>>> Tweakable HCTR: A BBB Secure Tweakable Enciphering Scheme

Name: Avijit Dutta and Mridul Nandi (Indian Statistical Institute, Kolkata, India.)

Date: December 10, 2018

INDOCRYPT, 2018

>>> Outline

* Introduction

* HCTR Construction

* Tweakable HCTR

* Security Proof

>>> Tweakable Enciphering Scheme

TES is a triplet of three algorithms: $\mathcal{I} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$.

>>> Tweakable Enciphering Scheme

TES is a triplet of three algorithms: $\mathcal{I} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$.

* Alice and Bob shares a secret key $K \leftarrow \mathsf{KGen}(1^n)$.
* Alice generates the ciphertext $C \leftarrow \mathsf{Enc}(K, M, T)$ and sends C to Bob.
* Bob decrypts the ciphertext C to $M \leftarrow \mathsf{Dec}(K, C, T)$.

>>> Tweakable Enciphering Scheme

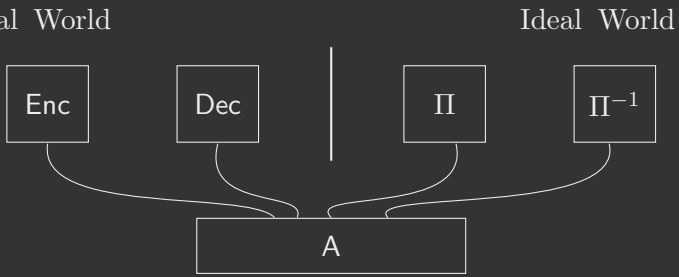
TES is a triplet of three algorithms: $\mathcal{I} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$.

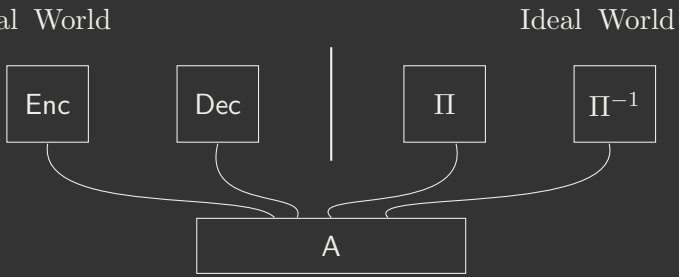
* Alice and Bob shares a secret key $K \leftarrow \mathsf{KGen}(1^n)$.
* Alice generates the ciphertext $C \leftarrow \mathsf{Enc}(K, M, T)$ and sends C to Bob.
* Bob decrypts the ciphertext C to $M \leftarrow \mathsf{Dec}(K, C, T)$.

Correctness Condition

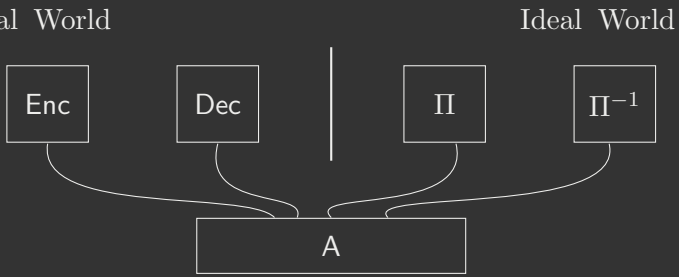
$$\forall K, M, T: \quad \mathsf{Dec}(K, \mathsf{Enc}(K, M, T), T) = M\,.$$

>>> Security Game of TES





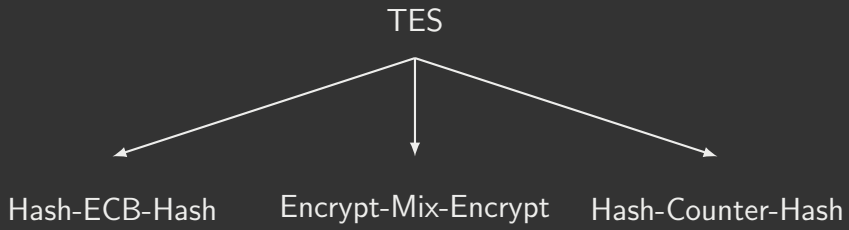
$$\mathbf{Adv}^{\mathrm{tes}}_{\mathcal{I}}(\mathsf{A}) = |\ \Pr[\mathsf{A}^{\mathcal{I}.\mathsf{Enc},\mathcal{I},\mathsf{Dec}} = 1] - \Pr[\mathsf{A}^{\Pi,\Pi^{-1}} = 1]\ |.$$



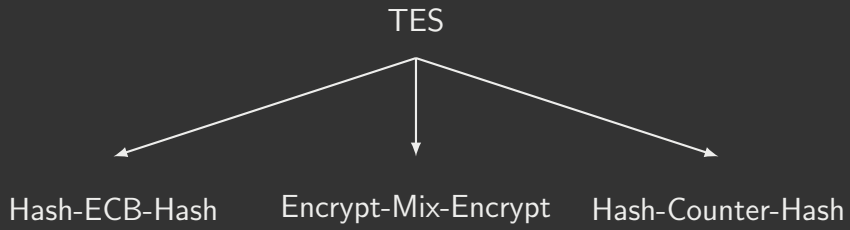
$$\mathbf{Adv}^{\mathrm{tes}}_{\mathcal{I}}(\mathsf{A}) = |\ \Pr[\mathsf{A}^{\mathcal{I}.\mathsf{Enc},\mathcal{I},\mathsf{Dec}} = 1] - \Pr[\mathsf{A}^{\Pi,\Pi^{-1}} = 1]\ |.$$

$\mathcal{I}$ is secure against all such computationally bounded adversary A, if the advantage is small.

