On the Influence of Message Length in PMAC's Security Bounds

Atul Luykx[1] Bart Preneel[1] Alan Szepieniec[1] Kan Yasuda[2]

[1]COSIC, KU Leuven, Belgium

[2]NTT Secure Platform Laboratories, Japan

May 11, 2016

Security Bounds

Factors:

1. Adversarial Resources

Security Bounds

Factors:

1. Adversarial Resources
2. Scheme parameters

Security Bounds

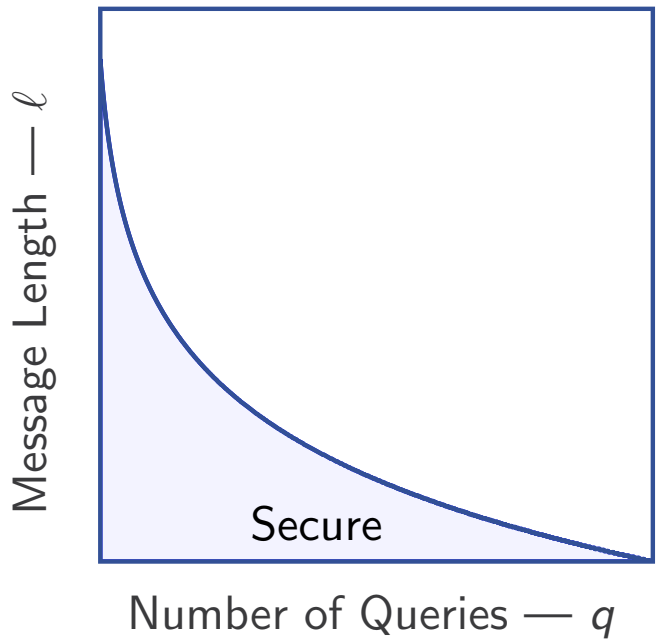
Factors:

1. Adversarial Resources
2. Scheme parameters
3. Confidence level

Security Bounds

Factors:

1. Adversarial Resources
2. Scheme parameters
3. Confidence level



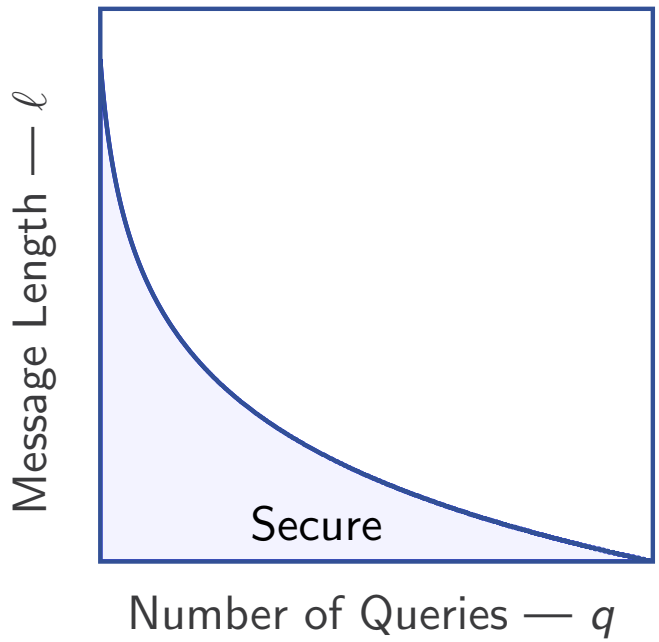
Security Bounds

Factors:

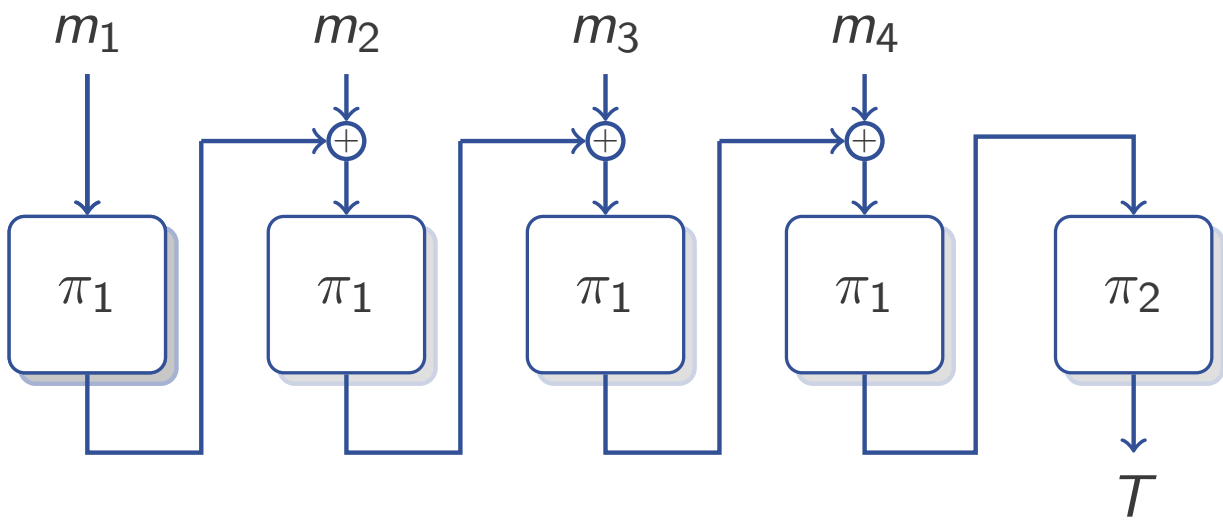
1. Adversarial Resources
2. Scheme parameters
3. Confidence level

TLS 1.3: GCM, ChaCha20 + Poly1305

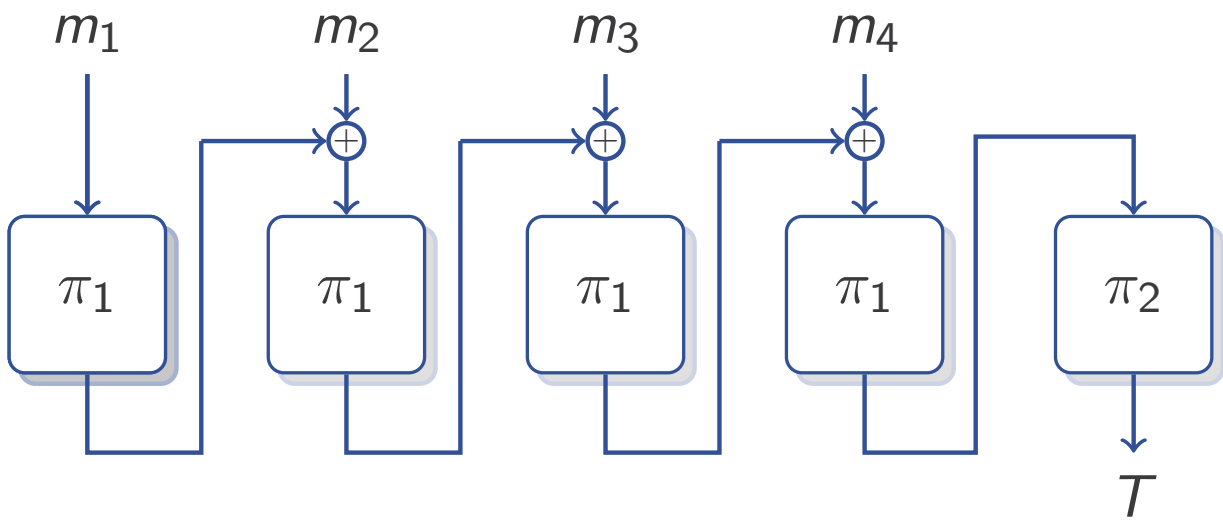
ISO/IEC SC27 WG2: 48 bit block size?



Example : EMAC



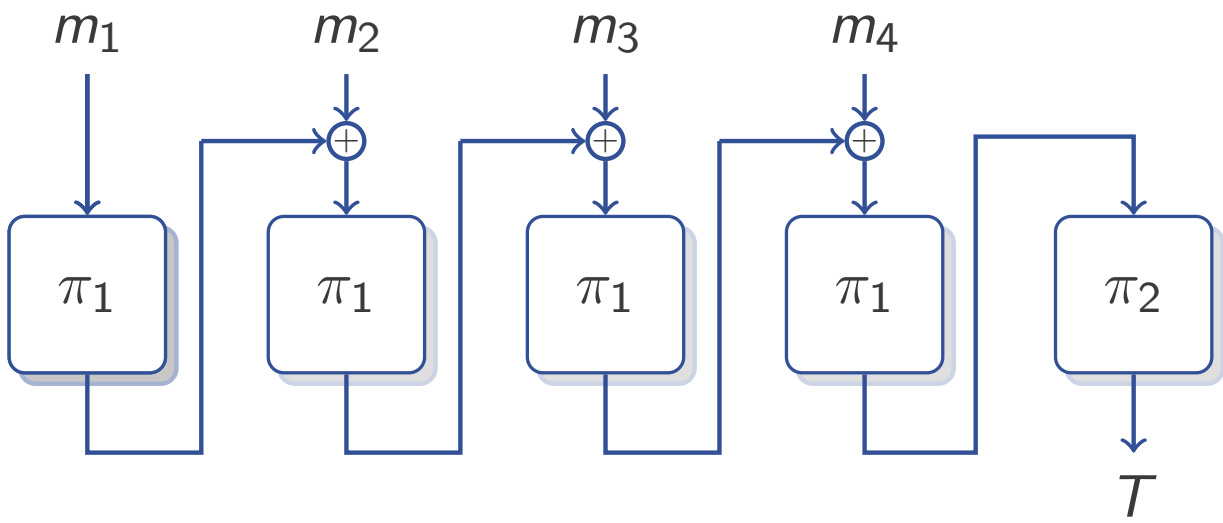
Example : EMAC



$$\frac{q^2\ell^2}{2^n} \leq \epsilon$$

- n Block size
- q Number of queries
- ℓ Query length in blocks
- ϵ Confidence

Example : EMAC



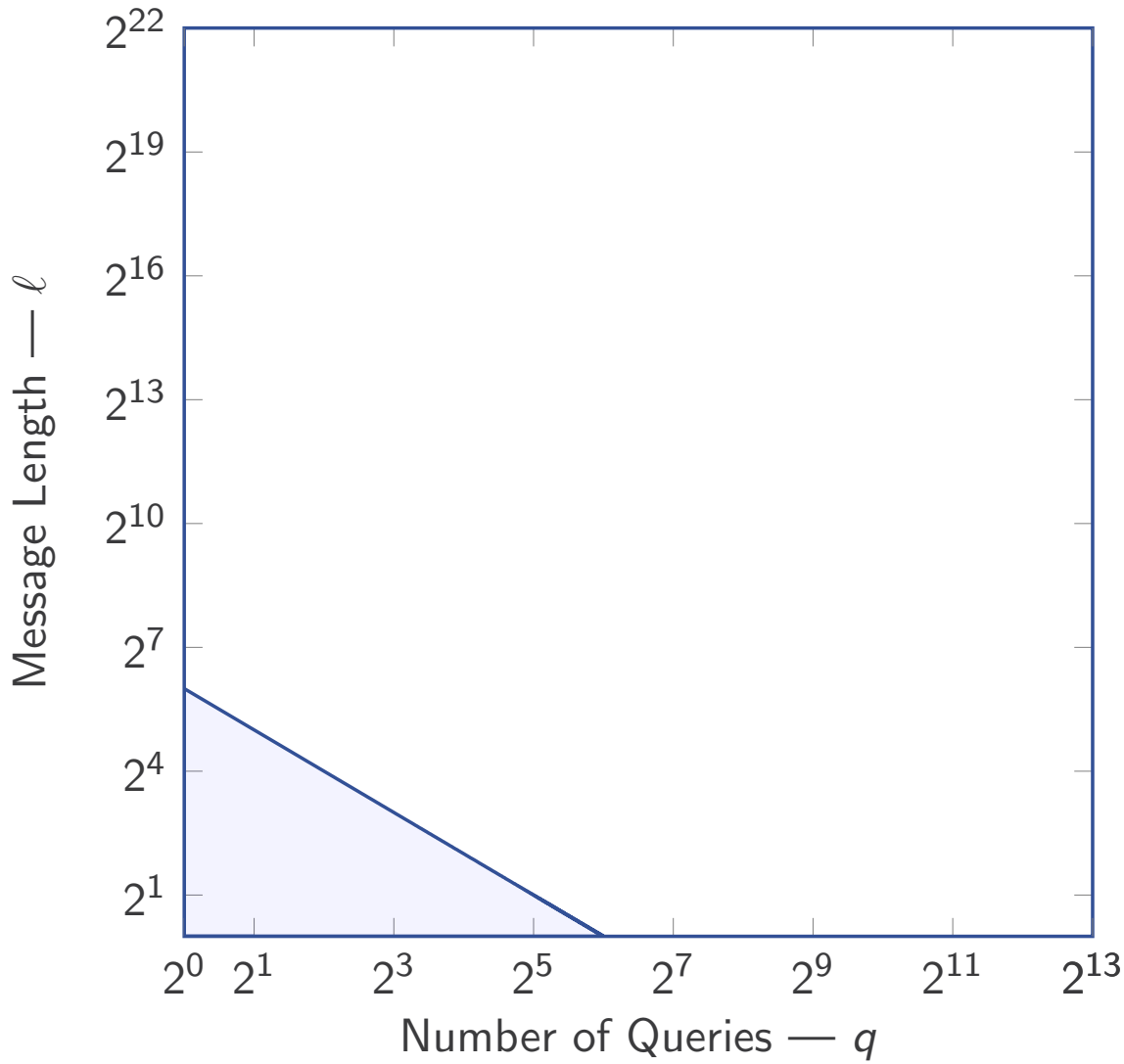
$$\frac{q^2\ell^2}{2^n} \leq \epsilon$$

- n Block size
- q Number of queries
- ℓ Query length in blocks
- ϵ Confidence

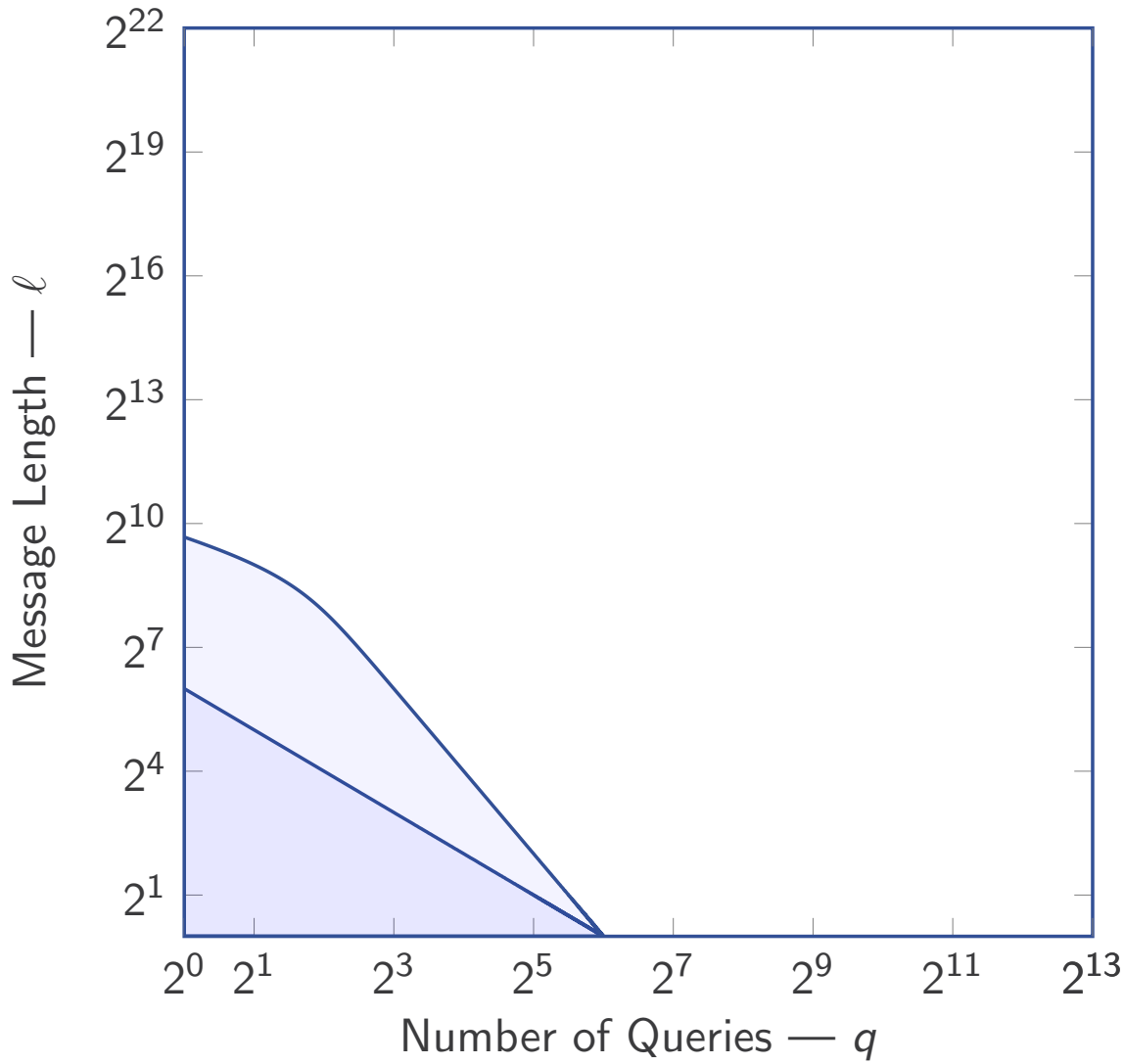
Table: $\epsilon = 1/2^{20}$, $\ell = 1\text{KB}$

