Secure Channels
Summer Term 2018

Problem Set 5

Prof. Stefan Lucks, Eik List

Bauhaus-Universität Weimar

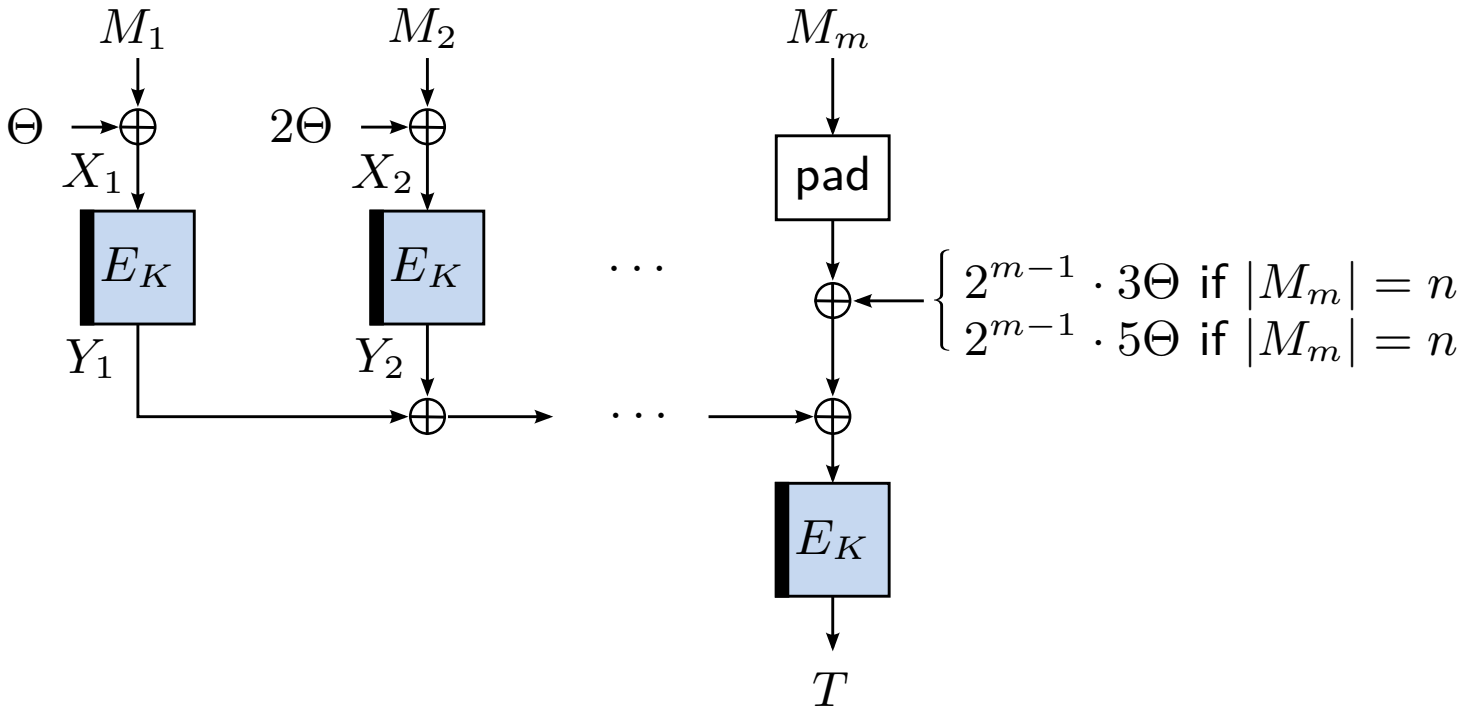
June 14, 2018

Agenda

In this problem set, you should learn/deepen your understanding in...

