Forking a Blockcipher for Authenticated Encryption of Very Short Messages

Damian Vizár (CSEM, Switzerland)

ASK 2018, Kolkata

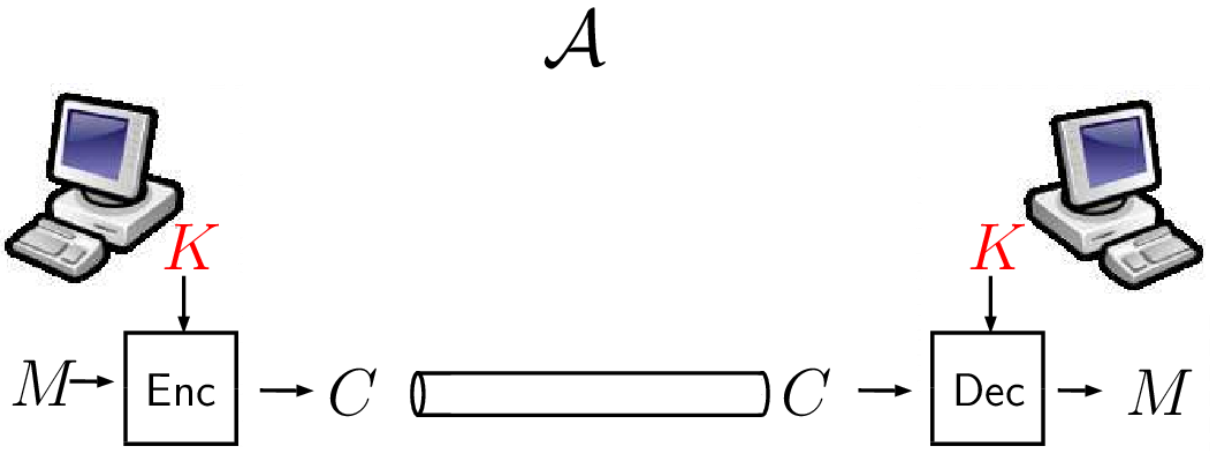
Joint work with:

Elena Andreeva (KU Leuven, Belgium)

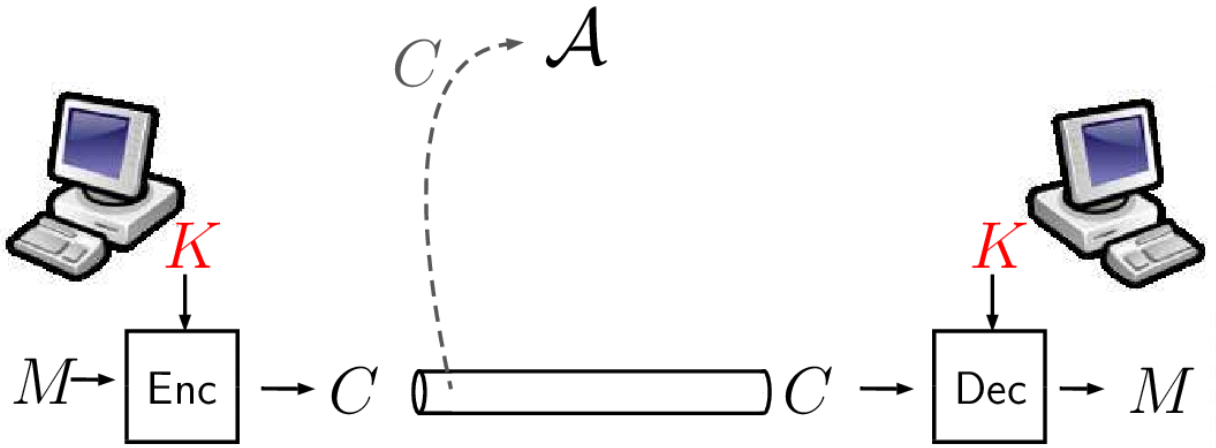
Reza Reyhanitabar (Elektrobit, Germany)

Kerem Varici (KU Leuven, Belgium)

Authenticated Encryption

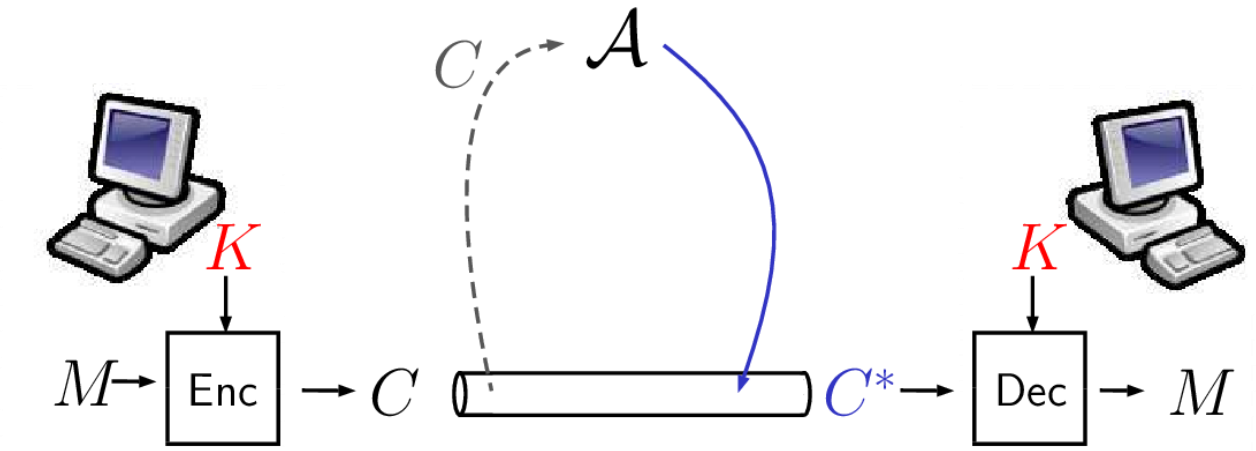


Authenticated Encryption



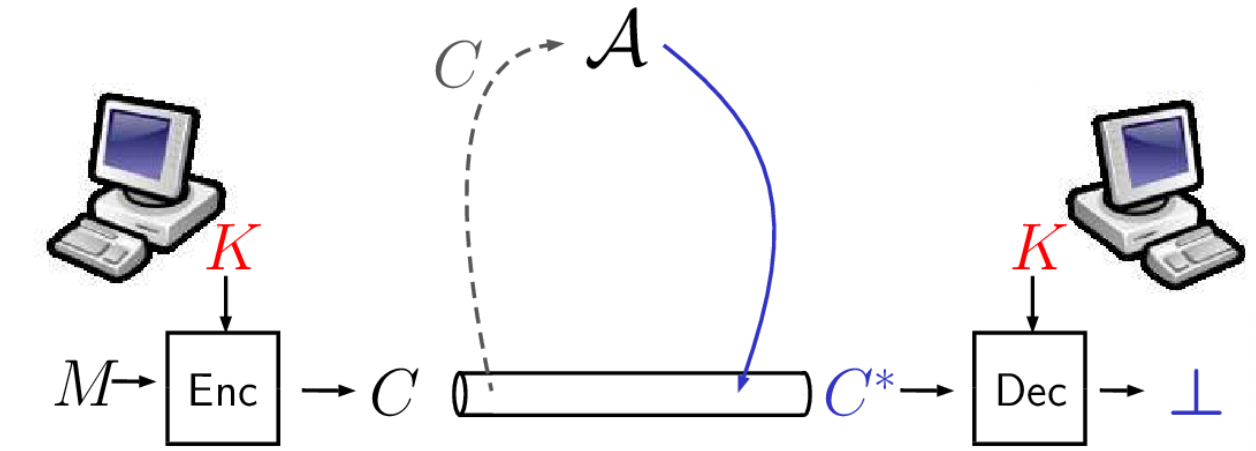
- Confidentiality

Authenticated Encryption



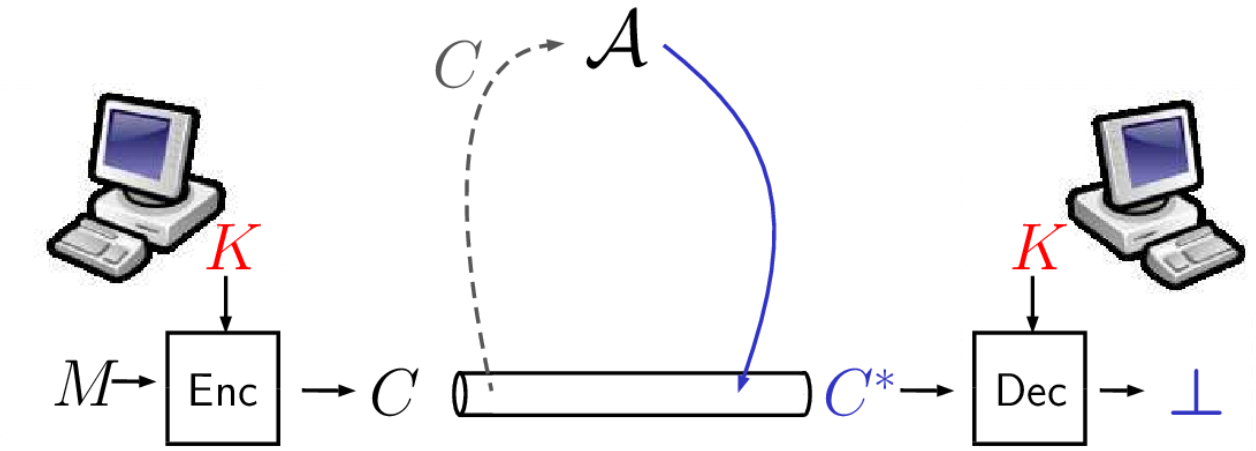
- Confidentiality

Authenticated Encryption



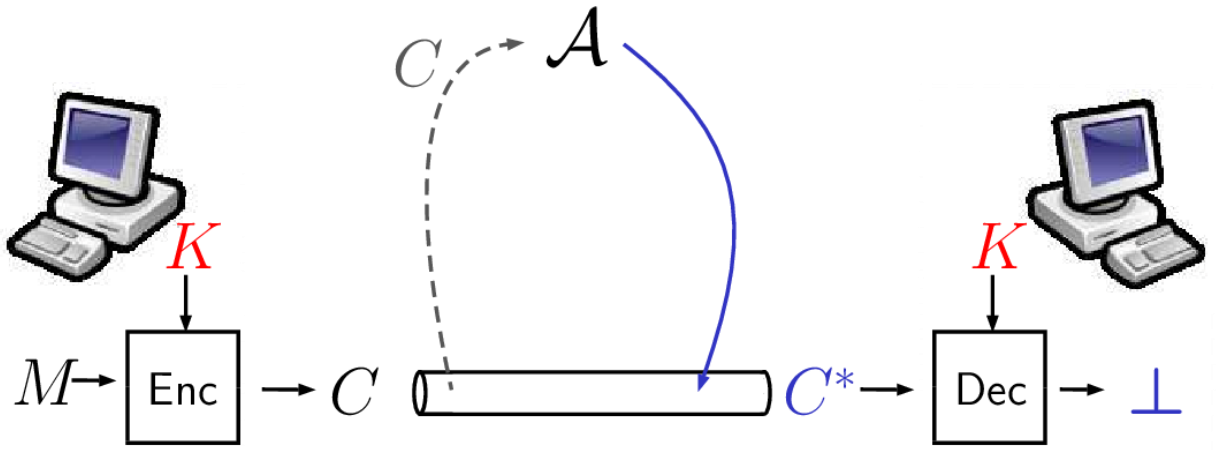
- Confidentiality and Integrity

Authenticated Encryption



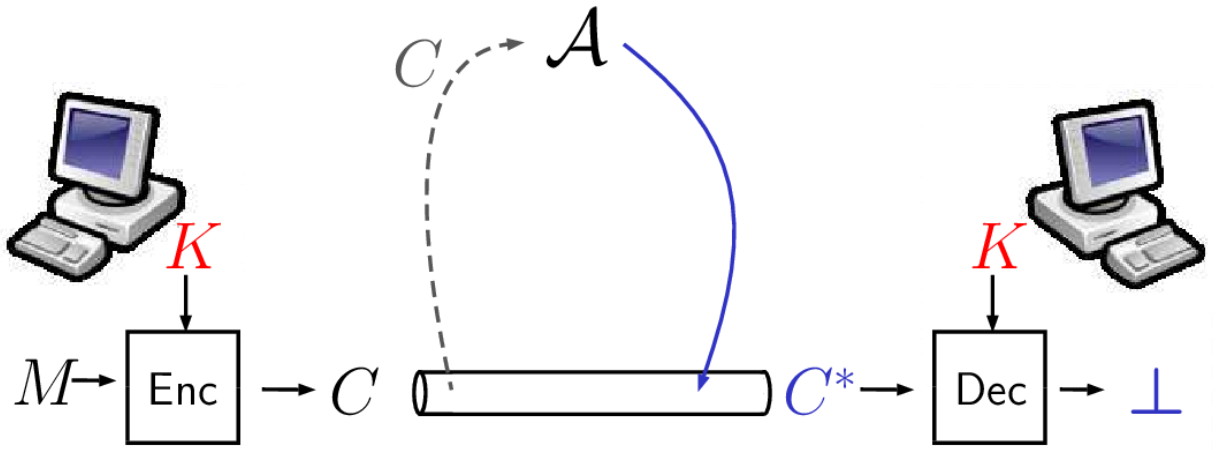
- Confidentiality and Integrity
- Standalone primitive [Bellare, Rogaway 00], [Katz, Yung 00]
  - OCB [BBKR 01], CCM [HWF 03], GCM [McGrew, Viega 04]

Authenticated Encryption



- Confidentiality and Integrity
- Standalone primitive [Bellare, Rogaway 00], [Katz, Yung 00]
  - OCB [BBKR 01], CCM [HWF 03], GCM [McGrew, Viega 04]
- Useful and widely used

