On Leakage-Resilient Authenticated Encryption with Decryption Leakages

Francesco Berti, Olivier Pereira,
Thomas Peters, François-Xavier Standaert,

ICTEAM/ELEN/Crypto Group, Université catholique de Louvain,
Louvain-la-neuve, Belgium

FSE – March, 6th 2018

Main objective

Ciphertext Integrity with

- Randomness misuse
- Leakage in encryption & decryption

We provide

- CIML2: an extension of $\mathrm{INT}-\mathrm{CTXT}$ with misuse and leakage
- DTE2: a mode of operation achieving CIML2
- Analysis of confidentiality of DTE2 in presence of leakage

Scenario: firmware update

Adversaries has

- encrypted firmware
- leakage in decryption

Adversaries should not be able to

- create a valid update
- know the plaintext

Practical issue:

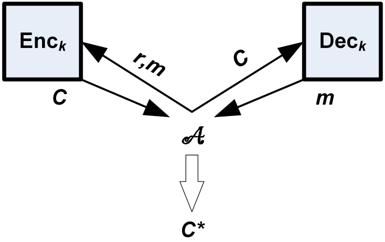
- O'Flynn [OC15]
- Moradi et al. [MBKP11]

Plan

- Background
- Authenticated Encryption with Decryption Leakage
- Why previous solutions do not work
- Eavesdropping with Decryption Leakage

INT – CTXT

Ciphertext Integrity property.



If C^* fresh and valid, adversary $\mathcal{A}$ wins

Physical leakage

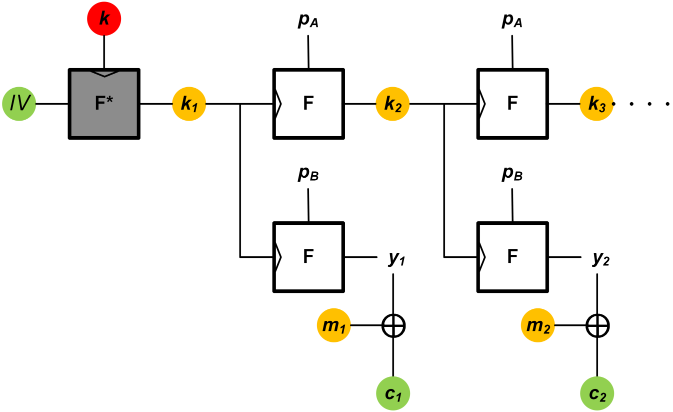
Our model for implementations:

- one component **leak free** (*slow, used twice per enc.*)
  [e.g. AES with higher order masking]
- other components with little/no leakage protection
  [e.g. AES]

Weakly protected components:

- can leak their full state for integrity
- must resist weak side-channel attacks for privacy

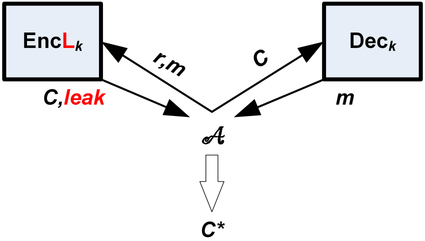
CPA *with leakage*



- It uses rekeying

CIML

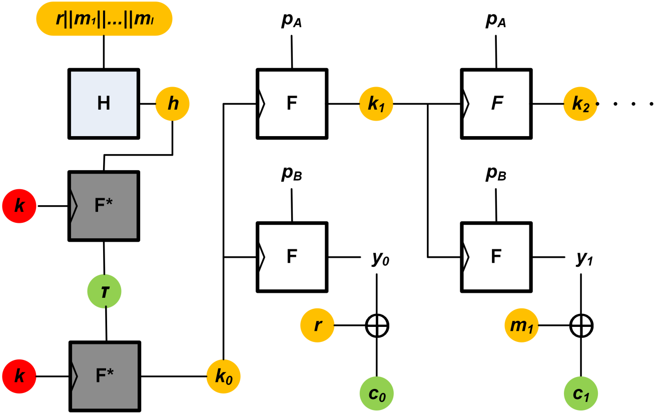
Ciphertext Integrity with leakage in encryption.



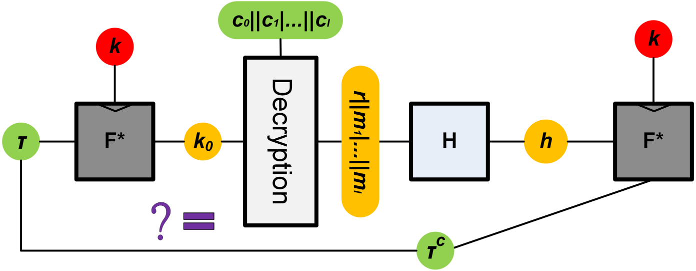
If C^* fresh and valid, adversary $\mathcal{A}$ wins

DTE *(Digest, Tag, Encrypt) [BKP$^+$16]*

Ciphertext $C = (\tau, c)$ with $c = (c_0, \dots, c_l)$



Decryption of $(\tau, c_0, .., c_l)$:



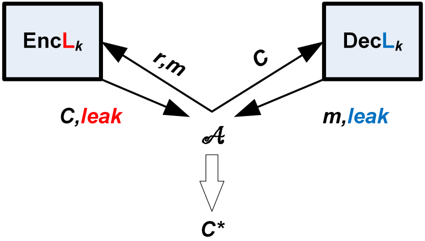
- DTE is MR + Imcpa + CIML-secure.
- **Problem:** Authenticity when decryption leaks?
  - *No*: use the leakage of k_0 to get a correct tag.

