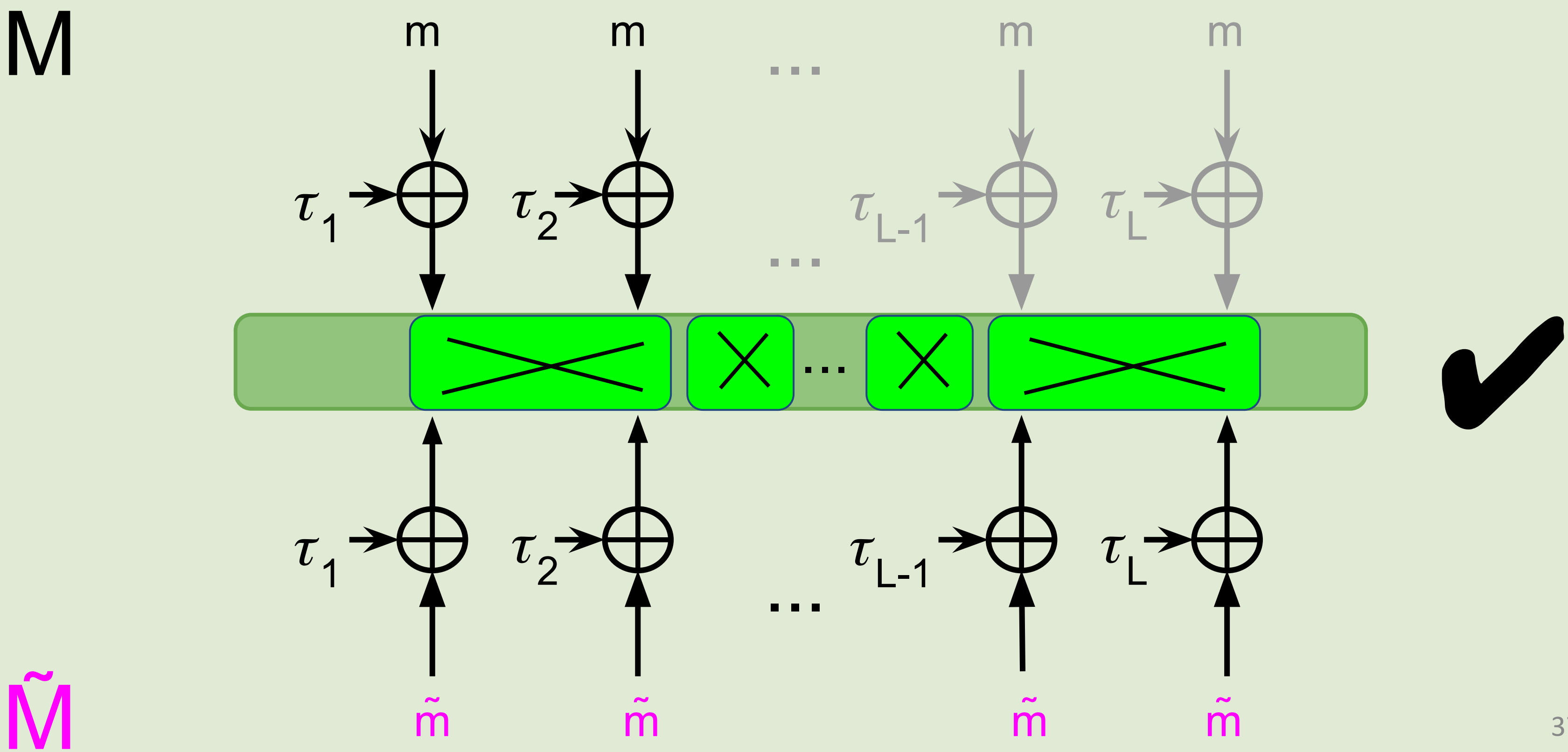


The Attack magic



The Attack

- **Collision on the output of sPMAC for M and $\tilde{M}$**
  - works for L-1 different values of R
    - hence with probability $L-1 / 2^n$



Moving from 2 to q messages

$$\max_{M_1,M_2} \Pr_{\tau_1,\ldots,\tau_L} \left[\left\{ m_1 \oplus \tau_1, \ldots, m_L \oplus \tau_L \right\} = \left\{ \tilde{m}_1 \oplus \tau_1, \ldots, \tilde{m}_L \oplus \tau_L \right\} \right]$$

- ≈ $L/2^n$ advantage

Moving from 2 to q messages

$$\max_{M_1,M_2}\ \Pr_{\tau_1,\ldots,\tau_L}\left[\left\{m_1 \oplus \tau_1,\ldots,m_L \oplus \tau_L\right\} = \left\{\tilde{m}_1 \oplus \tau_1,\ldots,\tilde{m}_L \oplus \tau_L\right\}\right]$$

- ≈ $L/2^n$ advantage

$$\max_{M_1,\ldots,M_q}\ \Pr_{\tau_1,\ldots,\tau_L}\left[\exists i < j\ :\ \left\{m_1^i \oplus \tau_1,\ldots,m_L^i \oplus \tau_L\right\} = \left\{m_1^j \oplus \tau_1,\ldots,m_L^j \oplus \tau_L\right\}\right]$$

- Random $m^1,\ldots, m^q$; $M_i = m^i||\ldots||m^i$
- Use union bound
  - $q^2 \cdot L / 2^n$ advantage