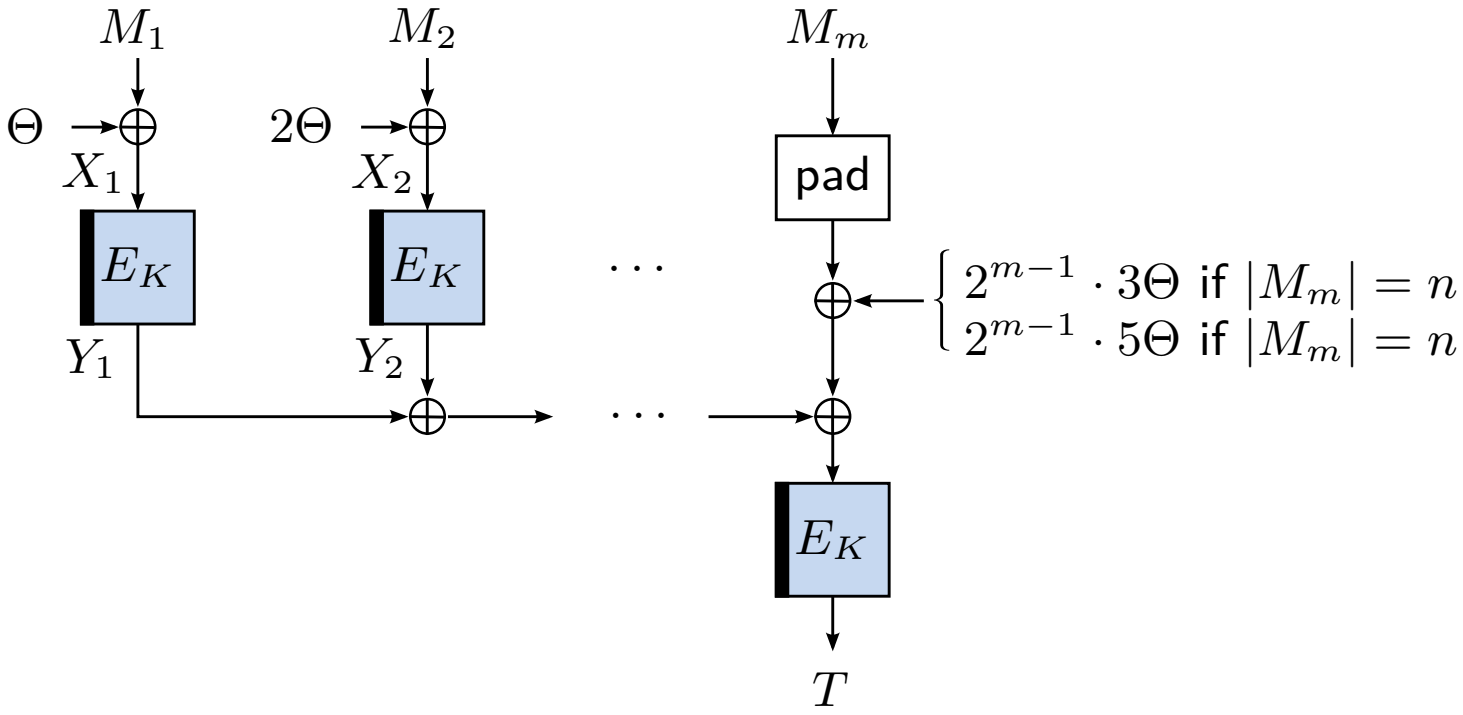
- ...authenticated encryption
- ...consequences of nonce use and misuse.

PMAC1



- Given M_1, M_2 and M_1', M_2' with $T = T'$

PMAC1



- Given M_1, M_2 and M_1', M_2' with $T = T'$
- With non-negl. probability: $X_1 = X_2'$ and $X_2 = X_1'$

