Two Decades of Research on Tweakable Enciphering Schemes

Palash Sarkar

Indian Statistical Institute, Kolkata

The 11th Asian-workshop on Symmetric Key Cryptography (ASK 2024)
17th December, 2024

Tweakable Enciphering Scheme

Halevi-Rogaway (Crypto 2003)

- Length preserving encryption.
  - Handle “large” block sizes.
  - Handle variable length messages.
- Supports a tweak.
  - Provides flexibility in applications.
- Security: strong pseudo-random permutation.

Motivating application: low-level disk encryption.

Accordion Mode

NIST of USA[1] (April 2024)

> *We define an accordion (cipher) mode to be a tweakable enciphering mode that takes message input with variable input lengths (VIL) and behaves as a strong pseudorandom permutation (SPRP).*
>
> *NIST is interested in standardizing an accordion mode that could support derived functions for at least three applications: AEAD, tweakable encryption, and deterministic authenticated encryption.*

[1] https://csrc.nist.gov/files/pubs/other/2024/04/10/proposal-of-requirements-for-an-accordion-mode-dis/iprd/docs/proposal-of-requirements-for-an-accordion-mode-discussion-draft.pdf

Strong Pseudo-Random Permutation

(n, n)-PRF to $(2n, 2n)$-SPRP:

- *Luby-Rackoff (SIAM.JC 1988)*: construction based on a 4-round Feistel network requiring 4 different (n, n)-PRF.
- *Naor-Reingold (JoC 1999)*: 2 different (n, n) PRFs + 2 almost XOR universal (AXU) hash functions.
- A long line of further improvements.
  - *Iwata-Kurosawa (IEICE 2007)*: four rounds, with the same PRF in the inner two rounds and the same AXU hash function in the outer two rounds, with the key for the hash function derived using the PRF.
  - More rounds with improved security bounds.

Strong Pseudo-Random Permutation

Length preserving encryption

- *Naor-Reingold (JoC 1999)*: A 3-layer construction.
  - First and third layers are invertible blockwise AXU hash functions.
  - Middle layer is an encryption layer consisting of multiple copies of $(2n, 2n)$ 2-round Feistel permutations built using two PRFs.
- NR mode of operation[2]: A 3-layer construction.
  - First and third layers are invertible blockwise AXU hash functions.
  - Middle layer is an ECB encryption using a block cipher.

[2] https://omereingold.wordpress.com/wp-content/uploads/2014/10/nr_mode.pdf

CMC

Halevi-Rogaway (Crypto 2003)

- Incorporates the notion of tweak (due to *Moses-Liskov-Wagner (Crypto 2002)*) into the notion of length preserving SPRP.
- Encrypt-mix-encrypt: 2 encryption layers sandwiching a lightweight mixing layer.
- Both encryption layers are built from a block cipher using CBC mode ($\Rightarrow$ sequential).
  - Switch from Naor-Reingold's hash-encrypt-hash approach to encrypt-mix-encrypt because the authors found it difficult to construct an appropriate invertible blockwise AXU hash function.

Note: A previous construction called EMD[3] by *Rogaway (ePrint 2002)* was broken by *Joux (Eurocrypt 2003)*.

Encrypt-mix-encrypt (CMC/EME/EME*): US Patent Application 20040131182A1 from the University of California.

[3] https://eprint.iacr.org/2002/148

EME

Halevi-Rogaway (CT-RSA 2004)

- Encrypt-mix-encrypt approach.
- Both encryption layers are built from a block cipher using ECB mode.
  - Supports parallelism.
  - Does not support all message lengths.

Halevi (Indocrypt 2004)

- EME*: modifies EME to handle messages of granularity 1.
- Standardised by the IEEE in 2010 (1619.2).

Sarkar (IPL 2008)

- Generalises the lightweight mixing layer; potentially faster mixing functions.

XCB

McGrew-Fluhrer (ePrint 2004, SAC 2007)

- Hash-encrypt-hash construction using a block cipher.
- Use of the counter mode of operation.
- Patented (US Patent 7418100, issued on August 26, 2008 to Cisco).
- XCB version 2 was standardised by the IEEE in 2010 (1619.2).

