Universal Forgery and Key Recovery Attacks on ELmD Authenticated Encryption Algorithm

Aslı Bay[1], Oğuzhan Ersoy[2], Ferhat Karakoç[1]

[1] TÜBİTAK-BİLGEM-UEKAE [2] Boğaziçi University

ASIACRYPT 2016, Hanoi, VIETNAM

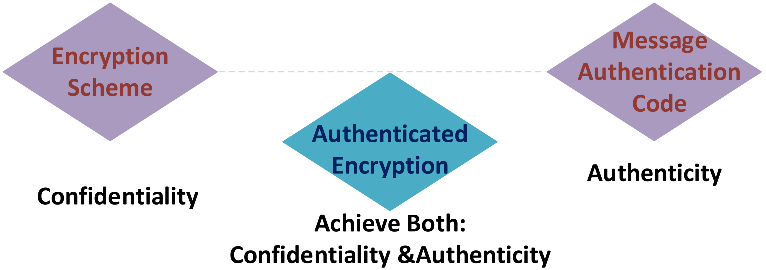
Outline

Encryption vs. Authenticated Encryption

- Encryption $\xrightarrow{\text{Provides}}$ Confidentiality
- Message Authentication $\xrightarrow{\text{Provides}}$ Data-Origin Authentication
- In many applications, with encryption, message authentication is needed:

Encryption vs. Authenticated Encryption

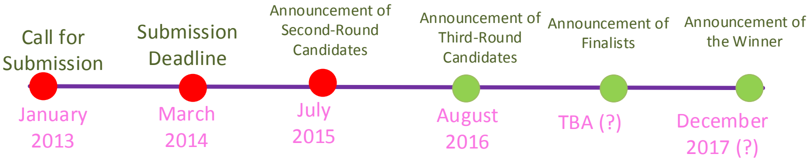
- Encryption $\xrightarrow{\text{Provides}}$ Confidentiality
- Message Authentication $\xrightarrow{\text{Provides}}$ Data-Origin Authentication
- In many applications, with encryption, message authentication is needed:



CAESAR Competition

- CAESAR: **C**ompetition for **A**uthenticated **E**ncryption: **S**ecurity, **A**pplicability, and **R**obustness
- **Aim:** identify a portfolio of authenticated ciphers that
  1. offer advantages over AES-GCM
  2. are suitable for widespread adoption
- Funded by NIST

CAESAR Competition Timeline



CAESAR Competition: Submissions

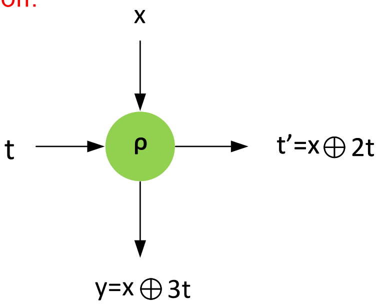
- Block Cipher Based: AEGIS, AES-COPA, AES-JAMBU, AES-OTR, AEZ, CLOC, Deoxys, **ELmD**, Joltik, OCB, POET, SCREAM, SHELL, SILC, Tiaoxin,...
- Stream Cipher Based: ACORN, HS1-SIV, MORUS, TriviA-ck
- Sponge Based: Ascon, ICEPOLE, Ketje, Keyak, NORX, PRIMATEs, STRIBOB, π-Cipher,...
- Permutation Based: Minalpher, PAEQ,...
- Compression Function Based: OMD

Specification of ELmD

- Proposed by Datta and Nandi for CAESAR
- A Third-Round CAESAR candidate
- A block cipher based Encrypt-Linear-mix-Decrypt authentication mode:
  Process message in the Encrypt-Mix-Decrypt paradigm
- Accepts Associated Data (AD)
- Online and Parallelizable

Linear Mixing Function ρ

- ρ function:



- Field multiplication modulo $p(x) = x^{128} + x^7 + x^2 + x + 1$ in $GF(2^{128})$

Message Padding Rule

Message: $M = M_1 \| M_2 \| \cdots \| M_\ell^*$

- Submitted Version:

$$M_\ell = \begin{cases} (M_\ell^* \| 10^*) \text{ if } |M_\ell^*| < 128, \\ M_\ell^* \text{ else} \end{cases} \quad \text{and } M_{\ell+1} = \oplus_{i=1}^{\ell} M_i$$

