Accordion mode based on Hash-Encrypt-Hash

Hieu Nguyen Duy[2], Pablo García Fernández[2], Aleksei Udovenko[2], Alex Biryukov[1,2]

FSTM, University of Luxembourg
SnT, University of Luxembourg
first-name.last-name@uni.lu

June 21, 2024

Outline

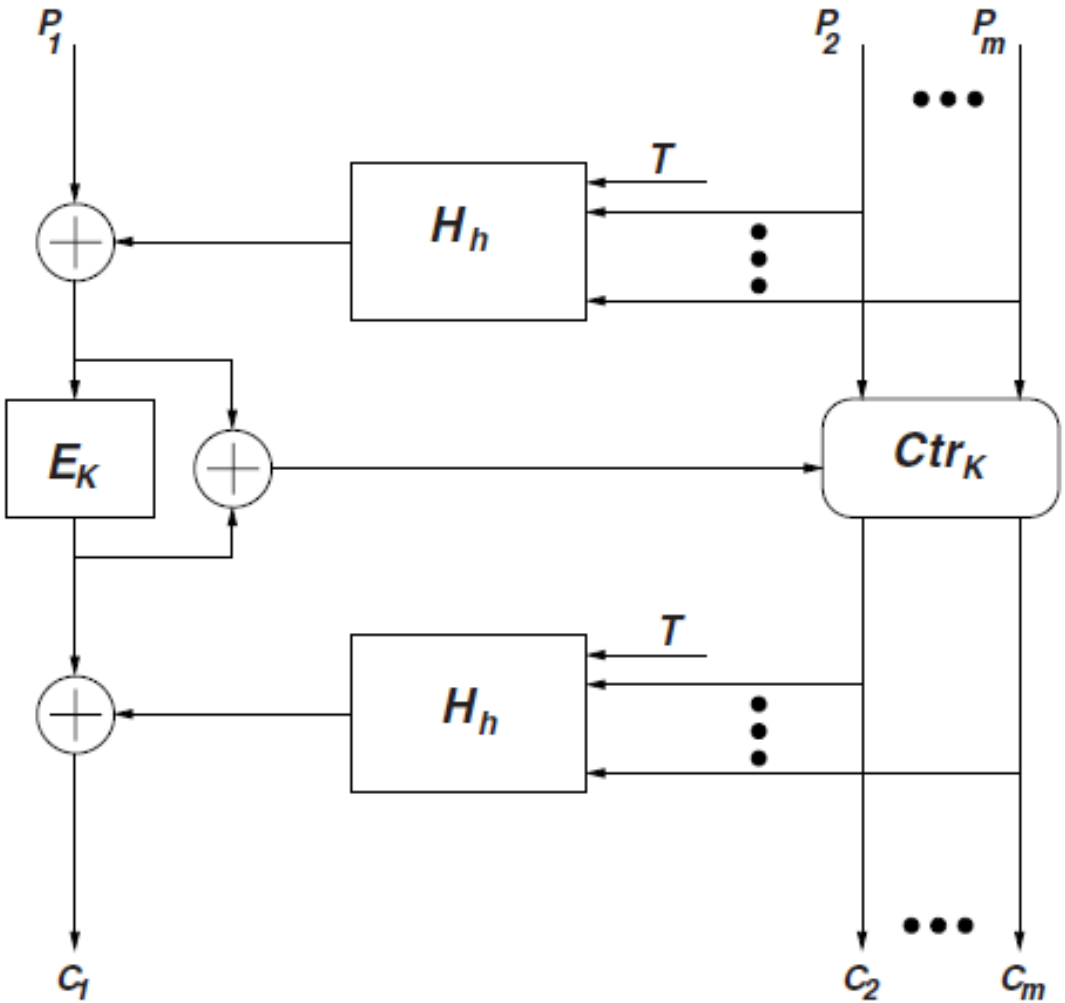
Introduction

- Tweakable block ciphers are block ciphers that include a tweak (public input) as one of their parameters
- Accordion mode: tweakable block cipher mode, variable input length strong pseudorandom permutation (VIL-SPRP)
- Advantages over modes in SP 800-38 series (AES-GCM), (ex. nonce-misuse resistance, support for short tags, nonce hiding, and key commitment)