But…

- [BR'02] omit $\gamma^n_0 = 0^n$
  - $\gamma_1, \gamma_2, \dots, \gamma_{L-1}, \gamma_L$ **NOT a group in GF(2^n)**
  - attack breaks

But…

- [BR'02] omit $\gamma^n{}_0 = 0^n$
  - $\gamma_1, \gamma_2, \ldots, \gamma_{L-1}, \gamma_L$ **NOT a group in GF(2^n)**
  - attack breaks

- $\gamma_1, \gamma_2, \ldots, \gamma_{L-1}, \gamma_L$ contains a **coset** of size L/2
  - sufficient for attack

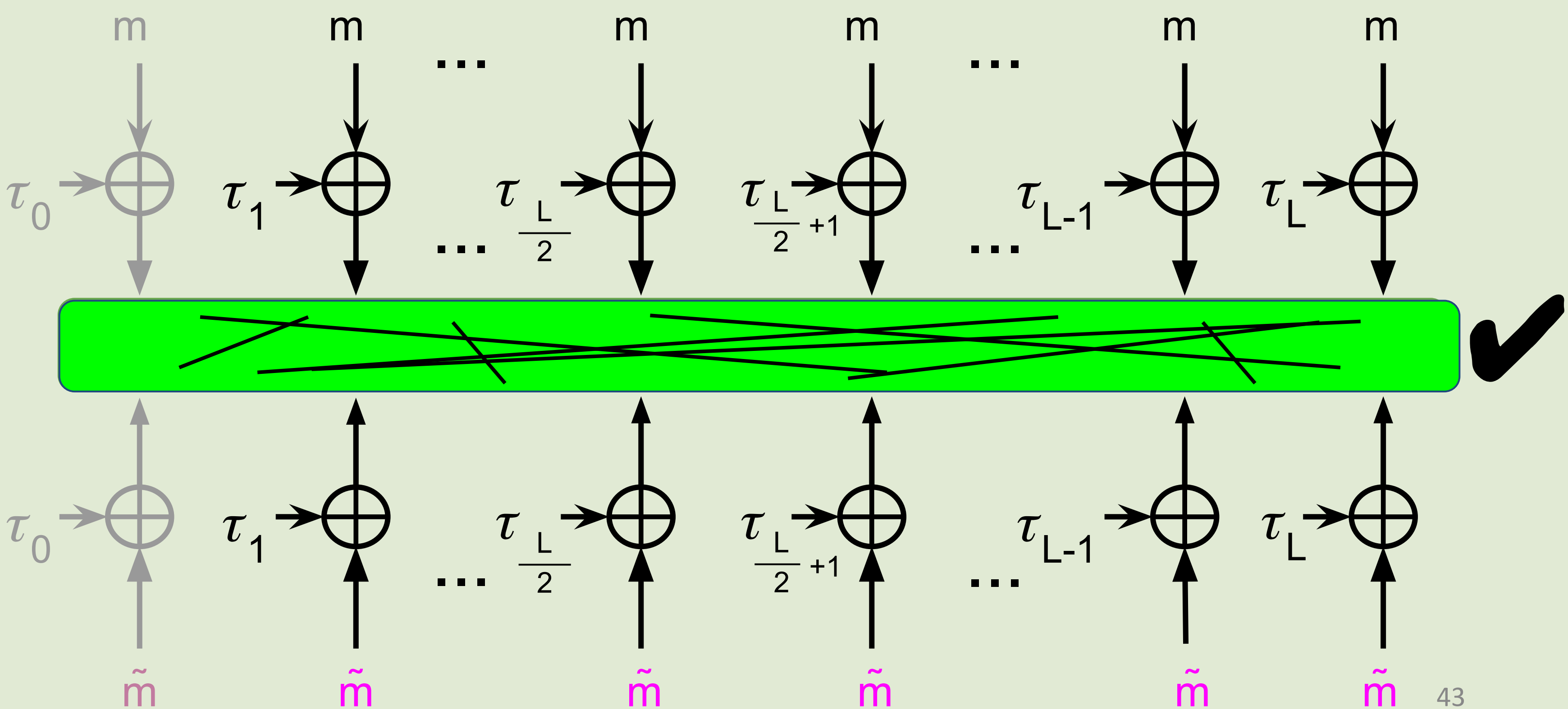
But…

- [BR'02] omit $\gamma^n_0 = 0^n$
  - $\gamma_1, \gamma_2, \ldots, \gamma_{L-1}, \gamma_L$ **NOT a group in GF(2^n)**
  - attack breaks

- $\gamma_1, \gamma_2, \ldots, \gamma_{L-1}, \gamma_L$ contains a **coset** of size L/2
  - sufficient for attack (losing factor 2 in advantage)

