Short Tweak tBC and Its Applications in Symmetric Ciphers

A. Chakraborti, N. Datta, A. Jha, C. Mancilias Lopez, M. Nandi, Y. Sasaki

IAI, TCG CREST, Kolkata, India
CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
Computer Science Department, CINVESTAV-IPN, Mexico
Indian Statistical Institute, Kolkata, India
NTT Secure Platform Laboratories, Japan & NIST USA

October 2023

Contents

Tweakable Block Cipher (TBC)

What is a TBC?

$$E : \{0,1\}^k \times \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^n$$

Properties

- For any fixed key K and T, $E(K, T, \cdot) := E_K^T(\cdot)$ is a permutation over $\{0,1\}^n$
- TPRP Security: it is hard to distinguish from a random permutation

TBC Design Choice I: XE and XEX [Rogaway et al.]

XE and XEX

$$XE : E_K^{i_1,\cdots,i_t}(M) := E_K(\Delta \oplus M)$$
$$XEX : E_K^{i_1,\cdots,i_t}(M) := E_K(\Delta \oplus M) \oplus \Delta,$$

where $\Delta = \alpha_1^{i_1} \cdots \alpha_t^{i_t} \cdot L$ and $L = E_K(0)/E_K(N)$

- Examples: OCB (XEX), COLM (XE,XE)

TBC Design Chpice II: TWEAKEY Framework

TWEAKEY Framework (Jean-Nikolic-Peyrin: ASIACRYPT 2014)

- Iterated key alternating approach
- Tweak and Key processed together in the same fashion

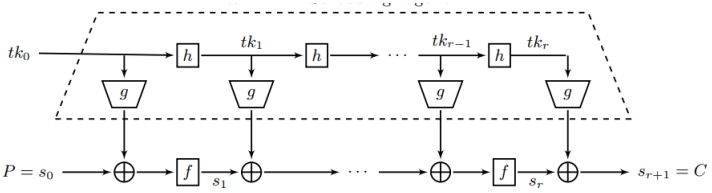


Figure: TWEAKEY Framework

Contents

Motivation for Short Tweak TBC (tBC)

Shortcomings of XE(X) Construction

- Additional block cipher invocation
- Storage overhead
- Degradation to Birthday bound security (General Weakness)

Shortcomings of TWEAKEY (STK) Framework

- Costly tweak schedule
- Difficult to optimize for short tweaks
- Increased number of rounds affects the throughput of the cipher

Contents

- Introduction
- Motivation of short-tweak Tweakable Block Ciphers
- Elastic Tweak Framework
- Instantiations
  - TweAES
  - TweGIFT
- Applications
  - Key Reduction
  - Simplicity in Design
  - Efficient Short Message Processing

Elastic Tweak Framework

Idea

- Elastic Tweak refers to elastic expansion of short tweaks
- Typically considers tweaks of size 4, 8 and 16 bits

Generic Design Framwork (BC $\rightarrow$ tBC)

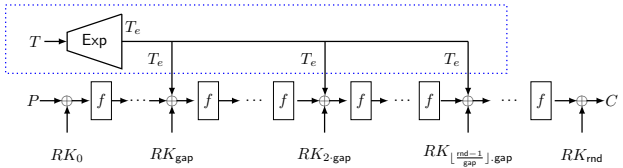
Generic framework, by which one can convert a block cipher (BC) (SPN based) to a short tweak tweakble block cipher (tBC)

Elastic Tweak Framework: Overview

BC → tBC Conversion: High-level Idea

- Expands a small tweak T (size t) to T_e (size t_e) by a linear code of high distance
- T_e is xored with the internal BC state affecting tic S-boxes
- Apply the tweak injection after a certain interval (*gap* number of rounds)
- $w := t_e/tic$ is the word size. It says how many bits of each S-box get affected

Tweak Expansion and Injection



Parameters and Recommended Instances

Parametrize tBC

- tBC is parameterized by four-tuple: (t, t_e, tic, gap), denoted by tBC$[t, t_e, tic, gap]$

