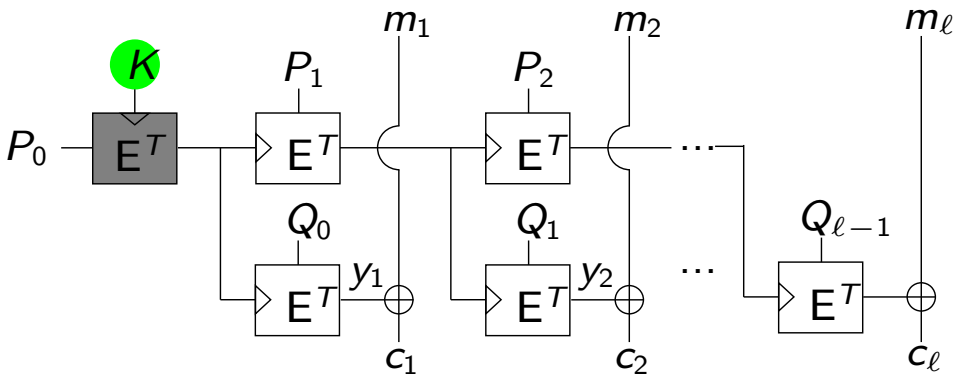
TEDT, a Leakage-Resistant AEAD Mode for High Physical Security Applications

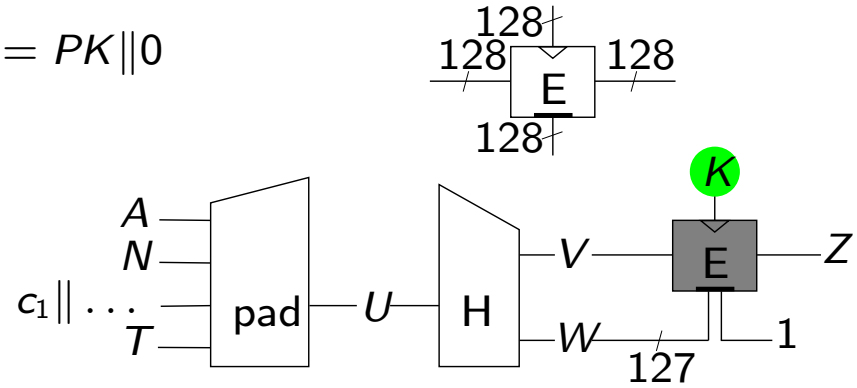
Francesco Berti Chun Guo Olivier Pereira
Thomas Peters François-Xavier Standaert

CHES 2020 – August 31, 2020

A new AEAD for Tweakable Blockciphers (TBCs)

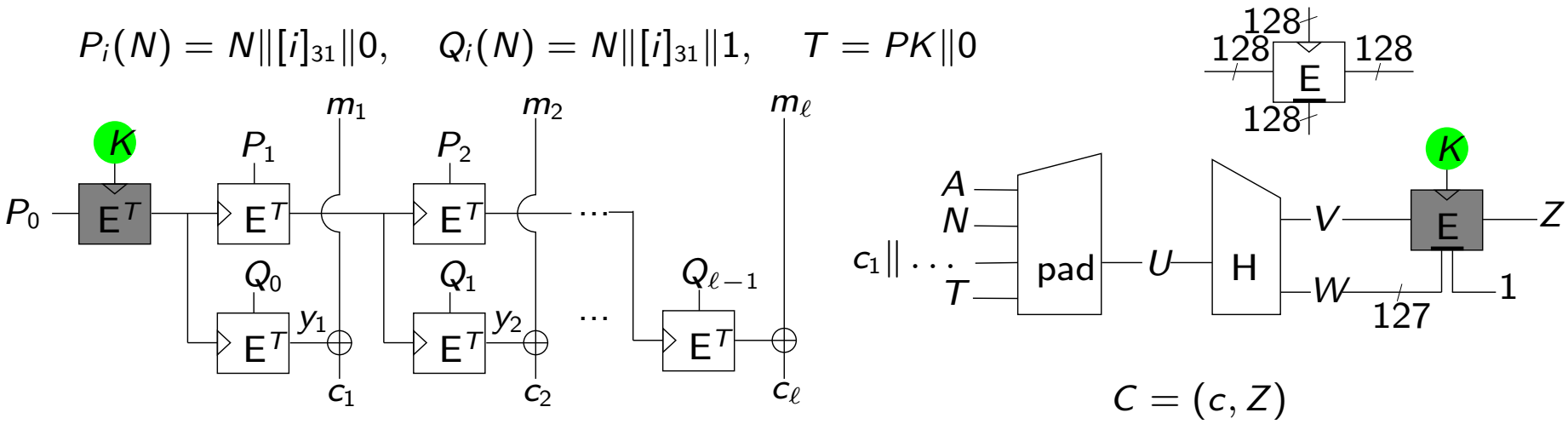
$$P_i(N) = N \| [i]_{31} \| 0, \quad Q_i(N) = N \| [i]_{31} \| 1, \quad T = PK \| 0$$





$$C = (c, Z)$$

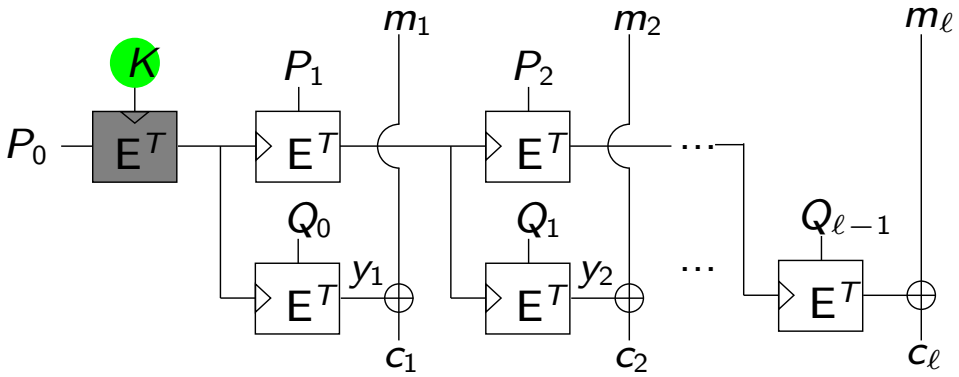
A new AEAD for Tweakable Blockciphers (TBCs)

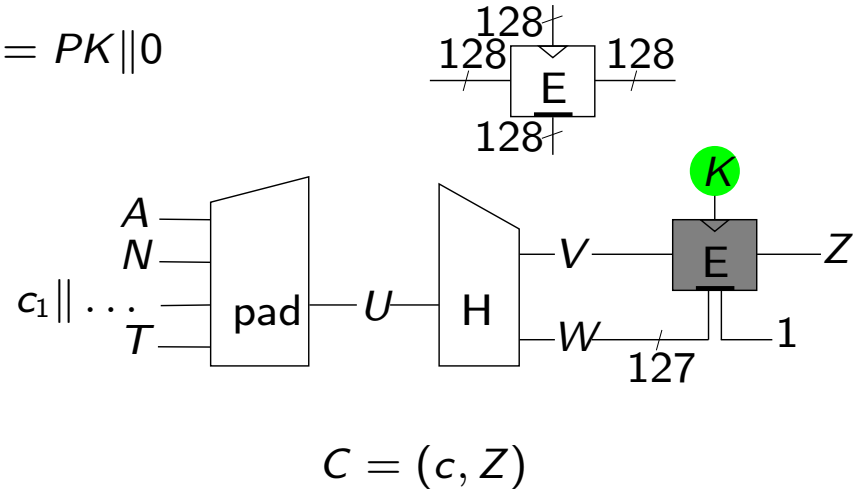


1. Full leakage-resistance: mode-level side-channel security

A new AEAD for Tweakable Blockciphers (TBCs)

