Ежегодная международная научно-практическая конференция
«РусКрипто’2019»

# О решении систем уравнений одного класса статистическими методами

Попов Владимир Олегович, к.ф.-м.н.,
директор по научной работе, ООО «КриптоПро», ассоциация «РУСКРИПТО»
Ошкин Игорь Борисович, к.ф.-м.н., начальник отдела, ООО «КриптоПро»

# Обзор литературы по теме Side-Channel Attacks

- YongBin Zhou, DengGuo Feng «Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing». 2005 г.
  Цель обзора - подготовить материалы для FIPS 140-3 (были редакции от 2012 и 2014 годов, но до сих пор не принят), основанные на обзоре 169 публикаций и TEMPEST.

- Раздел 5.1.12 Combination of SCA and Mathematical Attacks: комбинация методов SCA (Side Channel Attacks) и математических методов может дать полезные результаты.

- Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, Aurélien Francillon. Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers. EURECOM. (2018г.)
- Каналы линейной передачи для устройств с радиопередатчиком.

# Каналы утечки по TEMPEST

EXCERPT FROM NACSIM5000

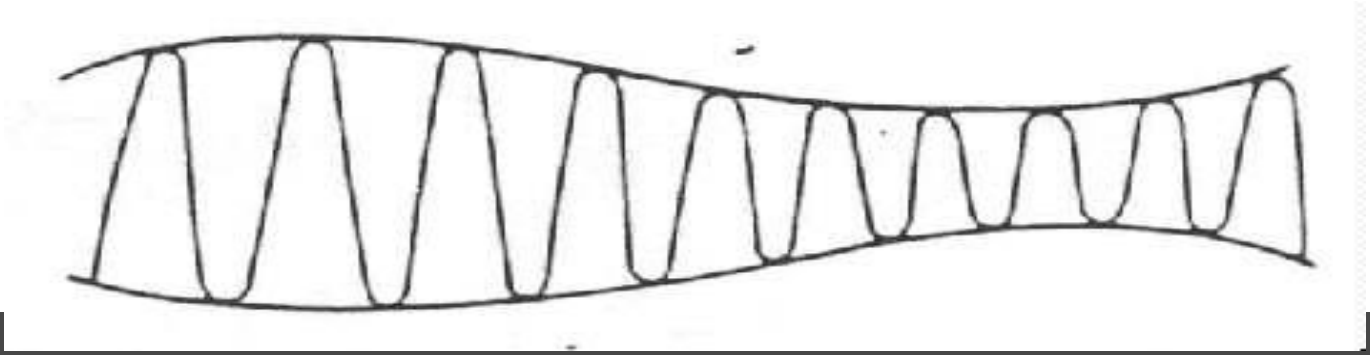
**1-5. (~~C~~) Propagation of TEMPEST Signals (U).** - There are four basic means by which compromising emanations may be propagated. They are: electromagnetic radiation; conduction; modulation of an intended signal; and acoustics. A brief explanation of each follows.

a. (~~C~~) Electromagnetic Radiation (U). - Whenever a RED signal is generated or processed in an equipment, an electric, magnetic or electromagnetic field is generated. If this electromagnetic field is permitted to exist outside of an equipment, a twofold problem is created; first the electromagnetic field may be detected outside the Controlled Space (CS); second the electromagnetic field may couple onto BLACK lines connected to or located near the equipments, which exit the CS of the installation.

b. (~~C~~) Line Conduction. - Line Conduction is defined as the emanations produced on any external or interface line of an equipment, which, in any way, alters the signal on the external or interface lines. The external lines include signal lines, control and indicator lines, and a.c. and d.c. powerlines.

c. (~~C~~) Fortuitous Conduction. - Emanations in the form of signals propagated along any unintended conductor such as pipes, beams, wires, cables, conduits, ducts, etc.

d. (~~C~~) (Six lines redacted.)



# Российская нормативная база

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации. Москва 2016.

КОИ и понятие функция энергии, $\omega()$

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования. (Проект).

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2).

S. Smyshlyaev, Ed. Re-keying Mechanisms for Symmetric Keys. Internet-Draft. IETF. 2018. https://datatracker.ietf.org/doc/draft-irtf-cfrg-re-keying/?include_text=1

RFC 4357. Additional Cryptographic Algorithms for Use with GOST 28147-89,GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms.