Authenticated Encryption

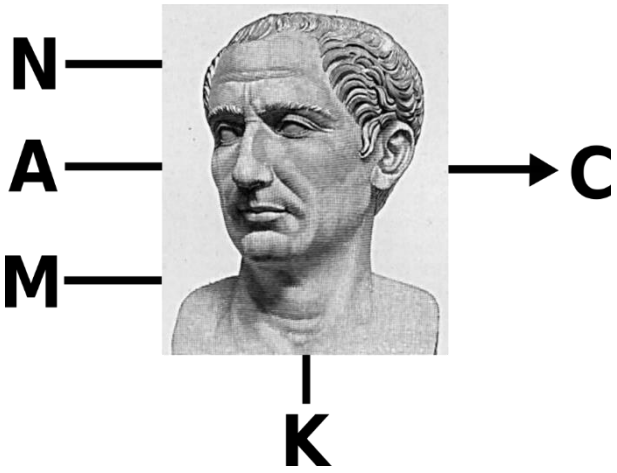


- Confidentiality and Integrity
- Standalone primitive [Bellare, Rogaway 00], [Katz, Yung 00]
  - OCB [BBKR 01], CCM [HWF 03], GCM [McGrew, Viega 04]
- Useful and widely used
- BUT issues with performance, robustness, patent burden …

Authenticated Encryption

CAESAR competition:

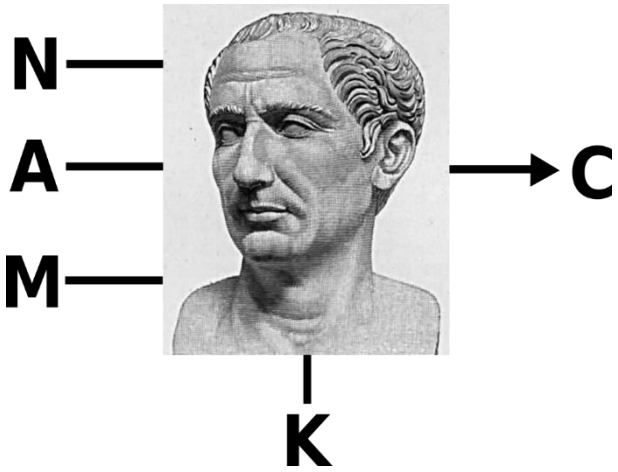
- Boost research, find new AEAD schemes
  - 57 submissions
  - ~~3~~ 5 years of activity



Authenticated Encryption

CAESAR competition:

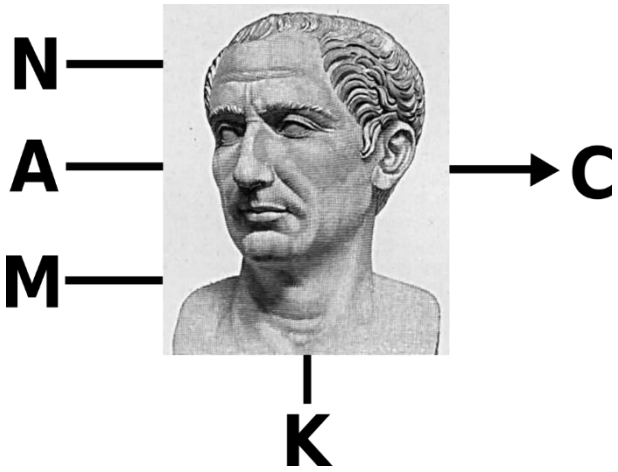
- Boost research, find new AEAD schemes
  - 57 submissions
  - ~~3~~ 5 years of activity
- A LOT of results
  - Primitives, constructions, security notions



Authenticated Encryption

CAESAR competition:

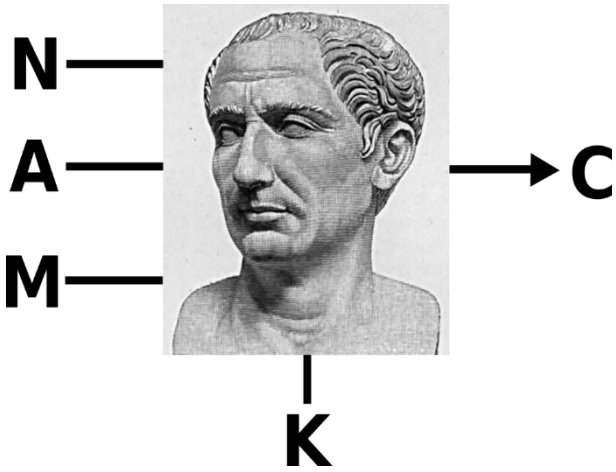
- Boost research, find new AEAD schemes
  - 57 submissions
  - ~~3~~ 5 years of activity
- A LOT of results
  - Primitives, constructions, security notions
- AE schemes for different use cases
  - High speed  Robustness  Lightweight 



Authenticated Encryption

CAESAR competition:

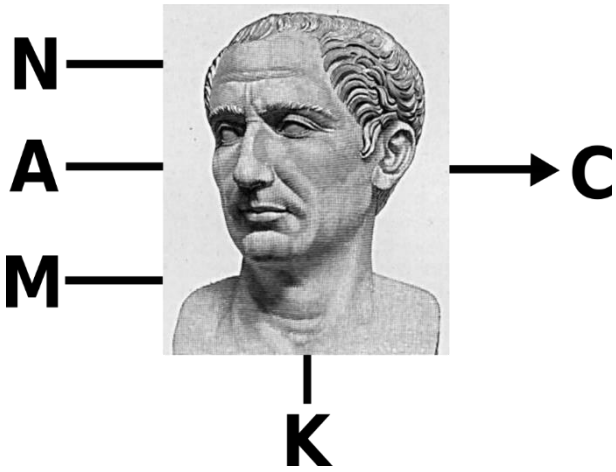
- Boost research, find new AEAD schemes
  - 57 submissions
  - ~~3~~ 5 years of activity
- A LOT of results
  - Primitives, constructions, security notions
- AE schemes for different use cases
  - High speed  Robustness  Lightweight 
- **7 schemes in final portfolio**



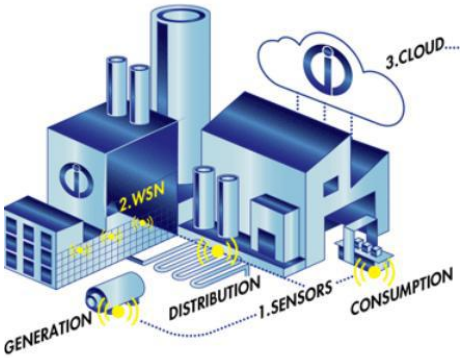
Authenticated Encryption: is it solved?

CAESAR competition:

- Boost research, find new AEAD schemes
  - 57 submissions
  - ~~3~~ 5 years of activity
- A LOT of results
  - Primitives, constructions, security notions
- AE schemes for different use cases
  - High speed  Robustness  Lightweight 
- **7 schemes in final portfolio**

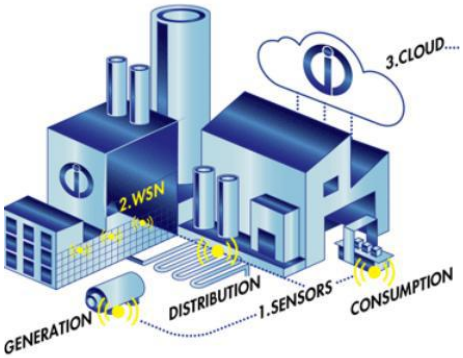


New Challenges



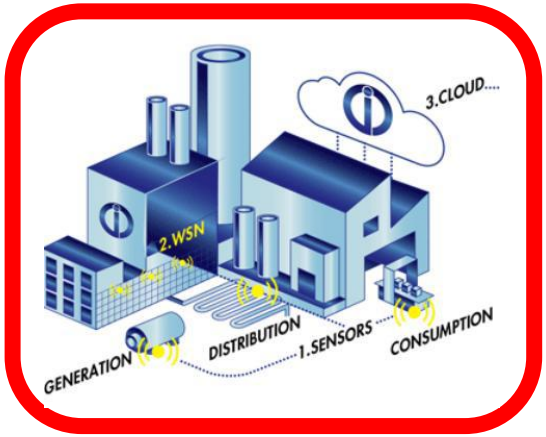
- “IoT” devices

New Challenges



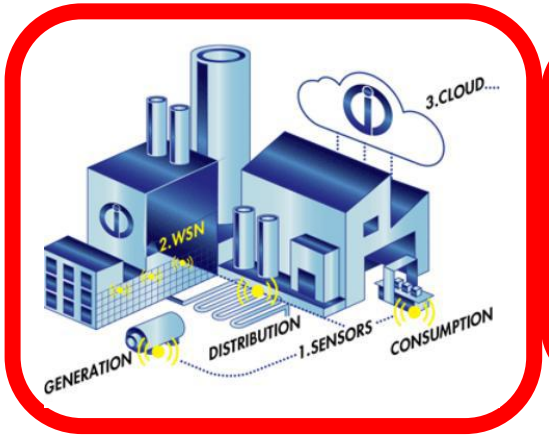
- “IoT” devices
- Distinct constraints

New Challenges



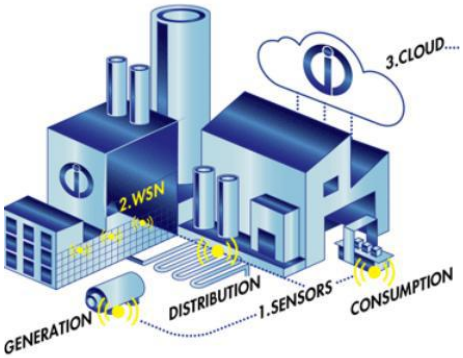
- "IoT" devices
- Distinct constraints
  - Latency

New Challenges



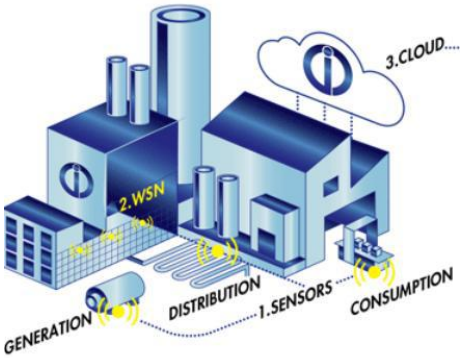
- "IoT" devices
- Distinct constraints
  - Latency, throughput

New Challenges



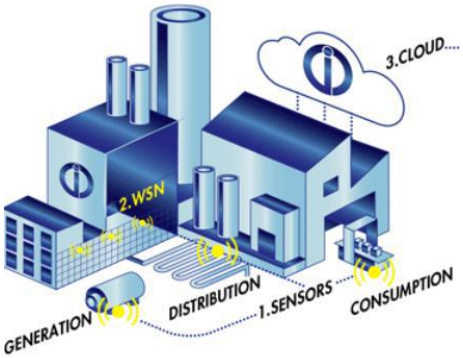
- "IoT" devices
- Distinct constraints
  - Latency, throughput, power

New Challenges

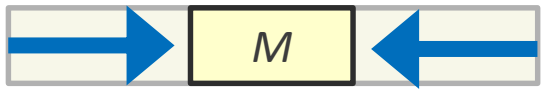


- "IoT" devices
- Distinct constraints
  - Latency, throughput, power, code size/area, …

New Challenges



- "IoT" devices
- Distinct constraints
  - Latency, throughput, power, code size/area, …
- New communication patterns
  - Dominated by (very) short messages



(Very) Short Messages

- Short data burst [5G spec]
  - “Small status updates **(few bits)**”

(Very) Short Messages

- Short data burst [5G spec]
  - “Small status updates **(few bits)**”
- Low-latency processing short messages [SecOC (automotive)]
  - Payload **<= 64 bytes** [CAN FD standard (ISO 11898-1)]

(Very) Short Messages

- Short data burst [5G spec]
  - "Small status updates **(few bits)**"
- Low-latency processing short messages [SecOC (automotive)]
  - Payload **<= 64 bytes** [CAN FD standard (ISO 11898-1)]
- Constrained channels [NB-IoT]
  - **16 bits <=** transport block size <= 680 bits/1000bits

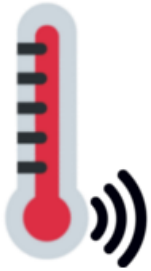
(Very) Short Messages

- Short data burst [5G spec]
  - "Small status updates **(few bits)**"
- Low-latency processing short messages [SecOC (automotive)]
  - Payload **<= 64 bytes** [CAN FD standard (ISO 11898-1)]
- Constrained channels [NB-IoT]
  - **16 bits <=** transport block size <= 680 bits/1000bits
- NIST's call for lightweight crypto
  - "Be efficient for short messages (e.g., as short as **8 bytes**)"

(Very) Short Messages: Possibly <= 1 AES Block

- Short data burst [5G spec]
  - "Small status updates **(few bits)**"
- Low-latency processing short messages [SecOC (automotive)]
  - Payload **<= 64 bytes** [CAN FD standard (ISO 11898-1)]
- Constrained channels [NB-IoT]
  - **16 bits <=** transport block size <= 680 bits/1000bits
- NIST's call for lightweight crypto
  - "Be efficient for short messages (e.g., as short as **8 bytes**)"



Existing AES-based AE vs Very Short Messages

Existing AES-based AE vs Very Short Messages

scheme	Cost of encryption in (# of AES rounds)/10 + GF(2^{128})mul									
	$a=0$				$a=1$				$a=2$	
	m=1	m=2	m=3	m=4	m=0	m=1	m=2	m=3	m=1	m=2
GCM	2+2	3+3	4+4	5+5	1+2	2+3	3+4	4+5	2+4	3+5
CCM	4	6	8	10	3	5	7	9	6	8
OCB3	3	4	5	6	3	4	5	6	5	6
CLOC	3	5	7	9	2	4	6	8	5	7
Deoxys-I	2.8	4.2	5.6	7	2.8	4.2	5.6	7	5.6	7
KIASU$^{\neq}$	2	3	4	5	2	3	4	5	4	5

a,m: length of A and M in 128-bit blocks; per-session key derivation excluded

Existing AES-based AE vs Very Short Messages

scheme	Cost of encryption in (# of AES rounds)/10 + GF(2^{128})mul
	$m=1$
GCM	
CCM	4
OCB3	3
CLOC	3
Deoxys-I	2.8
KIASU$^{\neq}$	2

GHASH: $a + m + 1$ GF(2^{128}) mul.