$P_i(N) = N\|[i]_{31}\|0, \quad Q_i(N) = N\|[i]_{31}\|1, \quad T = PK\|0$



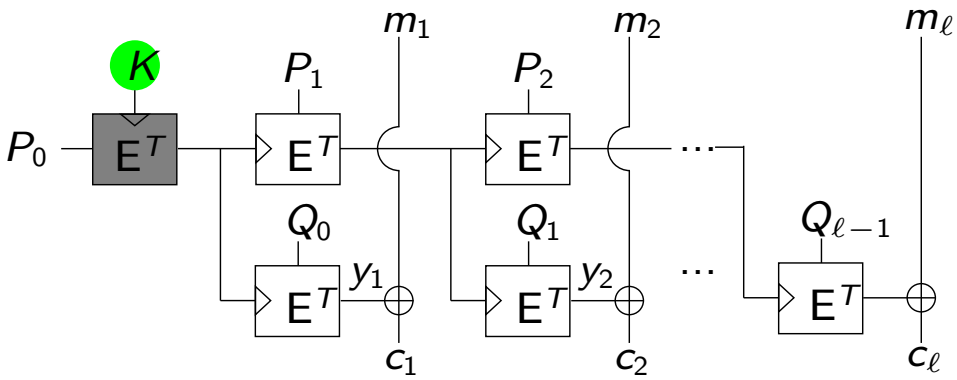


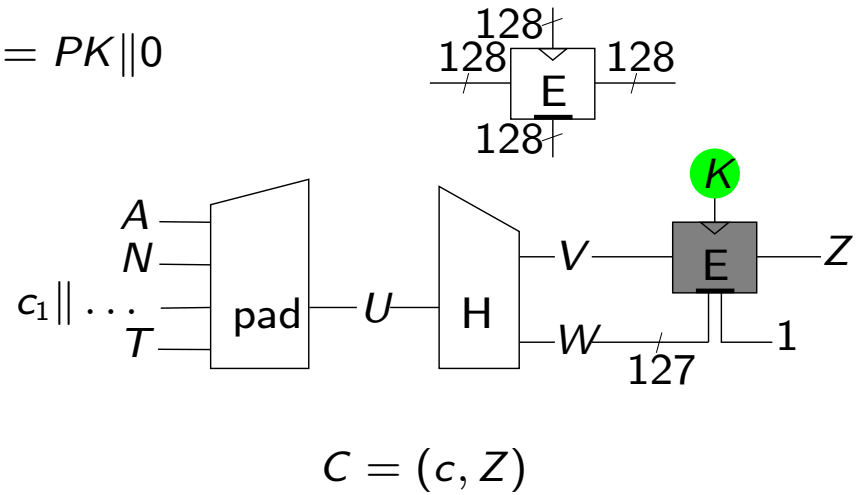
$C = (c, Z)$

1. Full leakage-resistance: mode-level side-channel security
2. Nonce misuse-resilience: confidentiality at fresh nonces

A new AEAD for Tweakable Blockciphers (TBCs)

$$P_i(N) = N\|[i]_{31}\|0, \quad Q_i(N) = N\|[i]_{31}\|1, \quad T = PK\|0$$

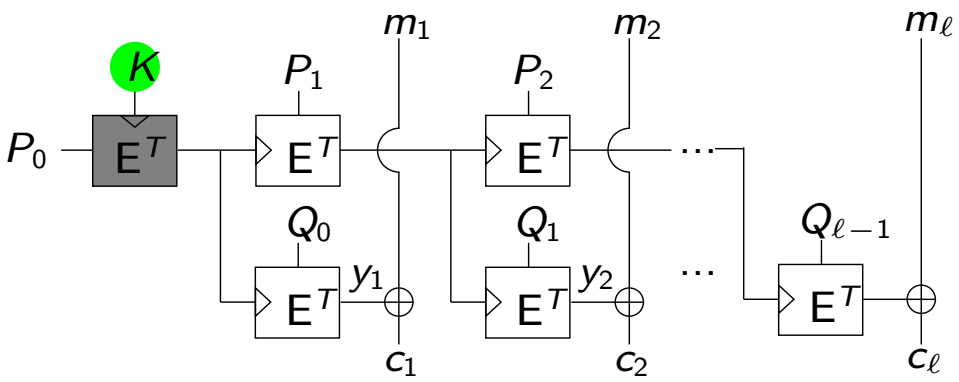


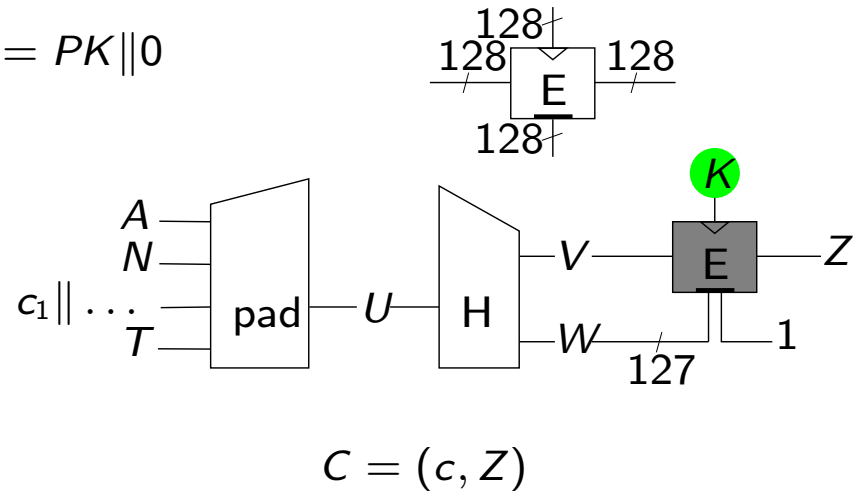


1. Full leakage-resistance: mode-level side-channel security
2. Nonce misuse-resilience: confidentiality at fresh nonces
3. High multi-user security: 114-bit security up to 2^{126} users

A new AEAD for Tweakable Blockciphers (TBCs)

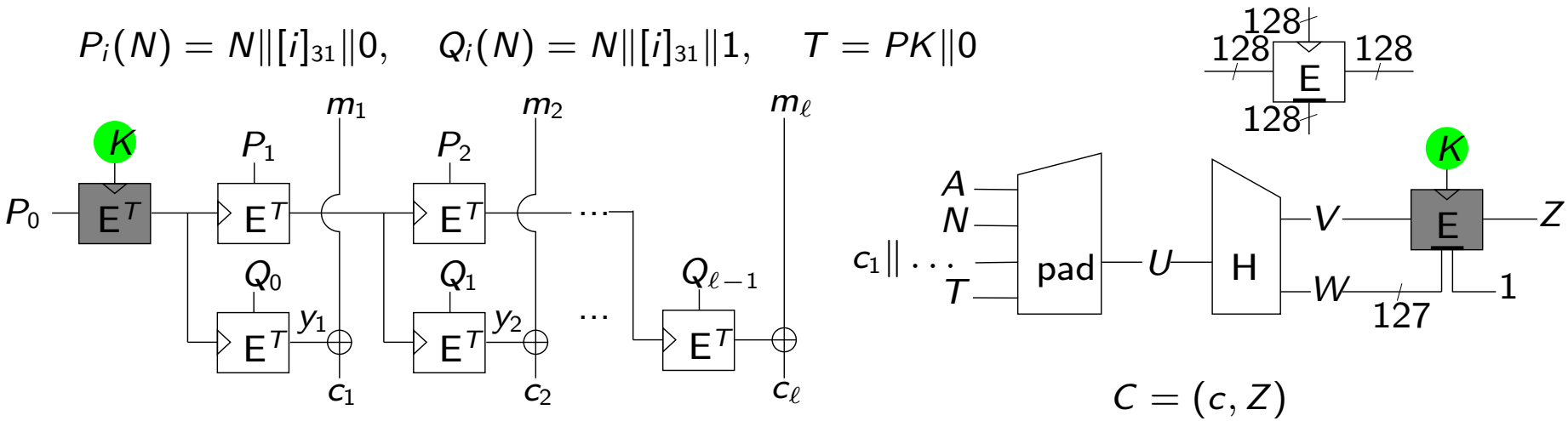
$P_i(N) = N\|[i]_{31}\|0, \quad Q_i(N) = N\|[i]_{31}\|1, \quad T = PK\|0$





