CTET$^+$: A Beyond-Birthday-Bound Secure Tweakable Enciphering Scheme Using a Single Pseudorandom Permutation

Benoît Cogliati[1] Jordan Ethan[1] Virginie Lallemand[2] Byeonghak Lee[3]
Jooyoung Lee[3] Marine Minier[2]

[1]CISPA Helmholtz Center for Information Security, Saarbrücken, Germany

[2]Université de Lorraine, CNRS, Inria, LORIA, Nancy, France

[3]KAIST, Daejeon, Korea

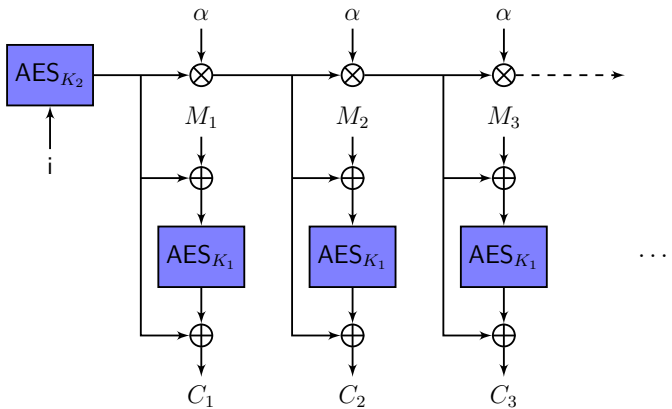
FSE 2022, March 24th 2022

Disk Encryption

- context: encrypted data storage (full disk encryption)
- typical disk sector size: 512B to a few KB
- problem: no room to store additional data (nonce/random IVs/authentication tag)
- workaround: encrypt each sector independently

Current Standard: AES-XTS [IEE08, Dwo10]

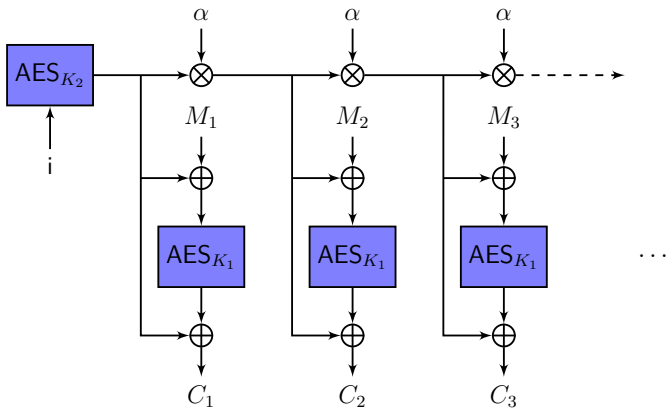
- Tweakable mode of opertation combined with the XEX transformation for AES (security when the number of queried blocks is $\ll 2^{64}$)



- Problems: small granularity, big data centers most likely hold $> 2^{50}$ bytes

Current Standard: AES-XTS [IEE08, Dwo10]

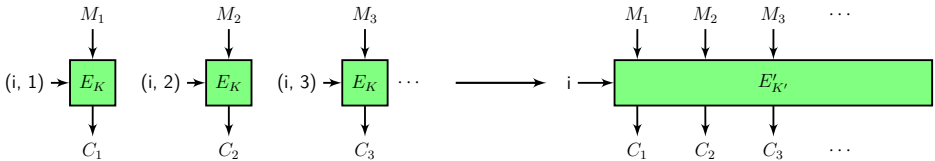
- Tweakable mode of opertation combined with the XEX transformation for AES (security when the number of queried blocks is $\ll 2^{64}$)



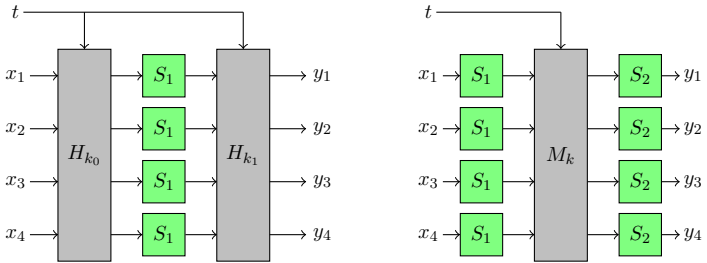
- Problems: small granularity, big data centers most likely hold $> 2^{50}$ bytes