>>> Types of TES

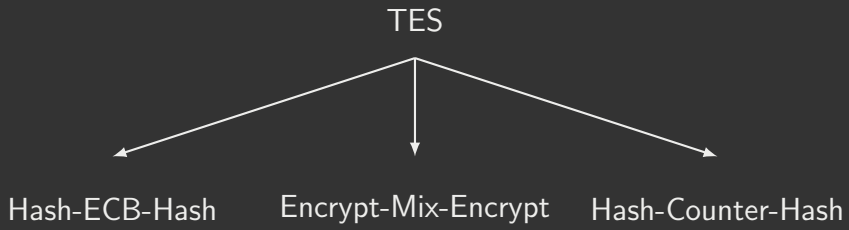


>>> Types of TES



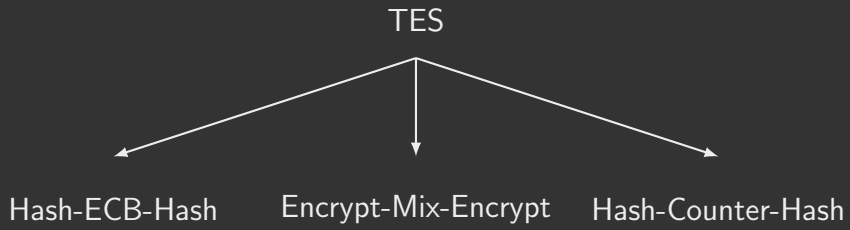
* I. Hash-ECB-Hash: PEP, TET, HEH.

>>> Types of TES



* I. Hash-ECB-Hash: PEP, TET, HEH.
* II. Encypt-Mix-Encrypt: CMC, EME, EME*, FMix.

>>> Types of TES



* I. Hash-ECB-Hash: PEP, TET, HEH.
* II. Encypt-Mix-Encrypt: CMC, EME, EME*, FMix.
* III. Hash-Counter-Hash: XCB, HCTR, HCH, FAST.

>>> Comparison Chart for various TES

Type	Constructions	Prim. Calls	Mult. Calls	Bound
I	PEP	$(\ell+5)$	$(4\ell-6)$	$\sigma^2/2^n$
	TET	$(\ell+2)$	$(\ell-1)$	$\sigma^2/2^n$
	HEH	$(\ell+2)$	$2(\ell-1)$	$\sigma^2/2^n$
II	CMC	$(2\ell+1)$	0	$\sigma^2/2^n$
	EME	$(2\ell+2)$	0	$\sigma^2/2^n$
	EME*	$(2\ell+\ell/n+1)$	0	$\sigma^2/2^n$
	FMix	$(2\ell+1)$	0	$q^2+\ell^2/2^n$
III	XCB	$(\ell+6)$	$2(\ell+1)$	-
	HCTR	ℓ	$2(\ell-1)$	$\sigma^2/2^n$
	HCH	$(\ell+3)$	$2(\ell-2)$	$\sigma^2/2^n$
	FAST ($\star$)	ℓ	$2(\ell-3)$	$\sigma^2/2^n$

>>> Comparison Chart for various TES

Type	Constructions	Prim. Calls	Mult. Calls	Bound
I	PEP	$(\ell+5)$	$(4\ell-6)$	$\sigma^2/2^n$
	TET	$(\ell+2)$	$(\ell-1)$	$\sigma^2/2^n$
	HEH	$(\ell+2)$	$2(\ell-1)$	$\sigma^2/2^n$
II	CMC	$(2\ell+1)$	0	$\sigma^2/2^n$
	EME	$(2\ell+2)$	0	$\sigma^2/2^n$
	EME*	$(2\ell+\ell/n+1)$	0	$\sigma^2/2^n$
	FMix	$(2\ell+1)$	0	$q^2+\ell^2/2^n$
III	XCB	$(\ell+6)$	$2(\ell+1)$	-
	HCTR	ℓ	$2(\ell-1)$	$\sigma^2/2^n$
	HCH	$(\ell+3)$	$2(\ell-2)$	$\sigma^2/2^n$
	FAST ($\star$)	ℓ	$2(\ell-3)$	$\sigma^2/2^n$

$\star$ FAST is a PRF based TES.

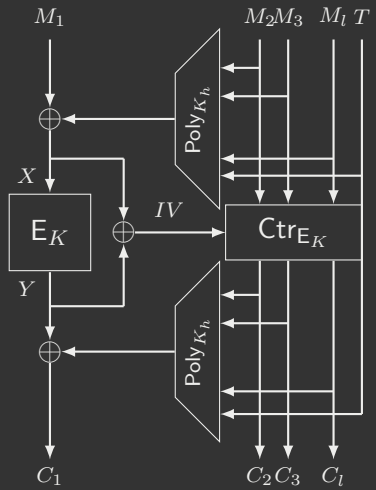
>>> Key Points

* Only CMC, EME and EME* are based only on block ciphers.
* Field Multiplication for other constructions.
* HCTR is the efficient one [1].
* Secured upto the birthday bound.

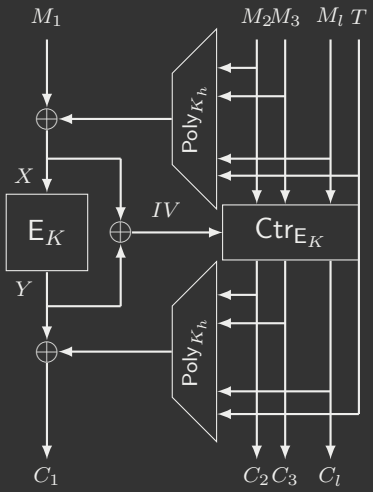
[1] Lopez et al., INDOCRYPT 07.

HCTR Construction

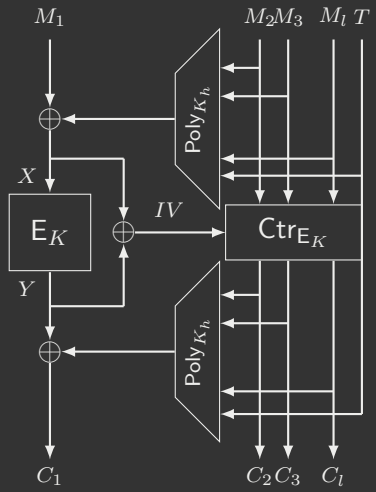
* Most efficient candidate.



* Most efficient candidate.
* Sec. bound $\sigma^3/2^n$ [Wang et al.].

