Multivariate Profiling of Hulls for Linear Cryptanalysis

Andrey Bogdanov Elmar Tischhauser **Philip S. Vejre**
{anbog,ewti,psve}@dtu.dk
Technical University of Denmark

March 7, 2018

DTU Compute
Department of Applied Mathematics and Computer Science

Linear Cryptanalysis in a Nutshell

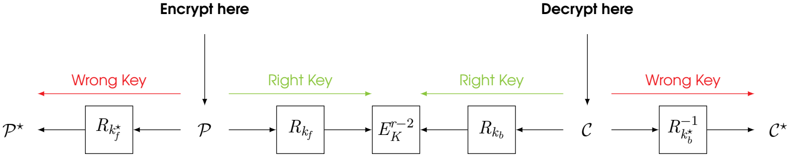
- Introduced in 1993 by Matsui to analyse DES.
- Uses linear approximations (α, β) over E_K with large absolute correlation defined by

$$C^K_{\alpha,\beta} = 2 \cdot \Pr(\langle \alpha, x \rangle \oplus \langle \beta, E_K(x) \rangle = 0) - 1,$$

as a distinguisher.

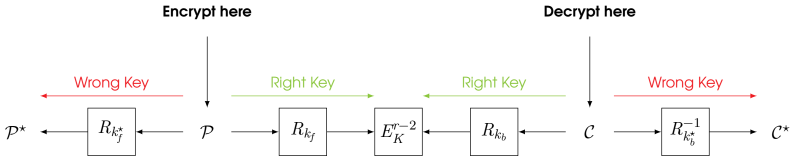
Linear Cryptanalysis in a Nutshell

- Key-recovery through Matsui's Algorithm 2.



Linear Cryptanalysis in a Nutshell

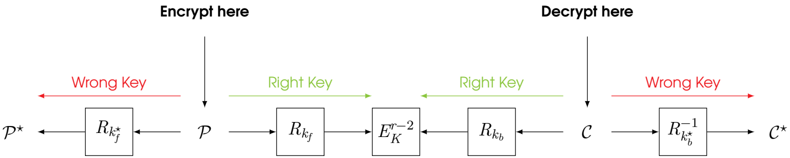
- Key-recovery through Matsui's Algorithm 2.



- High absolute correlation $\longrightarrow$ Likely right key guess.
- Low absolute correlation $\longrightarrow$ Likely wrong key guess.

Linear Cryptanalysis in a Nutshell

- Key-recovery through Matsui's Algorithm 2.



- High absolute correlation $\longrightarrow$ Likely right key guess.
- Low absolute correlation $\longrightarrow$ Likely wrong key guess.
- Central question when estimating attack complexity:

How is the correlation distributed for right and wrong key guesses?

Key Dependent Correlations

- The key-dependent correlation can be expressed as (Daemen, Rijmen, 2007)

$$C^K_{\alpha,\beta} = \sum_{U=(\alpha,\ldots,\beta)} (-1)^{s_{U,K}} |C^K_U|.$$

Key Dependent Correlations

- The key-dependent correlation can be expressed as (Daemen, Rijmen, 2007)

$$C^K_{\alpha,\beta} = \sum_{U=(\alpha,\ldots,\beta)} (-1)^{s_{U,K}} |C^K_U|.$$

- First works assumed that

$$\begin{aligned} |C^K_{\alpha,\beta}| &= 0 && \text{for a wrong key guess,} \\ |C^K_{\alpha,\beta}| &= |C^K_U| && \text{for a right key guess.} \end{aligned}$$

Key Dependent Correlations

- The key-dependent correlation can be expressed as (Daemen, Rijmen, 2007)

$$C^K_{\alpha,\beta} = \sum_{U=(\alpha,\ldots,\beta)} (-1)^{s_{U,K}} |C^K_U|.$$

- First works assumed that

$$\begin{aligned} |C^K_{\alpha,\beta}| &= 0 && \text{for a wrong key guess,} \\ |C^K_{\alpha,\beta}| &= |C^K_U| && \text{for a right key guess.} \end{aligned}$$

- Daemen and Rijmen (2007) show that $C^K_{\alpha,\beta} \sim \mathcal{N}(0, 2^{-n})$ for an ideal cipher.

