ZCZ: Achieving n-bit SPRP Security with a Minimal Number of Tweakable-block-cipher Calls

Ritam Bhaumik, Indian Statistical Institute, Kolkata

Eik List, Bauhaus-Universität Weimar, Weimar

Mridul Nandi, Indian Statistical Institute, Kolkata

ASIACRYPT 2018
Brisbane, Australia
3 December 2018

Introduction

Optimising SPRPs

SPRP: *Strong Pseudorandom Permutations* (indistinguishable under chosen-ciphertext attacks)

Common optimisation goals for SPRPs:

- Low implementation costs
- High provable-security guarantees
- High performance

Provable security of SPRPs

Adversary $\mathcal{A}$ making queries with at most σ blocks in all in CCA setting

Birthday Bound:
Distinguishing advantage $O\left(\frac{\sigma^2}{2^n}\right)$
(n: width of underlying primitive in bits, e.g., 128)

Here $\mathcal{A}$ needs $O\left(2^{n/2}\right)$ query-blocks to attack

Beyond Birthday Bound:
Number of query-blocks required of a higher order than $2^{n/2}$

Tweakable Block Ciphers

Blockcipher with additional public input

Dedicated Designs:
Deoxys-BC, Joltik-BC, Skinny

TBC-based MAC:
ZMAC [CRYPTO '17]

- Parallelisable
- Single-keyed
- Based on an internal hash function ZHash

Our Contributions

Theoretical:
Proof that 1.5 primitive calls per message block is close to optimal

Practical:
New TBC-based SPRP construction ZCZ:

- 1.5 TBC calls per message block
- Full *n*-bit provable security

ZCZ*: Extended version of ZCZ that can handle partial blocks

Preliminaries

Simple Random Sampling

Sample space: $\mathcal{S} = \{0, \ldots, N-1\}$
Sample: $(X_1, \ldots, X_q)$

With replacement (SRSWR):

- $X_1, \ldots, X_q$ independent
- For any $x_1, \ldots, x_q \in \mathcal{S}$, $\Pr[X_1 = x_1, \ldots, X_q = x_q] = 1/N^q$.

Without replacement (SRSWOR):

- $X_1, \ldots, X_q$ distinct, this is the only dependence
- For any $x_1, \ldots, x_q \in \mathcal{S}$,
  $\Pr[X_1 = x_1, \ldots, X_q = x_q] = (N-q)!/N!$ when $x_1, \ldots, x_q$ are distinct and 0 otherwise.

Collision Probabilities

Assume $X_1, \ldots, X_q$ is an SRSWR-sample from $\{0, \ldots, N-1\}$

Single collision:

$$\alpha_0 + \alpha_1 X_1 + \ldots + \alpha_q X_q = 0$$

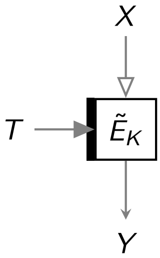
If $\alpha_i \neq 0$ for any $i \in \{1, \ldots, q\}$, the probability is $1/N$.

Double collision:

$$\alpha_0 + \alpha_1 X_1 + \ldots + \alpha_q X_q = 0,$$
$$\beta_0 + \beta_1 X_1 + \ldots + \beta_q X_q = 0.$$

If $\alpha_i \beta_j \neq \beta_i \alpha_j$ for any $i, j \in \{1, \ldots, k\}$, the probability is $1/N^2$.

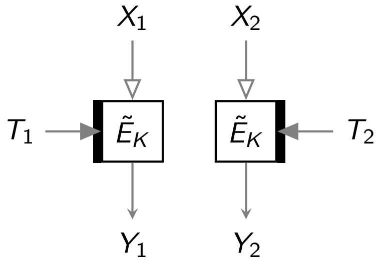
Tweakable Blockciphers



$$\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{B} \longrightarrow \mathcal{B}$$

$\mathcal{K}$: Key space, $\mathcal{T}$: Tweak space, $\mathcal{B}$: Block space
For fixed K and T, $\tilde{E}_K(T, \cdot)$ is injective

Constraints



$$(X_1, T_1) = (X_2, T_2) \implies Y_1 = Y_2$$
$$(Y_1, T_1) = (Y_2, T_2) \implies X_1 = X_2$$

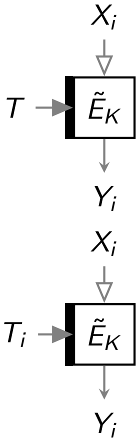
[No constraints when $T_1 \neq T_2$]

Ideal Tweakable Blockciphers

For random $K \in \mathcal{K}$:

- For fixed $T \in \mathcal{T}$, for distinct $X_1, \dots, X_q \in \mathcal{B}$, $(Y_1, \dots, Y_q)$ should form an SRSWOR-sample from $\mathcal{B}$.

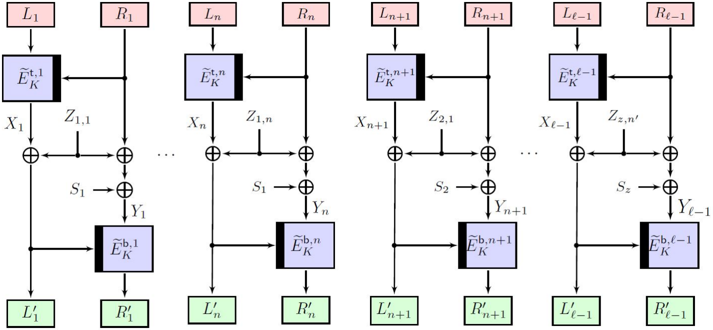
- For distinct $T_1, \dots, T_q \in \mathcal{T}$, for any $X_1, \dots, X_q \in \mathcal{B}$, $(Y_1, \dots, Y_q)$ should form an SRSWR-sample from $\mathcal{B}$.



