COLM

Elena Andreeva[1], Andrey Bogdanov[2], Nilanjan Datta[3], Atul Luykx[1], Bart Mennink[1], **Mridul Nandi**[3], Elmar Tischhauser[2], Kan Yasuda[4]

[1]KU Leuven and iMinds, Belgium

[2]DTU Compute, Denmark

[3]Indian Statisftical Institute, India

[4]NTT Secure Platform Laboratories, Japan

September 27, 2016

CAESAR Overview

Table: CAESAR Round 3 Candidates. *Deoxys uses tweakable block cipher modes and creates a new tweakable block cipher.

Dedicated	Block Cipher Mode	Permutation-based
ACORN	AES-OTR	Ascon
AEGIS	CLOC and SILC	Ketje
AEZ	COLM	Keyak
MORUS	JAMBU	NORX
Tiaoxin	OCB	
	Deoxys*	

Block Cipher Mode Disadvantages

1. Usually birthday bound security

2. Efficiency cannot improve beyond block cipher
(see e.g. AEGIS vs. CTR)

Block Cipher Mode Advantages

1. Block ciphers are ubiquitous

2. Can be used with any block cipher

3. A safe bet: security reduction to underlying block cipher

Block size ≥ 128 bits $\Rightarrow$ Can process petabytes of data with success probability well below 2^{-30}

Block Cipher Modes in Candidates

Table: CAESAR Round 3 Candidates. *Deoxys uses tweakable block cipher modes and creates a new tweakable block cipher.

Dedicated	**Block Cipher Mode**	Permutation-based
ACORN	**AES-OTR**	Ascon
AEGIS	**CLOC and SILC**	Ketje
AEZ	**COLM**	Keyak
MORUS	**JAMBU**	NORX
Tiaoxin	**OCB**	
	Deoxys*	

Block Cipher Modes in Candidates

Table: CAESAR Round 3 Candidates. *Deoxys uses tweakable block cipher modes and creates a new tweakable block cipher.

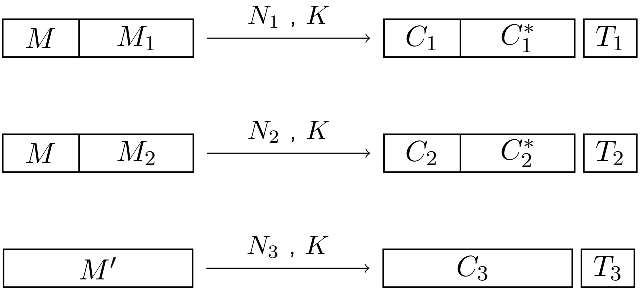
Dedicated	**Block Cipher Mode**	Permutation-based
ACORN	**AES-OTR**	Ascon
AEGIS	**CLOC and SILC**	Ketje
AEZ	**COLM**	Keyak
MORUS	**JAMBU**	NORX
Tiaoxin	**OCB**	
	Deoxys*	
	(ΘCB and SCT)	

Robustness

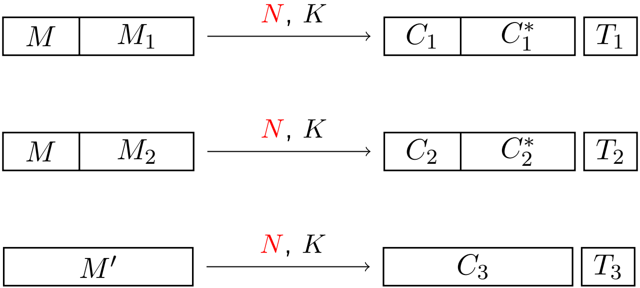
Table: Levels of resistance to nonce misuse.

