The Landscape of Committing Authenticated Encryption

Mihir Bellare
UC San Diego

Viet Tung Hoang
Florida State University

Cong Wu
Florida State University

NIST Workshop 2023— October 3, 2023

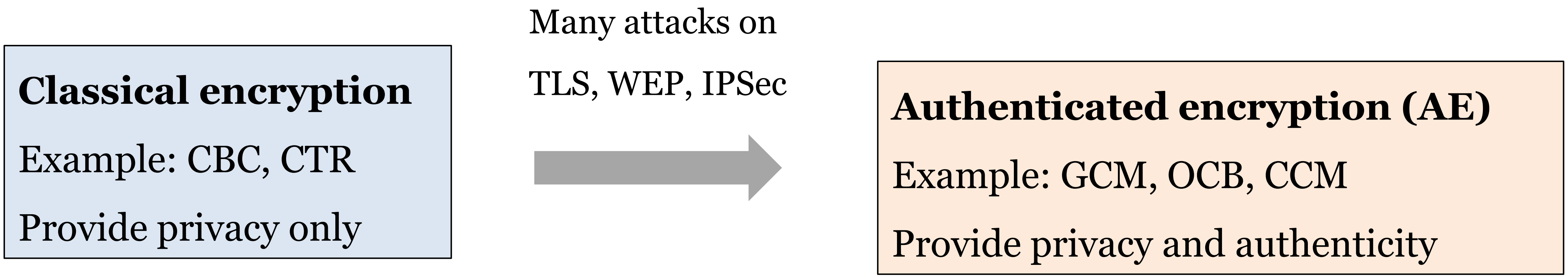
What Kind of Security Should Encryption Offer?

Classical encryption

Example: CBC, CTR

Provide privacy only

What Kind of Security Should Encryption Offer?



Classical encryption

Example: CBC, CTR

Provide privacy only

Many attacks on

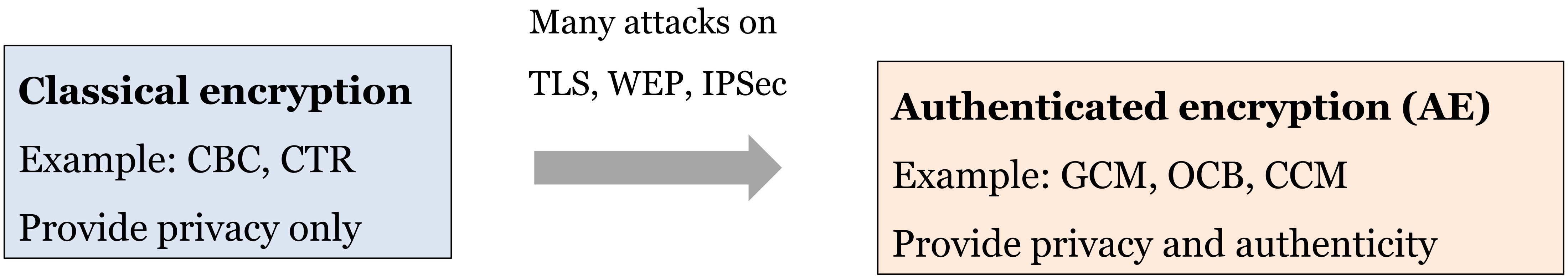
TLS, WEP, IPSec

Authenticated encryption (AE)

Example: GCM, OCB, CCM

Provide privacy and authenticity

What Kind of Security Should Encryption Offer?



Classical encryption

Example: CBC, CTR

Provide privacy only

Many attacks on

TLS, WEP, IPSec

Authenticated encryption (AE)

Example: GCM, OCB, CCM

Provide privacy and authenticity

Many recent attacks show that privacy and authenticity are **not enough**

What Kind of Security Should Encryption Offer?

Classical encryption

Example: CBC, CTR

Provide privacy only

Many attacks on

TLS, WEP, IPSec

→

Authenticated encryption (AE)

Example: GCM, OCM, CCM

Provide privacy and authenticity

Many recent attacks show that privacy and authenticity are **not enough**

Message franking

aws

Amazon Clo

OPAQUE

pw-based key exchange

Googl

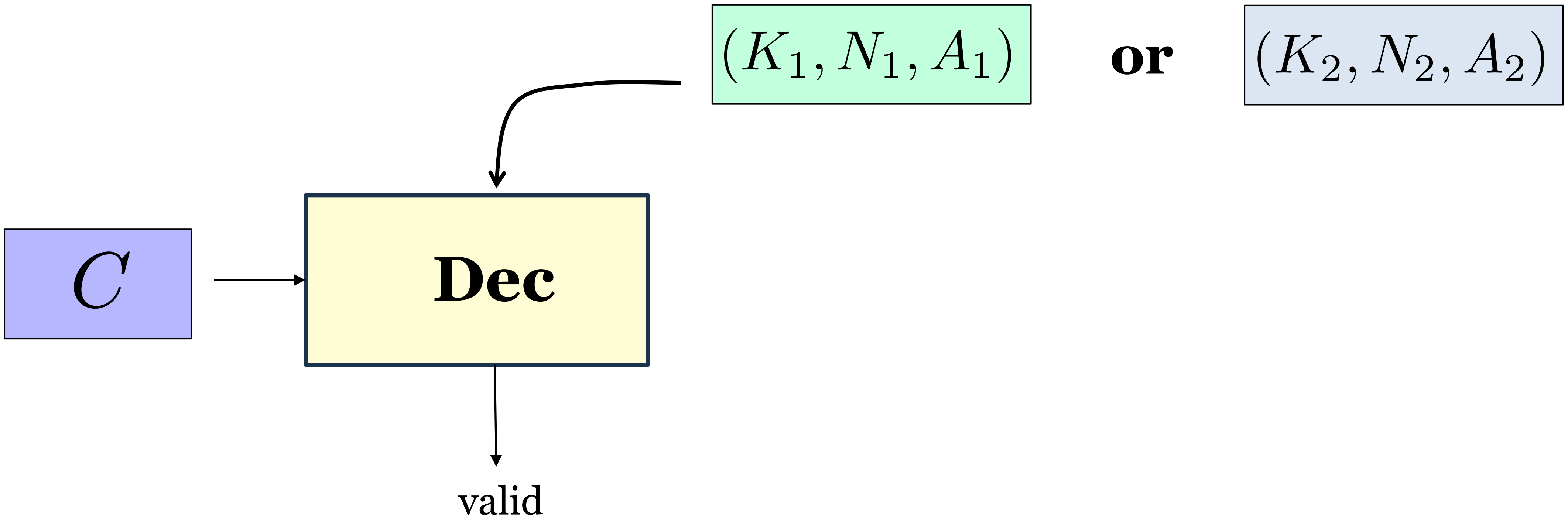
bscribe with Go

Shadowsocks

VPN

What We Need: Committing Security

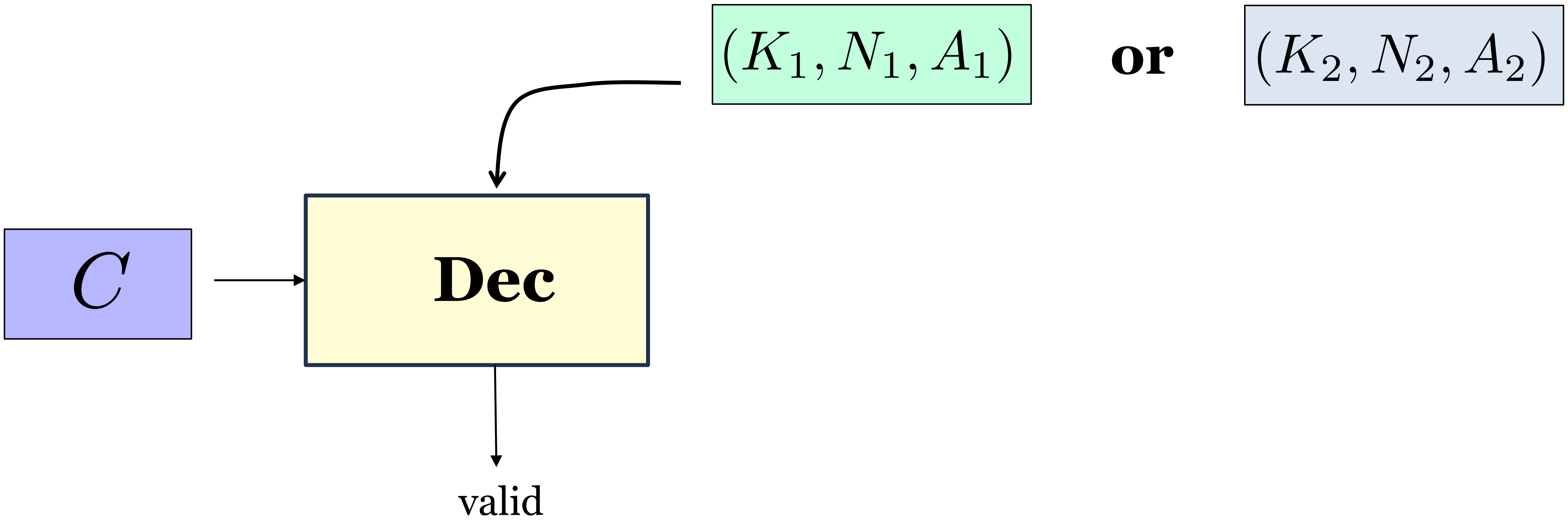
[FOR17]



Intuition: A ciphertext cannot be opened properly under two different contexts (possibly to different messages)

What We Need: Committing Security

[FOR17]



(K_1, N_1, A_1) **or** (K_2, N_2, A_2)

C

Dec

valid

Intuition: A ciphertext cannot be opened properly under two different contexts (possibly to different messages)

Not supported by standard encryption schemes

A Hierarchy of Committing Definitions

[BH22]

App: Facebook's message franking

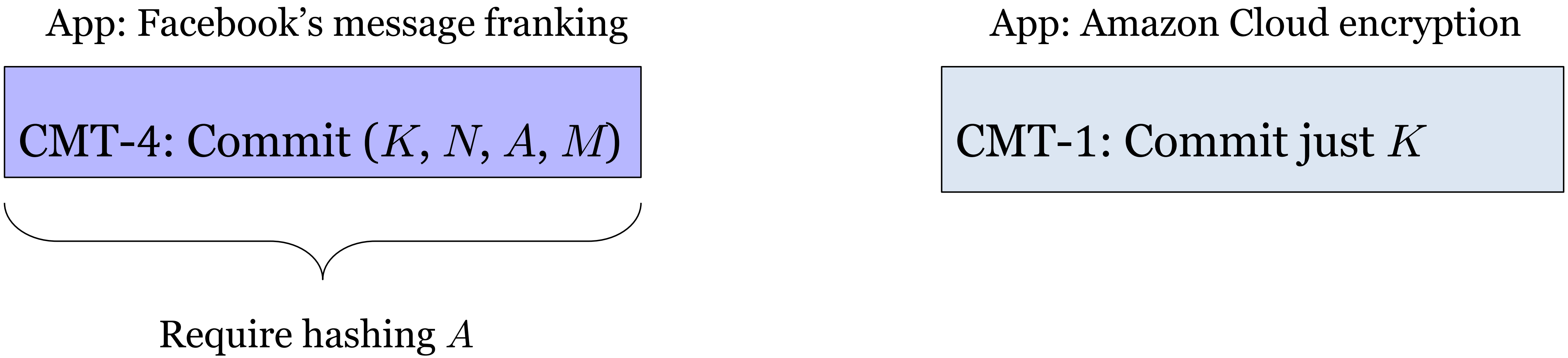
CMT-4: Commit (K, N, A, M)

App: Amazon Cloud encryption

CMT-1: Commit just K

A Hierarchy of Committing Definitions

[BH22]



App: Facebook's message franking

CMT-4: Commit (K, N, A, M)

Require hashing A

App: Amazon Cloud encryption

CMT-1: Commit just K

A Hierarchy of Committing Definitions

[BH22]

App: Facebook's message franking

CMT-4: Commit (K, N, A, M)

Require hashing A

App: Amazon Cloud encryption

CMT-1: Commit just K

Question #1: Why two notions? Doesn't CMT-4 subsume CMT-1?

A Hierarchy of Committing Definitions

[BH22]

App: Facebook's message franking

$$\underbrace{\text{CMT-4: Commit } (K,\ N,\ A,\ M)}_{\text{Require hashing } A}$$

App: Amazon Cloud encryption

CMT-1: Commit just K

Question #1: Why two notions? Doesn't CMT-4 subsume CMT-1?

Hashing is costly, even for short AD. Most apps only need CMT-1.

A Hierarchy of Committing Definitions

[BH22]

App: Facebook's message franking

CMT-4: Commit (K, N, A, M)

Require hashing A

App: Amazon Cloud encryption

CMT-1: Commit just K

Question #1: Why two notions? Doesn't CMT-4 subsume CMT-1?

Hashing is costly, even for short AD. Most apps only need CMT-1.

Question #2: Is birthday-bound security (64 bits) enough?

