APE(X): Authenticated Permutation-Based Encryption with Extended Misuse Resistance

Atul Luykx

COSIC, KU Leuven

October 30, 2013

Joint work with A. Bogdanov, E. Andreeva, B. Mennink, N. Mouha, K. Yasuda

Stateless, Deterministic Encryption

$$E(M_1) = C_1 \qquad\qquad E(M_2) = C_2$$

$$M_1 = M_2 \Rightarrow C_1 = C_2$$

Nonces

$$E(N_1, M_1) = C_1 \qquad\qquad E(N_2, M_2) = C_2$$

$$N_1 \neq N_2 \text{ and } M_1 = M_2 \quad \not\Rightarrow \quad C_1 = C_2$$

Nonce Repetition

Nonce repeated? Usually no security guarantees.

Misuse Resistance.

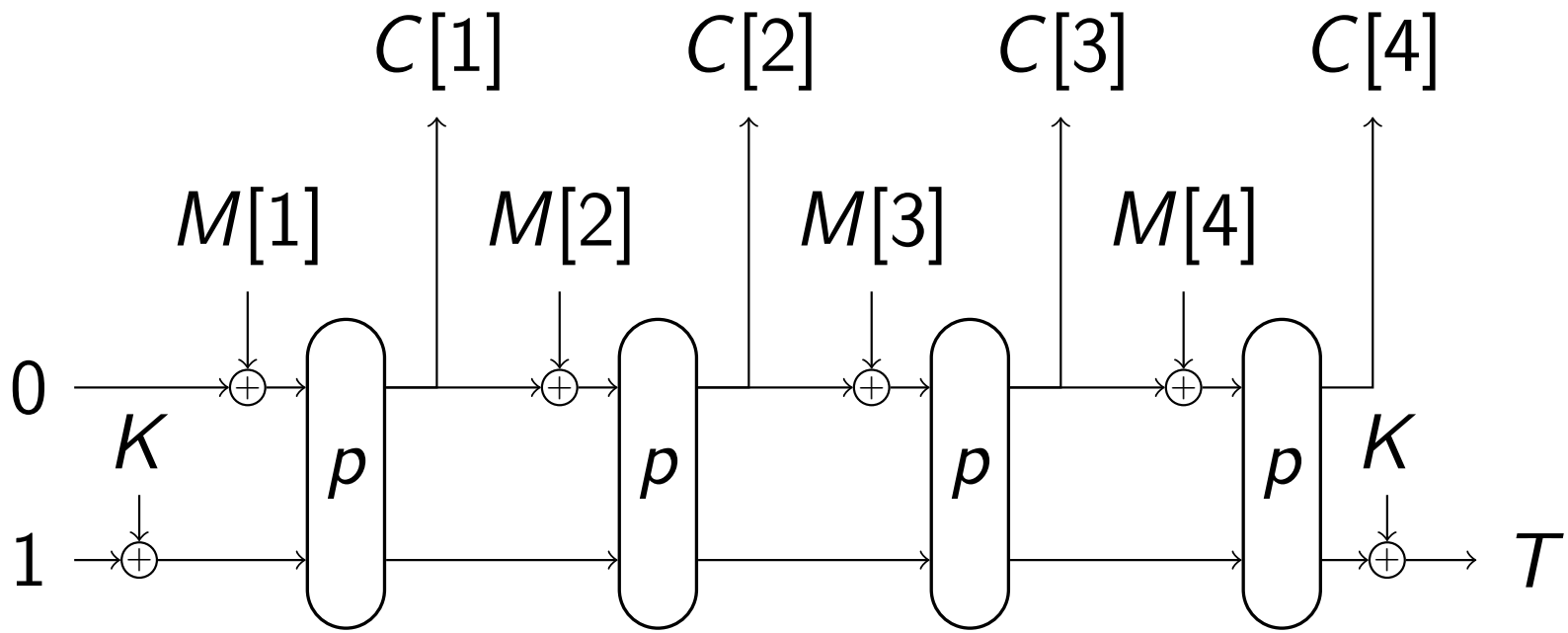
Some AE Schemes

	Nonce-dependent	**Misuse Resistant**
Block Cipher	IAPM '01, OCB '01 XECB '01, CCM '01 GCM '04	SIV '06 BTM '09 McOE-G '11
Permutation	SpongeWrap '11	

