

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

Atul Luykx

COSIC, KU Leuven

August 14, 2013

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

# Stateless, Deterministic Encryption

$$E(M_1) = C_1$$

$$E(M_2) = C_2$$

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

# Nonces

$$E(N_1, M_1) = C_1$$

$$E(N_2, M_2) = C_2$$

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

# Nonce Repetition

Nonce repeated? Usually no security guarantees.

Misuse Resistance.

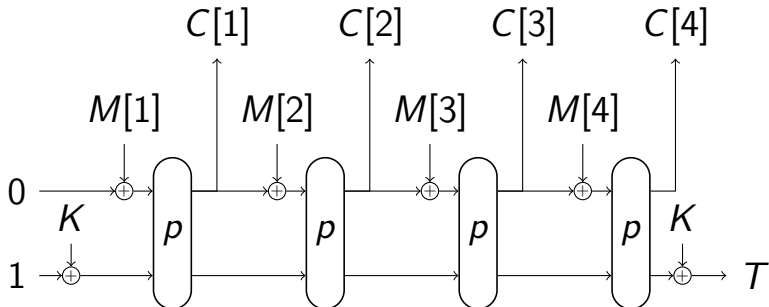
# Some AE Schemes

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

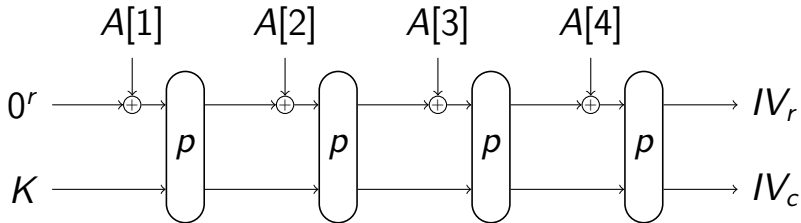
# Some AE Schemes

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

# APE

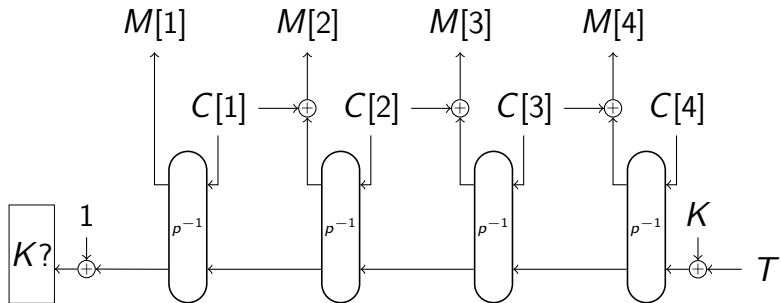


# APE - Associated Data





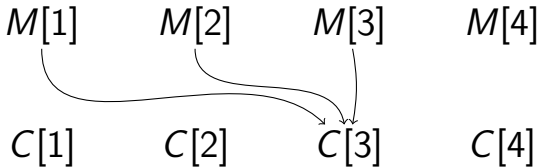
# APE - Decryption



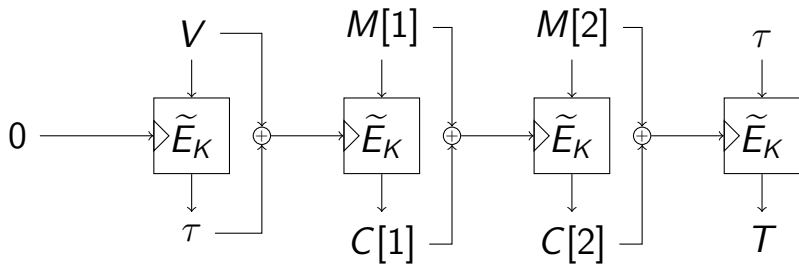
# Properties

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

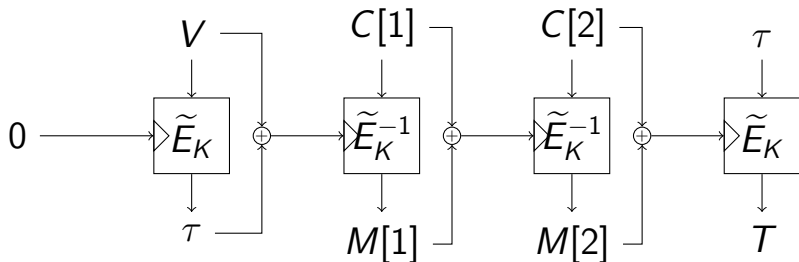
# Online



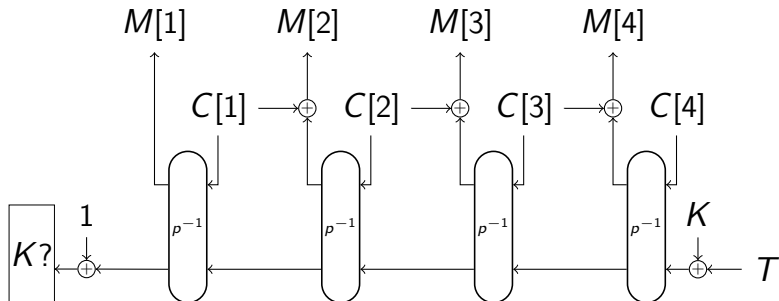
# McOE



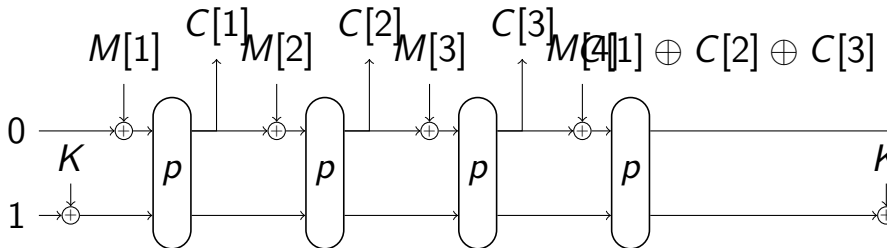
# McOE - Decryption



# Extra Misuse Resistance



# APEX



# 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.