Cipher	Block Size	Limit
AES128	128	2^{51}
PRESENT	64	$2^{18.5}$
KATAN32	32	4

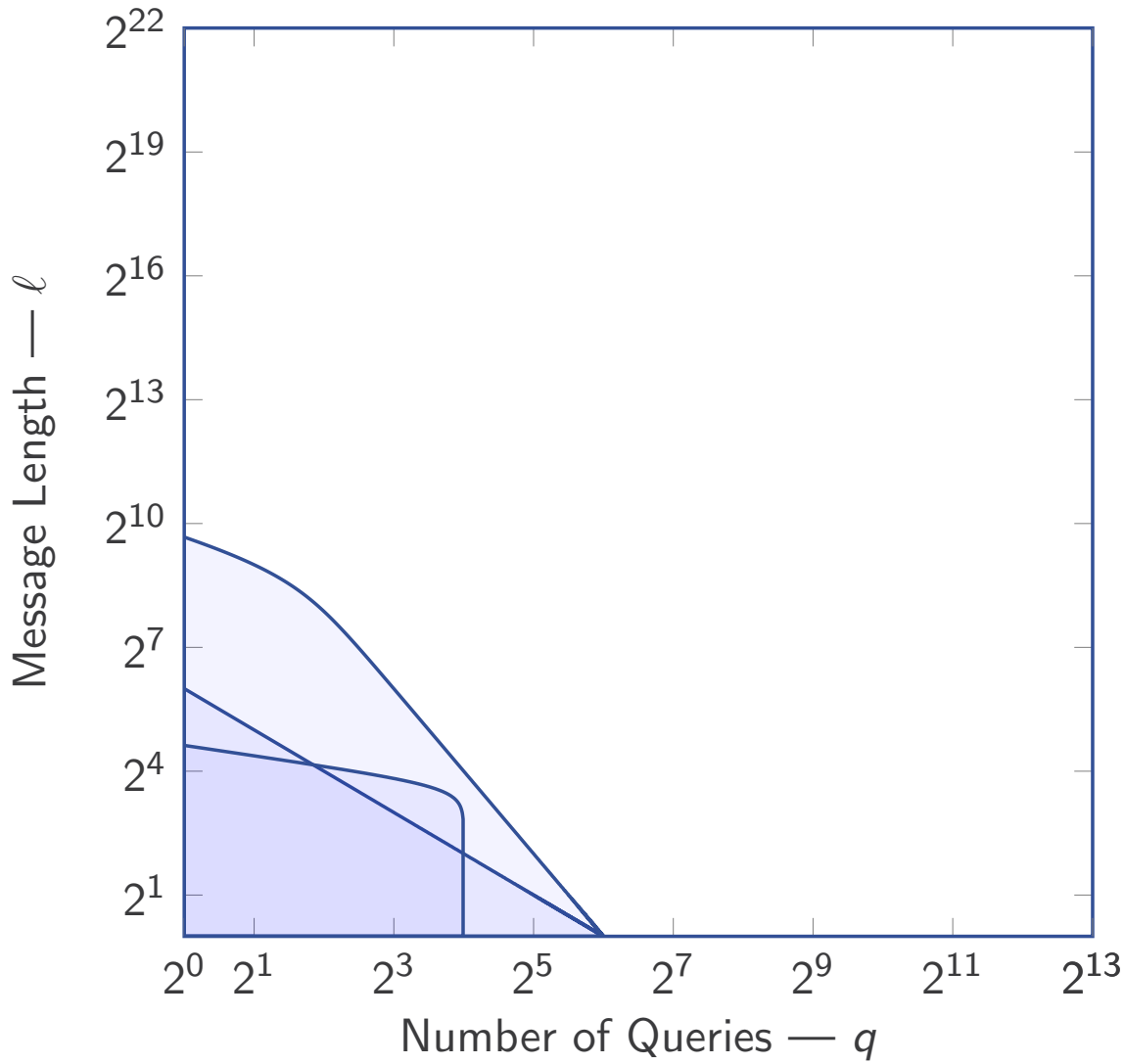
EMAC Bounds


2^{22}
2^{19}
2^{16}
2^{13}
2^{10}
2^{7}
2^{4}
2^{1}
Message Length — ℓ
2^{0} 2^{1} 2^{3} 2^{5} 2^{7} 2^{9} 2^{11} 2^{13}
Number of Queries — q

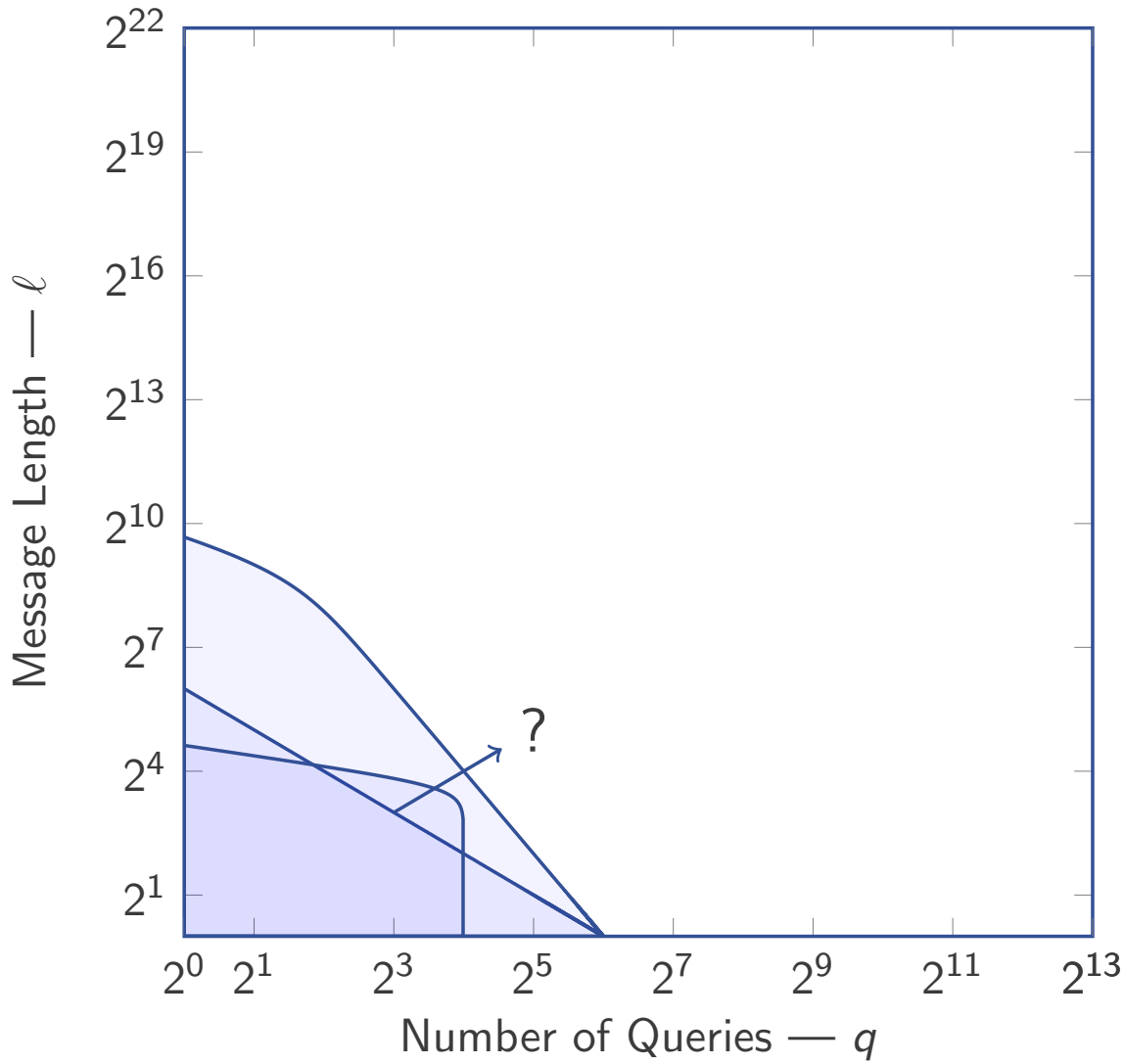
EMAC Bounds


2^{22}
2^{19}
2^{16}
2^{13}
2^{10}
2^{7}
2^{4}
2^{1}
Message Length — ℓ
2^{0} 2^{1} 2^{3} 2^{5} 2^{7} 2^{9} 2^{11} 2^{13}
Number of Queries — q

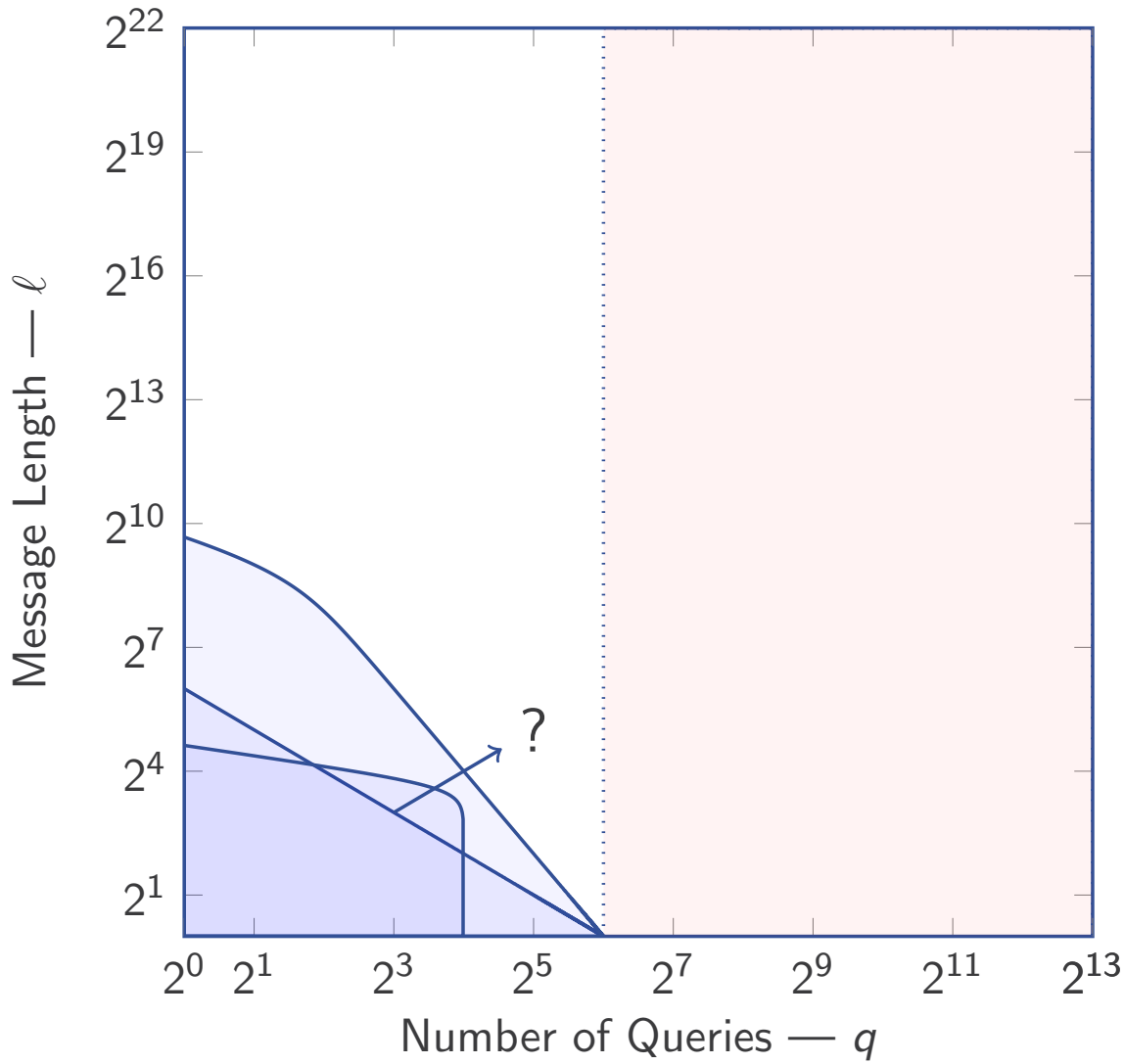
EMAC Bounds


2^{22}
2^{19}
2^{16}
2^{13}
2^{10}
2^{7}
2^{4}
2^{1}
Message Length — ℓ
2^{0} 2^{1} 2^{3} 2^{5} 2^{7} 2^{9} 2^{11} 2^{13}
Number of Queries — q

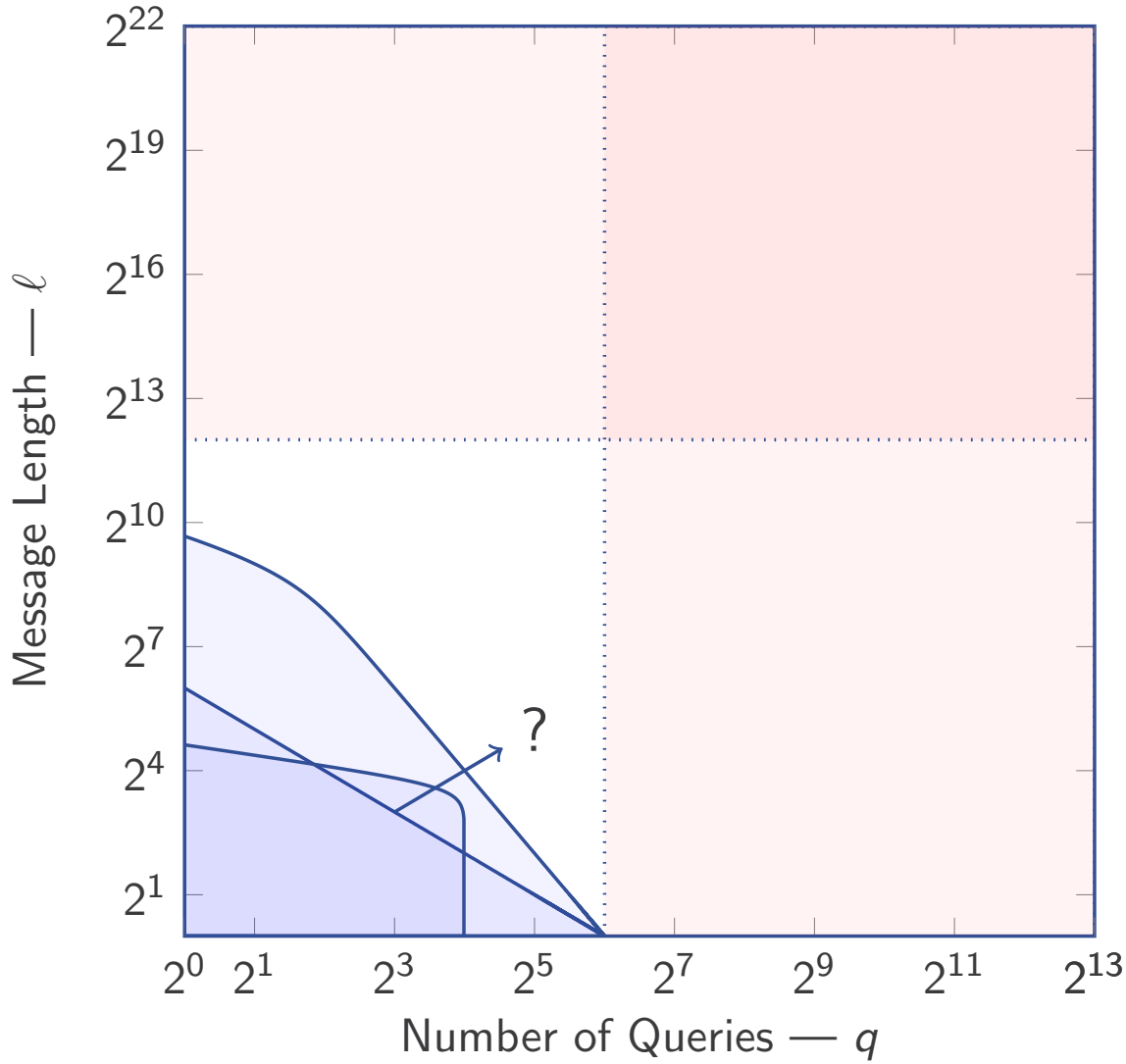
EMAC Bounds


2^{22}
2^{19}
2^{16}
2^{13}
2^{10}
2^{7}
2^{4}
2^{1}
Message Length — ℓ
?
2^{0} 2^{1} 2^{3} 2^{5} 2^{7} 2^{9} 2^{11} 2^{13}
Number of Queries — q

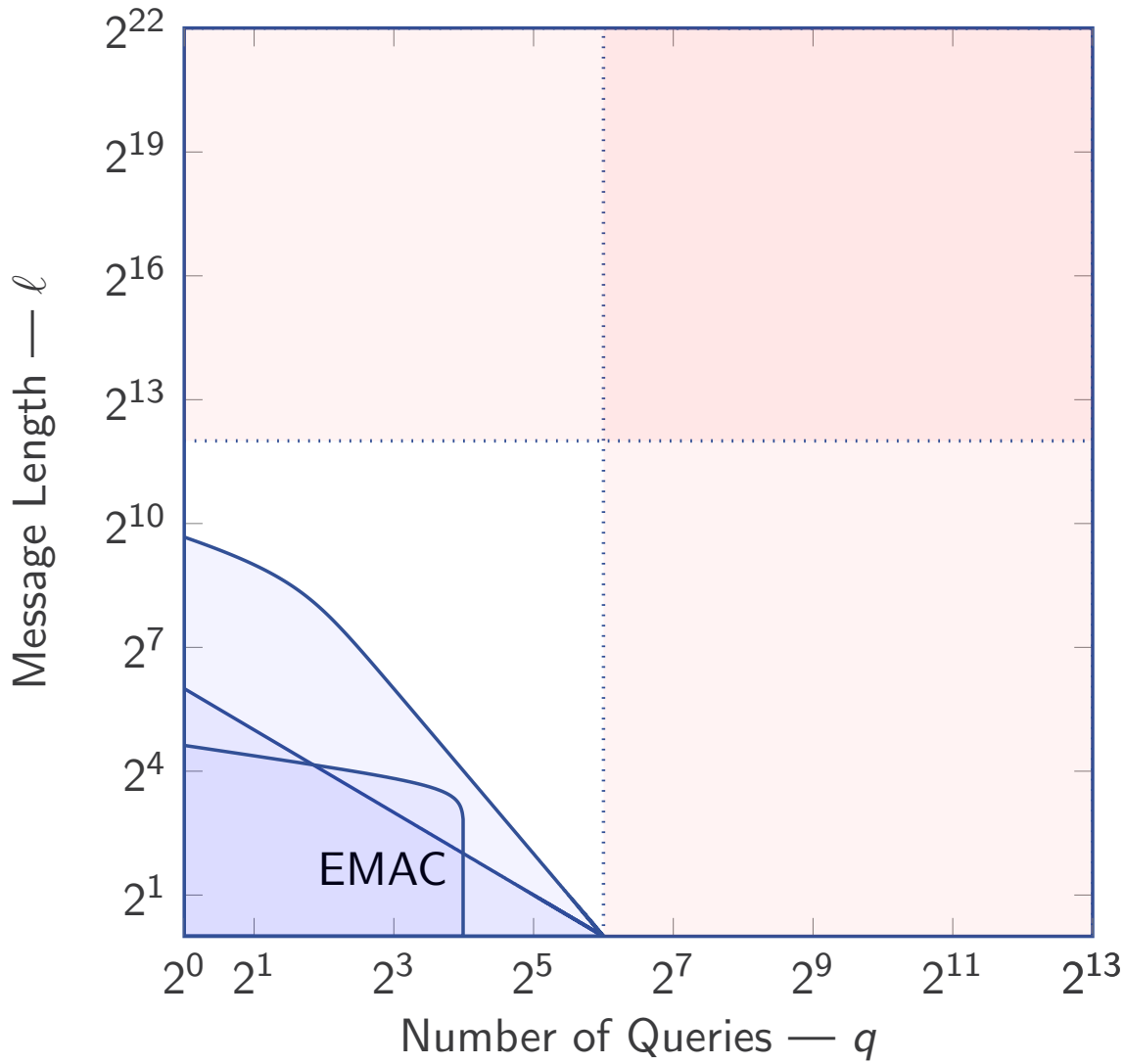
EMAC Bounds


2^{22}
2^{19}
2^{16}
2^{13}
2^{10}
2^{7}
2^{4}
2^{1}
Message Length — ℓ
?
2^{0} 2^{1} 2^{3} 2^{5} 2^{7} 2^{9} 2^{11} 2^{13}
Number of Queries — q