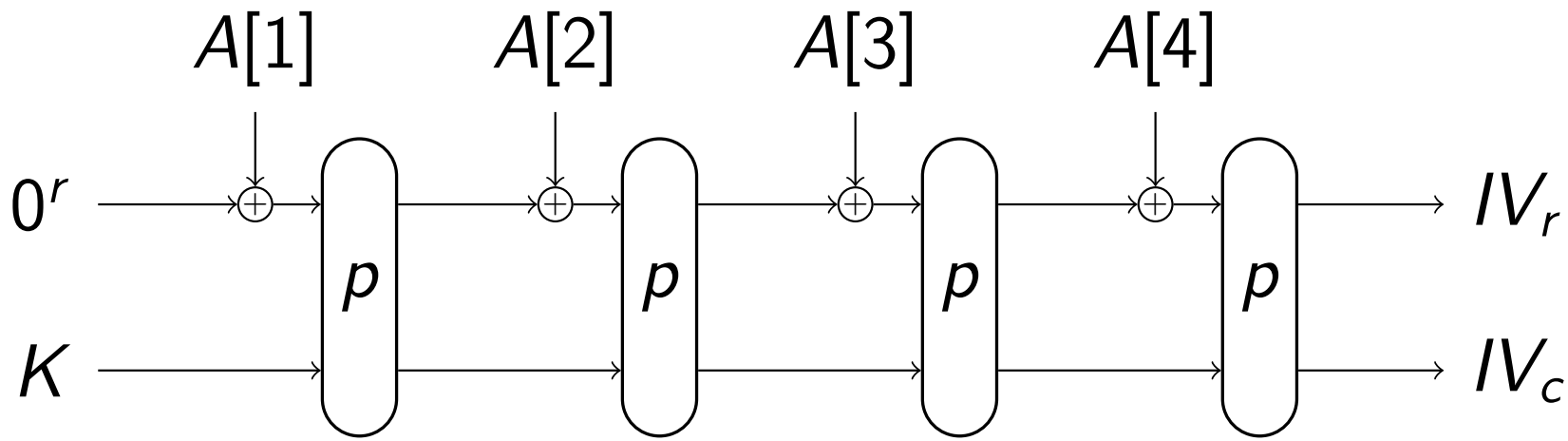
Some AE Schemes

	Nonce-dependent	**Misuse Resistant**
Block Cipher	IAPM '01, OCB '01 XECB '01, CCM '01 GCM '04	SIV '06 BTM '09 McOE-G '11
Permutation	SpongeWrap '11	APE