Key Dependent Correlations

- The key-dependent correlation can be expressed as (Daemen, Rijmen, 2007)

$$C_{\alpha,\beta}^{K} = \sum_{U=(\alpha,\ldots,\beta)} (-1)^{s_{U,K}} |C_U^K|.$$

- First works assumed that

$$\begin{aligned} |C_{\alpha,\beta}^{K}| &= 0 && \text{for a wrong key guess,} \\ |C_{\alpha,\beta}^{K}| &= |C_U^K| && \text{for a right key guess.} \end{aligned}$$

- Daemen and Rijmen (2007) show that $C_{\alpha,\beta}^{K} \sim \mathcal{N}(0, 2^{-n})$ for an ideal cipher.
- $|C_{\alpha,\beta}^{K}|$ is not constant for ciphers with a strong linear hull effect.

Using Multiple Approximations

- Multiple Linear Cryptanalysis (Kaliski and Robshaw (1994), Biryukov *et al.* (2004)):
  - Uses a set of M approximations.
  - Assumes statistical independence of correlations.

Using Multiple Approximations

- Multiple Linear Cryptanalysis (Kaliski and Robshaw (1994), Biryukov *et al.* (2004)):
  - Uses a set of M approximations.
  - Assumes statistical independence of correlations.
- Multidimensional Linear Cryptanalysis (Hermelin *et al.* (2008)):
  - Uses all $2^m - 1$ approximations in an m-dimensional subspace.
  - Does not assume statistical independence.

Using Multiple Approximations

- Multiple Linear Cryptanalysis (Kaliski and Robshaw (1994), Biryukov *et al.* (2004)):
  - Uses a set of M approximations.
  - Assumes statistical independence of correlations.
- Multidimensional Linear Cryptanalysis (Hermelin *et al.* (2008)):
  - Uses all $2^m - 1$ approximations in an m-dimensional subspace.
  - Does not assume statistical independence.
- Both use the *capacity* as measure of distinguishing power:

$$\mathcal{C}^K = \sum (C^K_{\alpha_i,\beta_i})^2$$

Using Multiple Approximations

- Multiple Linear Cryptanalysis (Kaliski and Robshaw (1994), Biryukov *et al.* (2004)):
  - Uses a set of M approximations.
  - Assumes statistical independence of correlations.
- Multidimensional Linear Cryptanalysis (Hermelin *et al.* (2008)):
  - Uses all $2^m - 1$ approximations in an m-dimensional subspace.
  - Does not assume statistical independence.
- Both use the *capacity* as measure of distinguishing power:

$$\mathcal{C}^K = \sum (C^K_{\alpha_i,\beta_i})^2 = \sum \frac{(\eta_i^K - 2^{-m})^2}{2^{-m}}$$

Using Multiple Approximations

- Multiple Linear Cryptanalysis (Kaliski and Robshaw (1994), Biryukov *et al.* (2004)):
  - Uses a set of M approximations.
  - Assumes statistical independence of correlations.
- Multidimensional Linear Cryptanalysis (Hermelin *et al.* (2008)):
  - Uses all $2^m - 1$ approximations in an m-dimensional subspace.
  - Does not assume statistical independence.
- Both use the *capacity* as measure of distinguishing power:

$$\mathcal{C}^K = \sum (C^K_{\alpha_i,\beta_i})^2 = \sum \frac{(\eta_i^K - 2^{-m})^2}{2^{-m}}$$

- Difficult to analyse if the multivariate distributions of the C_i^K or η_i^K are not "simple".

Key Dependent Capacity

	Key dependent capacity	Data dependent capacity	Right-key case	Wrong-key case	Practical distribution estimates	Arbitrary key-schedule	Explicit capacity distribution	Free approximation choice

Key Dependent Capacity

	Key dependent capacity	Data dependent capacity	Right-key case	Wrong-key case	Practical distribution estimates	Arbitrary key-schedule	Explicit capacity distribution	Free approximation choice
Huang *et al.* (2015)	✓		✓				✓	

Key Dependent Capacity

	Key dependent capacity	Data dependent capacity	Right-key case	Wrong-key case	Practical distribution estimates	Arbitrary key-schedule	Explicit capacity distribution	Free approximation choice
Huang *et al.* (2015)	✓	✗	✓	✗	✗	✗	✓	

Key Dependent Capacity

	Key dependent capacity	Data dependent capacity	Right-key case	Wrong-key case	Practical distribution estimates	Arbitrary key-schedule	Explicit capacity distribution	Free approximation choice
Huang *et al.* (2015)	✓	✗	✓	✗	✗	✗	✓	?

