Secure Channels
Summer Term 2016

Problem Set 7

Prof. Stefan Lucks, Eik List

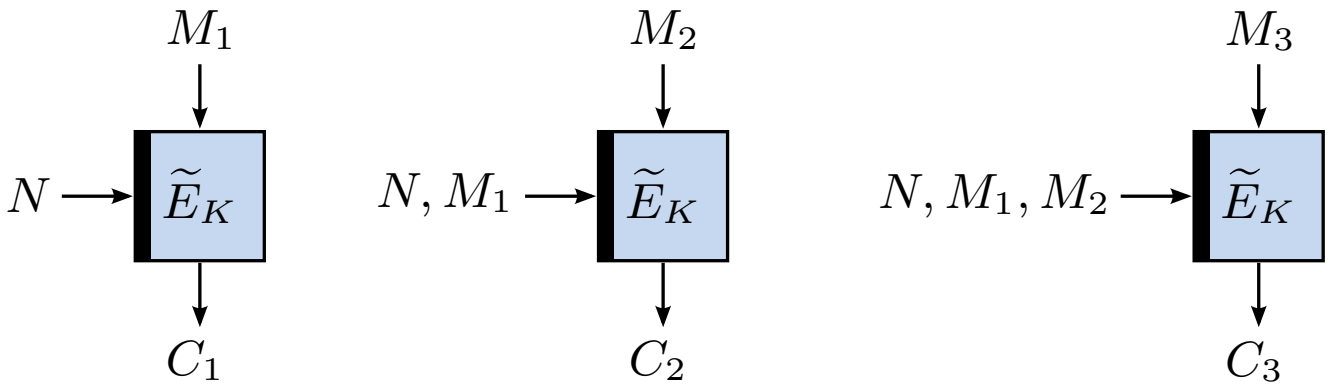
Bauhaus-Universität Weimar

June 28, 2018

Agenda

- On-line Encryption
- On-line Authenticated Encryption
- Stateful AE

On-line Encryption



- Prefix behavior:

M_1	M_2	M_3	M_4	M_5
$=$	$=$	$\neq$	\$	\$

On-line Encryption Schemes

Definition 1 (OCPA and OCCA Security)

Let $\Pi = (\mathcal{E}, \mathcal{D})$ be an on-line cipher with associated key space $\mathcal{K}$ and block space $\mathcal{B}$. Let $K \twoheadleftarrow \mathcal{K}$, and let $\mathbf{A}$ be an adversary on Π that has access to an oracle, and let further $\mathbf{A}'$ be an adversary on Π that has access to two oracles. Let $\pi \twoheadleftarrow \mathrm{OPERM}(\mathcal{B})$. Then, the OCPA advantage of $\mathbf{A}$ and the OCCA advantage of $\mathbf{A}'$ w.r.t. Π are defined as

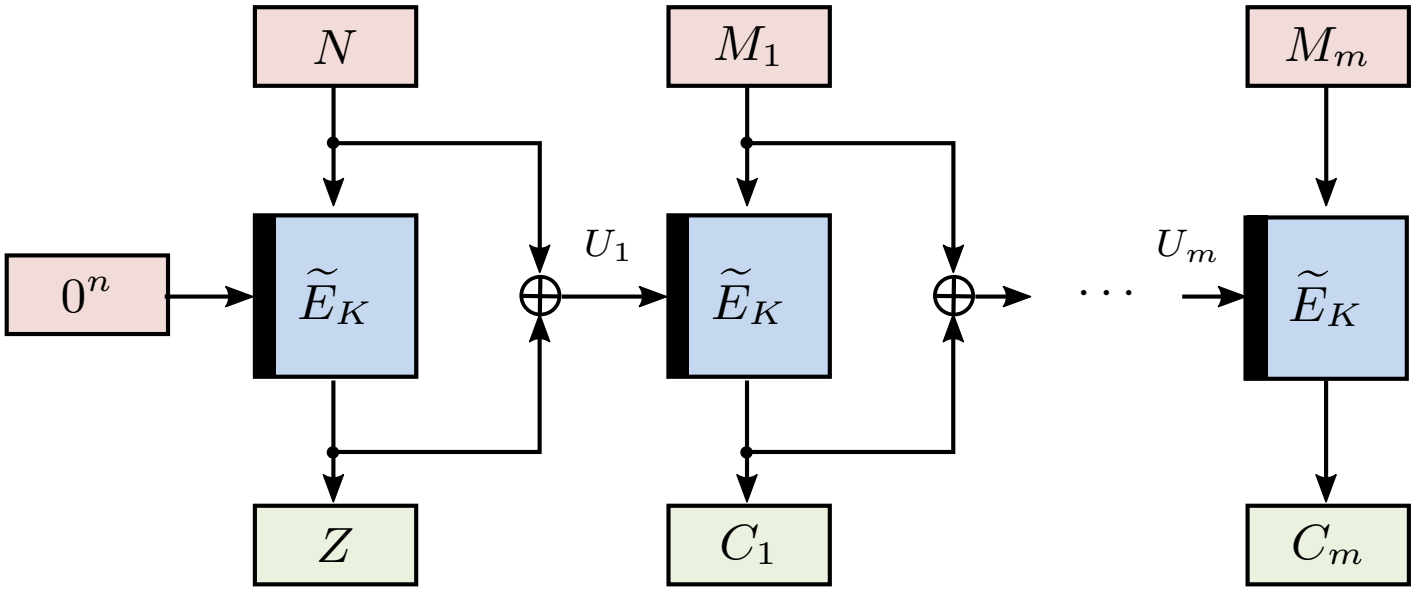
$$\mathbf{Adv}_{\Pi}^{OCPA}(\mathbf{A}) \stackrel{\text{def}}{=} \underset{\mathbf{A}}{\triangle}\left(\mathcal{E}_K; \pi\right)(\mathbf{A}), \text{ and}$$

