Методы защиты от атак по побочным каналам аппаратной реализации схем постквантовой подписи, построенных на основе протокола идентификации Штерна

Смирнов Дмитрий Константинович, магистр, МГУ имени М.В. Ломоносова,
АО «ИнфоТеКС». Smirnov.DK@infotecs.ru
Чижов Иван Владимирович, к. ф.-м. н., доцент, МГУ имени М.В. Ломоносова,
ФИЦ «Информатика и управление» РАН, АО «НПК „Криптонит“».
ichizhov@cs.msu.ru

РусКрипто XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Другие исследования

РусКрипто

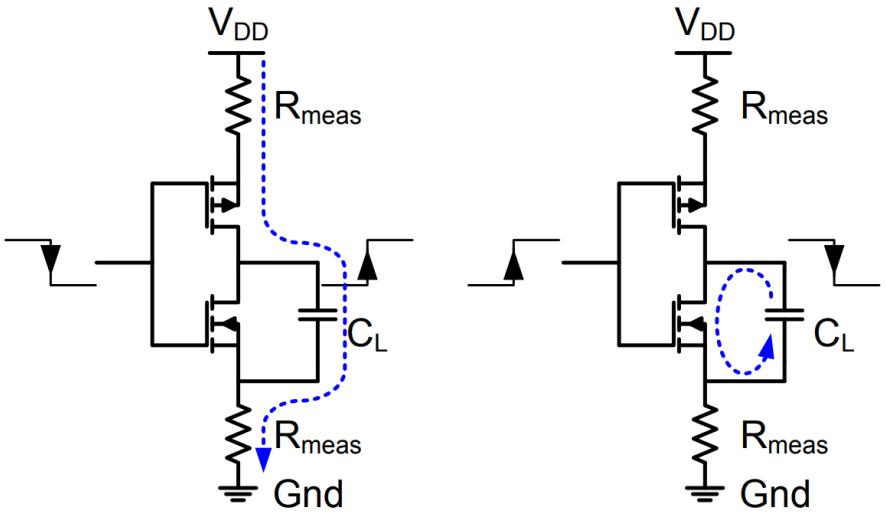
Secure Implementation of the Stern Authentication and Signature Schemes for Low-Resource Devices

Pierre-Louis Cayrel[1], Philippe Gaborit[1], and Emmanuel Prouff[2]

[1] Université de Limoges, XLIM-DMI,
123, Av. Albert Thomas 87060 Limoges Cedex France
{pierre-louis.cayrel,philippe.gaborit}@xlim.fr
[2] Oberthur Technologies
71-73, rue des hautes pâtures 92726 Nanterre Cedex France
e.prouff@oberthurcs.com

Атаки по энергопотреблению

РусКрипто



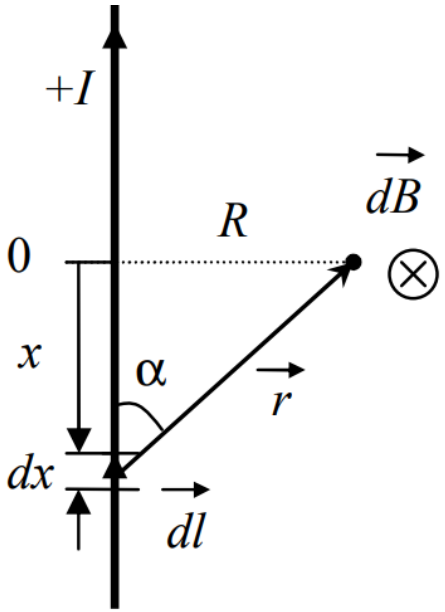
$$E_s = C_L V_{DD}^2$$

C_L – нагрузочная ёмкость

V_{DD} – напряжение источника питания

Rabaey J. Digital Integrated Circuits: A Design Perspective. — Prentice Hall, 1996. — (Prentice Hall International editions).