Key Dependent Capacity

	Key dependent capacity	Data dependent capacity	Right-key case	Wrong-key case	Practical distribution estimates	Arbitrary key-schedule	Explicit capacity distribution	Free approximation choice
Huang *et al.* (2015)	✓	✗	✓	✗	✗	✗	✓	?
Blondeau and Nyberg (2017)	✓	✓	✓	✓			✓	

Key Dependent Capacity

	Key dependent capacity	Data dependent capacity	Right-key case	Wrong-key case	Practical distribution estimates	Arbitrary key-schedule	Explicit capacity distribution	Free approximation choice
Huang *et al.* (2015)	✓	✗	✓	✗	✗	✗	✓	?
Blondeau and Nyberg (2017)	✓	✓	✓	✓	✗	✗	✓	

Key Dependent Capacity

	Key dependent capacity	Data dependent capacity	Right-key case	Wrong-key case	Practical distribution estimates	Arbitrary key-schedule	Explicit capacity distribution	Free approximation choice
Huang *et al.* (2015)	✓	✗	✓	✗	✗	✗	✓	?
Blondeau and Nyberg (2017)	✓	✓	✓	✓	✗	✗	✓	?

Key Dependent Capacity

	Key dependent capacity	Data dependent capacity	Right-key case	Wrong-key case	Practical distribution estimates	Arbitrary key-schedule	Explicit capacity distribution	Free approximation choice
Huang *et al.* (2015)	✓	✗	✓	✗	✗	✗	✓	?
Blondeau and Nyberg (2017)	✓	✓	✓	✓	✗	✗	✓	?
Blondeau and Nyberg (2016)	✓	✓	✓	✓	✓			✓

Key Dependent Capacity

	Key dependent capacity	Data dependent capacity	Right-key case	Wrong-key case	Practical distribution estimates	Arbitrary key-schedule	Explicit capacity distribution	Free approximation choice
Huang *et al.* (2015)	✓	✗	✓	✗	✗	✗	✓	?
Blondeau and Nyberg (2017)	✓	✓	✓	✓	✗	✗	✓	?
Blondeau and Nyberg (2016)	✓	✓	✓	✓	✓	✗	✗	✓

About Independence Assumptions

- Most ciphers do not have independent round-keys.
  - We demonstrate that the key-schedule affects the joint correlation distribution, and that it is not necessarily multivariate normal.

About Independence Assumptions

- Most ciphers do not have independent round-keys.
  - We demonstrate that the key-schedule affects the joint correlation distribution, and that it is not necessarily multivariate normal.
- Nyberg recently demonstrated a connection between linear and statistical dependence of correlations.
  - Poses a problem for the wrong-key model and signal/noise decomposition when using linearly dependent approximations.

About Independence Assumptions

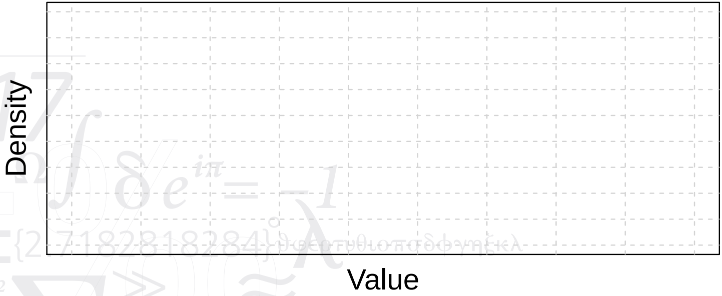
- Most ciphers do not have independent round-keys.
  - We demonstrate that the key-schedule affects the joint correlation distribution, and that it is not necessarily multivariate normal.
- Nyberg recently demonstrated a connection between linear and statistical dependence of correlations.
  - Poses a problem for the wrong-key model and signal/noise decomposition when using linearly dependent approximations.

$\boxed{\text{We propose Multivariate Linear Cryptanalysis as a next step}}$

Multivariate Linear Cryptanalysis – Three Steps

The Main Model: Arbitrary Right-Key Distribution

- We consider a set of M linearly independent approximations.