$$\mathbf{Adv}_{\Pi}^{OCCA}(\mathbf{A}) \stackrel{\text{def}}{=} \underset{\mathbf{A}}{\triangle}\left(\mathcal{E}_K, \mathcal{D}_K; \pi, \pi^{-1}\right)(\mathbf{A}'),$$

respectively.

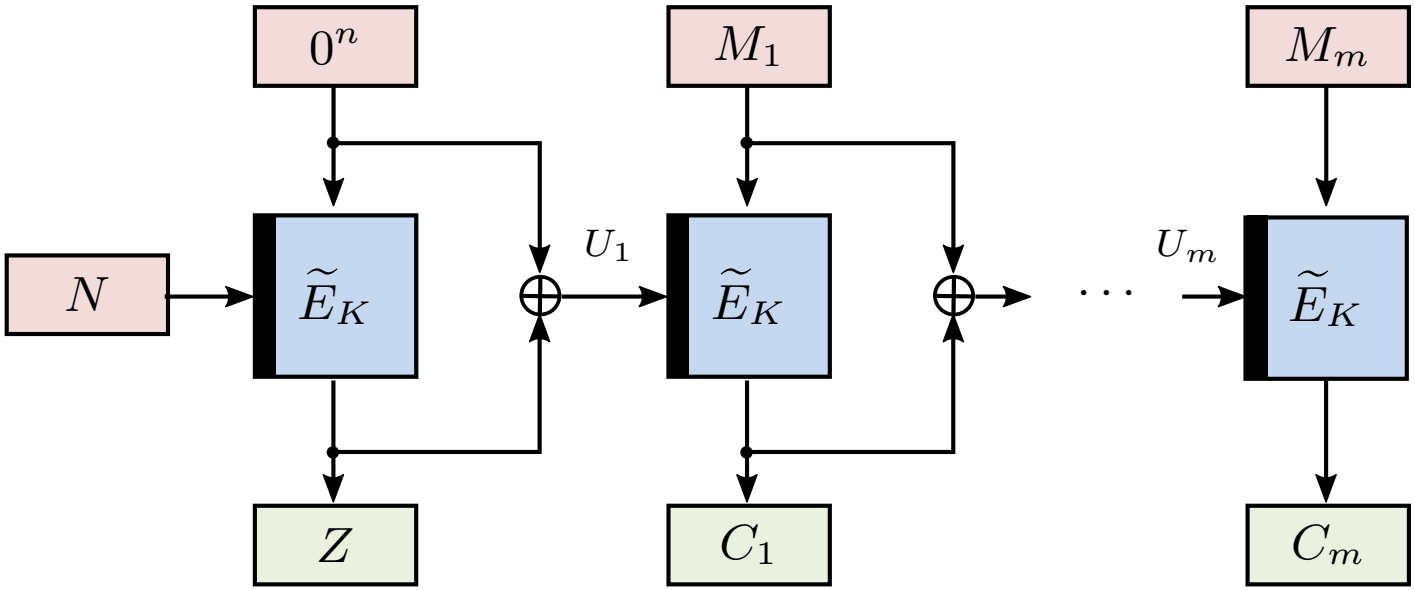
McOE

a)


N
M_1
M_m
0^n
$\widetilde{E}_K$
U_1
$\widetilde{E}_K$
$\cdots$
U_m
$\widetilde{E}_K$
Z
C_1
C_m

McOE

b)


0^n
M_1
M_m
N
$\widetilde{E}_K$
U_1
$\widetilde{E}_K$
$\cdots$
U_m
$\widetilde{E}_K$
Z
C_1
C_m

OAE2

Segmented AE [HRRV'15]