A Hierarchy of Committing Definitions

[BH22]

App: Facebook's message franking

CMT-4: Commit (K, N, A, M)

Require hashing A

App: Amazon Cloud encryption

CMT-1: Commit just K

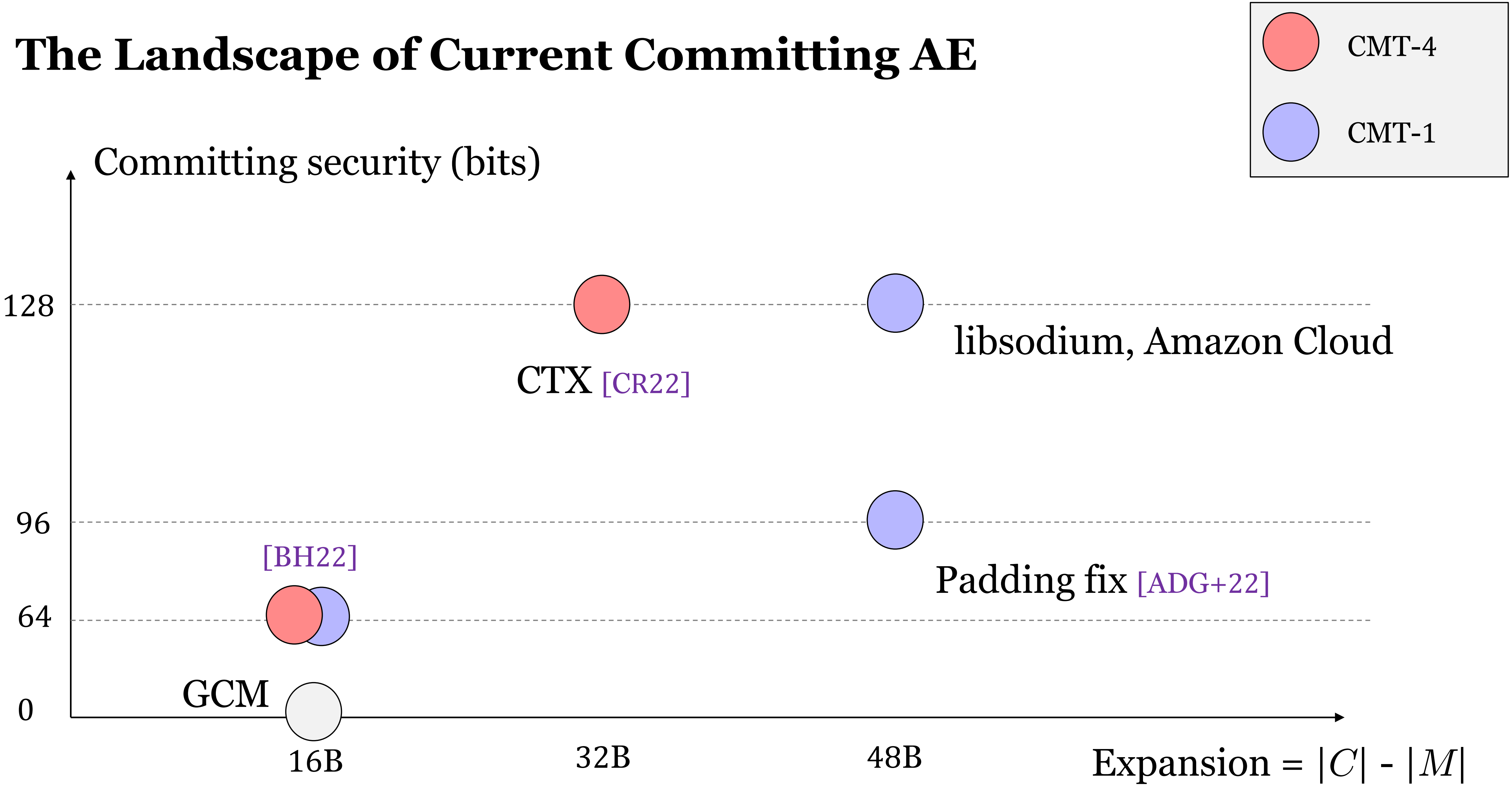
Question #1: Why two notions? Doesn't CMT-4 subsume CMT-1?

Hashing is costly, even for short AD. Most apps only need CMT-1.

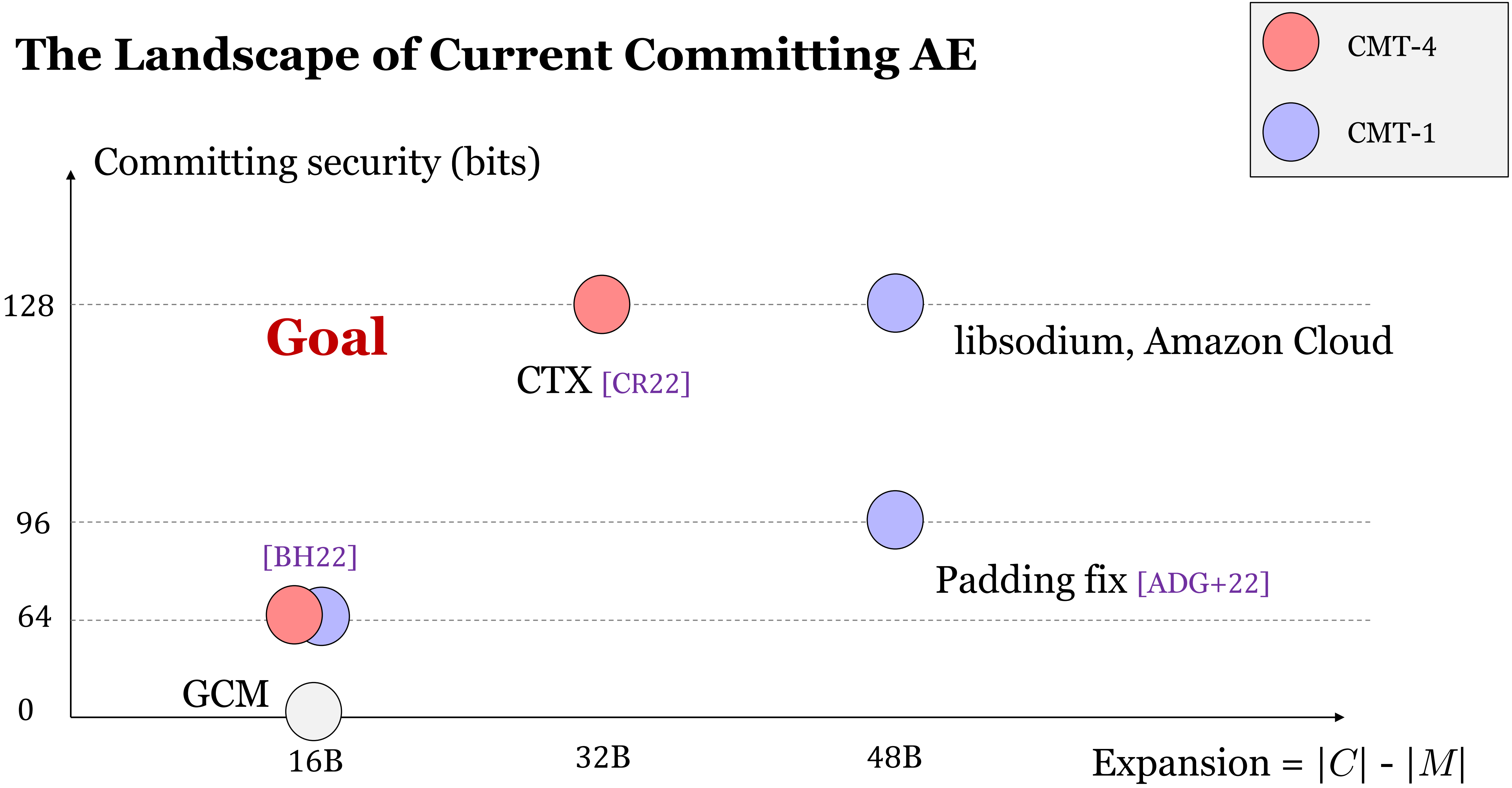
Question #2: Is birthday-bound security (64 bits) enough?

No, here attacks are offline. Should go close to 128-bit security.