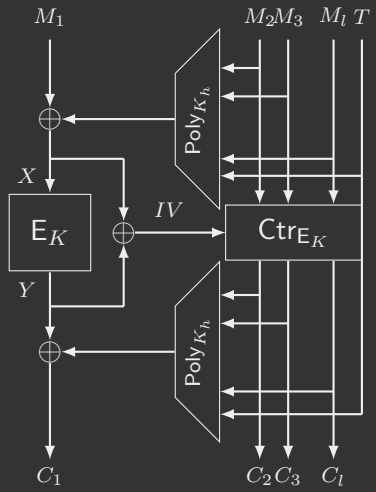


* Most efficient candidate.
* Sec. bound $\sigma^3/2^n$ [Wang et al.].
* Improved bound $\sigma^2/2^n$ [Chakraborty and Nandi, FSE 08].

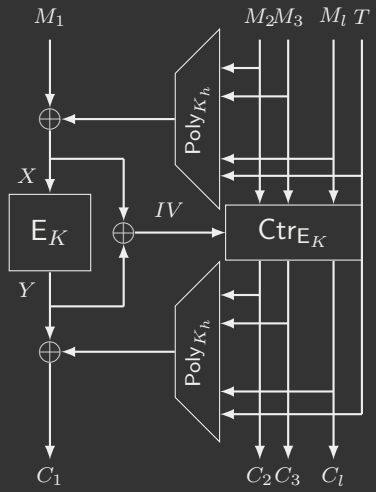


>>> HCTR [Wang et al., CISC 05]

* Most efficient candidate.
* Sec. bound $\sigma^3/2^n$ [Wang et al.].
* Improved bound $\sigma^2/2^n$ [Chakraborty and Nandi, FSE 08].
* The bound is tight (due to hash collision).

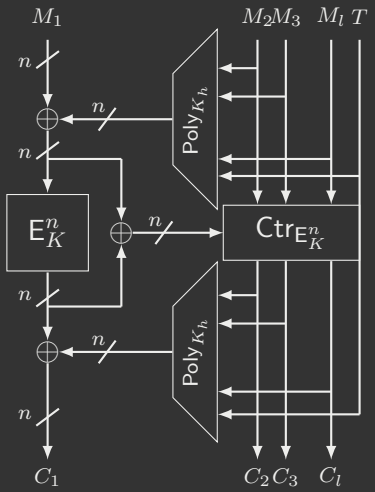


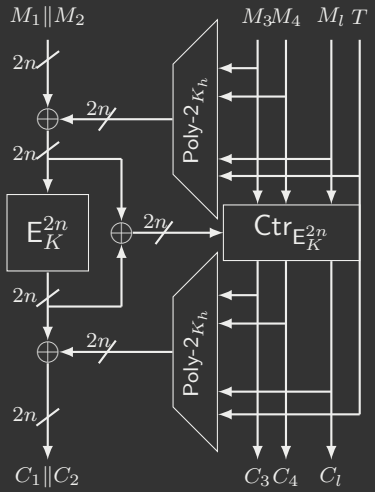
* Most efficient candidate.
* Sec. bound $\sigma^3/2^n$ [Wang et al.].
* Improved bound $\sigma^2/2^n$ [Chakraborty and Nandi, FSE 08].
* The bound is tight (due to hash collision).



Can we construct a BBB secure variant of HCTR ?

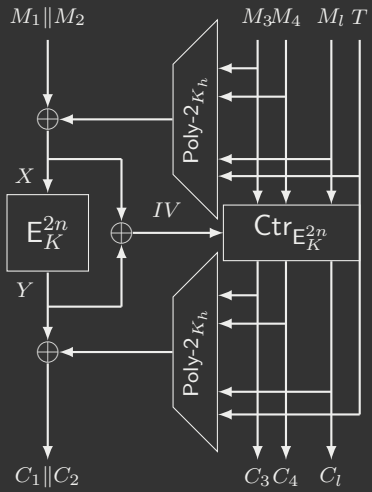
>>> Naive Approach to construct BBB Secure variant of HCTR





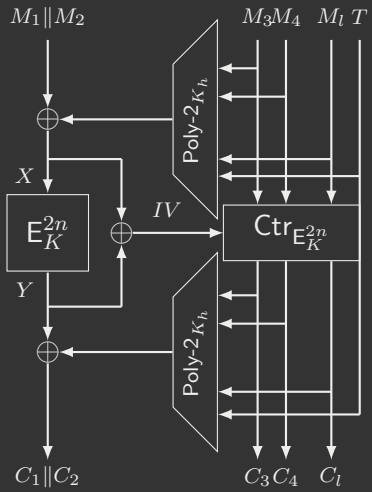
>>> Drawback of the Scheme

* 2 * field mutiplications.



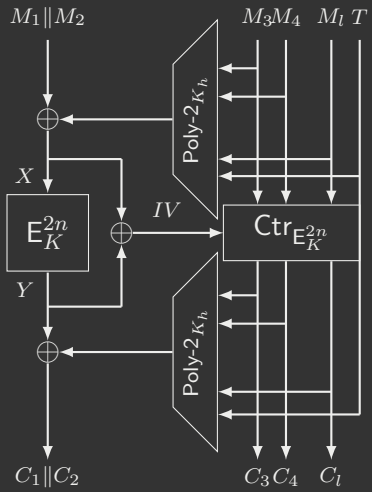
>>> Drawback of the Scheme

* 2 * field mutiplications.
* 2 * state size.



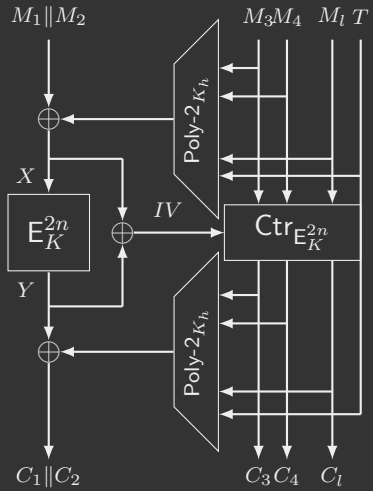
>>> Drawback of the Scheme

* 2 * field mutiplications.
* 2 * state size.
* Optimally secure SPRP requires at least 6 BC calls.