Introduction

- Derived functions and Applications: Encrypting with associated data (AEAD); Tweakable Encryption; Deterministic Authenticated Encryption (DAE)
- We survey SOTA and study a method based on the Hash-Encrypt-Hash paradigm, inspired by HCTR

HCTR



Survey of VIL Tweakable Block Ciphers, no BBB security

Name	Year	Security	Efficiency
EME	2003	$7q^2a^2/2^n$	$(2m+2)\mathrm{BC}$
CMC	2003	$7q^2a^2/2^n$	$(2m+1)\mathrm{BC}$
XCB	2004	$8q^2a^2/2^n$	$(m+1)\mathrm{BC}+2\mathrm{HF}$
OCB1	2004	$9.5q^2a^2/2^n + 2^{n-\tau}/2^n$	$(m+2)\mathrm{BC}$
HCTR	2005	$q^3a^2/2^n$	$m\mathrm{BC}+2\mathrm{HF}$
HCH	2006	$7q^2a^2/2^n$	$(m+3)\mathrm{BC}+2\mathrm{HF}$
HSE	2007	$5q^2a^2/2^n$	$m\mathrm{BC}+2\mathrm{HF}$
Adiantum	2018	$q^2a/2^{116}$	$\mathrm{BC}+\mathrm{SC}$ (output: $m-1$ blocks)$+2\mathrm{HF}$
THCTR	2018	$2qa/2^n + 2qa^2/2^{n+s^*}$	$m\mathrm{TBC}+3\mathrm{HF}$
Deck-based	2019	$q^2/2^{127}$	$2\mathrm{VIL}-\mathrm{SC}+2\mathrm{HF}$
HCTR2	2021	$1.5q^2a^2/2^n$	$m\mathrm{BC}+2\mathrm{HF}$
TIE-plus	2022	$q^2a^2/2^n\ell + q^2a^2(1-1/\ell)/2^n + 2q^2a/2^n$	$2m\mathrm{MF}+\mathrm{mPERM}$
ACCOR-S	2024	$q^2a^2/2^{129}$	$m\mathrm{BC}+2\mathrm{HF}$

