

A BBB Secure Accordion Mode from HCTR

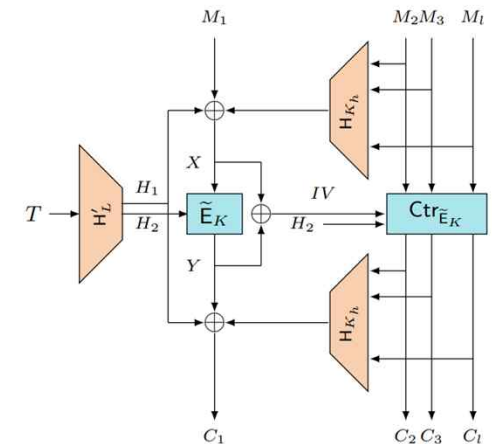
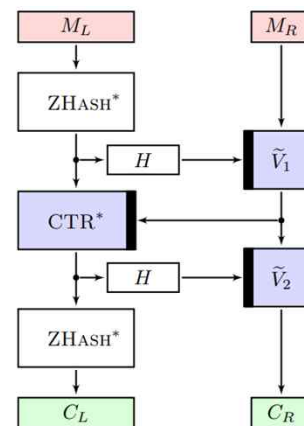
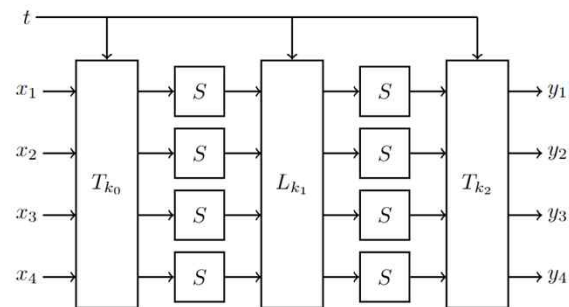
2024.06.19

Byeonghak Lee

SAMSUNG SDS

Accordion Mode

- A length preserving tweakable encryption $\simeq$ tweakable wide block cipher
 - Security Goal: Variable Input Length Strong Tweakable Pseudorandom Permutation (VILSTPRP)
- There are only few accordion modes with **beyond-birthday bound security**
 - CTET+
 - ZCZ
 - Tweakable HCTR

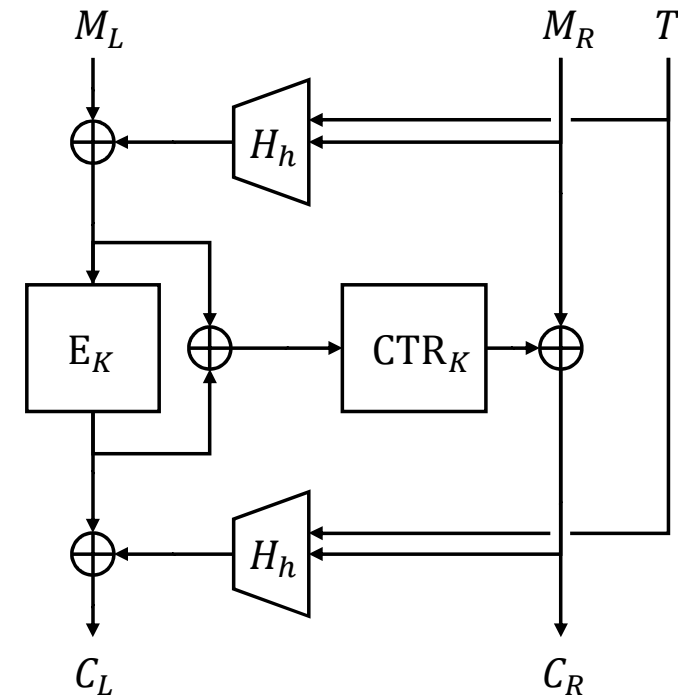


Goal

- Block Cipher based Accordion Mode
- Provide beyond-birthday bound security
 - Currently, only CTET+ is the option for BBB-security
- Support arbitrary length message and tweak
 - required to apply generic AE conversion
- Minimize the number of block cipher calls

Starting Point - HCTR

- HCTR
 - Hash-Counter-Hash style
 - BC based, $n/2$ -bit security
 - 1 BC call + 2 Field Mults per block
- Modification: use $2n$ -bit state size
 - $2n$ -bit universal hash $\leftarrow$ use $GF(2^{2n})$ or $GF(2^n)^2$
 - $2n$ -bit E_K $\leftarrow$ use BBB-secure accordion mode (e.g. CTET+)
 - **BBB-secure variant of CTR_K** from block cipher?