1. Full leakage-resistance: mode-level side-channel security
2. Nonce misuse-resilience: confidentiality at fresh nonces
3. High multi-user security: 114-bit security up to 2^{126} users
4. Leveled implementation: strong side-channel security with low energy

A new AEAD for Tweakable Blockciphers (TBCs)



1. Full leakage-resistance: mode-level side-channel security
2. Nonce misuse-resilience: confidentiality at fresh nonces
3. High multi-user security: 114-bit security up to 2^{126} users
4. Leveled implementation: strong side-channel security with low energy
5. Online encryption, efficient handling static/incremental associated data

Outline

Background - Authenticated Encryption

Nonce-based authenticated encryption schemes with associated data (AEAD) (Enc, Dec)

- A single primitive/scheme for both confidentiality and authenticity [BN08, Rog02]

Background - Authenticated Encryption

Nonce-based authenticated encryption schemes with associated data (AEAD) (Enc, Dec)

- A single primitive/scheme for both confidentiality and authenticity [BN08, Rog02]
- Encryption: $\mathrm{Enc}(K, N, A, M) \rightarrow C$

Background - Authenticated Encryption

Nonce-based authenticated encryption schemes with associated data (AEAD) (Enc, Dec)

- A single primitive/scheme for both confidentiality and authenticity [BN08, Rog02]
- Encryption: $\mathrm{Enc}(K, N, A, M) \rightarrow C$
- Decryption: $\mathrm{Dec}(K, N, A, C) \rightarrow M$ (if integrity checking succeeds) or $\perp$ (if integrity checking fails)

Background - Authenticated Encryption

Nonce-based authenticated encryption schemes with associated data (AEAD) (Enc, Dec)

- A single primitive/scheme for both confidentiality and authenticity [BN08, Rog02]
- Encryption: $\mathrm{Enc}(K, N, A, M) \rightarrow C$
- Decryption: $\mathrm{Dec}(K, N, A, C) \rightarrow M$ (if integrity checking succeeds) or $\perp$ (if integrity checking fails)
- Confidentiality and Integrity of the message M

Background - Authenticated Encryption

Nonce-based authenticated encryption schemes with associated data (AEAD) (Enc, Dec)

- A single primitive/scheme for both confidentiality and authenticity [BN08, Rog02]
- Encryption: $\mathrm{Enc}(K, N, A, M) \rightarrow C$
- Decryption: $\mathrm{Dec}(K, N, A, C) \rightarrow M$ (if integrity checking succeeds) or $\perp$ (if integrity checking fails)
- Confidentiality and Integrity of the message M
- Integrity of the associated data A

Background - Side-channel Attacks

Simple Power Analysis (SPA)

Takes advantage of the leakages resulting from a single input (message) provided for encryption, with measurements that are possibly repeated multiple times in order to remove the noise in measurements.

Background - Side-channel Attacks

Simple Power Analysis (SPA)

Takes advantage of the leakages resulting from a single input (message) provided for encryption, with measurements that are possibly repeated multiple times in order to remove the noise in measurements.

Differential Power Analysis (DPA)

Takes the leakages resulting from the same data processing multiple data and exploits data dependency of power consumption. Reduces the computational secrecy of this state at a rate that is exponential in the number of distinct inputs.

Background - Side-channel protection

Masking, shuffling, hiding [MOP07]

Background - Side-channel protection

Masking, shuffling, hiding [MOP07]

Overheads

Background - Side-channel protection

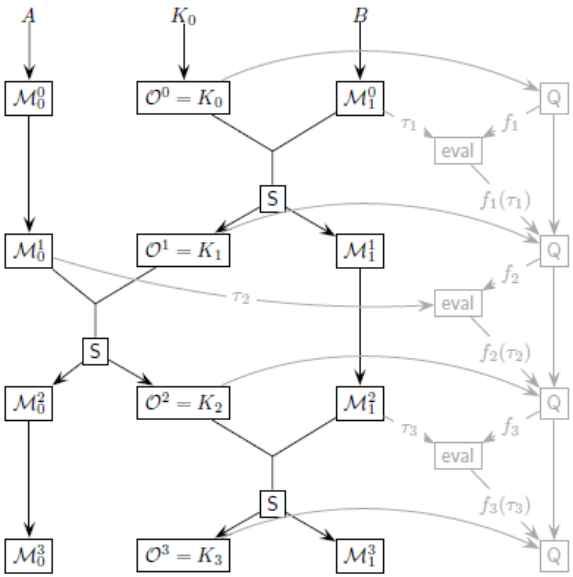
Masking, shuffling, hiding [MOP07]

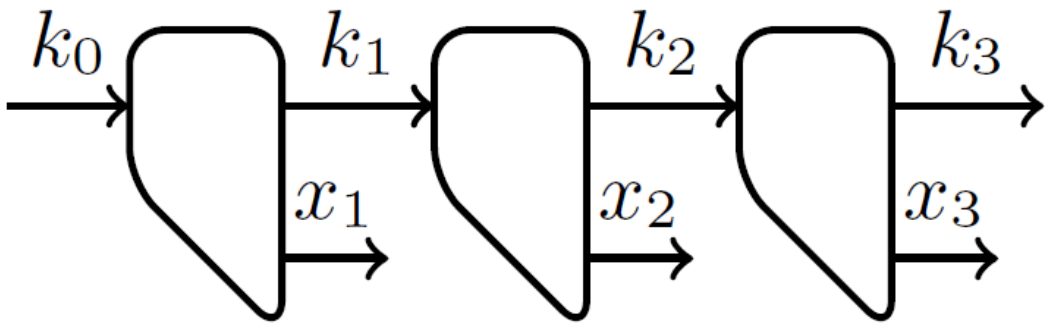
Overheads

Inevitable for a single cipher call. But what about $|M|$ cipher calls in an encryption?

