Multidimensional Linear Distinguishers with Correlation Zero

Andrey Bogdanov, Gregor Leander, Kaisa Nyberg and Meiqin Wang

K.U.Leuven, DTU, Aalto University and Shandong University

ASK 2012, August 28, 2012

Outline

Background

- Differential, linear and impossible differential cryptanalysis: basic evaluation tools for block ciphers.
  - Differential cryptanalysis: differentials with higher probability
  - Linear cryptanalysis: linear approximations whose probability deviates from 1/2
  - Impossible differential cryptanalysis: differentials with zero probability
- Zero correlation linear cryptanalysis
  - Recently, proposed by Andrey Bogdanov and Vincent Rijmen (IACR Eprint Report:2011/123)
  - Uses linear approximations with probability p=1/2, or the correlation c is zero

$$c = 2p - 1.$$

Background

- Differential, linear and impossible differential cryptanalysis: basic evaluation tools for block ciphers.
  - Differential cryptanalysis: differentials with higher probability
  - Linear cryptanalysis: linear approximations whose probability deviates from $1/2$
  - Impossible differential cryptanalysis: differentials with zero probability
- Zero correlation linear cryptanalysis
  - Recently, proposed by Andrey Bogdanov and Vincent Rijmen (IACR Eprint Report:2011/123)
  - Uses linear approximations with probability p=$1/2$, or the correlation c is zero

$$c = 2p - 1.$$

Motivation

- Zero correlation linear cryptanalysis
  - Similar to impossible differential cryptanalysis, but essentially different mathematical theory
  - Applied to 6-round AES-256 and 13-round CLEFIA-256 with the full codebook or half of the full codebook
  - Motivation:
    - reduce the data complexity
    - find ciphers with longer zero-correlation linear approximations
    - attack more rounds of ciphers

Linear Approximations with Zero Correlation

- Consider an n-bit block cipher $C = f_K(P)$, the linear approximation $\Gamma_P \rightarrow \Gamma_C$: $\Gamma_P^T P \oplus \Gamma_C^T C = 0$.
  Γ_P, Γ_C: nonzero plaintext and ciphertext masks.
  The probability of $\Gamma_P \rightarrow \Gamma_C$:
  $p_{\Gamma_P,\Gamma_C} = \Pr_{P \in \mathbf{F}_2^n}\{\Gamma_P^T P \oplus \Gamma_C^T C = 0\}$.
  The correlation of $\Gamma_P \rightarrow \Gamma_C$: $c_{\Gamma_P,\Gamma_C} = 2p_{\Gamma_P,\Gamma_C} - 1$
  $p_{\Gamma_P,\Gamma_C} = \frac{1}{2} \Rightarrow c_{\Gamma_P,\Gamma_C} = 0$: **zero correlation**
- The probability that a linear approximation has zero correlaiton for n-bit random permutation:

$$\frac{1}{\sqrt{2\pi}} 2^{\frac{4-n}{2}}$$

Linear Approximations with Zero Correlation

- Consider an n-bit block cipher $C = f_K(P)$, the linear approximation $\Gamma_P \rightarrow \Gamma_C$: $\Gamma_P^T P \oplus \Gamma_C^T C = 0$.
  Γ_P, Γ_C: nonzero plaintext and ciphertext masks.

  The probability of $\Gamma_P \rightarrow \Gamma_C$:
  $p_{\Gamma_P,\Gamma_C} = \Pr_{P \in \mathbf{F}_2^n}\{\Gamma_P^T P \oplus \Gamma_C^T C = 0\}$.
  The correlation of $\Gamma_P \rightarrow \Gamma_C$: $c_{\Gamma_P,\Gamma_C} = 2p_{\Gamma_P,\Gamma_C} - 1$
  $p_{\Gamma_P,\Gamma_C} = \frac{1}{2} \Rightarrow c_{\Gamma_P,\Gamma_C} = 0$: **zero correlation**
- The probability that a linear approximation has zero correlaiton for n-bit random permutation:

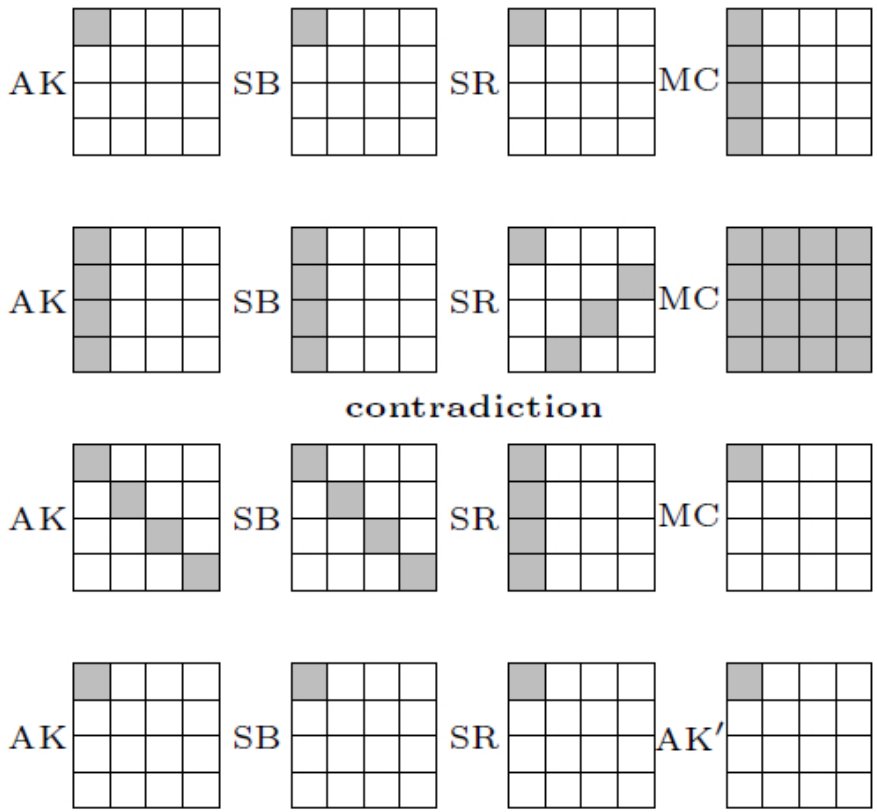
$$\frac{1}{\sqrt{2\pi}} 2^{\frac{4-n}{2}}$$

Relations for linear mask for three operations[Bogdanov-Vincent 2011]

- **Lemma 1(XOR approximation):** Either the three linear selection patterns at an XOR $\oplus$ are equal or the correlation over $\oplus$ is exactly zero.
- **Lemma 2(Branching approximation):** Either the three linear selection patterns at a branching point $\cdot$ sum up to 0 or the correlation over $\cdot$ is exactly zero.
- **Lemma 3(Permutation approximation):** Over a permutation ϕ, if the input and output selection patterns are neither both zero nor both nonzero. the correlation over ϕ is exactly zero.

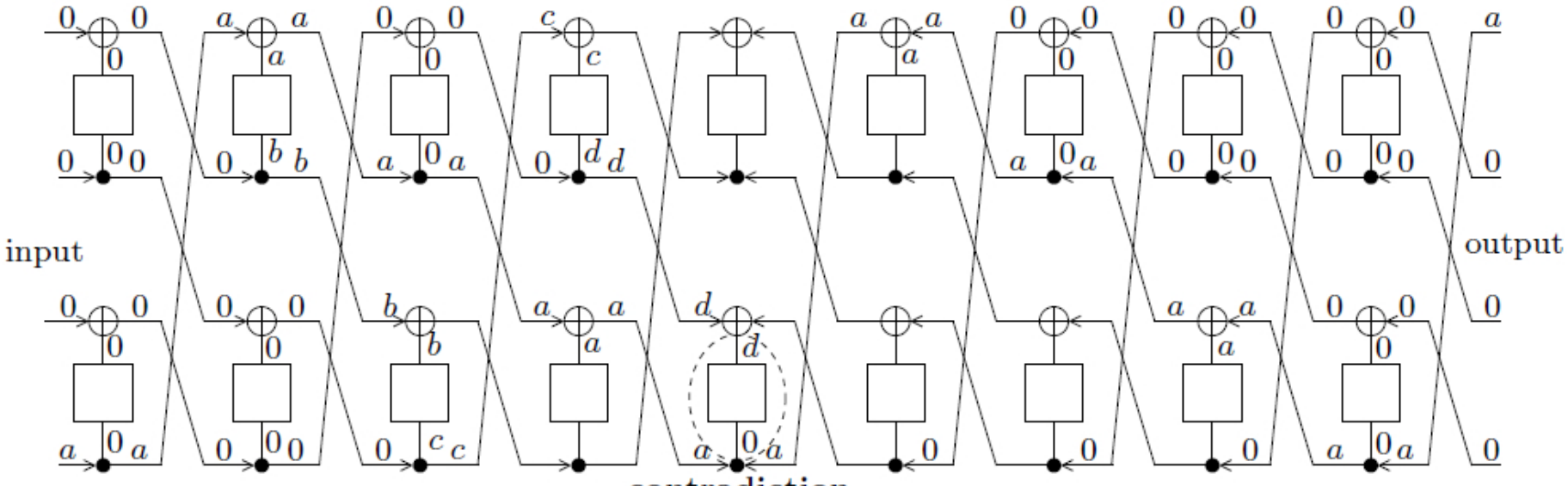
Zero correlation linear approximation for AES