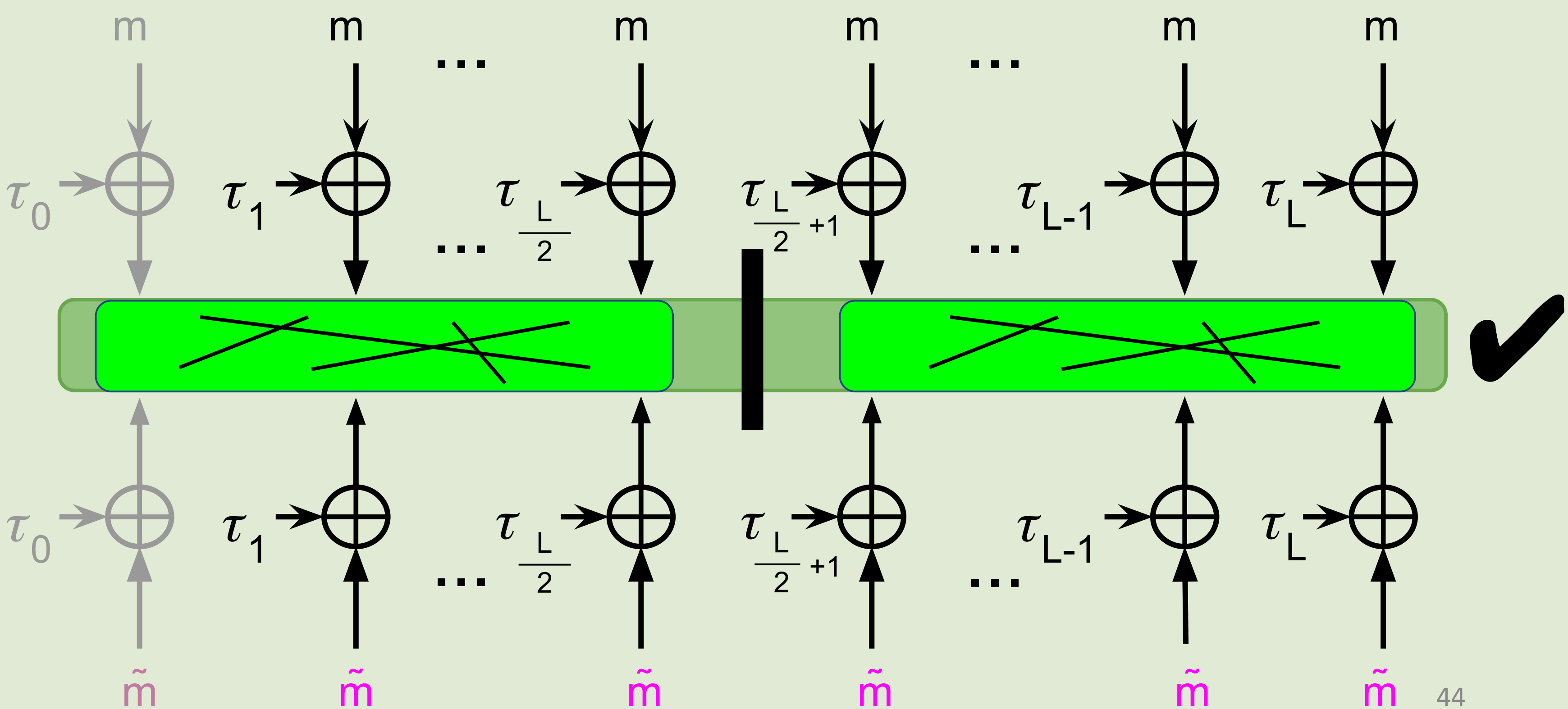
Why is a coset sufficient?

- Assume we do not remove γ^n_0



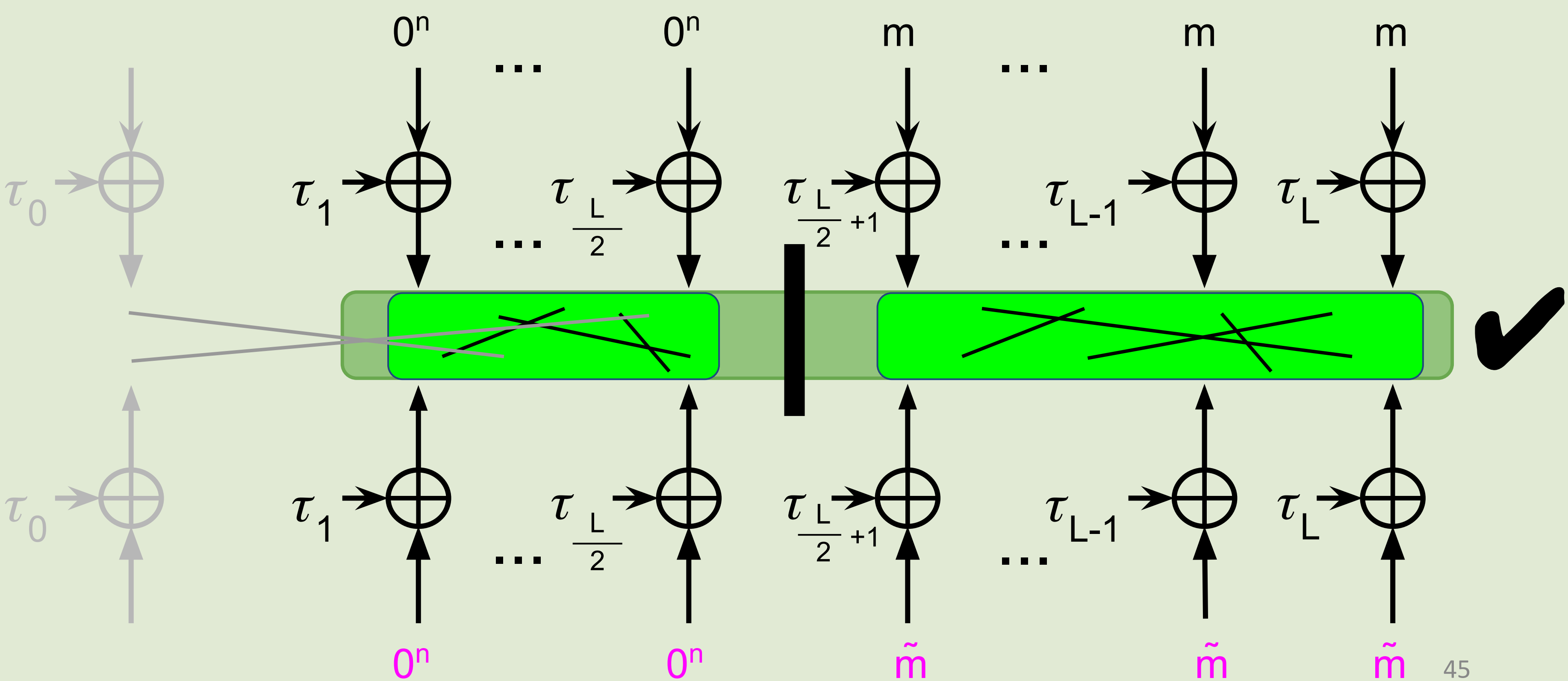
Why is a coset sufficient?