Background - Leakage-resilience/resistance

Excluding DPAs by design of protocols/modes [DP08, Pie09, YSPY10]





Outline

We start from EDT in ToSC 2017 [BPPS17]

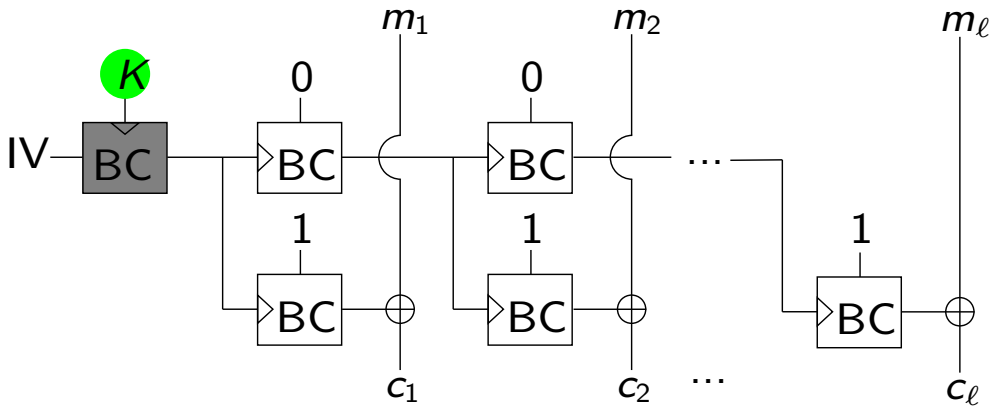
Ideas

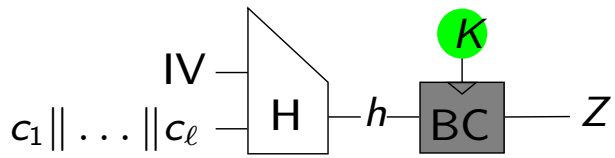
Rekeying: against side-channel key recovery
Minimal message manipulation: maximize confidentiality
Encrypt-then-MAC: resistance to decryption leakages
Hash-then-SPRP: avoid computing the correct tag using inverse BC^{-1}

We start from EDT in ToSC 2017 [BPPS17]

Ideas

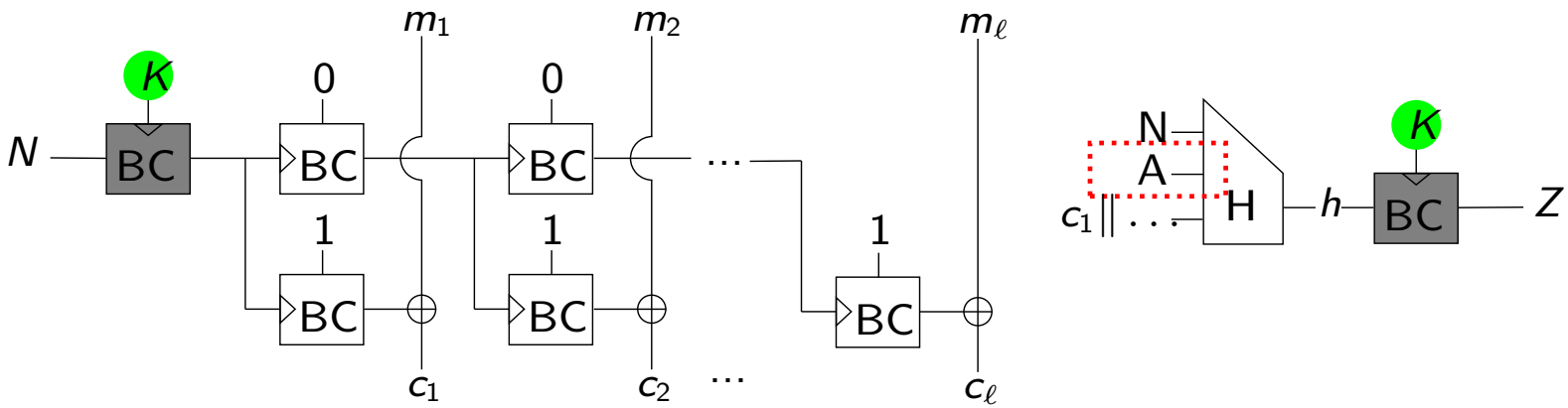
Rekeying: against side-channel key recovery
Minimal message manipulation: maximize confidentiality
Encrypt-then-MAC: resistance to decryption leakages
Hash-then-SPRP: avoid computing the correct tag using inverse BC^{-1}
Shortage: weak security bounds





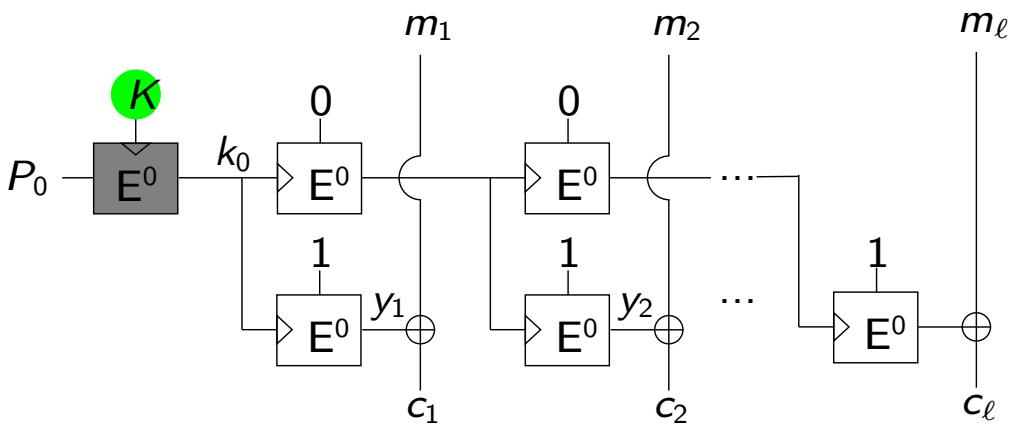
What we do?

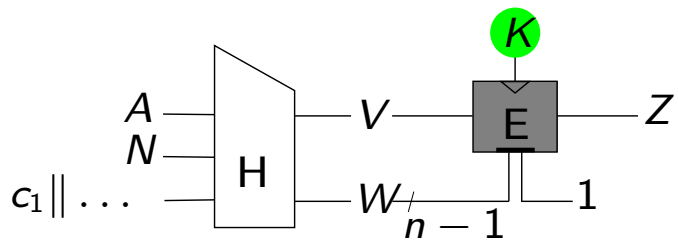
1. **Plugging AD**
2. Hash-then-TBC
3. GCM-style counter
4. Concretize the hashing
5. Better multi-user security via public keys/public randomness



What we do?

1. Plugging AD
2. **Hash-then-TBC**
3. GCM-style counter
4. Concretize the hashing
5. Better multi-user security via public keys/public randomness

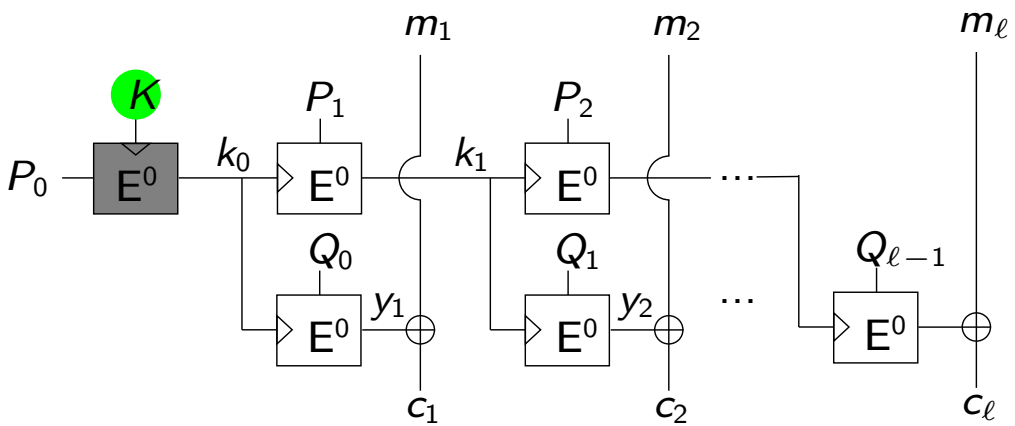


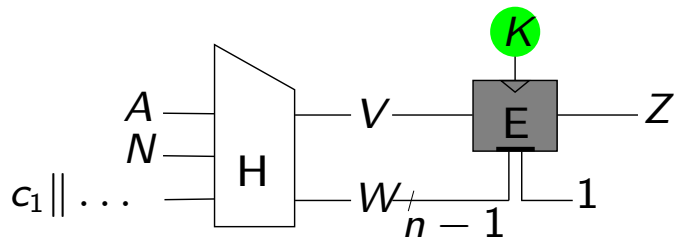


What we do?