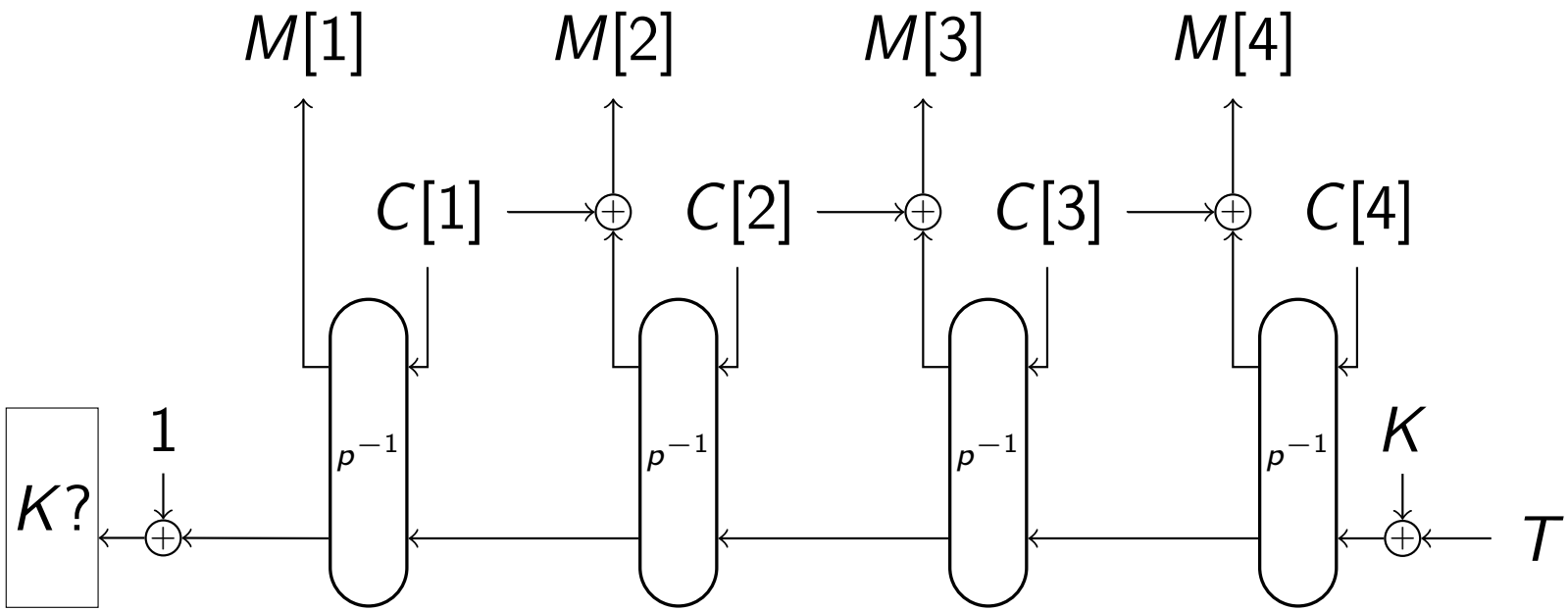
APE



APE - Associated Data



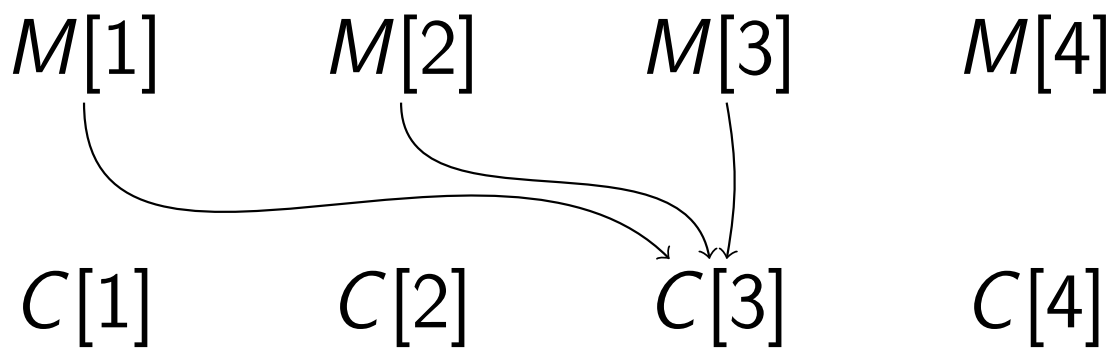
APE - Decryption



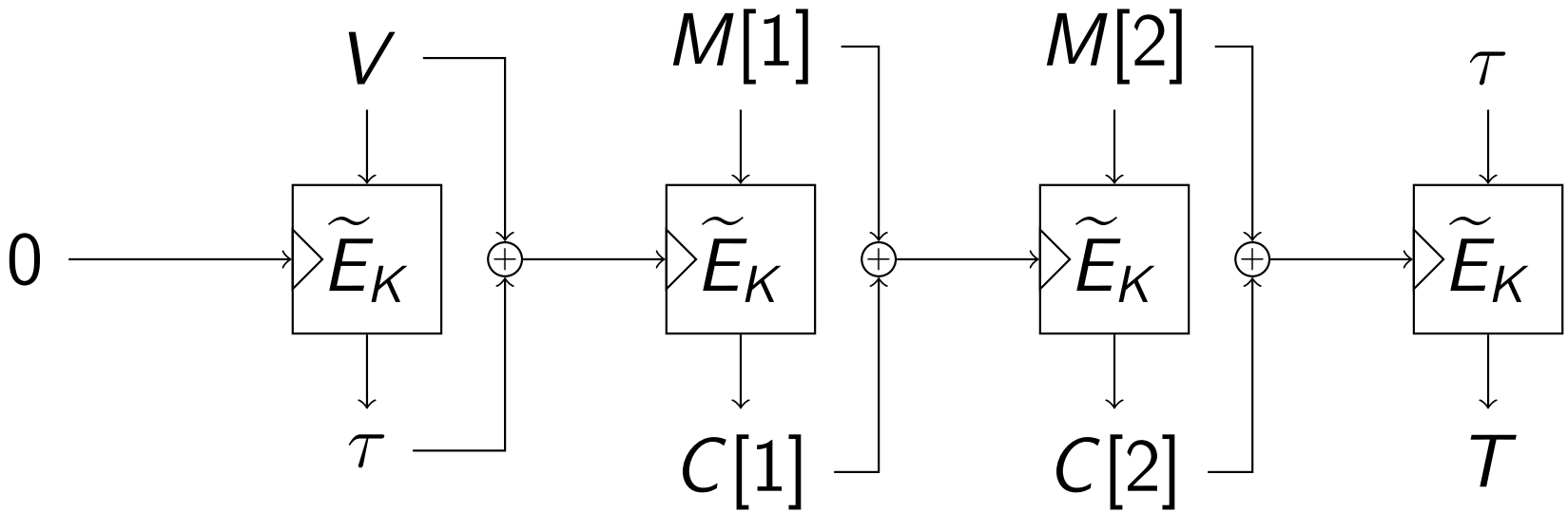
Properties

1. Proof with ideal permutation (sponge)
2. Tag cannot be truncated
