APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography

Elena Andreeva, Begül Bilgin, Andrey Bogdanov, Atul Luykx, Bart Mennink, Nicky Mouha, Kan Yasuda

KU Leuven, UTwente, DTU, NTT

FSE 2014 — March 3, 2014

Authenticated Encryption

- Privacy
- Authenticity

Authenticated Encryption for Lightweight Cryptography

Authenticated Encryption

- Privacy
- Authenticity

Lightweight

- Constrained environments
- Online
- Nonce-reuse

Authenticated Encryption for Lightweight Cryptography

Authenticated Encryption

- Privacy
- Authenticity

Lightweight

- Constrained environments
- Online
- Nonce-reuse

Primitive

- Block cipher
- Permutation

Authenticated Encryption for Lightweight Cryptography

Authenticated Encryption

- Privacy
- Authenticity

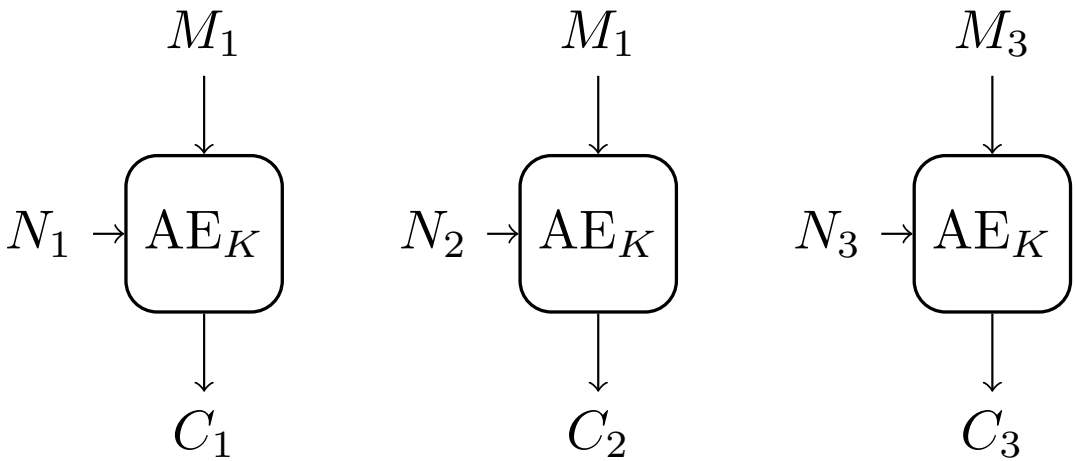
Lightweight

- Constrained environments
- Online
- Nonce-reuse

Primitive

- Block cipher ✗
- Permutation ✓