Recommended Instances where BC $\in$ {AES-128, GIFT-128}

- TweAES-128 [4,8,8,2]
- TweAES-128 [8,16,8,2]
- TweAES-128 [16,32,8,2]
- TweGIFT [4,16,16,4]
- TweGIFT [4,32,32,5]
- TweGIFT [16,32,32,4]

Elastic Tweak Framework: Exp module

Algorithm to Expand the Tweak: Exp Module

- Define $\tau = t/w$
- Parse T as $T \leftarrow (T_1, T_2, \ldots, T_\tau)$, where $\forall i,\ T_i \in \mathbb{F}_{2^w}$
- Compute $S := T_1 \oplus \cdots \oplus T_\tau$
- Expand the Tweak: $T' := (T_1, \ldots, T_\tau, S \oplus T_1, \ldots, S \oplus T_\tau)$
- Optional Copy: $T_e := T' \| \cdots \| T'$ (Depends on the choice of the underlying BC)

Elastic Tweak Framework: Features

Features

- tBC can be applied to any SPN based block ciphers
- tBC with zero tweak turns out to be same as the underlying block cipher
- Low storage to store the tweak
- Lightweight operations to process the tweak

Contents

TweAES-128 with 4-bit Tweaks

TweAES-128 [4,8,8,2]

- $t = 4$ bit tweak is extended to $t_e = 8$ bit tweaks
- Tweaks are affected in $tic = 8$ S-Boxes
- Tweaks are injected at the least significant bits of each of the 8 S-Boxes in the top two rows
- Tweaks are injected at the interval of $gap = 2$ rounds

Other Instances

Other instances TweAES-128 [8,16,8,2] and TweAES-128 [16,32,8,2] are defined similarly

Cryptanalysis: TweAES

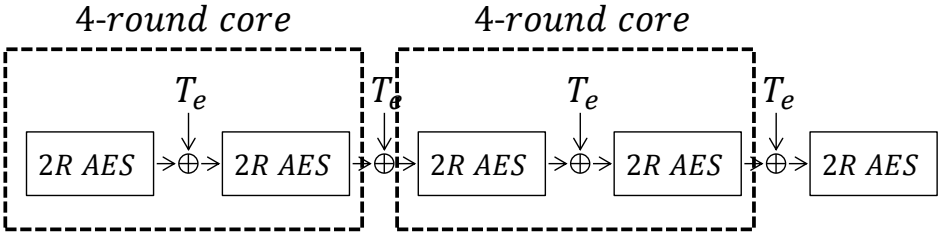


Figure: TweAES: 4-round Core

Differential Propagation through 4-round core

- 4-round core: 15 Active S-Boxes (next slide)

Cryptanalysis: TweAES

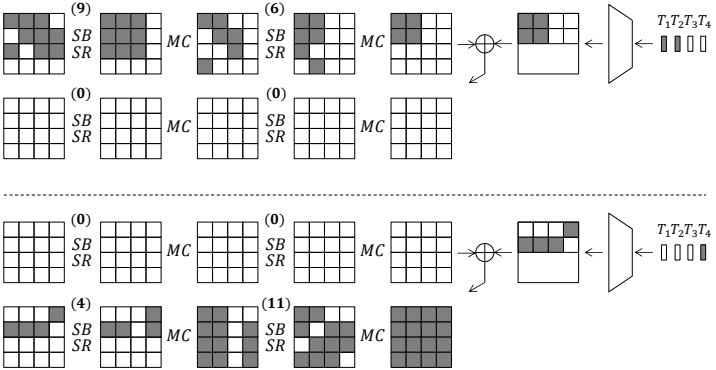


Figure: Differential Trails with 15 S-Boxes

Cryptanalysis: TweAES

Differential Propagation through 4-round core

- 4-round core: 15 Active S-Boxes
- Differential Probability: 2^{-6}
- Overall probability: 2^{-90}

- The probability of differential propagation of TweAES is bounded by 2^{-180}

TweGIFT-64 with 4-bit Tweaks

TweGIFT-64 [4,16,16,4]