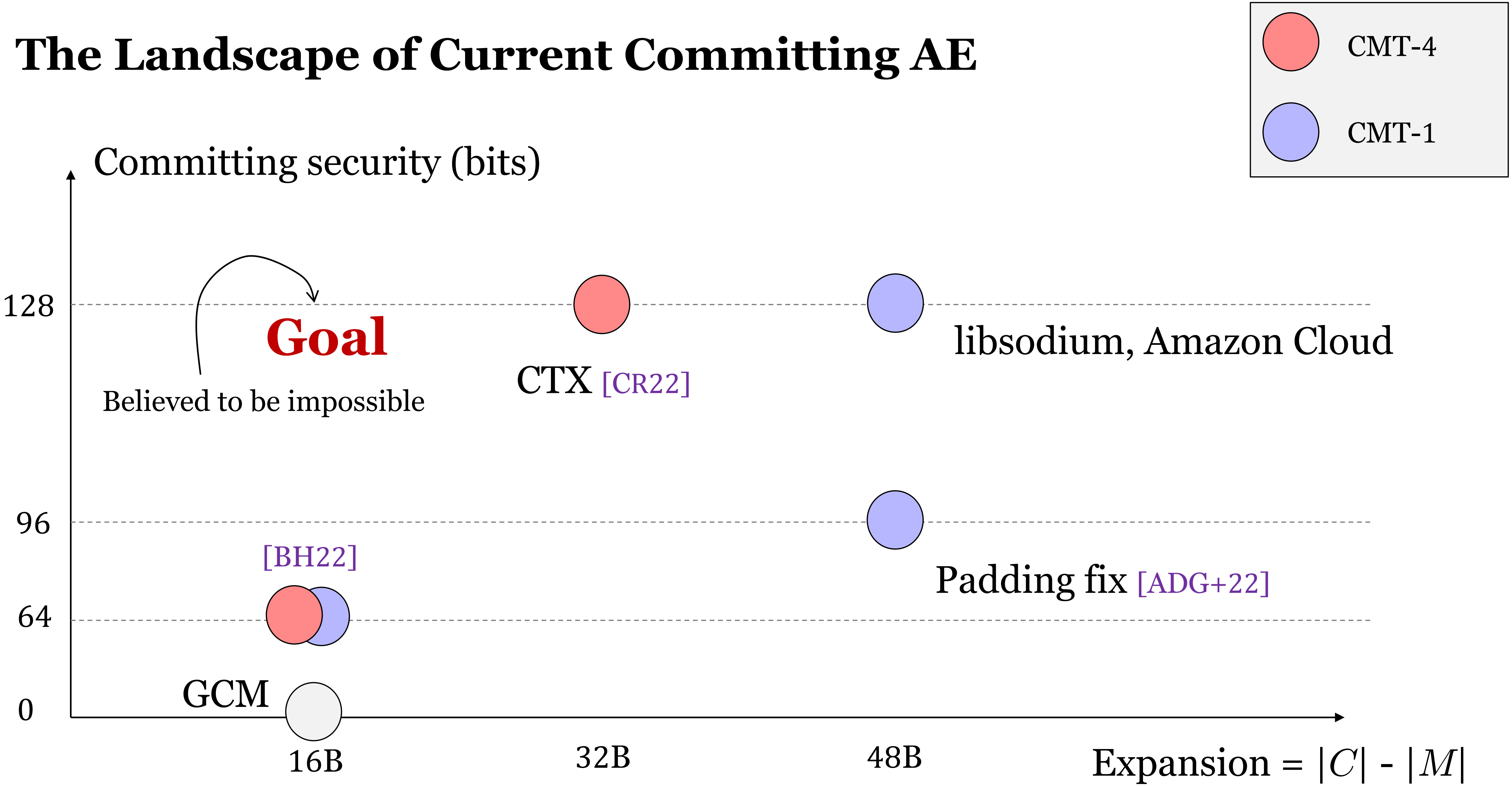
The Landscape of Current Committing AE



The Landscape of Current Committing AE



The Landscape of Current Committing AE

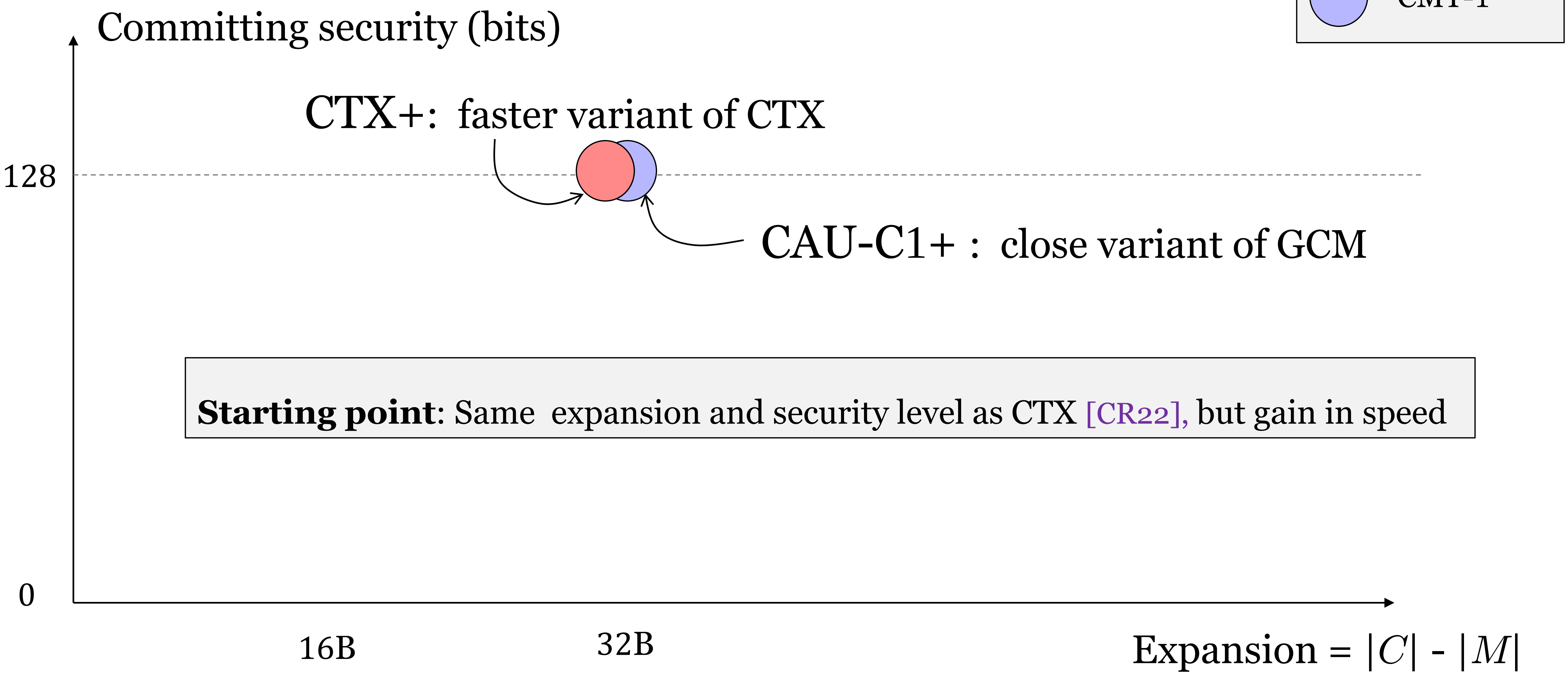


Our Work: Achieve The Goal Efficiently

[BHW23]

🔴 CMT-4

🔵 CMT-1



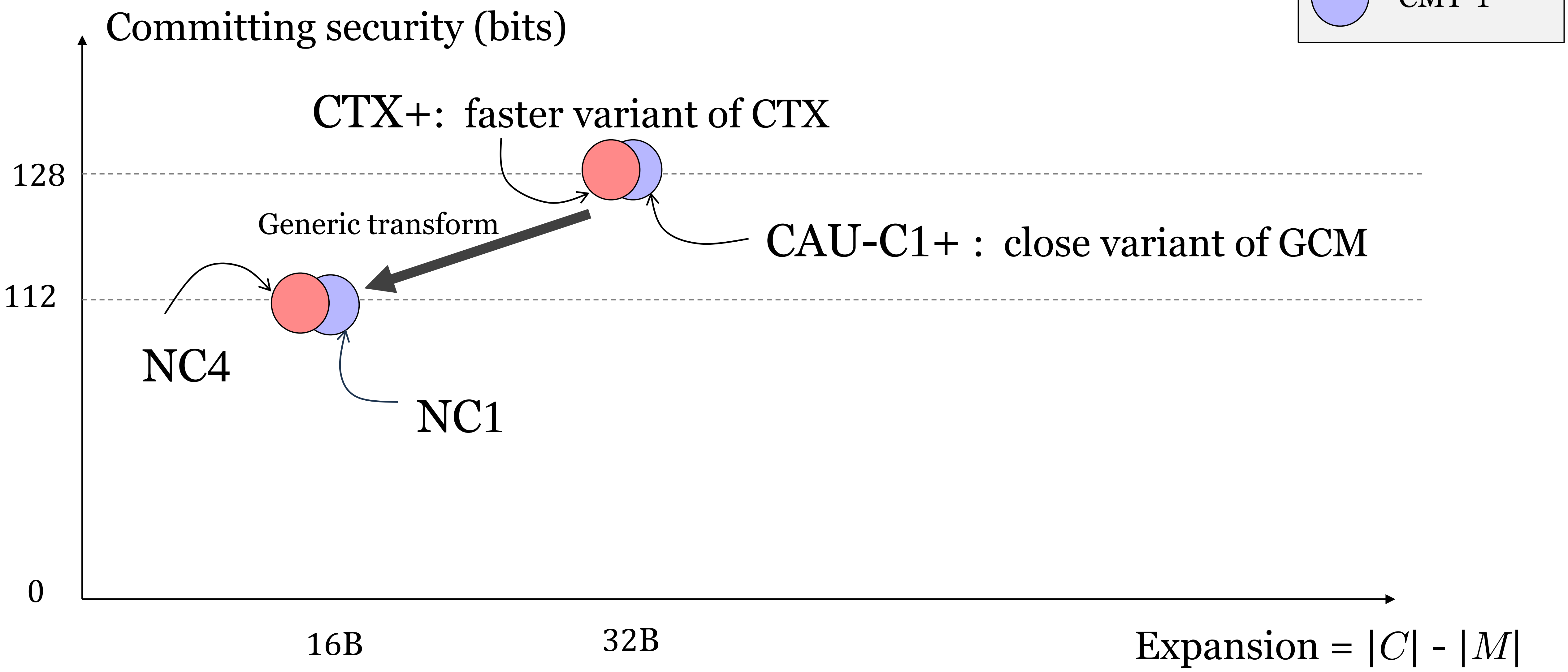
CTX+: faster variant of CTX

CAU-C1+ : close variant of GCM

Starting point: Same expansion and security level as CTX [CR22], but gain in speed

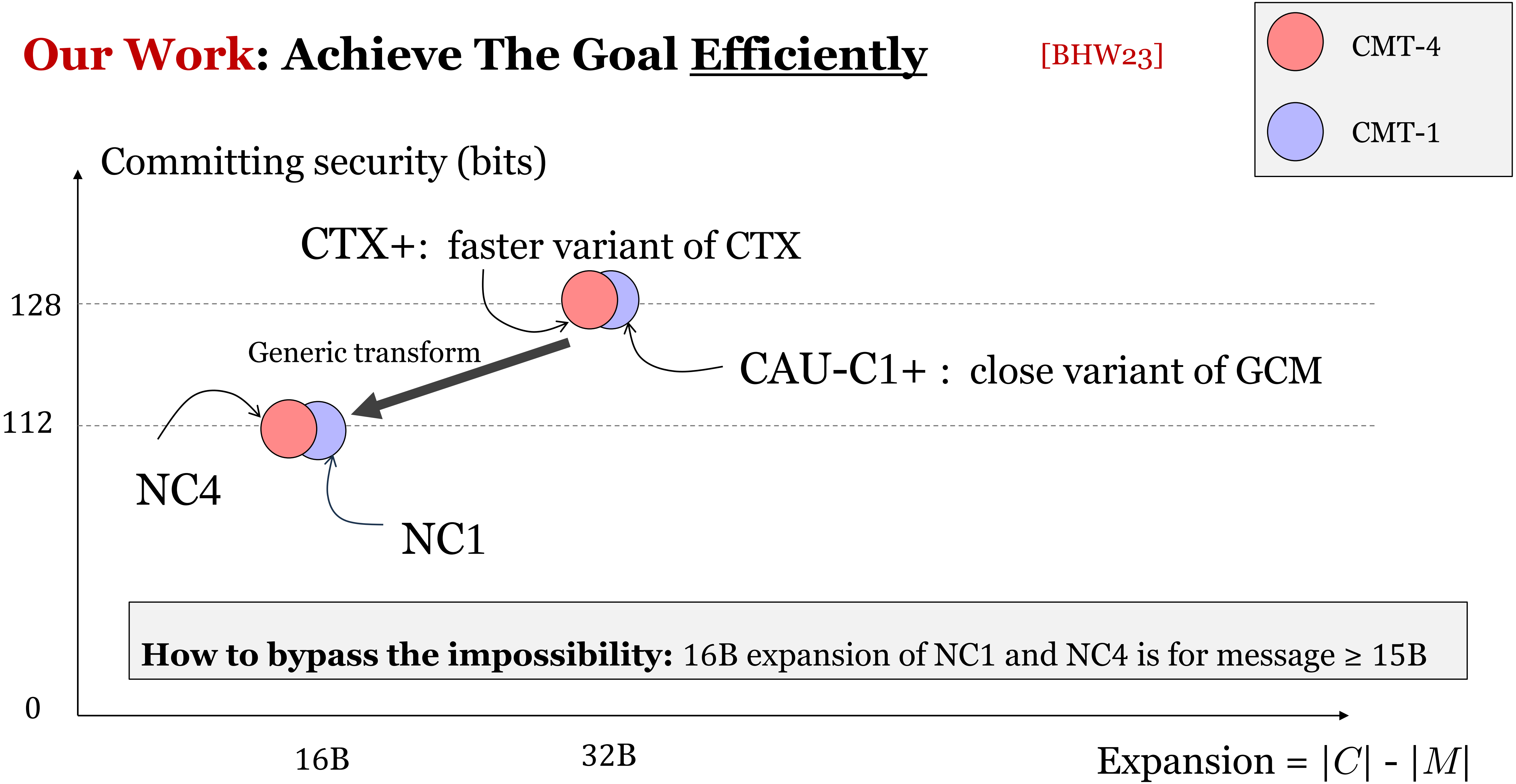
Our Work: Achieve The Goal Efficiently

[BHW23]



Our Work: Achieve The Goal Efficiently

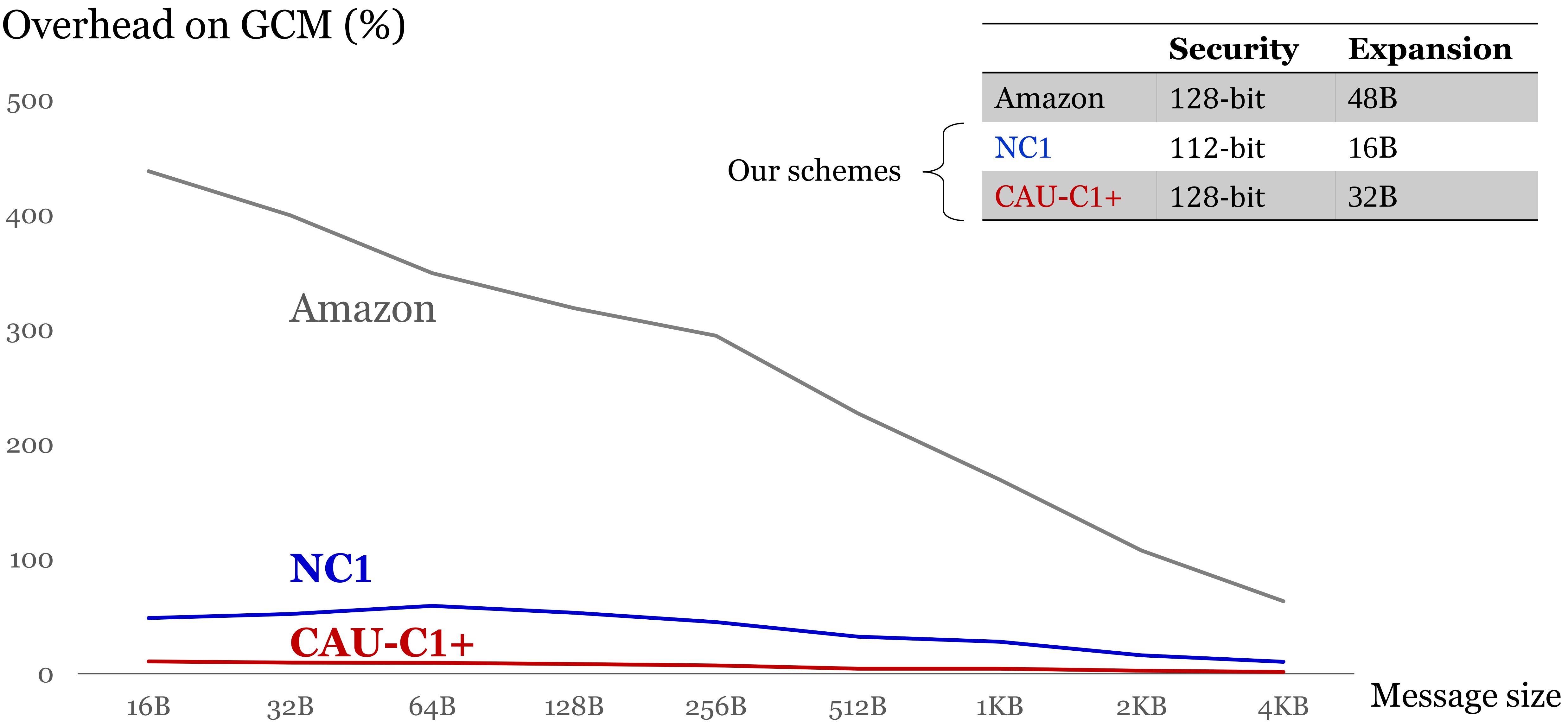
[BHW23]



How to bypass the impossibility: 16B expansion of NC1 and NC4 is for message ≥ 15B