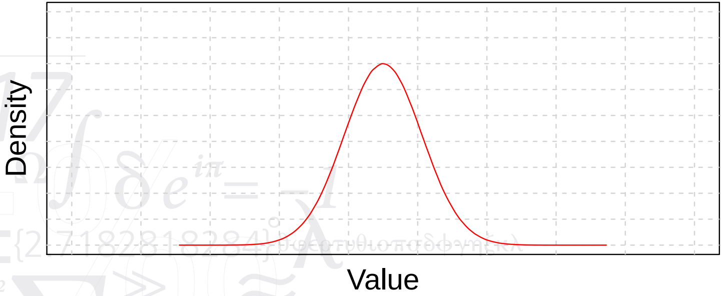


Multivariate Linear Cryptanalysis – Three Steps

The Main Model: Arbitrary Right-Key Distribution

- We consider a set of M linearly independent approximations.
- Wrong-key model:

$$\boldsymbol{C}^K \sim \mathcal{N}_M(\mathbf{0}, \boldsymbol{\Sigma}^\delta) \quad \text{with } \boldsymbol{\Sigma}^\delta = \text{diag}(2^{-n}).$$



Multivariate Linear Cryptanalysis – Three Steps

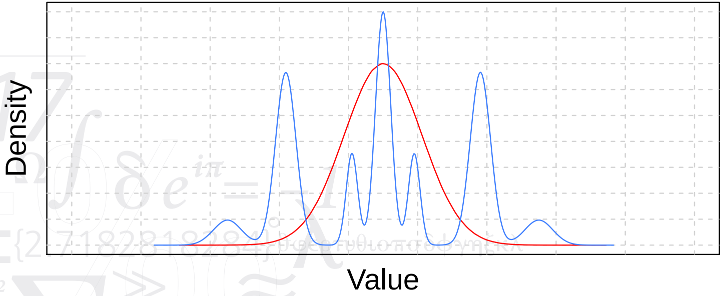
The Main Model: Arbitrary Right-Key Distribution

- We consider a set of M linearly independent approximations.
- Wrong-key model:

$$\boldsymbol{C}^K \sim \mathcal{N}_M(\mathbf{0}, \boldsymbol{\Sigma}^\delta) \quad \text{with } \boldsymbol{\Sigma}^\delta = \mathrm{diag}(2^{-n}).$$

- Right-key model:

$$\boldsymbol{C}^K \sim \mathcal{D}_M.$$



Multivariate Linear Cryptanalysis – Three Steps

- Bogdanov and Tischhauser (2013) proposed signal/noise decomposition when only part of the linear hull is known.
- We find a set of linear trails called the signal $\mathcal{S}$.

Multivariate Linear Cryptanalysis – Three Steps

- Bogdanov and Tischhauser (2013) proposed signal/noise decomposition when only part of the linear hull is known.
- We find a set of linear trails called the signal $\mathcal{S}$.
- Profile the signal distribution $\mathcal{D}^\star$:

$$C_{\alpha,\beta}^{K\star} = \sum_{U \in \mathcal{S}} (-1)^{s_{U,K}} |C_U^K|.$$

Multivariate Linear Cryptanalysis – Three Steps

- Bogdanov and Tischhauser (2013) proposed signal/noise decomposition when only part of the linear hull is known.
- We find a set of linear trails called the signal $\mathcal{S}$.
- Profile the signal distribution $\mathcal{D}^\star$:

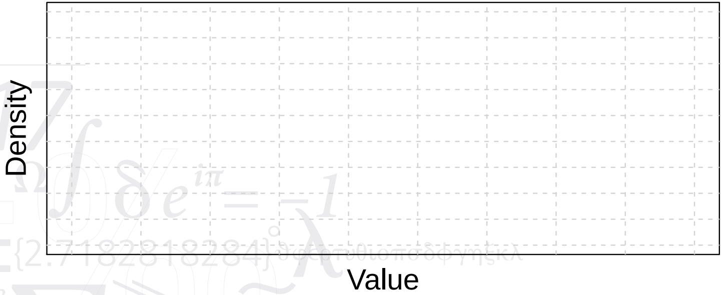
$$C_{\alpha,\beta}^{K\star} = \sum_{U \in \mathcal{S}} (-1)^{s_{U,K}} |C_U^K|.$$