- Assume we do not remove γ^n_0
  - For (L-1) / 2 values of R, we have this picture



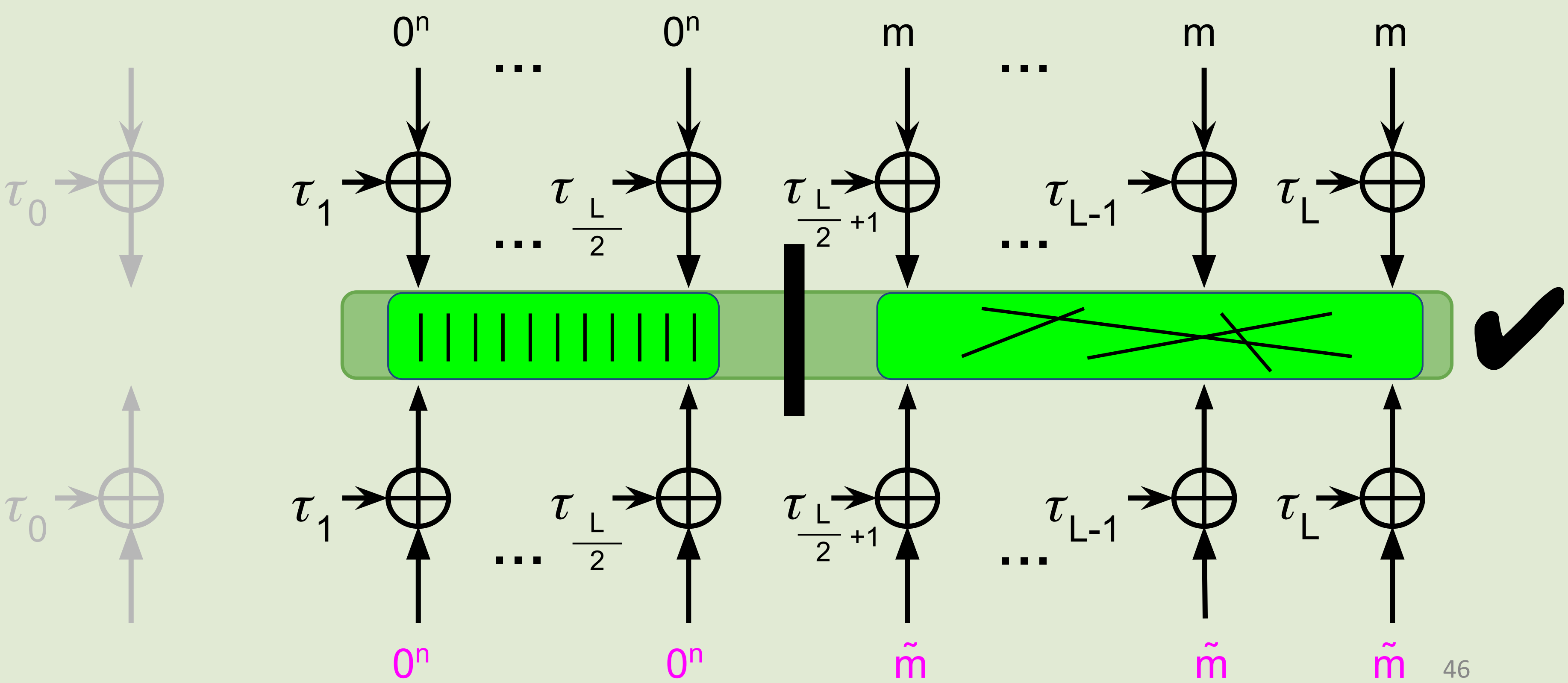
Why is a coset sufficient?

- Modify messages
  - change first L/2 blocks to 0^n



Why is a coset sufficient?