Construction

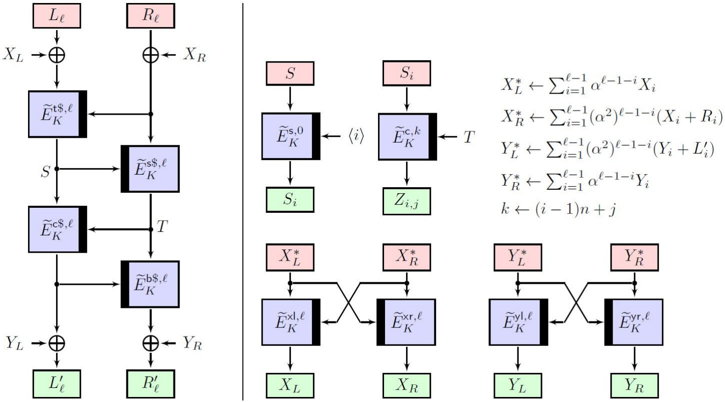
The ZCZ Encryption Scheme

(a) The first $\ell - 1$ diblocks ($Z_{i,j}$, S_i mixing variables):



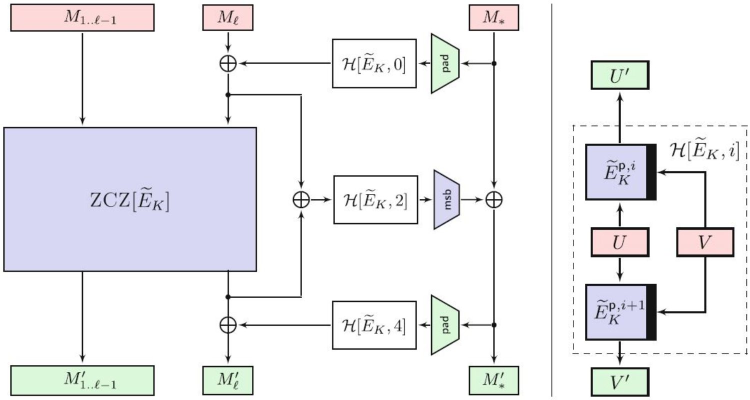
The ZCZ Encryption Scheme

(b) The final diblock and the mixing layer:

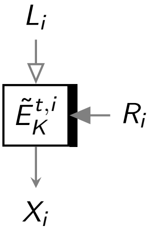


The ZCZ* Encryption Scheme

Version of ZCZ that can handle partial blocks:



Breaking it down



Top Layer

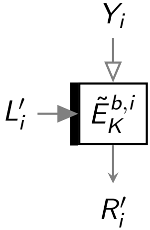
$$\{(X_i, R_i) \mid 1 \leq i \leq \ell - 1\}, (L_\ell, R_\ell)$$

$$\downarrow$$

$$\boxed{\text{Mixing Layer}}$$

$$\downarrow$$

$$\{(L'_i, Y_i) \mid 1 \leq i \leq \ell - 1\}, (L'_\ell, R'_\ell)$$



Bottom Layer

(The different tweakable blockciphers used are obtained from a single key using standard domain separation techniques)

Proof Approach

Main Tool

Coefficient H Technique: For real oracle $\mathcal{O}_1$ and ideal oracle $\mathcal{O}_0$, consider the conditions below:

- *Condition 1:* The probability of certain **bad** events occurring under the ideal oracle is bounded above by ϵ;
- *Condition 2:* When a bad event has not occurred, a transcript is at least as probable under $\mathcal{O}_1$ as under $\mathcal{O}_0$.

When these conditions hold, the advantage of an adversary distinguishing between $\mathcal{O}_0$ and $\mathcal{O}_1$ is bounded above by ϵ.

Oracles

Real Oracle:

- Uses ZCZ to answer queries;
- At the end reveals all internal inputs and outputs to $\tilde{E}_K$.

Ideal Oracle:

- Uses an ideal random wide permutation to answer queries;
- At the end *samples* all internal inputs and outputs to $\tilde{E}_K$;
- Sampling is first done over a **basis**;
- This sample is then **extended** to the other inputs and outputs.

Bad Events: Main Idea

Broad strategy:

- Ban (tweak, input) collisions;
- Ban (tweak, output) collisions.

We need to ensure that each bad event is a double collision.

Bounding Bad Probabilities

Approach:

- Fix all parameters;
- Identify underlying double collision;
- Check conditions for $1/N^2$ bound (where $N = 2^n$).
- Count over parameter choices;
- Bound using union bound.

Final bound obtained on distinguishing advantage: $\frac{21\sigma^2}{2^{2n}}$

Thank you for your attention

The authors regret not being able to attend the conference, and are grateful to Aleksei Udovenko of the University of Luxembourg for agreeing to present the paper on their behalf. Questions on the work are welcome to be addressed to the authors on their listed email addresses.