- The rest of the hull is modeled as noise:

$$\mathcal{N}(0, 2^{-n}).$$

Multivariate Linear Cryptanalysis – Three Steps

The Practical Model: Profiling with Signal/Noise Decomposition

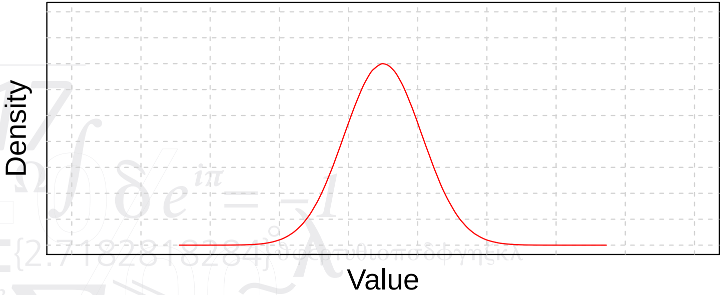


Multivariate Linear Cryptanalysis – Three Steps

The Practical Model: Profiling with Signal/Noise Decomposition

- Wrong-key model:

$$\boldsymbol{C}^K \sim \mathcal{N}_M(\mathbf{0}, \boldsymbol{\Sigma}^\delta) \quad \text{with } \boldsymbol{\Sigma}^\delta = \text{diag}(2^{-n}).$$



Multivariate Linear Cryptanalysis – Three Steps

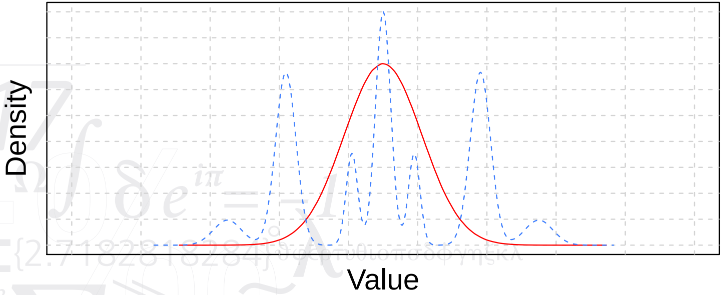
The Practical Model: Profiling with Signal/Noise Decomposition

- Wrong-key model:

$$\boldsymbol{C}^K \sim \mathcal{N}_M(\mathbf{0}, \boldsymbol{\Sigma}^\delta) \quad \text{with } \boldsymbol{\Sigma}^\delta = \text{diag}(2^{-n}).$$

- Right-key model:

$$\boldsymbol{C}^K \sim \mathcal{D}_M^\star$$



Multivariate Linear Cryptanalysis – Three Steps

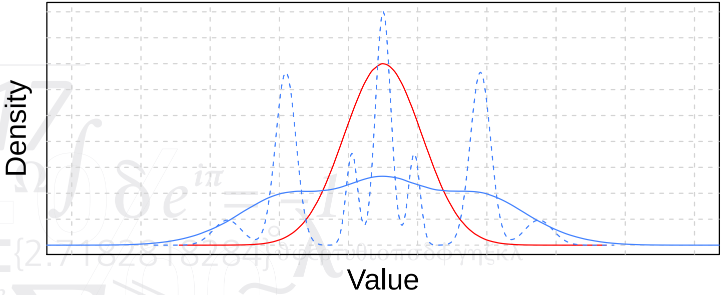
The Practical Model: Profiling with Signal/Noise Decomposition

- Wrong-key model:

$$\boldsymbol{C}^K \sim \mathcal{N}_M(\mathbf{0}, \boldsymbol{\Sigma}^\delta) \quad \text{with } \boldsymbol{\Sigma}^\delta = \text{diag}(2^{-n}).$$

- Right-key model:

$$\boldsymbol{C}^K \sim \mathcal{D}^\star_M + \mathcal{N}_M(\mathbf{0}, \boldsymbol{\Sigma}^\delta).$$