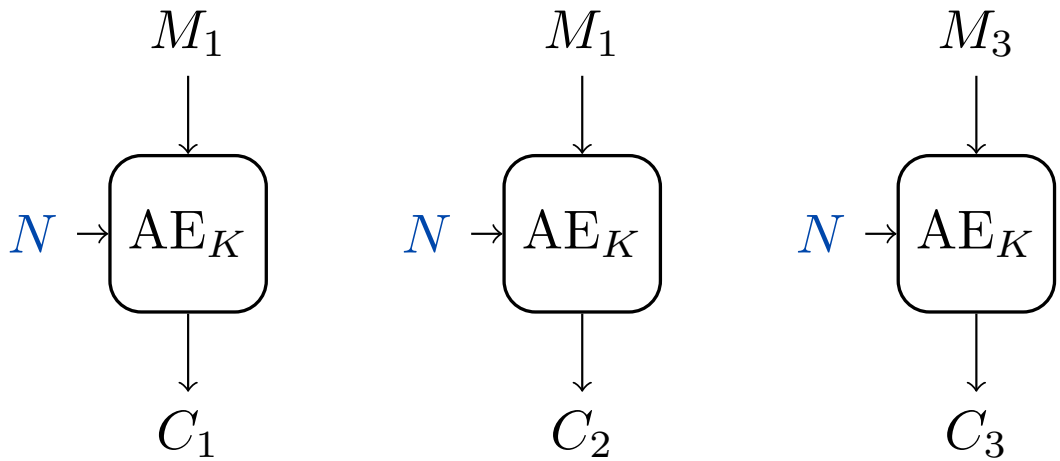
Misuse Resistance



Nonce

- Counter or random number
- Requires non-volatile memory or hardware randomness

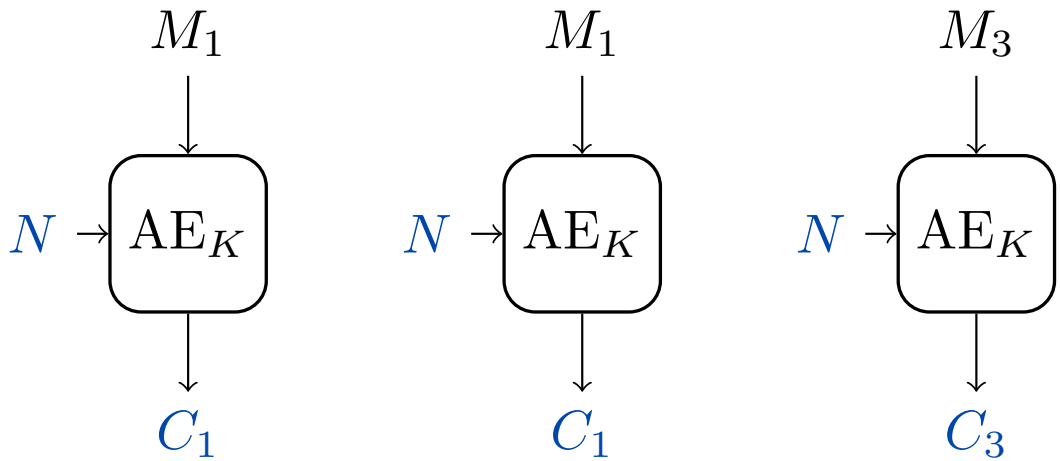
Misuse Resistance



Nonce

- Counter or random number
- Requires non-volatile memory or hardware randomness

Misuse Resistance

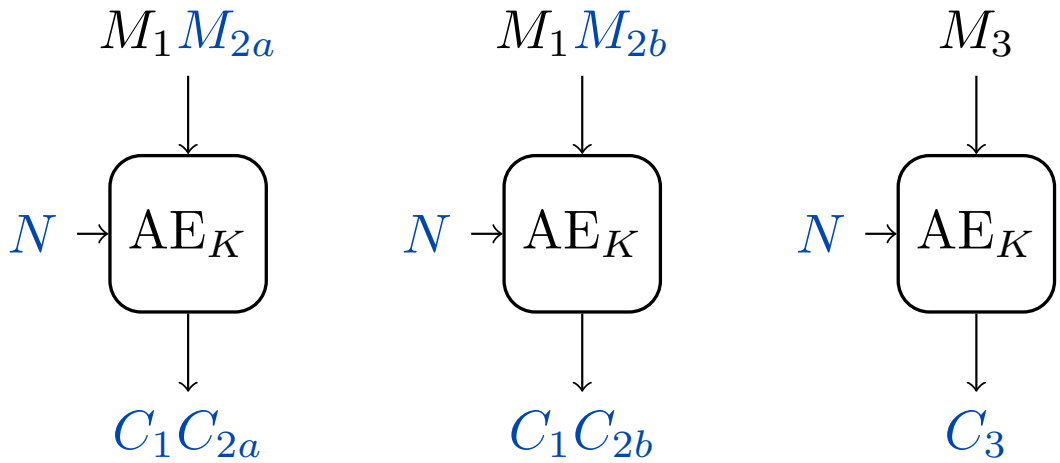


Nonce

- Counter or random number
- Requires non-volatile memory or hardware randomness

Misuse Resistance

Misuse Resistance



Nonce

- Counter or random number
- Requires non-volatile memory or hardware randomness

Misuse Resistance

- Online misuse resistance
- Security up to common prefix

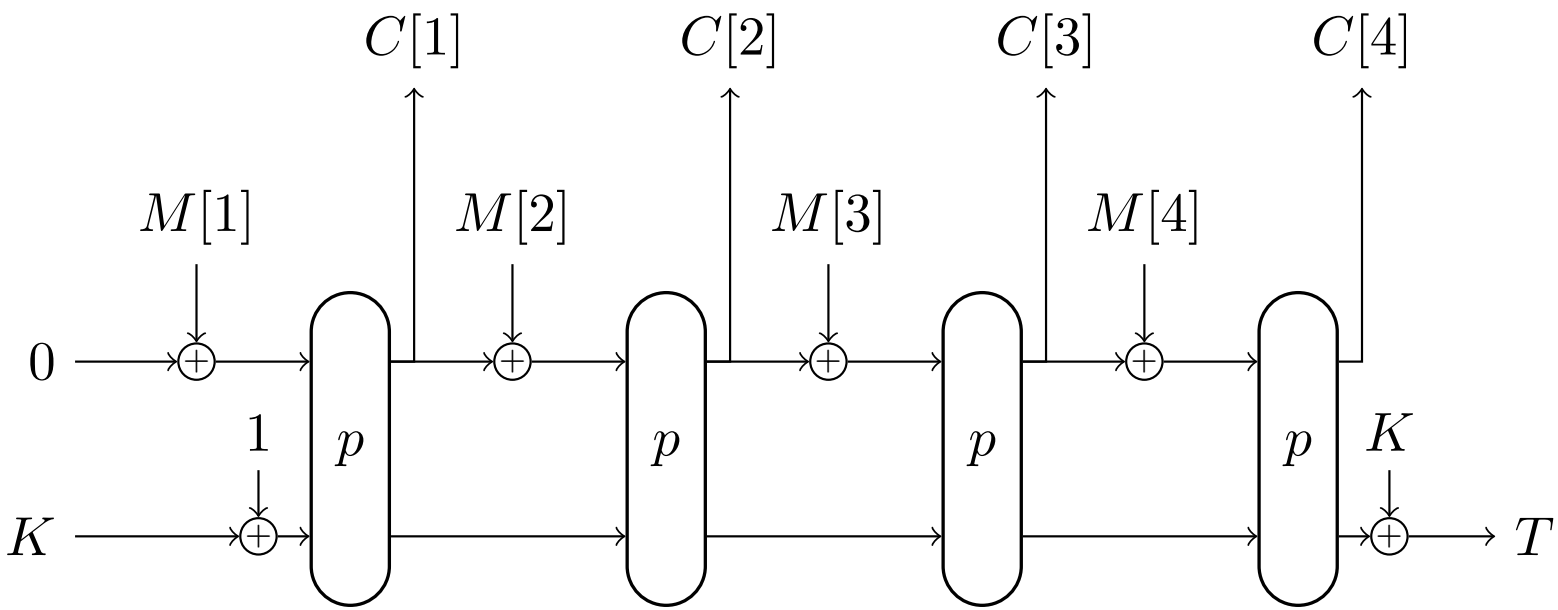
State of the Art

	nonce-dependent	**misuse resistant**
block cipher	IAPM '00, OCB '01 XECB '01, CCM '03 GCM '04, CLOC '14	SIV '06, BTM '09 McOE-G '11, COPA '13 POET '14, COBRA '14
permutation	SpongeWrap '11 Keyak&Ketje '14 NORX '14	