1. Plugging AD
2. Hash-then-TBC
3. **GCM-style counter**
4. Concretize the hashing
5. Better multi-user security via public keys/public randomness

$$P_i(N) = N \| [i]_{\frac{n}{4}-1} \| 0, \quad Q_i(N) = N \| [i]_{\frac{n}{4}-1} \| 1$$





What we do?

1. Plugging AD
2. Hash-then-TBC
3. GCM-style counter
4. **Concretize the hashing**
5. Better multi-user security via public keys/public randomness

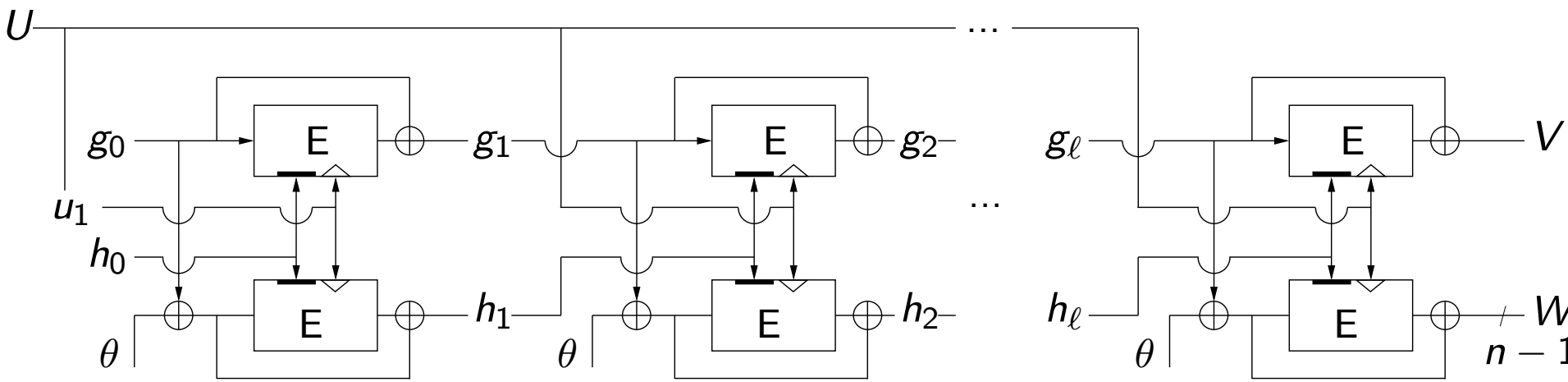
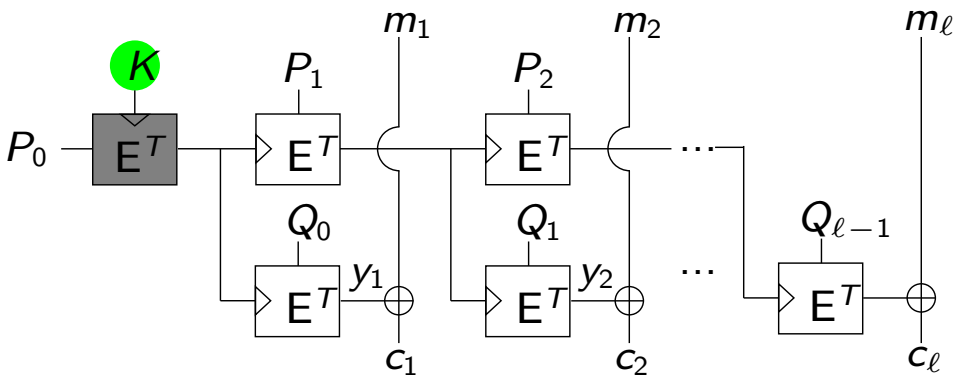


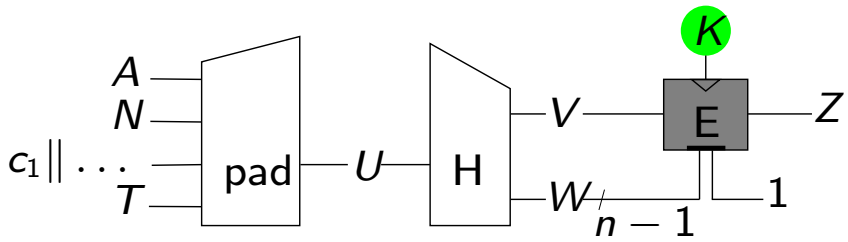
Figure: The computation of $\mathsf{H}(U) = \mathsf{H}(U_1 \| U_2 \| ... \| U_\ell)$ using the Hir[E] DBL compression function.

What we do?

1. Plugging AD
2. Hash-then-TBC
3. GCM-style counter
4. Concretize the hashing
5. **Better multi-user security via public keys/public randomness**

$$P_i(N) = N\|[i]_{\frac{n}{4}-1}\|0, \quad Q_i(N) = N\|[i]_{\frac{n}{4}-1}\|1, \quad T = PK\|0$$





$$C = (c, Z)$$

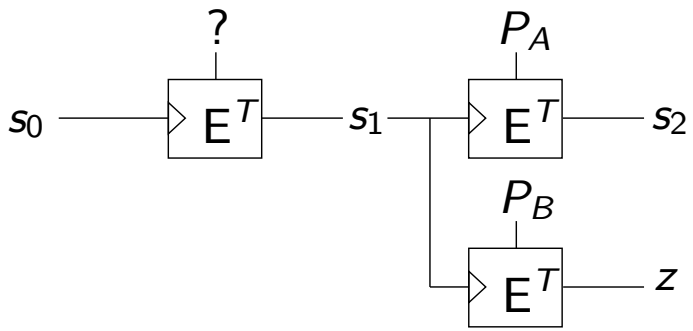
Outline

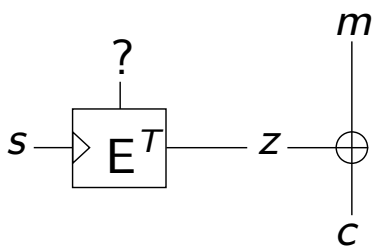
More on leakage assumptions & interpretations

Assumptions

For confidentiality: leak-free initialization & finalization, and *sufficiently hard to recover the state using SPA*

For integrity: just leak-free initialization & finalization





More on leakage assumptions & interpretations

Assumptions

For confidentiality: leak-free initialization & finalization, and *sufficiently hard to recover the state using SPA*

For integrity: just leak-free initialization & finalization

Interpretations

1. If SPA is hard then the state is safe...
   - The concrete hardness can be experimentally verified!
2. The message encryption is extended in a security preserving manner...
   - I would say this is the *best possible security*. (yes I know, the advantage may not be "negligible")