Multivariate Linear Cryptanalysis – Three Steps

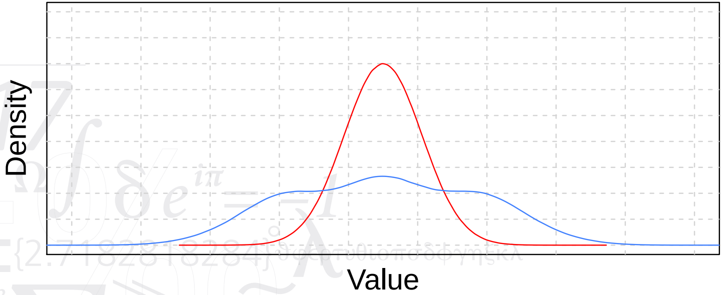
The Practical Model: Profiling with Signal/Noise Decomposition

- Wrong-key model:

$$\boldsymbol{C}^K \sim \mathcal{N}_M(\mathbf{0}, \boldsymbol{\Sigma}^\delta) \quad \text{with } \boldsymbol{\Sigma}^\delta = \text{diag}(2^{-n}).$$

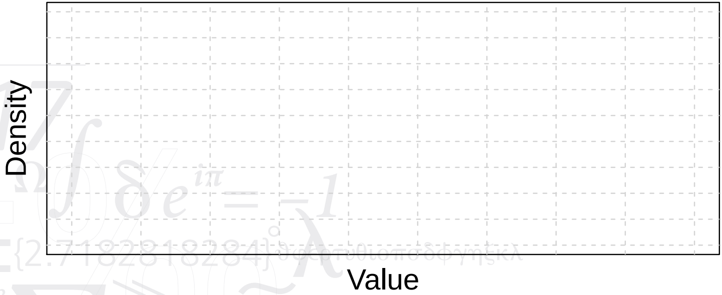
- Right-key model:

$$\boldsymbol{C}^K \sim \mathcal{D}^\star_M + \mathcal{N}_M(\mathbf{0}, \boldsymbol{\Sigma}^\delta).$$



Multivariate Linear Cryptanalysis – Three Steps

The Attack Model: Dealing with Undersampling

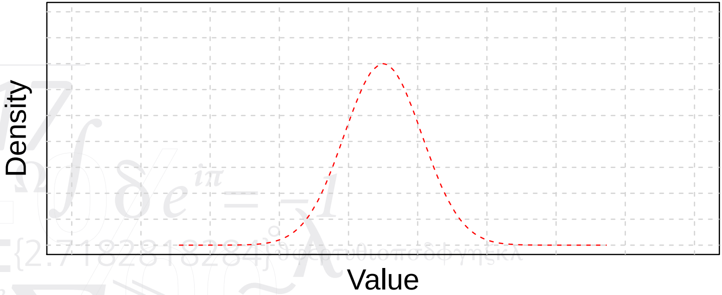


Multivariate Linear Cryptanalysis – Three Steps

The Attack Model: Dealing with Undersampling

- Wrong-key model:

$$C^K \sim \mathcal{N}_M(\mathbf{0}, \mathbf{\Sigma}^\delta \qquad)$$

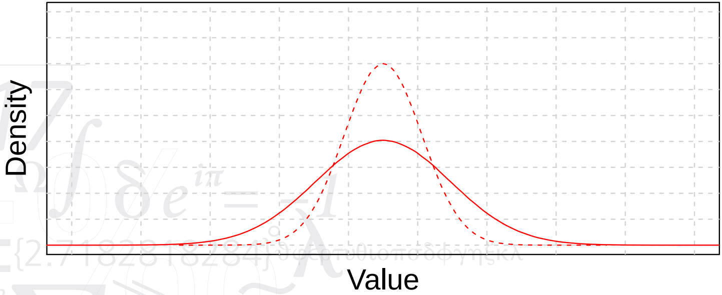


Multivariate Linear Cryptanalysis – Three Steps

The Attack Model: Dealing with Undersampling

- Wrong-key model:

$$\boldsymbol{C}^K \sim \mathcal{N}_M(\mathbf{0}, \boldsymbol{\Sigma}^\delta + \boldsymbol{\Sigma}^N) \quad \text{with } \boldsymbol{\Sigma}^N = \mathrm{diag}(N^{-1}).$$