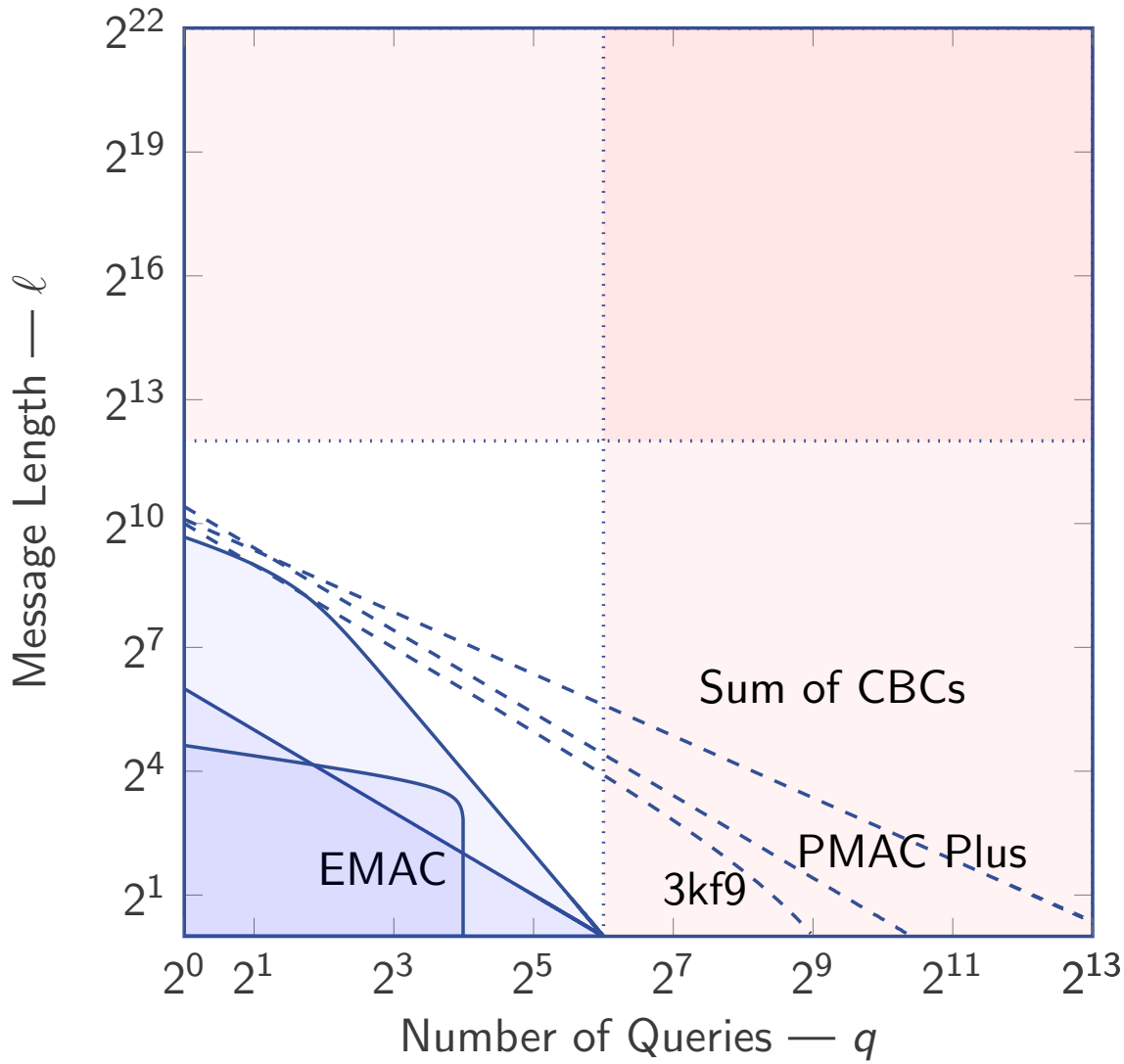
EMAC Bounds


2^{22}
2^{19}
2^{16}
2^{13}
2^{10}
2^{7}
2^{4}
2^{1}
Message Length — ℓ
?
2^{0} 2^{1} 2^{3} 2^{5} 2^{7} 2^{9} 2^{11} 2^{13}
Number of Queries — q