- Modify messages
  - change first L/2 blocks to 0^n
- For (L-1) / 2 values of R, we have this picture



Outline

- Motivation
- PMAC
- Collisions and sPMAC

- Results
  - New attack - exact upper bound on security of PMAC
  - **PMAC security bounds independent of query length L**

Exploring different mask options

- Recall masks $\tau_1, \tau_2, \ldots, \tau_{L-1}, \tau_L$
  - $\tau_i = \gamma_i \cdot R$
  - until now γ_i was a Gray code
    - 1-wise independent distribution
- We look at at $\tau_1, \tau_2, \ldots, \tau_{L-1}, \tau_L$ that are:
  - randomly distributed
  - 4-wise independent
  - 2-wise independent

2-wise independent masks

- Masks of [BR'02] are 1-wise independent
  - $\tau_i = \boldsymbol{\gamma}_i \cdot R$

2-wise independent masks

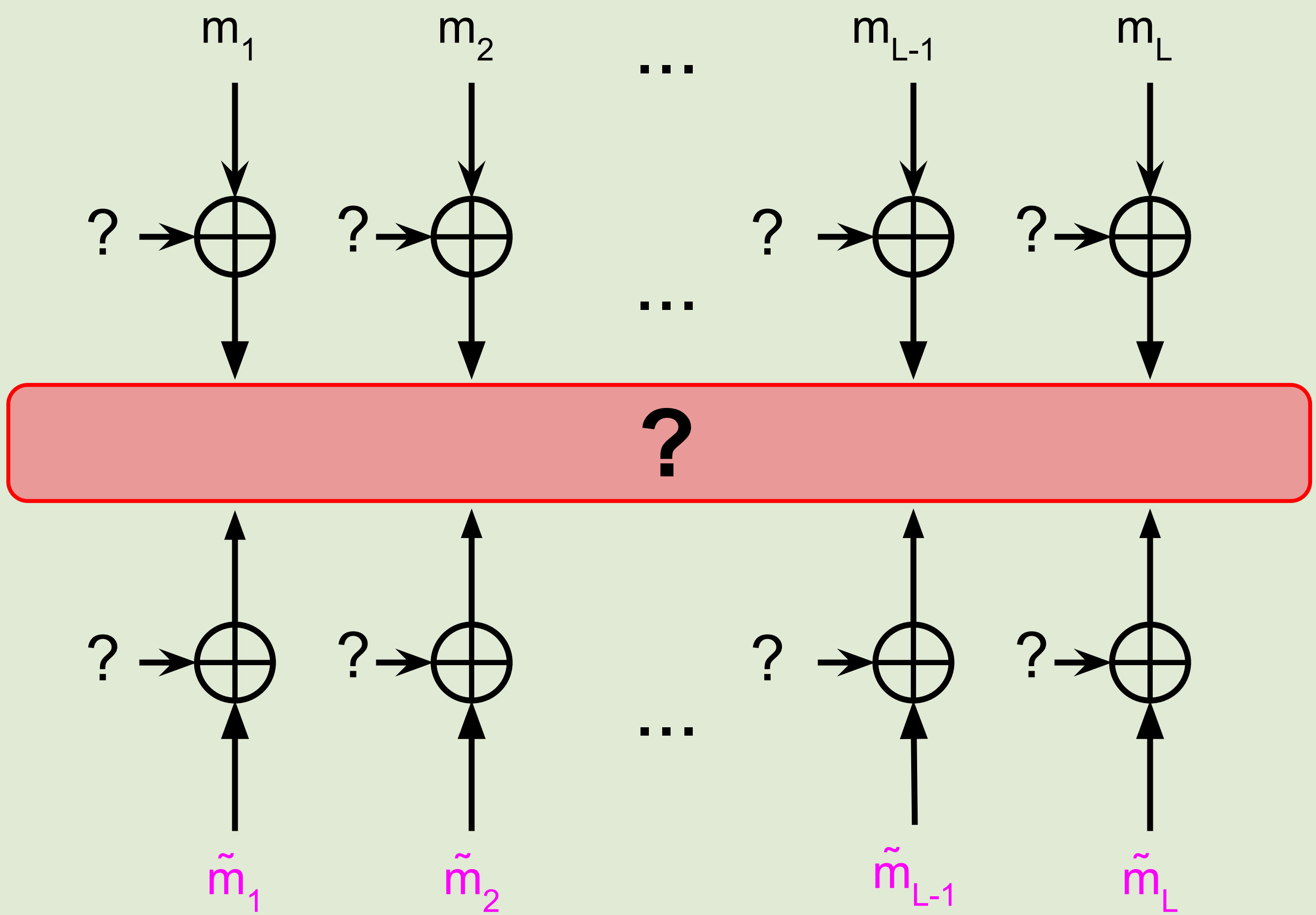
- Masks of [BR'02] are 1-wise independent
  - $\tau_i = \boldsymbol{\gamma}_i \cdot R$
- Make it 2-wise independent
  - $\tau_i = \boldsymbol{\gamma}_i \cdot R \oplus \tilde{R}$

2-wise independent masks

- Masks of [BR'02] are 1-wise independent
  - $\tau_i = \gamma_i \cdot R$
    - $m_x \oplus \tau_x = m_y \oplus \tau_y$
- Make it 2-wise independent
  - $\tau_i = \gamma_i \cdot R \oplus \tilde{R}$
    - $m_x \oplus \tau_x \oplus \tilde{R} = m_y \oplus \tau_y \oplus \tilde{R}$
- 2-wise independent distribution **does improve security**