3. Suited for lightweight
4. Online?

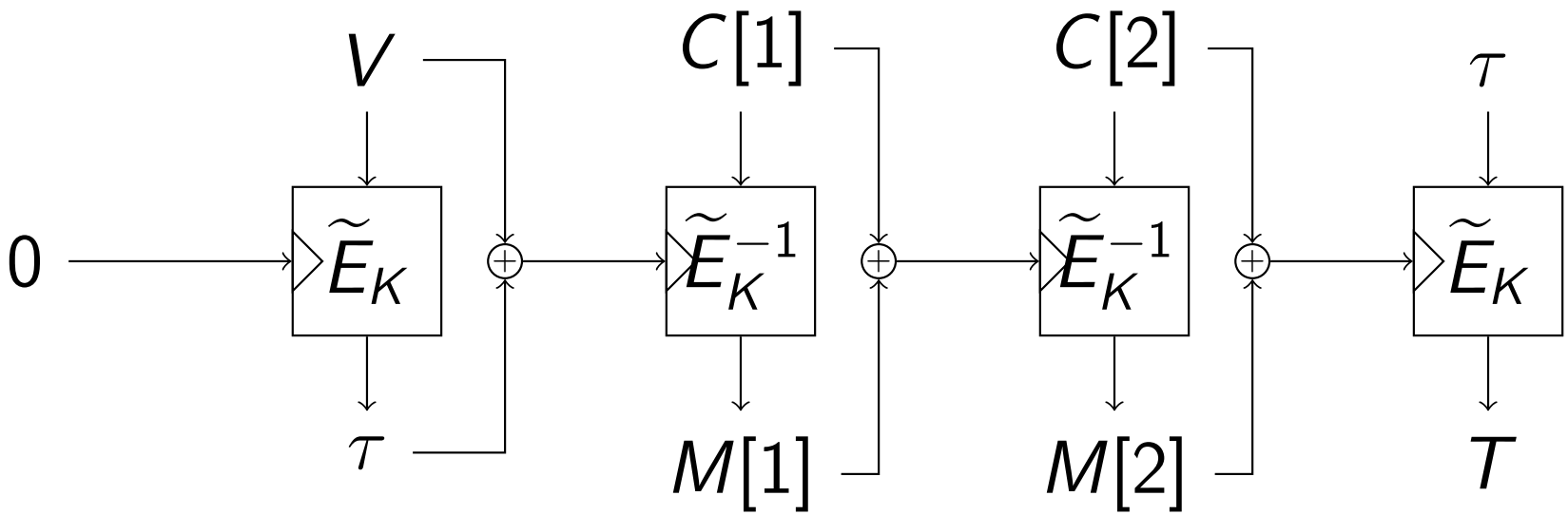
Online



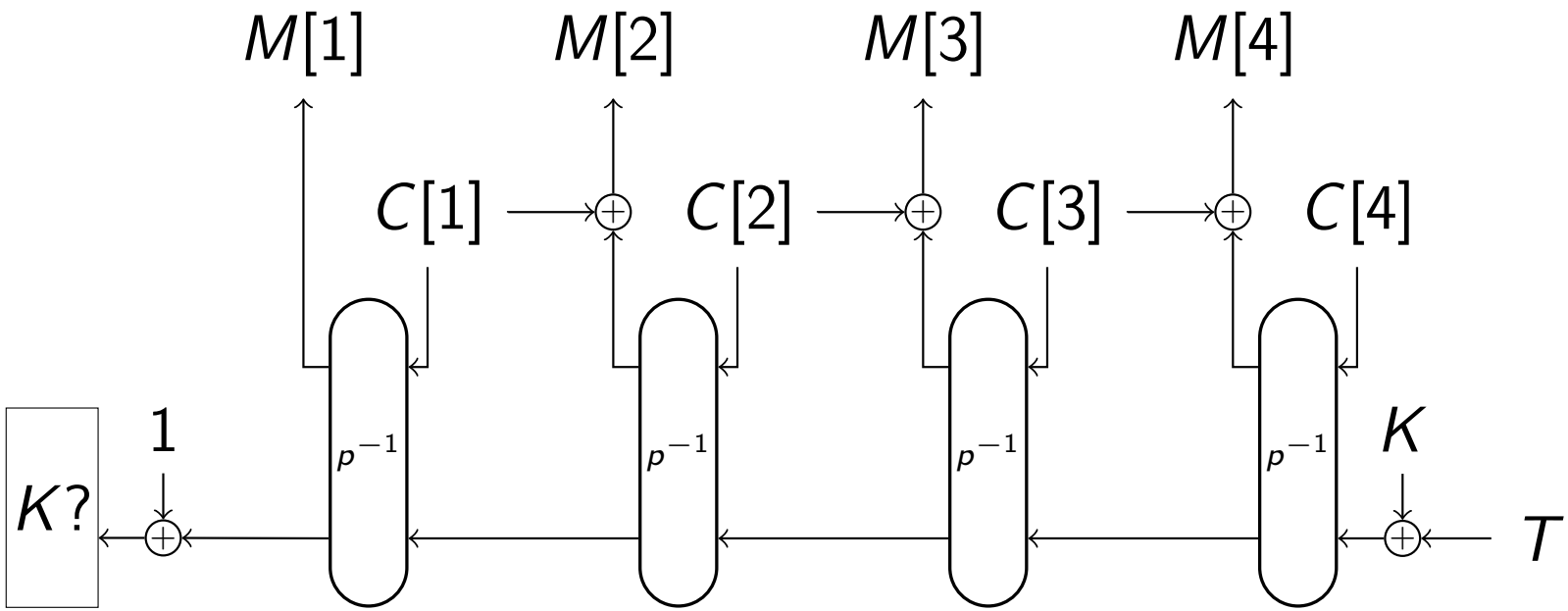
McOE


V
M[1]
M[2]
τ
0
$\widetilde{E}_K$
$\widetilde{E}_K$
$\widetilde{E}_K$
$\widetilde{E}_K$
τ
C[1]
C[2]