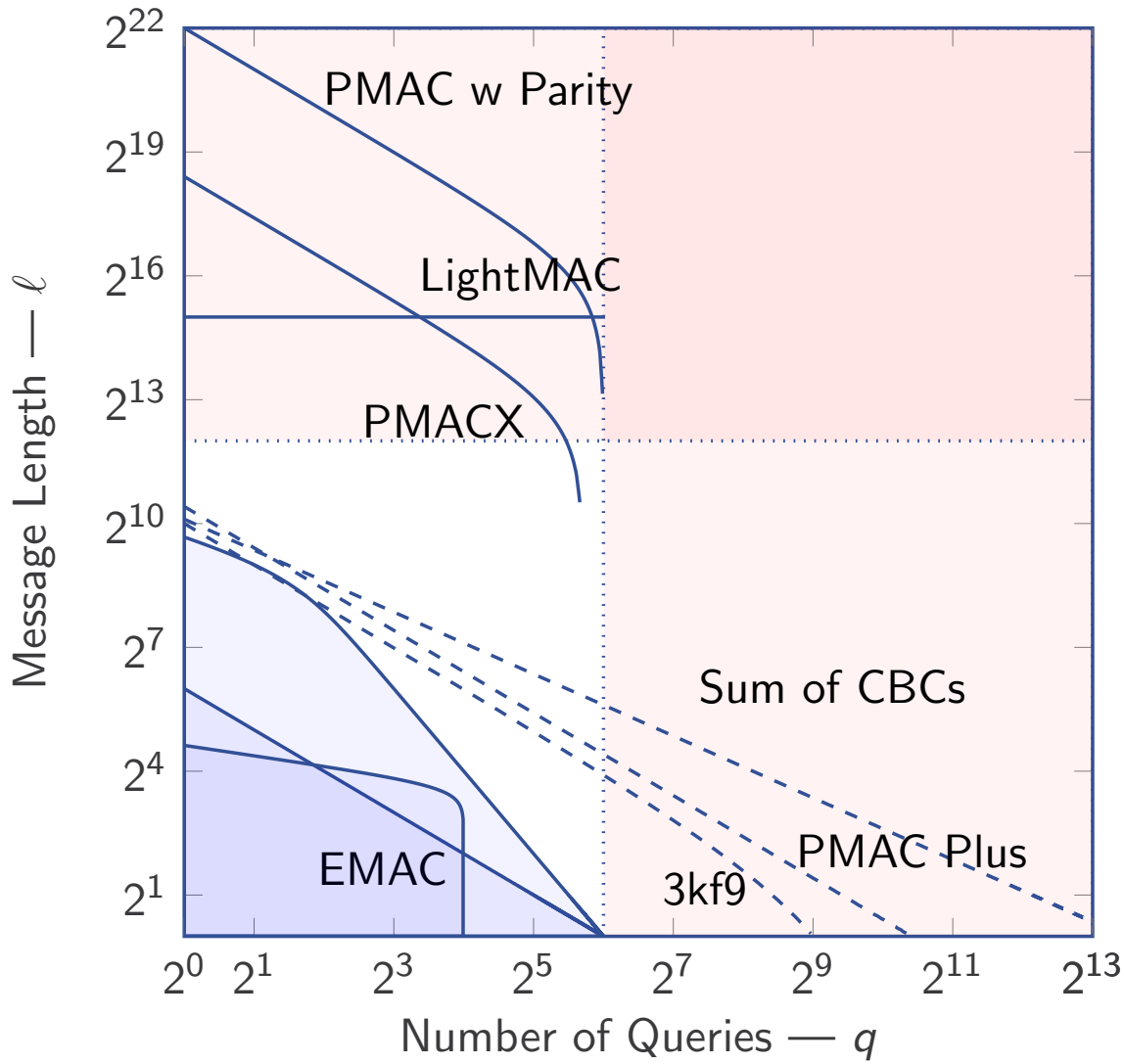
Switching Schemes



Switching Schemes



Switching Schemes



XOR-Style PRF

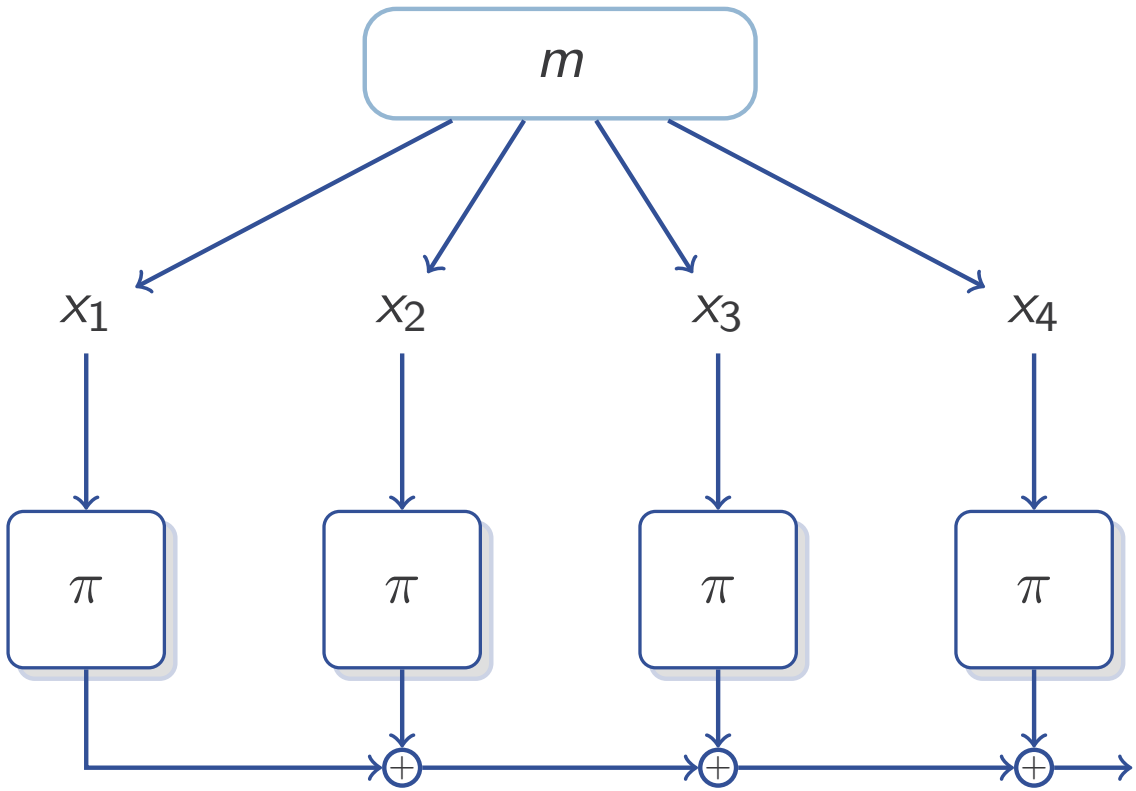
PMAC w Parity

PMACX

LightMAC

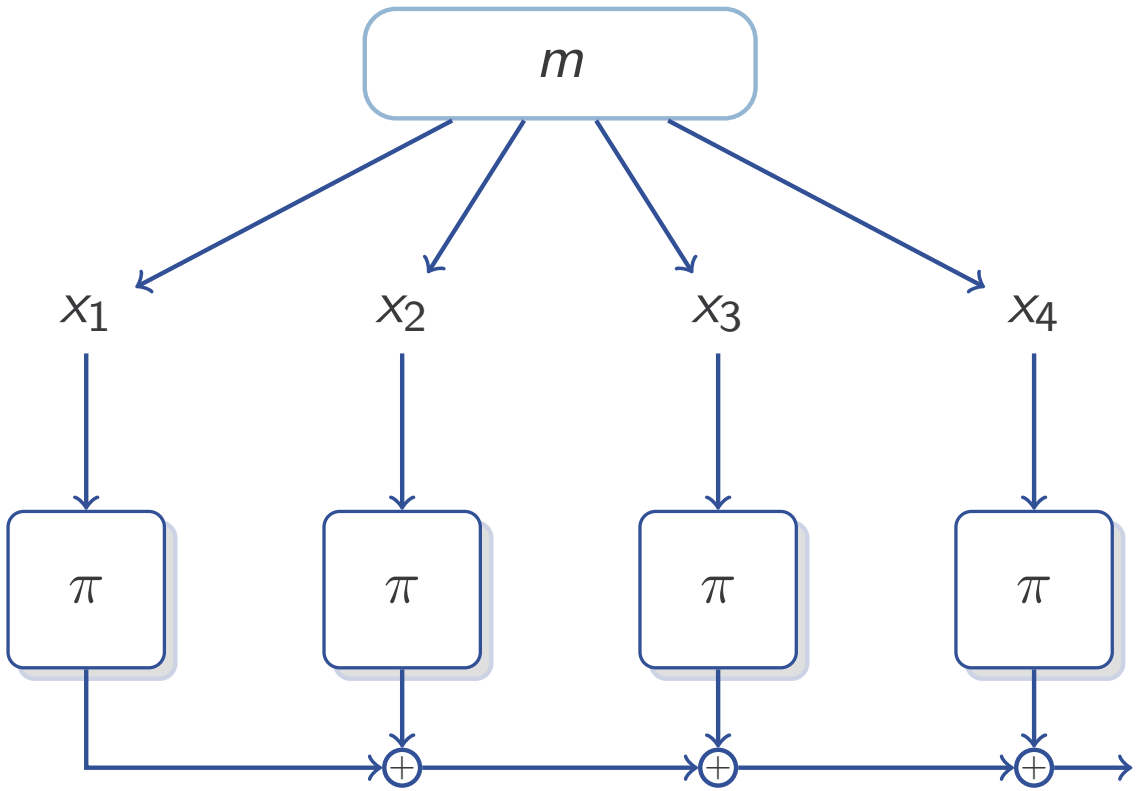
XOR-Style PRF

PMAC w Parity PMACX LightMAC

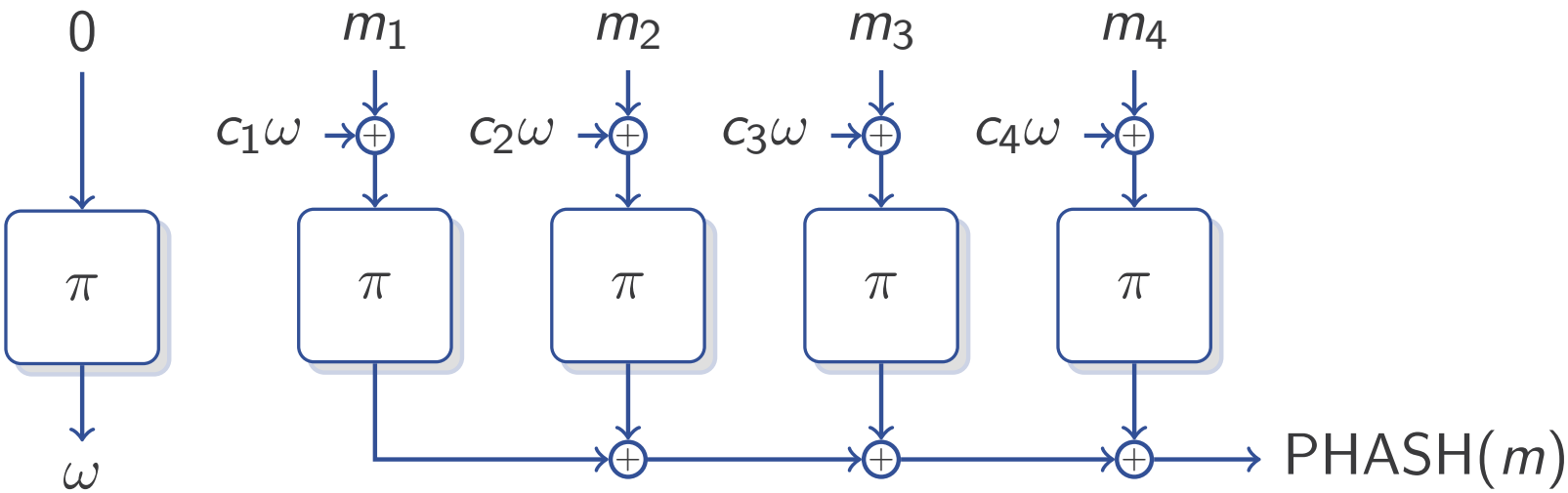


XOR-Style PRF

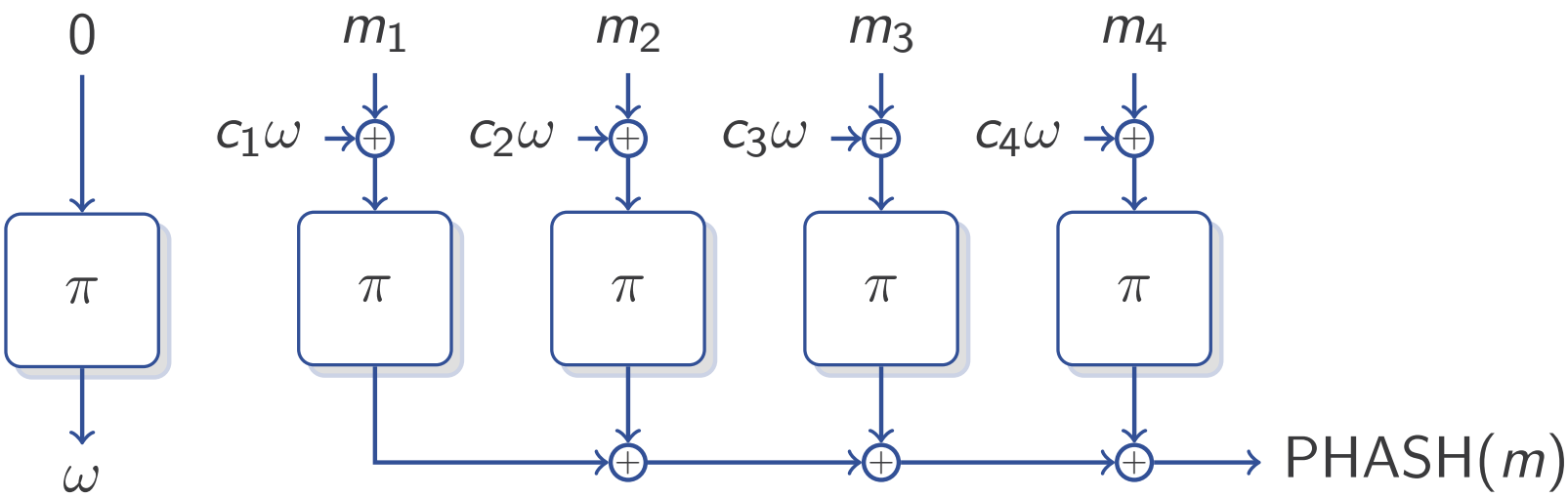
PMAC w Parity PMACX LightMAC



PMAC and PHASH

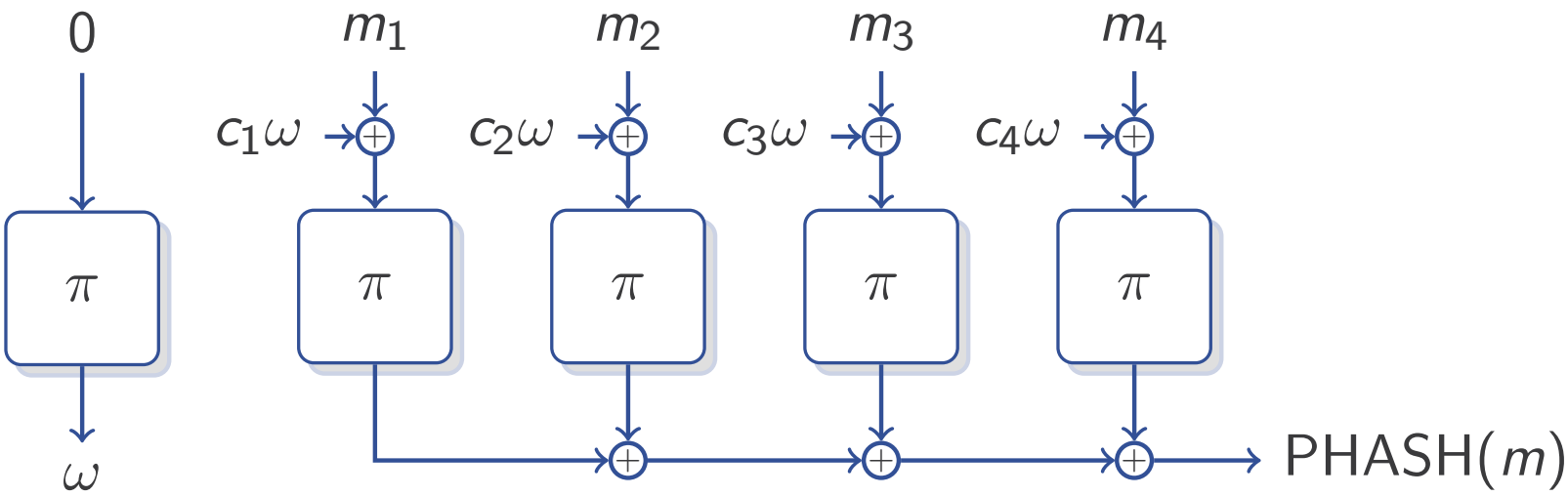


PMAC and PHASH



$$\mathrm{PMAC}(m) = \mathrm{OutputTransform}\Big(\mathrm{PHASH}(m)\Big)$$

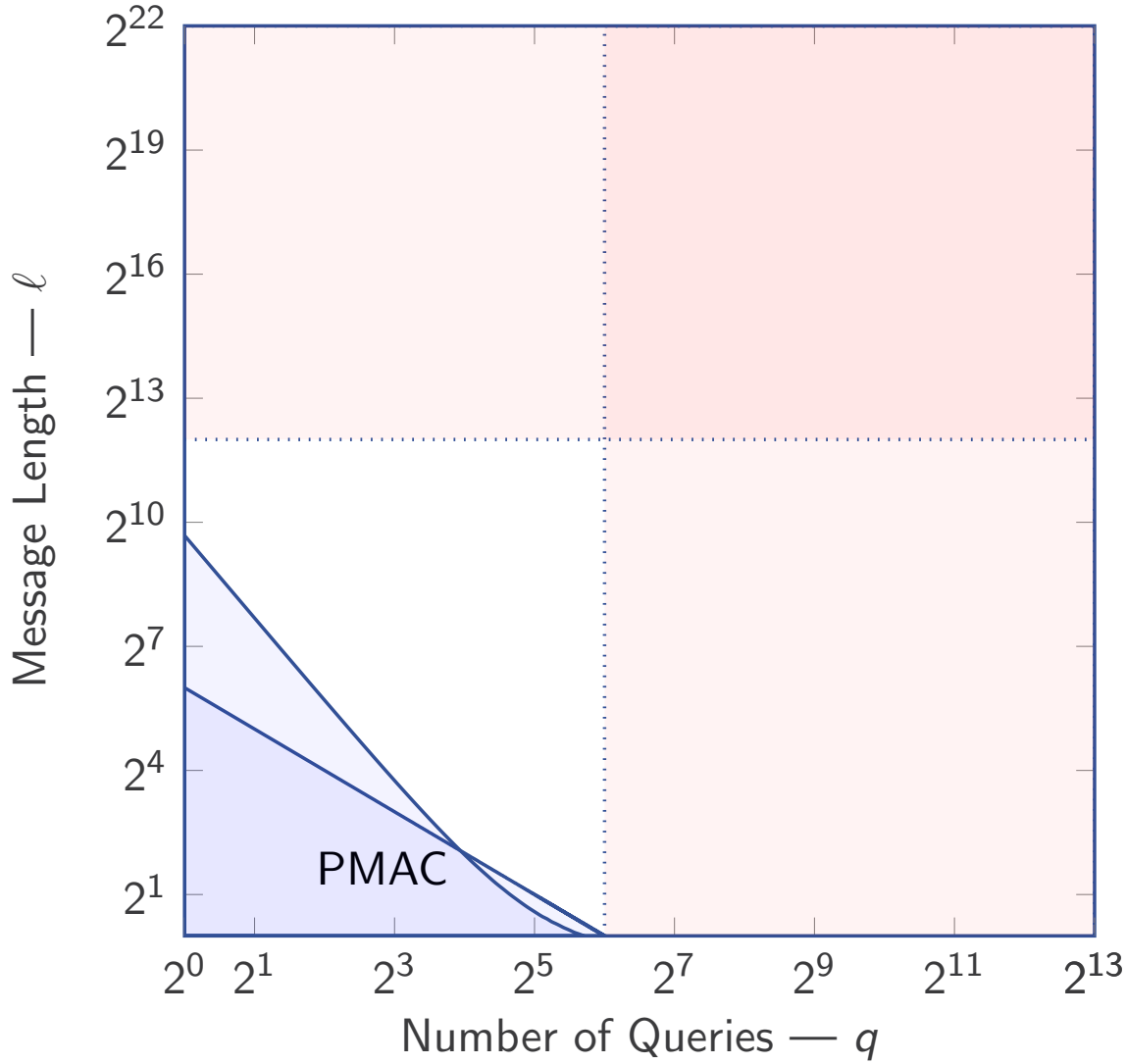
PMAC and PHASH



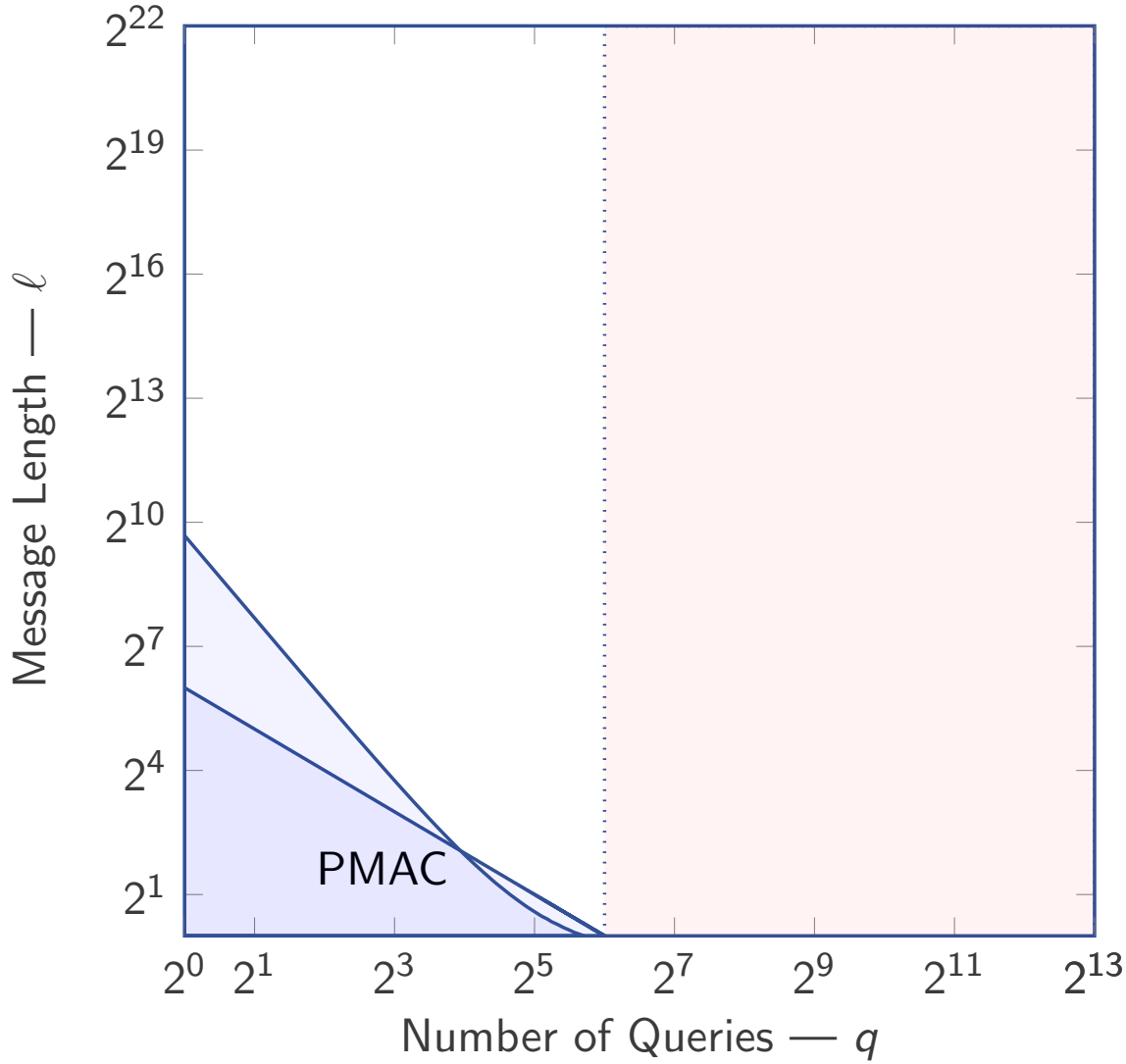
$$\mathrm{PMAC}(m) = \mathrm{OutputTransform}\Big(\mathrm{PHASH}(m)\Big)$$

1. Gray codes
2. Powering up

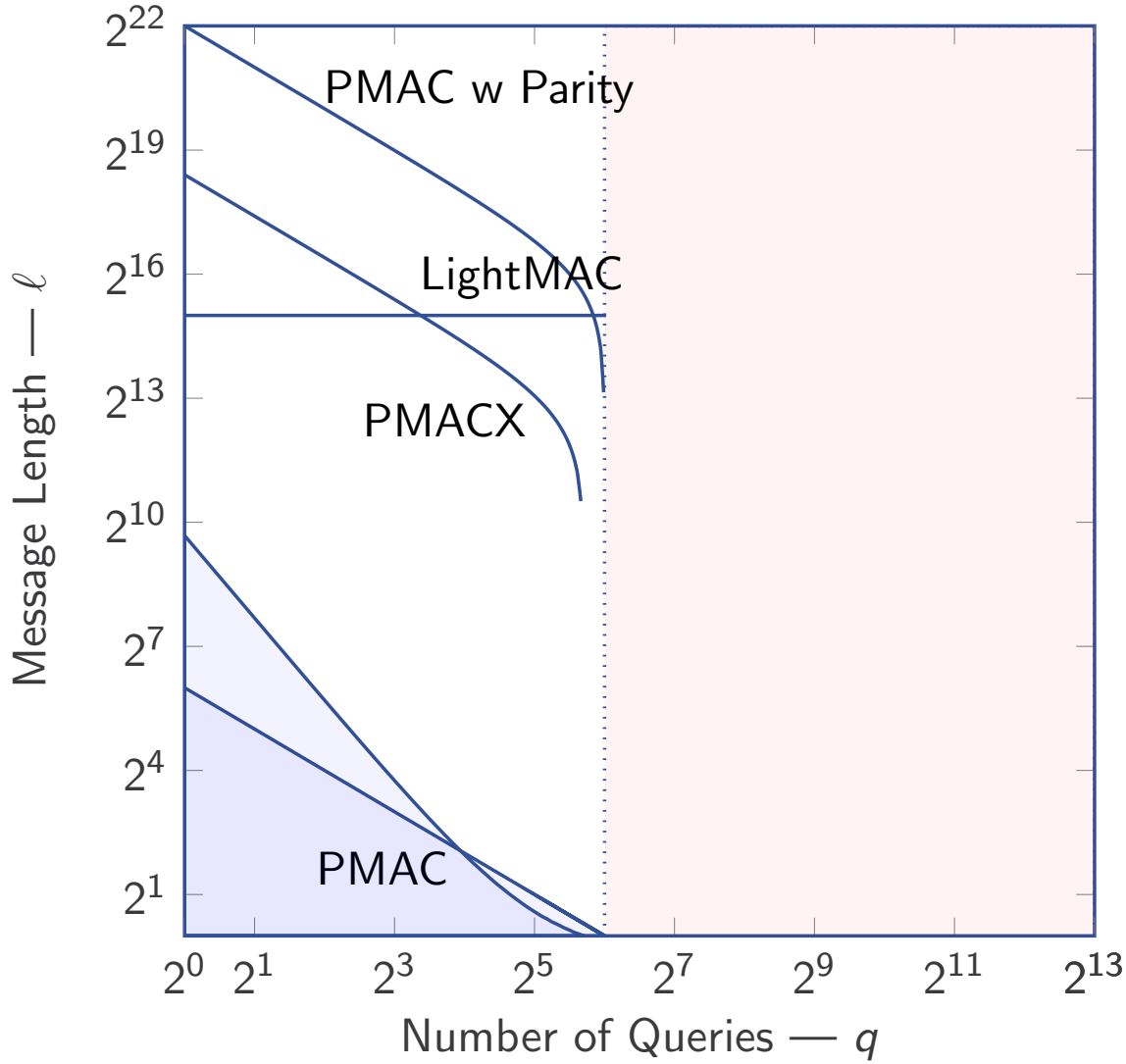
PMAC Bounds


2^{22}
2^{19}
2^{16}
2^{13}
2^{10}
2^{7}
2^{4}
2^{1}
Message Length — ℓ
PMAC
2^{0} 2^{1} 2^{3} 2^{5} 2^{7} 2^{9} 2^{11} 2^{13}
Number of Queries — q

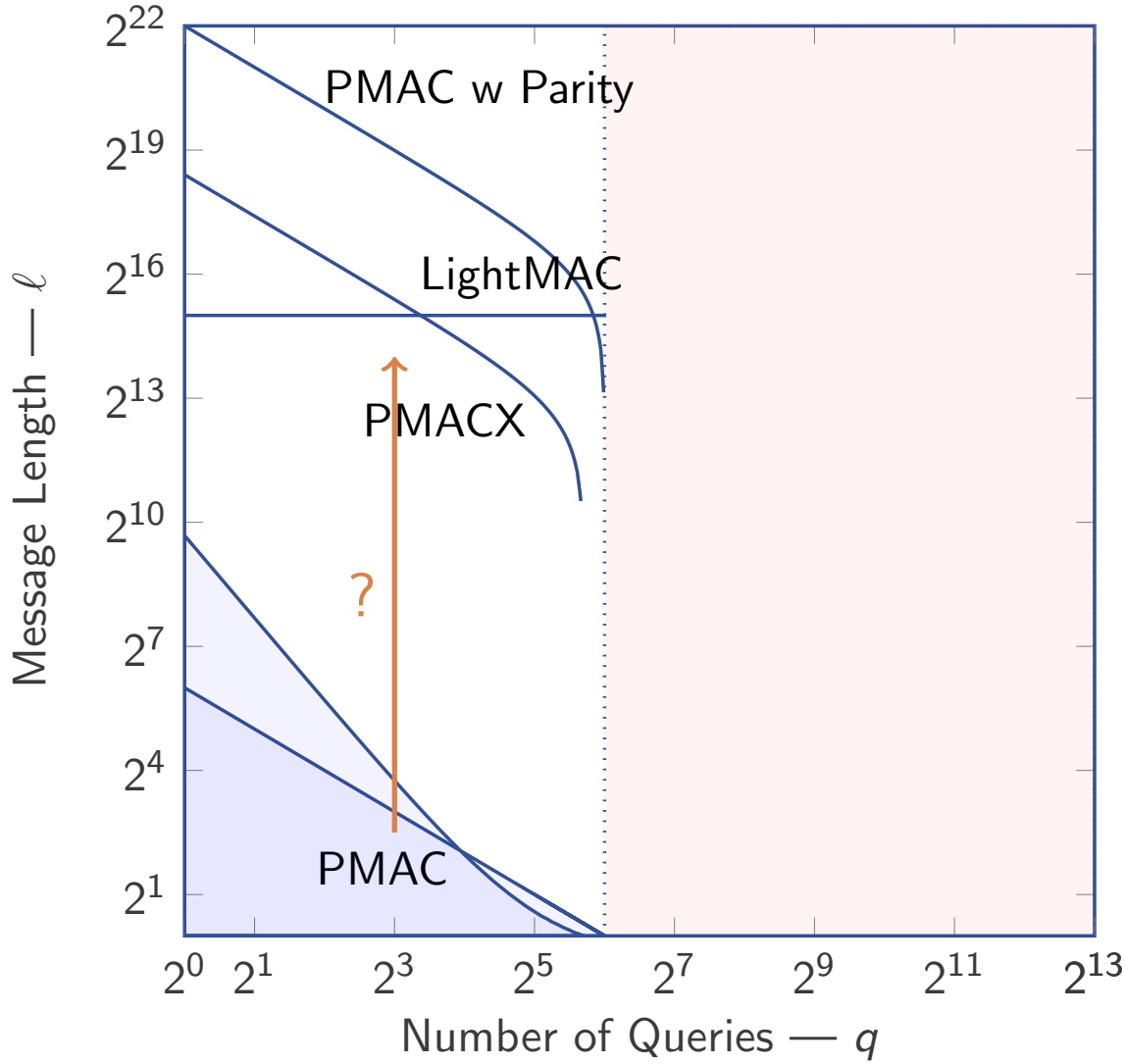
PMAC Bounds


2^{22}
2^{19}
2^{16}
2^{13}
2^{10}
2^{7}
2^{4}
2^{1}
Message Length — ℓ
PMAC
2^{0} 2^{1} 2^{3} 2^{5} 2^{7} 2^{9} 2^{11} 2^{13}
Number of Queries — q