[1] m: number of plaintext blocks

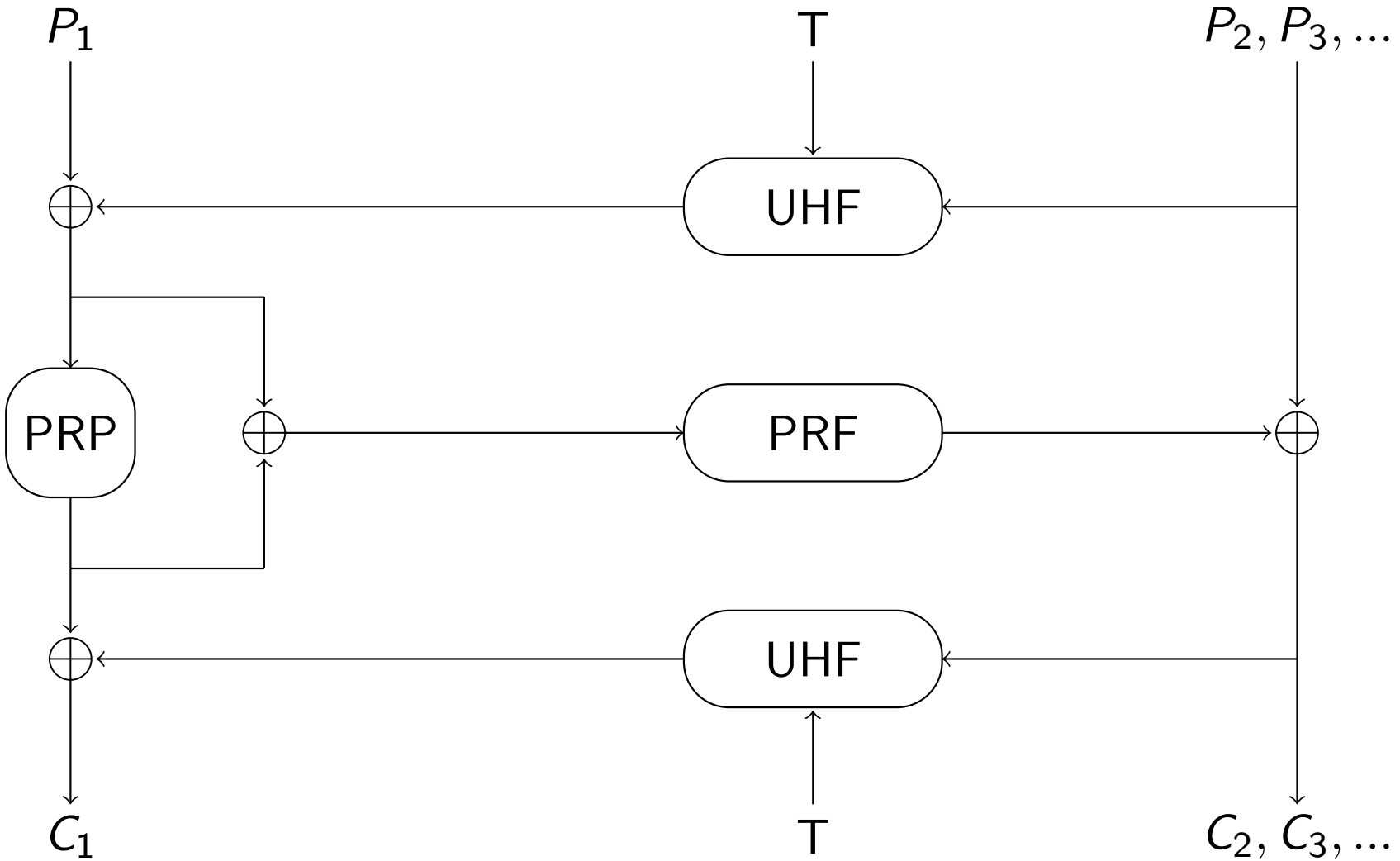
Survey of VIL Tweakable Block Ciphers, BBB security

Name	Year	Security	Efficiency
LBC1	2011	$3q^2a^2/2^{2n}$	$(m-1)(n,n)-\mathrm{TBC}+4\mathrm{HF}$
TCT_2	2013	$qa^2/2^n + 6a^3q^3/(2^{2n-2}-a^3q^3) + 1296q^3/(2^{2n-2}-216q^3)$	$(6m+6)\mathrm{BC}+(7\mathrm{m}+7)\mathrm{HF}$
ZMAC	2017	$2.5q^2a^2/2^{n+min\{s,n\}} + 4q/2^n$	$(6+m)\mathrm{TBC}$
ZCZ	2018	$3q^2a^2/2^{2n+1}$	$(2m+6+m/n)\mathrm{TBC}+4\mathrm{HF}$
ACCOR-L	2024	$qa\ell/2^{128}$	$m\mathrm{BC}+2\mathrm{HF}$

[2]