Wide Tweakable Block Ciphers

- workaround: use whole sectors as input blocks to a "wide" TBC based on a Block Cipher
- 1-bit change in $M_1 \rightarrow$ all cipher text blocks affected (solves granularity issue)

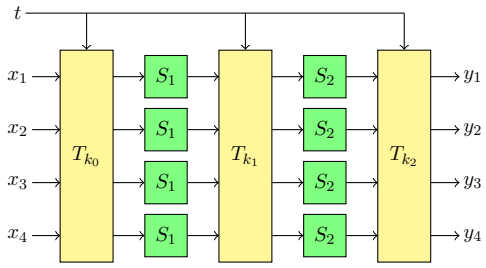


Examples



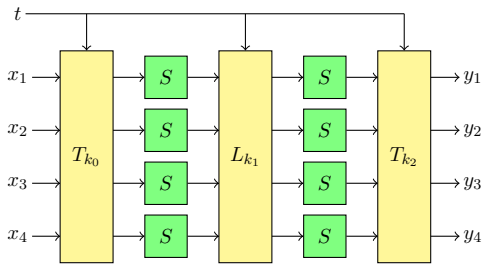
- 3 families of constructions:
  - Encrypt-Mix-Encrypt [HR03, HR04, Hal04]
  - Hash-Encrypt-Hash [CS06b, Hal07]
  - Hash-Counter-Hash [WFW05, CS06a, FM07]
- require either ≈ 2 AES calls, or ≈ 1 AES call and 2 field multiplications per block
- secure up to 2^{64} queries (Beyond Birthday Bound security $\rightarrow$ more layers)

2-Round SPN as a Tweakable Domain Extender for Block Ciphers



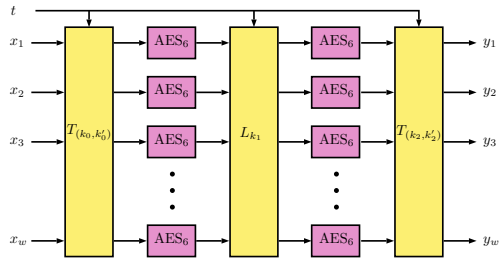
- Hash-Encrypt-Hash-Encrypt-Hash paradigm
- Secure up to $2^{2n/3}$ queries as long as T and T^{-1} are almost Super-Blockwise-Universal and Uniform (SBU) [CDK+18]

CTET$^+$



- Optimisation of the 2-round SPN: same permutation, more efficient middle layer (1 field multiplication per block $\rightarrow$ 1 doubling per block).
- secure up to $2^{2n/3}$ queries as long as T and T^{-1} are SBU

AES_6-CTET+



- block x_i, tweak t of 128 bits
- $T_{(k_0,k_0')}$ and $T_{(k_2,k_2')}$, L_{k_1}
- "*AES-box*": 6 rounds of AES-128 with a secret key
- claim: 127-bit of security

total: 5×128-bit key $(k_0, k_0'), k_1, (k_2, k_2')$ for the 3 affine layers, 128-bit key for the AES-box

Security Analysis

Our **security proof** justifies the fact that the generic structure of $\mathrm{AES}_6-\mathrm{CTET}+$ is sound, and will resist generic attacks with high probability

- H-coefficients technique

We need **dedicated cryptanalysis** to justify our security claims when the Sbox is 6 rounds of AES

- Exploit weakness of AES and extend it to full construction (AES's strength)
- Structural attacks: yoyo technique,truncated differentials

Conclusion

Scheme	Key size	Security	Efficiency (cycles/byte)		References
			512 bytes	4096 bytes	
XTS	2κ	$n/2$	0.80	0.66	[IEE08, Dwo10]
EME	κ	$n/2$	1.66	1.50	[HR04]
XCB	κ	$n/2$	1.40	1.15	[FM07]
TET	2κ	$n/2$	1.49	1.47	[Hal07]
AES_6-CDK	$6n$	$2n/3$	1.91	1.83	[CDK^+18]
AES_6-CTET^+	$5n + \kappa$	$2n/3$	1.55	1.46	This work
AES-CTET^+			2.32	2.22	

Thank you for your attention!