PMAC Bounds


PMAC w Parity
LightMAC
PMACX
PMAC
Message Length — ℓ
Number of Queries — q
2^{22}
2^{19}
2^{16}
2^{13}
2^{10}
2^{7}
2^{4}
2^{1}
2^{0} 2^{1} 2^{3} 2^{5} 2^{7} 2^{9} 2^{11} 2^{13}

PMAC Bounds


PMAC w Parity
LightMAC
PMACX
?
PMAC
Message Length — ℓ
Number of Queries — q
2^{22}
2^{19}
2^{16}
2^{13}
2^{10}
2^{7}
2^{4}
2^{1}
2^{0} 2^{1} 2^{3} 2^{5} 2^{7} 2^{9} 2^{11} 2^{13}

Focusing on Collisions

$$\mathrm{PHASH}(m^1) = \mathrm{PHASH}(m^2)$$

$$\mathrm{PMAC}(m^1) = \mathrm{PMAC}(m^2)$$

Focusing on Collisions

$$\mathrm{PHASH}(m^1) = \mathrm{PHASH}(m^2)$$

$$\mathrm{PMAC}(m^1) = \mathrm{PMAC}(m^2)$$

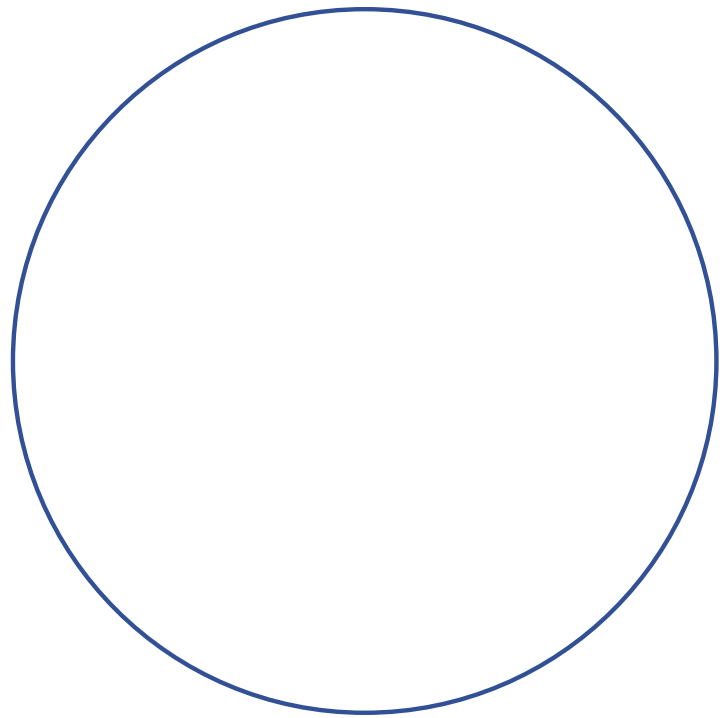
PHASH collision implies a PMAC attack

Results

Message length dependence changes according to masks

Results

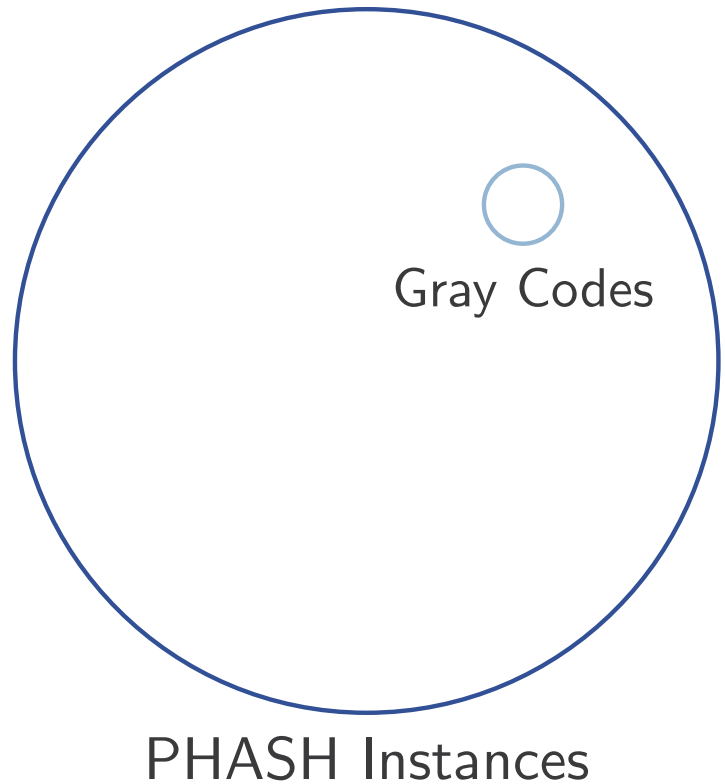
Message length dependence changes according to masks



PHASH Instances

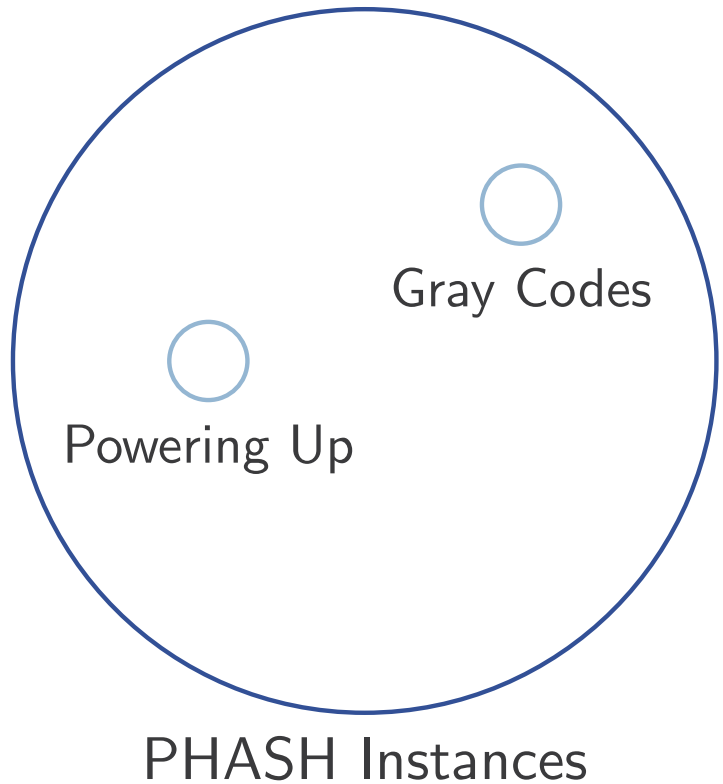
Results

Message length dependence changes according to masks



Results

Message length dependence changes according to masks

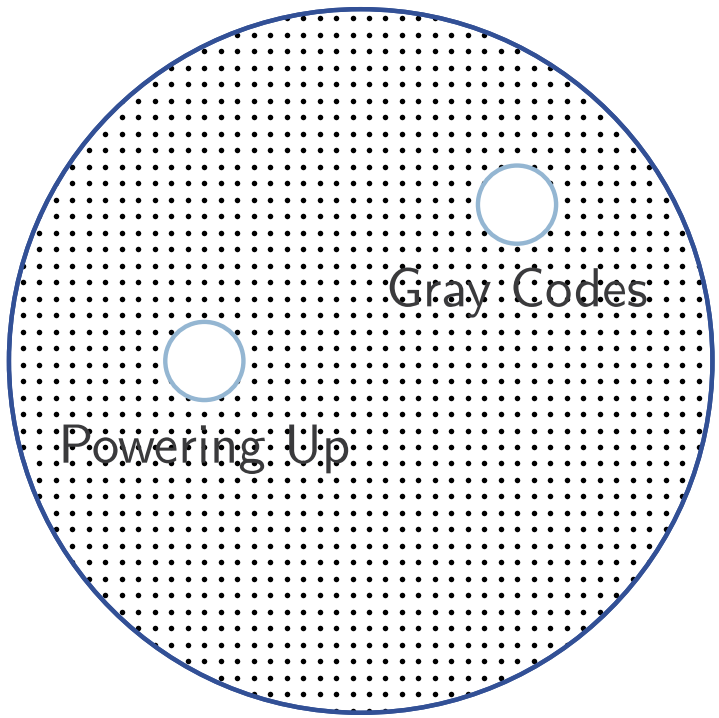


Results

Message length dependence changes according to masks

Infinitely many with collision
upper bound $2/2^n$

or



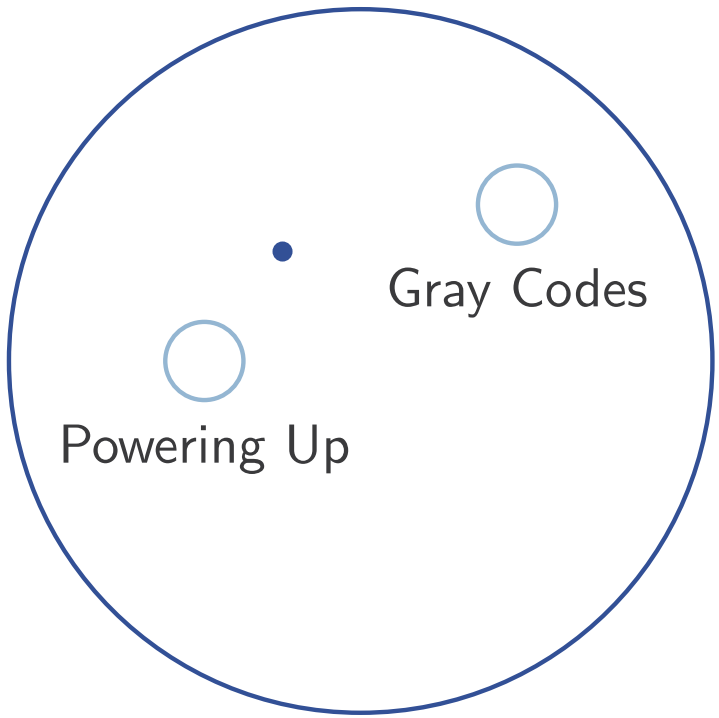
Results

Message length dependence changes according to masks

Infinitely many with collision
upper bound $2/2^n$

or

Computationally hard to find
high probability collision
(based on conjecture)



Results

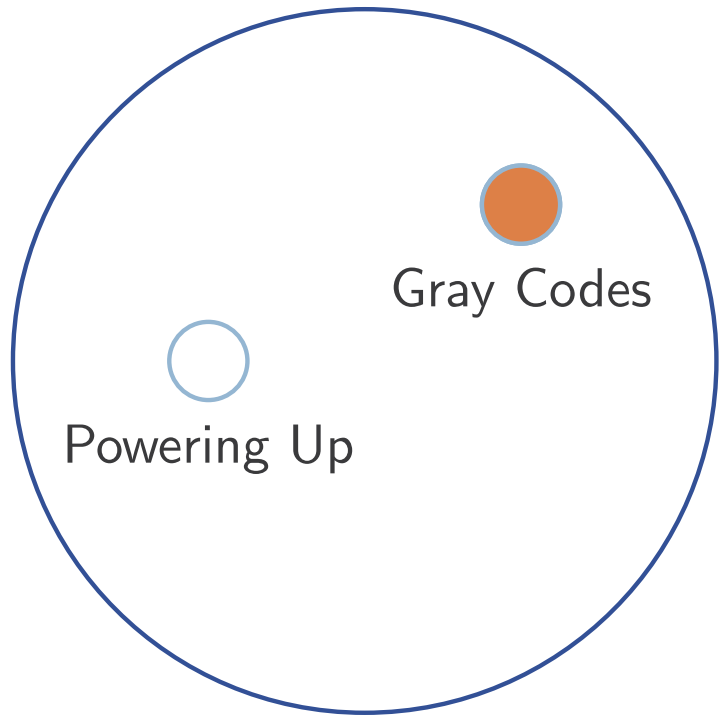
Message length dependence changes according to masks

Infinitely many with collision upper bound $2/2^n$

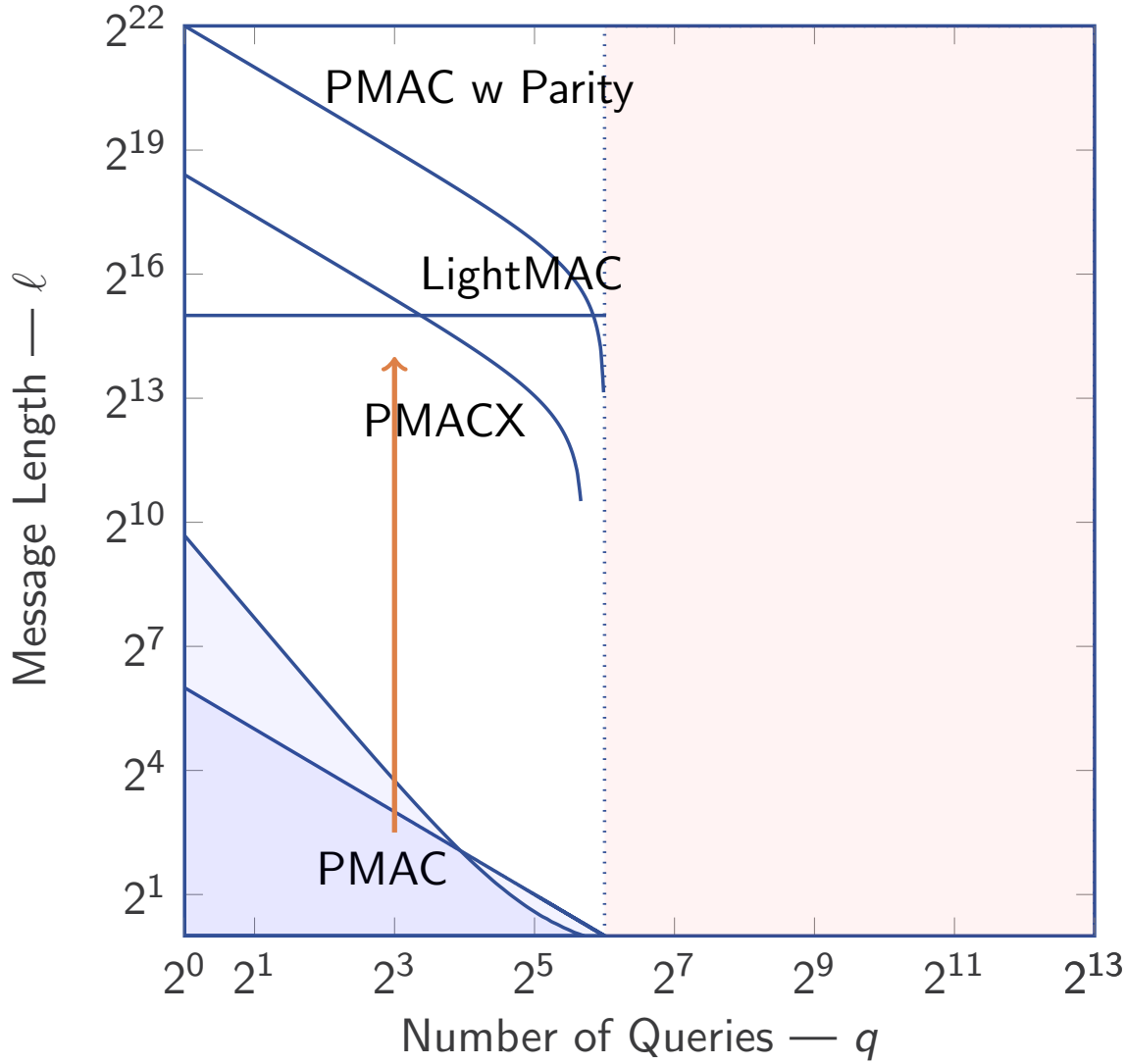
or

Computationally hard to find high probability collision (based on conjecture)