AES: 4 rounds zero correlation linear approximations(3 full rounds +1 round without MixColumns):

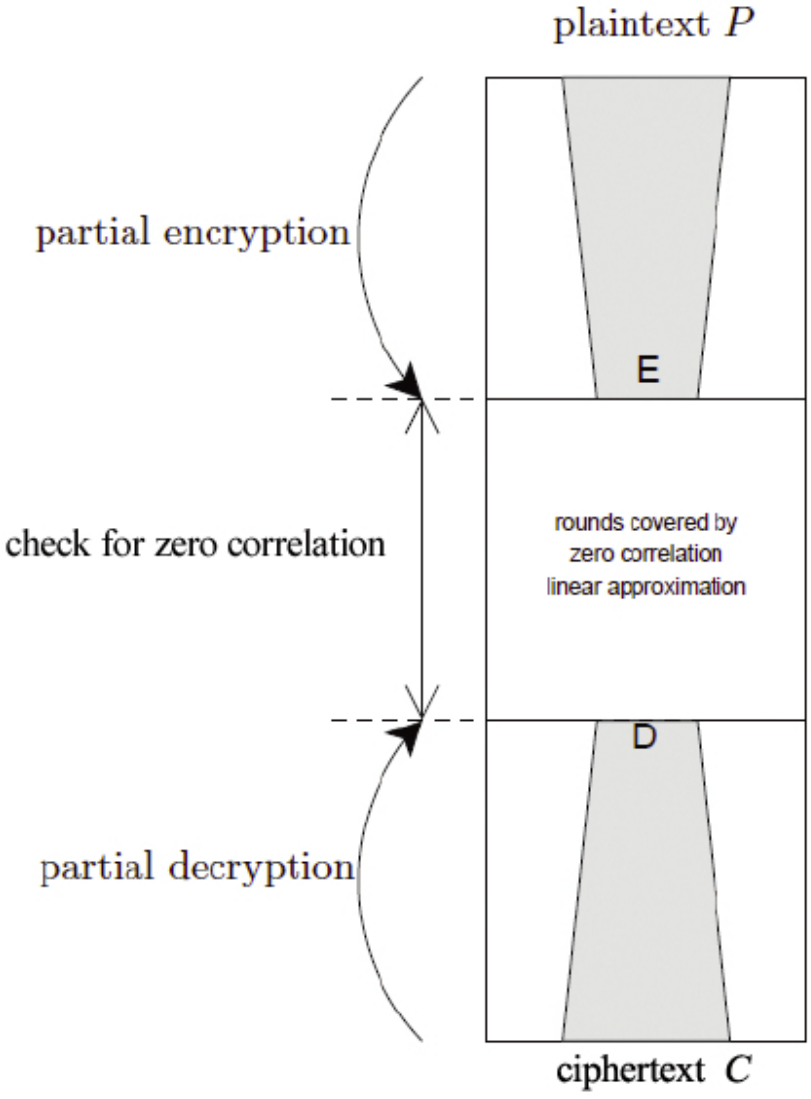


Zero correlation linear approximation for CLEFIA

CLEFIA: 9 rounds zero correlation linear approximations



Key Recovery with Zero Correlation Linear Approximations



Distinguishing Between Two Normal Distributions

- Two normal distributions: $\mathcal{N}(\mu_0, \sigma_0)$, $\mathcal{N}(\mu_1, \sigma_1)$, $\mu_0 < \mu_1$.
- The sample s is from $\mathcal{N}(\mu_0, \sigma_0)$ or $\mathcal{N}(\mu_1, \sigma_1)$? Perform the test to compare the value s to some threshold value t.
  - if $s \leq t$, $s \in \mathcal{N}(\mu_0, \sigma_0)$
  - if $s > t$, $s \in \mathcal{N}(\mu_1, \sigma_1)$.
- Two error probabilities:

$$\begin{aligned} \beta_0 &= \Pr\{\text{"}s \in \mathcal{N}(\mu_1, \sigma_1)\text{"} | s \in \mathcal{N}(\mu_0, \sigma_0)\}, \\ \beta_1 &= \Pr\{\text{"}s \in \mathcal{N}(\mu_0, \sigma_0)\text{"} | s \in \mathcal{N}(\mu_1, \sigma_1)\}. \end{aligned}$$

Proposition 1

For the test to have error probabilities of β_0 *and* β_1*, the parameters of the normal distributions* $\mathcal{N}(\mu_0, \sigma_0)$ *and* $\mathcal{N}(\mu_1, \sigma_1)$ *with* $\mu_0 \neq \mu_1$ *have to be such that*

$$\frac{z_{1-\beta_1}\sigma_1 + z_{1-\beta_0}\sigma_0}{|\mu_1 - \mu_0|} = 1,$$

where $z_{1-\beta_1}$ *and* $z_{1-\beta_0}$ *are the quantiles of the standard normal distribution.*

Correlation under Right and Wrong Keys

Consider the key recovery procedure with N known plaintext-ciphertext pairs and for each of the ℓ given linear hulls, an empirical correlation value $\hat{c}_i = 2\frac{T_i}{N} - 1$.

- Right key guess: $\hat{c}_i \sim \mathcal{N}(0, 1/\sqrt{N})$, [Junod01,selcuk08]
- Wrong key guess: $\hat{c}_i \sim \mathcal{N}(c_i, 1/\sqrt{N})$, $c_i \sim \mathcal{N}(0, 2^{-n/2})$, c_i: the exact value of the correlation, [O'Connor95,Daemen07]
- **For one linear hull**: only focus on $\hat{c}_i$, but need full codebook or half of the codebook.
- **For ℓ linear hulls**: focus on the statistic value of $\sum_{i=1}^{\ell} \hat{c}_i^2$,

$$\sum_{i=1}^{\ell} \hat{c}_i^2 = \sum_{i=1}^{\ell} \left(2\frac{T_i}{N} - 1\right)^2.$$

Distribution of the Statistic under Right Key

Proposition 2

Consider ℓ nontrivial zero correlation linear approximations for a block cipher with a fixed key. If N is the number of known plaintext-ciphertext pairs, T_i is the number of times such a linear approximation is fulfilled for $i \in \{1, \ldots, \ell\}$, and ℓ is high enough, then the following approximate distribution holds for sufficiently large N:

$$\sum_{i=1}^{\ell} \left(2\frac{T_i}{N} - 1\right)^2 \sim \mathcal{N}\left(\frac{\ell}{N}, \frac{\sqrt{2\ell}}{N}\right).$$

Distribution of the Statistic under Wrong Key

Proposition 3

Consider ℓ nontrivial linear approximations for a randomly drawn permutation. If N is the number of known plaintext-ciphertext pairs, T_i is the number of times a linear approximation is fulfilled for $i \in \{1, \ldots, \ell\}$, and ℓ is high enough, then the following approximate distribution holds for sufficiently large N:

$$\sum_{i=1}^{\ell} \left(2\frac{T_i}{N} - 1\right)^2 \sim \mathcal{N}\left(\frac{\ell}{N} + \frac{\ell}{2^n}, \frac{\sqrt{2\ell}}{N} + \frac{\sqrt{2\ell}}{2^n}\right).$$