Level 1	**Level 2**	**Level 3**
AES-OTR	COLM	Deoxys-II (SCT)
CLOC and SILC		
JAMBU		
OCB		
Deoxys-I		

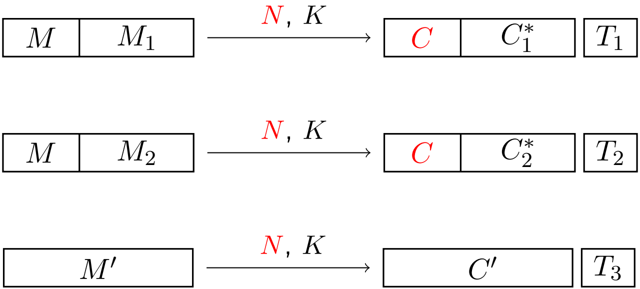
Background: Online Nonce Misuse Resistance



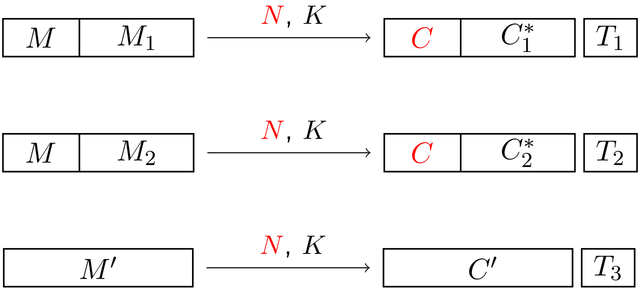
Background: Online Nonce Misuse Resistance



Background: Online Nonce Misuse Resistance

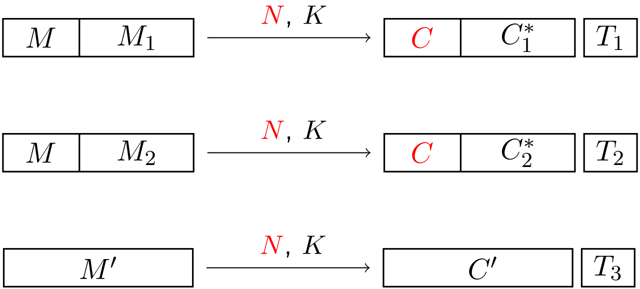


Background: Online Nonce Misuse Resistance



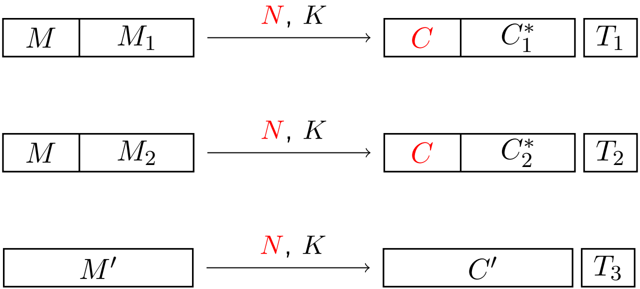
1. Equality of prefixes of messages determined

Background: Online Nonce Misuse Resistance



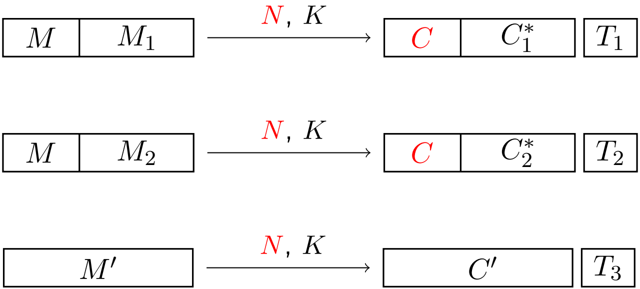
1. Equality of prefixes of messages determined
2. No relationship past common prefix

Background: Online Nonce Misuse Resistance



1. Equality of prefixes of messages determined
2. No relationship past common prefix
3. Hoang et al. CRYPTO 2015 attack. . .

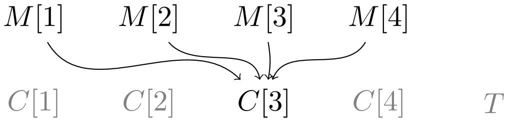
Background: Online Nonce Misuse Resistance



1. Equality of prefixes of messages determined
2. No relationship past common prefix
3. Hoang et al. CRYPTO 2015 attack. . .
4. but still much more robust than GCM, OCB, OTR, . . .