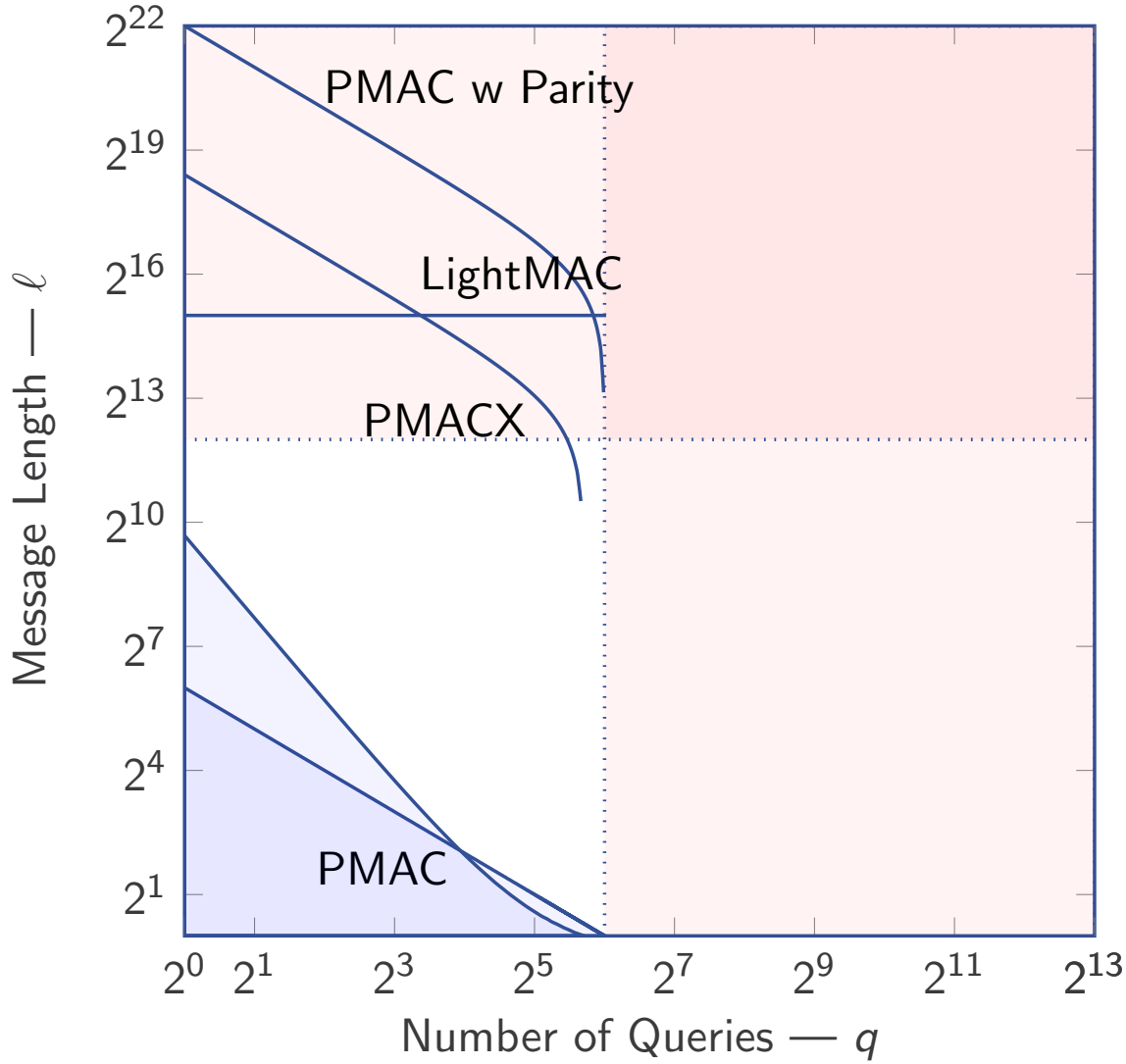
Gray codes instances depend on message length