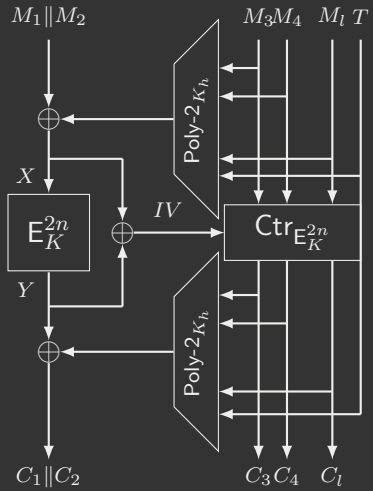
>>> Drawback of the Scheme

* 2 * field mutiplications.
* 2 * state size.
* Optimally secure SPRP requires at least 6 BC calls.
* Ctr mode requires 2 BC calls per block of message.



>>> Drawback of the Scheme

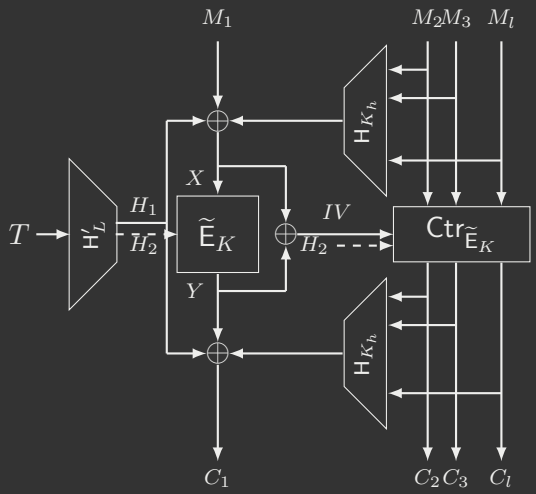
* 2 * field mutiplications.
* 2 * state size.
* Optimally secure SPRP requires at least 6 BC calls.
* Ctr mode requires 2 BC calls per block of message.



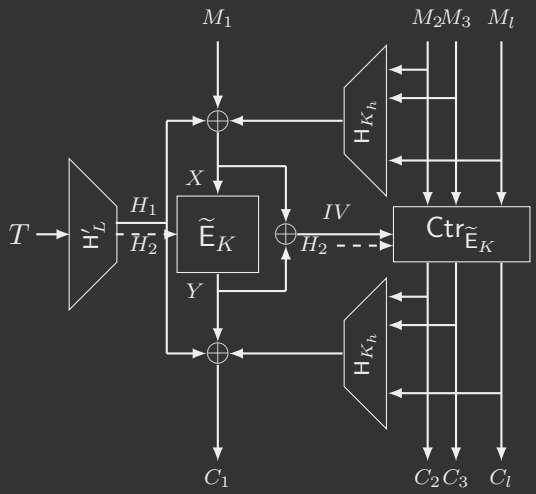
Can we make the scheme BBB secure without increasing state size?

Tweakable HCTR

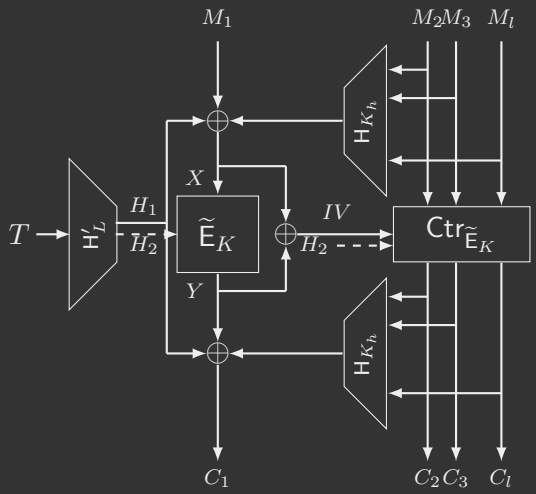
* BC $\rightarrow$ m-bit TBC.



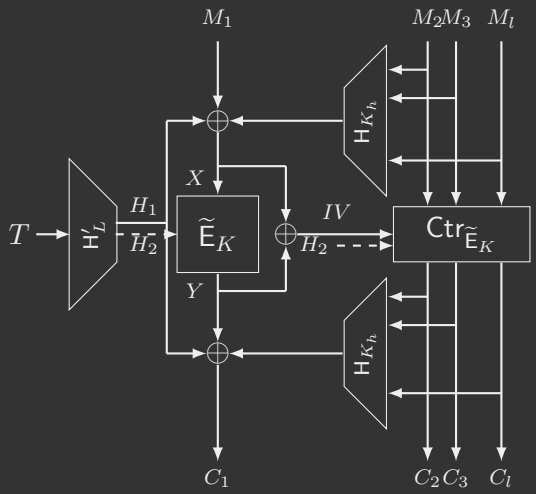
* BC $\rightarrow$ m-bit TBC.
* $\mathsf{H}'_L(T)$ for processing variable length tweak.



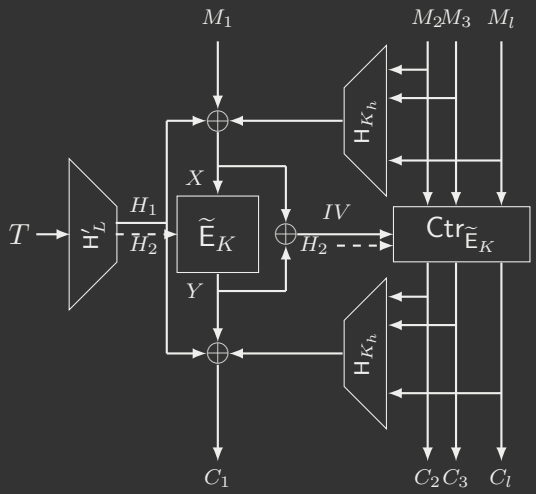
* BC $\rightarrow$ m-bit TBC.
* $\mathsf{H}'_L(T)$ for processing variable length tweak.
* First n bit of $\mathsf{H}'_L(T)$ is xor-ed with the state.