Data Complexity of the Distinguisher

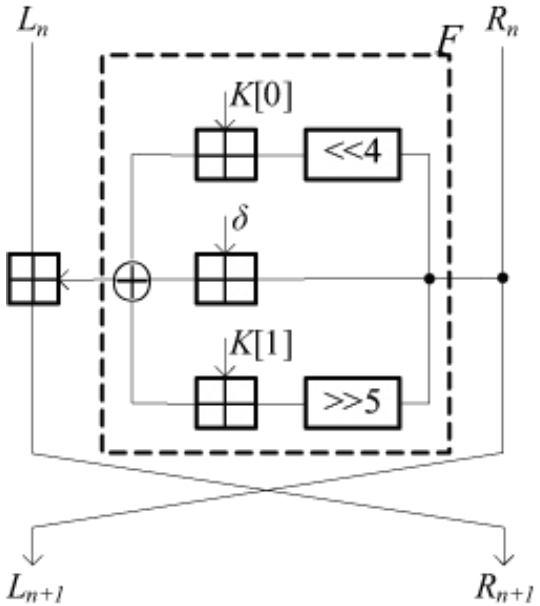
Theorem 1

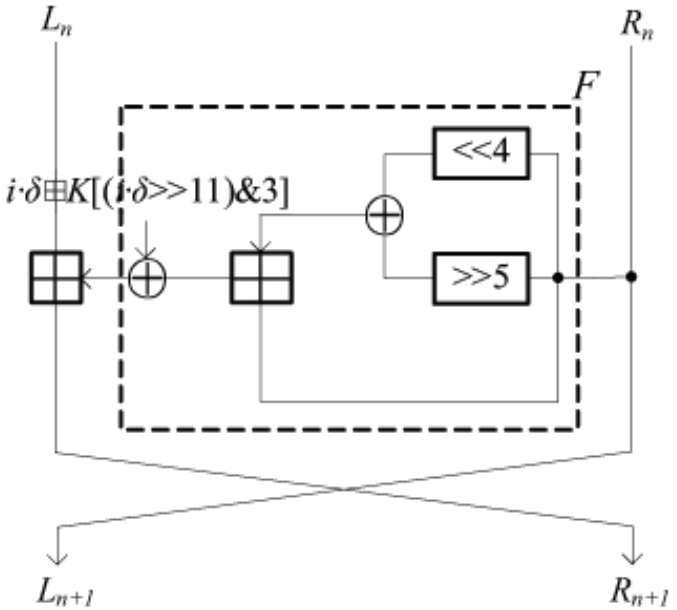
With the assumptions of Propositions 1 to 3, using ℓ nontrivial zero correlation linear approximations, to distinguish between a wrong key and a right key with probability β_1 of false positives and probability β_0 of false negatives, a number N of known plaintext-ciphertext pairs is sufficient if the following condition is fulfilled:

$$N = \frac{2^{n+0.5}\left(z_{1-\beta_0} + z_{1-\beta_1}\right)}{\sqrt{\ell} - z_{1-\beta_1}\sqrt{2}}.$$

The Block Ciphers TEA and XTEA

- TEA and XTEA: 64-round, 64-bit block size, 128-bit key, Feistel small cipher, implemented in the Linux kernel





Summary of Cryptanalytic Results on TEA

Attack	#Rounds	Data	Time	Memory	Ref.
ID	11	$2^{52.5}$ CP	2^{84}	Not given	[MHL 2002]
TD	17	1920 CP	$2^{123.37}$	Not given	[HHK 2004]
ID	17	2^{57} CP	$2^{106.6}$	2^{49}	[CWP 2011]
ZC LH	**21**	$\mathbf{2^{62.62}}$ **KP**	$\mathbf{2^{121.52}}$	**Negligible**	**[BW 2012]**
ZC LH	**23**	$\mathbf{2^{64}}$	$\mathbf{2^{119.48}}$	**Negligible**	**[BW 2012]**

CP: Chosen Plaintexts, KP: Known Plaintexts.

Memory: the number of 32-bit words.

*The effective key length for TEA is 126 bit

Summary of Cryptanalytic Results on XTEA

Attack	R	Data	Time	Memory	Ref.
ID	14	$2^{62.5}$ CP	2^{85}	Not given	[MHL 2002]
TD	23	$2^{20.55}$ CP	$2^{120.65}$	Not given	[HHK 2004]
MITM	23	18 KP	2^{117}		[SMVP 2011]
ID	23	$2^{62.3}$ CP	$2^{101}MA$ $+2^{105.6}$	$2^{94.3}$	[CWP 2011]
ID	23	2^{63}	$2^{114.5}$	2^{103}	[CWP 2011]
MITM	29	2^{45} CP	2^{124}	2^{4}	[IS 2012]
ZC LH	**25**	$\mathbf{2^{62.62}}$ **KP**	$\mathbf{2^{124.53}}$	$\mathbf{2^{30}}$	**[BW 2012]**
ZC LH	**27**	$\mathbf{2^{64}}$	$\mathbf{2^{120.71}}$	**Negligible**	**[BW 2012]**

CP: Chosen Plaintexts, KP: Known Plaintexts.

Memory: the number of 32-bit words.

*The effective key length for TEA is 126 bit

Linear Approximation of Modular Addition

- For the modular addition of two n-bit inputs x and y, the output z can be computed as:

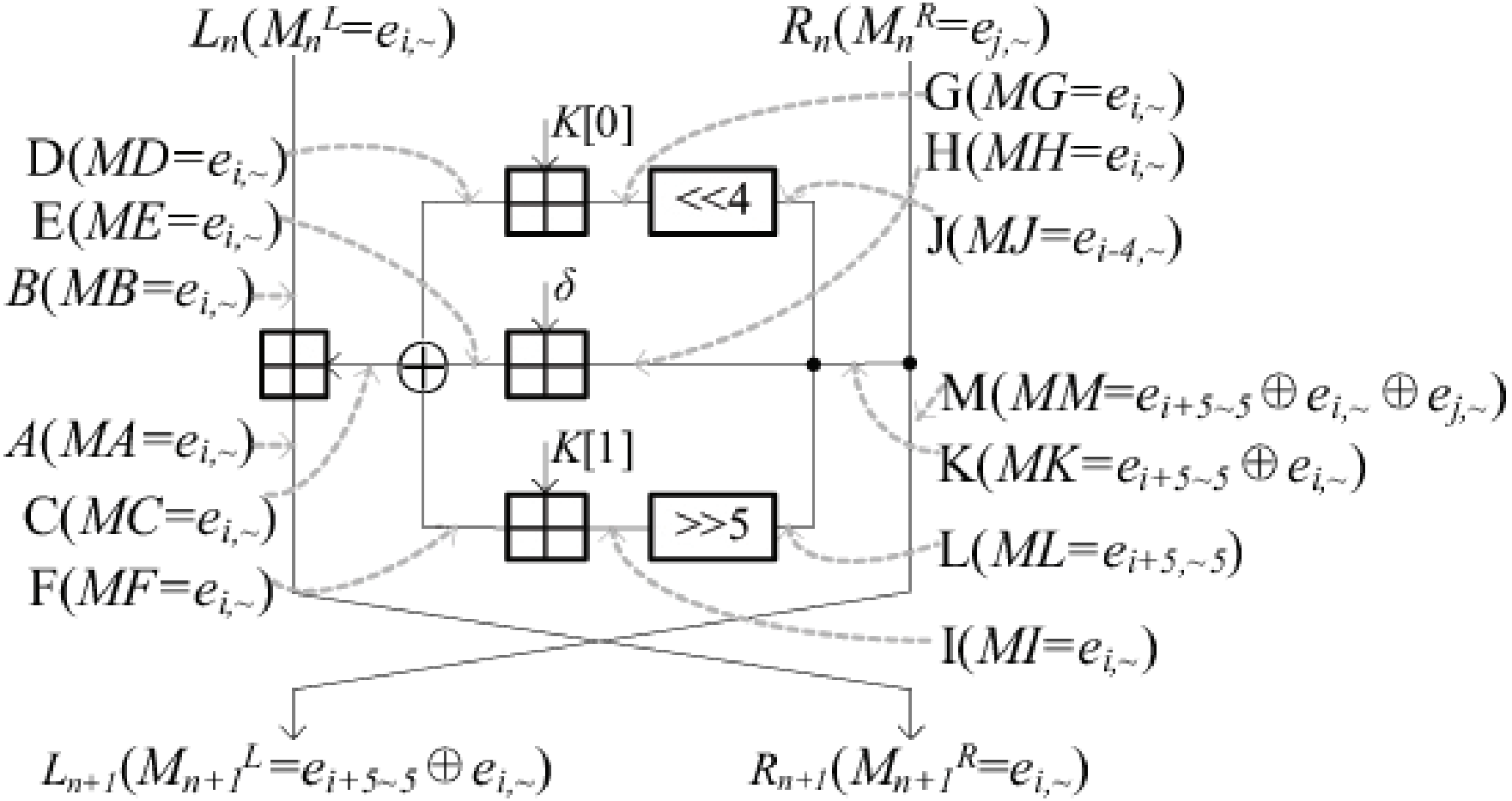
$$z = (x + y) \mod 2^n.$$

$$+ : (\Gamma x | \Gamma y) \rightarrow \Gamma z.$$

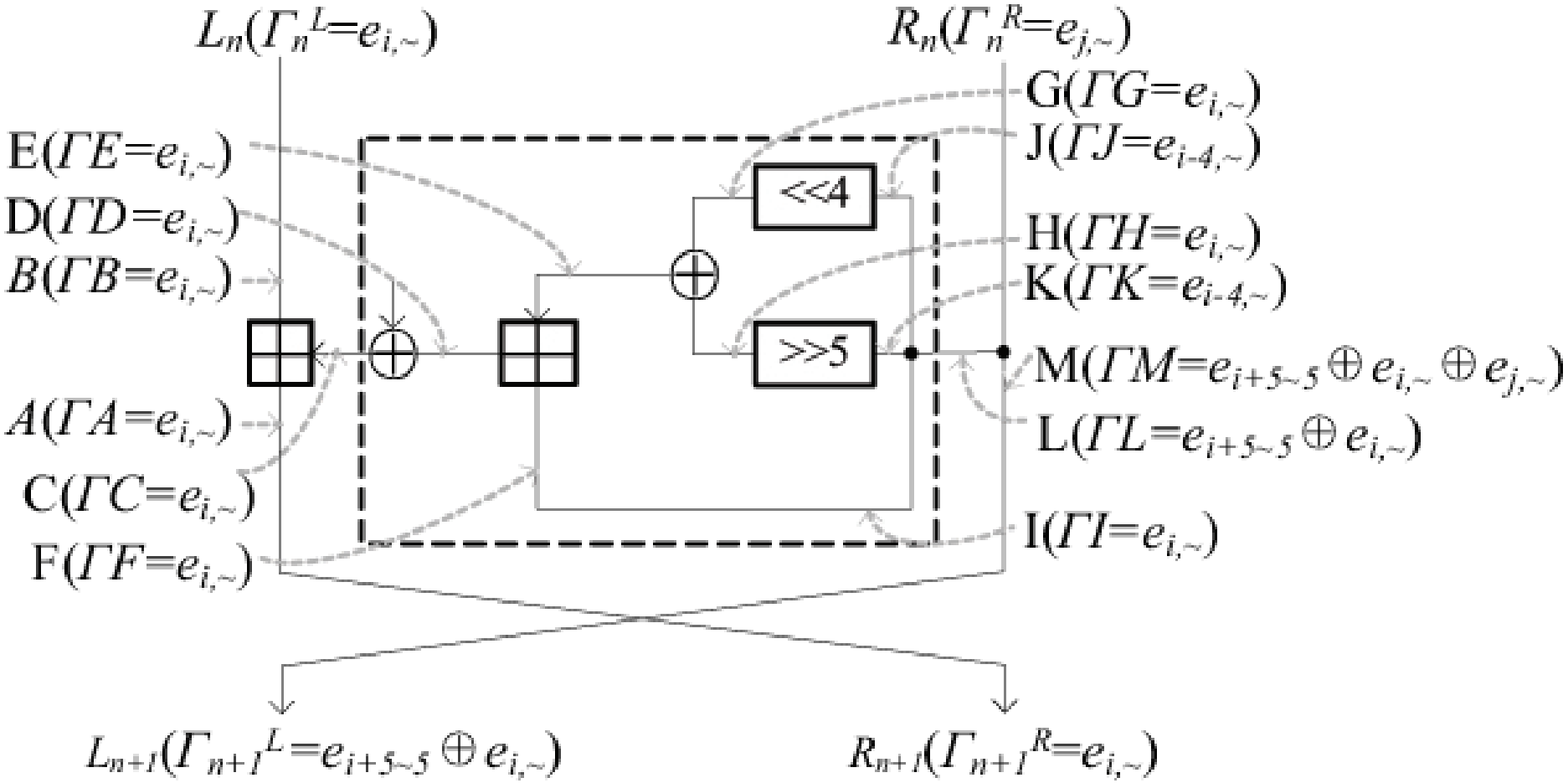
Property 1 (Modular addition)

In any linear approximation $(\Gamma x | \Gamma y) \rightarrow \Gamma z$ of the modular addition with a non-zero correlation, the most significant non-zero mask bit for $\Gamma x, \Gamma y$ and Γz is the same.

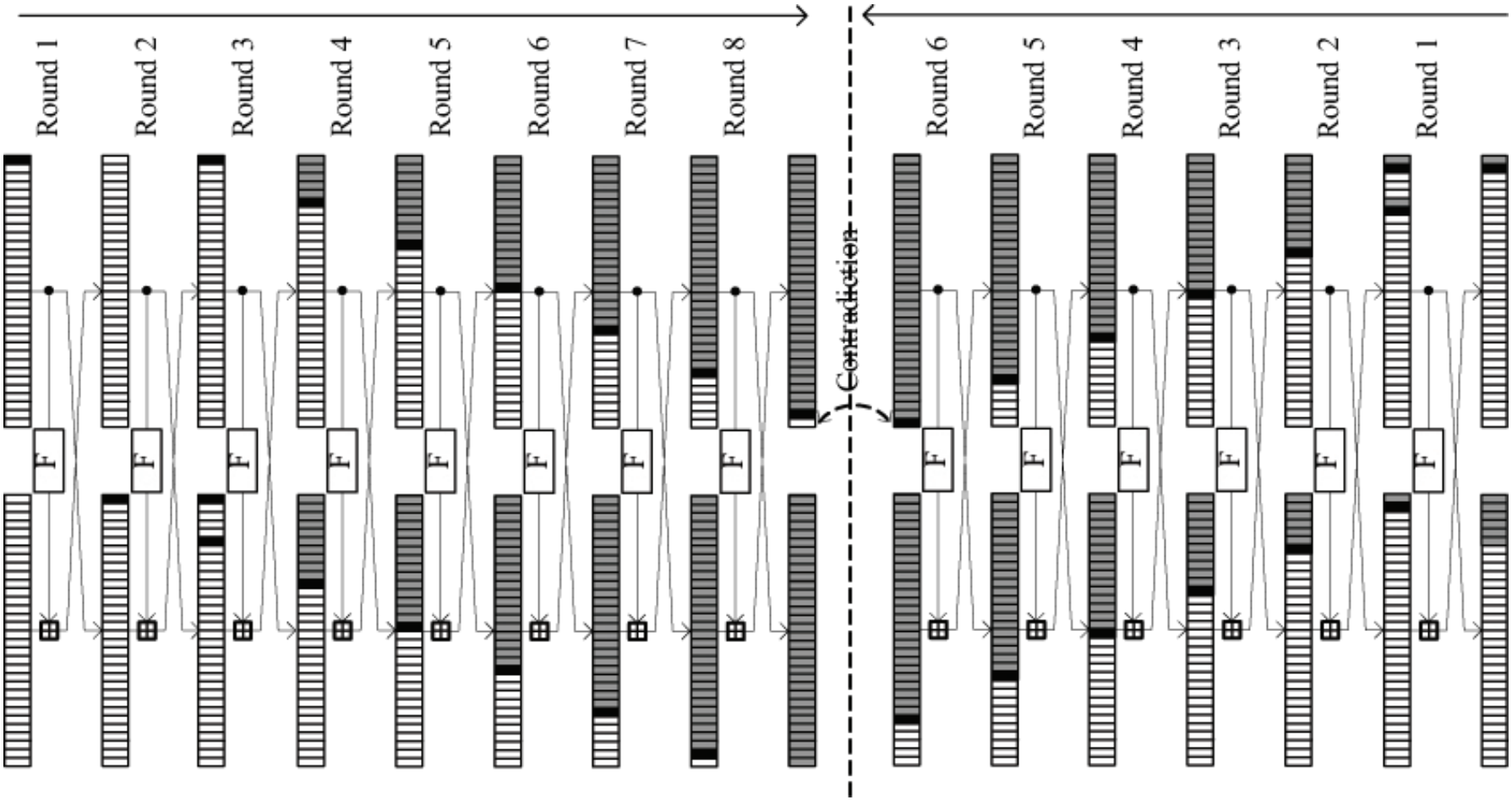
Linear Approximations for One Round of TEA