&

CTR mode: $m + 1$ AES calls

extra AES and $m+1$ mul. for tag

a,m: length of A and M in 128-bit blocks; per-session key derivation excluded

Existing AES-based AE vs Very Short Messages

scheme	Cost of encryption in (# of AES rounds)/10 + GF(2^{128})mul m=1
GCM	2
CCM	
OCB3	3
CLOC	3
Deoxys-I	2.8
KIASU$^{\neq}$	2

CBC MAC: *a + m +1* AES calls

&

CTR: *m + 1* AES calls

extra AES for tag, ***m+1* extra calls for MAC**

a,m: length of A and M in 128-bit blocks; per-session key derivation excluded

Existing AES-based AE vs Very Short Messages

scheme	Cost of encryption in (# of AES rounds)/10 + GF(2^{128})mul
	m=1
GCM	2+2
CCM	4
OCB3	3
CLOC	
Deoxys-I	2.8
KIASU$^{\neq}$	2

AD-HASH: *a* AES calls

&

OCB core: *m + 2* AES calls

2x extra AES for tag and for derived key

a,m: length of A and M in 128-bit blocks; per-session key derivation excluded

Existing AES-based AE vs Very Short Messages

scheme	Cost of encryption in (# of AES rounds)/10 + GF(2^{128})mul m=1
GCM	2+2
CCM	4
OCB3	3
CLOC	
Deoxys-I	2.8
KIASU$^{\neq}$	2

IV + CFB: *a + m* AES calls

&

Tag: *m + 1* AES calls

***m+1* extra AES** calls for tag

a,m: length of A and M in 128-bit blocks; per-session key derivation excluded

Existing AES-based AE vs Very Short Messages

scheme	Cost of encryption in (# of AES rounds)/10 + GF(2^{128})mul
	m=1
GCM	2+2
CCM	4
OCB3	3
CLOC	3
Deoxys-I	2.8
KIASU$^{\neq}$	2

AD-HASH: *a* Deoxys calls (1.4 AES)

&

OCB core: *m + 1* Deoxys calls (1.4 AES)

1.4 extra AES for tag

a,m: length of A and M in 128-bit blocks; per-session key derivation excluded

Existing AES-based AE vs Very Short Messages

scheme	Cost of encryption in (# of AES rounds)/10 + GF(2^{128})mul
	m=1
GCM	2+2
CCM	4
OCB3	3
CLOC	3
Deoxys-I	
KIASU$^{\neq}$	2

AD-HASH: *a* KIASU calls (~ AES)

&

OCB core: *m + 1* KIASU calls (~AES)

extra AES for tag

a,m: length of A and M in 128-bit blocks; per-session key derivation excluded

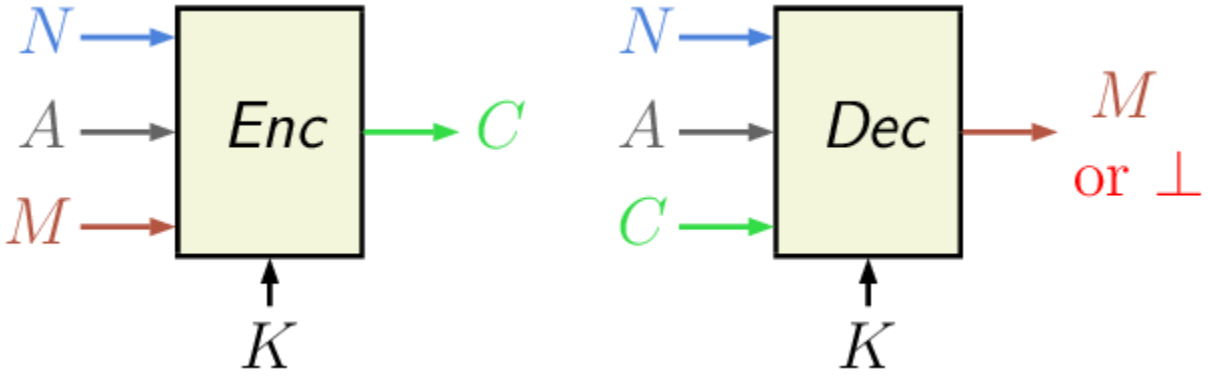
Existing AES-based AE vs Very Short Messages

scheme	Cost of encryption in (# of AES rounds)/10 + GF(2^{128})mul									
	$a=0$				$a=1$				$a=2$	
	m=1	m=2	m=3	m=4	m=0	m=1	m=2	m=3	m=1	m=2
GCM	2+2	3+3	4+4	5+5	1+2	2+3	3+4	4+5	2+4	3+5
CCM	4	6	8	10	3	5	7	9	6	8
OCB3	3	4	5	6	3	4	5	6	5	6
CLOC	3	5	7	9	2	4	6	8	5	7
Deoxys-I	2.8	4.2	5.6	7	2.8	4.2	5.6	7	5.6	7
KIASU$^{\neq}$	2	3	4	5	2	3	4	5	4	5

a,m: length of A and M in 128-bit blocks; per-session key derivation excluded

"The performance target is wrong · · · an authenticated cipher is applied to many small messages · · · The challenge here is to minimize overhead." [ECRYPT-CSA 2017]

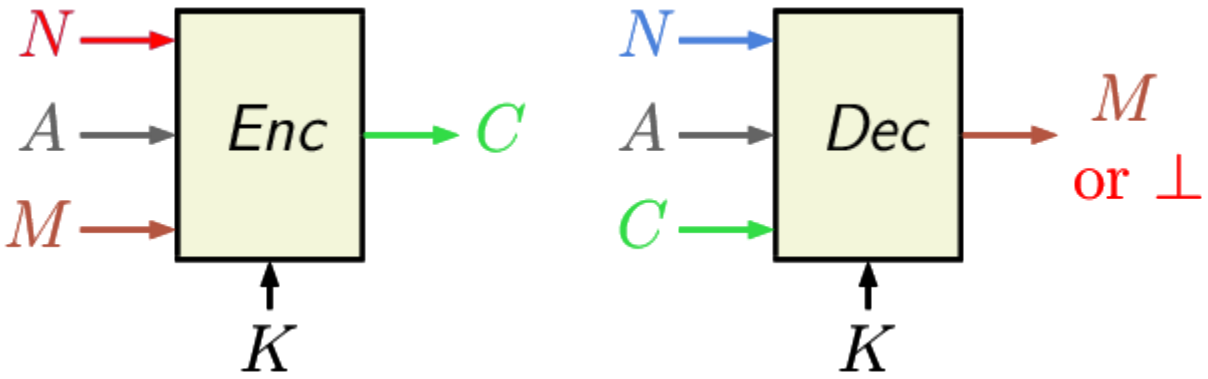
Nonce-based Authenticated Encryption with Associated Data



- **Enc,Dec:** deterministic algorithms
- **N: Nonce,** must not repeat
- **A: Associated Data,** authenticated, but not encrypted
- **M: Plaintext,** encrypted and authenticated
- **K: Secret key**

Also **|C| = |M| + τ** and Dec(K,N,A,Enc(K,N,A,M)) = M

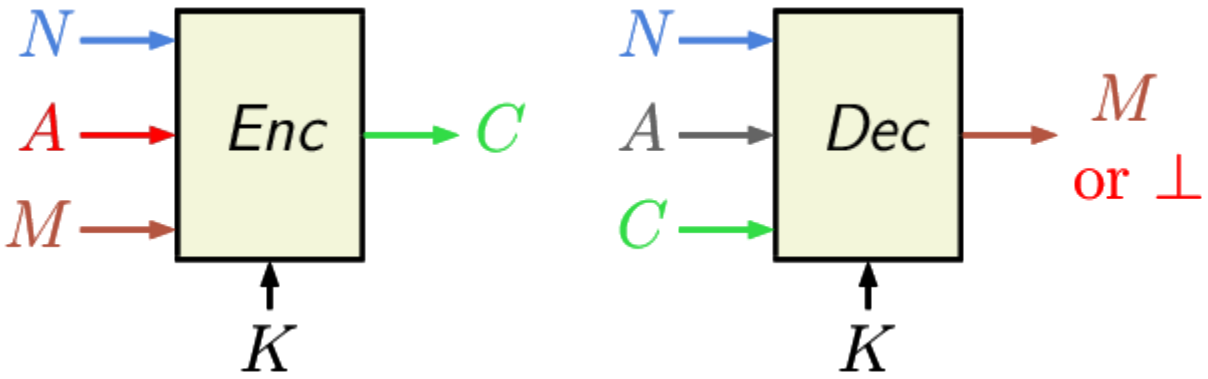
Nonce-based Authenticated Encryption with Associated Data



- **Enc,Dec:** deterministic algorithms
- **N: Nonce,** must not repeat
- **A: Associated Data,** authenticated, but not encrypted
- **M: Plaintext,** encrypted and authenticated
- **K: Secret key**

Also **|C| = |M| + τ** and Dec(K,N,A,Enc(K,N,A,M)) = M

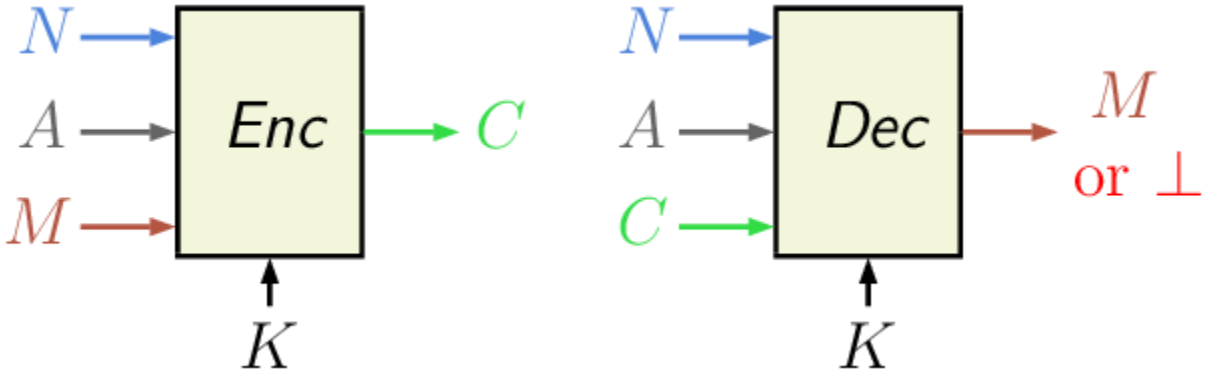
Nonce-based Authenticated Encryption with Associated Data



- **Enc,Dec:** deterministic algorithms
- **N: Nonce,** must not repeat
- **A: Associated Data,** authenticated, but not encrypted
- **M: Plaintext,** encrypted and authenticated
- **K: Secret key**

Also **|C| = |M| + τ** and Dec(K,N,A,Enc(K,N,A,M)) = M

Nonce-based Authenticated Encryption with Associated Data

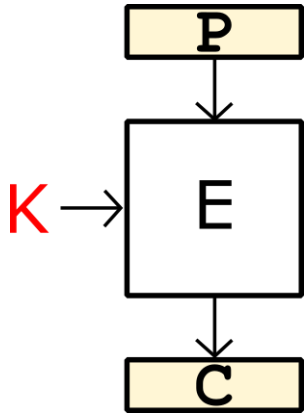


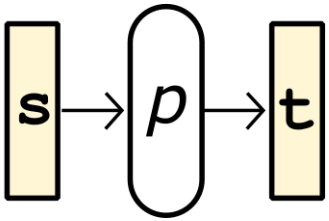
- **Enc,Dec:** deterministic algorithms
- **N: Nonce,** must not repeat
- **A: Associated Data,** authenticated, but not encrypted
- **M: Plaintext,** encrypted and authenticated
- **K: Secret key**

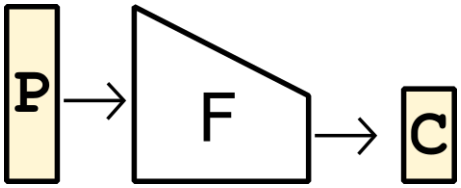
Also **|C| = |M| + τ** and Dec(K,N,A,Enc(K,N,A,M)) = M

The Notional Gap

Available primitives:

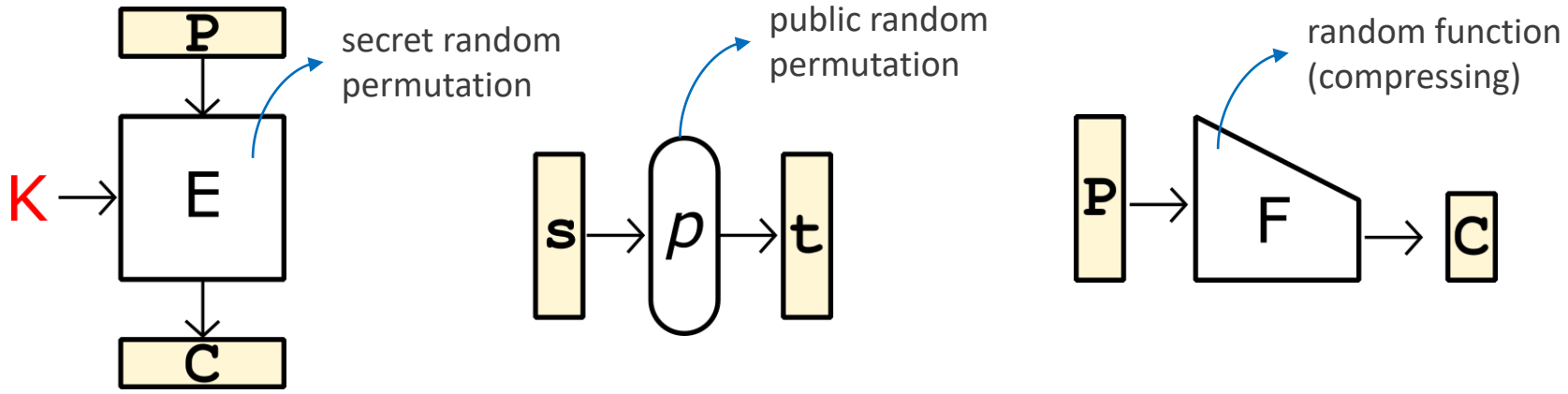






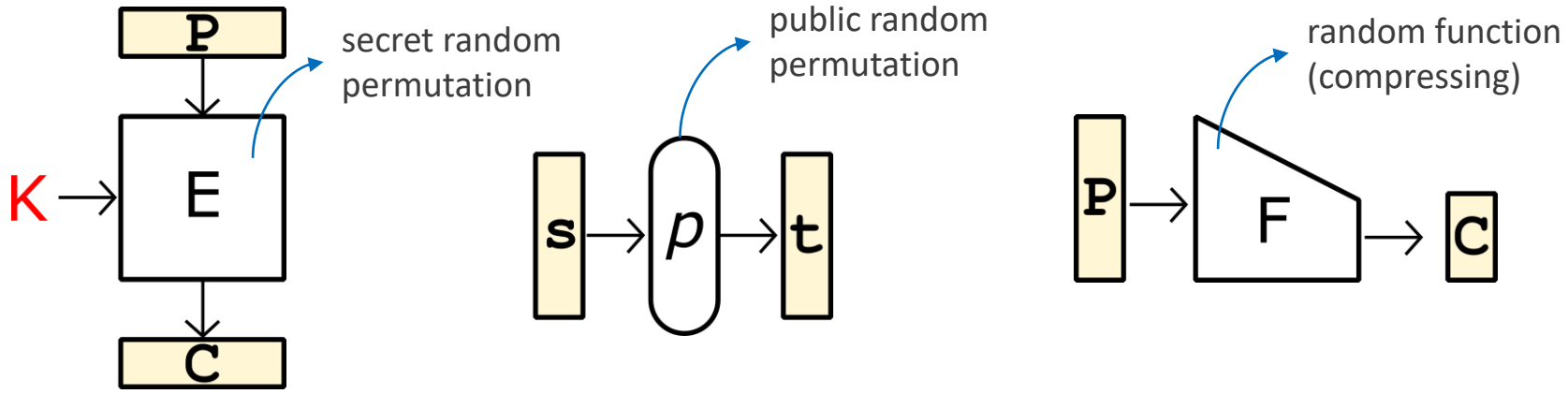
The Notional Gap

Available primitives:



The Notional Gap

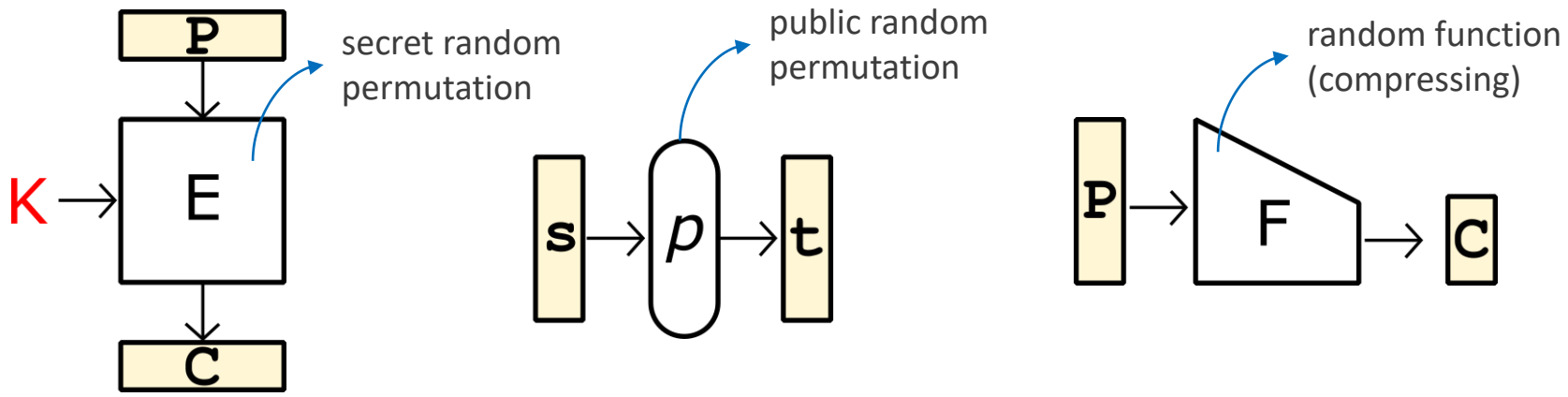
Available primitives:



- No integrity or non-trivial redundancy

The Notional Gap

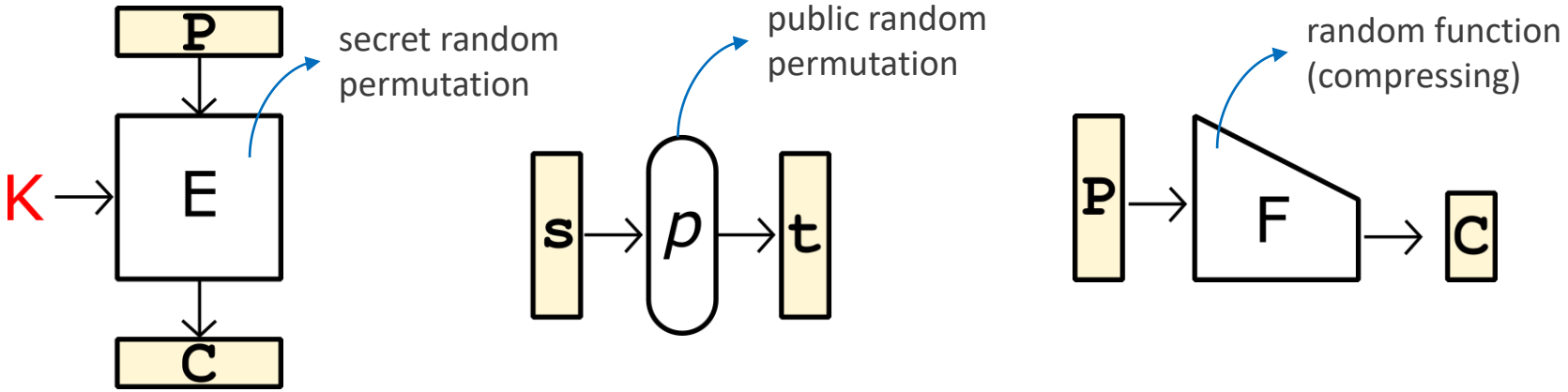
Available primitives:



- No integrity or non-trivial redundancy
- For AE: at least 1 extra call for integrity
  - Amortized in long queries
  - 100% overhead for short queries!

The Notional Gap

Available primitives:

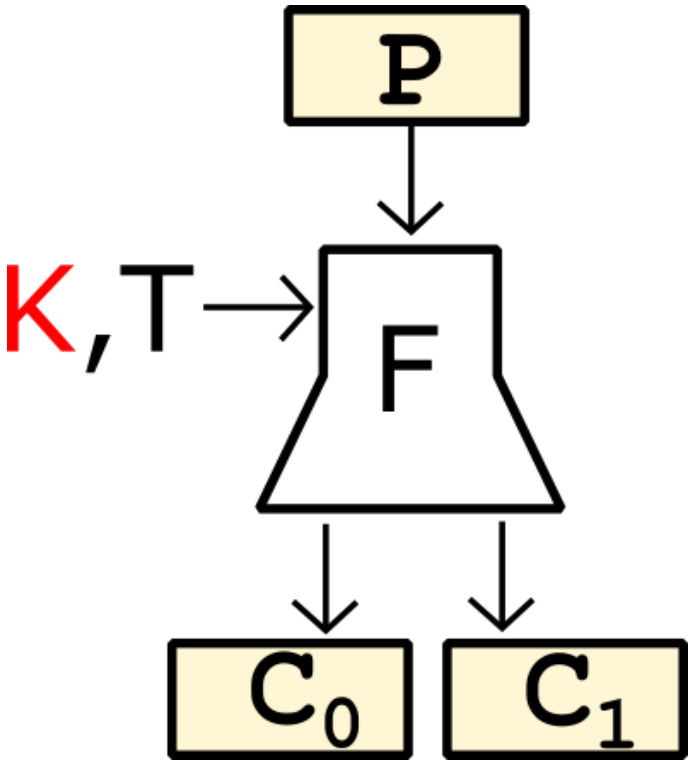


- No integrity or non-trivial redundancy
- For AE: at least 1 extra call for integrity
  - Amortized in long queries
  - 100% overhead for short queries!

Solution:

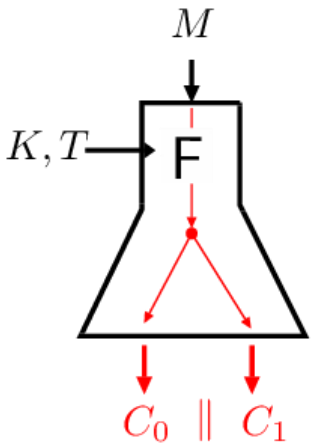
Invent a new primitive

Forkcipher



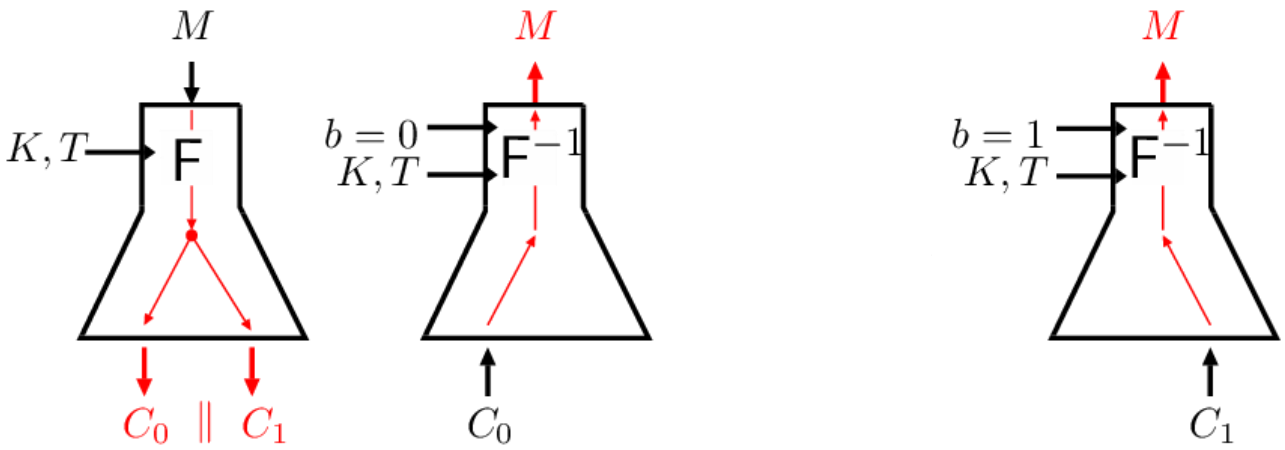
- Keyed
- Expanding
- Tweakable
- Invertible
  - Parallel permutations

Forkcipher: Syntax



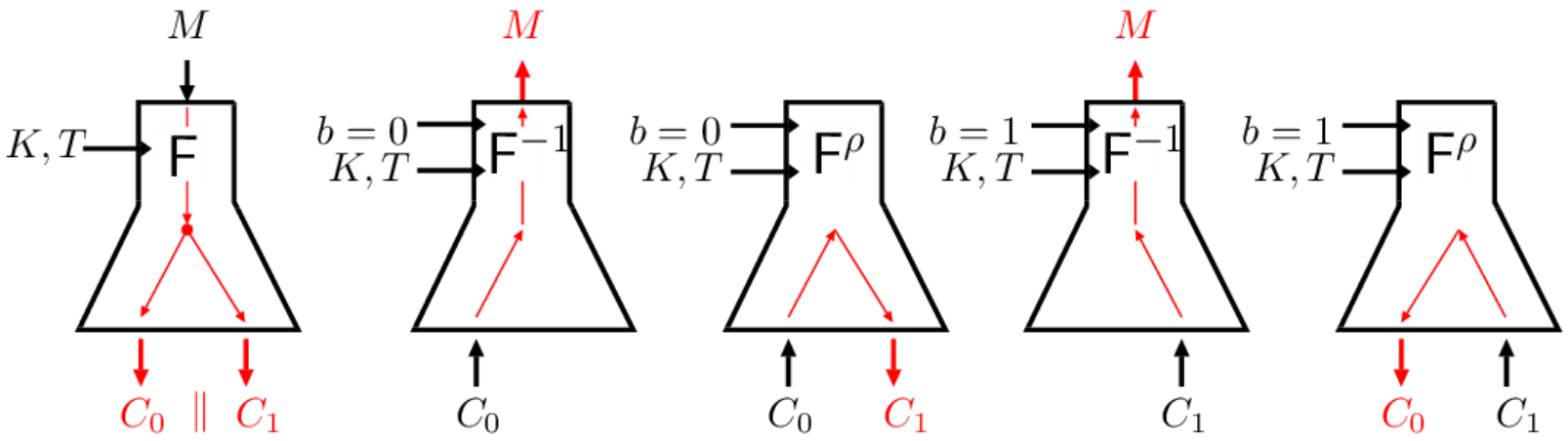
- Forward: *n*-bit block → **2 *n*-bit blocks**

Forkcipher: Syntax



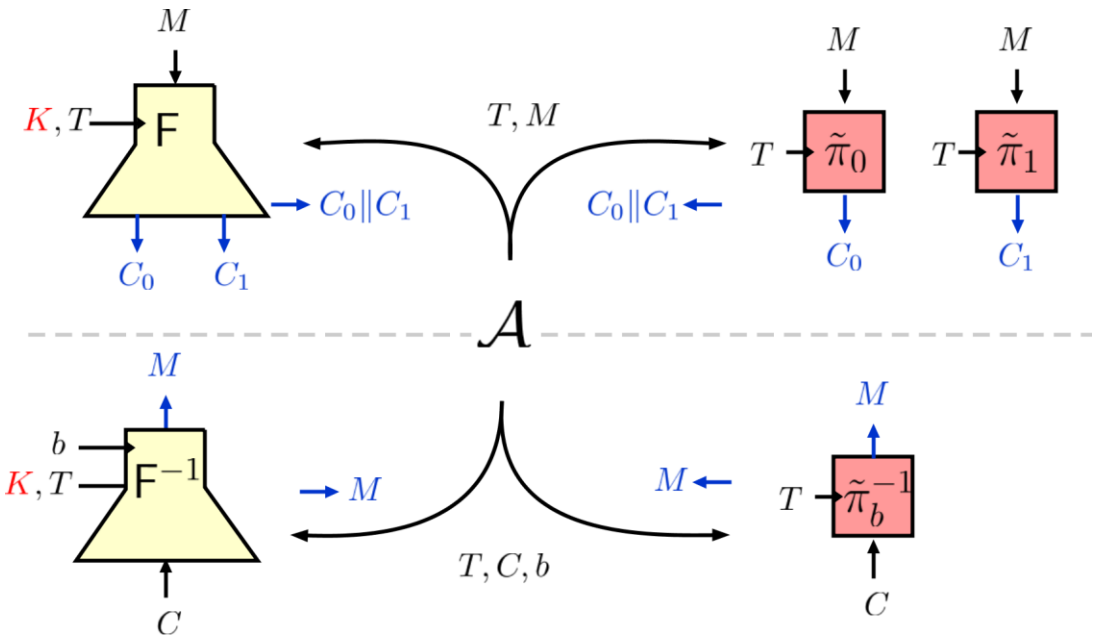
- Forward: *n*-bit block → **2 *n*-bit blocks**
- Inverse: ***n*-bit block, binary flag** → *n*-bit block
  - Can invert **either** output block

