AET-LR: Rate-1 Leakage-Resilient AEAD based on the Romulus Family

Extended Abstract

Chun Guo, Mustafa Khairallah and Thomas Peyrin

Shandong University, Shandong, China
201999900076@sdu.edu.cn
Nanyang Technological University, Singapore, Singapore
Temasek Laboratories@NTU, Singapore, Singapore
mustafam001@e.ntu.edu.sg,thomas.peyrin@ntu.edu.sg

October 20, 2020

Outline

Background

AET-LR

Security of AET-LR against Leakage Adversaries

INT-RUP (In)security of rate-1 AEAD

Outline

Background

AET-LR

Security of AET-LR against Leakage Adversaries

INT-RUP (In)security of rate-1 AEAD

Tweakable-Block Ciphers

- Interest in Tweakable Block Ciphers has been rising over the past few years.
- Six round 2 candidates use a TBC as their building block: Estate, ForkAE, LOTUS-AEAD and LOCUS-AEAD, Romulus, Skinny-AEAD and Spook.
- Some Candidates, *e.g.* GIFT-COFB, use TBCs as a tool in their analysis.

Leakage Resilience

Leakage Resilience

- Encryption Leakage vs. Decryption Leakage.
- Challenge leakage.
- Leak-free components.

Leakage Resilience from TBCs

- Recently, Berti *et. al.* [BGP+19] proposed TEDT as a TBC-based mode that is targeted towards leakage resilience. However, it required 4 TBC calls per message block.
- Independently, Naito *et. al.* [NSS20] studied the cost of masking TBCs, showing they exhibit a performance advantage over block ciphers and permutations.

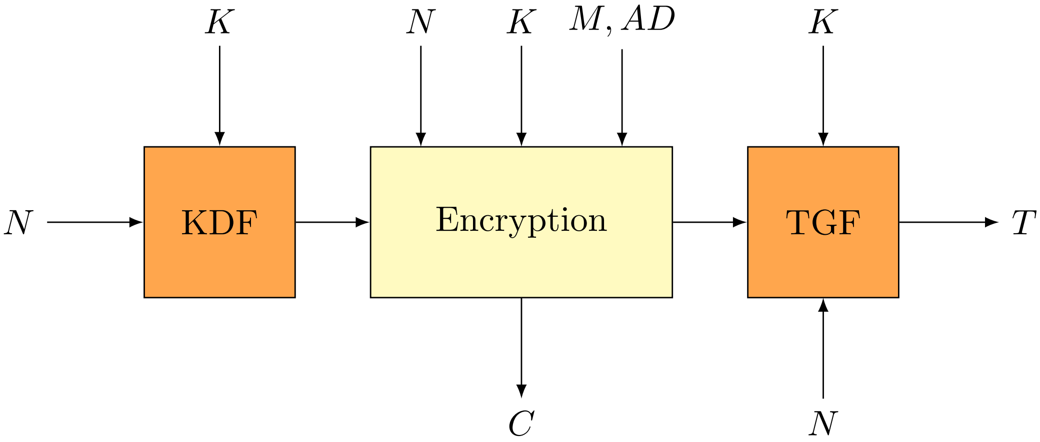
Leakage Resilience Security Targets

- Bellizia *et. al.* [BBC+20] proposed a group of targets for leakage resilience Ciphertext Integrity (CI) and confidentiality against Chosen Ciphertext Attacks (CCA).
- The targets can be classified according to three parameters: nonce, challenge-leakage and decryption-leakage.
- Possible combinations of first two parameters:

Nonce	Respecting (.)	Misuse-Resist. (M)	Misuse-Resilience (m)
Leakage	Leak-Free (.)	Leakage-Resist. (L)	Leakage-Resilience (l)

- A suffix 1 is used in the absence of decryption leakage and a suffix 2 is used in the presence of decryption leakage.

Leveled Implementations



Integrity

- Security against CIML2 adversaries is the highest target the designer can hope for in terms of integrity.
- Achieving CIML2 security with a leveled implementation is a desirable goal as it reduces the implementation cost significantly.
- Modes like TEDT and Spook achieve this goal, with rate 1/4 and 1/2 respectively.

Confidentiality

- CCAML2 is impossible to achieve [GPPS19].
- A more relaxed target is CCAmL2 achieved by TEDT. It requires a two-pass mode.
- For online modes, CCAmL1 and CCAml1 are more relaxed targets. However, they require decryption to be leak-free. Hence, they are good for modes where encryption is more resource constrained compared to decryption. Both are achieved by Spook.