- Modified Version:

$$M_\ell = \begin{cases} (\oplus_{i=1}^{\ell-1} M_i) \oplus (M_\ell^* \| 10^*) \text{ if } |M_\ell^*| < 128, \\ (\oplus_{i=1}^{\ell-1} M_i) \oplus M_\ell^* \text{ else} \end{cases}$$

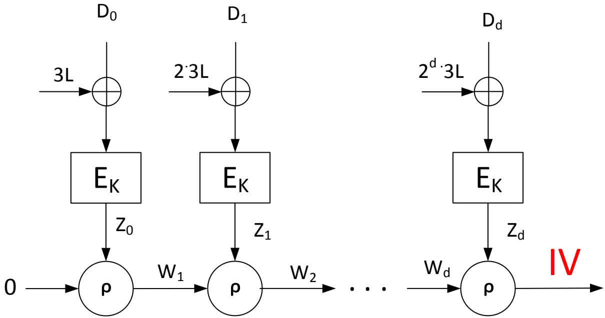
$$M_{\ell+1} = M_\ell$$

Parameters of ELmD

- AES-128 is used as E_K in either 6 or 10 rounds
  ELmD$(6, 6)$ and ELmD$(10, 10)$
- Provisions of intermediate tag (if required)
  Faster decryption and verification
- Internal parameter mask is either
  $L = \text{AES}^{10}(0)$ or $L = \text{AES}^{6}(\text{AES}^{6}(0))$

Processing Associated Data

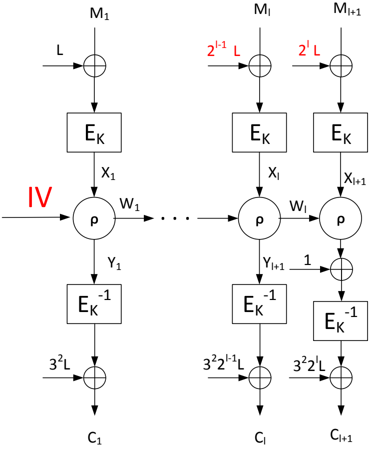
- IV is generated by processing Associated Data (D)
- D_0 = public number $\|$ parameters and $D = D_0 \| D_1 \| \cdots \| D_d^*$, where $D_d = D_d^* \| 10^*$ if $|D_d^*| \neq 128$, otherwise $D_d = D_d^*$
- If $|D_d^*| \neq 128$, Masking$= 7 \cdot 2^{d-1} \cdot 3L$



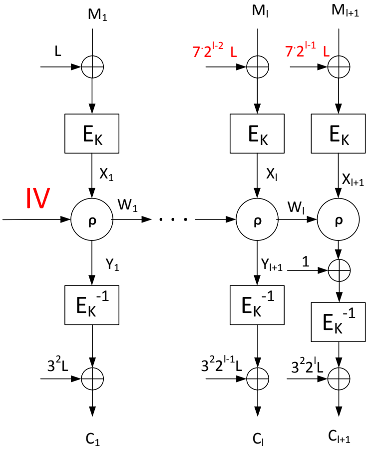
Encryption

Padded Message: $M = M_1 \| M_2 \| \cdots \| M_\ell$

Ciphertext: $(C, T) = (C_1 \| C_2 \| \cdots \| C_\ell, C_{\ell+1})$



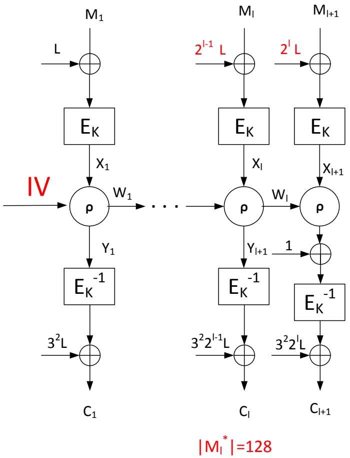
$|M_l^*| = 128$

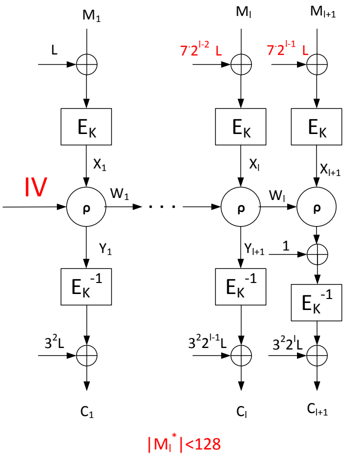


$|M_l^*| < 128$

Decryption and Tag Verification

- Decryption: Inverse of Encryption
- Tag Verification: Release plaintext if $M_{\ell+1} = M_\ell$ else $\perp$ is returned