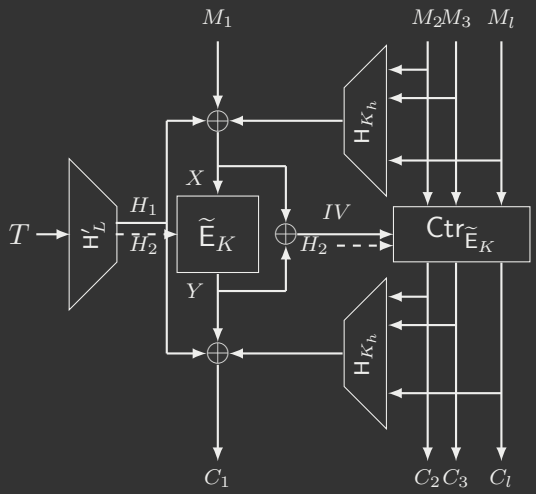
* BC $\rightarrow$ m-bit TBC.
* $\mathsf{H}'_L(T)$ for processing variable length tweak.
* First n bit of $\mathsf{H}'_L(T)$ is xor-ed with the state.
* Remaining m bit of $\mathsf{H}'_L(T)$ is the tweak to the underlying TBC.



* BC $\rightarrow$ m-bit TBC.
* $\mathsf{H}'_L(T)$ for processing variable length tweak.
* First n bit of $\mathsf{H}'_L(T)$ is xor-ed with the state.
* Remaining m bit of $\mathsf{H}'_L(T)$ is the tweak to the underlying TBC.
* n bit state.

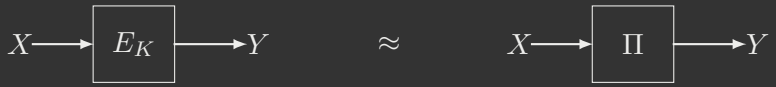


* BC $\rightarrow$ m-bit TBC.
* $\mathsf{H}'_L(T)$ for processing variable length tweak.
* First n bit of $\mathsf{H}'_L(T)$ is xor-ed with the state.
* Remaining m bit of $\mathsf{H}'_L(T)$ is the tweak to the underlying TBC.
* n bit state.
* Provides graceful security degradation.



>>> Block Cipher vs Tweakable Block Cipher

Indistinguishable from random permutation.



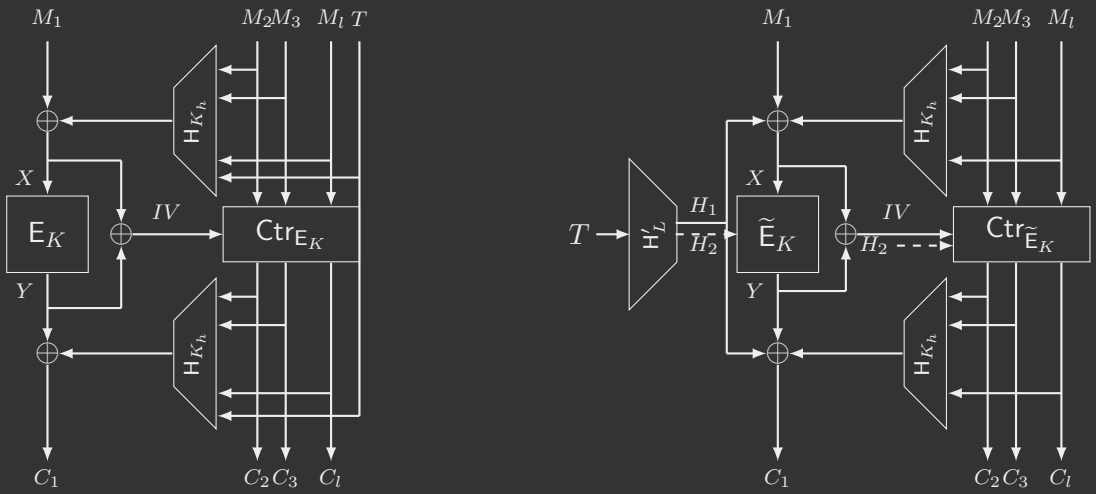
Indistinguishable from random permutation.

Indistinguishable from tweakable random permutation.

Author	Construction	Bound	Publication
Rogaway	PMAC1	$n/2$	ASIACRYPT, 04
Naito	PMAC_TBC3k, PMAC_TBC1k	n	Provsec, 15
Peyrin and Seurin	SCT	Graceful BBB	CRYPTO, 16
List and Nandi	PMACx, PMAC2x, SIVx	n	CT-RSA, 17
Iwata et al.	ZMAC, ZAE	$\min\{n, (n+t)/2\}$	CRYPTO, 17
List and Nandi	ZMAC+	$q(q+\sigma)/2^{n+\min\{n,t\}}$	ToSC, 17
Chen et al.	LDT	$n/2$ $(\star)$	FSE, 18
Chen et al.	LDT	$2n/3$	ASIACRYPT, 18

$(\star)$ Beyond the birthday bound for domain $[n, 3n/2)$.

>>> HCTR vs Tweakable HCTR



How H'_L is different from H_{K_h} ?

>>> How H'_L is different from H_{K_h} ?

* H_{K_h} requires to be n bit ϵ-AXU and ϵ-almost regular hash function.

>>> How H'_L is different from H_{K_h} ?

* H_{K_h} requires to be n bit ϵ-AXU and ϵ-almost regular hash function.
    * AXU:

$$\boxed{\forall M \neq M', \forall \delta,\ \Pr[\mathsf{H}_{K_h}(M) \oplus \mathsf{H}_{K_h}(M') = \delta] \leq \epsilon.}$$

    * Almost Regular:

$$\boxed{\forall M, \forall \delta,\ \Pr[\mathsf{H}_{K_h}(M) = \delta] \leq \epsilon.}$$

>>> How H'_L is different from H_{K_h} ?

* H_{K_h} requires to be n bit ϵ-AXU and ϵ-almost regular hash function.
    * AXU:

$$\boxed{\forall M \neq M', \forall \delta,\ \Pr[\mathsf{H}_{K_h}(M) \oplus \mathsf{H}_{K_h}(M') = \delta] \leq \epsilon.}$$

    * Almost Regular:

$$\boxed{\forall M, \forall \delta,\ \Pr[\mathsf{H}_{K_h}(M) = \delta] \leq \epsilon.}$$

* H'_L requires to be $(n+m)$ bit ϵ-partial AXU and $\mathsf{H}'_L[2]$ requires to be ϵ-almost universal hash function.

>>> How H'_L is different from H_{K_h} ?