Advantage over SCT: *Online* Scheme

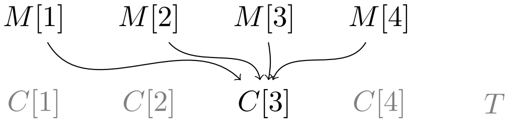
1. High latency (receive full message before first output)
2. Storage issues (large internal state)



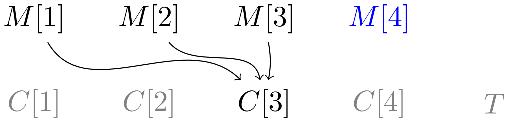
Dependency in SCT.

Advantage over SCT: *Online* Scheme

1. High latency (receive full message before first output)
2. Storage issues (large internal state)



Dependency in SCT.

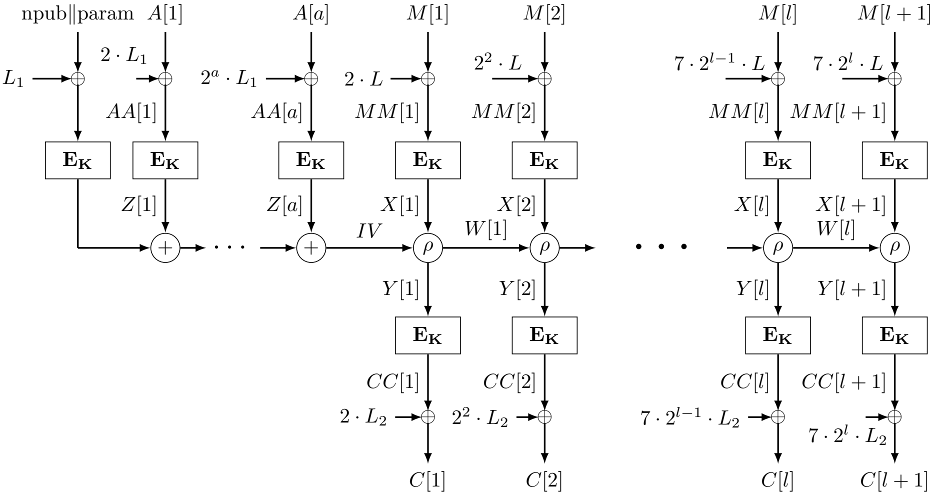


Dependency in COLM.

COLM Comparison with ELmD and COPA

	COPA	ELmD	COLM
Simplified masking			✓
Fully parallelizable authentication		✓	✓
XOR mixing for authentication	✓		✓
ρ mixing for encryption		✓	✓
Bottom layer encryption	✓		✓
Intermediate tags		✓	✓

COLM Description



Summary

COLM: strengths of COPA + ELmD

1. security reduction to block cipher
2. online misuse resistance: most robust AES-mode in the competition
3. highly parallelizable

Thank you for your attention.

1. Andreeva et al. “How to securely release unverified plaintext in authenticated encryption” ASIACRYPT 2014
2. Hoang et al. “Online authenticated-encryption and its nonce-reuse misuse-resistance” CRYPTO 2015
3. Dobraunig et al. “Related-Key Forgeries for Proest-OTR” FSE 2015
4. Nandi “XLS is Not a Strong Pseudorandom Permutation” ASIACRYPT 2014
5. Nandi “Revisiting Security Claims of XLS and COPA” eprint
6. Lu “On the Security of the COPA and Marble Authenticated Encryption Algorithms against (Almost) Universal Forgery Attack” eprint
7. Fuhr et al. “Collision Attacks against CAESAR Candidates” ASIACRYPT 2015
8. Bogdanov et al “Comb to Pipeline: Fast Software Encryption Revisited” FSE 2015
9. Dobraunig et al “Statistical Fault Attacks on Nonce-Based Authenticated Encryption Schemes” ASIACRYPT 2016
10. Nandi “On the Optimality of Non-Linear Computations of Length-Preserving Encryption Schemes” ASIACRYPT 2015
11. Kaplan et al. “Breaking Symmetric Cryptosystems using Quantum Period Finding” CRYPTO 2016
12. Bay et al. “Universal Forgery and Key Recovery Attacks on ELmD Authenticated Encryption Algorithm” ASIACRYPT 2016