Speed Comparison: CMT-1 Schemes

Intel Xeon Gold 6240
5B AD

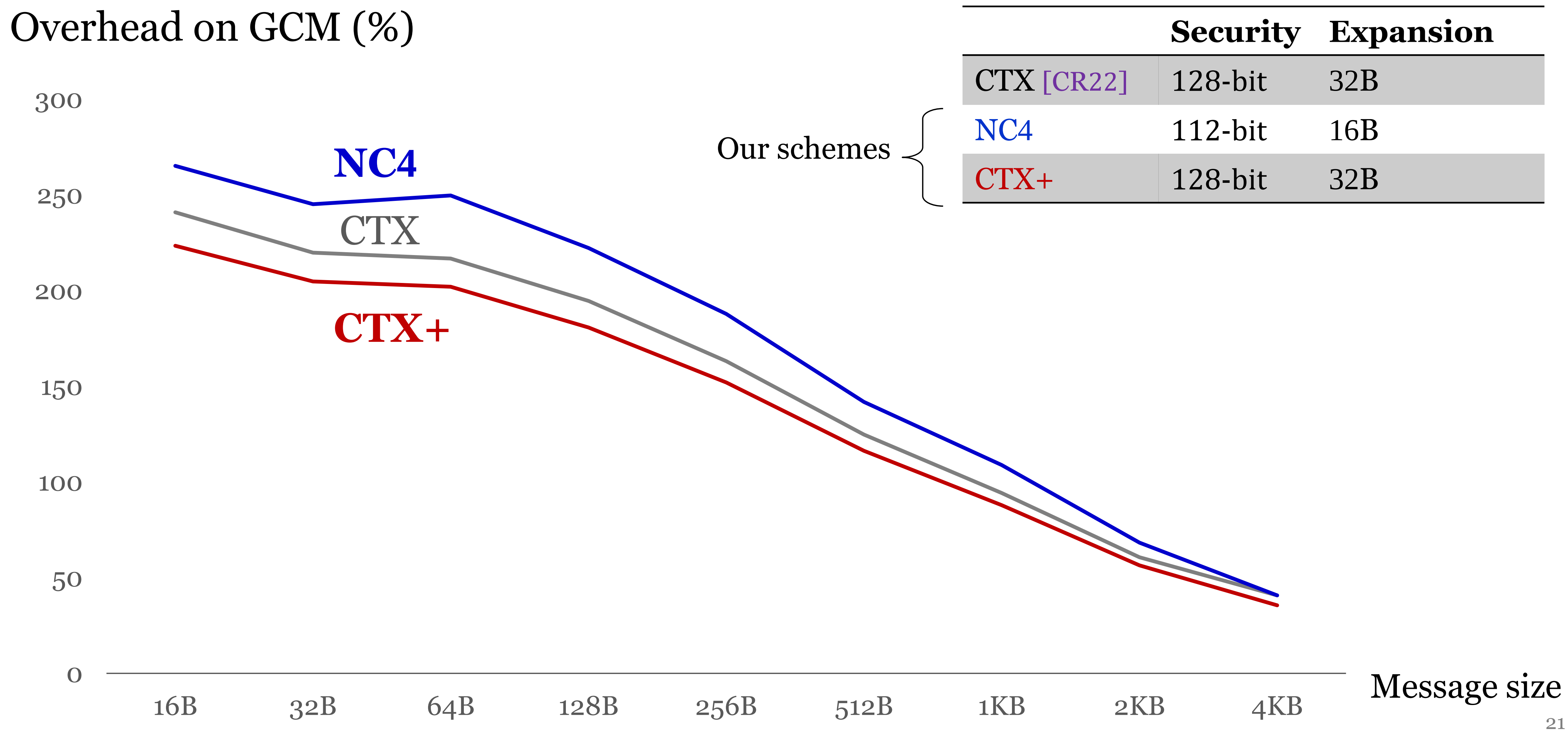


Our schemes

	Security	Expansion
Amazon	128-bit	48B
NC1	112-bit	16B
CAU-C1+	128-bit	32B

Speed Comparison: CMT-4 Schemes

Intel Xeon Gold 6240
5B AD



	Security	Expansion
CTX [CR22]	128-bit	32B
NC4	112-bit	16B
CTX+	128-bit	32B

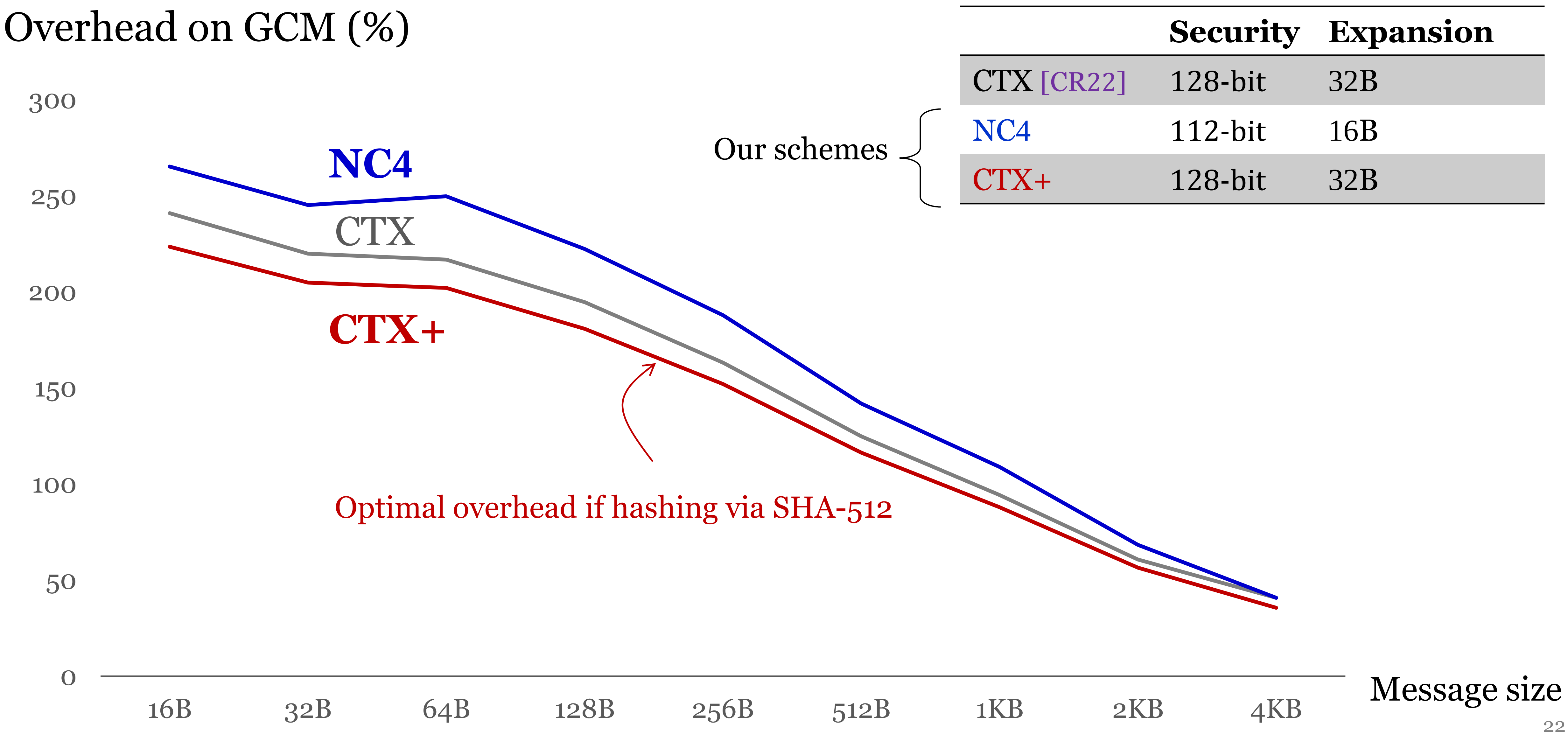
Our schemes: NC4, CTX+

Speed Comparison: CMT-4 Schemes

Intel Xeon Gold 6240
5B AD

	Security	Expansion
CTX [CR22]	128-bit	32B
NC4	112-bit	16B
CTX+	128-bit	32B

Our schemes

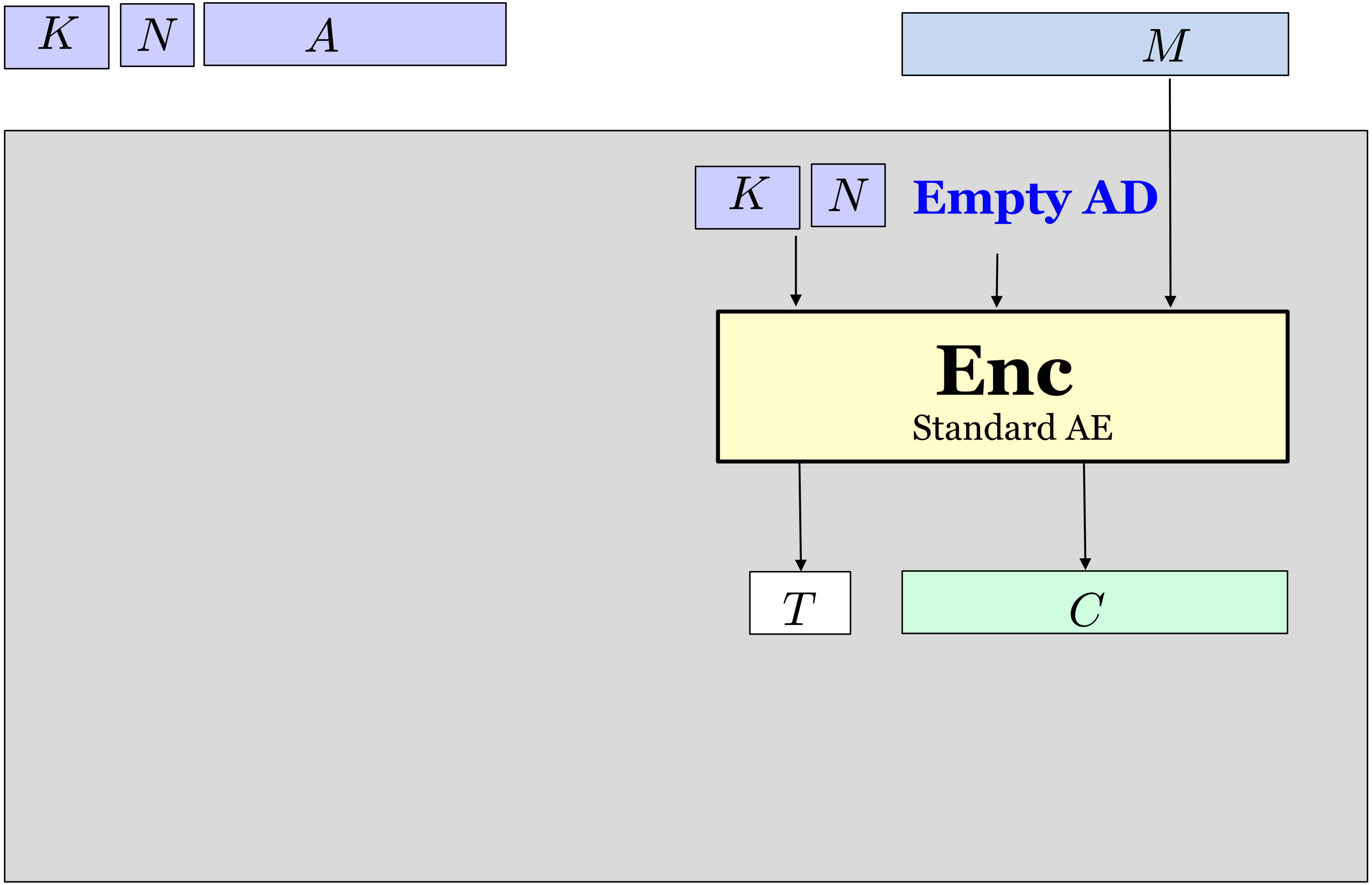


Optimal overhead if hashing via SHA-512

Achieving CMT-4 Security: The CTX+ Transform

[BHW23]