T

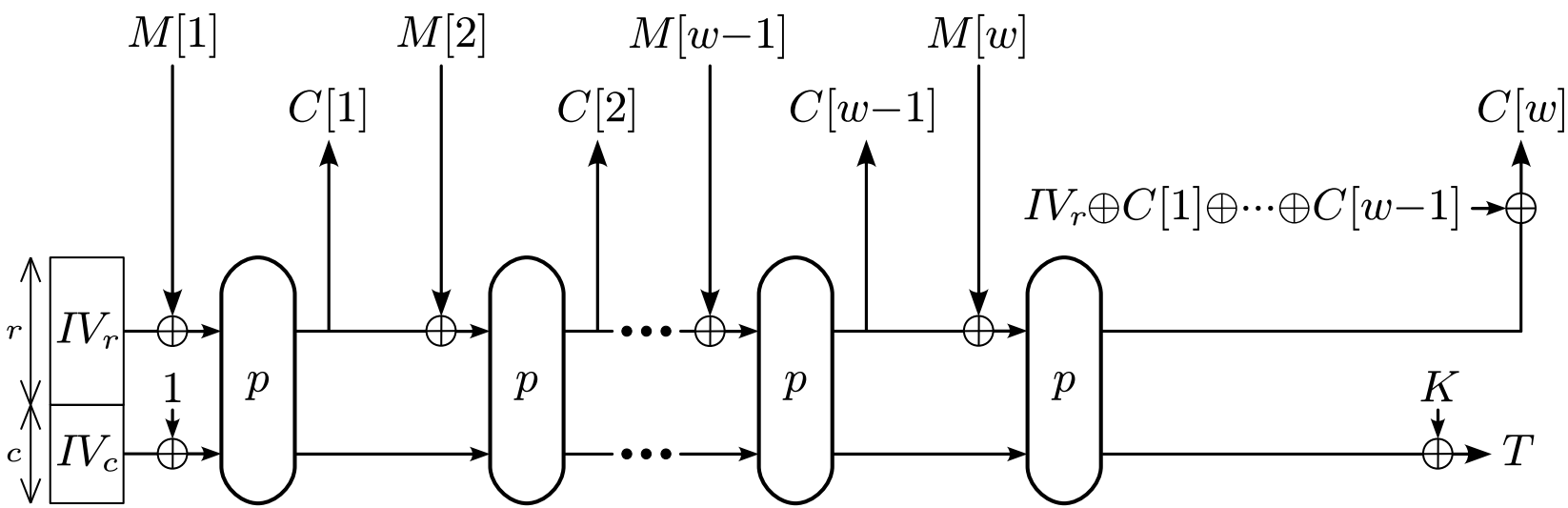
McOE - Decryption



Extra Misuse Resistance



APEX


$M[1]$
$M[2]$
$M[w-1]$
$M[w]$
$C[1]$
$C[2]$
$C[w-1]$
$C[w]$
$IV_r \oplus C[1] \oplus \cdots \oplus C[w-1]$
r
c
IV_r
IV_c
1
p
p
p
p
K
T

Conclusions and Future Work

Future work:

1. Reducing key size
2. Designing a permutation with efficient inverse
3. Ideal model versus standard model
4. How to deal with nonces: public message number versus secret message number

Thank you for your attention.