Multivariate Linear Cryptanalysis – Three Steps

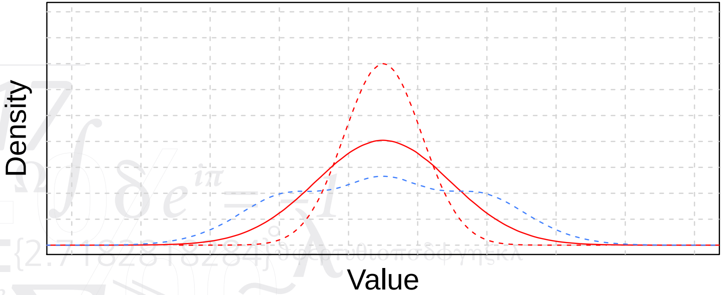
The Attack Model: Dealing with Undersampling

- Wrong-key model:

$$C^K \sim \mathcal{N}_M(\mathbf{0}, \mathbf{\Sigma}^\delta + \mathbf{\Sigma}^N) \quad \text{with } \mathbf{\Sigma}^N = \text{diag}(N^{-1}).$$

- Right-key model:

$$C^K \sim \mathcal{D}^\star_M + \mathcal{N}_M(\mathbf{0}, \mathbf{\Sigma}^\delta \qquad).$$



Multivariate Linear Cryptanalysis – Three Steps

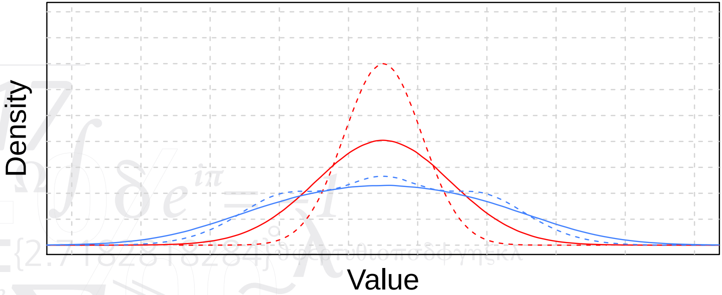
The Attack Model: Dealing with Undersampling

- Wrong-key model:

$$\boldsymbol{C}^K \sim \mathcal{N}_M(\mathbf{0}, \boldsymbol{\Sigma}^\delta + \boldsymbol{\Sigma}^N) \quad \text{with } \boldsymbol{\Sigma}^N = \text{diag}(N^{-1}).$$

- Right-key model:

$$\boldsymbol{C}^K \sim \mathcal{D}_M^\star + \mathcal{N}_M(\mathbf{0}, \boldsymbol{\Sigma}^\delta + \boldsymbol{\Sigma}^N).$$



Multivariate Linear Cryptanalysis – Three Steps

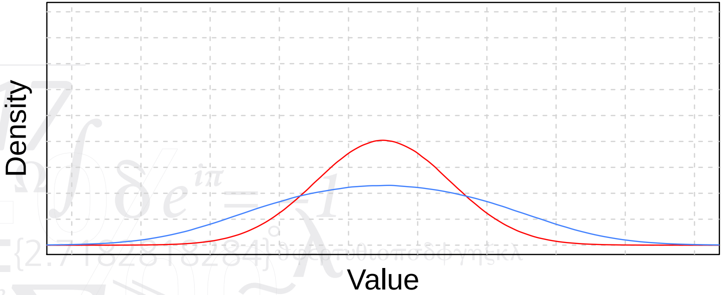
The Attack Model: Dealing with Undersampling

- Wrong-key model:

$$\boldsymbol{C}^K \sim \mathcal{N}_M(\mathbf{0}, \boldsymbol{\Sigma}^\delta + \boldsymbol{\Sigma}^N) \quad \text{with } \boldsymbol{\Sigma}^N = \mathrm{diag}(N^{-1}).$$

- Right-key model:

$$\boldsymbol{C}^K \sim \mathcal{D}^\star_M + \mathcal{N}_M(\mathbf{0}, \boldsymbol{\Sigma}^\delta + \boldsymbol{\Sigma}^N).$$



Multivariate Linear Cryptanalysis – Three Steps

	Key dependent capacity	Data dependent capacity	Right-key case	Wrong-key case	Practical distribution estimates	Arbitrary key-schedule	Explicit capacity distribution	Free approximation choice
Huang *et al.* (2015)	✓	✗	✓	✗	✗	✗	✓	?
Blondeau and Nyberg (2017)	✓	✓	✓	✓	✗	✗	✓	?
Blondeau and Nyberg (2016)	✓	✓	✓	✓	✓	✗	✗	✓*
This work	✓	✓	✓	✓	✓	✓	✓	✓*

An Application: New Attacks on PRESENT

- We consider a set of 135 linearly independent approximations over 22/23 rounds of PRESENT.
- We used a method similar to the partial, sparse correlation matrix method by Abdelraheem (2012) to compute $\mathcal{D}^{\star}_{135}$.
- The low number of approximations allow for efficient key-guessing over 4 rounds.