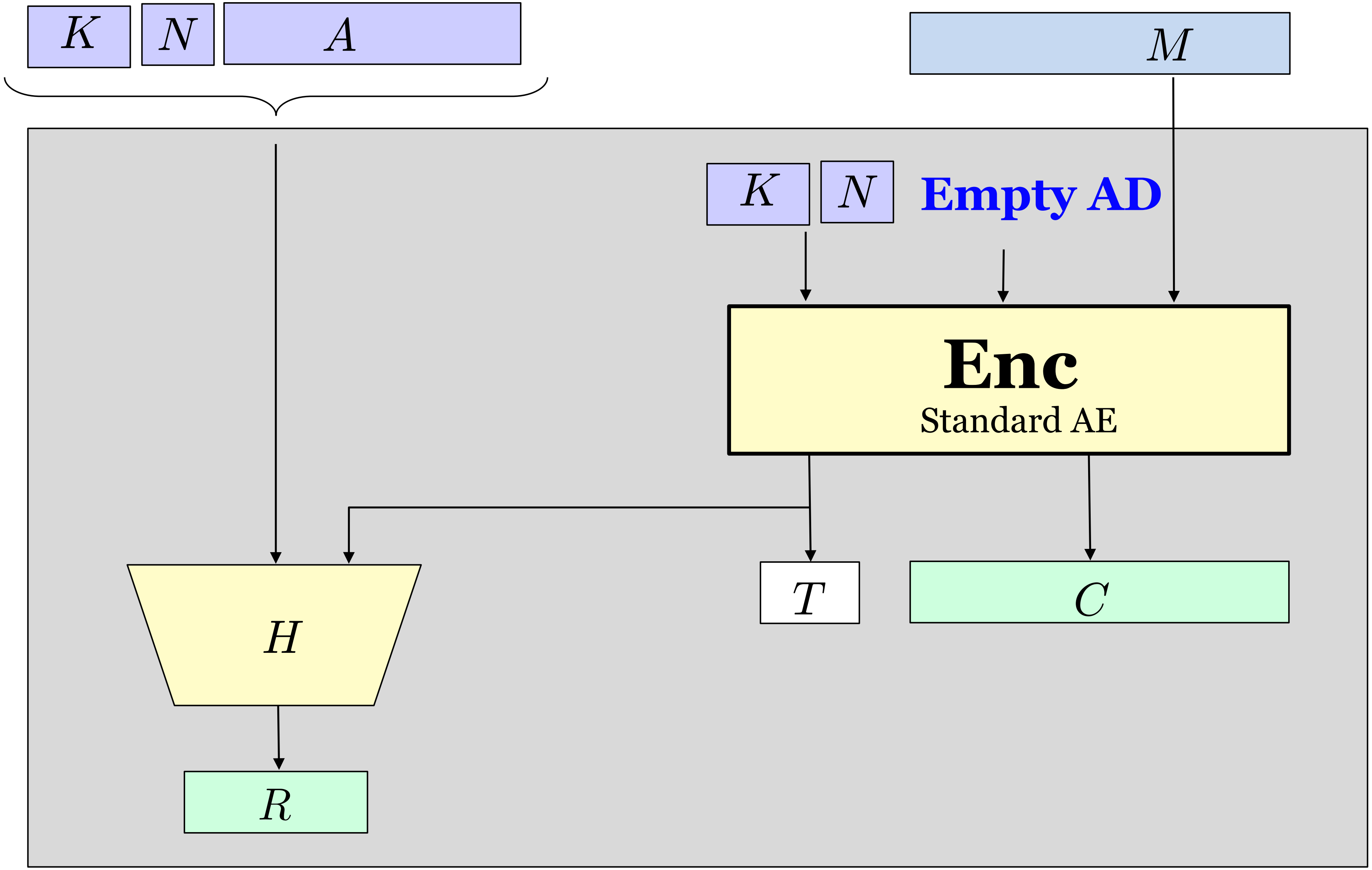
Faster variant of CTX [CR22]



Achieving CMT-4 Security: The CTX+ Transform

[BHW23]

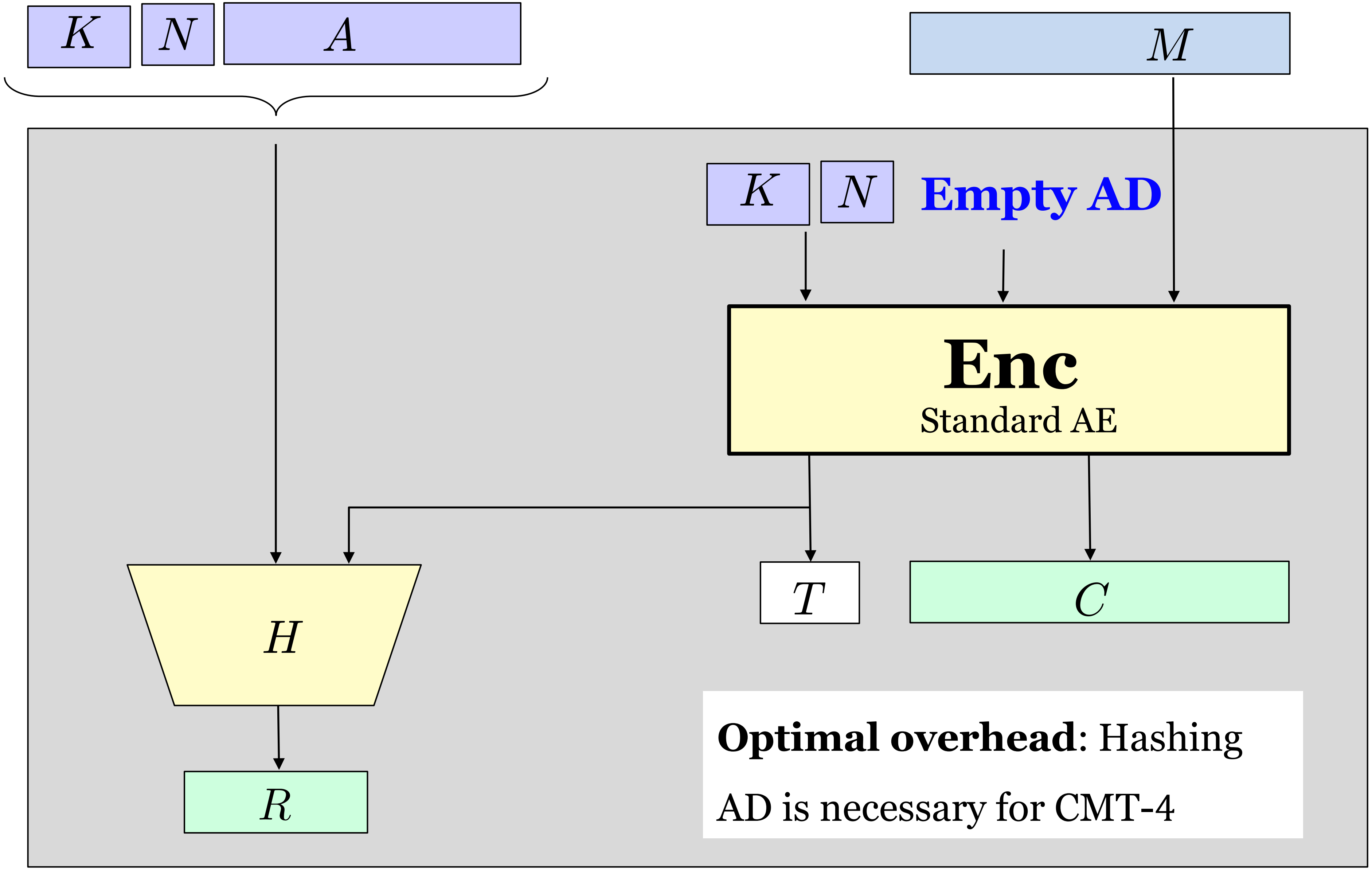
Faster variant of CTX [CR22]



Achieving CMT-4 Security: The CTX+ Transform

[BHW23]

Faster variant of CTX [CR22]



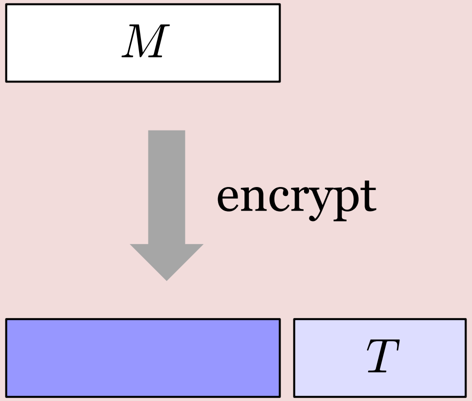
Optimal overhead: Hashing

AD is necessary for CMT-4

How To Reduce Ciphertext Expansion?

Common View

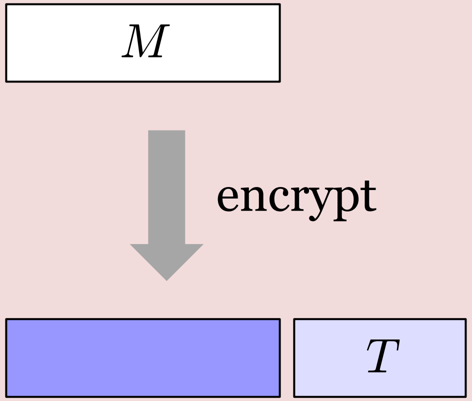
Commitment = Tag



How To Reduce Ciphertext Expansion?

Common View

Commitment = Tag



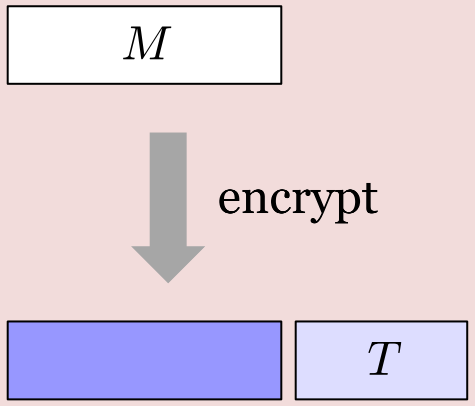
Birthday attack: $|T| \geq 256$

How To Reduce Ciphertext Expansion?

[BHW23]

Common View

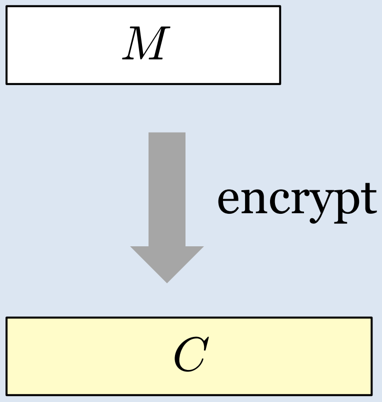
Commitment = Tag



Birthday attack: $|T| \geq 256$

Our View

Commitment = Whole ciphertext

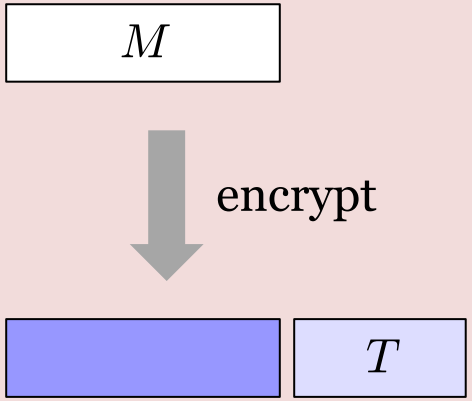


How To Reduce Ciphertext Expansion?

[BHW23]

Common View

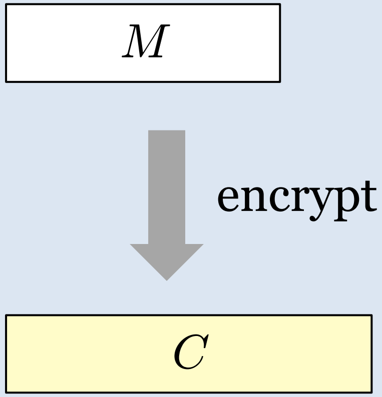
Commitment = Tag



Birthday attack: $|T| \geq 256$

Our View

Commitment = Whole ciphertext



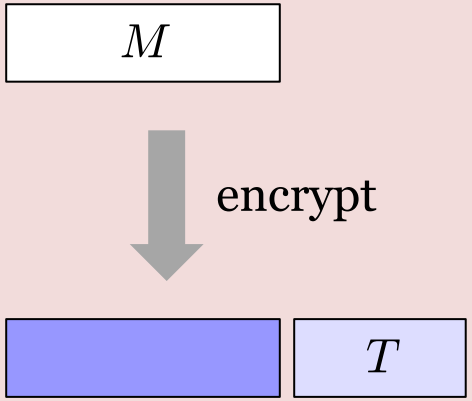
Birthday attack: $|C| \geq 256$

How To Reduce Ciphertext Expansion?