Outline

Background

AET-LR

Security of AET-LR against Leakage Adversaries

INT-RUP (In)security of rate-1 AEAD

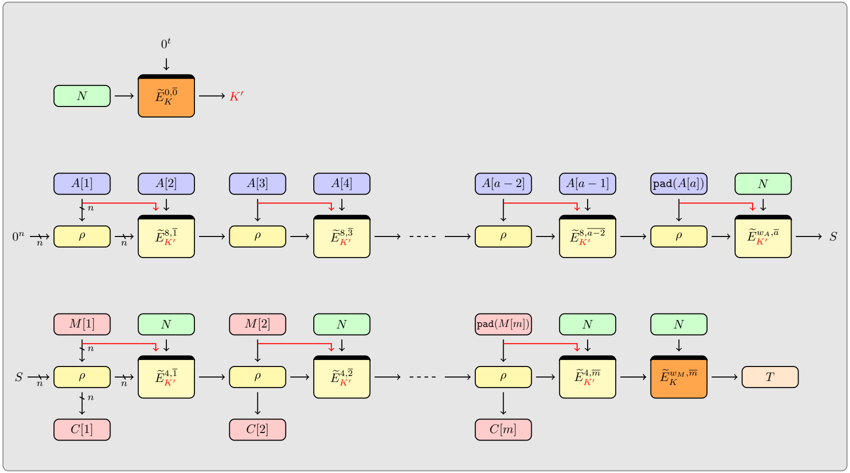
AET-LR

The philosophy of the design is to maintain the minimum lightweight performance for TBC:

1. Optimal computational efficiency, *i.e.* rate-1 operation.
2. Minimum state size of a TBC mode, *i.e.* $(n + t + k)$-bit for n-bit block, t-bit tweak and k-bit key TBC.

Simultaneously, the design adopts the leveled implementation philosophy, where only the first and last TBC calls need to be heavily protected against physical attacks.

AET-LR



0^t
N
$\widetilde{E}_K^{0,\overline{0}}$
K'
$A[1]$
$A[2]$
$A[3]$
$A[4]$
$A[a-2]$
$A[a-1]$
pad($A[a]$)
N
0^n
ρ
$\widetilde{E}_{K'}^{8,\overline{1}}$
$\widetilde{E}_{K'}^{8,\overline{3}}$
$\widetilde{E}_{K'}^{8,\overline{a-2}}$
$\widetilde{E}_{K'}^{w_A,\overline{a}}$
S
$M[1]$
$M[2]$
pad($M[m]$)
$\widetilde{E}_{K'}^{4,\overline{1}}$
$\widetilde{E}_{K'}^{4,\overline{2}}$
$\widetilde{E}_{K'}^{4,\overline{m}}$
$\widetilde{E}_K^{w_M,\overline{m}}$
T
$C[1]$
$C[2]$
$C[m]$
n

AET-LR

- AET-LR can be seen as a slight adaptation of the Romulus-N [IKMP19] AEAD mode.
- The main difference with the Romulus-N mode is simply a feed-forward of the message block into the tweak input of the TBC calls.

Outline

Background

AET-LR

Security of AET-LR against Leakage Adversaries

INT-RUP (In)security of rate-1 AEAD

CIML2 Security of AET-LR

Theorem (CIML2 Security of AET-LR)

Assume that E is an ideal cipher with n-bit blocks and $3n$-bit tweakey, then

$$\mathbf{Adv}^{\mathsf{CIML2}}_{\mathsf{AET-LR}^E}(\sigma_{\mathsf{priv}}, q_d, p) \leq \frac{6(\sigma_{\mathsf{priv}} + p + 1)(\sigma_{\mathsf{priv}} + p)}{2^n}.$$

INT-RUP Security of AET-LR

Theorem (INT-RUP Security of AET-LR)

Assume that E is an ideal cipher with n-bit blocks and $3n$-bit tweakey, then

$$\mathbf{Adv}^{\mathsf{INT\text{-}RUP}}_{\mathsf{AET-LR}^E}(\sigma_{\mathsf{priv}}, q_d, p) \leq \frac{6(\sigma_{\mathsf{priv}} + p + 1)(\sigma_{\mathsf{priv}} + p)}{2^n}.$$

CCAml Security of AET-LR

The CCAml1 security of AET-LR is studied under the following assumptions:

1. The Key Derivation Function (KDF) and Tag Generation Function (TGF) are leak-free. In practice, they are heavily protected against complex side-channel attacks, such as Differential Power Analysis (DPA).
2. The rest of the encryption operations of the mode leak everything.
3. The decryption operations are leak-free. In practice, they are heavily protected against complex side-channel attacks, such as Differential Power Analysis (DPA).