[2] ℓ: number of blocks before changing key in the CTR. Ex., $\ell = 16$

ACCOR-HEH



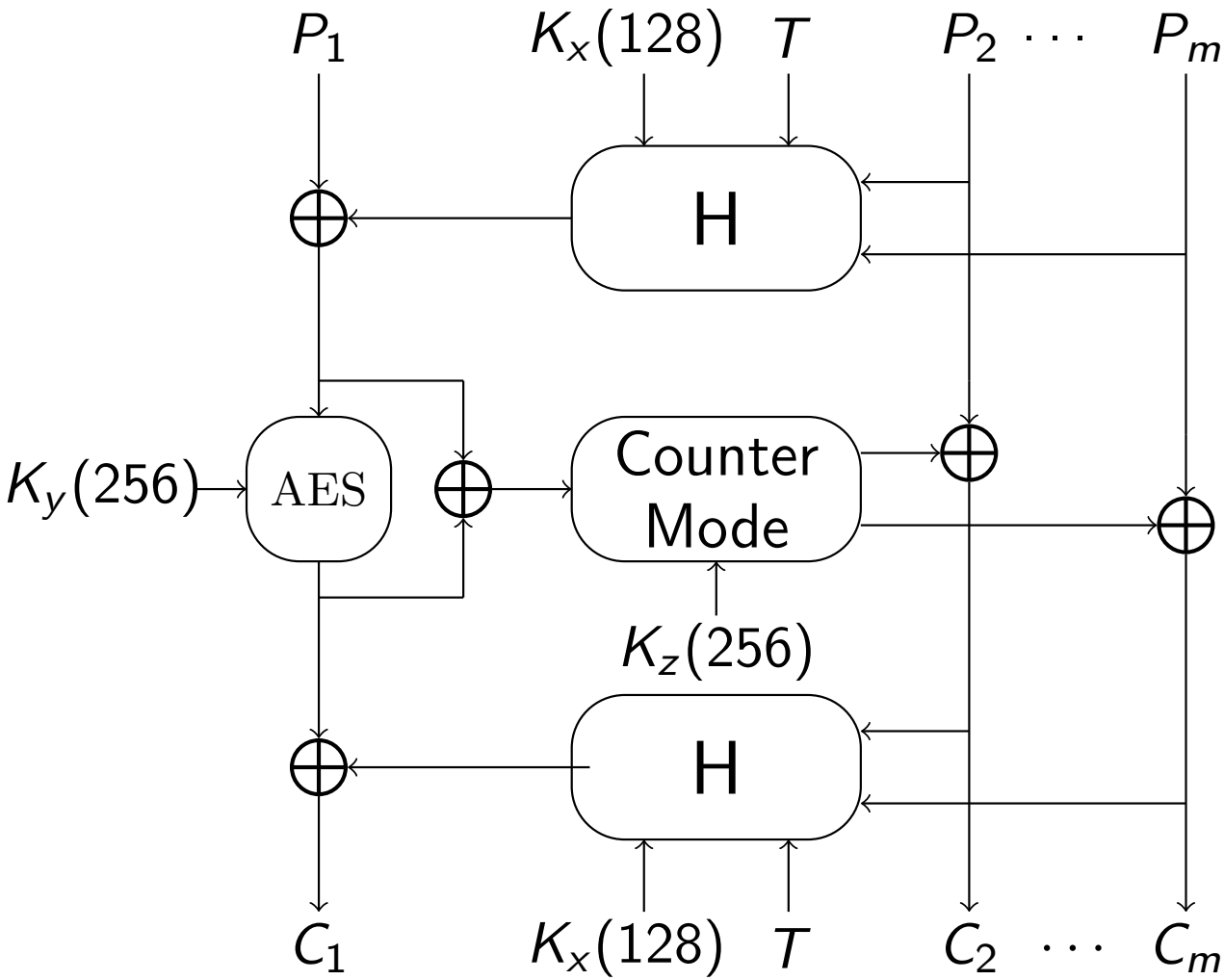
Key schedule

INPUT: 256-bit master key K_I
OUTPUT: 128-bit key K_x, 256-bit key K_y, 256-bit key K_z