Outline

Leveled versus Uniform

Deoxys-TEDT

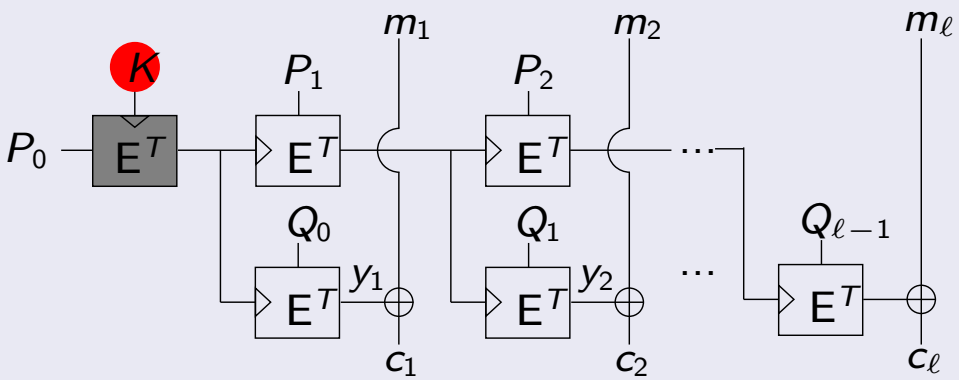
- Strongest leakage security (in the sense of [GPPS19a])
- Rate 1/4
- 1 Deoxys-BC-256 $\approx$ 1.4$\sim$1.6 AES-128
- 2 masked Deoxys-BC-256 calls + 4ℓ unprotected AES calls

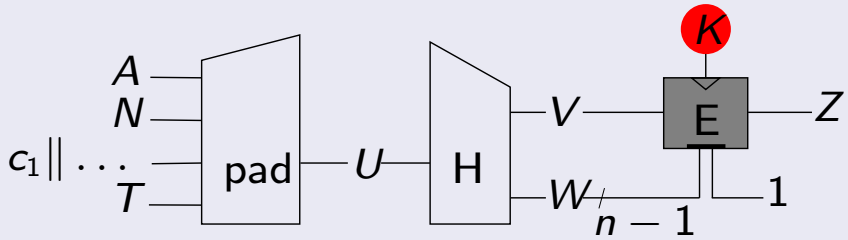
AES-OCB

- No mode-level leakage security at all
- Efficient: rate 1
- $\ell + 2$ masked AES calls