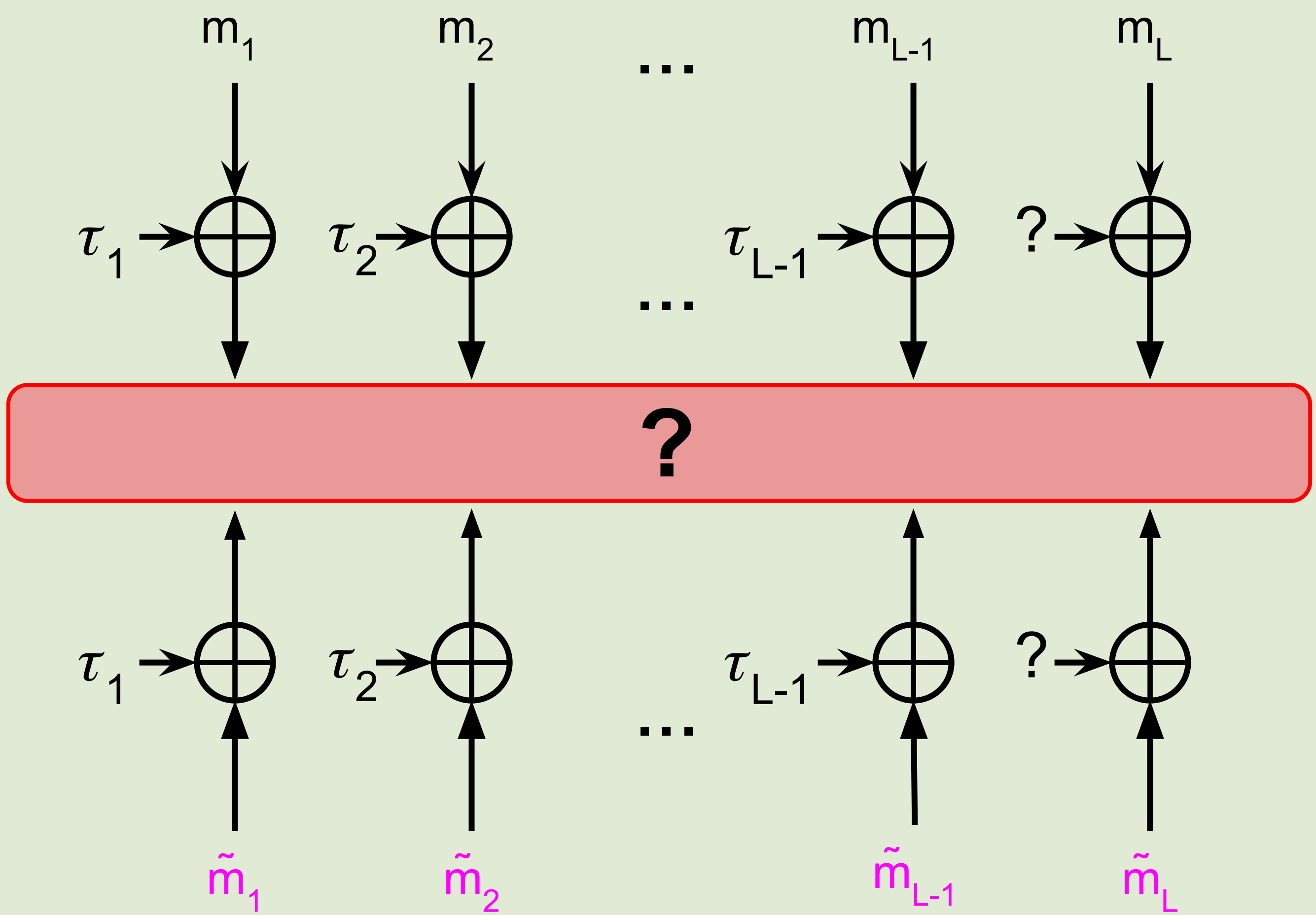
Randomly distributed masks

- Let $\tau_1, \tau_2, \ldots, \tau_{L-1}, \tau_L$ be uniform and independent



Randomly distributed masks

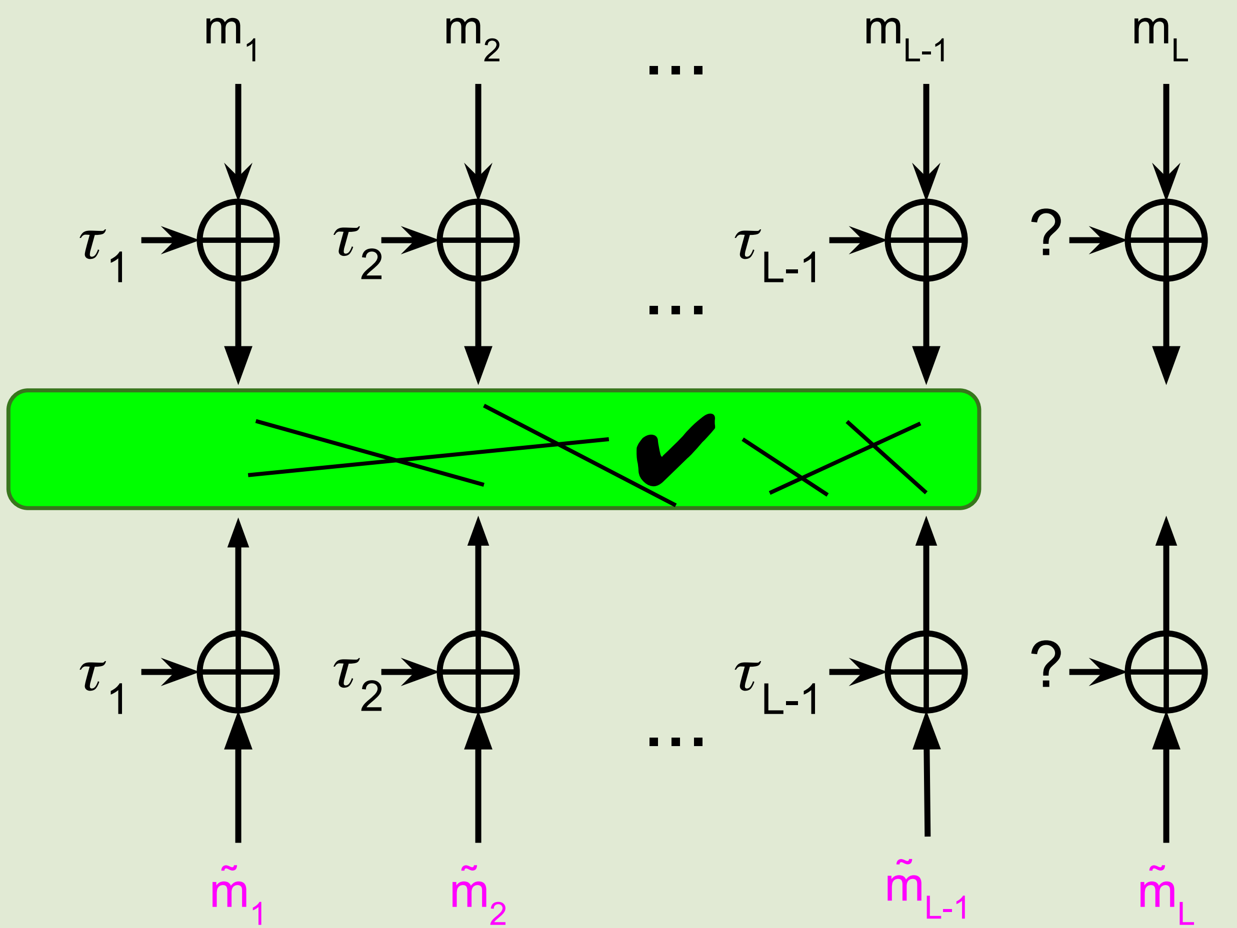
- Let $\tau_1, \tau_2, \ldots, \tau_{L-1}, \tau_L$ be uniform and independent
- Assume all values of τ_i are chosen, but τ_L