* H_{K_h} requires to be n bit ϵ-AXU and ϵ-almost regular hash function.
  * AXU:

$$\boxed{\forall M \neq M', \forall \delta,\ \Pr[\mathsf{H}_{K_h}(M) \oplus \mathsf{H}_{K_h}(M') = \delta] \leq \epsilon.}$$

  * Almost Regular:

$$\boxed{\forall M, \forall \delta,\ \Pr[\mathsf{H}_{K_h}(M) = \delta] \leq \epsilon.}$$

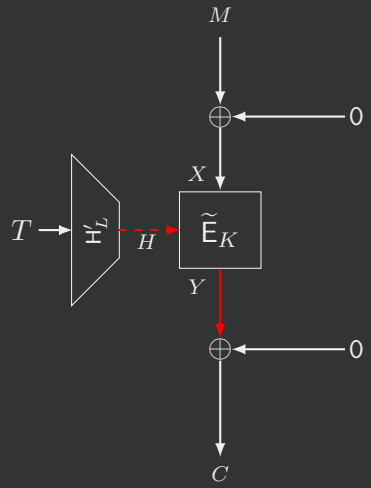
* H'_L requires to be $(n+m)$ bit ϵ-partial AXU and $\mathsf{H}'_L[2]$ requires to be ϵ-almost universal hash function.
  * partial AXU:

$$\boxed{\forall M \neq M', \forall \delta,\ \Pr[\mathsf{H}_{K_h}(M) \oplus \mathsf{H}_{K_h}(M') = (\delta, 0)] \leq \epsilon.}$$

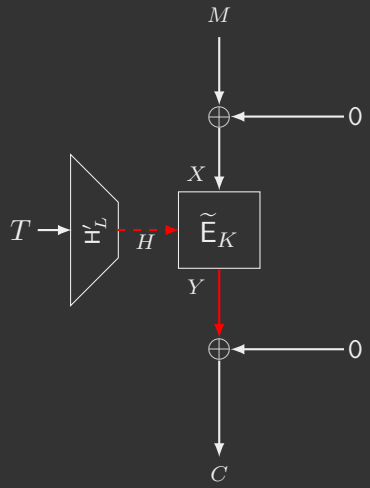
  * Almost Universal:

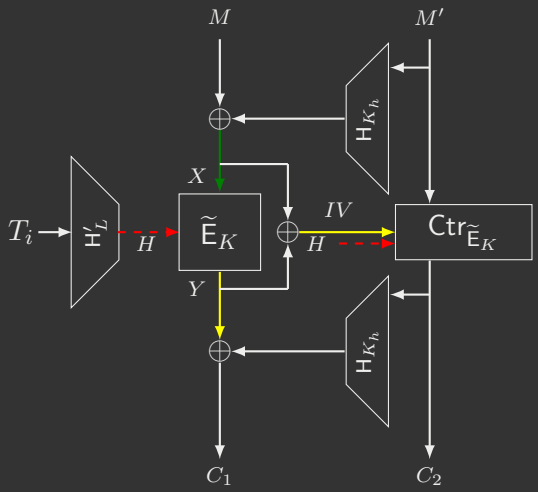
$$\boxed{\forall M \neq M',\ \Pr[\mathsf{H}'_L[2](M) = \mathsf{H}'_L[2](M')] \leq \epsilon.}$$

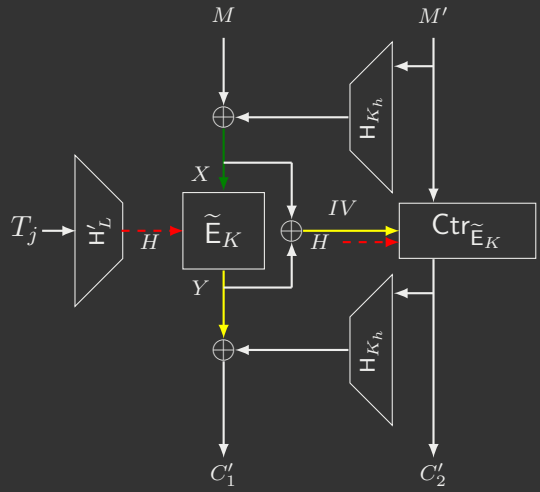
* A makes $2^{n/2}$ single block message query with distinct tweaks, i.e., $(M, T_1), \ldots, (M, T_{2^{n/2}})$.



* A makes $2^{n/2}$ single block message query with distinct tweaks, i.e., $(M, T_1), \ldots, (M, T_{2^{n/2}})$.
* Let $C_i = C_j$ (w.h.p due to m-bit hash collision).




M
M′
H_{K_h}
X
T_i
H'_L
H
$\widetilde{\mathsf{E}}_K$
IV
H
$\mathsf{Ctr}_{\widetilde{\mathsf{E}}_K}$
Y
H_{K_h}
C_1
C_2


M
M′
H_{K_h}
X
T_j
H'_L
H
$\widetilde{\mathsf{E}}_K$
IV
H
$\mathsf{Ctr}_{\widetilde{\mathsf{E}}_K}$
Y
H_{K_h}
C'_1
C'_2

Is $C_1 \| C_2 = C'_1 \| C'_2$?

Theorem

If H_{K_h} is ϵ-AXU and ϵ_1-almost regular hash function and H'_L be an (n, m, δ)-partial AXU hash function and $\mathsf{H}'[2]$ is a δ_{au}-almost univeral hash function. Then,

$$\begin{aligned}\mathbf{Adv}^{\mathrm{tsprp}}_{\mathsf{HCTR}} \leq\ & 2(\mu-1)(q\epsilon + \sigma/2^n) + 2q\sigma\delta_{\mathsf{au}}/2^n + q^2\delta \\ & + 2\max\{q\ell(\mu-1)/2^n + q\sigma\delta_{\mathsf{au}}/2^n, \sigma\epsilon_1\}.\end{aligned}$$

μ := # of repetition of tweaks.