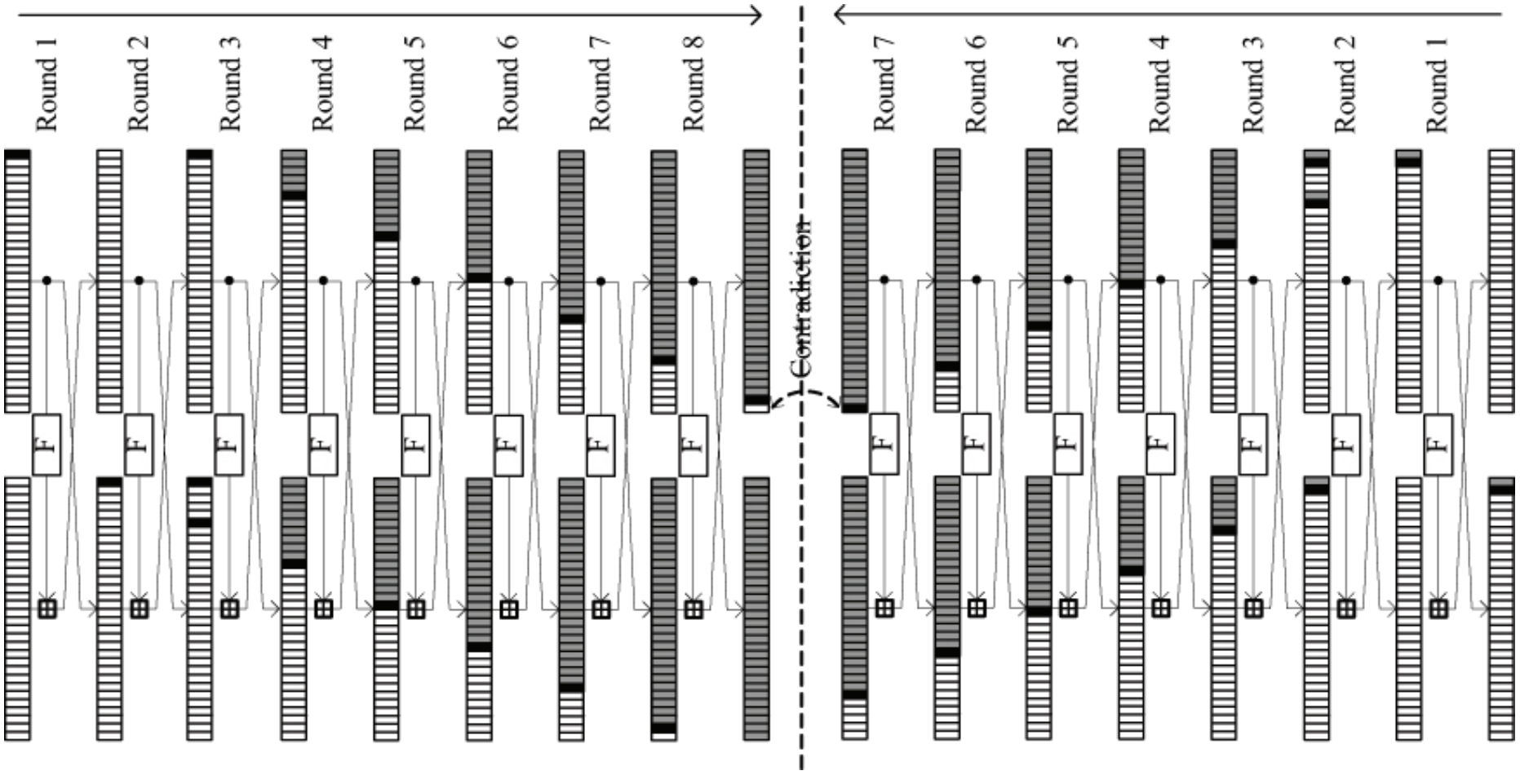
Linear Approximations for One Round of XTEA



Zero Correlation Linear Approximations of 14-R TEA/XTEA



Zero Correlation Linear Approximations 15-R TEA/XTEA



Compute N and τ:

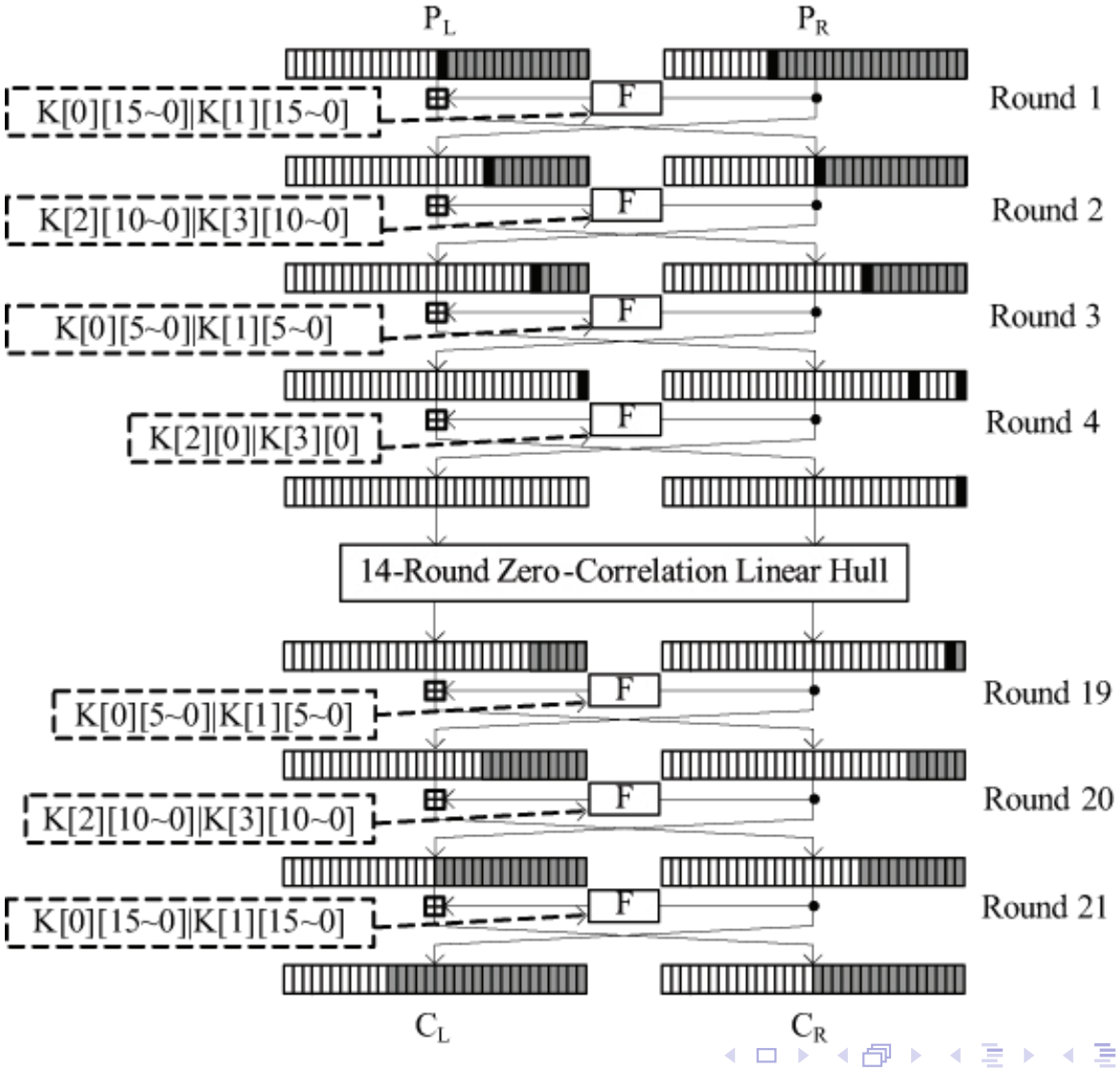
- The data complexity N:

$$N \geq \frac{2^{n+0.5}\left(z_{1-\beta_0} + z_{1-\beta_1}\right)}{\sqrt{\ell} - z_{1-\beta_1}\sqrt{2}}$$