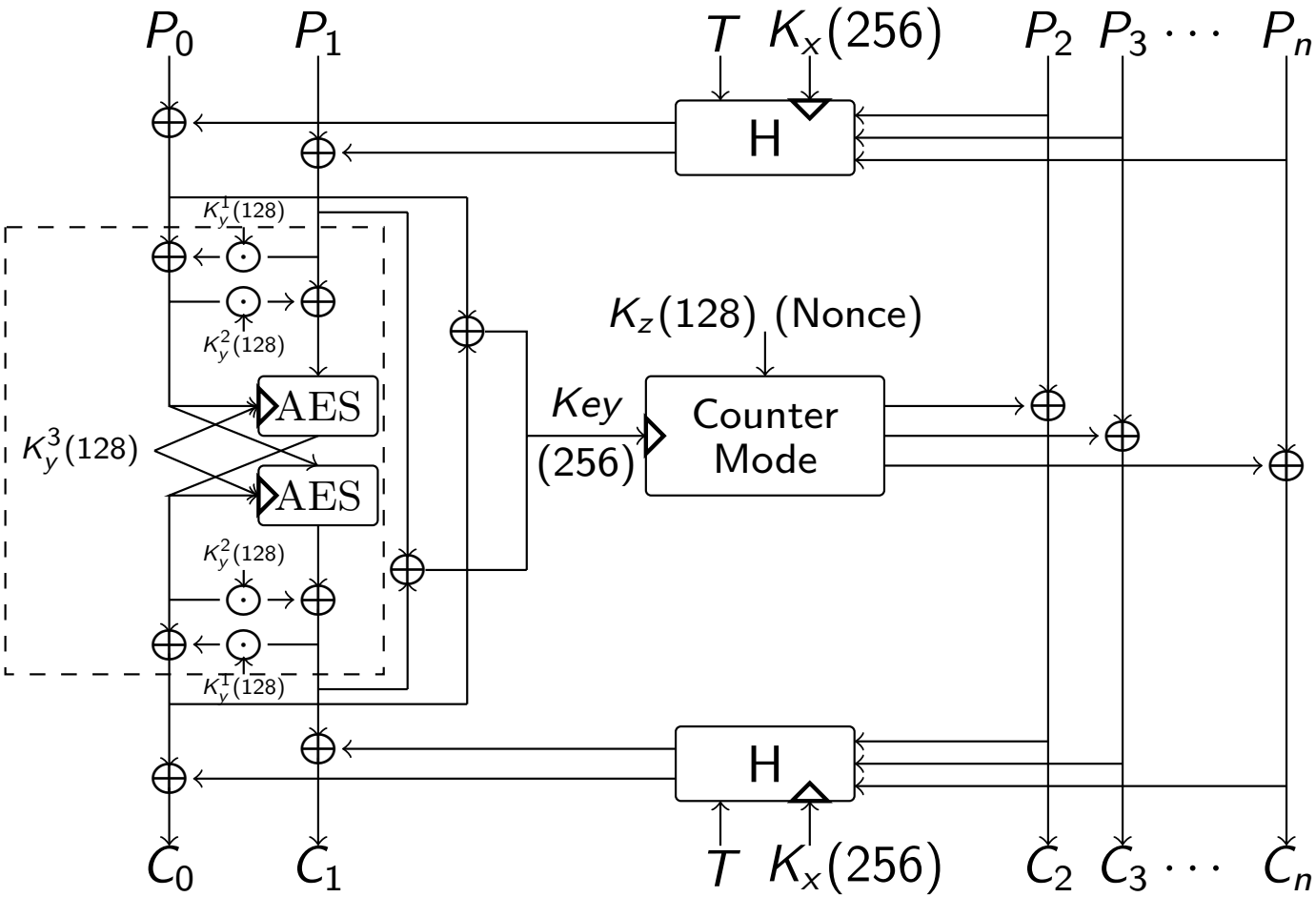
1. $$K_x = \mathrm{AES}^{\mathrm{E}}_{256}(\mathrm{K_I}, 1)\ (K_x \neq 0)$$
2. $$K_y = \mathrm{AES}^{\mathrm{E}}_{256}(\mathrm{K_I}, 2)||\mathrm{AES}^{\mathrm{E}}_{256}(\mathrm{K_I}, 3)$$
3. $$K_z = \mathrm{AES}^{\mathrm{E}}_{256}(\mathrm{K_I}, 4)||\mathrm{AES}^{\mathrm{E}}_{256}(\mathrm{K_I}, 5)$$

There is a variant where hash of the tweak is used in the key-derivation function.