CCAml Security of AET-LR

The security of AET-LR under these assumptions can be reduced to the security of the KDF.

$$\mathbf{Adv}^{\mathsf{CCAml1}}_{\mathsf{AET-LR}^E}(\sigma_{\mathsf{priv}}, q_d, p) \leq \mathbf{Adv}^{\mathsf{TPRP}}_{E}(q_e + q_d) + \mathbf{Adv}^{\mathsf{NAE}}_{\mathsf{AET-LR}^E}(\sigma, q_e, q_d, p)$$

where $\mathbf{Adv}^{\mathsf{TPRP}}_{E}(q_e + q_d)$ refers to the security of the KDF function and $\mathbf{Adv}^{\mathsf{NAE}}_{\mathsf{AET-LR}^E}(\sigma, q_e, q_d, p)$ refers to the black box security of AET-LR in the nonce-respecting model.

Outline

Background

AET-LR

Security of AET-LR against Leakage Adversaries

INT-RUP (In)security of rate-1 AEAD

INT-RUP Insecurity of rate-1 BC-based AEAD

In CT-RSA 2016, Chakraborti *et. al.* [CDN16] presented two results about rate-1 BC-based AEAD:

- Any rate-1 BC-based AEAD scheme is INT-RUP insecure.
- Any rate-1 BC-based AEAD scheme is not integrity-secure against Nonce-repeating adversaries.

INT-RUP Insecurity of rate-1 BC-based AEAD

- Chakraborti *et. al.* [CDN16] propose a generalization of rate-1 BC-based AEAD modes.
- A significant feature is that the key $\kappa[i]$ assigned to a BC call of index i depends on the master key K, nonce N and associated data AD.
- If K, N and AD are fixed, then each key $\kappa[i]$ is fixed, irrespective of the plaintext.
- In order to, break such relation, $\kappa[i]$ has to depend on the plaintext, which would normally require processing part of the plaintext beforehand. Hence, it would not be a rate-1 mode.

INT-RUP Insecurity of rate-1 BC-based AEAD

- The results from Chakraborti *et. al.* [CDN16] do not apply to AET-LR, as the tweakey at index i can be defined as

$$\kappa[i] = M[i] \| N \| K \| D \| B$$

  where D and B are the counter and domain separation values.
- Due to the ability of TBCs to process extra inputs without extra computational costs.
- This allows TBC-based modes to break some of the barriers on BC-based modes.

Conclusions

- AET-LR (Romulus-LR) provides a safe-guard against some side-channel attacks, achieving integrity with leakage and misuse resistance through CIML2 and confidentiality with misuse and leakage resilience through CCAml1.
- Strongest security notions possible (CIML2+CCAmL2) can be achieved using TBCs using TEDT (Romulus-LR-TEDT).

Bibliography I

Davide Bellizia, Olivier Bronchain, Gaëtan Cassiers, Vincent Grosso, Chun Guo, Charles Momin, Olivier Pereira, Thomas Peters, and François-Xavier Standaert.
Mode-Level vs. Implementation-Level Physical Security in Symmetric Cryptography.
In *Advances in Cryptology – CRYPTO 2020*, 2020.

Bibliography II

Francesco Berti, Chun Guo, Olivier Pereira, Thomas Peters, and François-Xavier Standaert.
TEDT, a Leakage-Resist AEAD Mode for High Physical Security Applications.

IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(1), 2019.

Avik Chakraborti, Nilanjan Datta, and Mridul Nandi.
INT-RUP Analysis of Block-cipher Based Authenticated Encryption Schemes.
In *Topics in Cryptology - CT-RSA 2016*, 2016.

Chun Guo, Olivier Pereira, Thomas Peters, and François-Xavier Standaert.
Authenticated Encryption with Nonce Misuse and Physical Leakage: Definitions, Separation Results and First Construction.
In *Progress in Cryptology – LATINCRYPT 2019*, 2019.

- Tetsu Iwata, Mustafa Khairallah, Kazuhiko Minematsu, and Thomas Peyrin.
  Romulus v1.
  Submission to NIST Lightweight Cryptography Project, 2019.
- Yusuke Naito, Yu Sasaki, and Takeshi Sugawara.
  Lightweight Authenticated Encryption Mode Suitable for Threshold Implementation.
  In *Advances in Cryptology – EUROCRYPT 2020*, 2020.