Randomly distributed masks

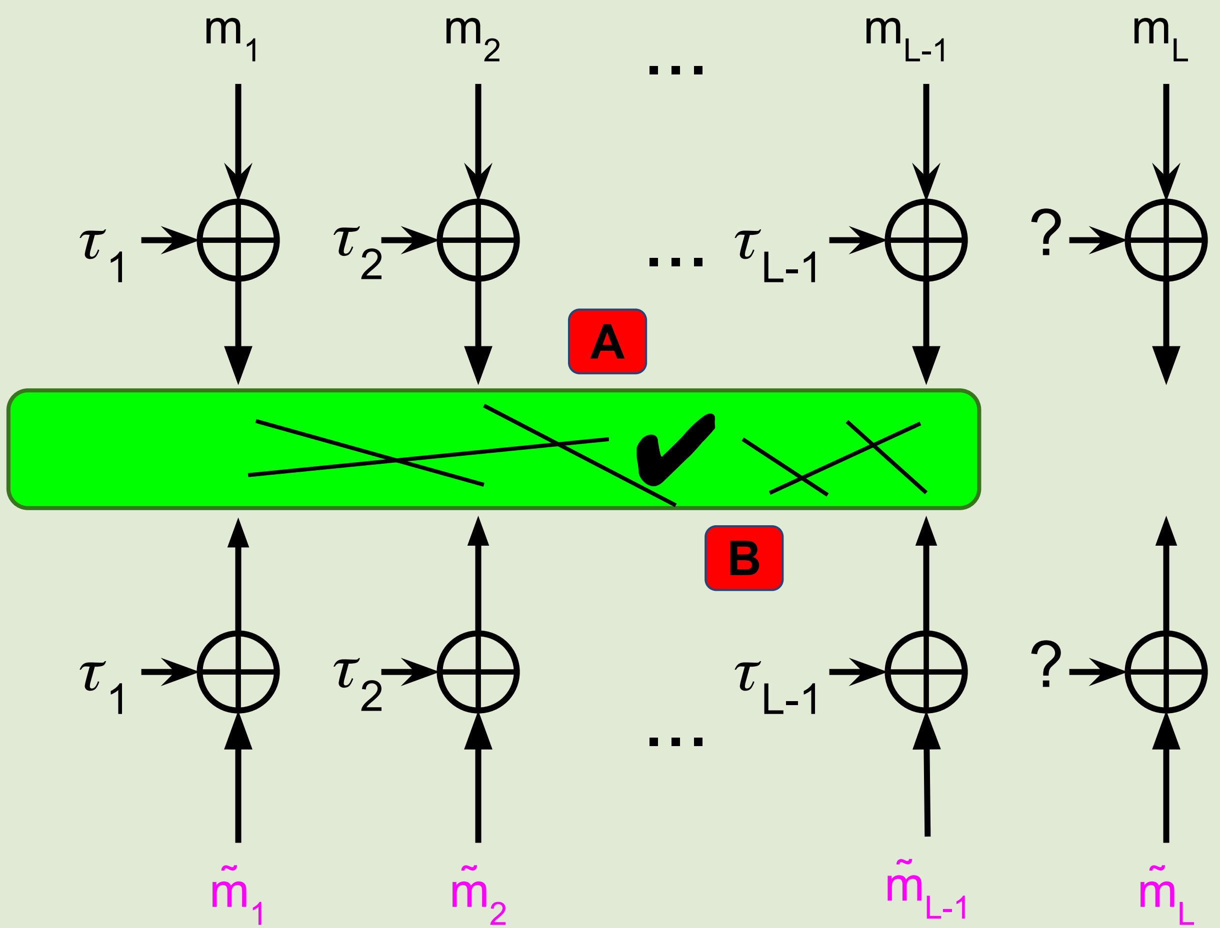
- Assume that all available values are paired-up with probability