$$M_1 \oplus \Theta = M_2' \oplus 2\Theta$$

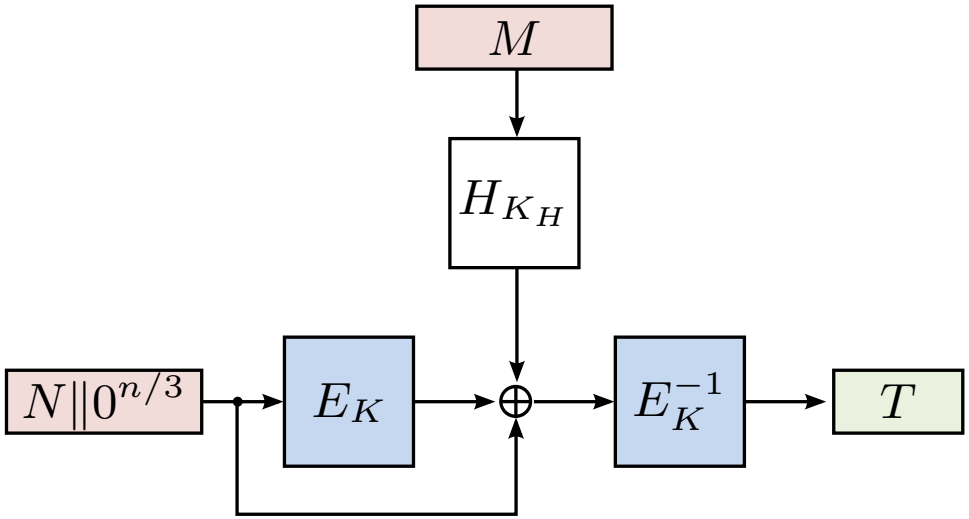
$$\Theta = (M_1 \oplus M_2') \cdot 3^{-1}$$

CWC

1: **function** $\mathrm{CWC}[E_K](N', A, M)$
2: $N \leftarrow 10^7 \parallel N \parallel 0^{32}$
3: $S \leftarrow \mathrm{CTR}[E_K](N)$
4: $C \leftarrow S[0..|M|] \oplus M$
5: $K_H \leftarrow E_K(110^{n-2})$
6: $R \leftarrow \textsc{PolyHash}_{K_H}(A, C)$
7: $T \leftarrow E_K(R \oplus E_K(N))$
8: $T \leftarrow T[0..8\tau]$
9: **return** (C, T)

1: **function** $\textsc{PolyHash}_{K_H}(A, C)$
2: $(A_1, \ldots, A_r) \xleftarrow{96} A$
3: **if** $|A_r| < 96$ **then**
4: $A_r \leftarrow A_r \parallel 0^{96-|A_r|}$
5: $Y \leftarrow A_1 \parallel \ldots \parallel A_r$
6: **if** $|C_m| < 96$ **then**
7: $C_m \leftarrow C_m \parallel 0^{96-|C_m|}$
8: $Y \leftarrow Y \parallel C_1 \parallel \ldots \parallel C_m$
9: $(Y_1, \ldots, Y_\beta) \xleftarrow{96} Y$
10: $Y_{\beta+1} \leftarrow 2^{64} \cdot |A| + |C|$
11: **return** $Y_{\beta+1} \oplus \bigoplus_{i=1}^{\beta} K_H^{\beta+1-i} \cdot Y_i \bmod 2^{127} - 1$