Рекомендуют ограничивать материал, обрабатываемый на одном значении ключа

# Методы DPA, CPA

- Differential Power Analysis
- Y. Fei, A. A. Ding, J. Lao, and L. Zhang, A statistics-based fundamental model for side-channel attack analysis," Cryptology ePrint Archive, Report 2014/152, 2014,
- A. Adam Ding, Liwei Zhang, Yunsi Fei, and Pei Luo. A Statistical Model for Higher Order DPA on Masked Devices (2015).
- Yunsi Fei, Qiasi Luo, and A. Adam Ding. A Statistical Model for DPA with Novel Algorithmic Confusion Analysis
- Correlation Power Attack
- E. Brier, C. Clavier, and F. Olivier, Correlation power analysis with a leakage model," in Int. Workshop on Cryptographic Hardware & Embedded Systems, 2004, pp. 135-152.
- Thanh-Ha Le, Jessy Clediere, Cecile Canovas, Bruno Robisson, Christine
- Serviµere, Jean-Louis Lacoume. A proposition for Correlation Power Analysis enhancement

конференция РусКрипто

# A Statistical Model for DPA with Novel Algorithmic Confusion Analysis

Yunsi Fei[1], Qiasi Luo[2], and A. Adam Ding[3]

[1] : Department of Electrical and Computer Engineering
Northeastern University
[2] : Marvell Technology Group Ltd., Santa Clara
[3] : Department of Mathematics, Northeastern University

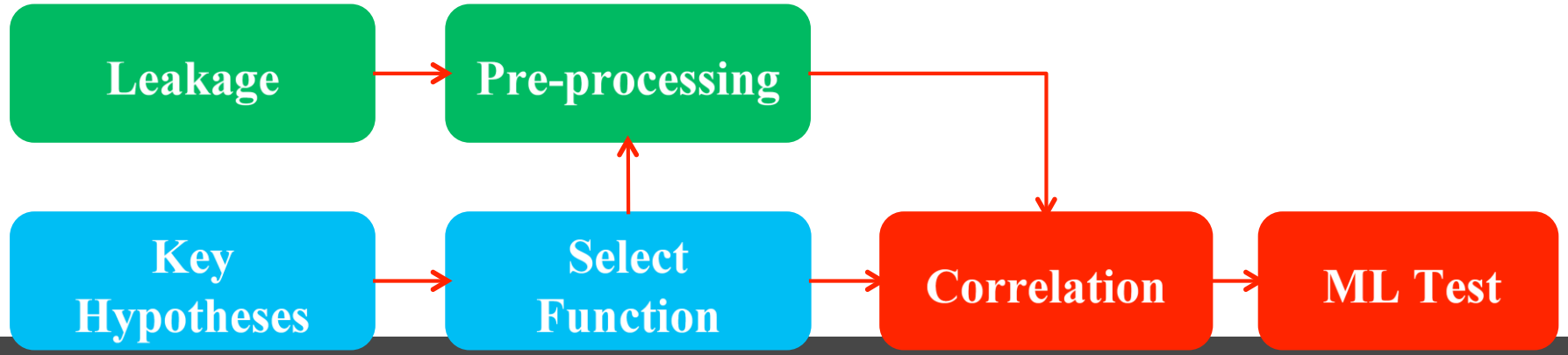
*Acknowledgment: NSF CNS-0845871*

Northeastern University

# Differential Power Analysis (DPA) Procedure

- Implementation:
- Leakage: $W=\{W_1, \ldots, W_{Nm}\}$, $W_i=\{W_{i,1}, \ldots, W_{i,p}\}$
- Algorithm:
- Select function: $V= \psi(d)$, where $d=\text{Sbox}(x \oplus k)$
- Attack:
- Correlation: For DPA, Difference-of-means (DoM):

$$\delta = \frac{\sum W_{\psi=1}}{N_{\psi=1}} - \frac{\sum W_{\psi}}{N_{\psi=0}} \qquad N_m = N_{\psi=1} + N_{\psi=0}$$



# Central Limit Theorem and DPA

- DPA: a sampling process on the entire waveform population
- $W_{\psi=1}$ and $W_{\psi=0}$: random variables with normal distribution:

$$N(\varepsilon + b, \frac{\sigma_w}{\sqrt{N_{\psi=1}}}) \qquad N(b, \frac{\sigma_w}{\sqrt{N_{\psi=0}}})$$

