Aalto University
School of Science

Improved Parameter Estimates for Correlation and Capacity Deviates in Linear Cryptanalysis

Céline Blondeau and Kaisa Nyberg

Aalto University School of Science
kaisa.nyberg@aalto.fi

FSE 2017 TOKYO March 8, 2017

Outline

Outline

Introduction

Key-Recovery Attack: One Linear Approximation

Application to SIMON 32/64

Multidimensional/Multiple Linear Cryptanalysis

Applications to PRESENT

Data Complexity in Linear Cryptanalysis

Known Plaintext (KP) or Distinct Known Plaintext (DKP) data

Linear cryptanalysis

- data complexity upperbounded based on expected absolute value of linear correlation (or bias), or when squared, *expected linear potential* ELP

Multiple/Multidimensional linear cryptanalysis

- data complexity upperbounded based on expected capacity (sum of the ELP of linear approximations)

Variance of Correlation and Capacity

Correlation of a linear approximation varies with key

[BN 2016] Model of classical case with single dominant trail

[this paper] Model of the case with several strong trails
Application to SIMON

Capacity of multiple/multidimensional varies with key

Problem: Obtain accurate variance estimate

[BN 2016] First estimate based on [Huang et al. 2015]

[this paper] Improved variance estimates

[Vejre 2016] Multivariate cryptanalysis: without independence assumptions on linear approximations

Outline

Observed Correlation

D	sample set of size N
K	encryption key
k_r	recoverable part of the key
κ	last round key candidate
G_κ^{-1}	decryption with κ

Observed correlation

$$\hat{c}(D, K, k_r, \kappa) = \frac{2}{N}\#\{(x, y') \in D \mid u \cdot x + v \cdot G_\kappa^{-1}(y') = 0\} - 1$$

Parameters of observed correlation

$$\mathrm{Exp}_D \hat{c}(D, K, k_r, \kappa) = c(K, k_r, \kappa)$$
$$\mathrm{Var}_D \hat{c}(D, K, k_r, \kappa) = \frac{B}{N}$$

$$B = \begin{cases} 1, & \text{for KP (binomial distribution),} \\ \dfrac{2^n - N}{2^n - 1}, & \text{for DKP (hypergeometric distribution).} \end{cases}$$

It remains to determine parameters of $c(K, k_r, \kappa)$

Parameters of $c(K, k_r, \kappa)$

We expect different behaviour for $\kappa = k_r'$ (cipher) and $\kappa \neq k_r'$ (random).

Random

$c(K, k_r, \kappa)$ is a correlation of a random linear approximation
[Daemen-Rijmen 2006] $c(K, k_r, \kappa)$ is a normal deviate with

$$\begin{aligned} \mathrm{Exp}_{K,k_r,\kappa} c(K, k_r, \kappa) &= 0 \\ \mathrm{Var}_{K,k_r,\kappa} c(K, k_r, \kappa) &= 2^{-n} \end{aligned}$$

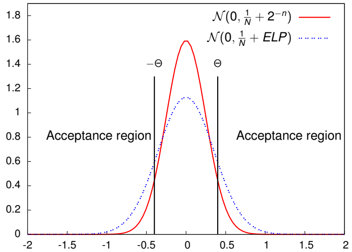
Cipher

denote $c(K) = c(K, k_r, \kappa)$

$$\begin{aligned} \mathrm{Exp}_K c(K) &= c \\ \mathrm{Exp}_K c(K)^2 &= ELP \\ \mathrm{Var}_K c(K) &= ELP - c^2 \end{aligned}$$

Case: Several Dominant Trails

Normal distribution, $c = 0$



Given advantage a and sample size N, then

$$P_S = 2 - 2\Phi\left(\sqrt{\frac{B + N2^{-n}}{B + N \cdot ELP}} \cdot \Phi^{-1}(1 - 2^{-a-1})\right)$$

where Φ is CDF of standard normal distribution

Outline

Experiments on SIMON

[Chen-Wang 2016] Attack on 20 rounds of SIMON32/64 using a 13-round linear approximation with $c \approx 0$ and experimentally determined $ELP = 2^{-18.19}$