>>> Security Result of Tweakable HCTR

Theorem

If H_{K_h} is ϵ-AXU and ϵ_1-almost regular hash function and H'_L be an (n, m, δ)-partial AXU hash function and $\mathsf{H}'[2]$ is a δ_{au}-almost univeral hash function. Then,

$$\begin{aligned}\mathbf{Adv}^{\mathrm{tsprp}}_{\mathsf{HCTR}} \leq\ & 2(\mu-1)(q\epsilon + \sigma/2^n) + 2q\sigma\delta_{\mathsf{au}}/2^n + q^2\delta \\ & + 2\max\{q\ell(\mu-1)/2^n + q\sigma\delta_{\mathsf{au}}/2^n, \sigma\epsilon_1\}.\end{aligned}$$

μ := # of repetition of tweaks.

Corollary

* Assuming $\epsilon, \epsilon_1 \approx 2^{-n}$, $\delta_{\mathsf{au}} \approx 2^{-m}, \delta \approx 2^{-(n+m)}$ and $m > n$, security $\approx 2^n/\mu\ell$ queries.

>>> Security Result of Tweakable HCTR

Theorem

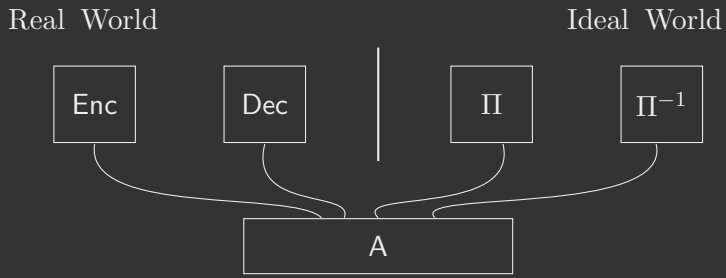
If H_{K_h} is ϵ-AXU and ϵ_1-almost regular hash function and H'_L be an (n, m, δ)-partial AXU hash function and $\mathsf{H}'[2]$ is a δ_{au}-almost univeral hash function. Then,

$$\begin{aligned}\mathbf{Adv}^{\mathrm{tsprp}}_{\mathsf{HCTR}} \leq\ & 2(\mu-1)(q\epsilon + \sigma/2^n) + 2q\sigma\delta_{\mathsf{au}}/2^n + q^2\delta \\ & + 2\max\{q\ell(\mu-1)/2^n + q\sigma\delta_{\mathsf{au}}/2^n, \sigma\epsilon_1\}.\end{aligned}$$

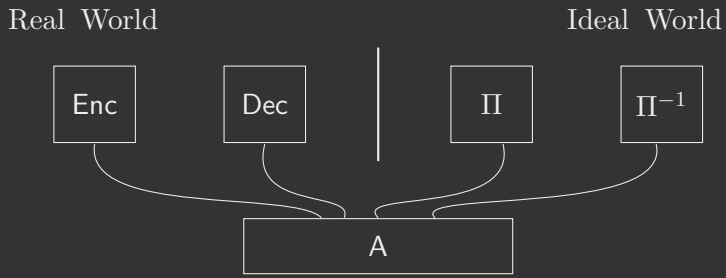
μ := # of repetition of tweaks.

Corollary

* Assuming $\epsilon, \epsilon_1 \approx 2^{-n}$, $\delta_{\mathsf{au}} \approx 2^{-m}, \delta \approx 2^{-(n+m)}$ and $m > n$, security $\approx 2^n/\mu\ell$ queries.
* Moreover, when $\mu = 1$, security $\approx 2^n$ many message blocks.



$$\mathbf{Adv}^{\text{real}}_{\text{ideal}}(\mathsf{A}) = \left| \ \Pr[\mathsf{A}^{\mathcal{I}.\mathsf{Enc},\mathcal{I}.\mathsf{Dec}_K} = 1] - \Pr[\mathsf{A}^{\Pi,\Pi^{-1}} = 1] \ \right|.$$



$$\mathbf{Adv}^{\text{real}}_{\text{ideal}}(\mathsf{A}) = \left| \ \Pr[\mathsf{A}^{\mathcal{I}.\mathsf{Enc},\mathcal{I}.\mathsf{Dec}_K} = 1] - \Pr[\mathsf{A}^{\Pi,\Pi^{-1}} = 1] \ \right|.$$

* Transcript: $\tau = (M_1, T_1, C_1), \ldots, (M_q, T_q, C_q)$.
* $X_{\text{re/id}} :=$ probability distribution of transcript in real / ideal world.
* $\mathcal{V} = \mathsf{GoodT} \sqcup \mathsf{BadT}$.

Main Theorm (H-Coefficient Technique)

If there exists $\epsilon_{\text{ratio}}, \epsilon_{\text{bad}} \geq 0$ such that

(i) for all $\tau \in \mathsf{GoodT}$, $\frac{\Pr[X_{\text{re}}=\tau]}{\Pr[X_{\text{id}}=\tau]} \geq 1 - \epsilon_{\text{ratio}}$ and

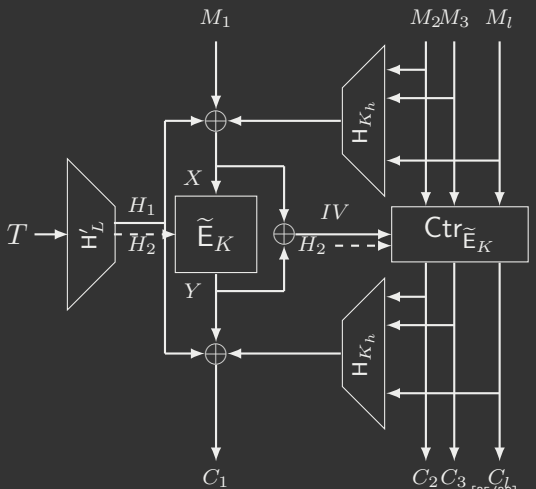
(ii) $\Pr[X_{\text{id}} \in \mathsf{BadT}] \leq \epsilon_{\text{bad}}$,

then

$$\mathbf{Adv}^{\text{real}}_{\text{ideal}}(\mathsf{A}) \leq \epsilon_{\text{ratio}} + \epsilon_{\text{bad}}.$$

Input or output collision for same tweak is bad.