Атаки по электромагнитному излучению



Закон Био-Савара-Лапласа:

$$d\vec{B} = \frac{\mu_0}{4\pi}\frac{I\left[d\vec{l}\times\vec{r}\right]}{r^3}$$

μ_0 – магнитная постоянная

I – ток в проводнике

$d\vec{l}$ – элемент проводника

$\vec{r}$ – радиус-вектор от элемента проводника до точки, в которой измеряется индукция магнитного поля

Модель утечек

РусКрипто

- Вес Хэмминга: $C(x) \sim wt(x)$
- Расстояние Хэмминга: $C(x, R) \sim wt(x \oplus R)$
- Расстояние смены бит:

Смена бита	Потребляемая мощность
$0 \rightarrow 0$	0
$0 \rightarrow 1$	1
$1 \rightarrow 0$	$1 - \delta$
$1 \rightarrow 1$	0

Peeters E., Standaert F.-X., Quisquater J.-J. Power and electromagnetic analysis: Improved model, consequences and comparisons // Integration. — 2007. — Янв. — Т. 40. — С. 52—60. — DOI: 10.1016/j.vlsi.2005.12.013.

Простой анализ энергопотребления (SPA)

РусКрипто

Пример атаки на RSA при возведении в степень

https://github.com/lord-feistel/power_analysis

Корреляционная атака (SCA)

РусКрипто

Для примера возьмём шифрование $E_K(M) = M \oplus K$.

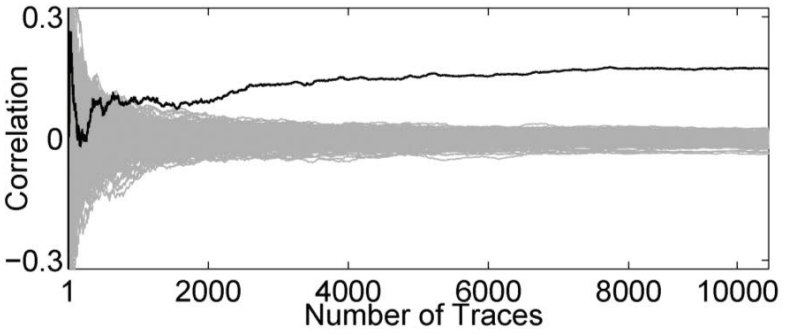
$$\rho_{WH}(R) = \frac{\sum W_i H_{i,R} - \frac{1}{N}\sum W_i \sum H_{i,R}}{\sqrt{\sum W_i^2 - (\sum W_i)^2}\sqrt{\sum H_{i,R}^2 - \left(\sum H_{i,R}\right)^2}}$$

R	– неизвестное значение (ключ)
M_i	– известные данные
W_i	– набор измерений
$H_{i,R} = wt(M_i \oplus R)$	– набор предположений
N	– размер каждого из наборов

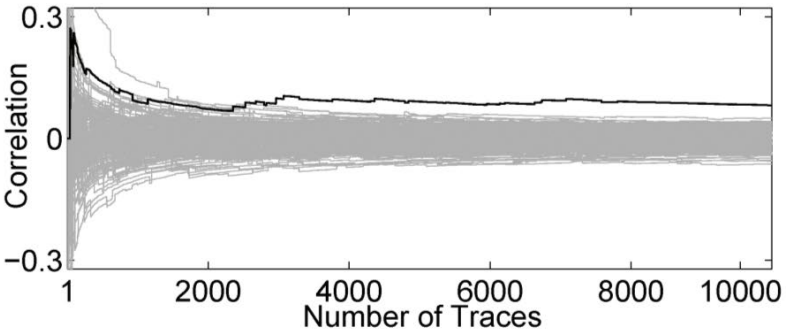
Brier E., Clavier C., Olivier F. Correlation Power Analysis with a Leakage Model //. Т. 3156. — 08.2004. — С. 16—29. — DOI: 10.1007/978-3-540-28632-5_2.