- The threshold τ:

$$\tau = \sigma_0 \cdot z_{1-\beta_0} + \mu_0 = \frac{\sqrt{2l}}{N} \cdot z_{1-\beta_0} + \frac{l}{N}$$

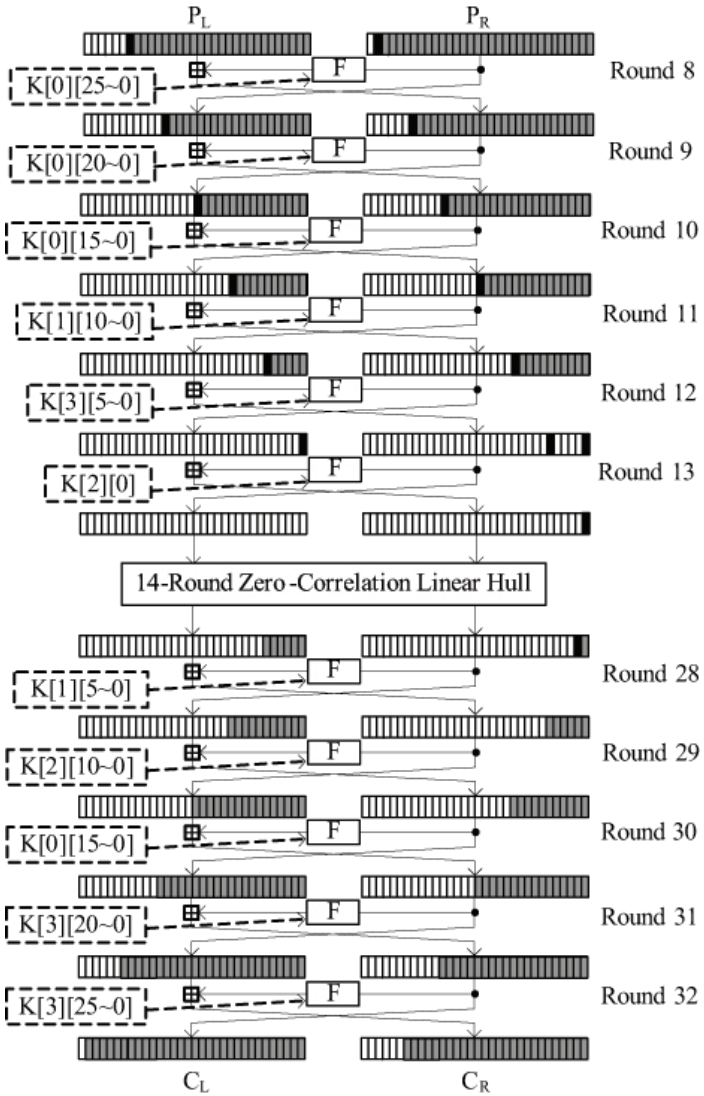
Key Recovery for 21 Rounds of TEA



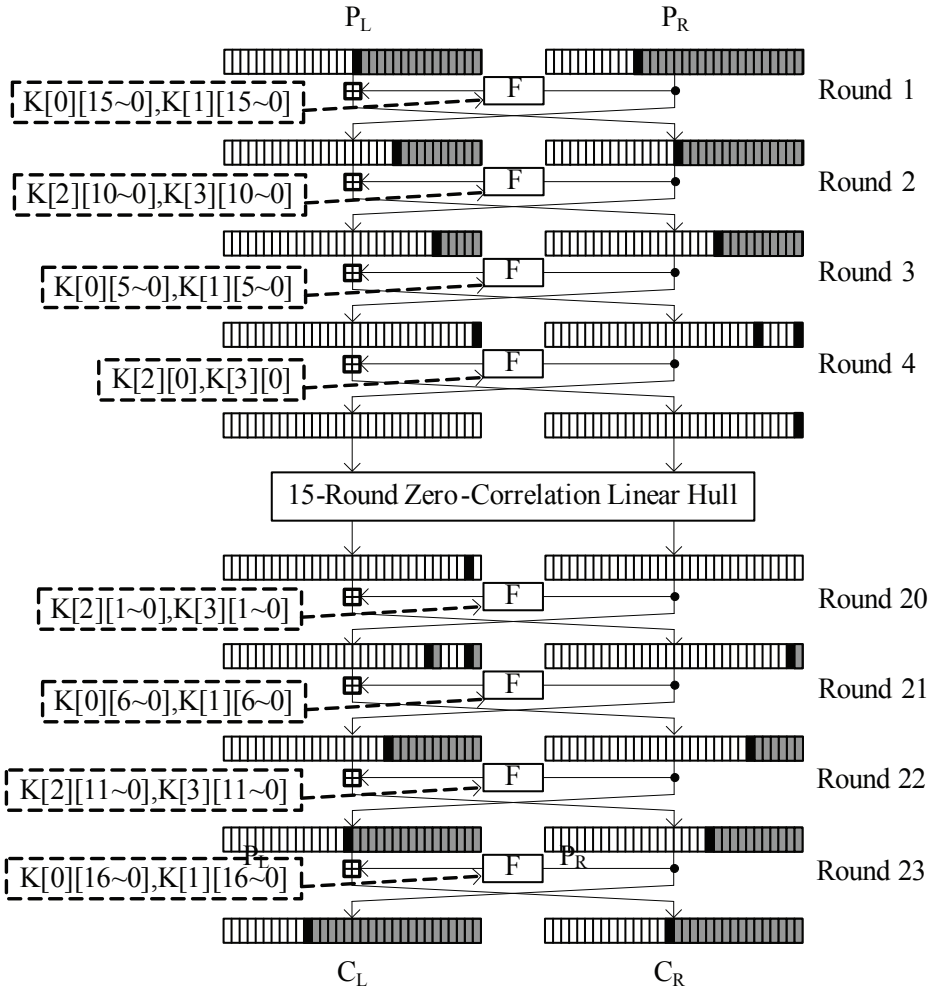
Key Recovery for 21 Rounds of TEA

1. Allocate 2^{54} counters $W[\kappa] \leftarrow 0$, $\kappa = (K_0^{15\sim0}|K_1^{15\sim0}|K_2^{10\sim0}|K_3^{10\sim0})$.
2. Guess κ:
   - 2.1 Allocate 2^9 counters $V[x] \leftarrow 0$, $x = (R_5^0|R_{19}^{1\sim0}|L_{19}^{5\sim0})$
   - 2.2 Encrypt 4 rounds and decrypt 3 rounds for N (P, C) pairs; get x and $V[x]++$.
   - 2.3 For 2^7 input and output linear masks:
     - 2.3.1 $U \leftarrow 0$.
     - 2.3.2 For 2^9 values of x, verify if the linear approximation holds. If so, $U = U + V[x]$.
     - 2.3.3 $W[\kappa] = W[\kappa] + (2 \cdot U/N - 1)^2$.
   - 2.4 If $W[\kappa] < \tau$, κ is possible right and exhaustively search all cipher keys.