An Application: New Attacks on PRESENT

Rounds	Success probability	#Approximations	Time complexity	Data complexity	Memory complexity	Key-dependent	Reference
25	95%	2295	$2^{65.0}$	$2^{62.4}$	$2^{34.0}$		Cho (2010)
	95%	2295	$2^{65.0}$	$2^{61.6}$	$2^{34.0}$	✓	Huang *et al.* (2015)
	74%	2295	$2^{72.0}$	$2^{61.0}$	$2^{34.0}$	✓	Blondeau and Nyberg (2016)
26	95%	2295	$2^{72.0}$	$2^{64.0}$	$2^{34.0}$		Cho (2010)
	80%	2295	$2^{76.0}$	$2^{62.5}$	$2^{34.0}$	✓	Huang *et al.* (2015)
	51%	2295	$2^{72.0}$	$2^{63.8}$	$2^{34.0}$	✓	Blondeau and Nyberg (2016)
	95%	**135**	$\mathbf{2^{68.6}}$	$\mathbf{2^{63.0}}$	$\mathbf{2^{48.0}}$	✓	**This work**
27	95%	405	$2^{74.0}$	$2^{64.0}$	$2^{70.0}$		Zheng and Zhang (2015)
	95%	**135**	$\mathbf{2^{77.3}}$	$\mathbf{2^{63.8}}$	$\mathbf{2^{48.0}}$	✓	**This work**

Thank you

Mohamed Ahmed Abdelraheem. Estimating the Probabilities of Low-Weight Differential and Linear Approximations on PRESENT-Like Ciphers. In *Information Security and Cryptology - ICISC 2012 - 15th International Conference, Seoul, Korea, November 28-30, 2012, Revised Selected Papers*, pages 368–382, 2012.

Alex Biryukov, Christophe De Cannière, and Michaël Quisquater. On Multiple Linear Approximations. In *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, pages 1–22, 2004.

Céline Blondeau and Kaisa Nyberg. Improved Parameter Estimates for Correlation and Capacity Deviates in Linear Cryptanalysis. *IACR Trans. Symmetric Cryptol.*, 2016(2):162–191, 2016.

Céline Blondeau and Kaisa Nyberg. Joint Data and Key Distribution of Simple, Multiple, and Multidimensional Linear Cryptanalysis Test Statistic and Its Impact to Data Complexity. *Design, Codes and Cryptography*, 82(1-2):319–349, 2017.

Andrey Bogdanov and Elmar Tischhauser. On the Wrong Key Randomisation and Key Equivalence Hypotheses in Matsui's Algorithm

2. In *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, pages 19–38, 2013.

Joo Yeon Cho. Linear Cryptanalysis of Reduced-Round PRESENT. In *Topics in Cryptology - CT-RSA 2010, The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings*, pages 302–317, 2010.

Joan Daemen and Vincent Rijmen. Probability Distributions of Correlation and Differentials in Block Ciphers. *J. Mathematical Cryptology*, 1(3):221–242, 2007.

Miia Hermelin, Joo Yeon Cho, and Kaisa Nyberg. Multidimensional Linear Cryptanalysis of Reduced Round Serpent. In *Information Security and Privacy, 13th Australasian Conference, ACISP 2008, Wollongong, Australia, July 7-9, 2008, Proceedings*, pages 203–215, 2008.

Jialin Huang, Serge Vaudenay, Xuejia Lai, and Kaisa Nyberg. Capacity and Data Complexity in Multidimensional Linear Attack. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, pages 141–160, 2015.

Burton S. Kaliski and Matthew J. B. Robshaw. Linear Cryptanalysis Using Multiple Approximations. In *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*, pages 26–39, 1994.

Lei Zheng and Shao-Wu Zhang. FFT-Based Multidimensional Linear Attack on PRESENT Using the 2-Bit-Fixed Characteristic. *Security and Communication Networks*, 8(18):3535–3545, 2015.