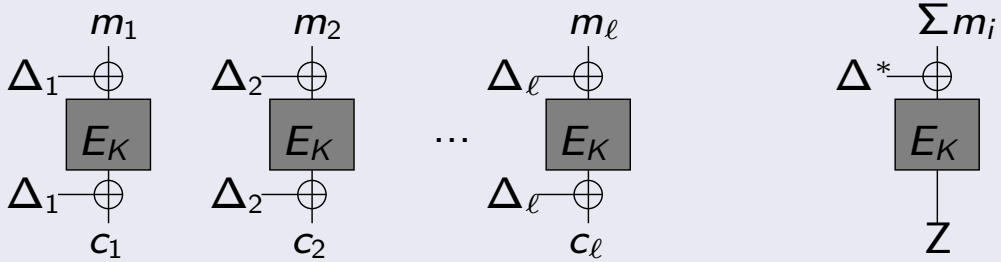
Leveled versus Uniform

Deoxys-TEDT

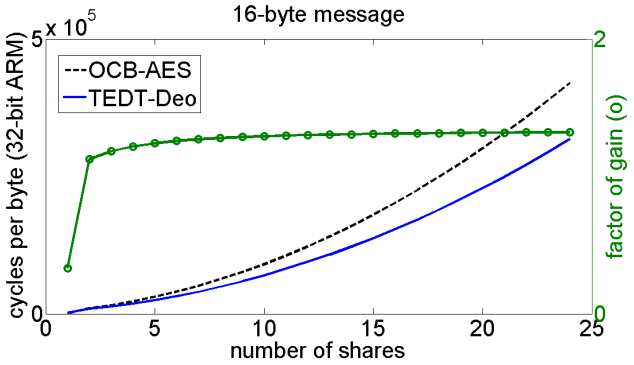


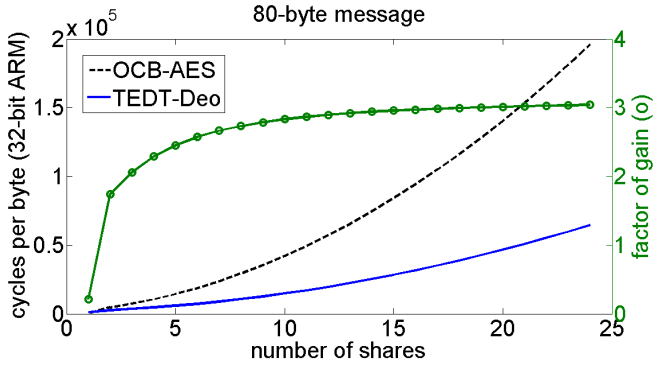


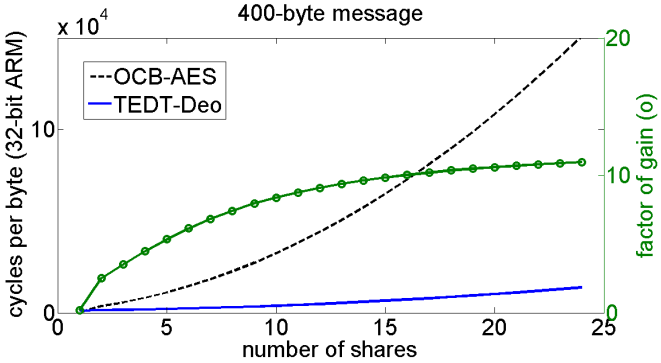
AES-OCB

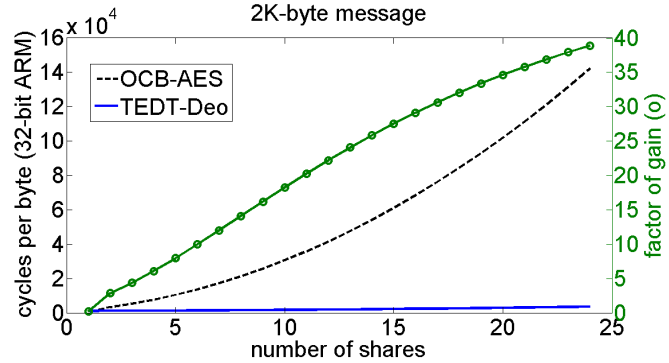


Performance

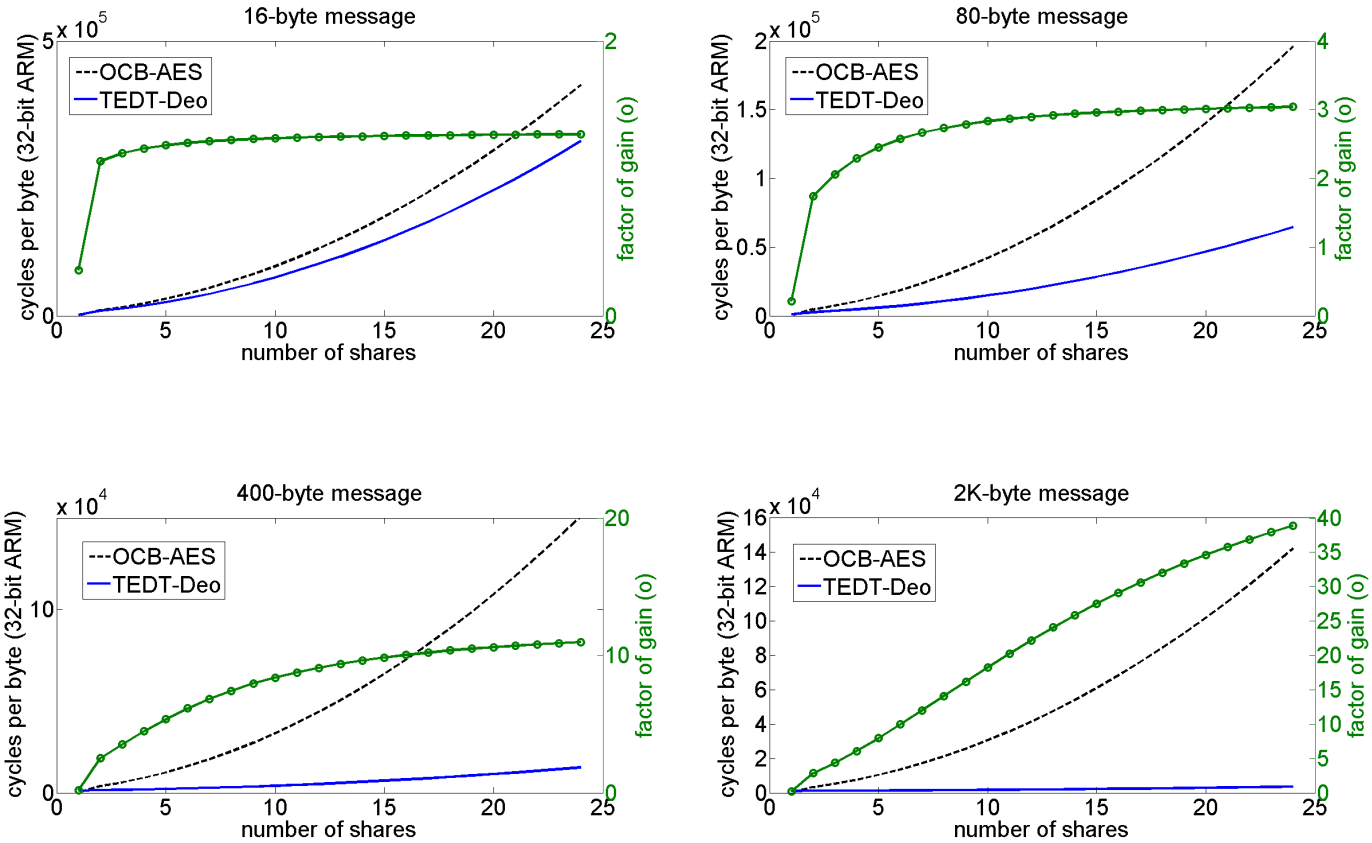






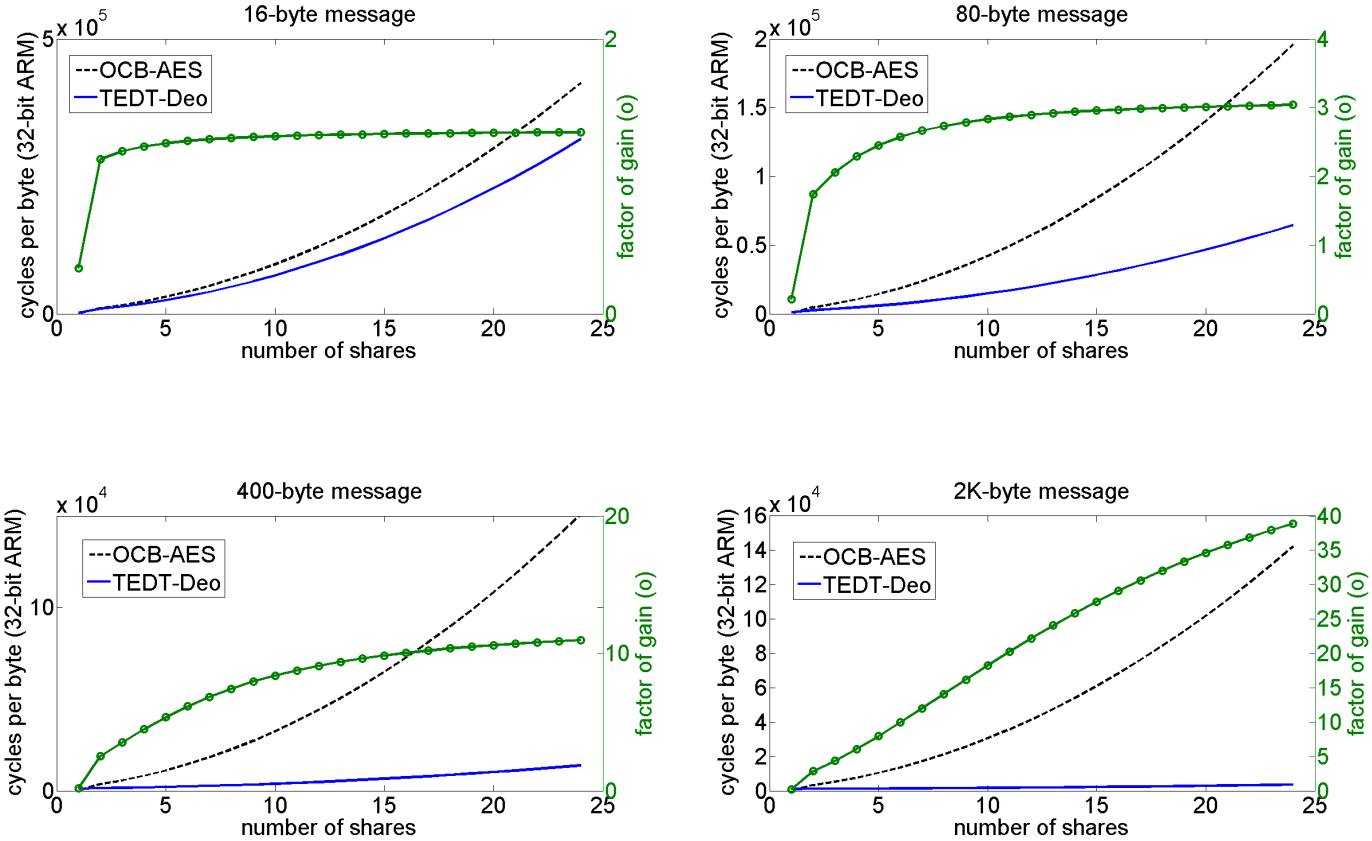


Performance



1. Starting from (the minimal) 2 shares, Deoxys-TEDT compares favorably to AES-OCB, independent of the message size.

Performance



1. Starting from (the minimal) 2 shares, Deoxys-TEDT compares favorably to AES-OCB, independent of the message size.
2. The factor of gain approximately converges towards $\frac{\ell+2}{2}$ as the number of shares increases.

To some other rekeying modes

EDT: our starting point [BPPS17]

- Multi-user security degradation
- Not fully specified
- Not so good black-box provable security

To some other rekeying modes

EDT: our starting point [BPPS17]

- Multi-user security degradation
- Not fully specified
- Not so good black-box provable security

FEMALE [GPPS19a]

- less efficient, 3 passes

To some other rekeying modes

EDT: our starting point [BPPS17]

- Multi-user security degradation
- Not fully specified
- Not so good black-box provable security

FEMALE [GPPS19a]

- less efficient, 3 passes

ISAP [DEM+17], TEDTSponge [GPPS19b]

- Very close Encrypt-then-MAC structures
- ISAP, TEDTSponge: less primitive calls
- TEDT: *forward secure*
- Ascon, Spook: 1 pass, weaker leakage confidentiality
    * The choice depends on the context.