nPolyMAC

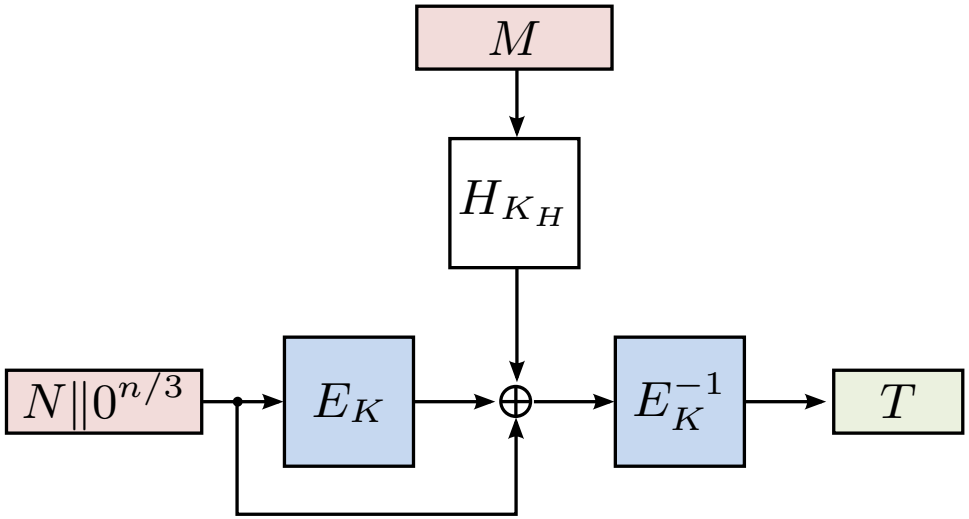


function $\textsc{nPolyMAC}[E_K](N', M)$
- $K_H = E_K(0^{n-1}1)$
- $N \leftarrow N' \,\|\, 0^{n/3}$
- $X \leftarrow E_K(N)$
- $Y \leftarrow \textsc{PolyHash}_{K_H}(M)$
- $Z \leftarrow X \oplus Y \oplus N$
- **return** $E_K^{-1}(X \oplus Y \oplus Z)$

function $\textsc{PolyHash}_{K_H}(M)$
- $(M_1, \ldots, M_m) \xleftarrow{n} M$
- **if** $|M_m| < n$ **then**
  - $M_m \leftarrow M_m \,\|\, 0^{n-|M_m|}$
- **return** $\bigoplus_{i=1}^{m} K_H^{m+1-i} \cdot M_i$

- PolyHash misses padding

nPolyMAC

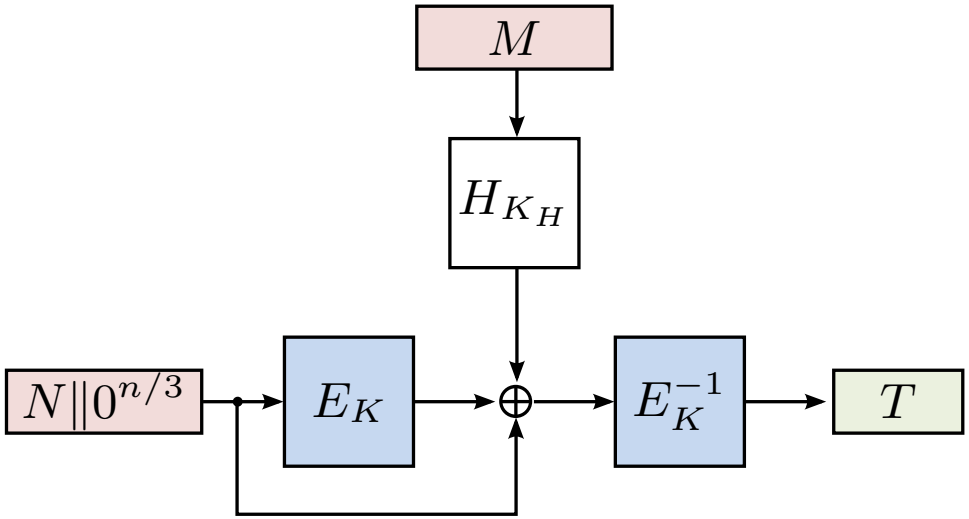


function $\textsc{nPolyMAC}[E_K](N', M)$
- $K_H = E_K(0^{n-1}1)$
- $N \leftarrow N' \,\|\, 0^{n/3}$
- $X \leftarrow E_K(N)$
- $Y \leftarrow \textsc{PolyHash}_{K_H}(M)$
- $Z \leftarrow X \oplus Y \oplus N$
- **return** $E_K^{-1}(X \oplus Y \oplus Z)$

function $\textsc{PolyHash}_{K_H}(M)$
- $(M_1, \ldots, M_m) \xleftarrow{n} M$
- **if** $|M_m| < n$ **then**
  - $M_m \leftarrow M_m \,\|\, 0^{n-|M_m|}$
- **return** $\bigoplus_{i=1}^{m} K_H^{m+1-i} \cdot M_i$