Attacks

- *Chakraborty, Hernandez-Jimenez and Sarkar (CCDS 2015)*.
- *Bhati, Verbauwhede and Andreeva (ePrint 2024)*.
- *Wang, Mao, Xu, Jing and Wang (ePrint 2024)*.

HCTR

Wang-Feng-Wu (CISC 2005)

- Hash-encrypt-hash construction using a block cipher.
- Use of a novel counter mode of operation.
- Cubic security bound.
  - *Chakraborty-Nandi (FSE 2008)* improved the security bound to quadratic. However, an error in the proof invalidates the bound (*Crowley-Huckleberry-Biggers, ePrint 2023*).
- HCTR's hash function is not AXU (*Kumar, M.Tech thesis 2018*).

Crowley-Huckleberry-Biggers (ePrint 2023)

- Introduced HCTR2.
  - Fixes the problems with HCTR.
  - The structure of HCTR2 is similar to HMCH in *Sarkar (IEEE.IT 2009)*.

HCH

Chakraborty-Sarkar (Indocrypt 2006, IEEE.IT 2008)

- Hash-encrypt-hash using a block cipher.
- A general version of the counter mode used by HCTR.
- Derives the hash key by encrypting the tweak.
- Messages with granularity 1.
- Single key.
- Quadratic security bound.
  - An easy hack: encrypt the IV to the counter ($\Rightarrow$ one extra BC call in the critical path).
  - Encryption of the IV avoided in later constructions.

TET

Halevi (Crypto 2007)

- Instantiates Naor-Reingold's hash-encrypt-hash approach.
  - Designs an invertible block-wise AXU hash function.
  - The encryption layer is ECB mode.
- Engineering overkill: the inverse of the hash function is also block-wise AXU.
  - Requires $\sigma = \sum_{i=1}^{m} \tau^{i-1}$ to be non-zero, where τ is the hash key.
  - Requires σ^{-1}.
  - First point $\Rightarrow$ less key agility; second point $\Rightarrow$ inefficiency.
- Motivation: avoid patent issues.
  - Back to Naor-Reingold's hash-encrypt-hash approach.
  - Avoid counter mode.

HEH

Sarkar (ICISC 2007)

- Hash-encrypt-hash using a block cipher.
- The encryption layer is ECB mode.
- Instantiates the Naor-Reingold approach by designing an invertible block-wise AXU hash function.
- Avoids the inefficiencies of TET.
  - The inverse of the hash function is not block-wise AXU.
- Incorporates other engineering simplifications.
- Fulfilled the patent-avoidance motivation of TET.

Improved HEH and Other Modes

Sarkar (IEEE.IT 2009)