Корреляционная атака (SCA)

РусКрипто



Модель расстояния Хэмминга



Модель веса Хэмминга

Moradi, A., Mischke, O., Eisenbarth, T. Correlation-Enhanced Power Analysis Collision Attack. // Cryptographic Hardware and Embedded Systems, CHES 2010. CHES 2010. Lecture Notes in Computer Science. -- T 6225. -- 2010. -- DOI: https://doi.org/10.1007/978-3-642-15031-9_9

Маскирование

РусКрипто

$$x = x_1 \oplus x_2 \oplus \cdots \oplus x_d$$

$x \in \{0,1\}^n$ секрет

$x_1, x_2, \ldots, x_d \in \{0,1\}^n$ набор долей

+ Для криптосистемы NTRU маскирование ключа оказалось наиболее эффективным способом защиты.[1]
+ Стойкость к SCA доказуема. [2]
- Уязвимо к DPA.

[1] Rabas T., Buček J. , Lorencz R. Single-Trace Side-Channel Attacks on NTRU Implementation // SN Computer Science. — 2024. — Янв. — Т. 5. — DOI: 10.1007/s42979-023-02493-7
[2] Prouff E., Rivain M. Masking against Side-Channel Attacks: A Formal Security Proof // Advances in Cryptology – EUROCRYPT 2013 / под ред. T. Johansson, P. Q. Nguyen. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2013. — С. 142—159.)

Дифференциальная атака высших порядков (DPA)

$$wt(x \oplus y) = |wt(x) - wt(y)| \sim |T_1 - T_2|$$

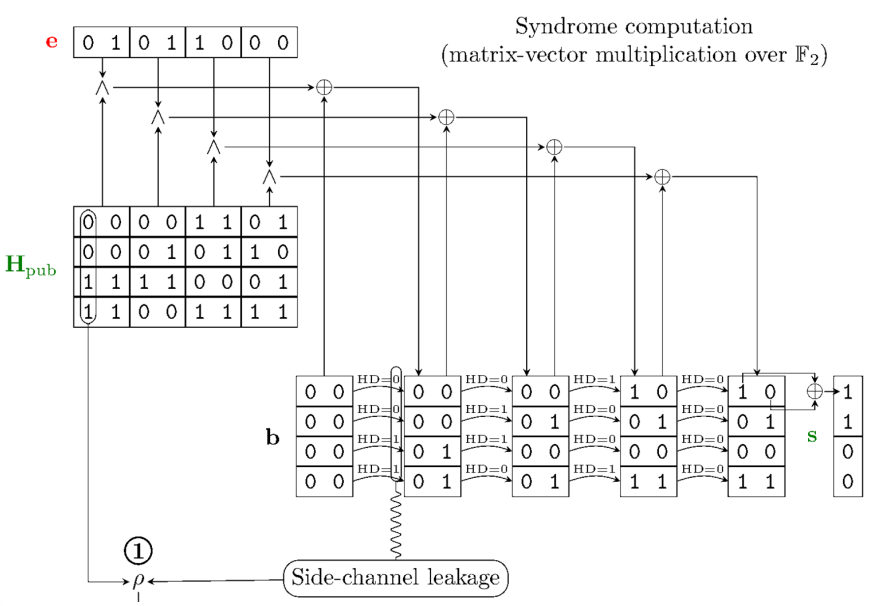
$x, y \in \{0,1\}$ – два бита, вычисленных на устройстве в разные моменты времени