Security Claims

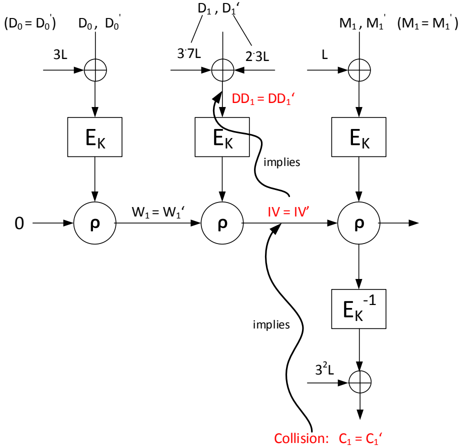
- 62.8-bit security for **Confidentiality** for any version
- 62.4-bit security for **Integrity** for any version
- Authors' claim for **Key Recovery Attacks**

  "*... one can not use this distinguishing attack to mount a plaintext or key recovery attack and we believe that our construction provides* **128 bits of security**, *against plaintext or key recovery attack*"
  We disprove by a key recovery attack on ELmD(6, 6)

Recovering Internal State L

- **Reminder:** $L = AES^6(AES^6(0))$ or $L = AES^{10}(0)$
- L is used to mask associated data, plaintexts and ciphertext
- By collision search of ciphertexts with approximate complexity 2^{65} due to birthday attack
- **Recovering L helps us to make forgery and key recovery attacks**

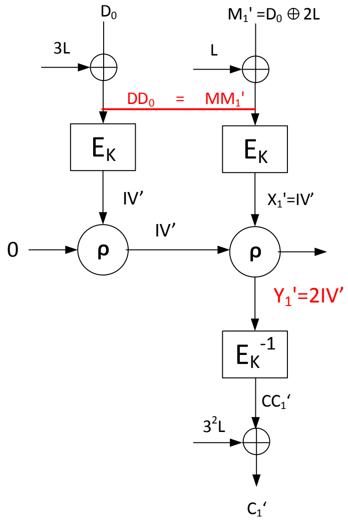
Recovering Internal State L



- Take fixed D_0, let $(D, M) = (D_1, M_1) = (\alpha, M)$ and $(D', M') = (D_1', M_1') = (\beta, M)$ be two sets of message pairs s.t. $\alpha, \beta \in \{0, 1, \ldots, 2^{64} - 1\}$
- α is an **incomplete** block and β is **complete**, i.e., $|\alpha| = 64$ and $|\beta| = 128$
- $(\alpha \| 10^{63}) \oplus \beta$ scans all values in $\mathbb{F}_{2^{128}}$
- Search a collision in the first ciphertexts, i.e., $C_1 = C_1'$
- We recover L by solving $DD_1 = DD_1'$

$$D_1 \oplus 3 \cdot 7 \cdot L = D_1' \oplus 3 \cdot 2 \cdot L,$$

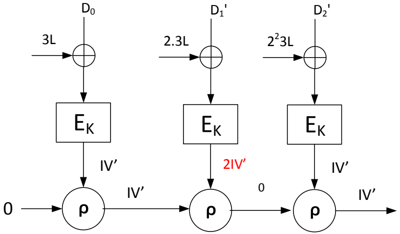
Universal Forgery



- **Target Message:** (D_0, D, M)
- First, query $(D_0, M_1 = D_0 \oplus 2L)$, and obtain (C_1, T)
- We obtain

$$E_K(C_1' \oplus 3^2 L) = 2IV'$$

Universal Forgery



- **Target Message:** (D_0, D, M)
- Query (D', M) such that $D'_0 = D_0$, $D'_1 = C_1 \oplus 3^2 L \oplus 2 \cdot 3L$, $D'_2 = D_0 \oplus 3L \oplus 2^2 \cdot 3L$ and D obtain ciphertext C and tag T
- (C, T) pair is also valid for (D, M)