Conclusion

Scheme	Key size	Security	Efficiency (cycles/byte)		References
			512 bytes	4096 bytes	
XTS	2κ	$n/2$	0.80	0.66	[IEE08, Dwo10]
EME	κ	$n/2$	1.66	1.50	[HR04]
XCB	κ	$n/2$	1.40	1.15	[FM07]
TET	2κ	$n/2$	1.49	1.47	[Hal07]
AES_6-CDK	$6n$	$2n/3$	1.91	1.83	[CDK^+18]
AES_6-CTET^+	$5n + \kappa$	$2n/3$	1.55	1.46	This work
AES-CTET^+			2.32	2.22	

Thank you for your attention!

References I


Benoît Cogliati, Yevgeniy Dodis, Jonathan Katz, Jooyoung Lee, John P. Steinberger, Aishwarya Thiruvengadam, and Zhe Zhang. Provable Security of (Tweakable) Block Ciphers Based on Substitution-Permutation Networks. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - Proceedings, Part 1*, volume 10991 of *LNCS*, pages 722–753. Springer, 2018.


Debrup Chakraborty and Palash Sarka. HCH: A New Tweakable Enciphering Scheme Using the Hash-Encrypt-Hash Approach. In Rana Barua and Tanja Lange, editors, *Progress in Cryptology - INDOCRYPT 2006*, volume 4329 of *LNCS*, pages 287–302. Springer, 2006.


Debrup Chakraborty and Palash Sarkar. A New Mode of Encryption Providing a Tweakable Strong Pseudo-random Permutation. In Matthew Robshaw, editor, *Fast Software Encryption - FSE 2006*, volume 4047 of *LNCS*, pages 293–309. Springer, 2006.


Morris Dworkin. Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices. *NIST SP 800-38E*, 2010.

References II


Scott R. Fluhrer and David A. McGrew. The Security of the Extended Codebook (XCB) Mode of Operation. In Carlisle Adams, Ali Miri, and Michael Wiener, editors, *SAC 2007: Selected Areas in Cryptography*, volume 4876 of *LNCS*, pages 311–327. Springer, 2007.


Shai Halevi. EME*: Extending EME to Handle Arbitrary-Length Messages with Associated Data. In Anne Canteaut and Kapaleeswaran Viswanathan, editors, *Progress in Cryptology - INDOCRYPT 2004*, volume 3348 of *LNCS*, pages 315–327. Springer, 2004.


Shai Halevi. Invertible Universal Hashing and the TET Encryption Mode. In Alfred Menezes, editor, *Advances in Cryptology - Crypto 2007*, volume 4622 of *LNCS*, pages 412–429. Springer, 2007.


Shai Halevi and Phillip Rogaway. A Tweakable Enciphering Mode. In Dan Boneh, editor, *Advances in Cryptology - Crypto 2003*, volume 2729 of *LNCS*, pages 482–499. Springer, 2003.


Shai Halevi and Phillip Rogaway. A Parallelizable Enciphering Mode. In Tatsuaki Okamoto, editor, *Topics in Cryptology - CT-RSA 2004*, volume 2964 of *LNCS*, pages 292–304. Springer, 2004.


IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices. *IEEE Std 1619-2007*, pages 17–30, April 2008.

References III


Peng Wang, Dengguo Feng, and Wenling Wu. The Security of the Extended Codebook (XCB) Mode of Operation. In Dengguo Feng, Dongdai Lin, and Moti Yung, editors, *CISC 2005: Information Security and Cryptology*, volume 3822 of *LNCS*, pages 175–188. Springer, 2005.

CTET+ construction

$$T_{k,k'}(t,x) = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_w \end{bmatrix} \oplus \left\langle \begin{bmatrix} k \\ k^2 \\ \vdots \\ k^w \end{bmatrix}, \begin{bmatrix} x_1 \oplus t \\ x_2 \oplus t \\ \vdots \\ x_w \oplus t \end{bmatrix} \right\rangle \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \oplus \begin{bmatrix} k' \\ \alpha k' \\ \vdots \\ \alpha^{w-1} k' \end{bmatrix}$$

$$L_k(t,x) = \begin{bmatrix} 3 & 2 & & 2 \\ 2 & 3 & & 2 \\ & & \ddots & \\ 2 & 2 & & 3 \end{bmatrix} x \oplus \begin{bmatrix} t \\ t \\ \vdots \\ t \end{bmatrix} \oplus \begin{bmatrix} k' \\ \alpha k' \\ \vdots \\ \alpha^{w-1} k' \end{bmatrix}$$