[BHW23]

Common View

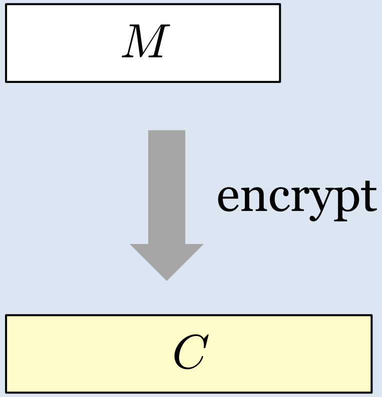
Commitment = Tag



Birthday attack: $|T| \geq 256$

Our View

Commitment = Whole ciphertext



Birthday attack: $|C| \geq 256$

Expansion is $\max\{256 - |M|, 128\}$

A Stepping Stone: Committing Concealer

[BHW23]

A special-purpose committing AE

Conventional AE

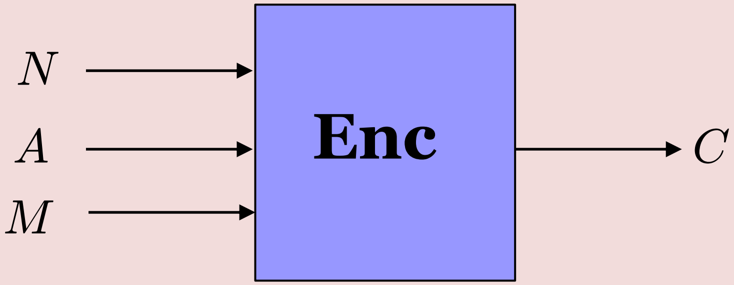
Committing Concealer

A Stepping Stone: Committing Concealer

[BHW23]

A special-purpose committing AE

Conventional AE



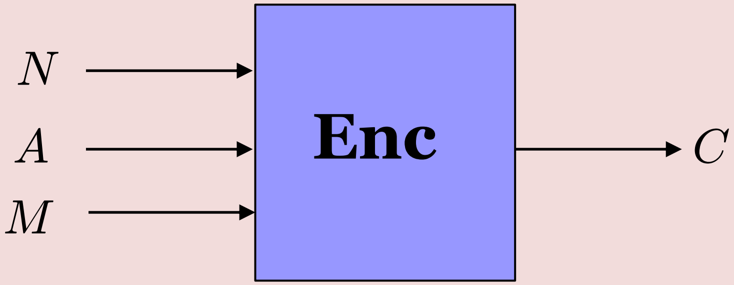
Committing Concealer

A Stepping Stone: Committing Concealer

[BHW23]

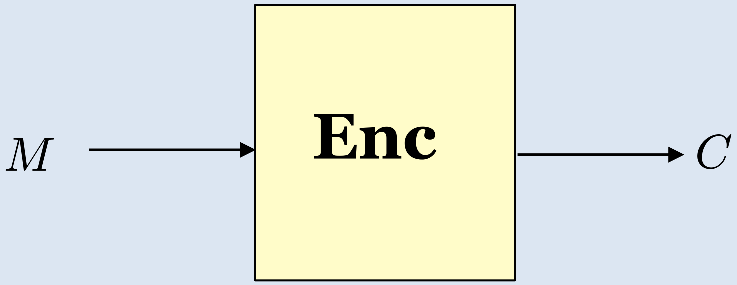
A special-purpose committing AE

Conventional AE



Committing Concealer

No nonce and AD

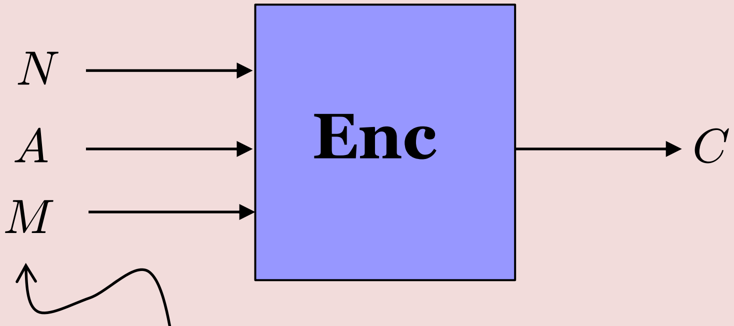


A Stepping Stone: Committing Concealer

[BHW23]

A special-purpose committing AE

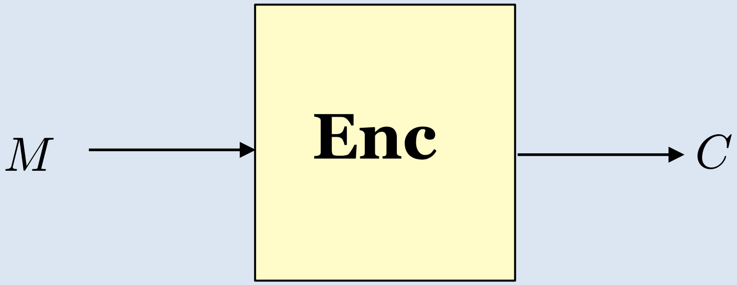
Conventional AE



arbitrary

Committing Concealer

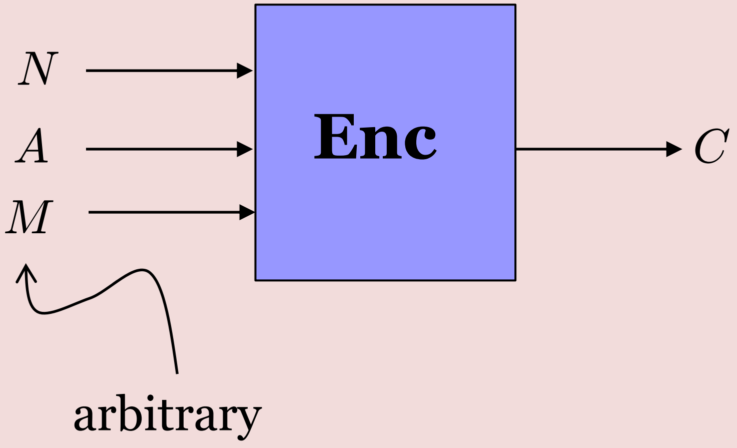
No nonce and AD



A Stepping Stone: $\underbrace{\text{Committing Concealer}}_{\text{A special-purpose committing AE}}$

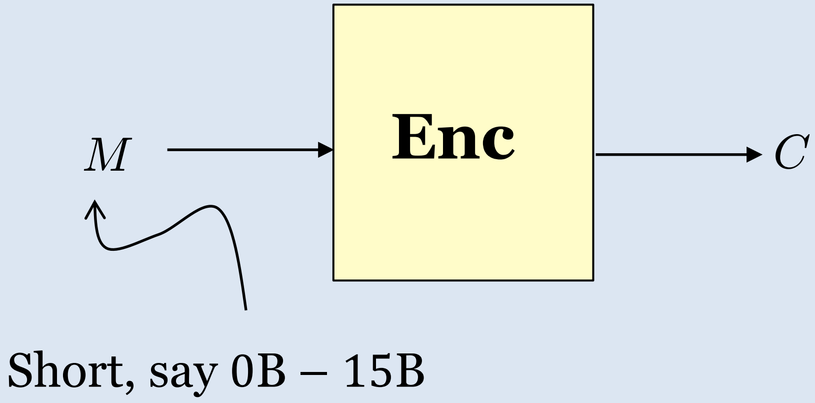
[BHW23]

Conventional AE



Committing Concealer

No nonce and AD

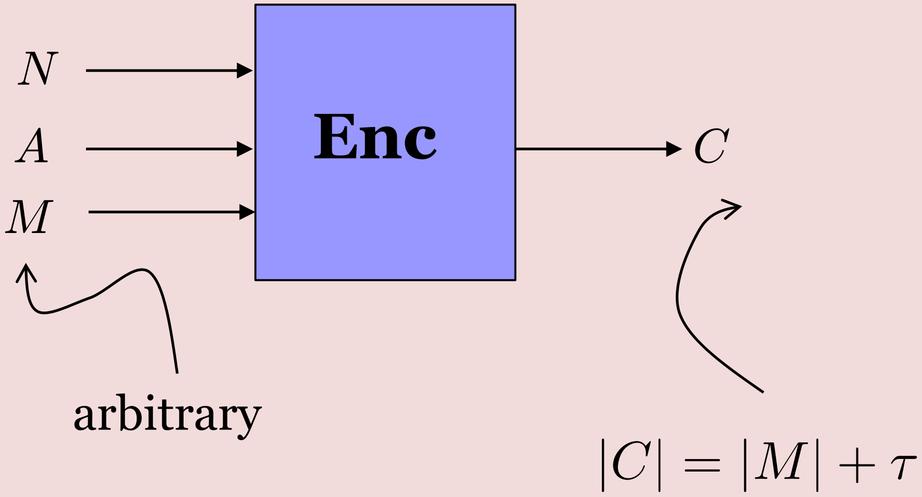


A Stepping Stone: Committing Concealer

[BHW23]

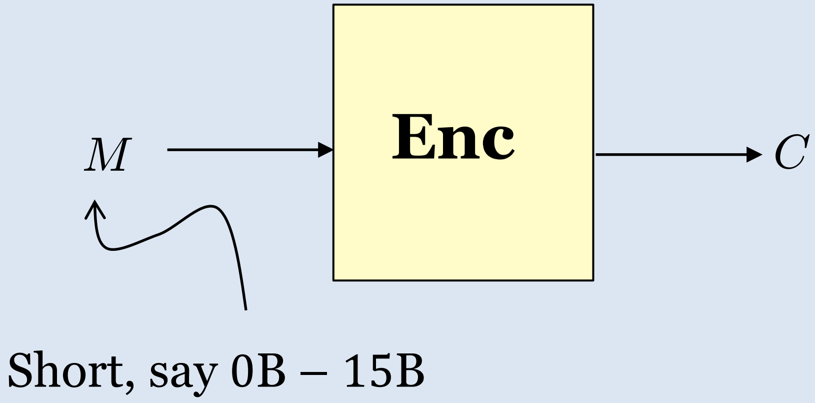
A special-purpose committing AE

Conventional AE



Committing Concealer

No nonce and AD

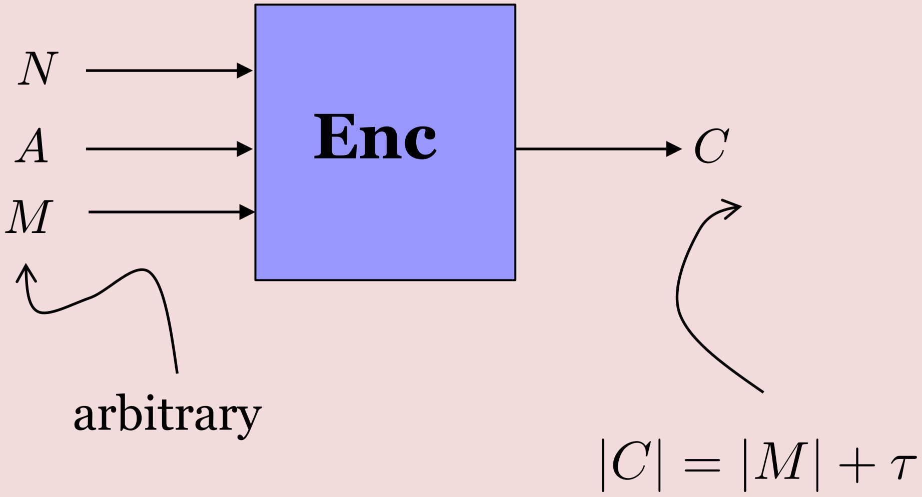


A Stepping Stone: Committing Concealer

[BHW23]