Exploiting the Structure of ELmD

Using the recovered L value, we can obtain two types of plaintext pairs for AES:

1. μ-multiplicative Pairs: For any P_1 and μ,

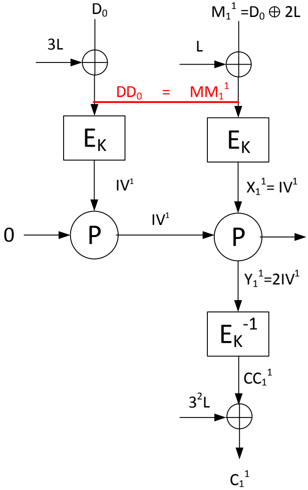
$$\mu \cdot E(P_1) = E(P_2)$$

2. 1-difference Pairs:

$$E(Q_1) = E(Q_2) \oplus 1$$

Using these pairs, we can query any ciphertext to the decryption mode of the cipher AES

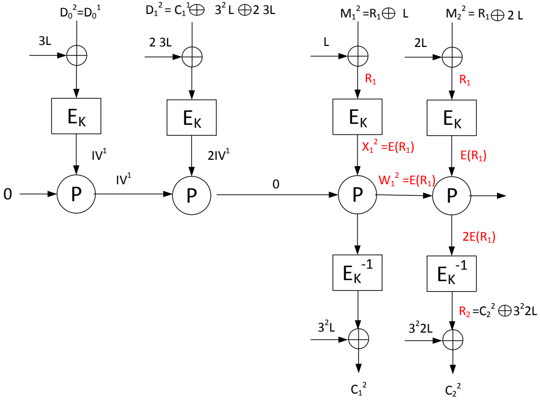
2-multiplicative Pairs: (R_1, R_2) with $2 \cdot E(R_1) = E(R_2)$



- **Similar method with Forgery Attack**
- First, query $(D_0, M_1 = D_0 \oplus 2L)$ and obtain (C_1, T)
- We obtain

$$E_K(C_1^1 \oplus 3^2L) = 2IV^1$$

2-multiplicative Pairs: (R_1, R_2) with $2 \cdot E(R_1) = E(R_2)$



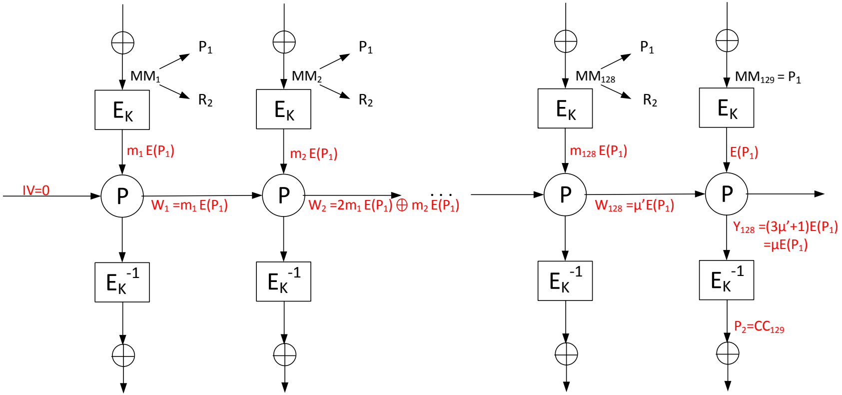
- Choose D_1 to make $IV = 0$
- Pick M_1 and M_2 s.t $MM_1 = MM_2 = R_1$
- We obtain R_2 from C_2 s.t.

$$2 \cdot E(R_1) = E(R_2)$$

μ-multiplicative Pairs: (P_1, P_2) with $\mu \cdot E(P_1) = E(P_2)$

- Obtain the plaintext R_2 such that $2 \cdot E(P_1) = E(R_2)$
- $\mu' = 3^{-1}(\mu \oplus 1)$, and $\mu' \in \mathbb{F}_{2^{128}}$ can be represented as