- $b$: mean power consumption for the waveform group $\psi=0$
- $\varepsilon$: power difference related to the bit under DPA attack $\lim_{N_m \to \infty} \delta_c = \varepsilon$
- Therefore, the DoM of the correct key ($k_c$), $\delta_c$, is a random variable with normal distribution:

$$N(\varepsilon, 2\frac{\sigma_w}{\sqrt{N_m}})$$

$$\delta = \frac{\sum W_{\psi=1}}{N_{\psi=1}} - \frac{\sum W_{\psi=0}}{N_{\psi=0}}$$

# Постановка задачи

G – конечное множество с операцией *, G×G->G; как правило G – векторное пространство над полем F (в основном над $GF_2$) размерности m и с некоторым фиксированным базисом (порядком координат), как правило * – групповая операция, либо групповая операция ^, усложненная некоторым преобразованием T, G*G = T(G^G), возможно иное.

$\omega$: G->R, R - действительные числа, $\omega()$ – центрирована.

$A = \{a_i\}_{i=1,N}$, $a_i \in G$ – множество элементов $G$, относительно которых будем предполагать равновероятность и независимость над $G$.

$x \in G$, априори равновероятный над G.

$$\omega(a_i * x) = d_i, \quad i = 1, N$$

$G$ разлагается в прямое произведение r блоков, $G = G_1 \times G_2 \times \cdots \times G_r$, $|G_j| = n_j$.
Если это разложение в прямую сумму пространств, то $b_j$- размерность $G_j$.
$\omega()$ – аддитивна над этим разложением, $\omega(g) = \omega_1(g_1) + \omega_2(g_2) \ldots + \omega_r(g_r)$.

# Постановка задачи (продолжение)

- $\sum_{j=1}^{r} \omega_j (a_{i,j} * x_j) = d_i, \quad i = 1, N$
- Пусть становятся известными величины $R_i = d_i + \xi_i$, где $\xi_i$ независимые нормальные величины $\mathfrak{N}(0, \sigma^2)$.
- $\sum_{j=1}^{r} \omega_j (a_{i,j} * x_j) = R_i, \quad i = 1, N$
- Предполагаем, система трудно решаемая (m, |G| - велики).
- Отметим, $d_i$– центрированы и могут рассматриваться как случайные, если $x \in G$ случайная величина.

# Используемые статистики

Линейная статистика:

$$S_j(x) = \frac{1}{N}\sum_{i=1}^{N} \omega_j(a_{i,j} * x)R_i\,, \qquad x \in G_j, \qquad j = 0, r-1 \qquad (1)$$

Квадратичная статистика:

$$S_j(x) = \frac{1}{N}\sum_{i=1}^{N} (R_i - \omega_j(a_{i,j} * x))^2\,, \qquad x \in G_j, \qquad j = 0, r-1 \qquad (2)$$

или эквивалентная:

$$S_j(x) = \frac{1}{N}\sum_{i=1}^{N} \omega_j(a_{i,j} * x)R_i\,, \qquad x \in G_j, \qquad j = 0, r-1 \qquad (3)$$

$\overline{\omega}_j(a) = \begin{cases} +1, & x > 0 \\ 0, & x = 0 \\ -1, & x < 0 \end{cases}$ знак числа.

# Бинарные системы (b=1, $GF_2$)

$\omega(x) = (-1)^x, x -$ битовая величина.

$S_j(0) = -S_j(1);$ $\quad S_j(0) \sim \mathcal{N}(-\frac{\omega(\overline{x}_j)}{2}, \frac{\sigma^2+\sigma_d^2}{N}),$ $\quad$ где $\sigma_d^2 = \frac{m-1}{4}$.

$p_e = \int_{x=0}^{\infty} \varphi_{\frac{-1}{2},\sigma_-^2}\, dx\,,$ $\quad \varphi_{\mu,\sigma_-^2} \sim \mathcal{N}(-\frac{1}{2}, \frac{\sigma^2+\sigma_d^2}{N}),$

$\psi = \frac{1}{2}\left(\varphi_{\frac{-1}{2},\sigma_-^2} + \varphi_{\frac{1}{2},\sigma_-^2}\right)$ – плотность распределения выборки $\{S_j\}_{j=1}^m$.

$E(\psi) = 0; D(\psi) = \sigma_-^2 + \frac{1}{4};$

Распределение числа ошибок в $\{S_j\}_{j=1}^m$ - биномиальное Bin(m,$p_e$).