Forkcipher: Syntax



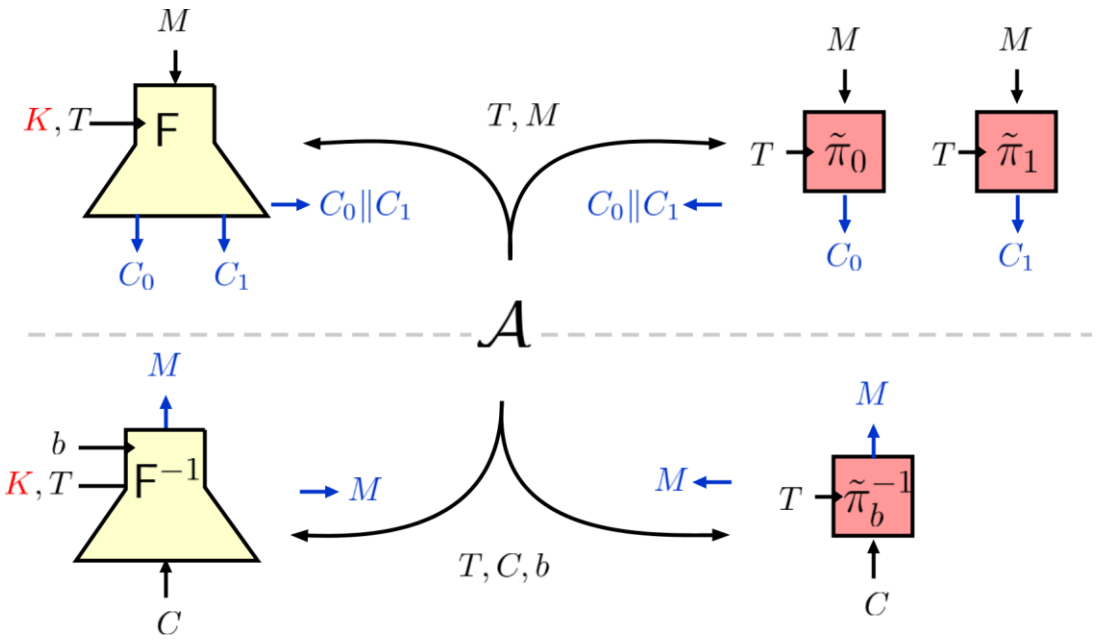
- Forward: *n*-bit block → **2 *n*-bit blocks**
- Inverse: ***n*-bit block, binary flag** → *n*-bit block
  - Can invert **either** output block
- **Reconstruction:** *n*-bit block, binary flag → *n*-bit block
  - Can reconstruct **either** ouput block **from the other output block**

Forkcipher: Security



$$\mathbf{Adv}_{\mathsf{F}}^{\mathrm{prtfp}}(\mathcal{A}) = \Pr\left[\mathcal{A}^{\mathrm{real}} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{\mathrm{ideal}} \Rightarrow 1\right]$$

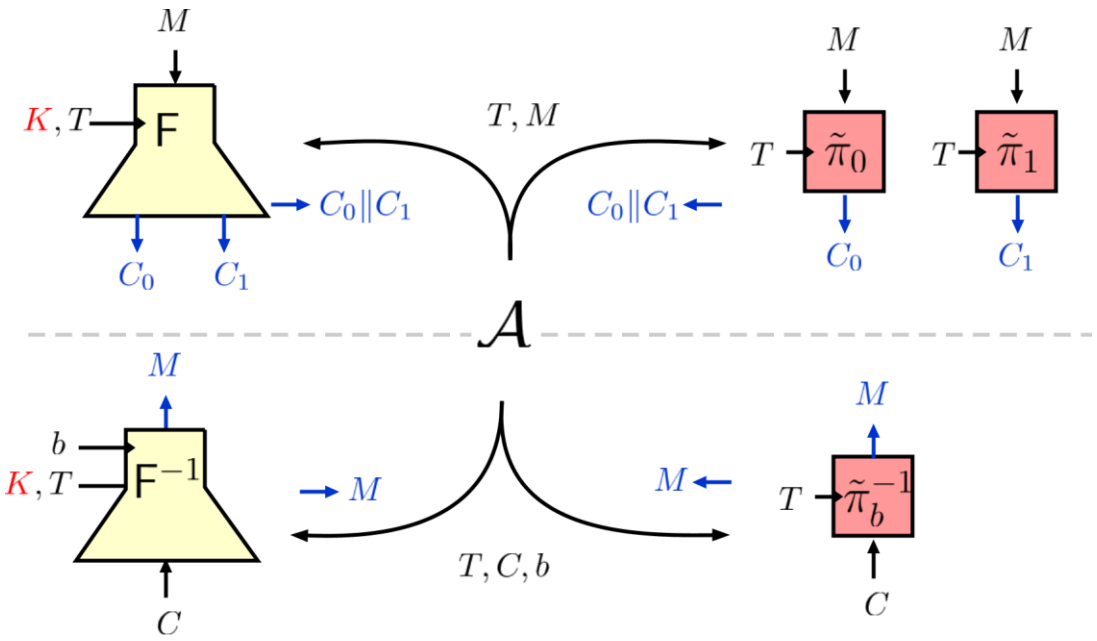
Forkcipher: Security



$$\mathbf{Adv}_{\mathsf{F}}^{\mathrm{prtfp}}(\mathcal{A}) = \Pr\left[\mathcal{A}^{\mathrm{real}} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{\mathrm{ideal}} \Rightarrow 1\right]$$

- **Almost AE security** (natural PRI construction)

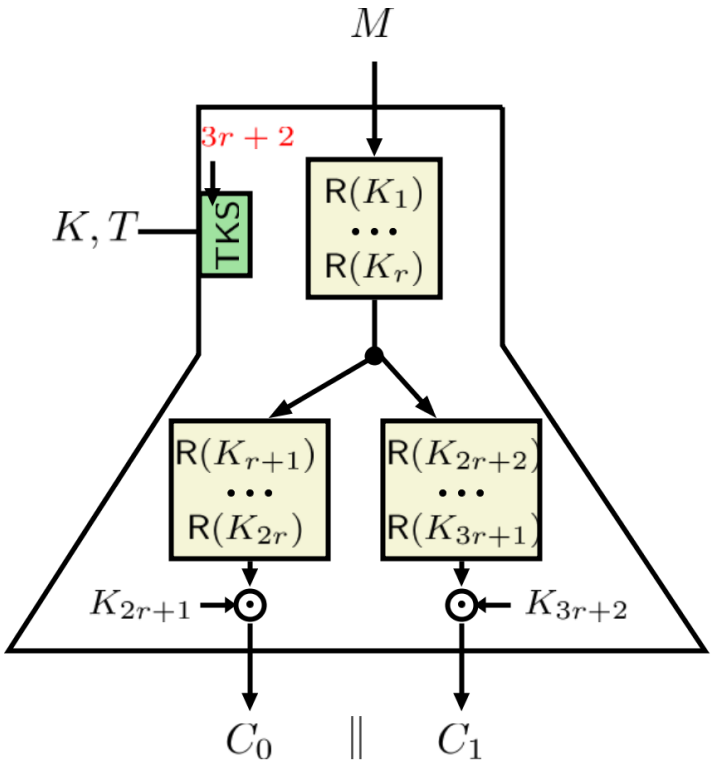
Forkcipher: Security

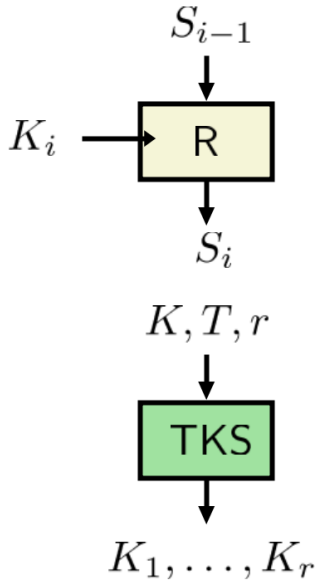


$$\mathbf{Adv}_{\mathsf{F}}^{\mathrm{prtfp}}(\mathcal{A}) = \Pr\left[\mathcal{A}^{\mathrm{real}} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{\mathrm{ideal}} \Rightarrow 1\right]$$

- **Almost AE security** (natural PRI construction)
- **“Two TBCs? What’s so novel about that?”**

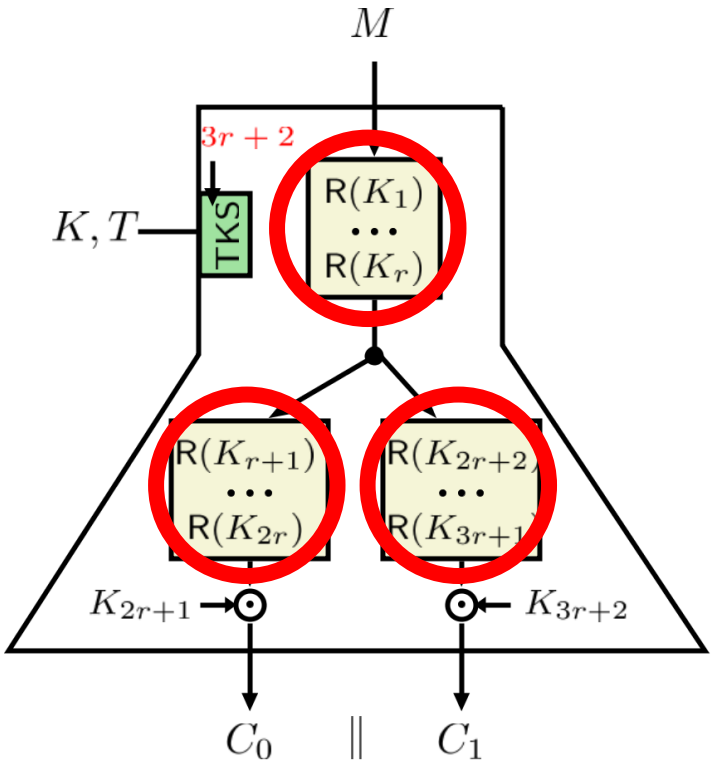
Forkcipher Instantiation: Iterate-Fork-Iterate

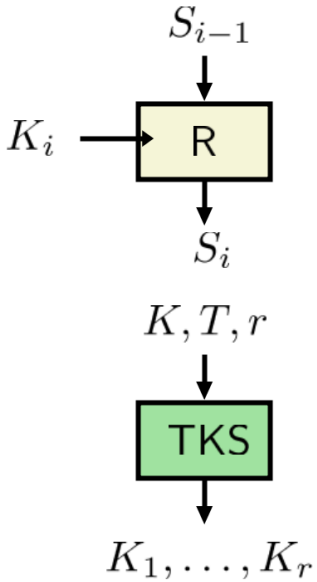




- IFI: **Round Function + Tweakey Schedule + #rounds/3**

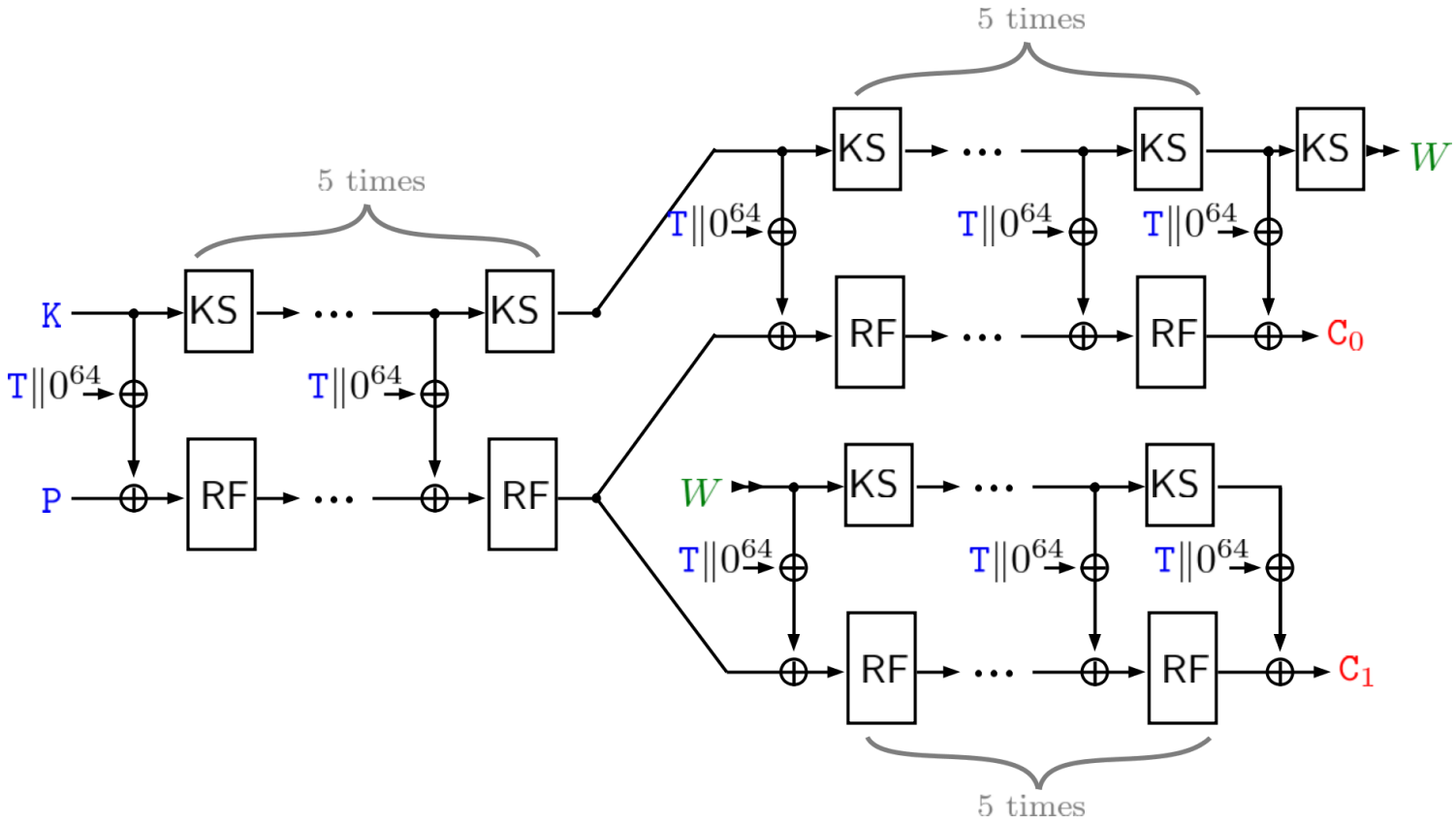
Forkcipher Instantiation: Iterate-Fork-Iterate