- PolyHash misses padding
- Use $N = 0^n$ and $M = 0^*$

nPolyMAC



1: **function** $\text{nPolyMAC}[E_K](N', M)$
2: $K_H = E_K(0^{n-1}1)$
3: $N \leftarrow N' \,\|\, 0^{n/3}$
4: $X \leftarrow E_K(N)$
5: $Y \leftarrow \text{PolyHash}_{K_H}(M)$
6: $Z \leftarrow X \oplus Y \oplus N$
7: **return** $E_K^{-1}(X \oplus Y \oplus Z)$

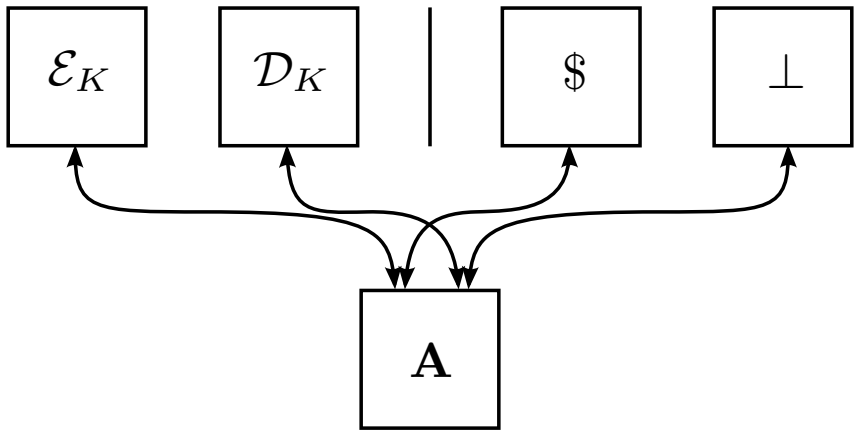
1: **function** $\text{PolyHash}_{K_H}(M)$
2: $(M_1, \ldots, M_m) \xleftarrow{n} M$
3: **if** $|M_m| < n$ **then**
4: $M_m \leftarrow M_m \,\|\, 0^{n-|M_m|}$
5: **return** $\bigoplus_{i=1}^{m} K_H^{m+1-i} \cdot M_i$

- PolyHash misses padding
- Use $N = 0^n$ and $M = 0^*$
- Obtain $E_K^{-1}(E_K(N) \oplus 0^n \oplus 0^n)) = N = 0^n$

Section 1

AE Security

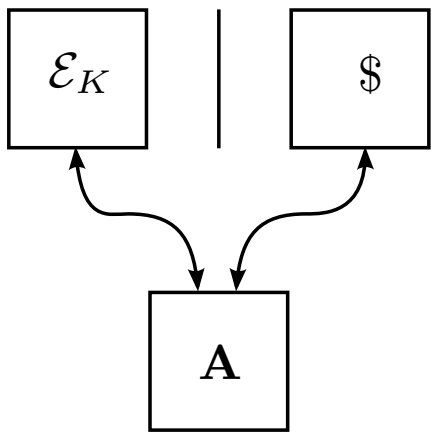
AE Security



- Privacy: Ciphertext/Tags are indistinguishable (often: in the left-or-right sense, Rogaway/Weimar: from random bits)
- Integrity: Tags are not efficiently forgeable
- All-in-one notion for CCA Security