Data	N	a	$P_S^{(exp)}$	$\mathbf{P_S^{(our)}}$	$P_S^{(bt)}$	$P_S^{(selcuk)}$	$P_S^{(min)}$	$P_S^{(max)}$
DKP	$2^{31.5}$	8	32.2%	**36.6%**	(26.7%)	(60.4%)	(23.5%)	(35.6%)
DKP	2^{32}	8	38.4%	**44.1%**	(36.8%)	(80.5%)	(24.9%)	(38.9%)
KP	2^{33}	8	30.6%	**35.3%**	61.7%	99.2%	26.1%	42.7%
KP	2^{35}	8	35.5%	**41.4%**	97.3%	100%	26.4%	43.7%
DKP	$2^{31.5}$	3	58.4%	**63%**	(87.4%)	(94.7%)	(25.9%)	(42.0%)
DKP	2^{32}	3	64.1%	**68.1%**	(94.2%)	(98.6%)	(26.2%)	(42.9%)
KP	2^{33}	3	60.5%	**62.2%**	99.5%	100%	26.4%	43.7%
KP	2^{35}	3	59.6%	**66.3%**	100%	100%	26.4%	43.7%

Summary of Linear Attack

Variance of correlation

$\mathrm{Var}_K c(K) = ELP - (\mathrm{Exp}_K c(K))^2$

[Selçuk 2008] & [Bogdanov-Tischhauser 2013]

$ELP = (\mathrm{Exp}_K c(K))^2 \Rightarrow \mathrm{Var}_K c(K) = 0$
that is, all keys behave as average.

[BN 2016]

$\mathrm{Var}_K c(K) > 0$ and $\mathrm{Exp}_K c(K) = \pm c$ where $c \neq 0$ (one dominant trail)

[this paper]

$\mathrm{Var}_K c(K) > 0$ and $\mathrm{Exp}_K c(K) \approx 0 \Rightarrow \mathrm{Var}_K c(K) \approx ELP$

Strong trails always count

Estimating *ELP*

$$c(K) = \sum_{\tau} (-1)^{\tau \cdot K} c(u, \tau, v)$$

where $c(u, \tau, v)$ is *trail correlation* of trail τ

[Bogdanov-Tischhauser 2013] Set $\mathcal{S}$ of identified trails. Write

$$c(K) = \sum_{\tau \in \mathcal{S}} (-1)^{\tau \cdot K} c(u, \tau, v) + R(K)$$

where $R(K)$ is assumed to behave like random.

$$ELP \approx \sum_{\tau \in \mathcal{S}} c(u, \tau, v)^2 + 2^{-n}.$$

Accuracy depends on the choice of $\mathcal{S}$

Outline

Introduction

Key-Recovery Attack: One Linear Approximation

Application to SIMON 32/64

Multidimensional/Multiple Linear Cryptanalysis

Applications to PRESENT

Attack Statistic

Given ℓ linear approximations, the attack statistic is computed as

$$T(D, K, k_r, \kappa) = N \sum_{j=1}^{\ell} \hat{c}_j(D, K, k_r, \kappa)^2.$$

In multidimensional attack the linear approximations form a linear subspace and the attack statistic can also be computed as

$$T(D, K, k_r, \kappa) = \sum_{\eta=0}^{\ell} \frac{(V[\eta] - N2^{-s})^2}{N2^{-s}},$$

where $V[\eta]$ corresponds to the number of occurrences of the value η of the observed data distribution of dimension s where $2^s = \ell + 1$.

Parameters of $T(D, K, k_r, \kappa)$

Given in terms of capacity $C(K)$ (= sum of squared correlations):

Cipher

[BN2016]

$\mathrm{Exp}_{D,K} T(D, K, k_r, \kappa) = B\ell + N \cdot \mathrm{Exp}_K C(K)$
$\mathrm{Var}_{D,K} T(D, K, k_r, \kappa) = 2B^2\ell + 4BN \cdot \mathrm{Exp}_K C(K) + N^2 \cdot \mathrm{Var}_K C(K)$

Multiple LC: assumption about independence of correlations $\hat{c}_j(D, K, k_r)$ for each fixed K, k_r

Multidimensional LC: No assumption

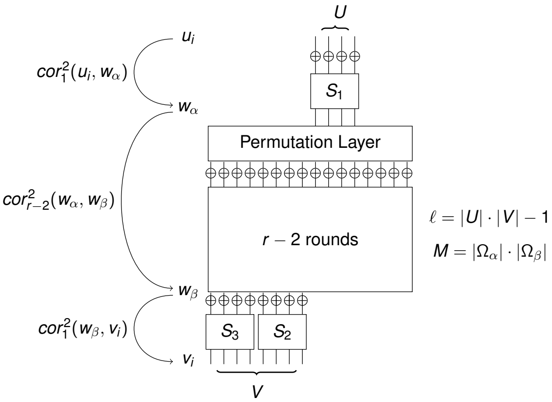
Random

$\mathrm{Exp}_{D,K}\,(T(D, K, k_r, \kappa)) = B\ell + N2^{-n}\ell$

$\mathrm{Var}_{D,K}\,(T(D, K, k_r, \kappa)) = \frac{2}{\ell}\,(B\ell + N2^{-n}\ell)^2$
non-central χ^2 distribution