  1 ("for free")



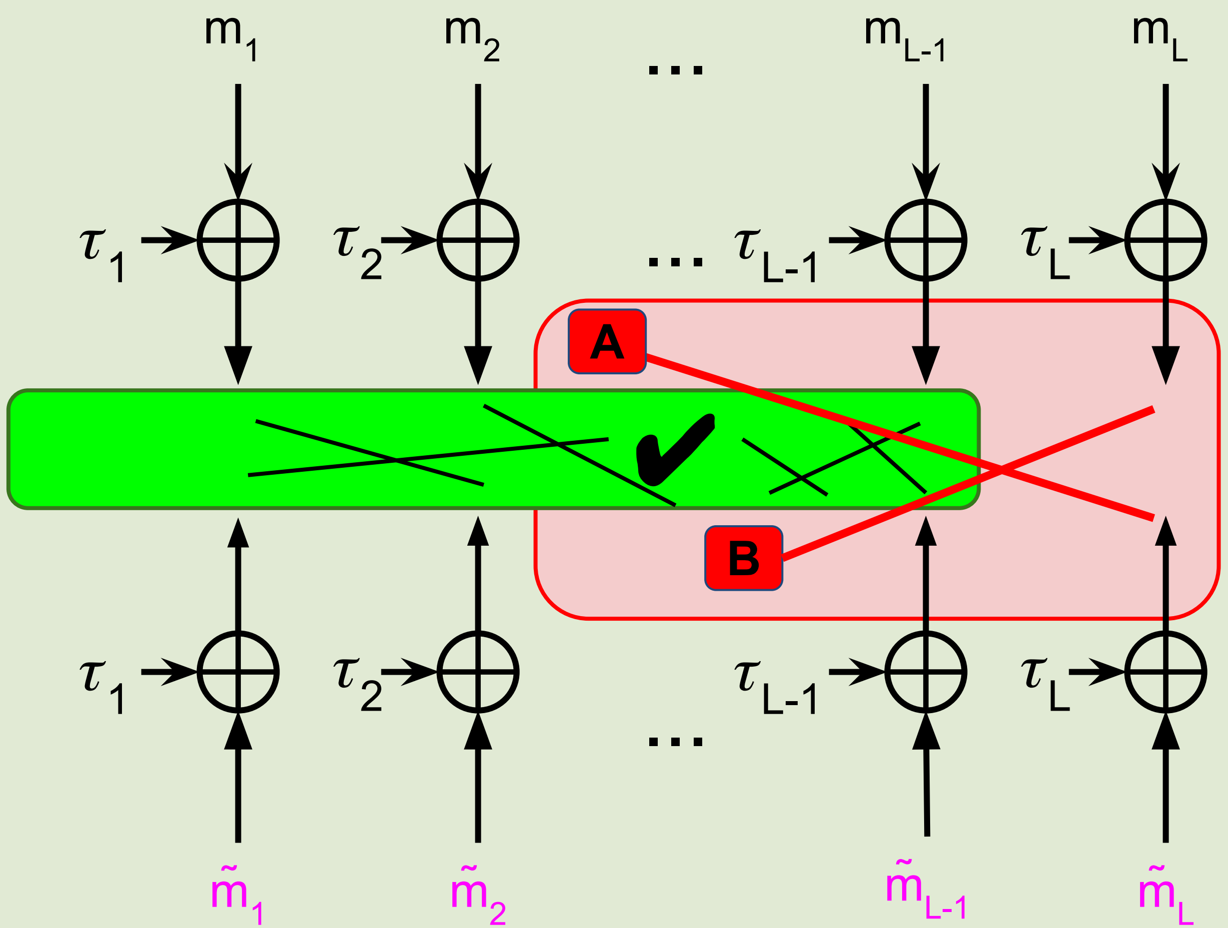
Randomly distributed masks

- For an output collision, there must be 2 values {A,B} left unpaired (otherwise, a collision will happen with probability 0)



Randomly distributed masks

- The probability that the value τ_L will be sampled such that a pairing does happen **is at most $2/2^n$**, hence **$q^2 / 2^n$ bound**



4-wise independent masks

- Argument is in a way similar to random masks
  - look at 2 pairings, 4 masked values
  - same bound $4 / 2^n$
  - BUT condition $L \leq 2^{n/2}$
- Full proof in the paper

Summary

- Security of PMAC using Gray codes is $\Theta(q^2 \cdot L / 2^n)$
- Open question: Exact security of PMAC1

Summary

- Security of PMAC using Gray codes is $\Theta(q^2 \cdot L / 2^n)$
- Open question: Exact security of PMAC1

- Using any 4-wise independent masks gives security $\Theta(q^2 / 2^n)$
- There is 2-wise distribution of mask with $q^2 \cdot L/2^n$ security
- Open question: is 3-wise independence enough for $q^2/2^n$ security?

Summary

- Security of PMAC using Gray codes is $\Theta(q^2 \cdot L / 2^n)$
- Open question: Exact security of PMAC1

- Using any 4-wise independent masks gives security $\Theta(q^2 / 2^n)$
- There is 2-wise distribution of mask with $q^2 \cdot L/2^n$ security
- Open question: is 3-wise independence enough for $q^2/2^n$ security?

Thank you!

http://eprint.iacr.org/2017/069