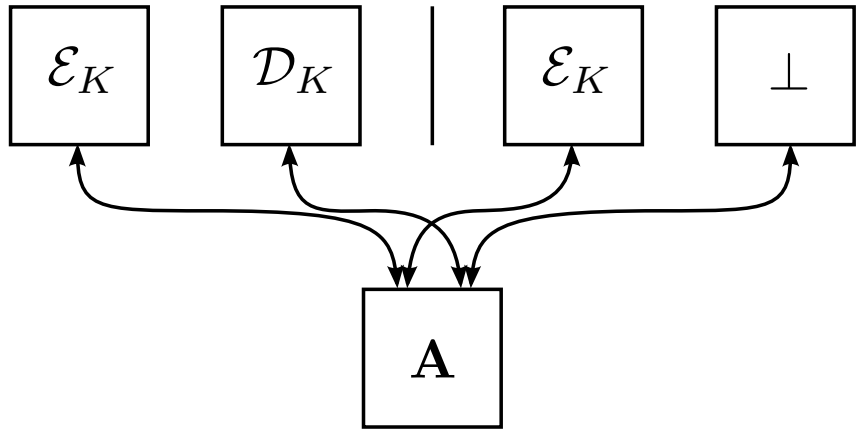
$$\underset{\mathbf{A}}{\Delta}\left(\mathcal{E}_K, \mathcal{D}_K; \$, \perp\right) = \left|\Pr\left[\mathbf{A}^{\mathcal{E}_K, \mathcal{D}_K} \Rightarrow 1\right] - \Pr\left[\mathbf{A}^{\$, \perp} \Rightarrow 1\right]\right|$$

AE Security



RoR-CPA

+



INT-CTXT

- RoR-CPA: Distinguish ciphertexts from random
- INT-CTXT: Forge a tag

$$\Pr\left[\mathbf{A}^{\mathcal{E}_K,\mathcal{D}_K} \text{ forges}\right] \approx \underset{\mathbf{A}}{\Delta}\left(\mathcal{E}_K, \mathcal{D}_K; \mathcal{D}_K, \perp\right)$$

Adversaries

- $\mathbf{A}$ = PPT Turing machine with access to oracles $O_1, \ldots, O_k$
- Here: $\mathbf{A}$ is statistical distinguisher between two distributions: real and ideal
- Here: w.l.o.g., $\mathbf{A}$ is deterministic
- #Queries: q_i to oracle O_i (often $q = \sum_i q_i$)
- #Blocks/query: m
- Total #blocks: σ_i to oracle O_i (often $\sigma = \sum_i \sigma_i$)

- Information-theoretic: $(q_1, \ldots, q_k, \sigma_1, \ldots, \sigma_k)$-adversary
- Complexity-theoretic (add time): $(q_1, \ldots, q_k, \sigma_1, \ldots, \sigma_k, t)$-adversary

AE Security

Reductionist Proofs

- Goal: If there $\exists$ an efficient $\mathrm{RoR\text{-}CCA}$-adversary on $\mathbf{A}$ that breaks AE-security of Π:
  - $\exists$ an $\mathrm{INT\text{-}CTXT}$-adversary $\mathbf{A}'$ that breaks the $\mathrm{INT\text{-}CTXT}$ security of Π OR
  - $\exists$ $\mathrm{RoR\text{-}CPA}$-adversary $\mathbf{A}''$ that breaks the $\mathrm{RoR\text{-}CPA}$ security of Π
- Assume: $\mathbf{A}$, $\mathbf{A}'$, and $\mathbf{A}''$ use equal/similar resources

Games and Worlds

- Starting game: G_0
- Destination game: G_k
- Create intermediate games $G_1, \ldots, G_{k-1}$

$$G_0 \rightarrow G_1 \rightarrow G_2 \rightarrow \ldots \rightarrow G_k$$

- We transform a distinguisher $\mathbf{A}_0$ that shall distinguish two worlds in G_0 into $\mathbf{A}_1$ that shall distinguish two worlds in G_1:

$$\mathbf{A}_0 \rightarrow \mathbf{A}_1 \rightarrow \ldots \rightarrow \mathbf{A}_k$$

- Assumption: All $\mathbf{A}_i$ use equal resources
- Triangle (In)Equality:

$$\underset{\mathbf{A}}{\Delta}\left(G_0; G_k\right)\left(\mathbf{A}\right) \leq \underset{\mathbf{A}}{\Delta}\left(G_0; G_1\right)\left(\mathbf{A}_0\right) + \underset{\mathbf{A}}{\Delta}\left(G_1; G_2\right)\left(\mathbf{A}_1\right) + \ldots + \underset{\mathbf{A}}{\Delta}\left(G_{k-1}; G_k\right)\left(\mathbf{A}_k\right)$$