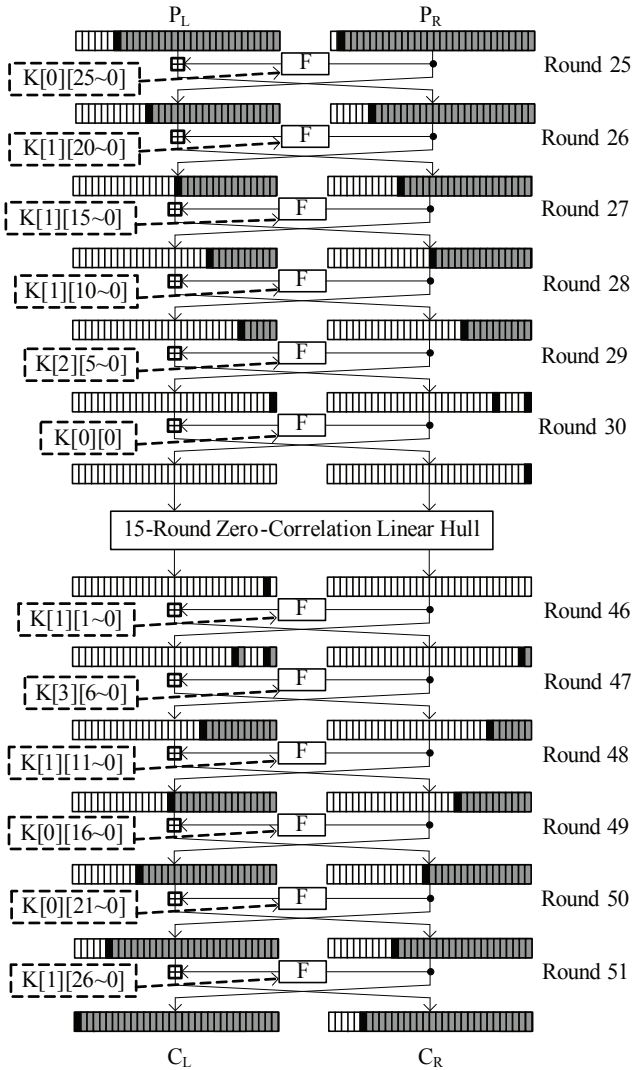
Key Recovery for 25 Rounds of XTEA



Key Recovery for 23-Round TEA with Full Codebook



Key Recovery for 27-Round XTEA with Full Codebook



Multidimensional Linear Setting

Given m linear approximations $\langle u_i, x\rangle + \langle w_i, y\rangle, \quad i = 1, \ldots, m$, $x \in \mathbb{F}_2^n$ is plaintext and $y \in \mathbb{F}_2^t$ is some part of data in the encryption process.

$$z = (z_1, \ldots, z_m), \quad z_i = \langle u_i, x\rangle + \langle w_i, y\rangle.$$

The Probability distribution of m-tuples z:

$$\Pr[z] = 2^{-m} \sum_{\gamma \in \mathbb{F}_2^m} (-1)^{\langle \gamma, z\rangle} c_\gamma.$$

c_γ: correlations of all linear approximations $\gamma \in \mathbb{F}_2^m$.

How to Make Zero-Correlation Multidimensional

- Zero-Correlation: the correlations of m linear approximation $\langle u_i, x\rangle + \langle w_i, y\rangle, \quad i = 1, \ldots, m$, and their nonzero linear combinations are zero.
- From $c_\gamma = 0$, for all $\gamma \neq 0$, get $\Pr[z] = 2^{-m} \sum_{\gamma \in \mathbb{F}_2^m} (-1)^{\langle \gamma, z\rangle} c_\gamma$, so z has uniform distribution in $\mathbb{F}_2^m$.
- Use less data than full codebook to evaluate distribution of z:
  - multivariate hypergeometric distribution with parameter $(2^n, 2^{n-m}, N)$, for the cipher data.
  - multinomial distribution with parameter $(N, 2^{-m})$ for the data drawn at random from uniform distribution on $\mathbb{F}_2^m$.

Multidimensional Distinguisher for Correlation Zero

- Initialize 2^m counters $V[z] = 0, z \in \mathbb{F}_2^m$;
- For $t = 1, \ldots, N$ do
  - draw (x_t, y_t) from cipher;
  - for $i = 1, \ldots, m$ do
    - calculate bit $z_i = u_i \cdot x_t \oplus w_i \cdot y_t$;
  - end
  - increment counter $V[z]$, where z is the vector $(z_1, \ldots, z_m)$.
- end
- compute the statistic $T = \sum_{z=0}^{2^m-1} \frac{(V[z]-N2^{-m})^2}{N2^{-m}(1-2^{-m})}$.

Multidimensional Distinguisher for Correlation Zero

Proposition 4

For sufficiently large sample size N and number ℓ of zero-correlation approximations given for the cipher, the statistic T follows a χ^2-distribution for the cipher approximately with mean and variance

$$\mu_0 = \mathrm{Exp}(T_{cipher}) = (\ell - 1)\frac{2^n - N}{2^n - 1},$$

$$\sigma_0^2 = \mathrm{Var}(T_{cipher}) = 2(\ell - 1)\left(\frac{2^n - N}{2^n - 1}\right)^2$$

and for a randomly drawn permutation with mean and variance

$$\mu_1 = \mathrm{Exp}(T_{random}) = \ell - 1, \quad \sigma_1^2 = \mathrm{Var}(T_{random}) = 2(\ell - 1).$$

Distinguishing Complexity

Corollary 1

Under the assumptions of Proposition 4, for type-I error probability α_0 (the probability to wrongfully discard the cipher), type-II error probability α_1 (the probability to wrongfully accept a randomly chosen permutation as the cipher), for an n-bit block cipher exhibiting ℓ zero-correlation linear approximations forming an $\log_2 \ell$-dimensional linear space, the distinguishing complexity N can be approximated as

$$N = \frac{2^n \left(q_{1-\alpha_0} + q_{1-\alpha_1} \right)}{\sqrt{\ell/2} - q_{1-\alpha_1}},$$

where $q_{1-\alpha_0}$ and $q_{1-\alpha_1}$ are the respective quantiles of the standard normal distribution.