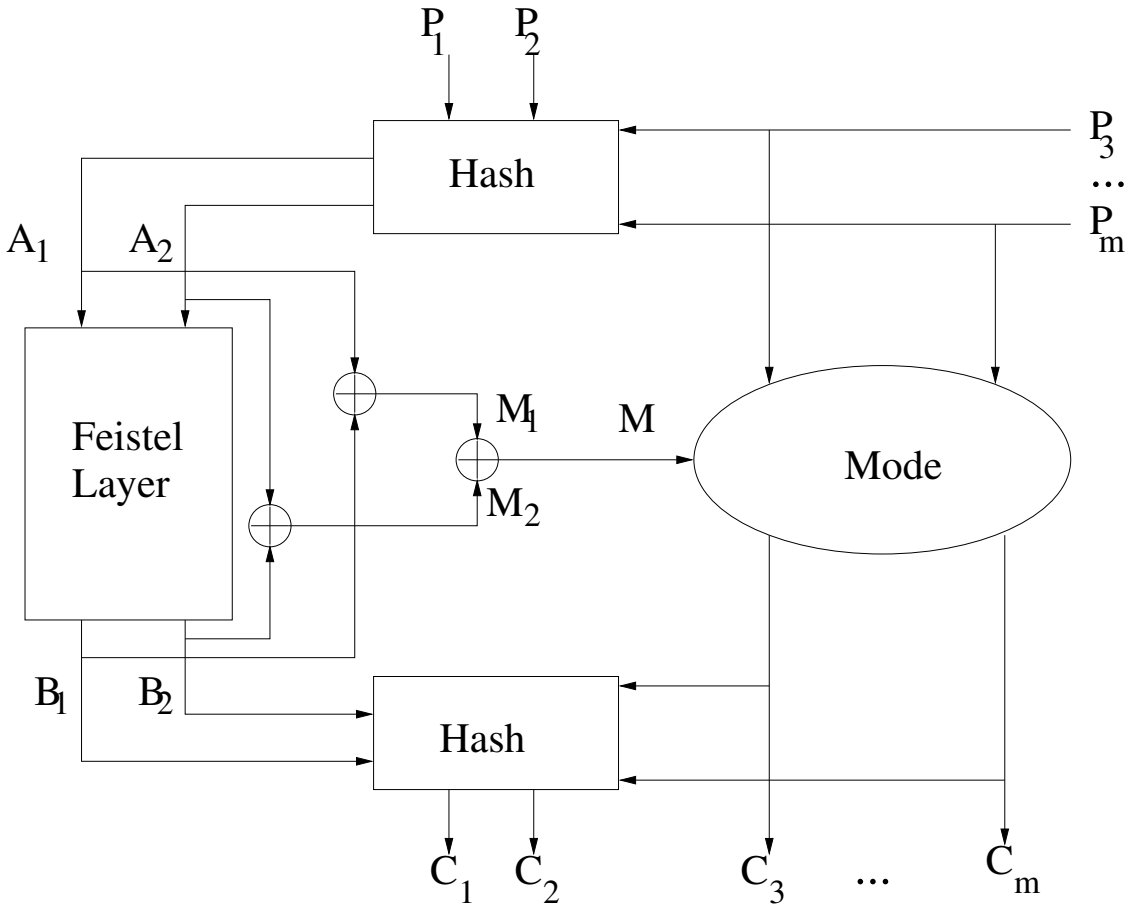
- Hash-encrypt-hash using a block cipher.
- Introduced Bernstein-Rabin-Winograd (BRW) polynomials to the construction of TES.
  - Leads to faster hashing.
- Three options for the encryption layer: ECB, modified counter (MCtr), and OFB.
  - MCtr generalises the counter mode of HCTR.
  - HMCH (MCtr based TES) avoids IV encryption used in HCH.
- Improves upon XCB, HCTR, HCH, TET and HEH.
- For requirement as below, faster schemes are not known till date.
  - Based on AES (or some other n-bit block cipher).
  - n-bit tweak.
  - Message length $\geq n$, granularity 1.

TES from PRF

Sarkar (ePrint 2009, IPL 2011)

- The first work to propose TES constructions using a PRF.
  - Theoretically a PRF is a weaker assumption than an SPRP.
  - PRF choice: encryption/decryption module of a block cipher, both not required; stream cipher with IV.
- Key idea: Construct a Feistel network on the first two blocks and process the rest using hash-encrypt-hash.
  - Limitation: message lengths must be greater than $2n$ bits.
- Two hash layers, and an encryption layer.
  - Encryption layer options: ECB, modified counter, OFB.

TES from PRF (*Sarkar, ePrint 2009, IPL 2011*)



A general template for constructing a TES.

- Two optimised constructions proposed later.
- Several more are possible.

TES from PRF

Sarkar (ePrint 2009, IPL 2011)

- (n, n)-PRF to length preserving SPRP (*Naor-Reingold (JoC 1999)*).
  - Applies a number of 2-round Feistel structures built using 2 (n, n)-PRFs to 2 n-bit blocks at a time.
  - Limited parallelism.
- All TES constructions subsequent to *Naor-Reingold (JoC 1999)* required both encryption and decryption modules of a block cipher.
- No previous schemes based on stream ciphers with IV.

STES

Sarkar (ePrint 2009)

- The first concrete proposal of TES from stream ciphers; follows the general template of Sarkar (2009, 2011) and corrects a bug.

Chakraborty, Mancillas-López, Sarkar (IEEE.TC 2015)

- Optimised version of *Sarkar (ePrint 2009)*.
- Focus: USB memories and SD cards; low hardware footprint.
- Stream ciphers: Mickey, Grain and Trivium.
- AXU hash function: Toeplitz versions of multi-linear hash, pseudo-dot product proposed in *Sarkar (DCC 2013)*.
  - In theory the pseudo-dot product requires about half the number of multiplications required by multi-linear hash.
  - In parallel hardware, the advantage disappears; pseduo-dot product has some advantage in terms of area.
- Extensive FPGA implementation.