Applying the Triangle Inequality

- Let's derive an intermediate world

$$\underset{\mathbf{A}}{\Delta}(\mathcal{E}_K, \mathcal{D}_K; \$, \perp) \leq \underset{\mathbf{A}}{\Delta}(\mathcal{E}_K, \mathcal{D}_K; \mathcal{E}_K, \perp) + \underset{\mathbf{A}}{\Delta}(\mathcal{E}_K, \perp; \$, \perp)$$

$$\overset{(*)}{=} \underbrace{\underset{\mathbf{A}}{\Delta}(\mathcal{E}_K, \mathcal{D}_K; \mathcal{E}_K, \perp)}_{\text{INT-CTXT}} + \underbrace{\underset{\mathbf{A}}{\Delta}(\mathcal{E}_K; \$)}_{\text{RoR-CPA}}$$

(*): since $\perp$ is indistinguishable from $\perp$ and gives no additional information

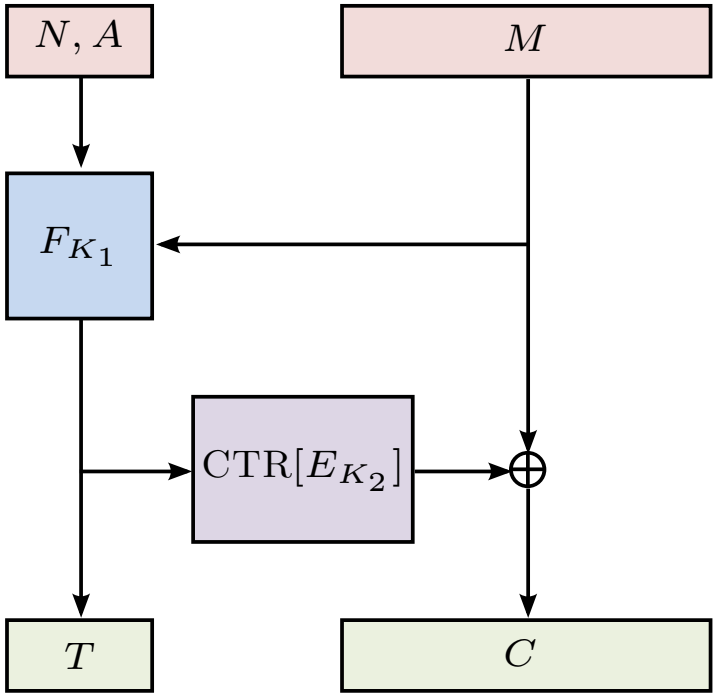
- Obtain

$$\mathbf{Adv}_{\Pi}^{\text{RoR-CCA}}(\mathbf{A}) \leq \mathbf{Adv}_{\Pi}^{\text{RoR-CPA}}(\mathbf{A}') + \mathbf{Adv}_{\Pi}^{\text{INT-CTXT}}(\mathbf{A}'').$$

INT-RUP Security of SIV

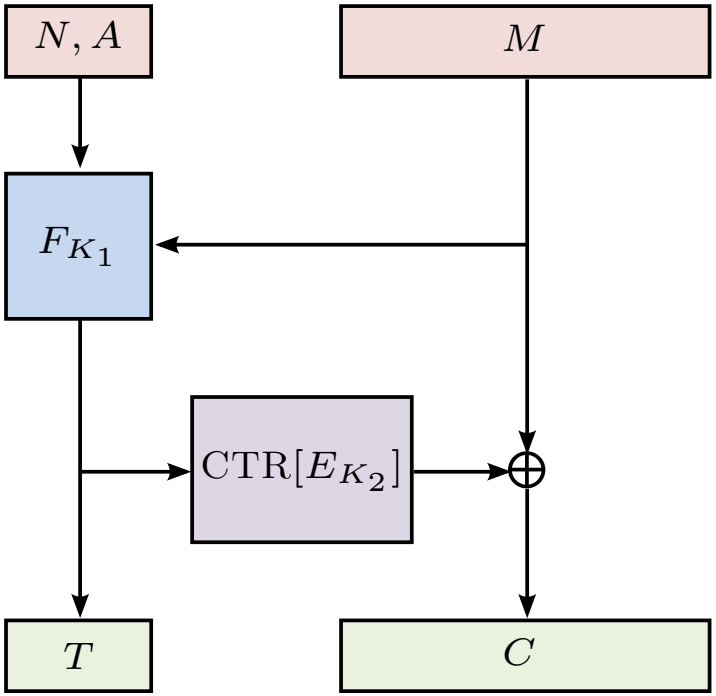
1: **function** $\mathcal{E}_{K_1,K_2}(N, A, M)$
2: $\quad T \leftarrow F_{K_1}(N, A, M)$
3: $\quad C \leftarrow \mathrm{CTR}[E_{K_2}](T, M)$
4: $\quad$ **return** (C, T)