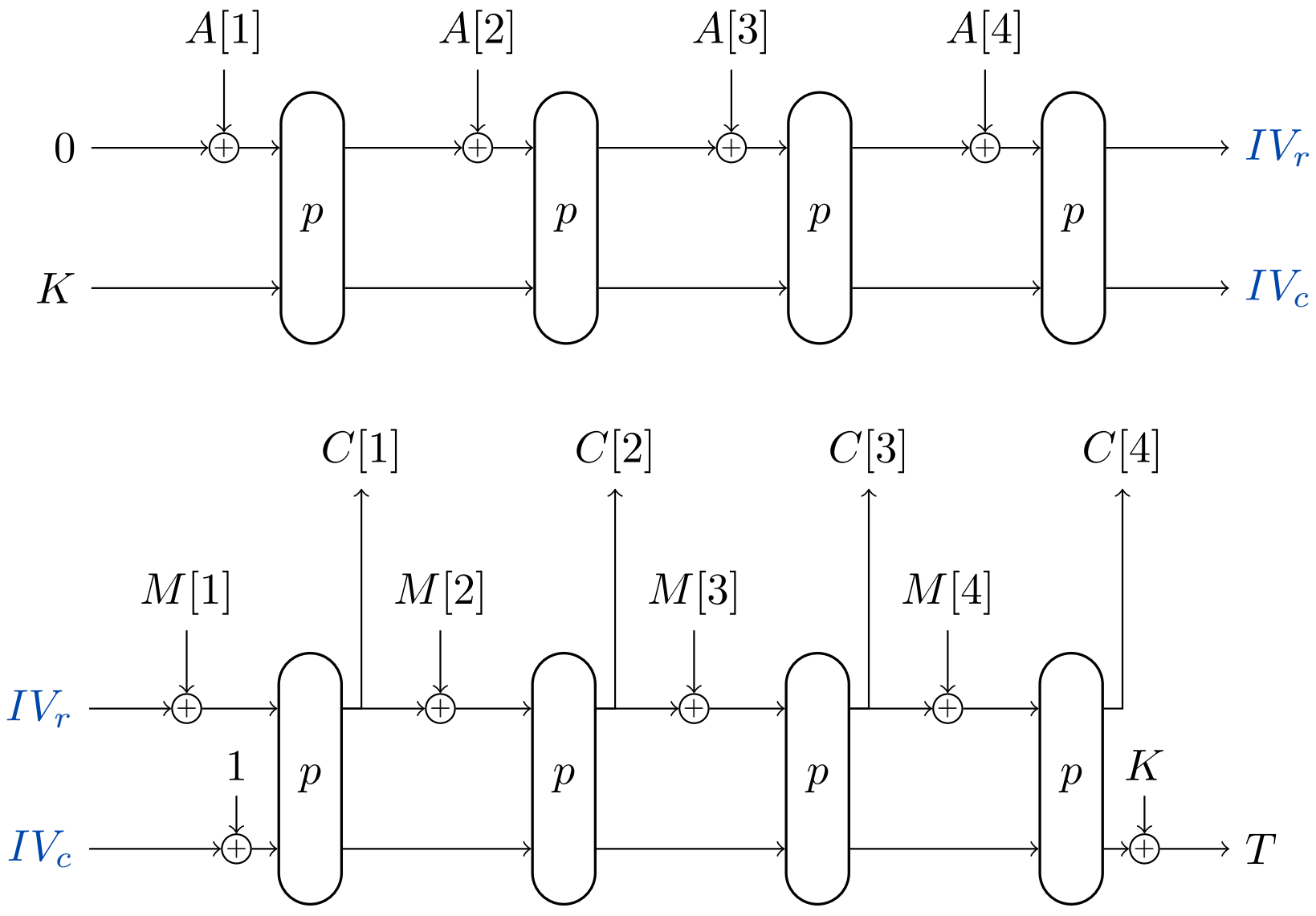
State of the Art

	nonce-dependent	**misuse resistant**
block cipher	IAPM '00, OCB '01 XECB '01, CCM '03 GCM '04, CLOC '14	SIV '06, BTM '09 McOE-G '11, COPA '13 POET '14, COBRA '14
permutation	SpongeWrap '11 Keyak&Ketje '14 NORX '14	**APE**