Multidimensional Trail for SPN Cipher

After encryption/decryption with key candidate, data pairs in $U \times V$



bijective S-boxes $\Rightarrow$

capacity on $U \times V$ is equal to capacity on $S_1(U) \times (S_2||S_3)^{-1}(V) \Rightarrow$

two nonlinear rounds for free

Capacity of Multidimensional Approximation

$S_1(U) \times (S_2||S_3)^{-1}(V)$ has a certain capacity $C(K)$.

In practice, it can be estimated by considering a subset of M strong linear approximations

$$(u_j, v_j) \in S_1(U) \times (S_2||S_3)^{-1}(V)$$

and assume all other linear approximations are random

In general, write

$$C(K) = \sum_{j=1}^{M} c(u_j, v_j)(K)^2 + \sum_{j=M+1}^{\ell} \rho_j^2$$

where ρ_j are correlations of random linear approximations.

Estimating Expected Capacity

Denote $ELP_j = \text{Exp}\left(c(u_j, k_j)^2\right)$. Then

$$\text{Exp}_K C(K) = \sum_{j=1}^{\ell} ELP_j.$$

Subset of linear approximations, numbered as $j = 1, \ldots, M$, with identified sets $\mathcal{S}_j$ of strong linear trails,
and the remaining are assumed to be random:

$$\text{Exp}_K C(K) \approx \sum_{j=1}^{M} ELP_j + (\ell - M)2^{-n}.$$

By $ELP_j \approx \sum_{\tau \in \mathcal{S}_j} c(u_j, \tau, v_j)^2 + 2^{-n}$, we obtain

$$C = \text{Exp}_K C(K) \approx \sum_{j=1}^{M} \sum_{\tau \in \mathcal{S}_j} c(u_j, \tau, v_j)^2 + \ell 2^{-n}.$$

Estimating Variance of Capacity

Starting from

$$C(K) = \sum_{j=1}^{M} c(u_j, v_j)(K)^2 + \sum_{j=M+1}^{\ell} c(u_j, v_j)(K)^2,$$

where the linear approximations (u_j, v_j), $j = M + 1, \ldots, \ell$, are random, we further assume:

Assumption: Correlations $c(u_j, v_j)(K)$, $j = 1, \ldots, M$, are independent and have expected value equal to zero.

Then

$$\mathrm{Var}_K C(K) = \sum_{j=1}^{M} 2ELP_j^2 + (\ell - M)2^{1-2n}.$$

Outline

Introduction

Key-Recovery Attack: One Linear Approximation

Application to SIMON 32/64

Multidimensional/Multiple Linear Cryptanalysis

Applications to PRESENT

Five Round SMALLPRESENT-[4]

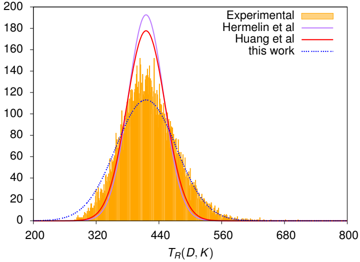


Figure : Comparison between the experimental distribution of $T(D, K, k_r, \kappa)$ and normal distributions with mean $\ell + NC$ and different variances. Left with $N = 2^{14}$. Right with $N = 2^{15}$.

Multidimensional Linear Attack on PRESENT

attacked rounds r	$\sum_{j=1}^{M} \sum_{\tau \in \mathcal{S}_j} c(u_j, \tau, v_j)^2$ (over $r-2$ rounds)	C	N	Success probability Cho 2010	Success probability This paper KP
24	$2^{-50.16}$	$2^{-49.95}$	$2^{58.5}$	97%	86%
25	$2^{-52.77}$	$2^{-51.80}$	2^{61}	94%	74%
26	$2^{-55.38}$	$2^{-52.60}$	$2^{63.8}$	98%	51%

Table : Multidimensional linear attacks on PRESENT. Success probability for advantage a of 8 bits.

Remark. Using DKP, the success probability is higher, e.g., for 26 round attack we get $P_S = 90\%$.

Conclusions

- Focus on linear approximations with several strong trails
- Improved formula of P_S of linear key recovery attack
- New better and simpler model of the attack on SIMON
- Parameters of test statistic in multiple/multidimensional cryptanalysis
- Improved estimates of expected value and variance of capacity

Thank you for your attention!