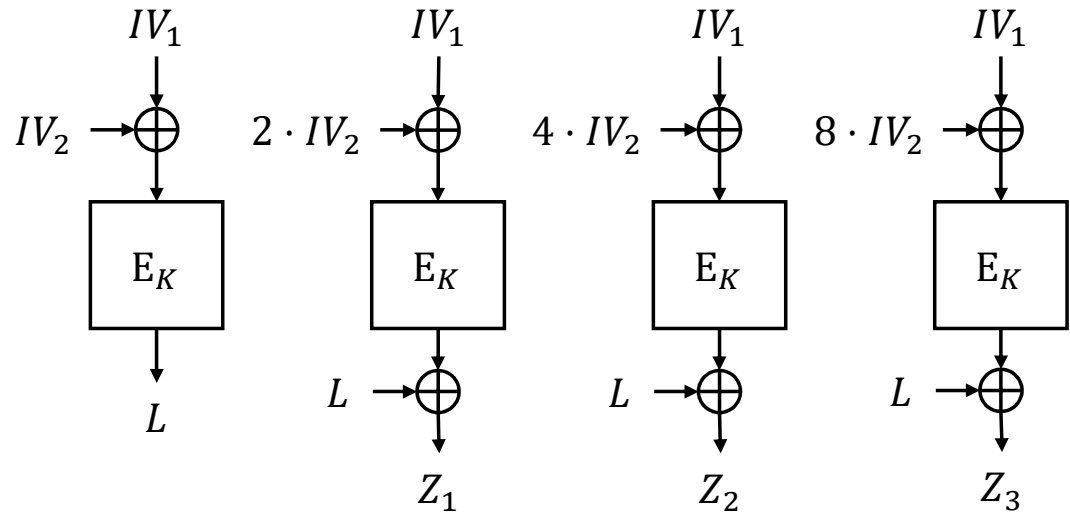
mCTR: BBB-secure PRF from PRP

- masked CTR
 - CTR mode with additional input/output masking
 - adapted from PRNG in synthetic-counter with masking (SCM) AE mode
 - $\text{mCTR}_K(IV_1, IV_2)[i] = E_K(IV_1 \oplus IV_2) \oplus E_K(2^i \cdot IV_1 \oplus IV_2)$
 - provide $2n/3$ -bit security

Lemma (Security of mCTR)

If IV_1 and IV_2 are chosen uniformly at random, one get

$$\text{Adv}_{\text{mCTR}}^{\text{PRF}}(q, \sigma, l) \leq \min \left\{ \frac{72q l^2}{2^n}, \frac{6\sigma^3 l}{2^{2n}} + \frac{12\sigma l}{2^n} \right\} + \frac{3q^4}{2^{3n}}.$$