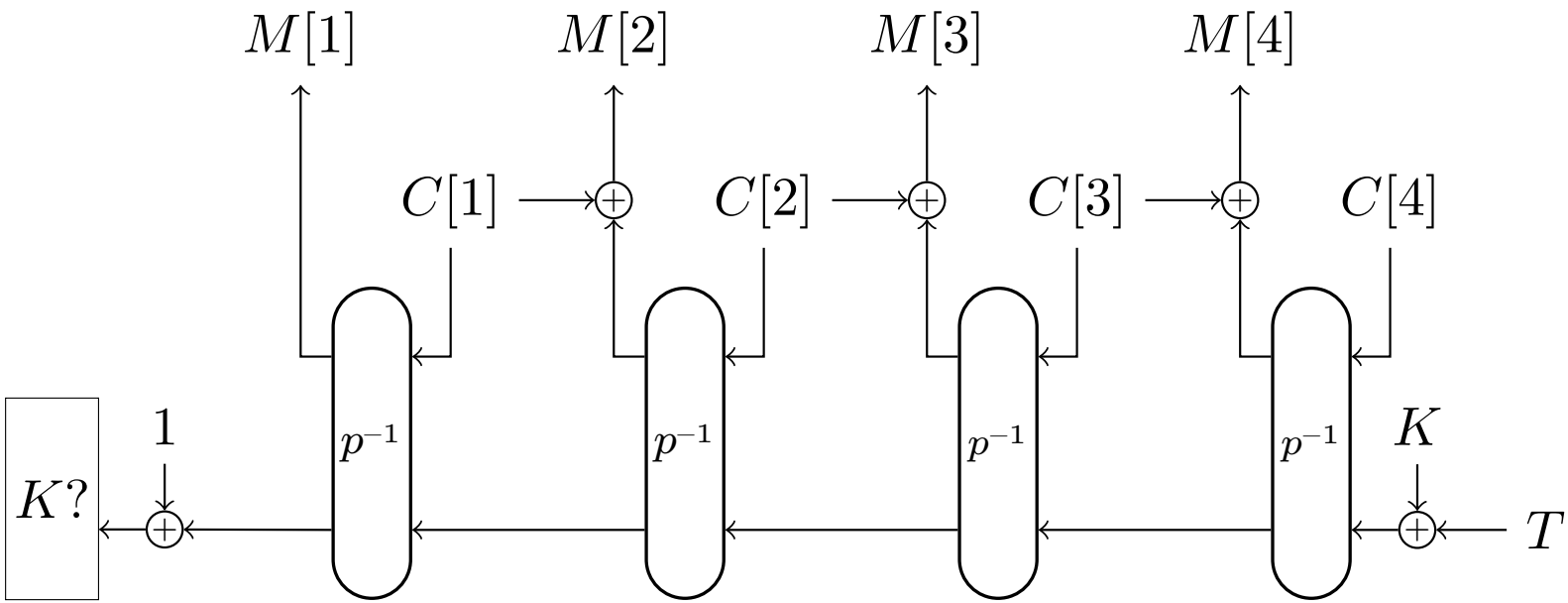
APE



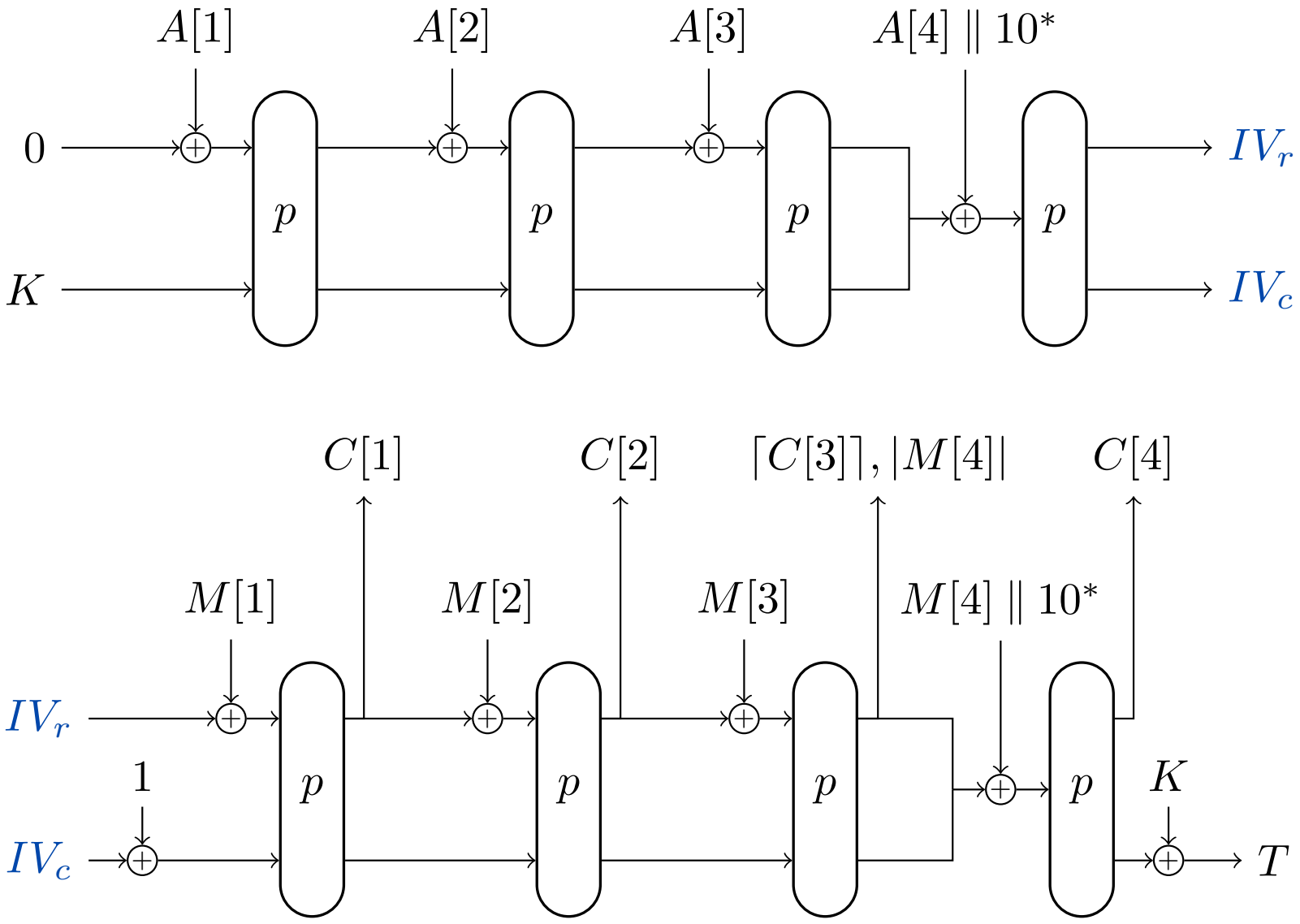
APE: Associated Data



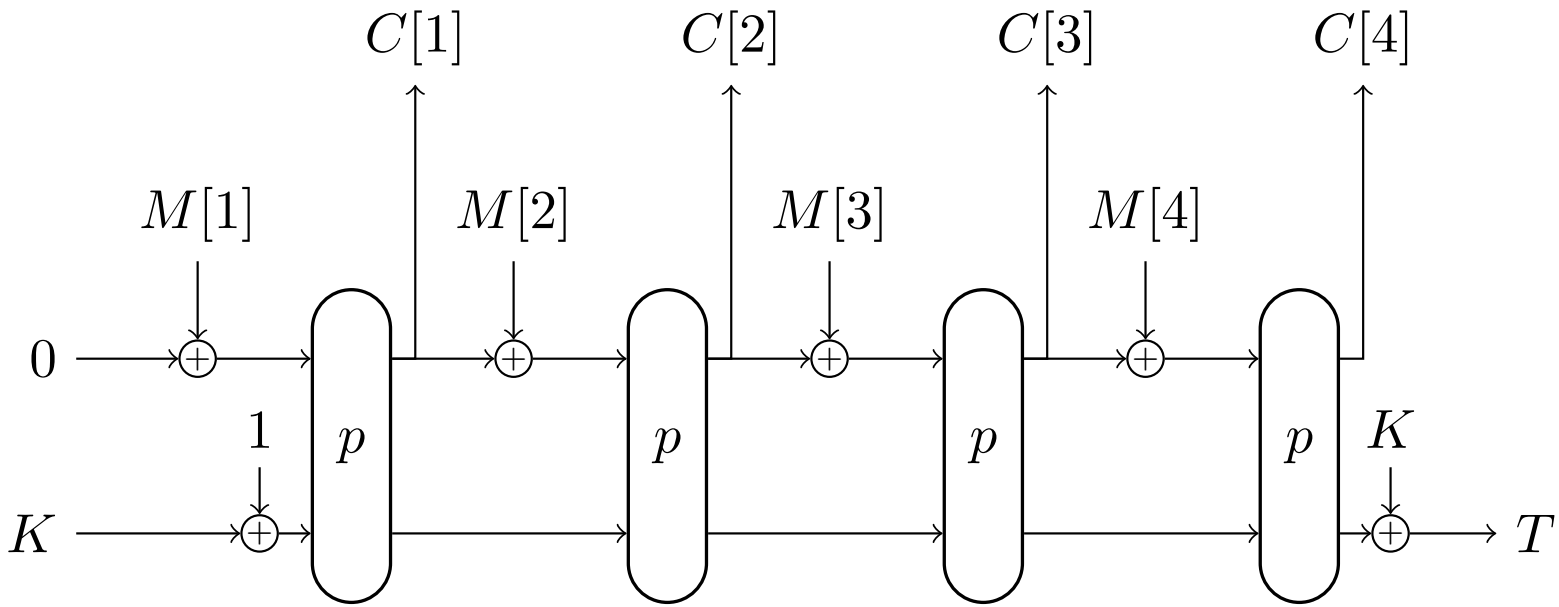
APE: Decryption and Verification