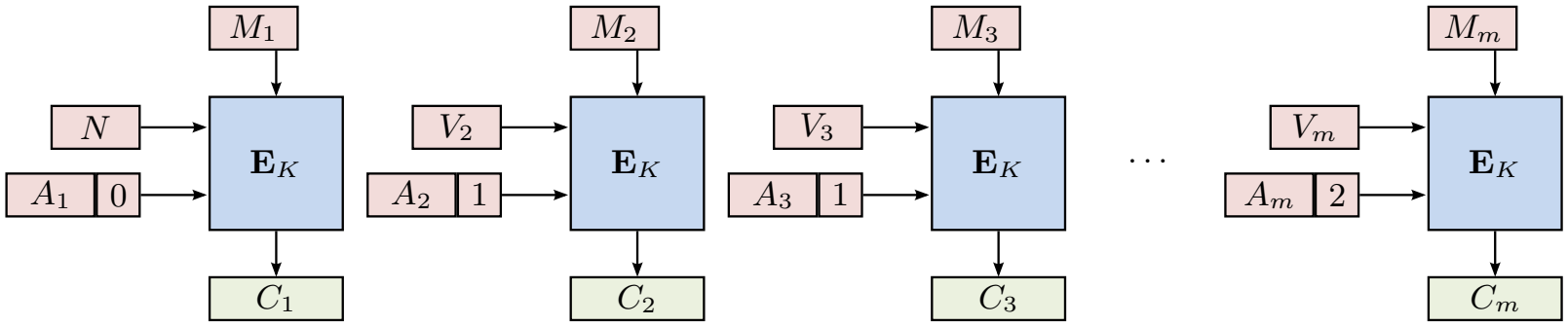
- Encryption and decryption are 3-tuples each:

$$\begin{array}{lll} \mathcal{E}.\text{INIT}: & \mathcal{K} \times \mathcal{N} \to \mathcal{S} & \mathcal{D}.\text{INIT}: \quad \mathcal{K} \times \mathcal{N} \to \mathcal{S} \\ \mathcal{E}.\text{NEXT}: & \mathcal{S} \times \mathcal{A} \times \mathcal{M} \to \mathcal{C} \times \mathcal{S} & \mathcal{D}.\text{NEXT}: \quad \mathcal{S} \times \mathcal{A} \times \mathcal{C} \to (\mathcal{M} \times \mathcal{S}) \times \{\perp\} \\ \mathcal{E}.\text{LAST}: & \mathcal{S} \times \mathcal{A} \times \mathcal{M} \to \mathcal{C} & \mathcal{D}.\text{LAST}: \quad \mathcal{S} \times \mathcal{A} \times \mathcal{M} \to \mathcal{M} \times \{\perp\}. \end{array}$$

- Use message (and AD) vectors: $\mathbf{M} = (M_1, \ldots, M_m)$

The CHAIN Construction

[HRRV15]



Stateful AE

	Protection against			
Level	Forgeries	Replay	Reordering	Dropping
Level 1				
Level 2				
Level 3				
Level 4				

Stateful AE

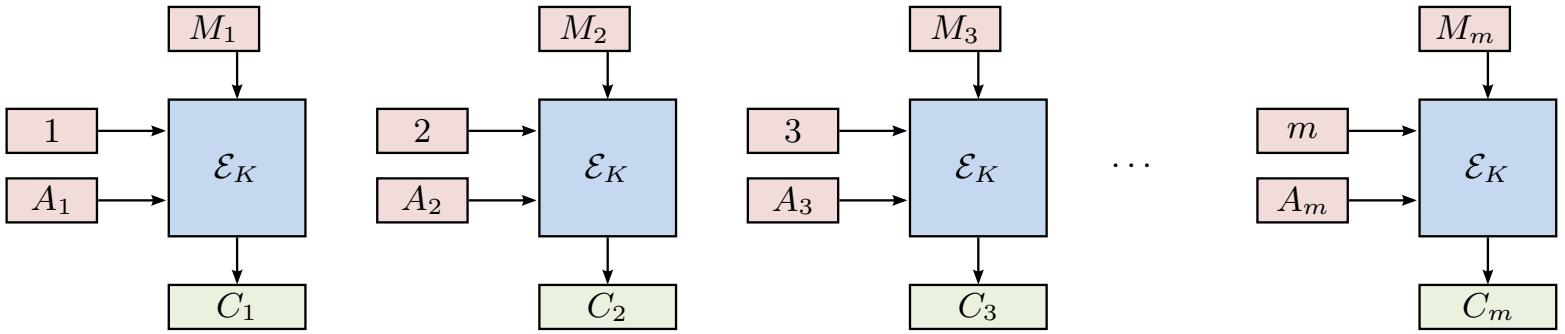
Levels			Protection against					
[KPB03]	[BHMS16]	[RZ18]	Forgeries	Replay	Reordering	Dropping	SM	Satisfied by (examples)
1	1	L_0	✓	–	–	–	–	DTLS, QUIC
2	2	L_1^∞	✓	✓	–	–	–	DTLS, IPsec AH
		L_1^ℓ	✓	✓	$\leq \ell$	–	–	
3	3	L_2^∞	✓	✓	✓	–	–	802.11
		L_2^ℓ	✓	✓	✓	$\leq \ell$	–	
4			✓	✓	✓	✓	–	TLS
5	4	L_3	✓	✓	✓	✓	✓	TLS

1

[1] SM = subsequent messages after an invalid ciphertext are rejected.

The STREAM′ Construction

[HRRV15]



Questions?