- $t = 4$ bit tweak is extended to $t_e = 16$ bit tweaks
- Tweaks are affected in $tic = 16$ S-Boxes
- Tweaks are injected at bit positions $4i + 2$, for $i = 0, \ldots, 15$
- Tweaks are injected at the interval of $gap = 4$ rounds

Other Instances

Other instances TweGIFT [4,32,32,5] and TweGIFT [16,32,32,4] are defined similarly

Cryptanalysis: TweGIFT-64

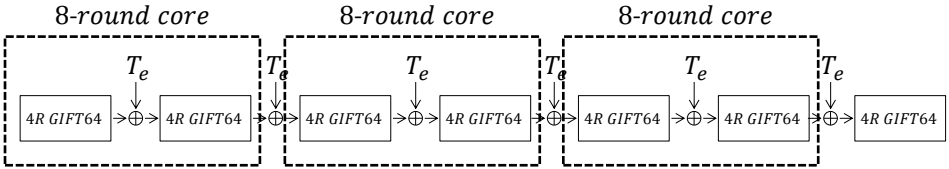


Figure: TweGIFT: 8-round Core

Differential Propagation through 8-round core

- 8-round core: 2^{-42} Differential Characteristic (next slide)

Cryptanalysis: TweGIFT-64

Table: The Best Differential Trail for 8-Round Core

Round	Differential Mask	Probability
1	0000 0000 0000 000c 0000 0000 0000 0004	2^{-2}
2	0000 0004 0000 0000 0000 0005 0000 0000	2^{-2}
3	0000 0400 0000 0100 0000 0500 0000 0500	2^{-5}
4	0000 0101 0000 0404 0000 0909 0000 0d0d	2^{-12}
tweak difference: 0808 0808 0808 0808		
5	0000 090d 0000 090d 0000 0104 0000 0104	2^{-10}
6	0000 0004 0000 0000 0000 0505 0000 0000	2^{-6}
7	0a00 0000 0000 0000 0100 0000 0000 0000	2^{-2}
8	0000 1000 0000 0000 0000 8000 0000 0000	2^{-3}

Cryptanalysis: TweGIFT-64

Differential Propagation through 8-round core

- 8-round core: 2^{-42} Differential Characteristic
- 28-round core: 2^{-126} Differential Characteristic

Differential Propagation through 10-round core

- 10-round core: $2^{-64.5}$ Differential Characteristic
- 40-round core: 2^{-258} Differential Characteristic

Contents

Applications

Application I: Reduce the Key Size

- Reduce Key size of FCBC by replacing $(E_{K_1}, E_{K_2}, \ldots, E_{K_j})$ by $(E_K^1, E_K^2, \ldots, E_K^j)$
- State size reduction

Application II: Simplify the Design

Simplify the design of CLOC by replacing the domain separators f, g_1, g_2, h_1, h_2 (see the main paper) by varying the tweaks (4-bit tweaks are sufficient)

Reduces the complexity of the circuit (for example, by reducing Multiplexers)

Application III: Efficient Short Message Processing

- Increase the rate of LightMAC and decrease the key-size of LightMAC

Other Application: Improve SUNDAE to ESTATE

- Energy Efficiency: 1 less block cipher invocation for ESTATE
- Design Simplicity: No constant multiplication for ESTATE
- RUP Security: ESTATE is INT-RUP secure

Significance of the Result: SUNDAE vs ESTATE

- Area Efficiency:

Mode	Area (LUTs)	Throughput/Area (Mbps/LUT)
SUNDAE [GIFT]	931	0.9
ESTATE [TweGIFT]	681	1.23

- Throughput for Short Messages (16 bytes):

Mode	Throughput (Mbps)
SUNDAE [AES]	945.36
ESTATE [TweAES]	1251.1

Conclusion

Conclusion

- Short Tweak tBC Proposal
- Efficient Instance Proposal with Cryptanalysis
- Several Applications

Future Direction

- Extending the framework to ARX-based constructions
- Designing short tweak TBCs for public permutation

Thank You..!!!