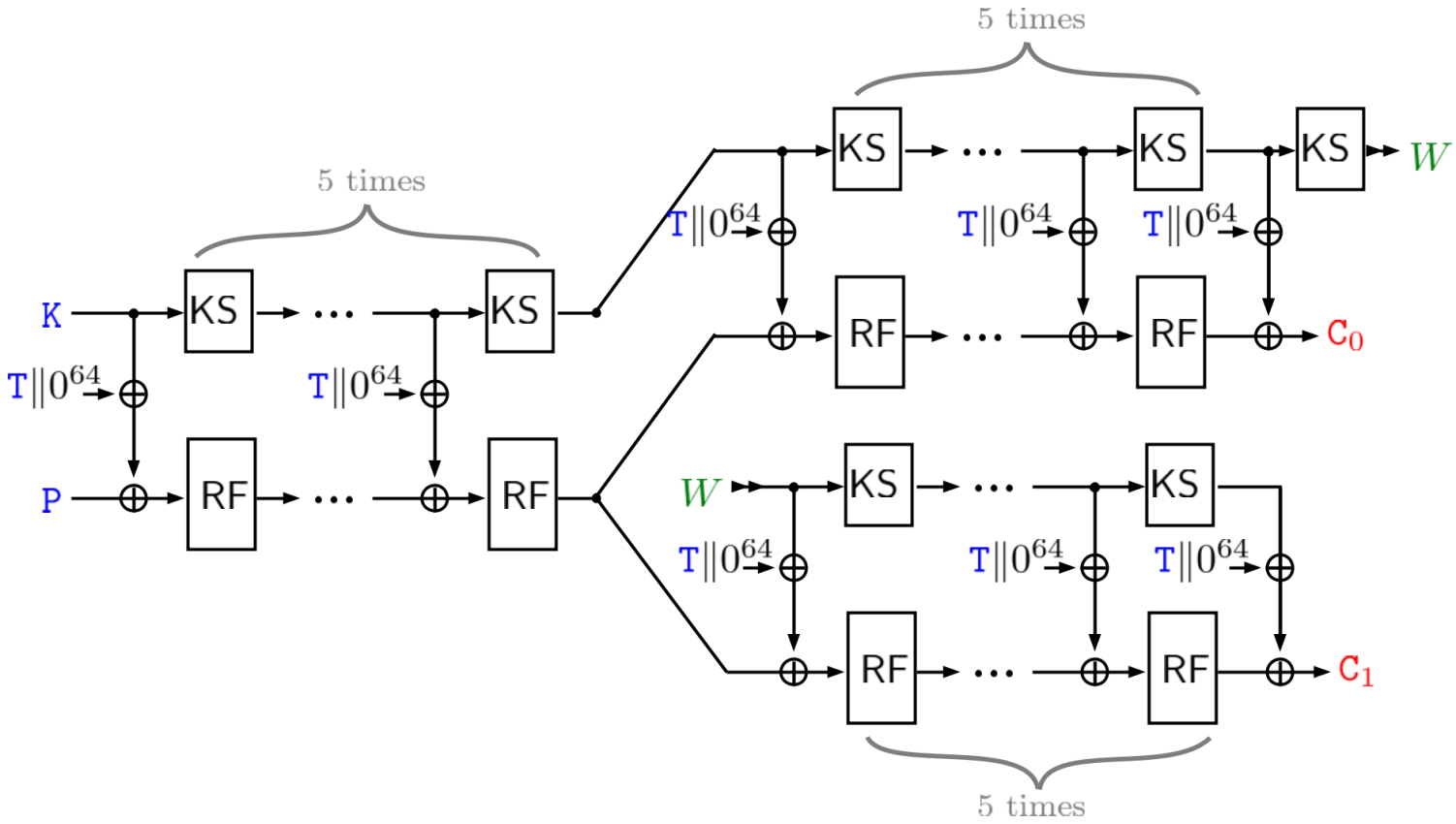
- IFI: **Round Function + Tweakey Schedule + #rounds/3**
- **No pathological structural weakness** (3 tweakable rand. perm. => perfectly secure)

ForkAES = IFI[KIASU,r=5]



- RF and KS from AES, 64 bit tweak

ForkAES = IFI[KIASU,r=5]



- RF and KS from AES, 64 bit tweak
- Provocative prototype: **Aggressively optimized for efficiency**

ForkAES: Security

- Mostly inherited from AES/KIASU
  - Differential/Linear propagation as in AES
  - Related tweakey properties as in KIASU

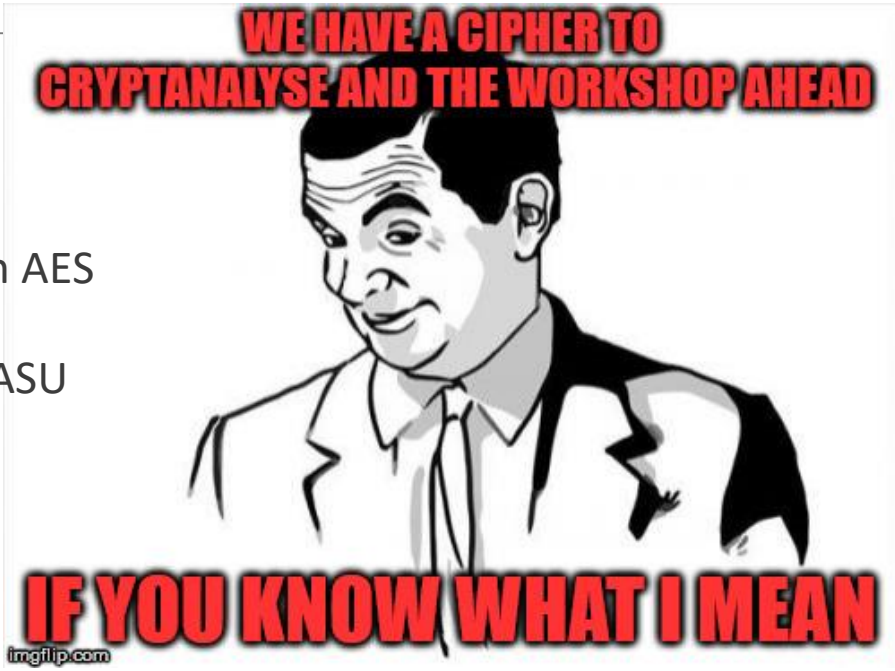
ForkAES: Security

- Mostly inherited from AES/KIASU
  - Differential/Linear propagation as in AES
  - Related tweakey properties as in KIASU
- **New attack vector in the fork?**

ForkAES: Security

- Mostly inherited from AES/KIASU
  - Differential/Linear propagation as in AES
  - Related tweakey properties as in KIASU
- **New attack vector in the fork?**
- **Seems so** [Bossert, List, Lucks 18]
  - Related tweakey rectangle on **9 rounds**
  - Related tweaky imposs. diff. on **9 rounds**
  - Sec margin: - 1 rnd compared to KIASU

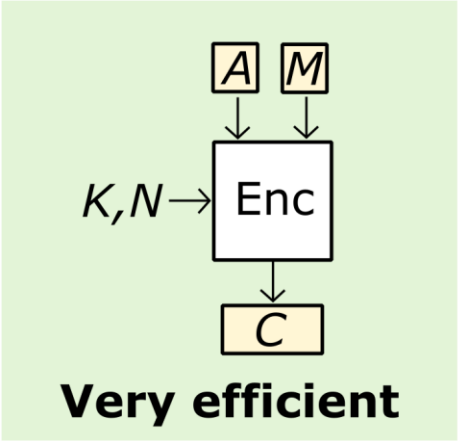
ForkAES: Security

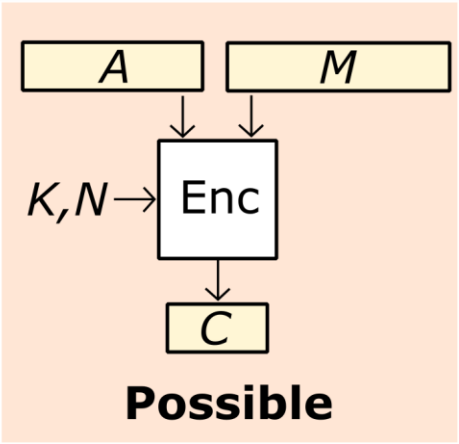


- Mostly inherited from AES/KIASU
  - Differential/Linear propagation as in AES
  - Related tweakey properties as in KIASU
- **New attack vector in the fork?**
- **Seems so** [Bossert, List, Lucks 18]
  - Related tweakey rectangle on **9 rounds**
  - Related tweaky imposs. diff. on **9 rounds**
  - Sec margin: - 1 rnd compared to KIASU
- **Need more cryptanalysis and constructive results**

Forkcipher Modes for Short-Input AE

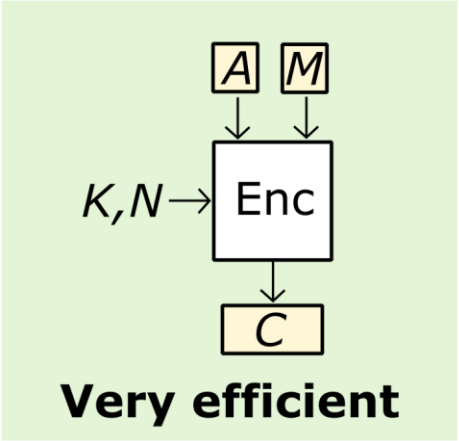
- Design target: Nonce-based AEAD
- Goal:

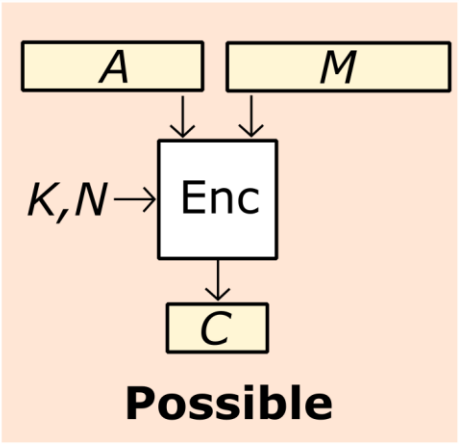




Forkcipher Modes for Short-Input AE

- Design target: Nonce-based AEAD
- Goal:

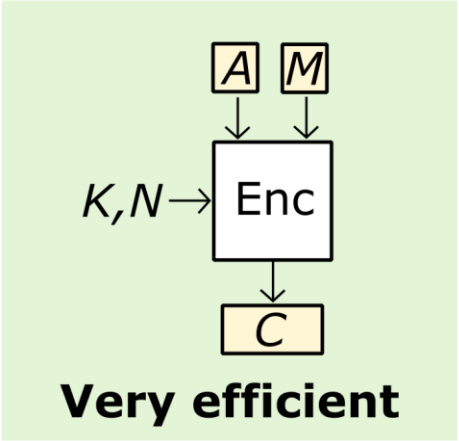


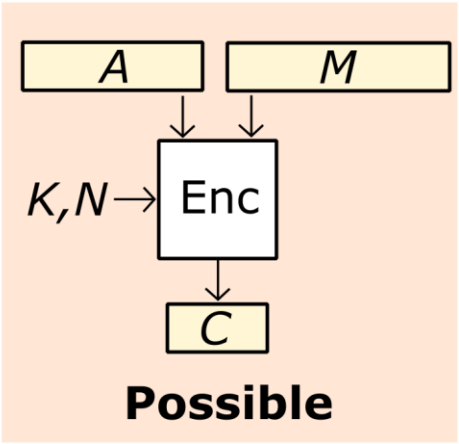


- **A single F-call for shortest messages**

Forkcipher Modes for Short-Input AE

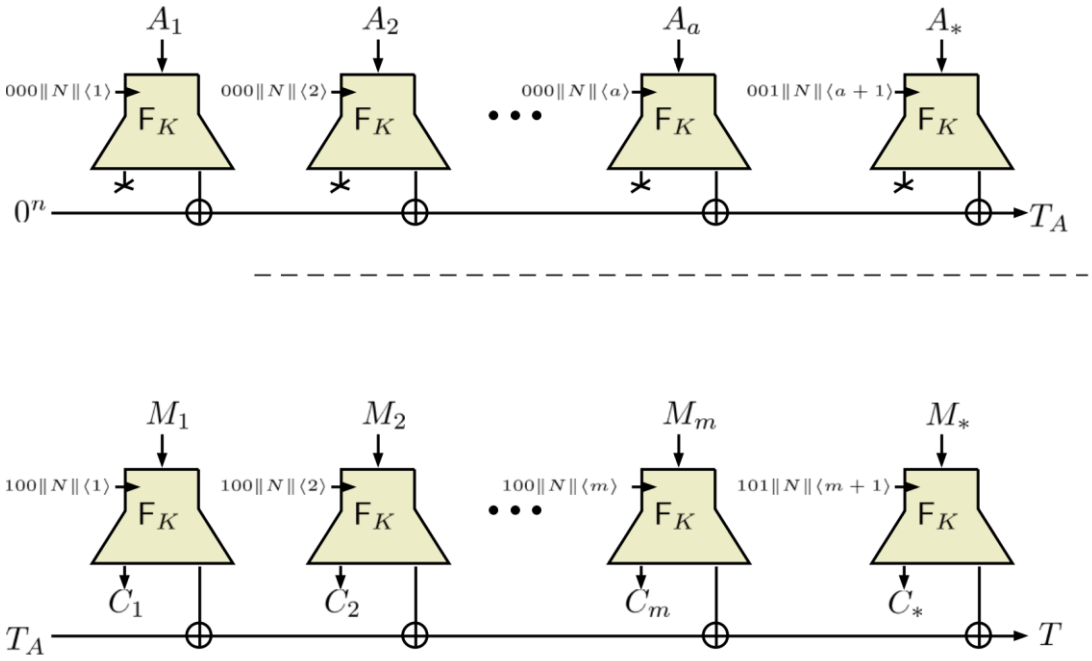
- Design target: Nonce-based AEAD
- Goal:





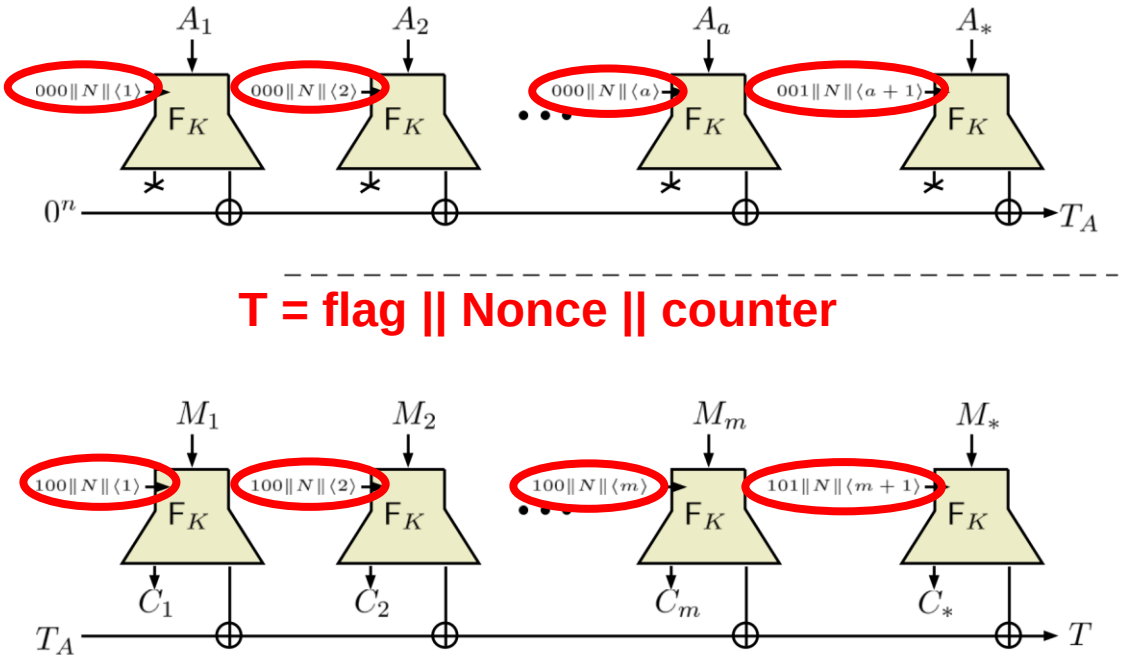
- **A single F-call for shortest messages**
- Parallelizable AE, Serial AE, a GCM variant

PAEF



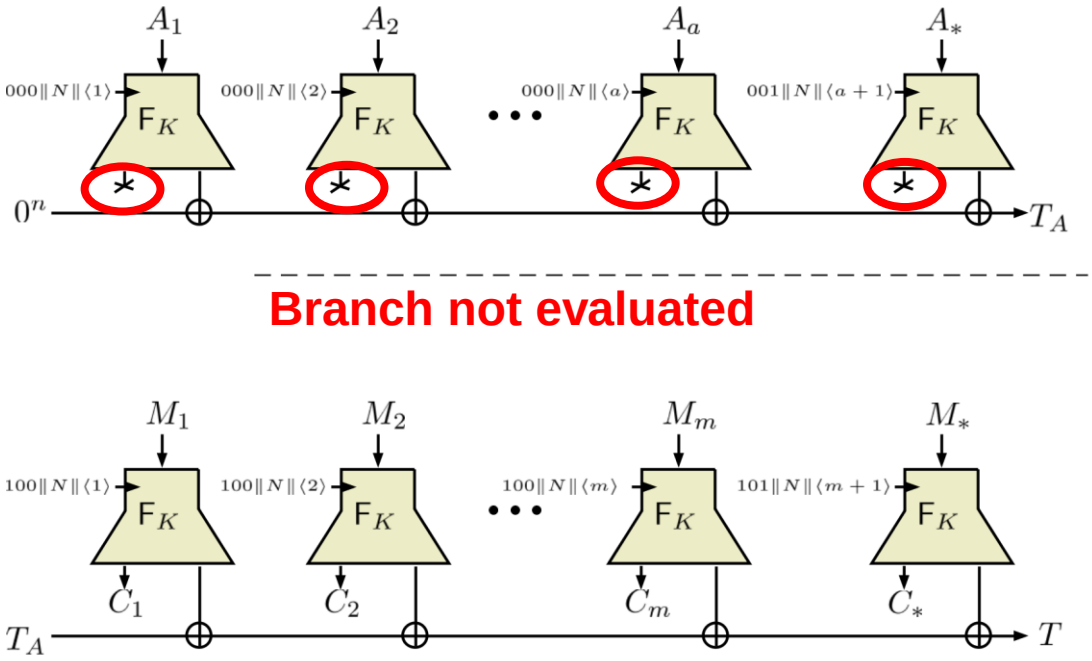
- Single F-call per block of data => **single F call for short queries**
- Ciphertext expansion: *n* bits
- Fully parallelizable

PAEF



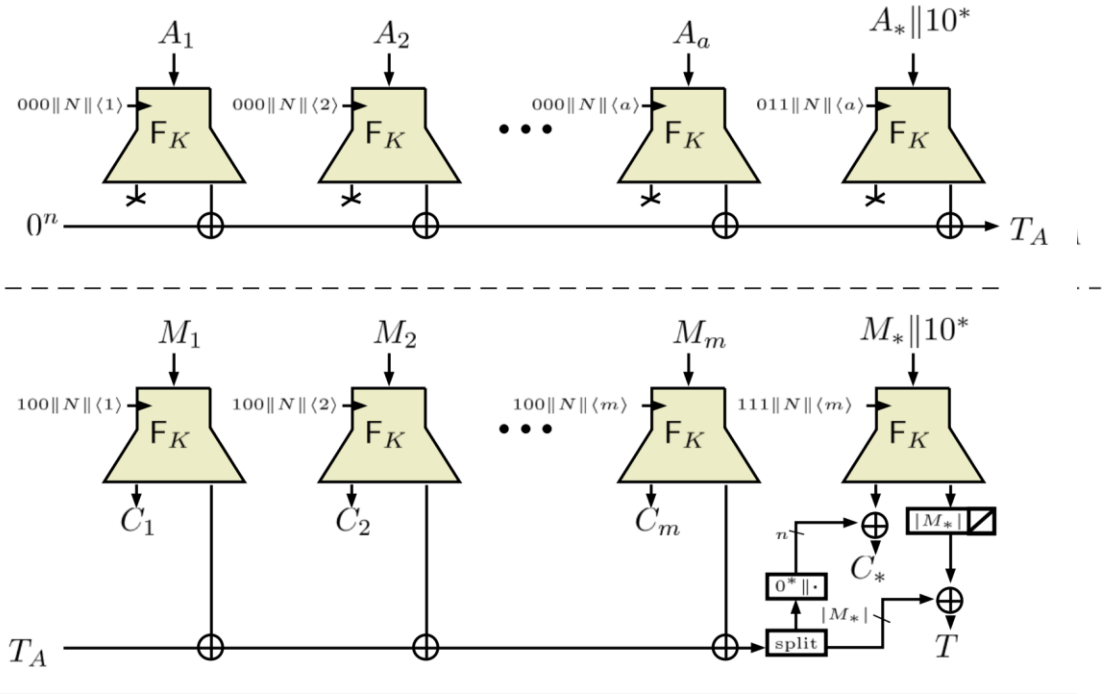
- Single F-call per block of data => **single F call for short queries**
- Ciphertext expansion: *n* bits
- Fully parallelizable

PAEF



- Single F-call per block of data => **single F call for short queries**
- Ciphertext expansion: *n* bits
- Fully parallelizable

PAEF



- Single F-call per block of data => **single F call for short queries**
- Ciphertext expansion: *n* bits
- Fully parallelizable

PAEF

q_v # of verification queries

n block size

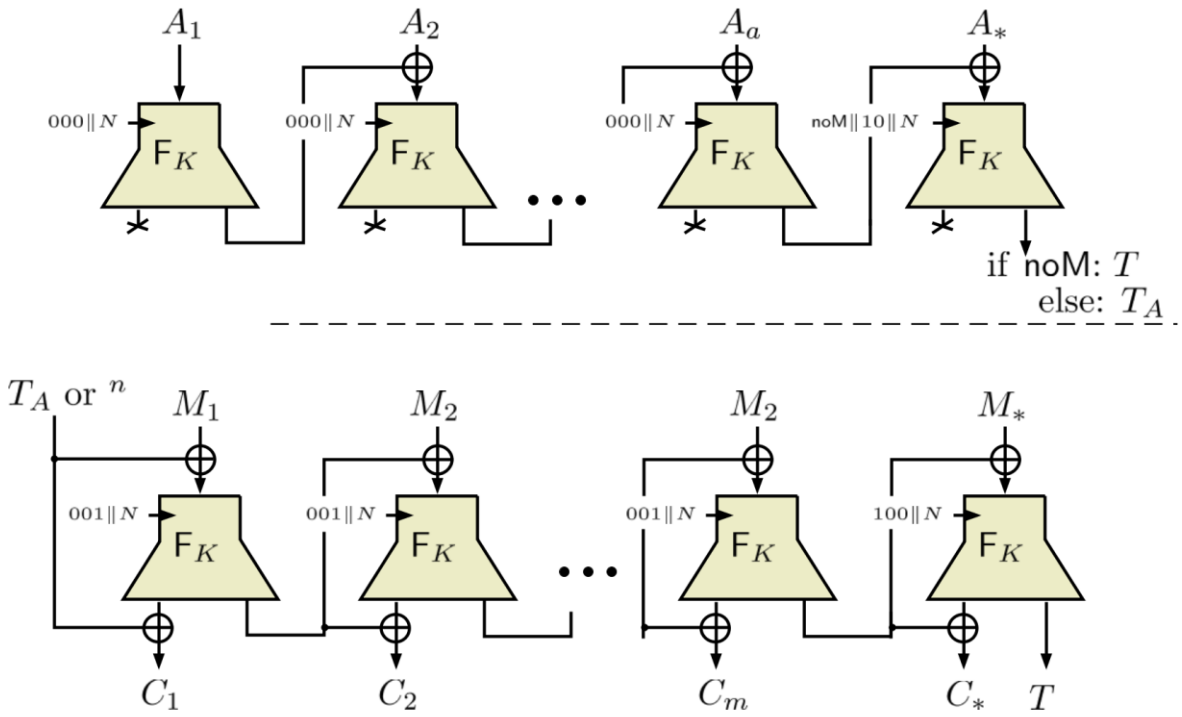
ν nonce size

Tradeoff: max # of enc: 2^{ν}; max len: $2^{|T|-(\nu+3)}$ blocks

$$\mathbf{Adv}^{\mathrm{priv}}_{\mathsf{PAEF}[\mathsf{F},\nu]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prtfp}}_{\mathsf{F}}(\mathcal{B})$$

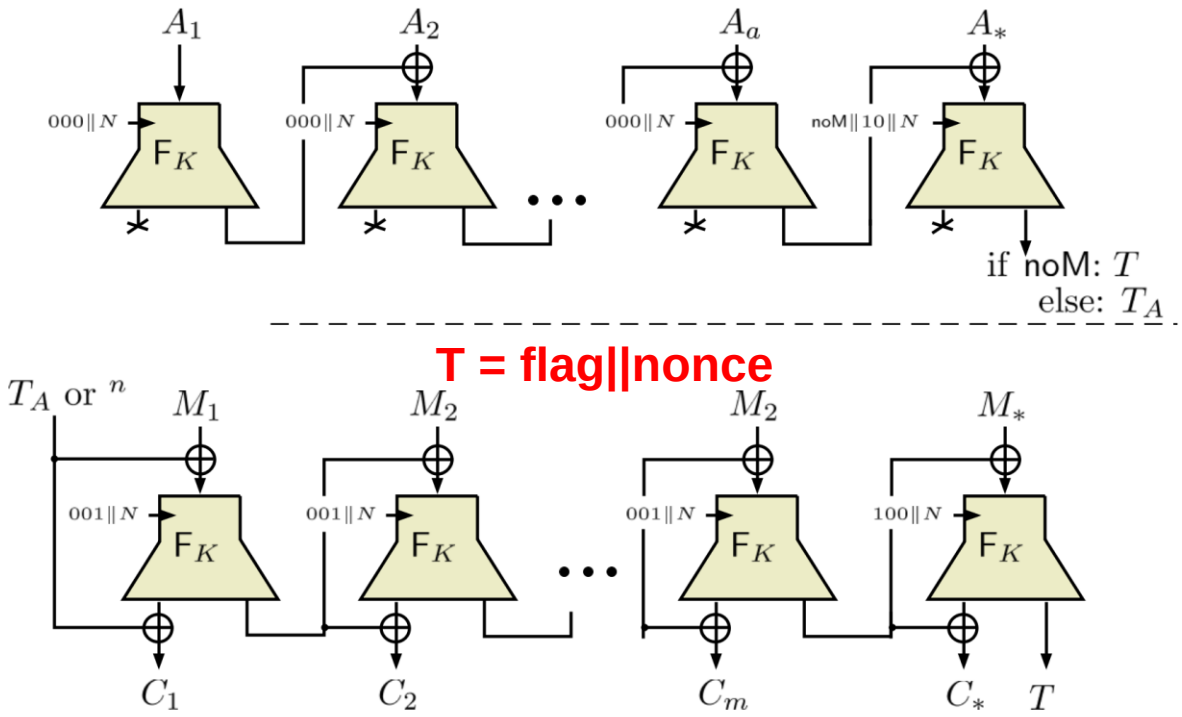
$$\mathbf{Adv}^{\mathrm{auth}}_{\mathsf{PAEF}[\mathsf{F},\nu]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prtfp}}_{\mathsf{F}}(\mathcal{C}) + \frac{q_v \cdot 2^n}{(2^n-1)^2}$$