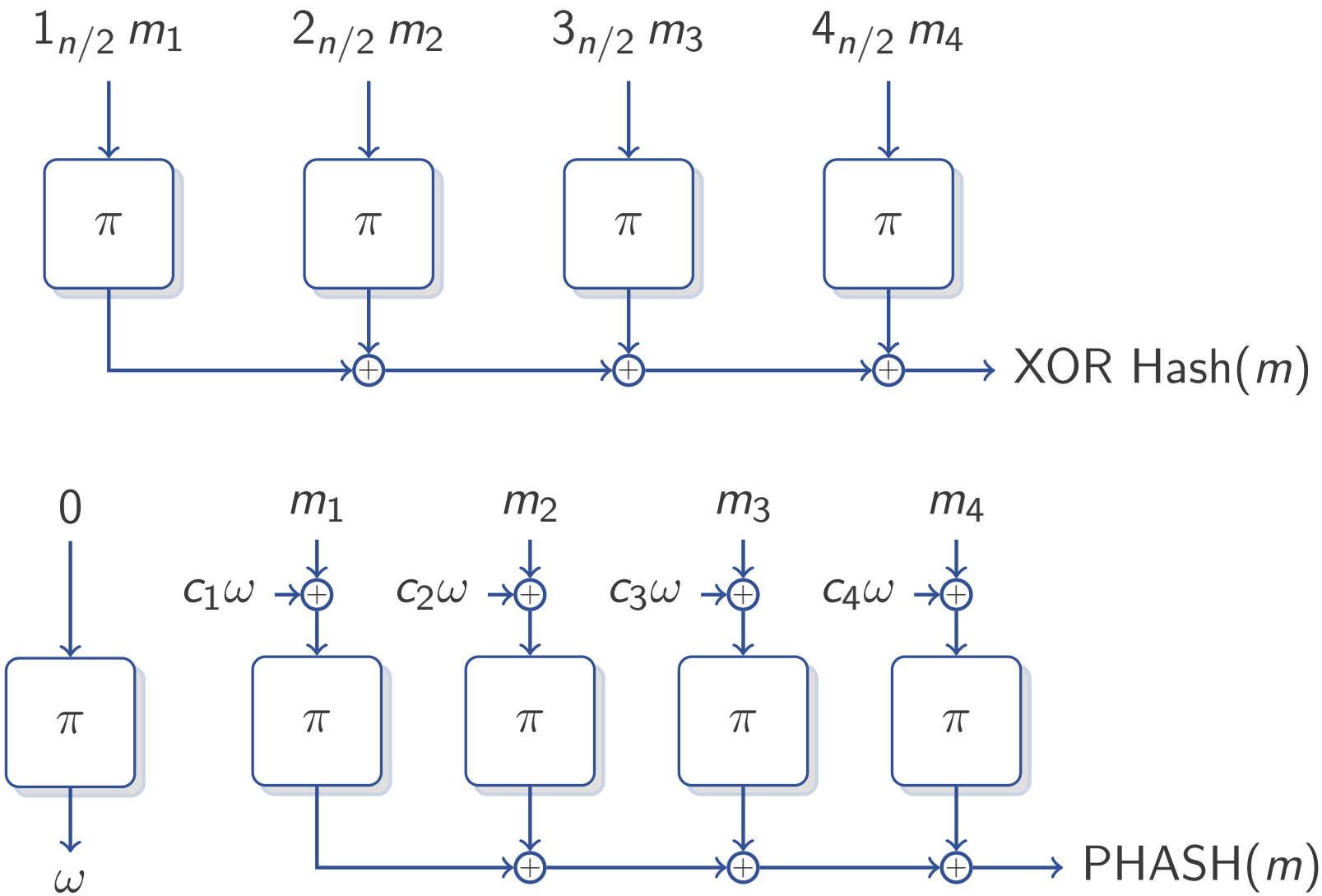
Results in Context



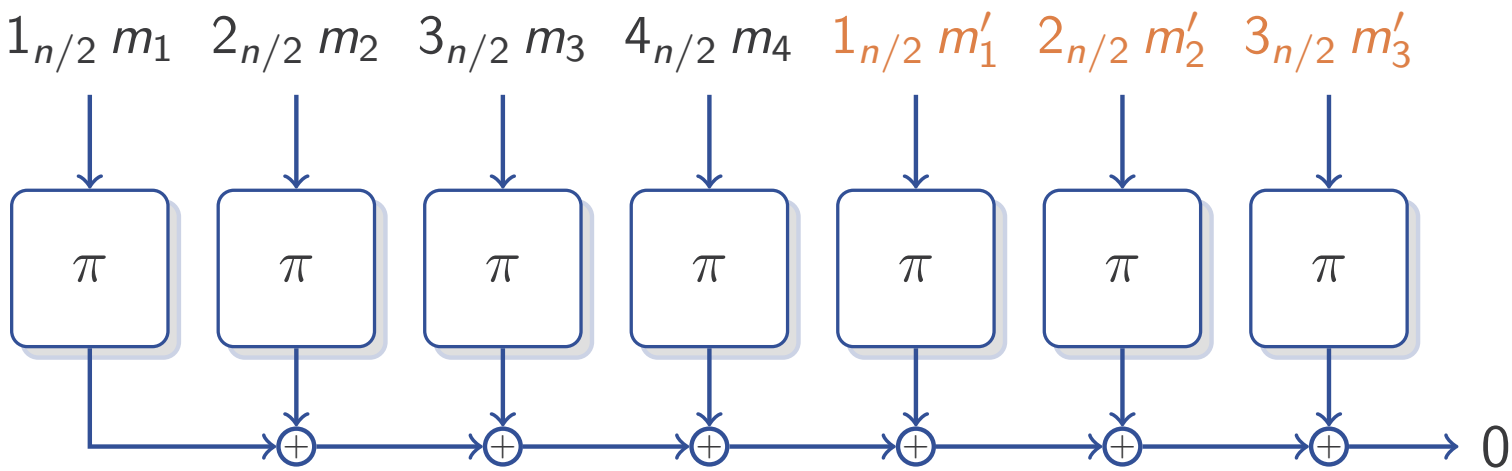
Results in Context



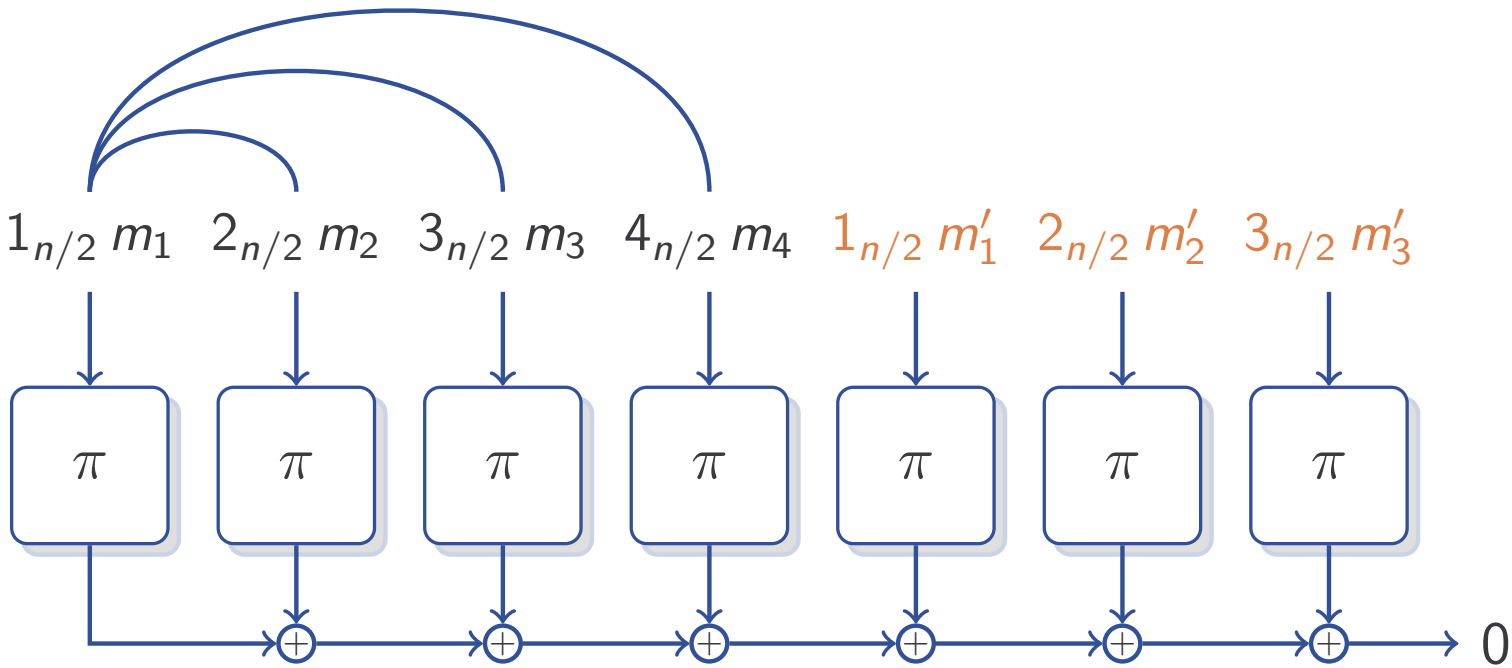
PHASH vs XOR Hash



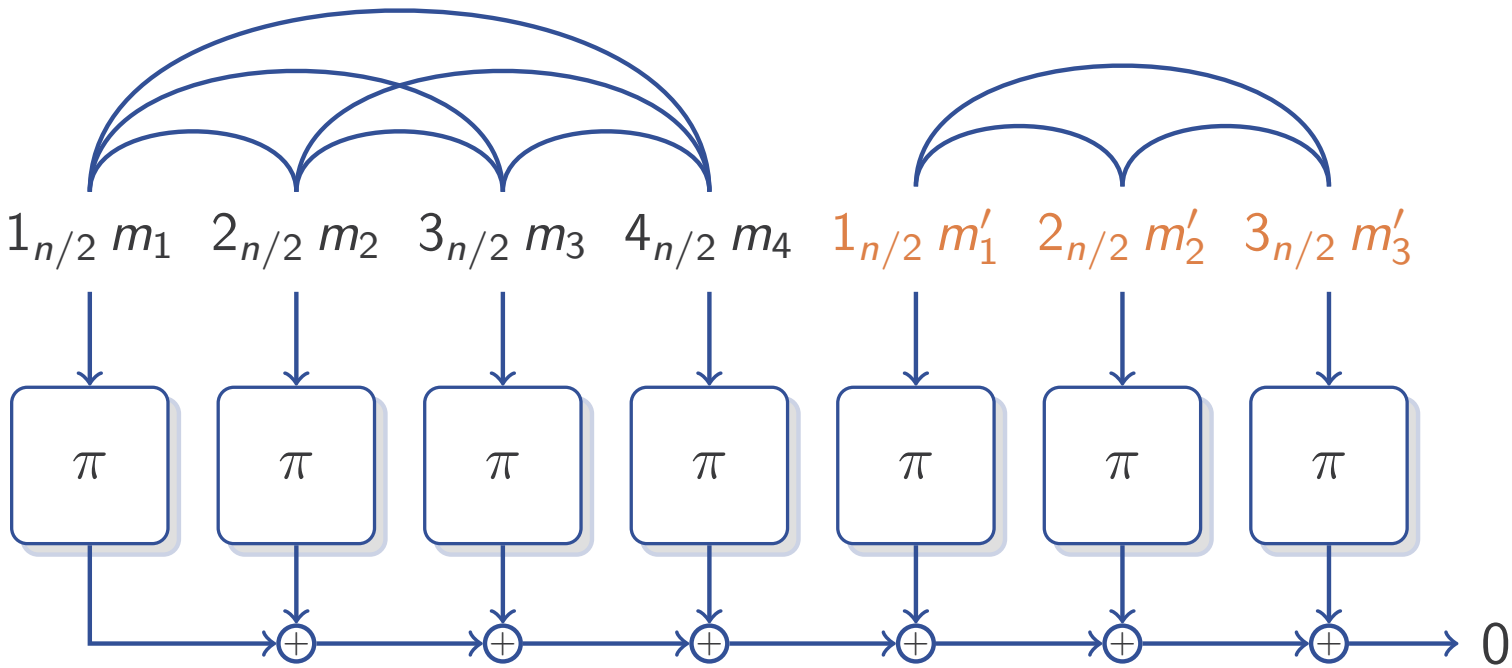
XOR Hash Collision



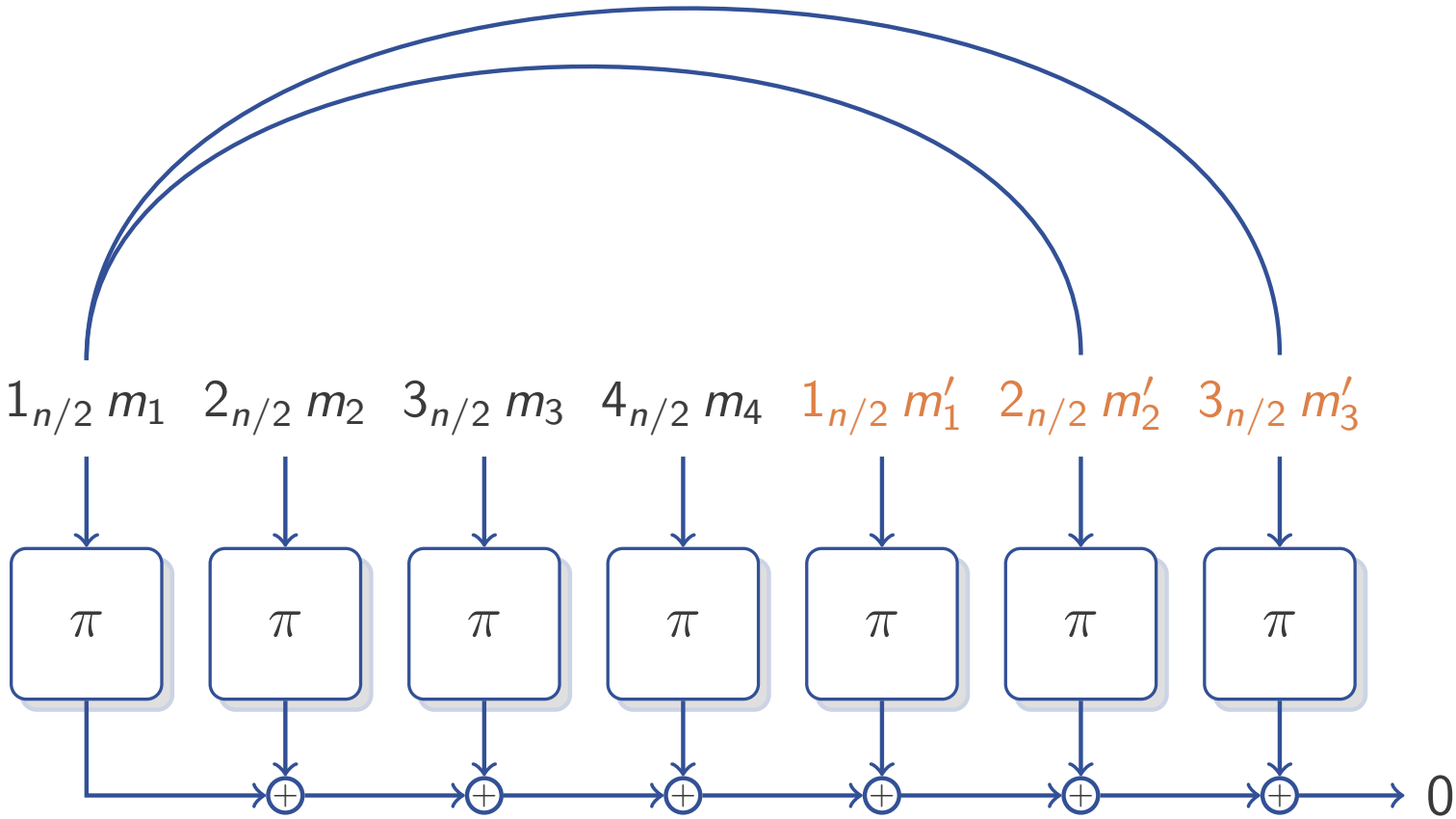
XOR Hash Collision



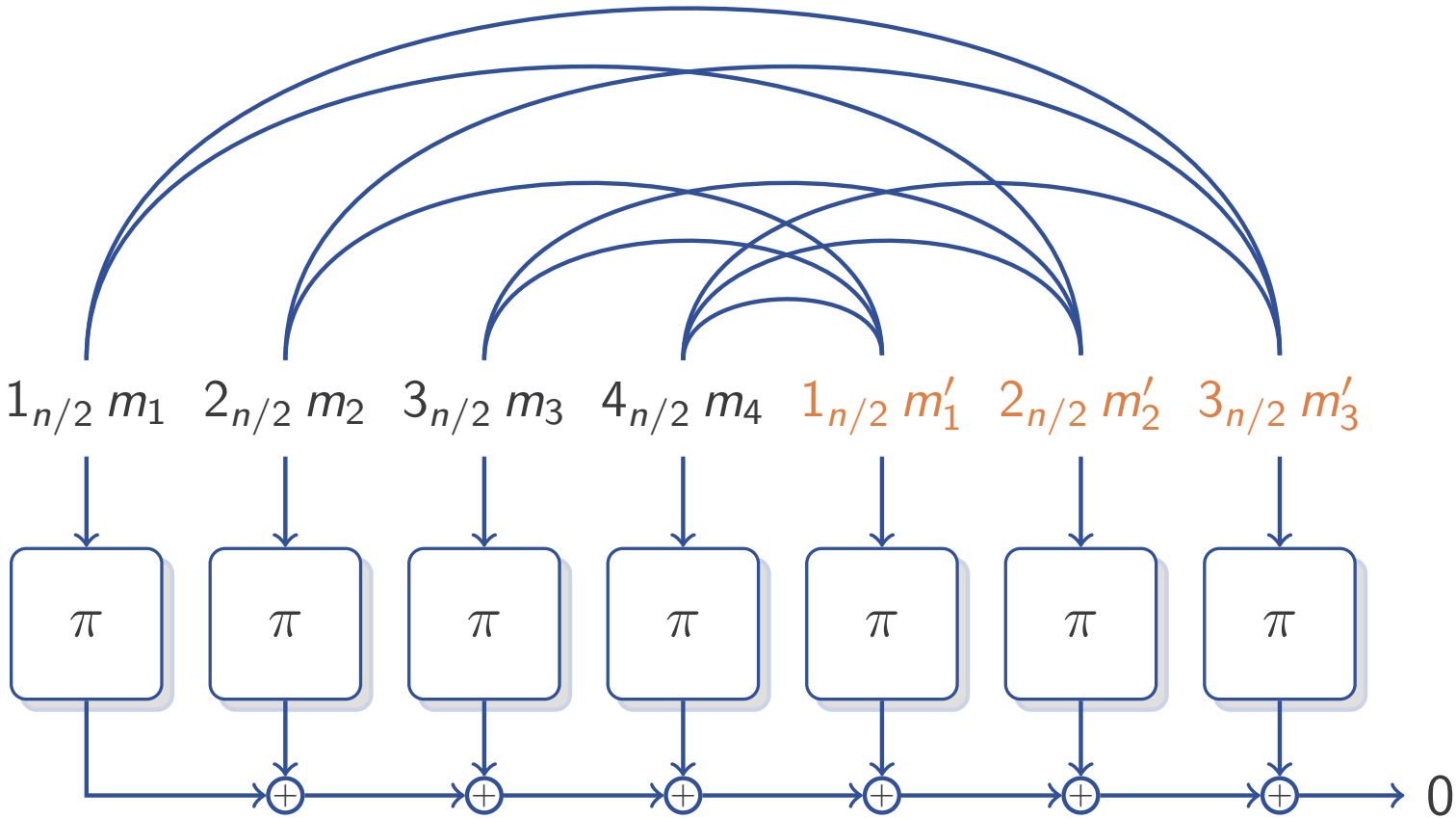
XOR Hash Collision



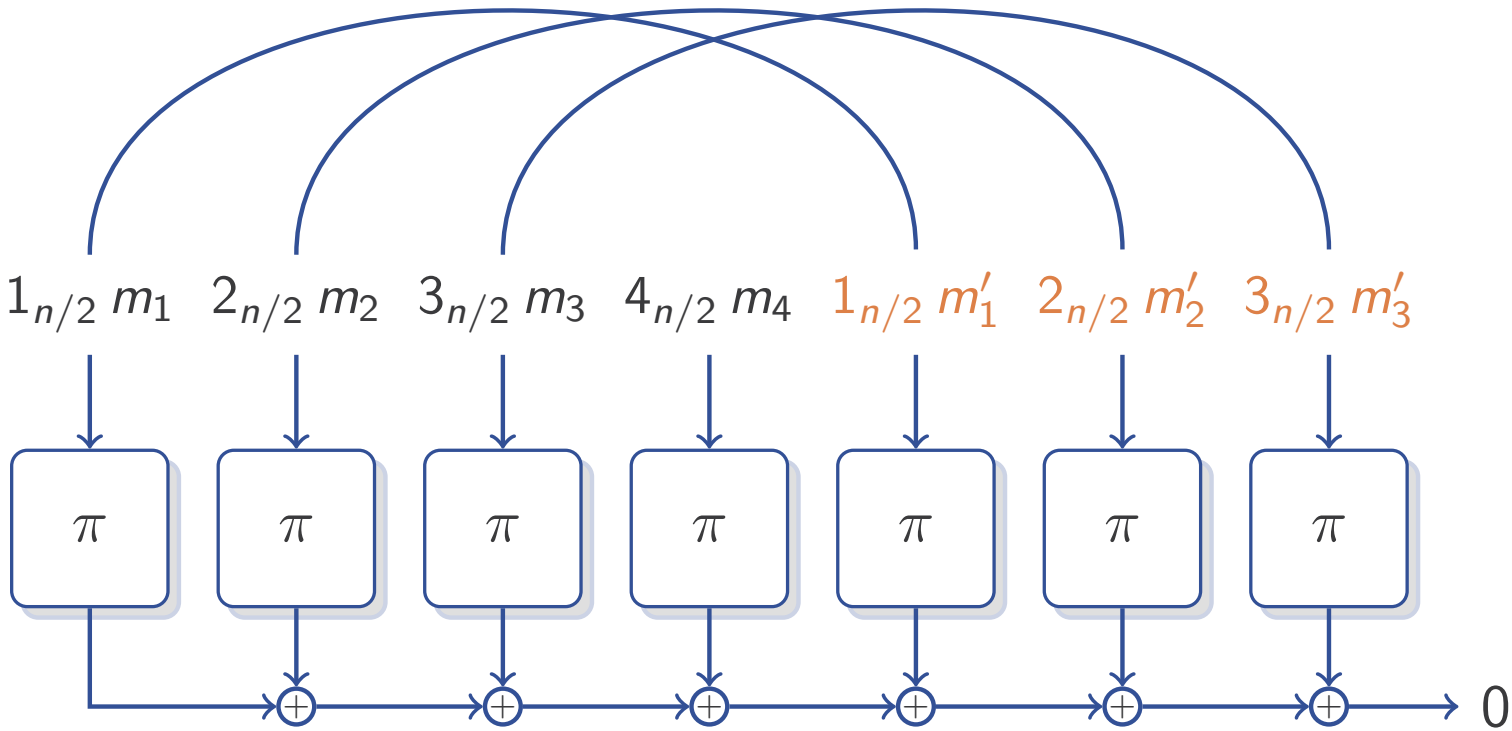
XOR Hash Collision



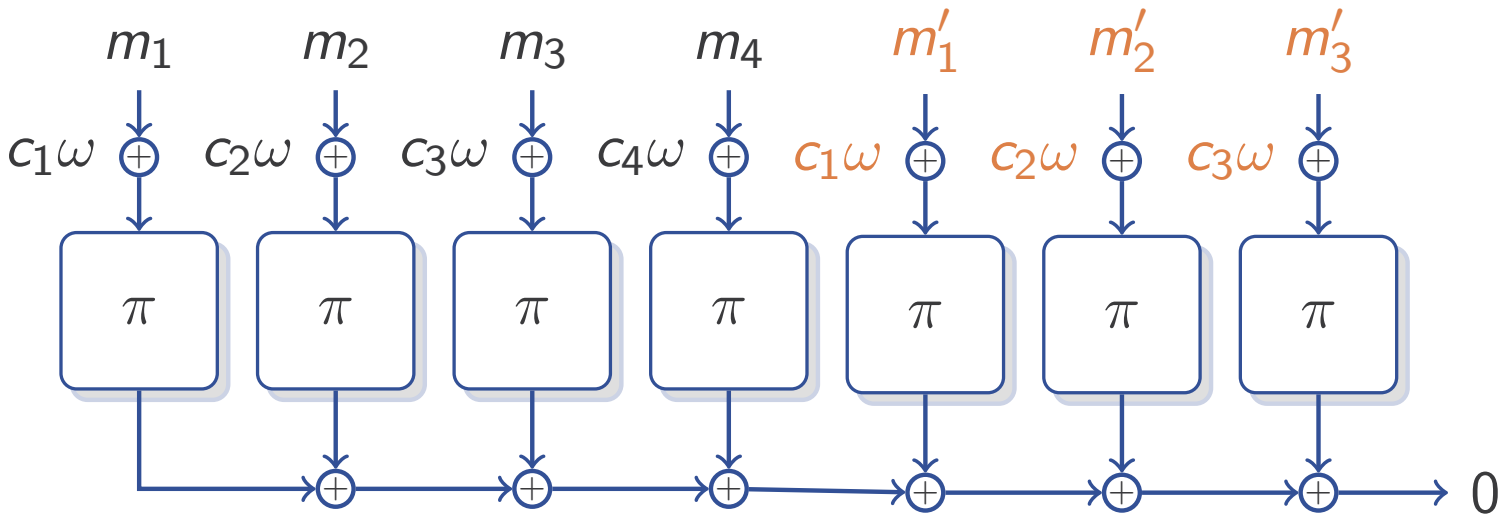
XOR Hash Collision



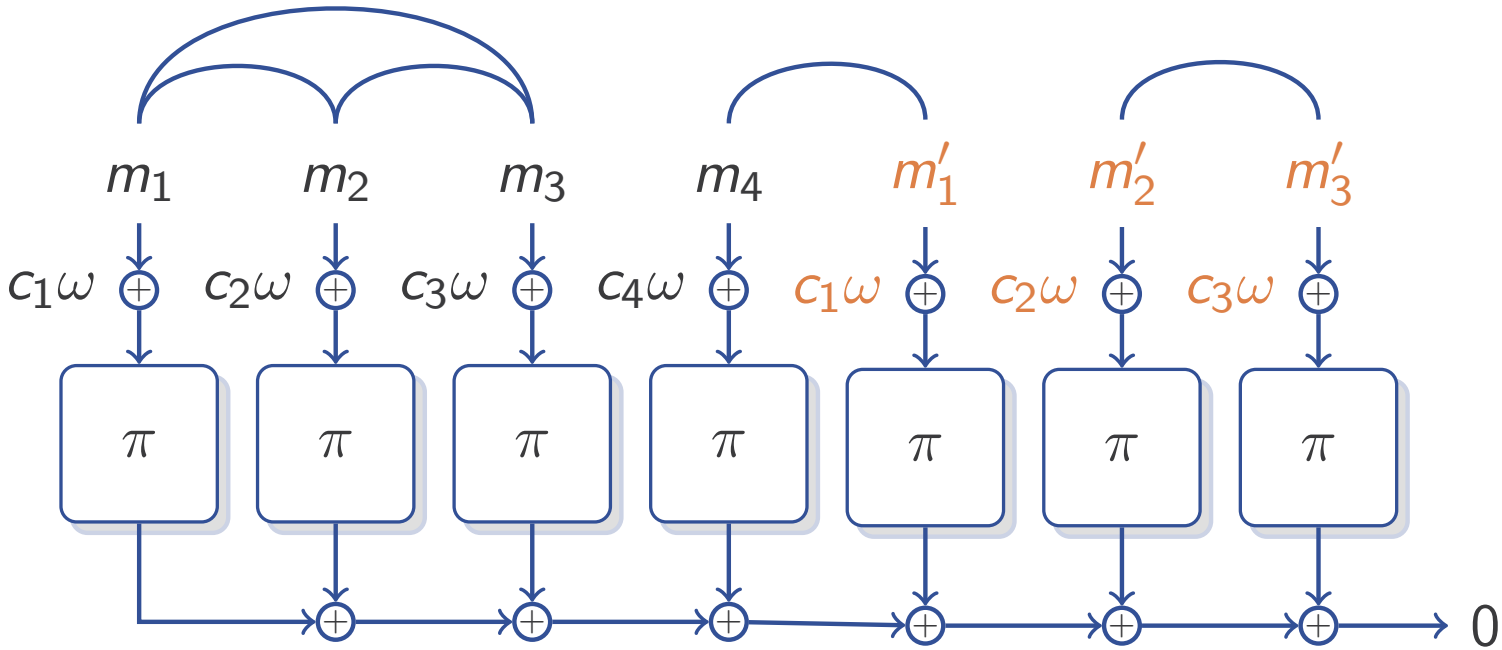
XOR Hash Collision



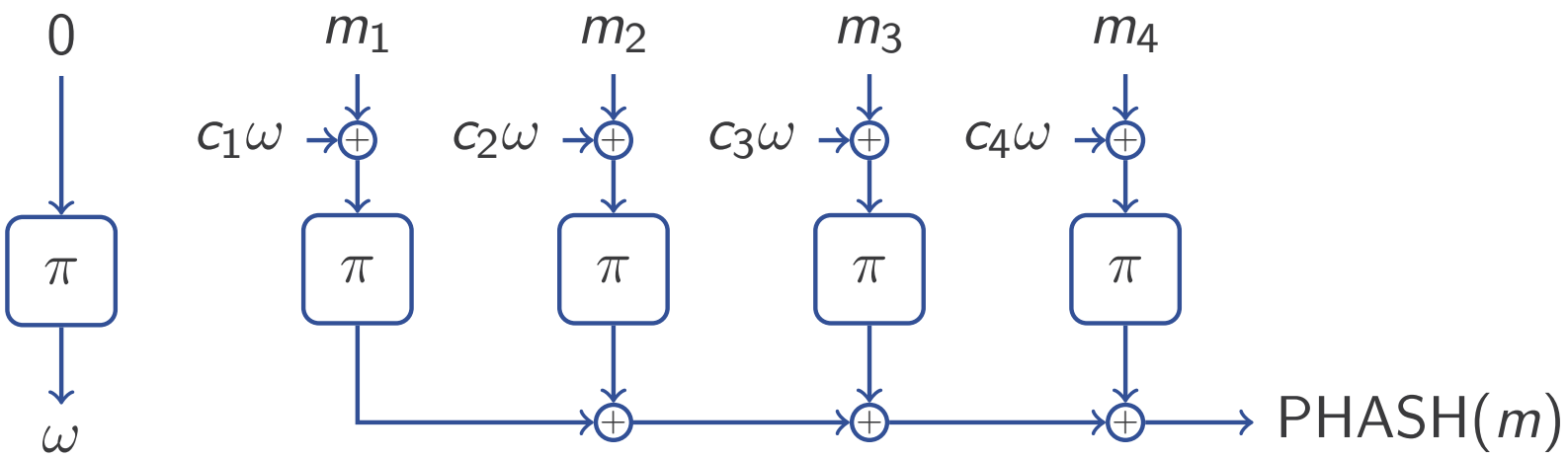
PHASH Collision

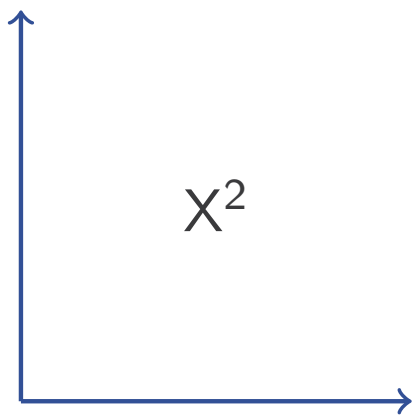


PHASH Collision

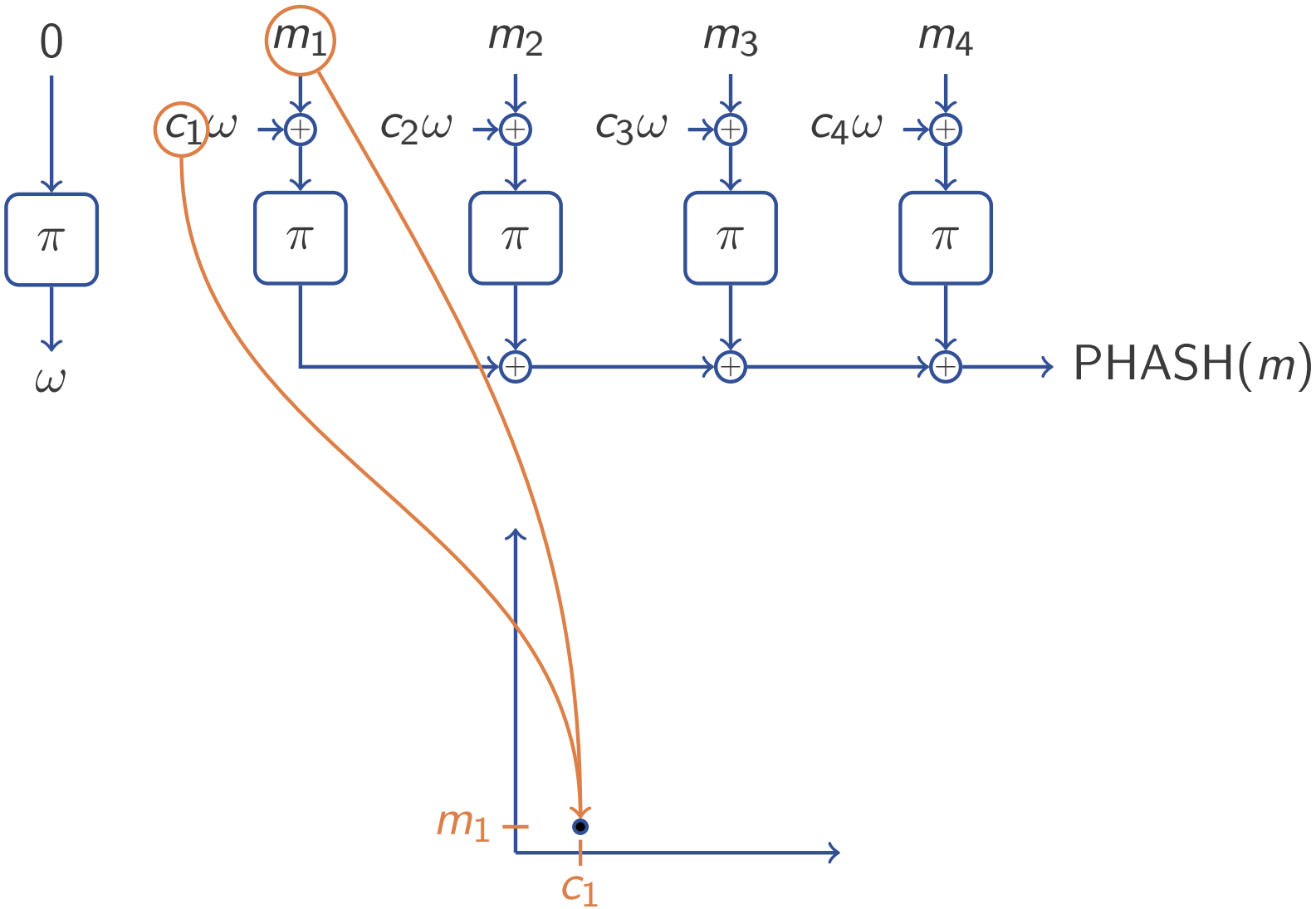


Approach

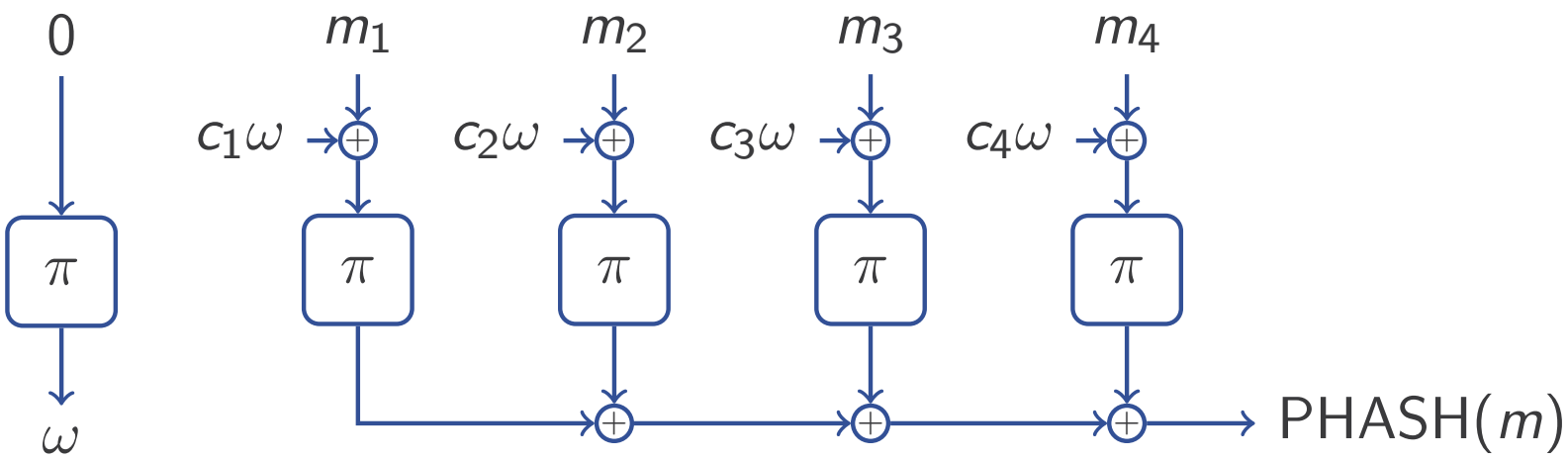

0
m_1
m_2
m_3
m_4
$c_1\omega$
$c_2\omega$
$c_3\omega$
$c_4\omega$
π
ω
PHASH(m)

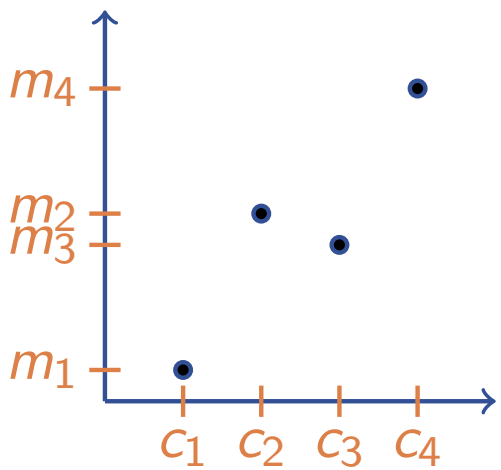

X^2

Approach

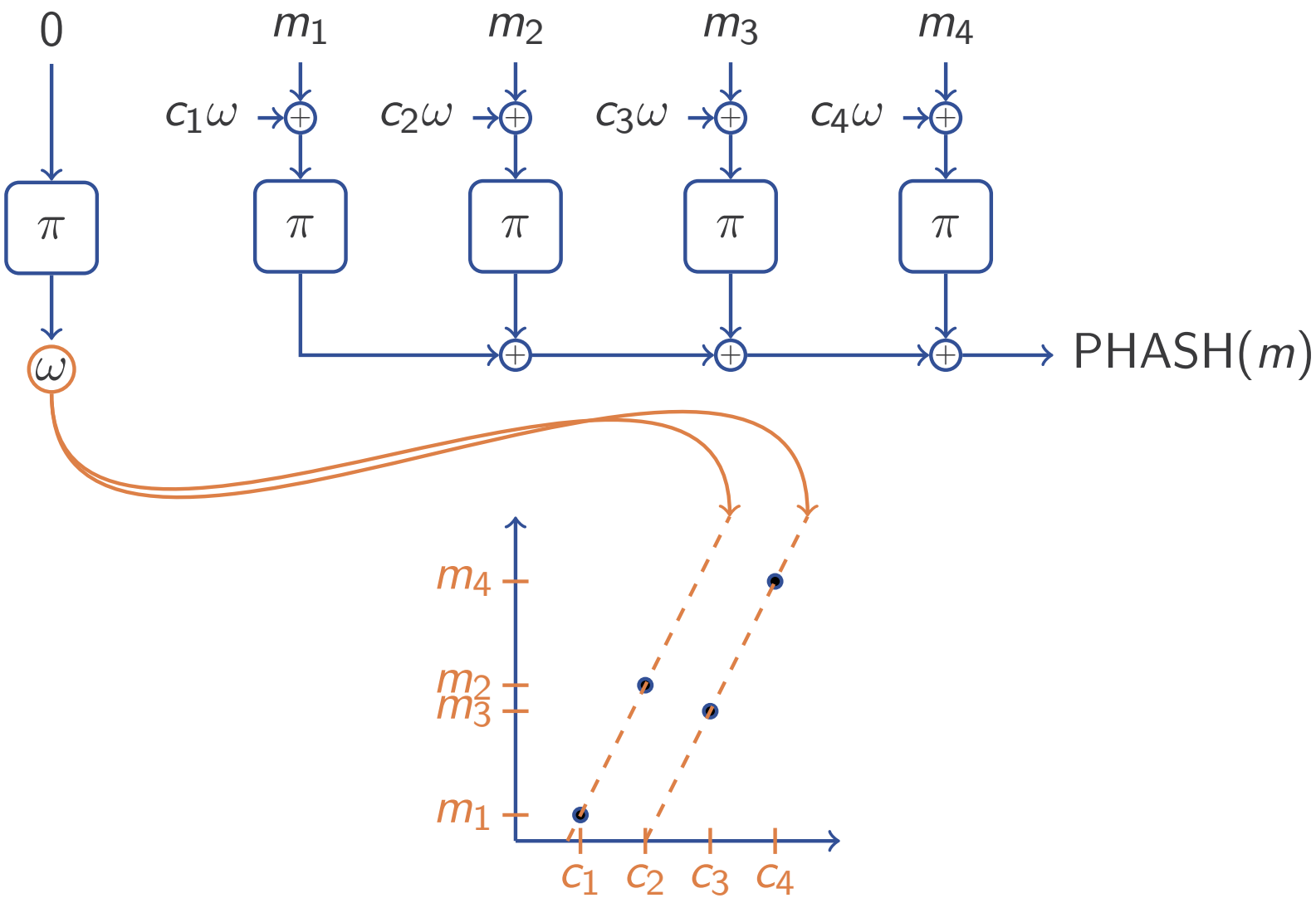

0
m_1
m_2
m_3
m_4
$c_1\omega$
$c_2\omega$
$c_3\omega$
$c_4\omega$
π
ω
PHASH(m)
m_1
c_1

Approach

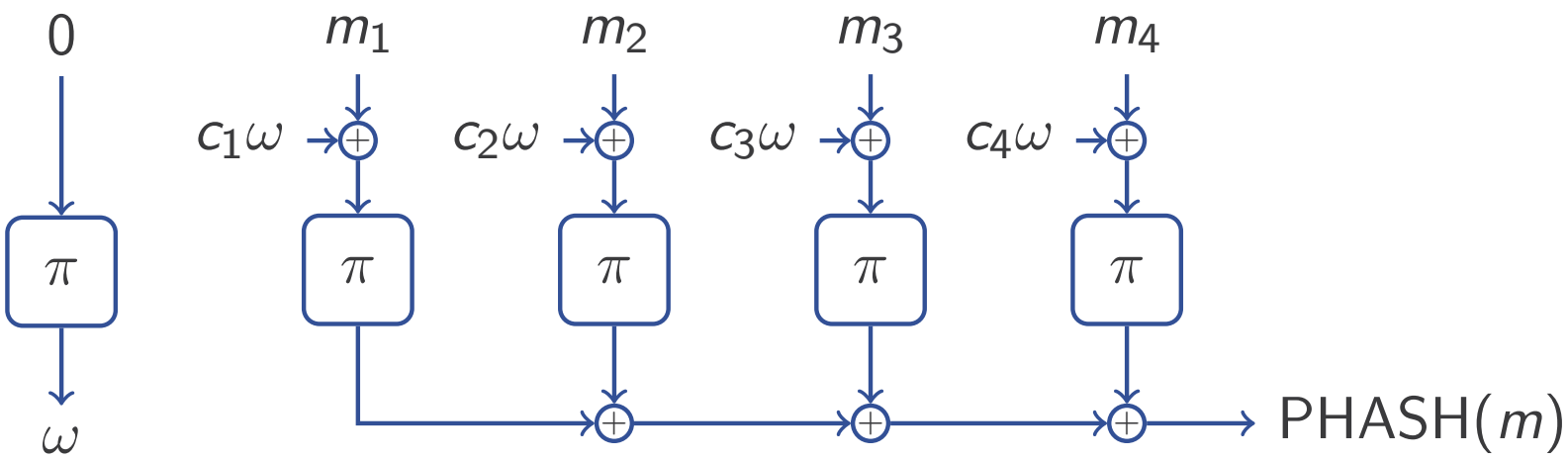

0
m_1
m_2
m_3
m_4
$c_1\omega$
$c_2\omega$
$c_3\omega$
$c_4\omega$
π
ω
PHASH(m)

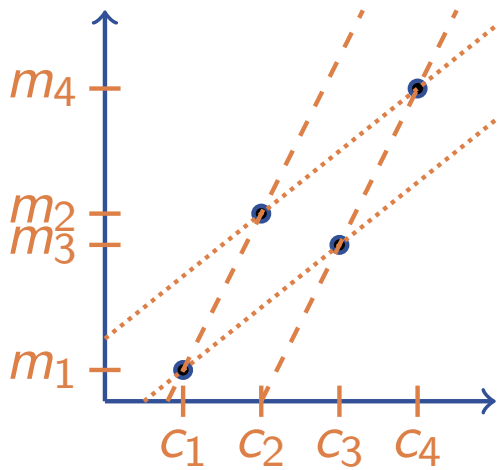

m_4
m_2
m_3
m_1
c_1
c_2
c_3
c_4

Approach


0
m_1
m_2
m_3
m_4
$c_1\omega$
$c_2\omega$
$c_3\omega$
$c_4\omega$
π
ω
PHASH(m)
m_4
m_2
m_3
m_1
c_1
c_2
c_3
c_4

Approach


0
m_1
m_2
m_3
m_4
$c_1\omega$
$c_2\omega$
$c_3\omega$
$c_4\omega$
π
ω
PHASH(m)


m_4
m_2
m_3
m_1
c_1
c_2
c_3
c_4

Conclusions and Open Problems

PMAC message length dependence is non-trivial

Conclusions and Open Problems

PMAC message length dependence is non-trivial

1. What happens with powering up?

Conclusions and Open Problems

PMAC message length dependence is non-trivial

1. What happens with powering up?
2. Optimal masks?

Conclusions and Open Problems

PMAC message length dependence is non-trivial

1. What happens with powering up?
2. Optimal masks?
3. Relationship between PMAC and PHASH when the output transform is not independent?

Conclusions and Open Problems

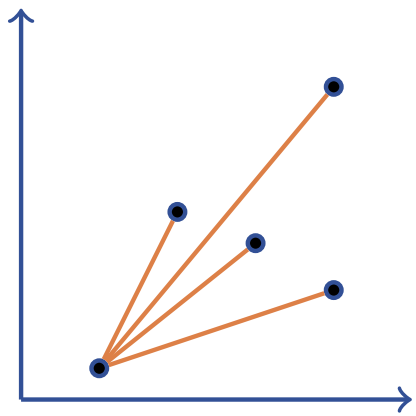
PMAC message length dependence is non-trivial