# Бинарные системы (продолжение)

Плотность ошибок $\varepsilon(x)$ в вариационном ряде $\{S_{(j)}\}_{j=1}^{m}$: $\varepsilon(x) = \begin{cases} \frac{\left(\varphi_{\frac{1}{2},\sigma\_^2}\right)}{2p_e} \text{ при } x < 0 \\ \frac{\left(\varphi_{\frac{-1}{2},\sigma\_^2}\right)}{2p_e} \text{ при } x \geq 0 \end{cases}$

Если решение системы существует: $\sum_{j=1}^{m} S_j^2$ - нецентральный $\chi^2$ с m степенями свободы и параметром не центральности $\lambda = m/(4\sigma\_^2)$.

Если решение системы не существует: $\sum_{j=1}^{m} S_j^2$ - $\chi^2$ с m степенями свободы.

Алексеев Е.К., Ошкин И.Б., Попов В.О., Смышляев С.В. Решение систем линейных уравнений булева типа с искаженной правой частью над полем действительных чисел. Дискретная математика. Том 29, выпуск 1. 2017.

# Модульное сложение, метод скользящего окна

$$\omega\,(a_i + x)\ mod\ 2^m = R_i, \quad i = 1, N$$

Окно ширины b содержит ранее восстановленные знаки с номерами j-b,…j-1; j знак определяется по статистикам

$$S_j = \frac{1}{N}\sum_{i=1}^{N} \omega(a_{i,j} + \gamma_j)R_i\ , \qquad j = 1, m$$

$\gamma_j$ – перенос результата сложения числа из окна с соответствующими знаками величин $a_i$.

Число ошибок в 1.8 – 2.3 раза превосходит числа ошибок бинарного метода с такими же параметрами.

# Блочные системы

$$S_j(x) = \frac{1}{N}\sum_{i=1}^{N}\Psi(\omega_j(a_{i,j} * x), R_i), \qquad x \in G_j, \qquad |G_j| = n_j, \qquad j = 0, r-1$$

$S_j(*)$ различает j-ый фрагмент решения системы $\overline{x}_j$, если её среднее значение (либо иная характеристика) для $\overline{x}_j$ отлична от общего среднего E( $S_j(*)$ ).

$\mu_j, \sigma_j$ - параметры распределения решения j-фрагмента, рассчитываемые величины,

$\mu_s, \sigma_s$ - параметры выборки $S_j(*)$, это вычисляемые величины, $\mu_s = 0$.

$\mu = \frac{\mu_j}{\sigma_s}$ - 1 -:- 5, метод Неймана – Пирсона по различению решения и членов вариационного ряда $S_{(j)}(*)$ не применим. $\sigma = \frac{\sigma_j}{\sigma_s}$.

Вероятность фрагмента решения на k месте ряда $S_{(j)}(*)$:

$$p_k = C_{n-1}^{k}\int_{x=-\infty}^{\infty}\varphi_{\mu,\sigma^2}(x)\,F_{0,1}(x)^{n-1-k}\,(1 - F_{0,1}(x))^{k}\,dx$$

# Блочные системы (продолжение)

Функция распределения имеет характер распределения типа Вейбулла на целочисленных точках:

$$\sum_{k=0}^{t-1} p_k \approx W_{\varkappa,\lambda}\ (\mathrm{t}-\mathrm{s}),\quad 0 < s \leq 1,\quad t = 1,2,\dots .$$

Данный вывод основан на экспериментальных исследованиях. Использовались метрики хи квадрат и Колмогорова для поиска ближайшего $W_{\kappa,\lambda}$(k+s) к данным, полученным экспериментально и по интегральному представлению $p_k$.

Построено отображение: $(\mu, \sigma) \to (\varkappa, \lambda, \mathrm{s})$

$k_j$ - принимаемое число значений переменной $x_j$,
$\pi_j$ - вероятность j – фрагмента решения находится среди этих $k_j$ значений.

$$\pi_j = W_{\varkappa,\lambda}\left(k_j - \mathrm{s}\right).$$

$$Q = \prod_{j=0}^{r-1} (k_j / \ \pi_j), \qquad P = \prod_{j=0}^{r-1} \pi_j \ .$$

# Заключение

$$k_N = \frac{N}{\sigma^2 + \sigma_d^2}$$

Пусть m =128.