SAEF



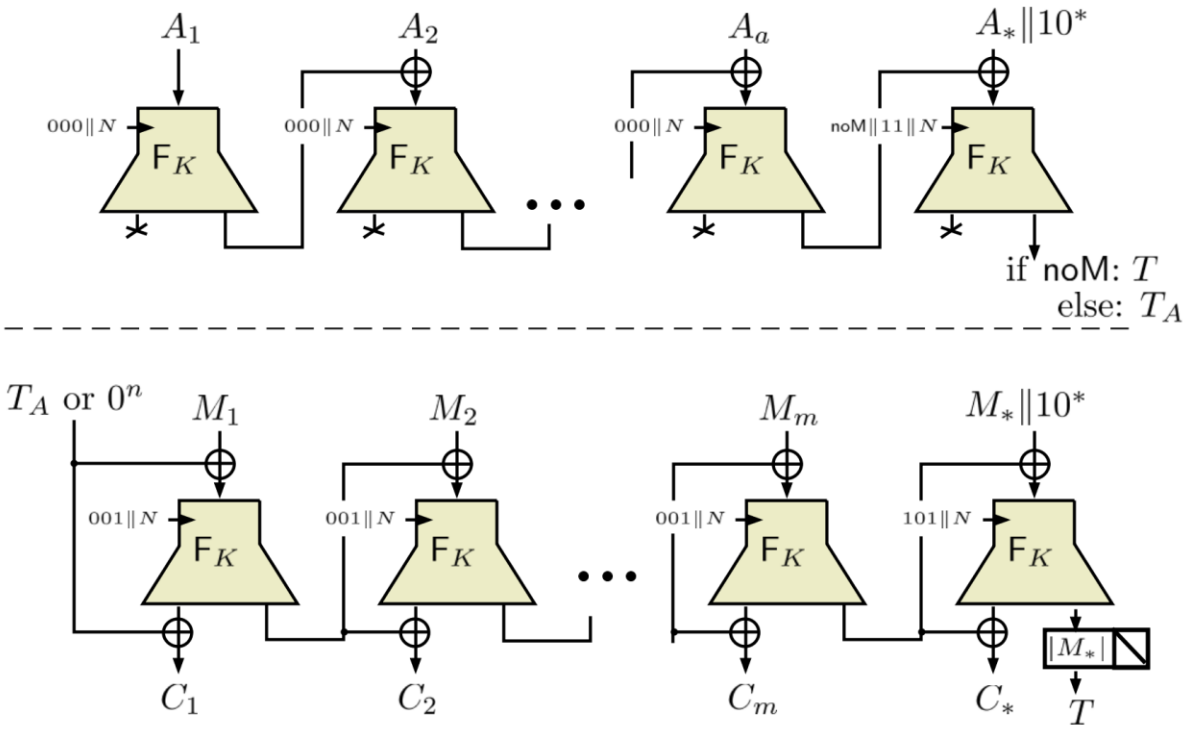
- Single F-call per block of data => **single F call for short queries**
- Ciphertext expansion: *n* bits
- No need to maintain a counter

SAEF



- Single F-call per block of data => **single F call for short queries**
- Ciphertext expansion: *n* bits
- No need to maintain a counter

SAEF



- Single F-call per block of data => **single F call for short queries**
- Ciphertext expansion: *n* bits
- No need to maintain a counter

SAEF

$\boldsymbol{L}$ set of possible block lengths

$\boldsymbol{\ell_{\max}}$ maximal blocklength (A or M)

$\boldsymbol{q_\ell}$ # of Enc queries w/ ℓ blocks $= \max|A|, |M|$

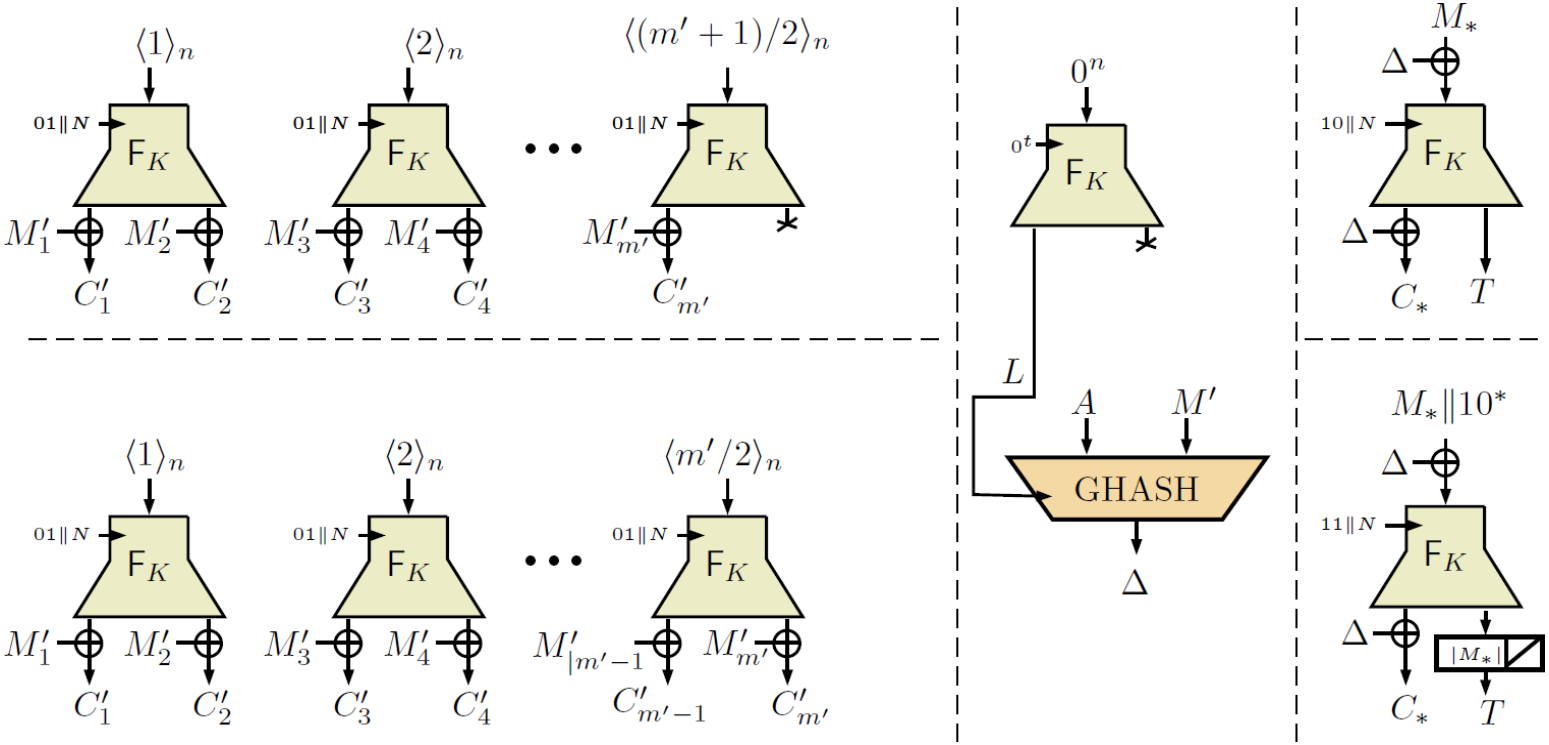
$\boldsymbol{q_v}$ # of verification queries

$\boldsymbol{n}$ block size

$$\mathbf{Adv}^{\text{priv}}_{\text{SAEF[F]}}(\mathcal{A}) \leq \mathbf{Adv}^{\text{prtfp}}_{\text{F}}(\mathcal{B}) + \sum_{\ell \in L} 3 \cdot \frac{\mathbf{q}_\ell \cdot \ell \cdot (\ell - 1)}{2^n}$$

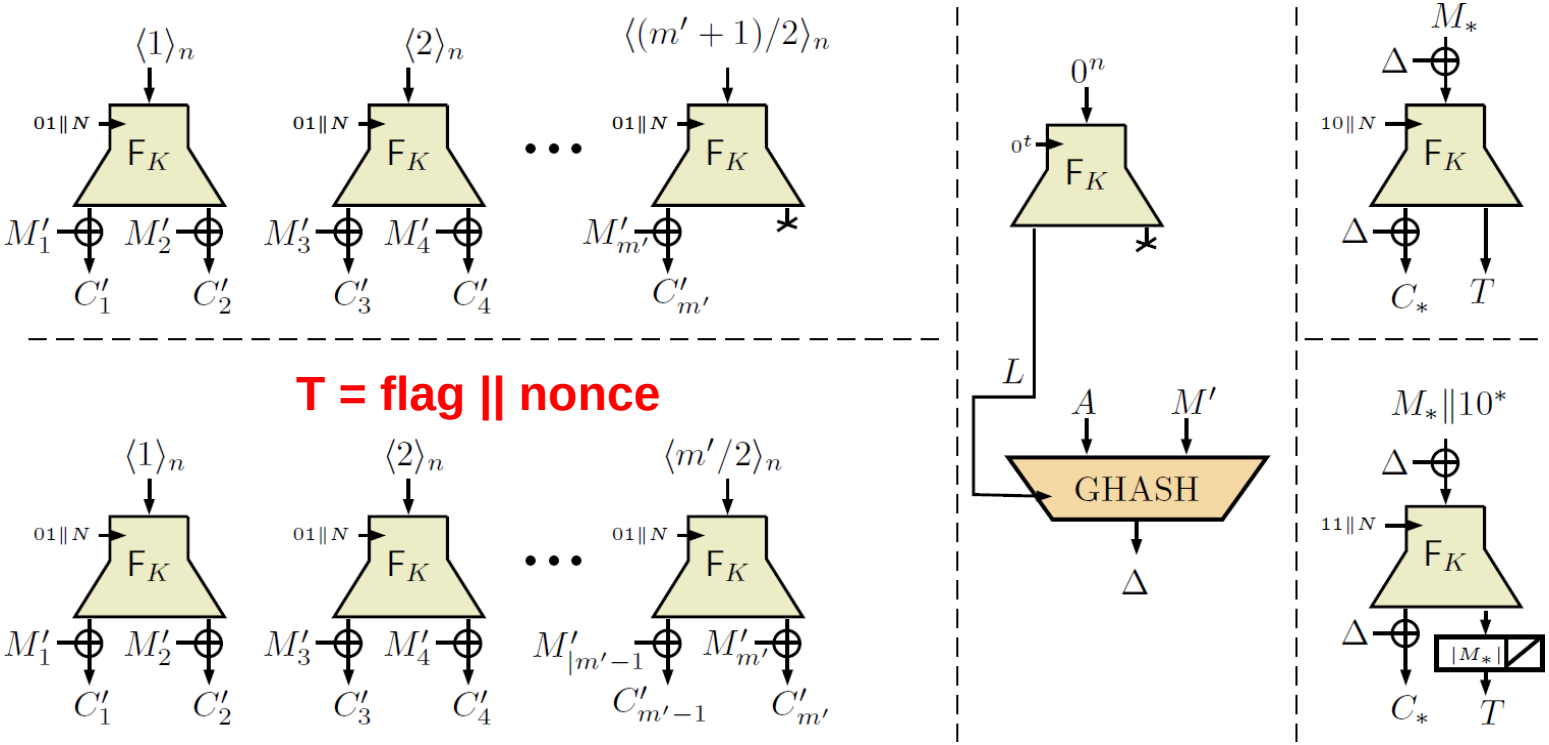
$$\mathbf{Adv}^{\text{auth}}_{\text{SAEF[F]}}(\mathcal{A}) \leq \mathbf{Adv}^{\text{prtfp}}_{\text{F}}(\mathcal{C}) + \sum_{\ell \in L} \frac{\mathbf{q}_\ell \cdot 3\ell \cdot (\ell - 1)}{2^n} + \frac{q_v \cdot (2\ell_{\max} + 1)}{2^n} + \frac{q_v}{(2^n - 1)}$$

fGCM



- F-call per **2 blocks** of *M,* last block = 1 F-call
- Ciphertext expansion: n bits
- Strictly more efficient than GCM

fGCM



- F-call per **2 blocks** of *M,* last block = 1 F-call
- Ciphertext expansion: n bits
- Strictly more efficient than GCM

fGCM

$\boldsymbol{L}$ set of possible block lengths

$\boldsymbol{\ell_{\max}}$ maximal blocklength (A or M)

$\boldsymbol{q_\ell}$ # of Enc queries w/ ℓ blocks $= \max|A|, |M|$

$\boldsymbol{q_v}$ # of verification queries

$\boldsymbol{n}$ block size

$$\mathbf{Adv}^{\mathrm{priv}}_{\mathsf{fGCM[F]}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prtfp}}_{\mathsf{F}}(\mathcal{B}) + \sum_{\ell \in L} \frac{\mathbf{q}_\ell \cdot \ell \cdot (\ell - 1)}{2^n}$$

$$\mathbf{Adv}^{\mathrm{auth}}_{\mathsf{fGCM[F]}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prtfp}}_{\mathsf{F}}(\mathcal{C}) + \frac{q_v \cdot \ell_{\max}}{2^n} + \frac{q_v \cdot 2^n}{(2^n - 1)^2}$$

Forkcipher Modes vs Very Short Messages

scheme	Cost of encryption in (# of AES rounds)/10 + GF(2^{128})mul									
	$a=0$				$a=1$				$a=2$	
	m=1	m=2	m=3	m=4	m=0	m=1	m=2	m=3	m=1	m=2
GCM	2+2	3+3	4+4	5+5	1+2	2+3	3+4	4+5	2+4	3+5
CCM	4	6	8	10	3	5	7	9	6	8
OCB3	3	4	5	6	3	4	5	6	5	6
CLOC	3	5	7	9	2	4	6	8	5	7
Deoxys-I	2.8	4.2	5.6	7	2.8	4.2	5.6	7	5.6	7
KIASU$^{\neq}$	2	3	4	5	2	3	4	5	4	5
PAEF	1.5	3	4.5	6	1.5	2.5	4	5.5	3.5	5
SAEF	1.5	3	4.5	6	1.5	2.5	4	5.5	3.5	5
fGCM	1.5+1	2.5+2	3+3	5+4	1.5+2	1.5+2	2.5+3	3+4	1.5+3	2.5+4

a,m: length of A and M in 128-bit blocks; per-session key derivation excluded

Conclusion

- **Forkcipher**
  - Expanding, almost AE-security
  - Aspiration: as 2 TBCs at lower cost
  - Aggressive prototype: **ForkAES** @ 1.5 AES-128

Conclusion

- **Forkcipher**
  - Expanding, almost AE-security
  - Aspiration: as 2 TBCs at lower cost
  - Aggressive prototype: **ForkAES** @ 1.5 AES-128
- **Forkcipher modes:**
  - Faster than all AES-based modular designs for **very short messages**

Conclusion

- **Forkcipher**
  - Expanding, almost AE-security
  - Aspiration: as 2 TBCs at lower cost
  - Aggressive prototype: **ForkAES** @ 1.5 AES-128
- **Forkcipher modes:**
  - Faster than all AES-based modular designs for **very short messages**
- **Open problems:**
  - Cryptanalysis of IFI, new instances
  - Modes: same efficiency, tunable expansion
  - Other applications of forkcipher (e.g., stream in fGCM)
  - Forkcipher ≠ PRI (Bday gap); a tweakable FIL PRI primitive?

Thank you for your attention!

Follow us on

www.csem.ch