APE: Fractional Messages and Associated Data

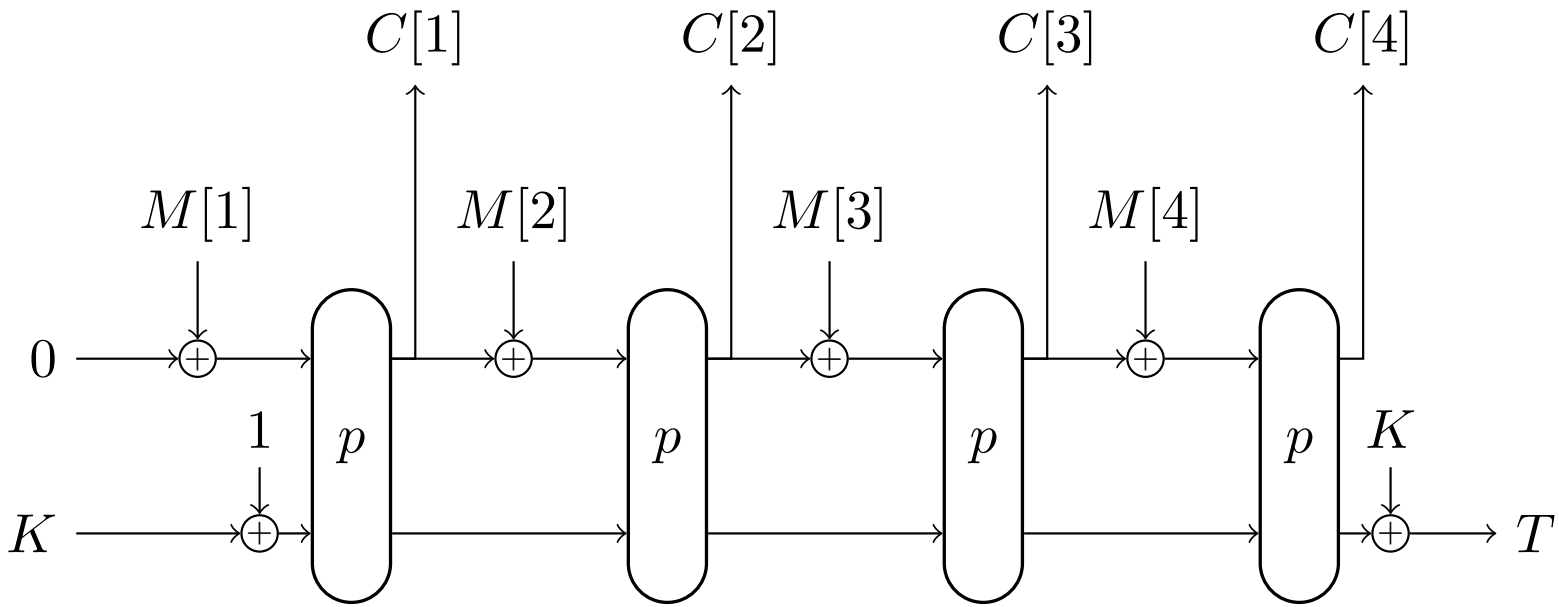


APE: Security



Ideal Permutation Model

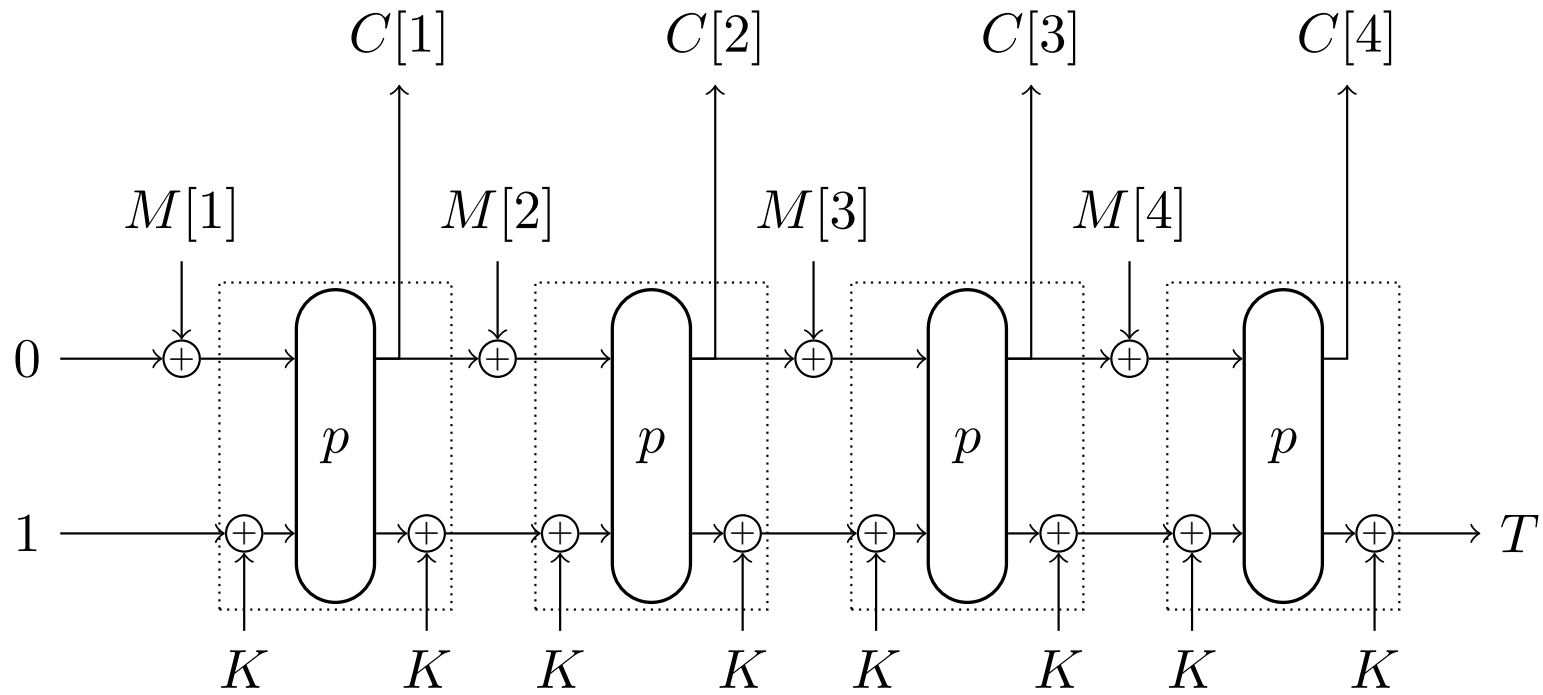
APE: Security



Ideal Permutation Model

- Privacy: $2^{c/2}$
- Integrity: $2^{c/2}$

APE: Security



Ideal Permutation Model

- Privacy: $2^{c/2}$
- Integrity: $2^{c/2}$

Standard Cipher Model

- $E := \oplus_{0\|K} \circ p \circ \oplus_{0\|K}$
- Privacy: $2^{c/2} + \mathsf{sprp}(E)$
- Integrity: $2^{c/2} + \mathsf{sprp}(E)$