ACCOR-S

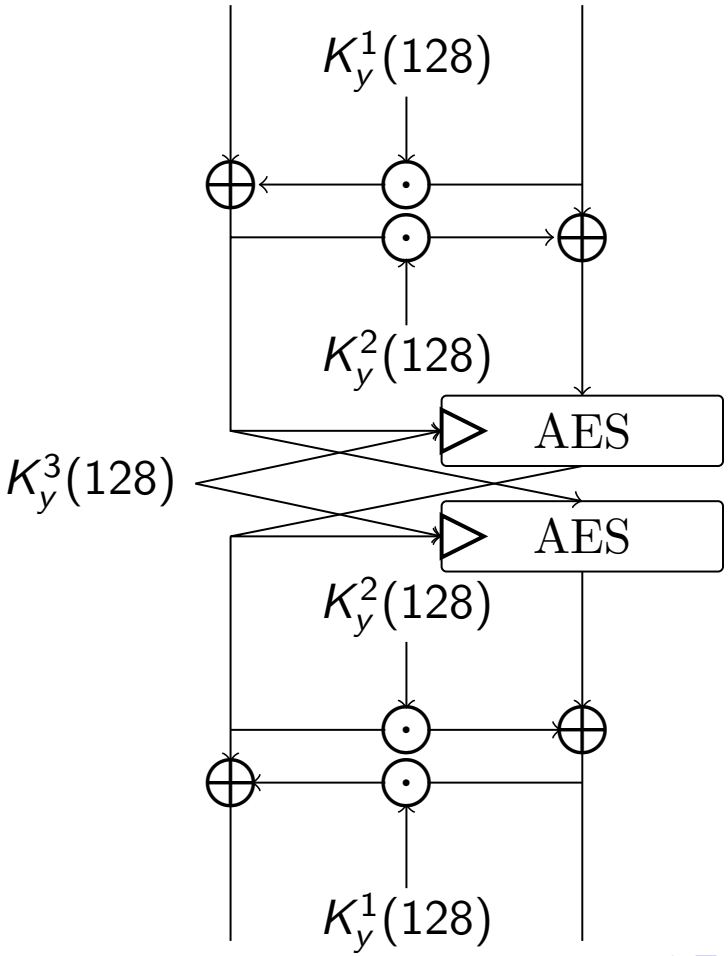

P_1
$K_x(128)$
T
P_2 $\cdots$ P_m
H
$K_y(256)$
AES
Counter Mode
$K_z(256)$
H
C_1
$K_x(128)$
T
C_2 $\cdots$ C_m

ACCOR-L


P_0
P_1
T
$K_x(256)$
P_2
$P_3 \cdots$
P_n
H
$K_y^1(128)$
$K_y^2(128)$
$K_z(128)$ (Nonce)
AES
$K_y^3(128)$
AES
Key
(256)
Counter Mode
$K_y^2(128)$
$K_y^1(128)$
H
C_0
C_1
T
$K_x(256)$
C_2
$C_3 \cdots$
C_n

ACCOR-L (256-bit SPRP, 384-bits of subkeys)

Figure: Two AES-based Feistel-like rounds, needs further analysis, especially against the related key (RK) attacks. Easy to add more rounds, will be amortised over long messages.



Main additional properties

Property	ACCOR-HEH	ACCOR-S	ACCOR-L
TS	UL	UL	UL
Min ML	1 block	1 block	2 blocks
Max ML	UL	2^{20} blocks	2^{30} blocks
MKS	Yes	Yes	Yes
CtxCom	Yes[3]	Yes[3]	Yes[3]

- TS: Tweak Size; UL unlimited
- ML: Message Length
- MKS: Multi-key Security
- CtxCom: Context Commitment Security

[3] Variant where hash of the tweak is used in the key-derivation function

Comparison

Construction	Message Length (a)	Number of queries (q)	Total data processed (σ)	Advantage
ACCOR-S	34 MB	$24 \cdot 2^{20}$	2^{45}B	2^{-40}
ACCOR-L	34 GB	2^{54}	2^{88}B	

$$\sigma = qa$$

ACCOR-S: $q^2a^2/2^{129}$

ACCOR-L: $qa/2^{124}$