Plan

- Background
- *Authenticated Encryption with Decryption Leakage*
- Why previous solutions do not work
- Eavesdropping with Decryption Leakage

CIML2

Goal: Ciphertext Integrity with in leakage in *both* encryption *and* decryption.



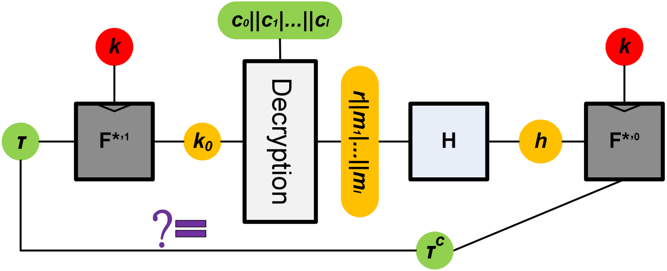
If C^* fresh and valid, adversary $\mathcal{A}$ wins

Plan

- Background
- Authenticated Encryption with Decryption Leakage
- *Why previous solutions do not work*
- Eavesdropping with Decryption Leakage

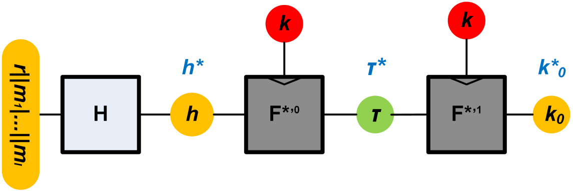
DTE′

Solution: Tweak DTE



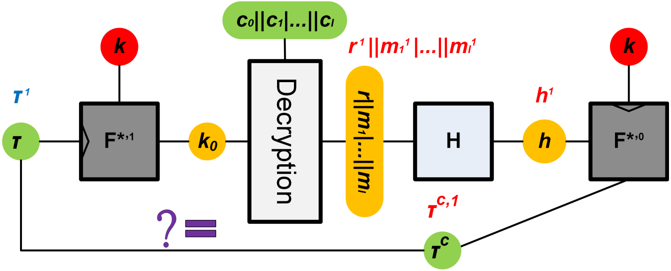
Attack against DTE′ *(1/3)*

Objective: Obtain a correct chain



Attack against DTE′ *(2/3)*

1) Get a correct tag

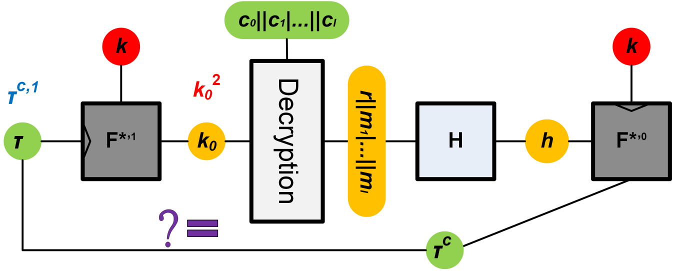


- Ask the decryption of $C^1 = (\tau^1, c^1)$. Get $r^1, m^1, h^1, \tau^{1,c}$.

Attack against DTE′ *(3/3)*

We have $r^1, m^1, h^1, \tau^{1,c}$.

2) Get the k_0 associated to $\tau^{1,c}$

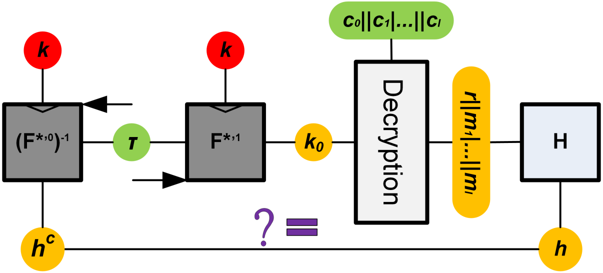


- Ask the decryption of $C^2 = (\tau^{1,c}, c^2)$. Get k_0^2.

DTE2: *A* CIML2, lmcpa *and* MR *mode*

Problem: The Dec oracle says it is invalid because the right tag is $\tau^c \neq \tau$.

Solution: The Dec oracle says it is invalid because the tag τ is the right tag for a certain hash value $h^c \neq h$.



Plan

- Background
- Authenticated Encryption with Decryption Leakage
- Why previous solutions do not work
- *Eavesdropping with Decryption Leakage*

Confidentiality

We define

- Eavesdropper security with decryption leakage (EavDL)

  [guarantees that leaking decryption of ciphertexts does not help distinguishing other ciphertexts]

We propose

- EDT, a mode achieving EavDL, CIML2 but not MR.

Conclusion

We proposed

- two new definitions:
  - CIML2
  - EavDL
- two new schemes
  - DTE2 [MR + CIML2-secure, no EavDL]
  - EDT [EavDL + CIML2-secure, no MR]

Questions ?