A special-purpose committing AE

Conventional AE

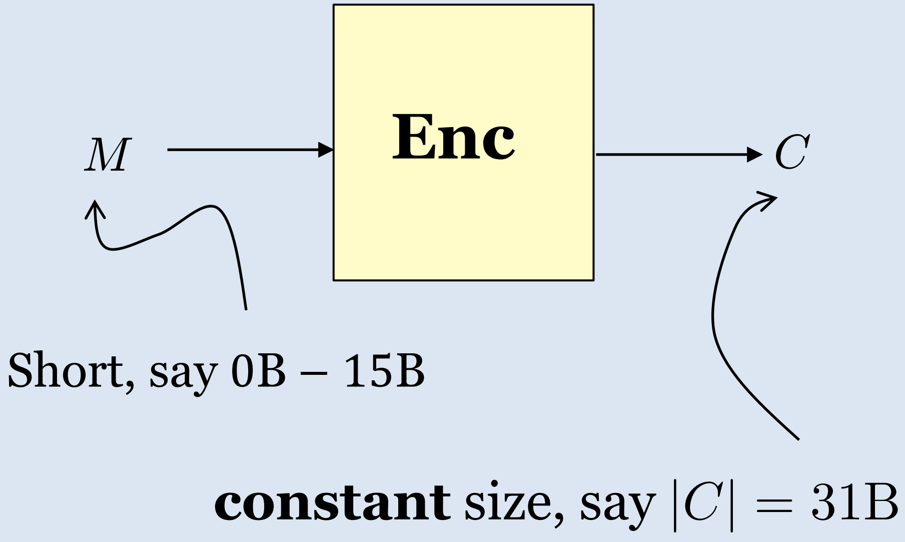


arbitrary

$|C| = |M| + \tau$

Committing Concealer

No nonce and AD



Short, say 0B – 15B

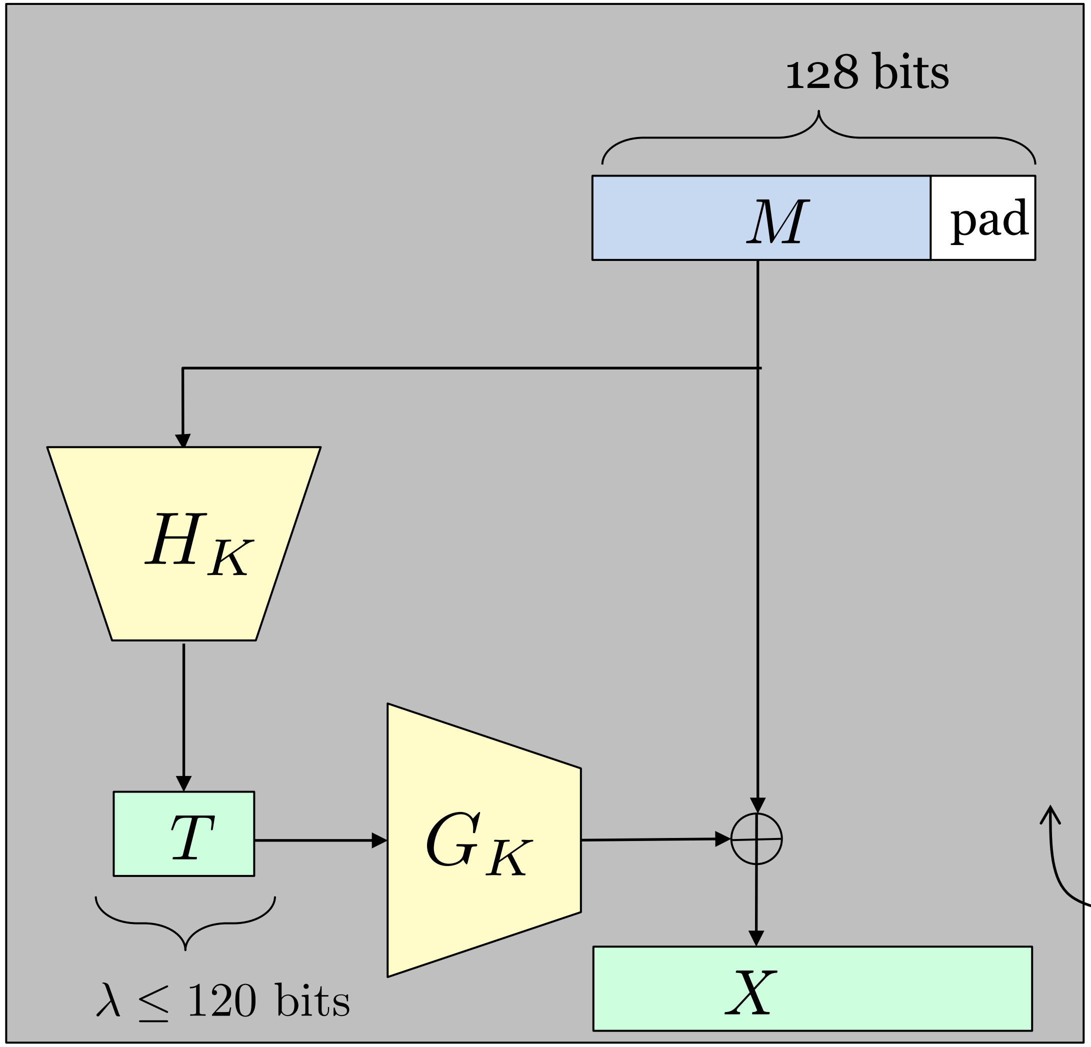
constant size, say $|C| = 31\text{B}$

Building Committing Concealer

The Hash-then-Mask (HtM) Construction

[BHW23]

The HtM construction, conceptual view

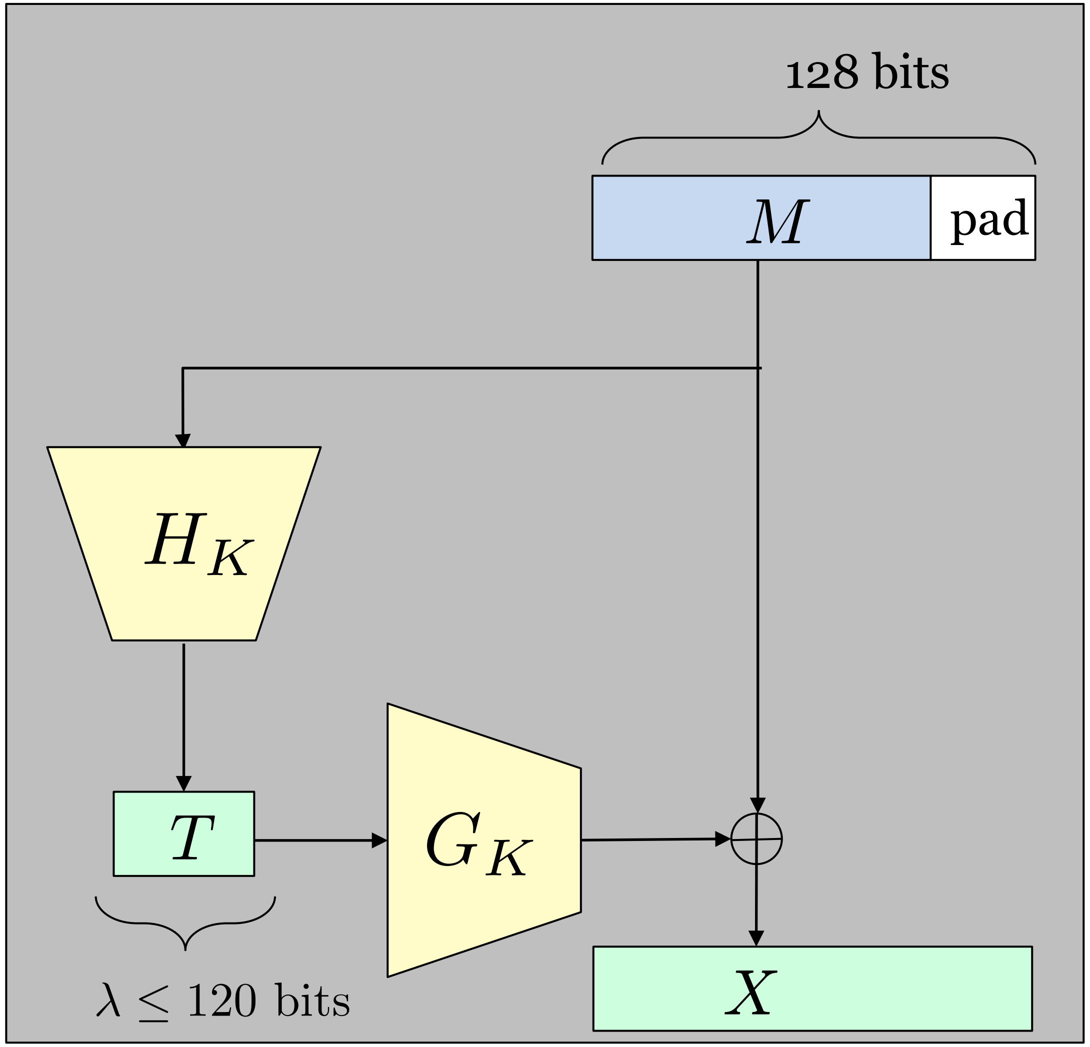


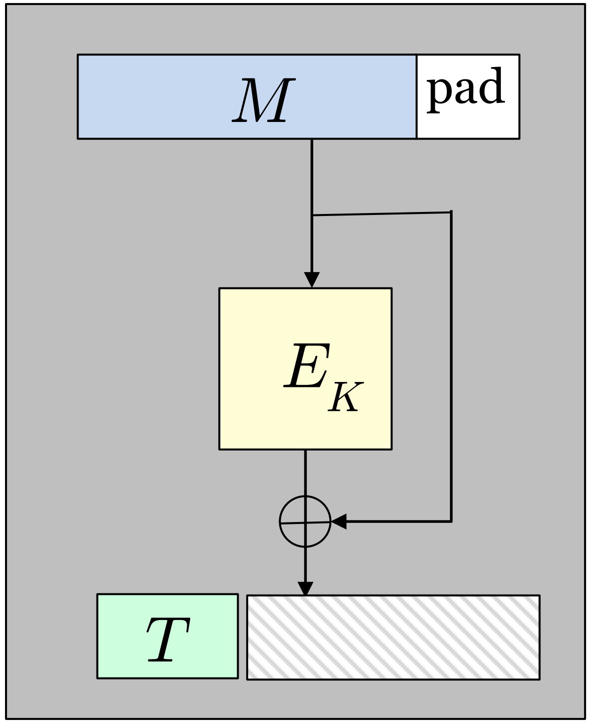
SIV paradigm [SR06]

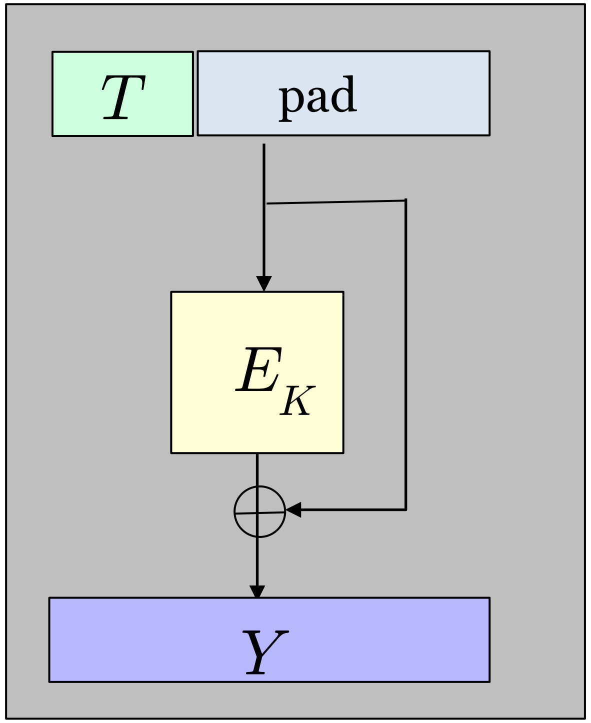
Building Committing Concealer

The Hash-then-Mask (HtM) Construction

[BHW23]


The HtM construction, conceptual view


Instantiate H

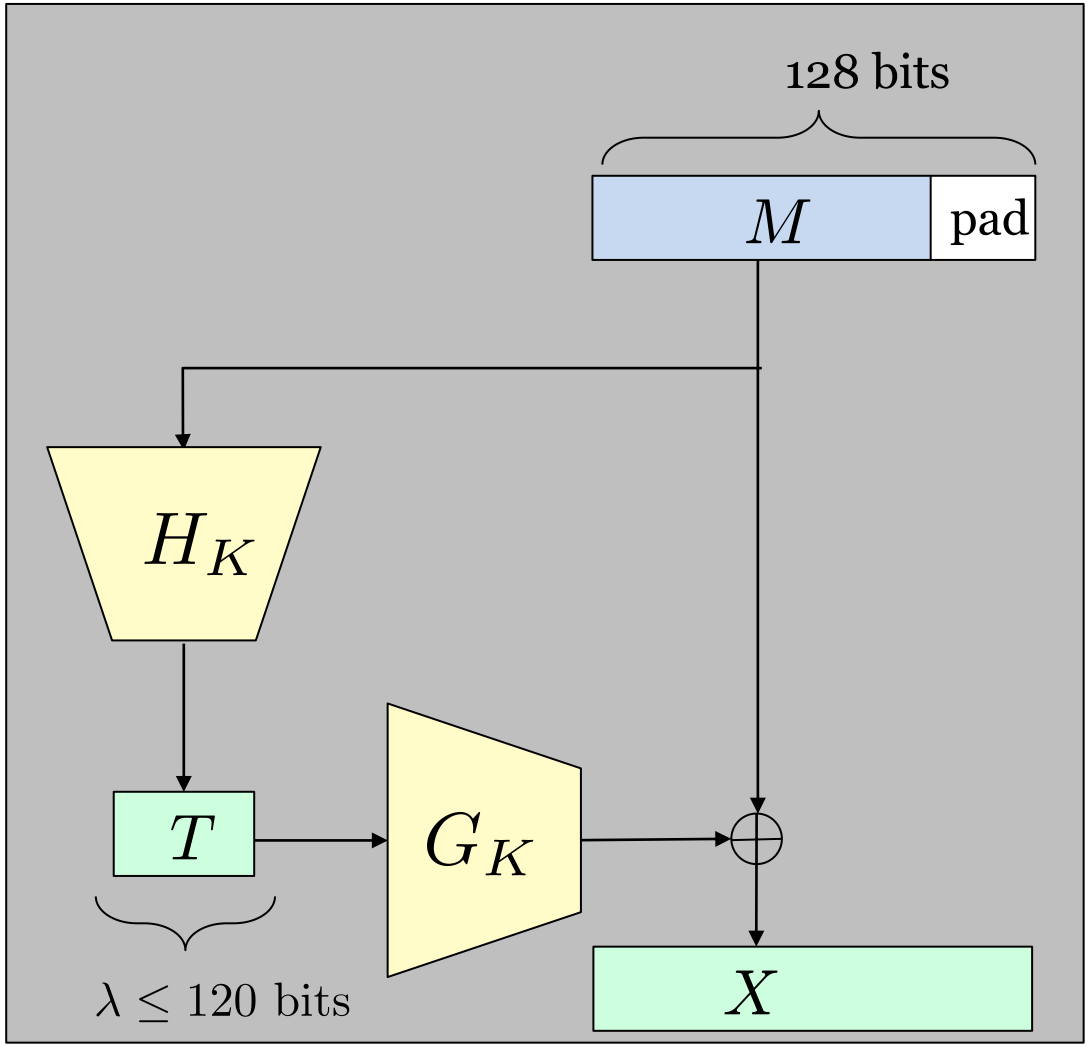

Instantiate G

Building Committing Concealer

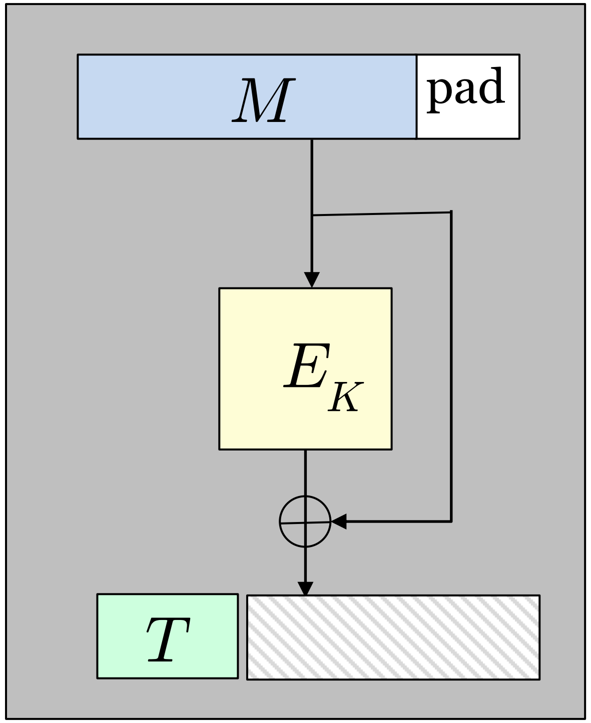
The Hash-then-Mask (HtM) Construction

[BHW23]