1. What happens with powering up?
2. Optimal masks?
3. Relationship between PMAC and PHASH when the output transform is not independent?

Thank you for your attention.

Connection With PHASH Collision Probability

Two messages $\vec{m}_1$ and $\vec{m}_2$ collide with probability $k/2^n$ if the corresponding set in X^2 is evenly covered by k slopes.
Simple proof of ℓ-bound:



Set Evenly Covered by Two Slopes

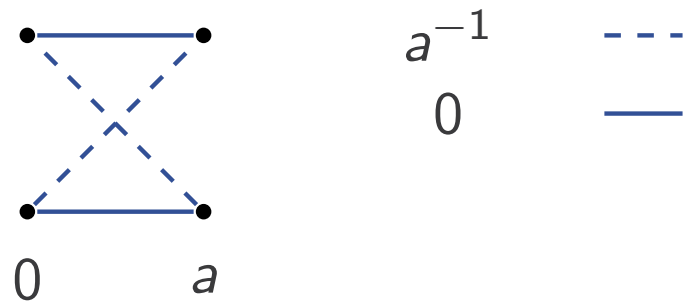


Figure: A set of four points evenly covered by the slopes 0 and a^{-1}. The x-coordinates of the points are 0 and a, and the y-coordinates are 0 and 1.

Guarantees a collision with probability $2/2^n$.

Set Evenly Covered by Three Slopes

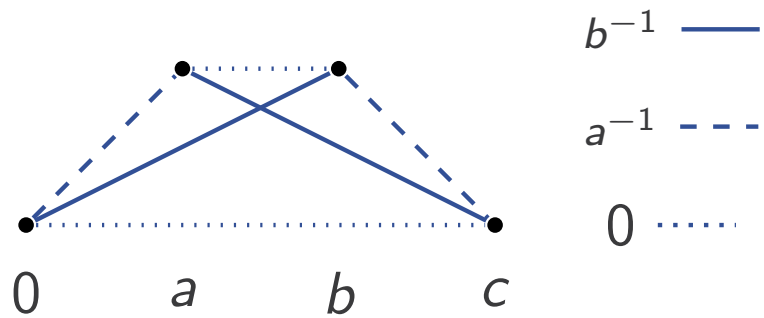


Figure: A set of four points evenly covered by the slopes 0, a^{-1}, and b^{-1}. The x-coordinates of the points are 0, a, b, and c, and the y-coordinates are 0 and 1.

Exists if and only if $a + b + c = 0$.

Another Set Evenly Covered by Three Slopes

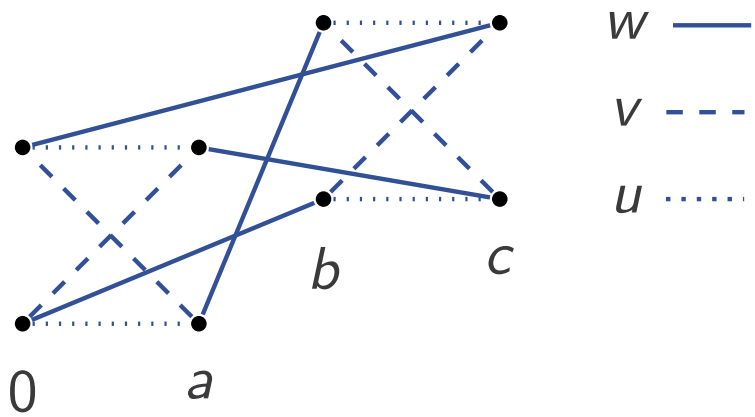


Figure: A set of points evenly covered by the slopes u, v, and w. Each point is accompanied by another point with the same x-coordinate. The x-coordinates of the pairs are indicated below the lower points.

Exists if and only if $a^2 + b^2 + c^2 + ab + ac = 0$.

Evenly Covered Sets in General

The x-coordinates of evenly covered sets satisfy one of the following:

1. They contain a subset summing to zero (NP-complete)
2. They are the solution to a non-trivial binary quadratic form (similar problem NP-complete)

Conjecture

Given $S \subset X$, finding a subset of S satisfying either of the above requirements is computationally hard.

Searching for Evenly Covered Sets

Proposition

An evenly covered set with distinct x-coordinates forms a complete graph if and only if the x-coordinates are an additive subgroup of X.

1. For sufficiently long messages, the masks will always contain an additive subgroup
2. Finding additive subgroups in Gray codes is easy for every power of two.

Success probability of Gray code attack:

$$\frac{2^{k-1}-1}{2^n} \text{ for } \ell = 2^k$$