1: **function** $\mathcal{D}_{K_1,K_2}(N, A, C, T)$
2: $\quad M \leftarrow \mathrm{CTR}[E_{K_2}](T, C)$
3: $\quad b \leftarrow F_{K_1}(N, A, M) \stackrel{?}{=} T.$
4: $\quad$ **return** (M, b)



- Leaks plaintexts of invalid ciphertexts
- Goal: forge

INT-RUP Security of SIV



- Replace F by ideal random function $\$_1$
- Replace CTR by independent ideal random function $\$_2$
- Difference:

$$\mathbf{Adv}^{\text{INT-RUP}}_{\text{SIV}[F,\text{CTR}]}(\mathbf{A}) \leq \mathbf{Adv}^{\text{INT-RUP}}_{\text{SIV}[F,\text{CTR}]}(\mathbf{A}) + \mathbf{Adv}^{\text{PRF}}_{F}(\mathbf{A}') + \mathbf{Adv}^{\text{PRF}}_{\text{CTR}}(\mathbf{A}'')$$

- F is fully secure, CTR secure until birthday bound: ✓

INT-RUP Security of SIV

- Assume $\mathbf{A}'''$ was successful:
  Forged valid (N, A, C, T) that decrypts to M and $b = 1$
- 2 cases:
  - (N, A, M) is old (was queried to $\mathcal{E}$ before)
  - (N, A, M) is fresh (not queried to $\mathcal{E}$ before)

INT-RUP Security of SIV

Case 1: (N, A, M) is old

- (C', T'): previous result of $\mathcal{E}$
- If $(C, T) = (C', T')$: violates game, no forgery
- If $T \neq T'$: impossible ($F/\$_1$ are deterministic)
- If $C \neq C'$ and $T = T'$:
  - $\$_2$ produces equal output for fixed $T = T'$

$$C \neq C' \Leftrightarrow C \oplus \$_2(T) \neq C' \oplus \$_2(T)$$
$$\Leftrightarrow M \neq M'$$

- $\Pr[\mathbf{A} \text{ forges}] = 0$ in this case

INT-RUP Security of SIV

Case 2: (N, A, M) is fresh

- $\$_1$ is random function, queried with fresh (N, A, M)

$$\Pr[\$_1(N, A, M) = T] = \frac{q}{2^\tau}$$

- Over all terms:

$$\mathbf{Adv}^{\text{INT-RUP}}_{\text{SIV}[F,\text{CTR}]}(\mathbf{A}) \leq \frac{q}{2^n} + \mathbf{Adv}^{\text{PRF}}_{F}(\mathbf{A}') + \mathbf{Adv}^{\text{PRF}}_{\text{CTR}}(\mathbf{A}'')$$

Summary

- $\mathrm{PMAC1}$ breaks at birthday bound
- Universal hashing needs proper padding
- Repetition of reductionist proofs
- AE $= \mathrm{RoR\text{-}CPA} + \mathrm{INT\text{-}CTXT}$
- SIV is $\mathrm{INT\text{-}RUP}$-secure

Questions?