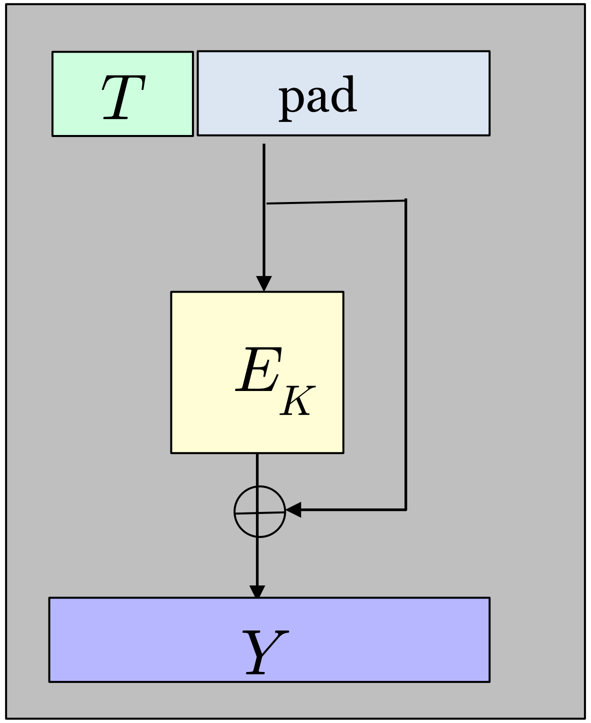
The HtM construction, conceptual view



Instantiate H



Instantiate G

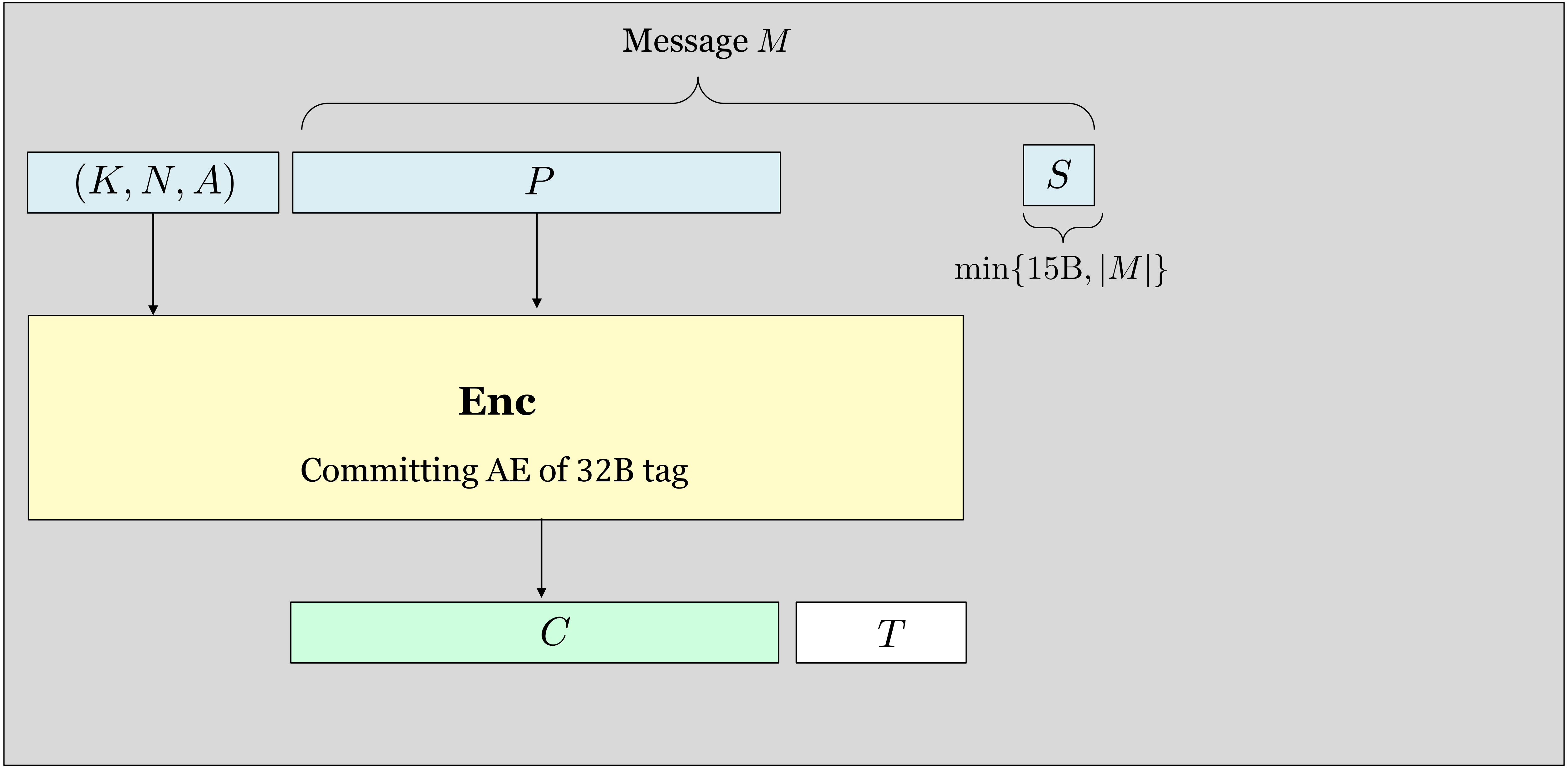


Ideal-cipher model

$\lambda - 8$ bits of committing security

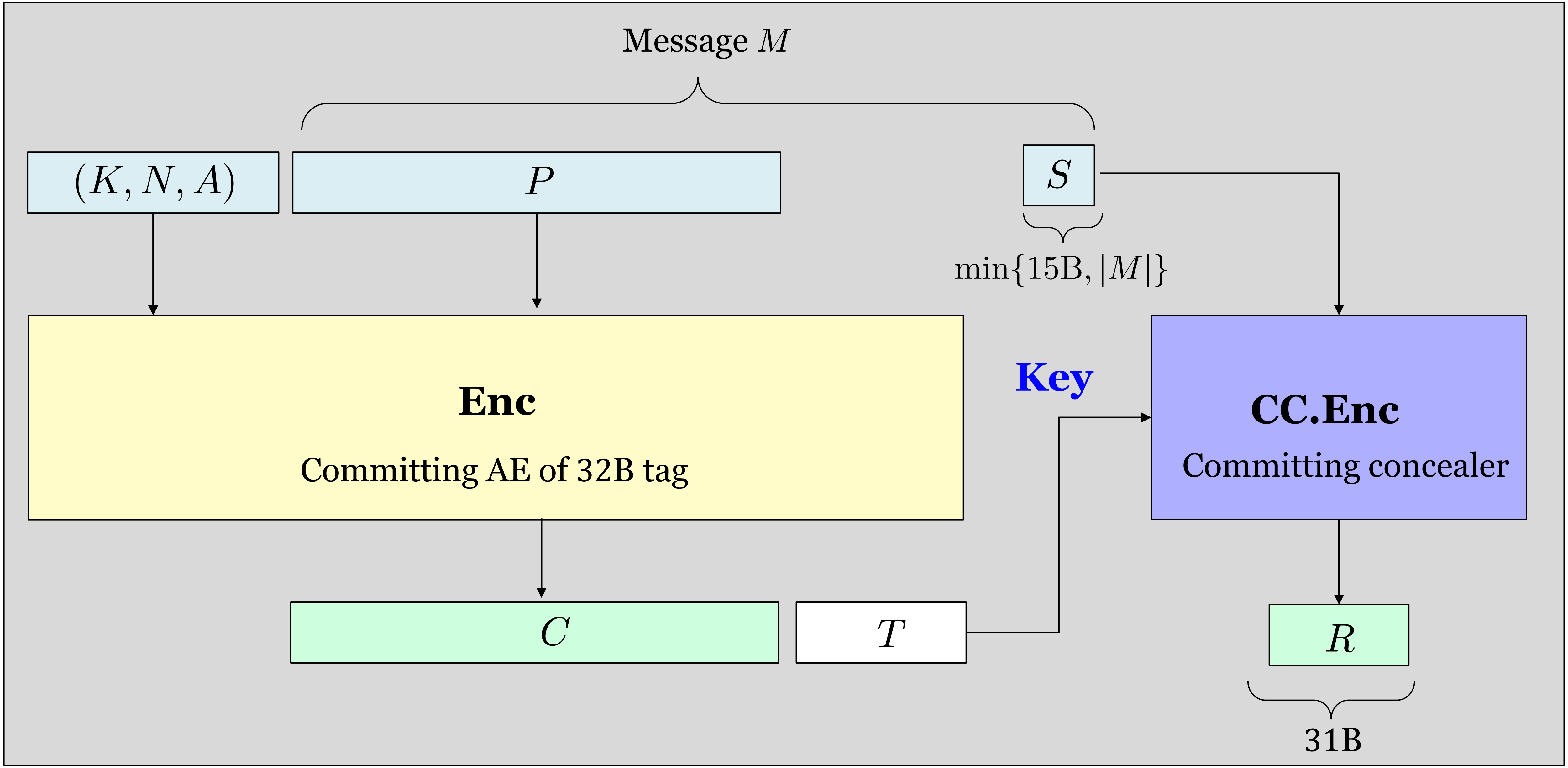
Using Committing Concealer To Reduce Size

[BHW23]



Using Committing Concealer To Reduce Size

[BHW23]



It’s Time To Have Committing AE Standard?

Many applications need committing security but each has its own (suboptimal) scheme

It’s Time To Have Committing AE Standard?

Many applications need committing security but each has its own (suboptimal) scheme

↓

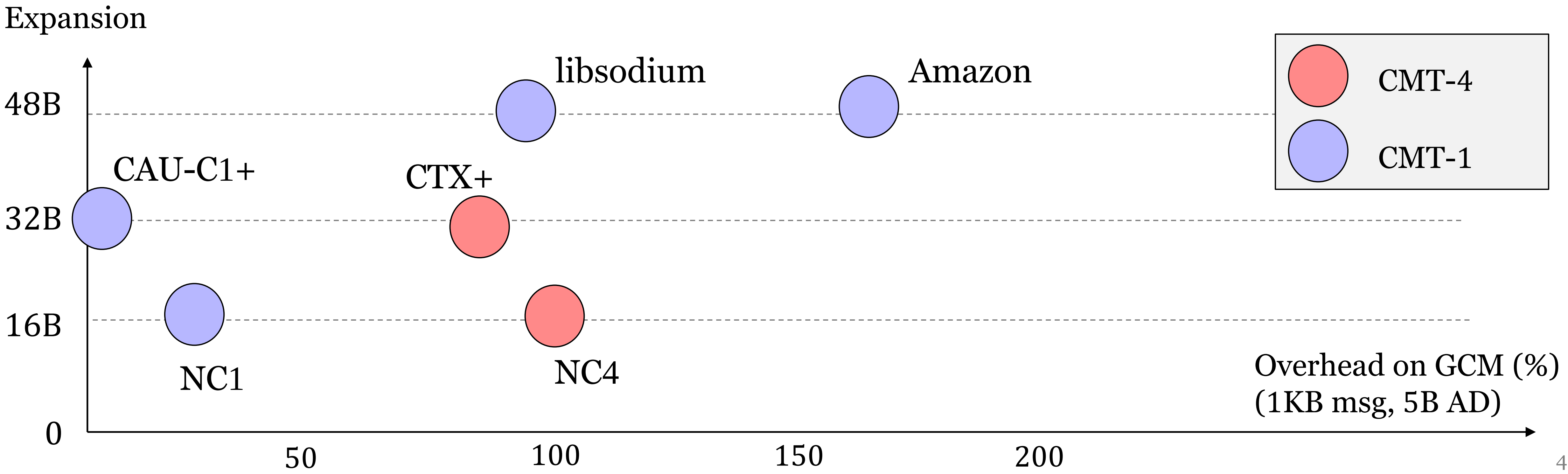
This won’t happen if we have committing AE standards. Our schemes offer a good starting choice

It’s Time To Have Committing AE Standard?

Many applications need committing security but each has its own (suboptimal) scheme

↓

This won’t happen if we have committing AE standards. Our schemes offer a good starting choice


Expansion
48B
32B
16B
Overhead on GCM (%)
(1KB msg, 5B AD)
libsodium
Amazon
CAU-C1+
CTX+
NC1
NC4
CMT-4
CMT-1