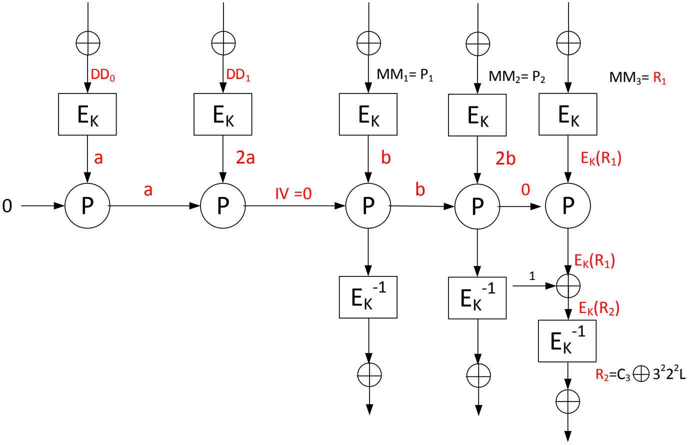
$$2^{127} \cdot m_1 \oplus 2^{126} \cdot m_2 \oplus \cdots \oplus 2 \cdot m_{127} \oplus m_{128} \text{ where } m_i \in \{1, 2\}$$



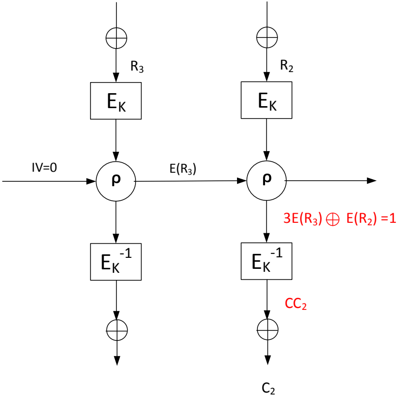
1-difference Pairs: (R_1, R_2) with $E(R_1) = E(R_2) \oplus 1$

Generate 2-multiplicative pairs:

$E(DD_1) = 2 \cdot E(DD_0)$ and $E(MM_2) = 2 \cdot E(MM_1)$



Querying Decryption Oracle of AES



- Obtain a pair (R_1, R_2) with $E(R_1) = E(R_2) \oplus 1$.
- Obtain plaintext R_3 such that $3^{-1}E(R_1) = E(R_3)$.
- By querying associated data satisfying $IV = 0$ and message with $MM_1 = R_3$, $MM_2 = R_2$, we obtain CC_2 which is equal to decryption of 1, i.e., $E(CC_2) = 0^{127}1$.
- This allows to mount a chosen ciphertext attack: pick ciphertext as μ and find P_2 s.t. $E(P_2) = \mu$
- Obtaining corresponding plaintext for any given ciphertext costs 2^8 encryption operations.

Key Recovery Attack on ELmD(6,6)

- In 2000, by using **partial sums** an attack on 6-round AES was given.
  - with a time and data complexities of 2^{44} and $2^{34.6}$, respectively.
  - This attack, in chosen plaintext scenario, can be easily adapted to chosen ciphertext case because of the AES structure.
  - The total time complexity is $2^{65} + 2^{8} \times 2^{34.6} + 2^{44} \approx 2^{65}$
- In addition, we propose a **Demirci-Selçuk meet-in-the-middle attack**
  - with (online) time and data complexities of 2^{66} and 2^{33}, respectively.
  - The total time complexity is $2^{65} + 2^{8} \times 2^{33} + 2^{66} \approx 2^{66.6}$

Comparison with the Previous Results

- Zhang and Wu analysed ELmD in terms of both authenticity and privacy
- **Authenticity:** They provide successful forgery attacks
- **Privacy:** they propose a truncated differential analysis of reduced version of ELmD with 2^{123} time and memory complexities, however they take:
  - $L = AES^4(0) \rightarrow$ **MITM attack is enough to find the key**
  - ELmD(4, 4) $\rightarrow$ **not in the proposal of ELmD**

Conclusion

- First cryptanalysis of full-round ELmD
- We disprove the security claim:
  We reduced the security of ELmD (ELmD(6, 6)) from 128 to 65 bits

Thank you for your attention!