To Barwell et al. [BMOS]

Encrypt-then-MAC, or MAC-then-Enc-then-MAC

Classical CFB mode instantiated with pairing-based leakage-resilient PRF

- The performance resembles a mode *uniformly* protected by *high-order masking*.

To Barwell et al. [BMOS]

Encrypt-then-MAC, or MAC-then-Enc-then-MAC

Classical CFB mode instantiated with pairing-based leakage-resilient PRF

- The performance resembles a mode *uniformly* protected by *high-order masking*.

Also MAC at the end, so that integrity checking goes before decrypting.

To Barwell et al. [BMOS]

Encrypt-then-MAC, or MAC-then-Enc-then-MAC

Classical CFB mode instantiated with pairing-based leakage-resilient PRF

- The performance resembles a mode *uniformly* protected by *high-order masking*.

Also MAC at the end, so that integrity checking goes before decrypting.

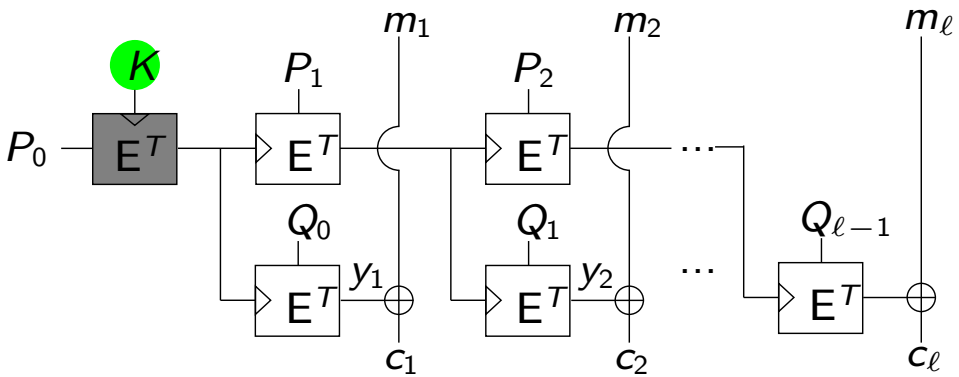
Different leakage security models

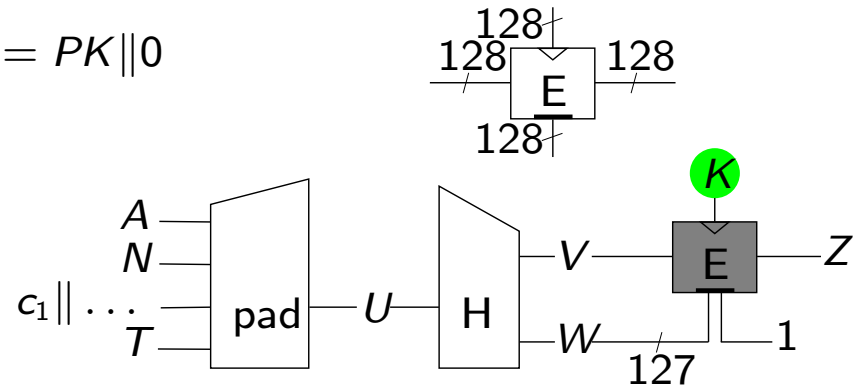
Outline

TEDT: a new AEAD for Tweakable Blockciphers

1. Full leakage-resistance
2. Nonce misuse-resilience
3. High multi-user security
4. Leveled implementation
5. Online encryption, efficient handling static and incremental AD

$$P_i(N) = N\|[i]_{31}\|0, \quad Q_i(N) = N\|[i]_{31}\|1, \quad T = PK\|0$$





$$C = (c, Z)$$

Discussion

Careful with the TBC: *chosen tweakey security* for the hashing

- Skinny [BJK+16] and Deoxys could be good.
- LRW1, LRW2 [LRW11], XEX [Rog04], etc. insufficient.

Discussion

Careful with the TBC: *chosen tweakey security* for the hashing

- Skinny [BJK+16] and Deoxys could be good.
- LRW1, LRW2 [LRW11], XEX [Rog04], etc. insufficient.

Public versus secret keys

You can of course use longer secret keys for better multi-user security. But public keys are:

- easier to generate: just pick a random string
- easier to transfer: just send PK in cleartext
    * Key agreement protocol is needed for secret keys.

Thanks for your attention!

Questions or Comments?


Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim.
The SKINNY family of block ciphers and its low-latency variant MANTIS.
In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 123–153. Springer, Heidelberg, August 2016.


Guy Barwell, Daniel P. Martin, Elisabeth Oswald, and Martijn Stam.
Authenticated Encryption in the Face of Protocol and Side Channel Leakage.
In *ASIACRYPT 2017, Part I*, pages 693–723.


Mihir Bellare and Chanathip Namprempre.
Authenticated encryption: Relations among notions and analysis of the generic composition paradigm.
Journal of Cryptology, 21(4):469–491, October 2008.


Francesco Berti, Olivier Pereira, Thomas Peters, and François-Xavier Standaert.
On leakage-resilient authenticated encryption with decryption leakages.
IACR Trans. Symm. Cryptol., 2017(3):271–293, 2017.


Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, and Thomas Unterluggauer.
ISAP - Towards Side-Channel Secure Authenticated Encryption.
IACR Trans. Symmetric Cryptol., 2017(1):80–105, 2017.


Stefan Dziembowski and Krzysztof Pietrzak.
Leakage-resilient cryptography.
In *49th FOCS*, pages 293–302. IEEE Computer Society Press, October 2008.


Chun Guo, Olivier Pereira, Thomas Peters, and François-Xavier Standaert.

Authenticated encryption with nonce misuse and physical leakage: Definitions, separation results and first construction - (extended abstract).
In *LATINCRYPT*, volume 11774 of *Lecture Notes in Computer Science*, pages 150–172. Springer, 2019.


Chun Guo, Olivier Pereira, Thomas Peters, and François-Xavier Standaert.
Towards Low-Energy Leakage-Resistant Authenticated Encryption from the Duplex Sponge Construction.
IACR Cryptology ePrint Archive, 2019:133, 2019.


Moses Liskov, Ronald L. Rivest, and David Wagner.
Tweakable block ciphers.
Journal of Cryptology, 24(3):588–613, July 2011.


Stefan Mangard, Elisabeth Oswald, and Thomas Popp.
Power Analysis Attacks - Revealing the Secrets of Smart Cards.
Springer, 2007.


Krzysztof Pietrzak.

A leakage-resilient mode of operation.
In Antoine Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 462–482. Springer, Heidelberg, April 2009.


Phillip Rogaway.
Authenticated-encryption with associated-data.
In Vijayalakshmi Atluri, editor, *ACM CCS 02*, pages 98–107. ACM Press, November 2002.


Phillip Rogaway.
Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC.
In Pil Joong Lee, editor, *ASIACRYPT 2004*, volume 3329 of *LNCS*, pages 16–31. Springer, Heidelberg, December 2004.


Yu Yu, François-Xavier Standaert, Olivier Pereira, and Moti Yung.
Practical leakage-resilient pseudorandom generators.
In Ehab Al-Shaer, Angelos D. Keromytis, and Vitaly Shmatikov, editors, *ACM CCS 10*, pages 141–151. ACM Press, October 2010.