APE: Hardware Implementation

Two platforms

- Faraday Standard Cell Library on UMC 180nm
- Open-cell 45nm NANGATE library

APE: Hardware Implementation

Two platforms

- Faraday Standard Cell Library on UMC 180nm
- Open-cell 45nm NANGATE library

Permutation

- Permutation from Photon/Quark/Spongent
- APE enc/dec

APE: Hardware Implementation

Two platforms

- Faraday Standard Cell Library on UMC 180nm
- Open-cell 45nm NANGATE library

Permutation

- Permutation from Photon/Quark/Spongent
- APE enc/dec

Parameters

- Security: 80, 128 bits
- Rate: 16, 32 bits

APE: Implementation Results

APE enc/dec

- 1309 GE: smallest impl. with 80-bit security
- 2104 GE: smallest impl. with 128-bit security

APE: Implementation Results

APE enc/dec

- 1309 GE: smallest impl. with 80-bit security
- 2104 GE: smallest impl. with 128-bit security

Decryption overhead

- Implement both p and p^{-1}
- 45nm: overhead $\leq$ 283 GE

APE: Implementation Results

APE enc/dec

- 1309 GE: smallest impl. with 80-bit security
- 2104 GE: smallest impl. with 128-bit security

Decryption overhead

- Implement both p and p^{-1}
- 45nm: overhead $\leq$ 283 GE

Area comparison

- $\approx$ ALE
- $\ll$ ASC-1 A, ASC-1 B, AES-CCM

Conclusions

Features

- First permutation-based online misuse-resistant AE
- Easy processing of fractional data
- Ideal for lightweight
- Ideal model security proof
- Standard model security proof

Thank you for your attention!

Questions?

Supporting Slides

How to Securely Release Unverified Plaintext in Authenticated Encryption

Elena Andreeva Andrey Bogdanov Atul Luykx Bart Mennink
Nicky Mouha Kan Yasuda

KU Leuven, iMinds, DTU, NTT

eprint.iacr.org/2014/144

APE on UMC 180 nm

APE on UMC 180 nm CMOS process @ 100 kHz					
Design	Security (bits)	Rate (bits)	Latency (cycles)	Throughput (kbps)	Area (GE)
Photon-196	80	36	1248	2.9	1398
Photon-196 e/d	80	36	1297	2.8	1634
Quark-176	80	16	880	1.81	1694
Quark-176 e/d	80	16	880	1.81	1871
Spongent-176	80	16	4050	0.4	1423
Spongent-176 e/d	80	16	4094	0.4	1868
Photon-288	128	32	924	3.45	2154
Photon-288 e/d	128	32	960	3.33	2449
Quark-256	112	32	1270	2.51	2286
Quark-256 e/d	112	32	1270	2.51	2470
Spongent-272	128	16	4480	0.4	2105
Spongent-272 e/d	128	16	4652	0.3	2781

APE on NANGATE 45 nm

APE on NANGATE 45 nm CMOS process @ 100 kHz					
Design	Security (bits)	Rate (bits)	Latency (cycles)	Throughput (kbps)	Area (GE)
Photon-196	80	36	1248	2.9	1309
Photon-196 e/d	80	36	1297	2.8	1536
Quark-176	80	16	880	1.81	1606
Quark-176 e/d	80	16	880	1.81	1773
Spongent-176	80	16	4050	0.4	1598
Spongent-176 e/d	80	16	4094	0.4	1838
Photon-288	128	32	924	3.45	2104
Photon-288 e/d	128	32	960	3.33	2327
Quark-256	112	32	1270	2.51	2228
Quark-256 e/d	112	32	1270	2.51	2331
Spongent-272	128	16	4480	0.4	2378
Spongent-272 e/d	128	16	4652	0.3	2661

Other AE Schemes on ST 65 nm

Other AE schemes on ST 65 nm CMOS LP-HVT process @ 20 MHz

Design	Security (bits)	Latency (cycles)	Throughput (kbps)	Area (GE)
ALE	128	105	121.9	2579
ALE e/d	128	105	121.9	2700
ASC-1 A	128	370	34.59	4793
ASC-1 A e/d	128	370	34.59	4964
ASC-1 B	128	235	54.47	5517
ASC-1 B e/d	128	235	54.47	5632
AES-CCM	128	452	28.32	3472
AES-CCM e/d	128	452	28.32	3765