По опыту исследований, если $k_N \geq 8-:-10$,
решение осуществимо на компьютере i7.

Изложенные материалы основаны на статистических исследованиях бинарных, модулярных и иных систем.

конференция РусКрипто

# Список литературы


1. Нормативная база.
    1. Росстандарт. Технический комитет 026. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации. Москва 2016.
    2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. От 21 февраля 2008 года
    3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности. 2015 года.
    4. TEMPEST, опубликована в интернете в 2002г. (National Security Agency. NACSIM 5000 Tempest Fundamentals)

1. Элементы модели методов DPA и CPA

    Вес Хемминга
    1. E. Brier, C. Clavier, and F. Olivier, Correlation power analysis with a leakage model," in Int. Workshop on Cryptographic Hardware & Embedded Systems, 2004, pp. 135-152.

    Определение аддитивной гауссовой помехи и веса Хемминга, как опасного сигнала.
    1. Stefan Mangard, Elisabeth Oswald, Fran¸cois-Xavier Standaert. One for All - All for One: Unifying Standard DPA Attacks Опубликована после 2010 г.

    Гауссова модель

2.3. M. Rivain, “On the exact success rate of side channel analysis in the gaussian model," in Selected Areas in Cryptography, ser. Lecture Notes in Computer Science, R. Avanzi, L. Keliher, and F. Sica, Eds. Springer. Berlin Heidelberg, 2009, vol. 5381, pp. 165-183.

2.4. Stefan Mangard, Elisabeth Oswald, Fran¸cois-Xavier Standaert. One for All - All for One: Unifying Standard DPA Attacks.

Отношение сигнал-помеха (SNR, signal-to-noise ratio)

2.5. T. S. Messerges, E. A. Dabbish, and R. H. Sloan, “Examining smart-card security under the threat of power analysis attacks," IEEE Trans. on Computers, vol. 51, no. 5, pp. 541-552, 2002.

1. Формальная модель методов DPA и CPA

3.1. Y. Fei, A. A. Ding, J. Lao, and L. Zhang, A statistics-based fundamental model for side-channel attack analysis," Cryptology ePrint Archive, Report 2014/152, 2014, http://eprint.iacr.org/.

3.2. A. Adam Ding, Liwei Zhang, Yunsi Fei, and Pei Luo. A Statistical Model for Higher Order DPA on Masked Devices (2015).

3.3. Yunsi Fei, Qiasi Luo, and A. Adam Ding. A Statistical Model for DPA with Novel Algorithmic Confusion Analysis

3.4. см. п. 2.1.

3.5. Thanh-Ha Le, Jessy Clediere, Cecile Canovas, Bruno Robisson, Christine
Servi¡ere, Jean-Louis Lacoume. A proposition for Correlation Power Analysis enhancement

1. Обзоры
    1. YongBin Zhou, DengGuo Feng «Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing». 2005 года. State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, 100080, China.
    2. Raphael Spreitzer, Veelasha Moonsamy, Thomas Korak, and Stefan Mangard. Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. 2017. https://arxiv.org/pdf/1611.03748.pdf

    IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. XX, NO. Z, MONTH YYY
    1. Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, Aurélien Francillon. Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers. EURECOM. http://s3.eurecom.fr/docs/ccs18_camurati_preprint.pdf

    Preprint to appear at ACM CCS 2018, Toronto, Canada

5. Ограничение материала, обрабатываемого на ключе.

5.1. РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ. Информационная технология. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования. (Проект). Москва. Стандартинформ.

5.2. Р 1323565.1.020-2018. РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ. Информационная технология. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2). Москва. Стандартинформ.

5.3. S. Smyshlyaev, Ed. Re-keying Mechanisms for Symmetric Keys. Internet-Draft. IETF. 2018. https://datatracker.ietf.org/doc/draft-irtf-cfrg-re-keying/?include_text=1.

5.4. RFC 4357. Additional Cryptographic Algorithms for Use with GOST 28147-89,GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms.

6. Работы по теме.

6.1. Алексеев Е.К., Ошкин И.Б., Попов В.О., Смышляев С.В. Решение систем линейных уравнений булева типа с искаженной правой частью над полем действительных чисел. Дискретная математика. Том 29, выпуск 1. 2017.

# Вопросы

# Контактная информация

Электронная почта:

vpopov@cryptopro.ru

Телефон:

+7 903 275-24-83