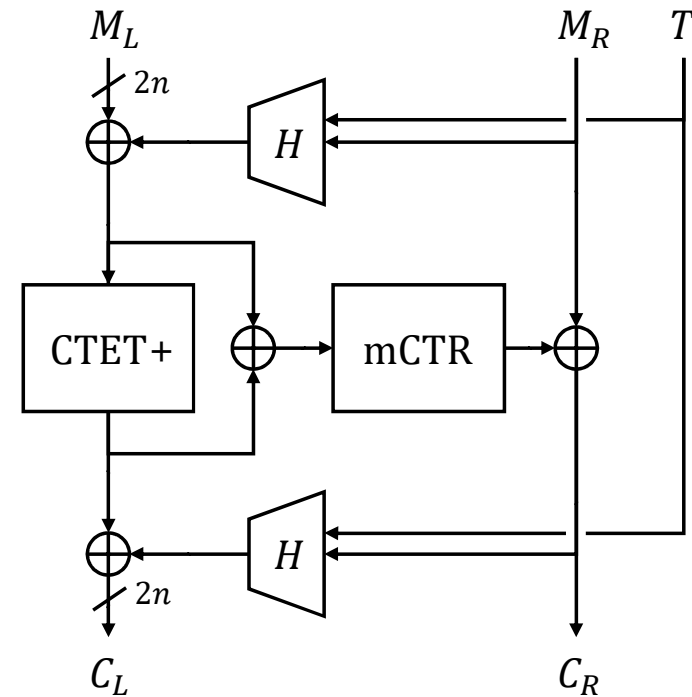
Our Proposal

- Double-block HCTR (DbHCTR)
 - BBB-secure variant of HCTR using $2n$ -bit state size
 - Message length should be at least $2n$ -bit
 - H is concatenation of two n -bit polynomial hashes
 - 1 BC call + 4 Field Mults per block
 - Support arbitrary length tweak

Lemma (Security of DbHCTR)

Let H is ϵ -almost xor universal hash with $2n$ -bit output. Then,

$$\begin{aligned} & \text{Adv}_{\text{DbHCTR}}^{\text{STPRP}}(q, \sigma, l) \\ & \leq \text{Adv}_{\text{CTET}+}^{\text{PRP}}(q) + \text{Adv}_{\text{mCTR}}^{\text{iPRF}}(q, \sigma, l) + O\left(q^2\epsilon + \frac{q^2}{2^{2n}}\right) \end{aligned}$$



Comparison

Scheme	Prim.	Security	#Ops per block		Arbitrary length		Ref
			(T)BC	FMult	Msg	Tweak	
EME*	BC	$n/2$	2	-	O	O	[Hal04]
HCTR	BC	$n/2$	1	2	O	O	[WFW05]
HEH*	BC	$n/2$	1	2	O	O	[Sar09]
Tweakable HCTR	TBC	$n/2 \sim n^{2)}$	1	2	O	O	[DN18]
ZCZ	TBC	n	1.5	-	O	X	[BLN18]
(Decked-)Double-decker	Deck ¹⁾	$n/2 \sim n^{2)}$	-	-	O	O	[GDM20]
CTET+	BC	$2n/3$	2	2	X	X	[CELL+21]
DbHCTR	BC	$2n/3$	1	4	O	O	Ours

1) Doubly-extendable cryptographic keyed functions (arbitrary-length input and output).

2) Depends on tweak repetition.

Conclusion and Discussion

- DbHCTR is the first block cipher based accordion mode that enjoys
 - $2n/3$ -bit security
 - arbitrary length tweak inputs
 - 1 BC call per message block
- Limitations and further topics
 - DbHCTR needs large amount of subkeys
 - $2n$ -bit for universal hash, $6n$ -bit for CTET+, n -bit for mCTR
 - Key-committing security is unknown when converting to AE
 - Its multi-user security is unknown

FAQ ?

Ref

- [Hal04] Halevi, S. (2004). EME*: Extending EME to Handle Arbitrary-Length Messages with Associated Data.
- [WFW05] Wang, P., Feng, D., Wu, W. (2005). HCTR: A Variable-Input-Length Enciphering Mode.
- [Sar09] Sarkar, P. (2009). Efficient Tweakable Enciphering Schemes From (Block-Wise) Universal Hash Functions.
- [BLN18] Bhaumik, R., List, E., Nandi, M. (2018). ZCZ – Achieving n -bit SPRP Security with a Minimal Number of Tweakable-Block-Cipher Calls.
- [DN18] Dutta, A., Nandi, M. (2018). Tweakable HCTR: A BBB Secure Tweakable Enciphering Scheme.
- [GDM20] Gunesing, A., Daemen, J., & Mennink, B. (2020). Deck-Based Wide Block Cipher Modes and an Exposition of the Blinded Keyed Hashing Model.
- [CELL+21] Cogliati, B., Ethan, J., Lallemand, V., Lee, B., Lee, J., & Minier, M. (2021). CTET+: A Beyond-Birthday-Bound Secure Tweakable Enciphering Scheme Using a Single Pseudorandom Permutation.