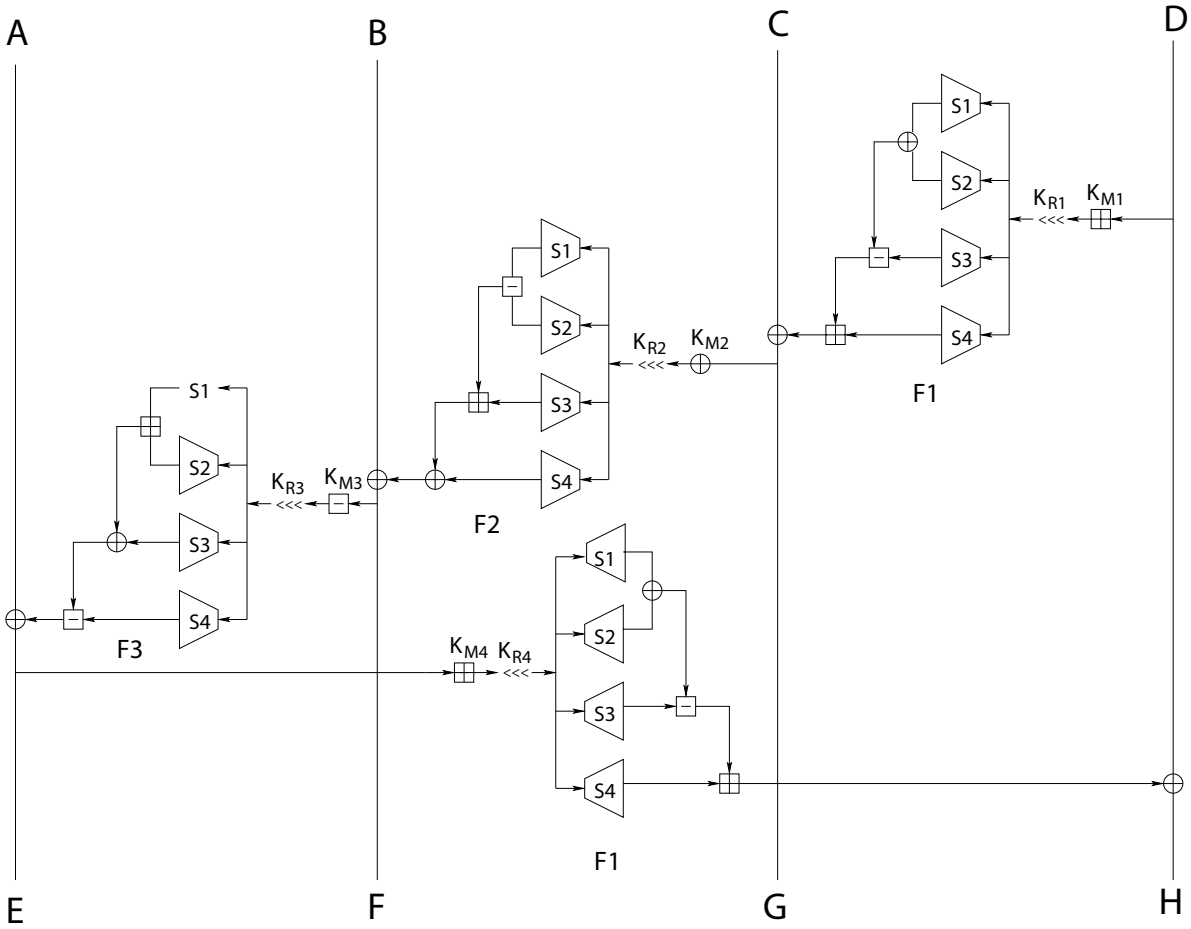
Distinguishing Complexity

- The decision threshold of $\tau = \mu_0 + \sigma_0 q_{1-\alpha_0} = \mu_1 - \sigma_1 q_{1-\alpha_1}$.
- If the statistic $T \leq \tau$, the test outputs 'cipher'.
- If the statistic $T > \tau$, the test returns 'random'.

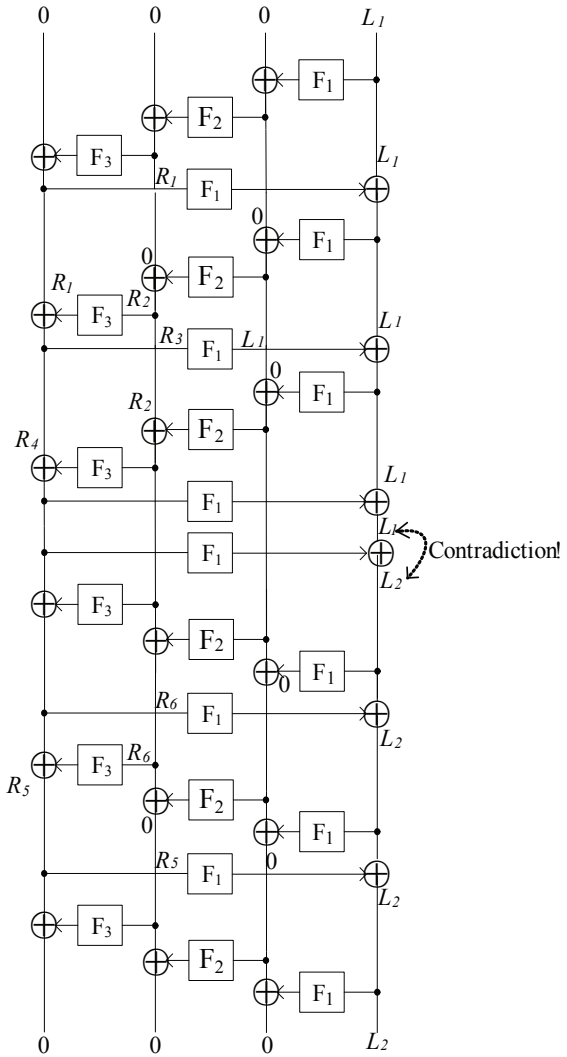
Description of CAST-256

- 48-round, 128-bit block size, key size: 128, 192 or 256 bits
- One first-round AES candidate
- 4-line generalized feistel network with 6 forward quad-rounds followed by 6 reverse quad-rounds

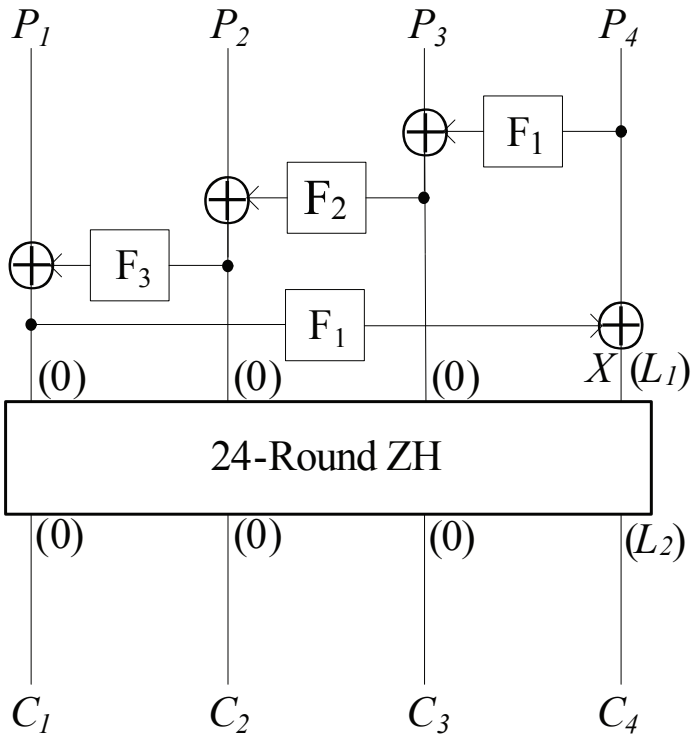
Description of CAST-256



24-round zero-correlation linear approximation for CAST-256



Key recovery for 28-round CAST-256



Key recovery for 28-round CAST-256

For each possible 148-bit subkey value $\kappa = {K_R}^{(1)} | {K_M}^{(1)}$:

1. Allocate a 64-bit global counter $V[z]$ for each of 2^{64} possible values of z and set it to 0.
2. For each of N distinct plaintext-ciphertext pairs:
   - 2.1 Partially encrypt 4 rounds and get value for $X|C_4$.
   - 2.2 Evaluate all 64 basis zero-correlation masks on $X|C_4$ and put the evaluations to z.
   - 2.3 Increment $V[z]$.
3. Compute the χ^2 statistic $T = N2^{64} \sum_{z=0}^{2^{64}-1} \left(\frac{V[z]}{N} - \frac{1}{2^{64}} \right)^2$.
4. If $T < \tau$, the subkey guess κ is a possible subkey candidate.

Summary of attacks on CAST-256

R	Key Size	Attack Type	Data	Time	Memory (bytes)	Source
16	All	BA	$2^{49.3}$CP	–	–	[Wagner 1999]
24	$192, 256$	LC	$2^{124.1}$KP	$2^{156.52}$	–	[WWH 2008]
24	256	TD	2^{24}CP	2^{244}	2^{29}	[Pestunow 2008]
28	256	MZC	$2^{98.8}$KP	$2^{244.6}$	2^{68}	[BLNW 2012]

BA: Boomerang Attack; LC: Linear Cryptanalysis;

TD: Truncated Differential; MZC: Multidimensional Zero-Correlation.

Conclusions

Conclusions

- Zero-correlation linear cryptanalysis is the counterpart of impossible differential cryptanalysis in the domain of linear cryptanalysis.
- Zero-correlation linear approximations are sometimes longer than impossible differentials
- Data complexity can be reduced to $\mathcal{O}(2^n/\sqrt{\ell})$
- Zero correlation can result in faster attacks for some ciphers

References


A. Bogdanov, M. Wang. Integral and Multidimensional Linear Distinguishers with Correlation Zero. ASIACRYPT'12, LNCS, Springer-Verlag, to appear, 2012.


A. Bogdanov, M. Wang. Zero Correlation Linear Cryptanalysis with Reduced Data Complexity. FSE'12, LNCS, Anne Canteaut (ed.), Springer-Verlag, to appear, 2012.

Thanks!