* 1. $H_{2,i} = H_{2,j}, X_i = X_j$ or (b) $H_{2,i} = H_{2,j}, Y_i = Y_j$.
* 2. $H_{2,i} = H_{2,j}, IV_a^i = IV_b^j$.
* 3. $H_{2,i} = H_{2,j}, M_a^i \oplus C_a^i = M_b^j \oplus C_b^j$.
* 4. $H_{2,i} = H_{2,j}, X_i = IV_a^j$.
* 5. $H_{2,i} = H_{2,j}, Y_i = M_a^j \oplus C_a^j$.



Analysing Bad Event I:

$$\mathsf{B} := H_{2,i} = H_{2,j}, X_i = X_j \Leftrightarrow H_{2,i} = H_{2,j}, \mathsf{H}_{K_h}(\widehat{M_i}) \oplus H_{1,i} \oplus M_i = \mathsf{H}_{K_h}(\widehat{M_j}) \oplus H_{1,j} \oplus M_j$$

where $\widehat{M_i} := M_2^i \| \ldots \| M_{l_i}^i, \widehat{M_j} := M_2^j \| \ldots \| M_{l_i}^j$.

Analysing Bad Event I:

$\mathsf{B} := H_{2,i} = H_{2,j}, X_i = X_j \Leftrightarrow H_{2,i} = H_{2,j}, \mathsf{H}_{K_h}(\widehat{M}_i) \oplus H_{1,i} \oplus M_i = \mathsf{H}_{K_h}(\widehat{M}_j) \oplus H_{1,j} \oplus M_j$

where $\widehat{M}_i := M_2^i \| \dots \| M_{l_i}^i, \widehat{M}_j := M_2^j \| \dots \| M_{l_i}^j$.

* Case a: $T_i = T_j \Leftrightarrow (H_{1,i}, H_{2,i}) = (H_{1,j}, H_{2,j})$.

$$\Pr[\mathsf{B}] \leq q(\mu - 1)\epsilon, \qquad \#\ \text{of}\ \ (i,j) = (q, (\mu - 1)).$$

Analysing Bad Event I:

$\mathsf{B} := H_{2,i} = H_{2,j}, X_i = X_j \Leftrightarrow H_{2,i} = H_{2,j}, \mathsf{H}_{K_h}(\widehat{M_i}) \oplus H_{1,i} \oplus M_i = \mathsf{H}_{K_h}(\widehat{M_j}) \oplus H_{1,j} \oplus M_j$
where $\widehat{M_i} := M_2^i \| \dots \| M_{l_i}^i, \widehat{M_j} := M_2^j \| \dots \| M_{l_i}^j$.

* Case a: $T_i = T_j \Leftrightarrow (H_{1,i}, H_{2,i}) = (H_{1,j}, H_{2,j})$.

$$\Pr[\mathsf{B}] \leq q(\mu - 1)\epsilon, \qquad \#\ \text{of}\ (i,j) = (q, (\mu - 1)).$$

* Case (b): $T_i \neq T_j$, then

$$\Pr[\mathsf{B}] \leq \binom{q}{2}\delta, \qquad \#\ \text{of}\ (i,j) = \binom{q}{2}.$$

Analysing Bad Event I:

$\mathsf{B} := H_{2,i} = H_{2,j}, X_i = X_j \Leftrightarrow H_{2,i} = H_{2,j}, \mathsf{H}_{K_h}(\widehat{M_i}) \oplus H_{1,i} \oplus M_i = \mathsf{H}_{K_h}(\widehat{M_j}) \oplus H_{1,j} \oplus M_j$
where $\widehat{M_i} := M_2^i \| \dots \| M_{l_i}^i, \widehat{M_j} := M_2^j \| \dots \| M_{l_i}^j$.

* Case a: $T_i = T_j \Leftrightarrow (H_{1,i}, H_{2,i}) = (H_{1,j}, H_{2,j})$.

$$\Pr[\mathsf{B}] \leq q(\mu - 1)\epsilon, \qquad \#\ \text{of}\ (i,j) = (q, (\mu - 1)).$$

* Case (b): $T_i \neq T_j$, then

$$\Pr[\mathsf{B}] \leq \binom{q}{2}\delta, \qquad \#\ \text{of}\ (i,j) = \binom{q}{2}.$$

Similarly, we can bound the other bad events too.

Summary of the Bad Events Bound

Bad Event	Bound
B.1	$2(\mu-1)q\epsilon + q^2\delta$
B.2	$\sigma(\mu-1)/2^n + q\sigma\delta_{\mathrm{au}}/2^n$
B.3	$\sigma(\mu-1)/2^n + q\sigma\delta_{\mathrm{au}}/2^n$
B.4	$\max\{q\ell(\mu-1)/2^n + q\sigma\delta_{\mathrm{au}}/2^n, \sigma\epsilon_1\}$
B.5	$\max\{q\ell(\mu-1)/2^n + q\sigma\delta_{\mathrm{au}}/2^n, \sigma\epsilon_1\}$

Summary of the Bad Events Bound

Bad Event	Bound
B.1	$2(\mu-1)q\epsilon + q^2\delta$
B.2	$\sigma(\mu-1)/2^n + q\sigma\delta_{\mathrm{au}}/2^n$
B.3	$\sigma(\mu-1)/2^n + q\sigma\delta_{\mathrm{au}}/2^n$
B.4	$\max\{q\ell(\mu-1)/2^n + q\sigma\delta_{\mathrm{au}}/2^n, \sigma\epsilon_1\}$
B.5	$\max\{q\ell(\mu-1)/2^n + q\sigma\delta_{\mathrm{au}}/2^n, \sigma\epsilon_1\}$

If Bad Events do not happen then for two same tweak to the BC, either its input or output is fresh. Therefore,

$$\frac{\Pr[X_{\mathrm{re}} = \tau]}{\Pr[X_{\mathrm{id}} = \tau]} \geq 1.$$

>>> Conclusion & Future Work

* Tweakable Enciphering Scheme with Tweakable Block Cipher
* Mode with n bit state.
* Provides BBB security with graceful degradation

BBB Secure TES using BC (other than trivial option) is still open.

>>> Conclusion & Future Work

* Tweakable Enciphering Scheme with Tweakable Block Cipher
* Mode with n bit state.
* Provides BBB security with graceful degradation

BBB Secure TES using BC (other than trivial option) is still open.

Thank You