FAST

Chakraborty, Ghosh, Mancillas-López, Sarkar (ePrint 2017, AMC 2022)

- TES using encryption module of a block cipher; follows the template of *Sarkar (IPL 2011)*.
- Supports parallelism.
- Specific block cipher: AES.
- Specific AXU hash function: both polynomial and BRW hash over binary extension fields.
- Rich tweak space: binding the encryption of the message to attributes (such as biometric information), e.g. Aadhaar database.
- Software implementation for fixed length messages.

AEZ and FMix

AEZ: *Hoang-Krovetz-Rogaway (Eurocrypt 2015)*;
FMix: *Bhaumik-Nandi (Asiacrypt 2015)*

- Both use only encryption module of block cipher; no hash function.
- AEZ uses three layers, FMix uses two layers.
- AEZ cost per block: about 2-and-half block cipher calls;
  FMix cost per block: 2 block cipher calls.
- AEZ is parallelisable, FMix is sequential.
- Both slower than FAST in either software or hardware (for any reasonable implementation).

Adiantum

Crowley-Biggers (FSE 2018)

- Target: entry level processors.
- Encryption primitives: AES, XChaCha12; Hash: NH, Poly1305.
- HPolyC: a variant built from AES, XChaCha12 and Poly1305.
- Template of *Sarkar (IPL 2011)* is likely to provide simpler and more efficient schemes.
  - A single hash function.
  - A single PRF: encryption module of a block cipher, or a stream cipher.

Docked Double Decker

Dobraunig, Matusiewicz, Mennink, Tereschenko (ePrint 2024)

- Uses only the encryption module of a block cipher.
- Hash-counter-hash strategy.
  - Polyval: hash over binary extension field.
- A 4-round Feistel on first and last n-bit blocks.
  - Message length at least $2n$ bits.
- Tweak is processed using encryption rather than hashing.
- Performance (with n-bit tweaks) is similar to FAST with usual polynomial hash; FAST with BRW is faster.

Generic Enciphering Mode

Bhati, Verbauwhede, Andreeva (ePrint 2024)

- Uses only the encryption module of a block cipher.
- Feistel on the first two n-bit blocks.
  - Input length $\geq 4n$.
- Two variable input length PRFs, and one variable output length PRF.
- Specific instantiations: KohiNoor and DaryaiNoor.

Hardware Implementation

Mancillas-López, Chakraborty and Rodríguez-Henríquez (IEEE.TC 2010)

- FPGA implementations of HCH, HCTR, XCB, EME, HEH, and TET for 512-byte sectors.
  - AES plus usual polynomial hash.

Chakraborty, Mancillas-López, Rodríguez-Henríquez and Sarkar (IEEE.TC 2013)

- FPGA implementations of HEH and HMCH for 512-byte sectors.
  - Strategies: AES plus usual polynomial; AES plus BRW.
  - Major contribution: efficient implementation of BRW polynomials.

Chakraborty, Ghosh, Mancillas-López and Sarkar (ePrint 2024)

- FPGA implementations of FAST, AEZ, XCB and EME2 for 4096-byte sectors.
  - Strategies for FAST: AES plus usual polynomial; AES plus BRW.
  - FAST turns out to be the best choice.

Beyond Birthday Bound

Dutta and Nandi (Indocrypt 2018)

- Tweakable HCTR: Beyond birthday bound security, when each tweak value is not used too often.
- Claim: security bound degrades linearly with max input length.
  - Disproved by *Khairallah (ePrint 2024)*; earlier by *Andreeva-Bhati-Preneel-Vizár (FSE 2021)*.

Dobraunig, Matusiewicz, Mennink, Tereschenko (ePrint 2024)

- A variant of docked double decker mode achieving beyond birthday bound security, when each tweak is not used too often.

Bhati, Verbauwhede, Andreeva (ePrint 2024)

- Provides n-bit security.

. . .

Other Aspects

Construction of TES from public permutations

- *Chakraborty-Dutta-Kundu (AMC 2023)*.
- *Eliasi-Ghosh-Daemen (SCN 2024)*.

Security of TES against quantum computers

- *Ghosh-Sarkar (ePrint 2019, DCC 2021)*.
- *Rahman-Paul (IEEE.QE 2020)*.

. . .

Thank you for your kind attention!