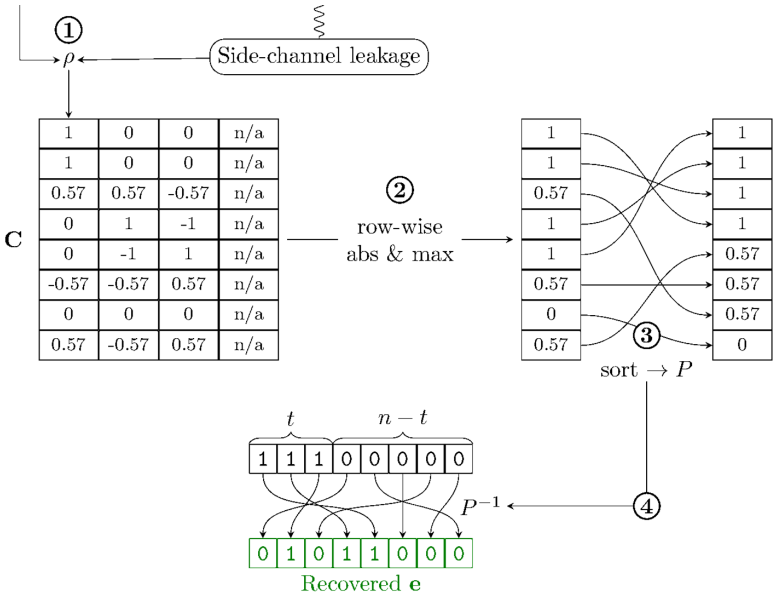
T_1, T_2 – трассы с измерениями энергопотребления в соответствующих моментах времени

Oswald, E., Mangard, S., Herbst, C., Tillich, S. Practical Second-Order DPA Attacks for Masked Smart Card Implementations of Block Ciphers // Topics in Cryptology – CT-RSA 2006. CT-RSA 2006. Lecture Notes in Computer Science – 2006. – T. 3860 – DOI: https://doi.org/10.1007/11605805_13

Горизонтальная корреляционная атака

РусКрипто





Horizontal Correlation Attack on Classic McEliece / B. Colombier [и др.]. — 2023. — URL: https://eprint.iacr.org/2023/546. Cryptology ePrint Archive, Paper 2023/546.

Защита матричного умножения

РусКрипто

$$\forall i = \overline{1,n}:$$
$$reg_0 = reg_0 \oplus He_i, \qquad s \cdot e_i = 0$$
$$reg_1 = reg_1 \oplus He_i, \qquad s \cdot e_i \neq 0$$

reg_0, reg_1 – регистры, хранящие сумму по нулевым и единичным битам соответственно

e_i – единичный вектор

H – проверочная матрица

s – секретный ключ

n – размер ключа с битах

Генерация маски

РусКрипто

Для генерации маски предлагается использовать Стрибог-К[1]:

$$H(K||M)$$

+ Стрибог неразличим от случайного оракула в модели идеального блочного шифра.[2]
+ Переиспользование реализованной на схеме логики.

[1] Akhmetzyanova L. R., Babueva A. A., Bozhko A. A. Streebog as a random oracle // ПДМ. — 2024. — № 64. — С. 27—42. — DOI: 10.17223/20710410/64/3. — URL: http://mi.mathnet.ru/pdm836.
[2] Kiryukhin V. Keyed Streebog is a secure PRF and MAC. — 2022. — URL: https://eprint.iacr.org/2022/972. Cryptology ePrint Archive, Paper 2022/972.

Модифицированный протокол

РусКрипто

Вводится пароль $Pass \in \{0,1\}^t, t < 256$.

Генерируется маска $M = F(Pass) \in \{0,1\}^n$

Абонент P обладает маскированным ключом $s' = s \oplus M$.

Вычисляется открытый ключ y:

$$y = Hs'^T \oplus HM^T = Hs^T$$

Kiryukhin V. About “k-bit security” of MACs based on hash function Streebog — 2023. — URL: https://eprint.iacr.org/2023/1305. Cryptology ePrint Archive, Paper 2023/1305.

Модифицированный протокол

РусКрипто

$$c_0 = h(\sigma \parallel Hu^T)$$
$$c_1 = h(\sigma(u))$$
$$c_2 = h\big(\sigma(u \oplus s)\big)$$

$$r_0 = \sigma, \quad r_1 = u, \quad b = 0$$
$$r_0 = \sigma, \quad r_1 = u \oplus s, \quad b = 1$$
$$r_0 = \sigma(u), \quad r_1 = \sigma(s), \quad b = 2$$

Оригинальная схема

$$u' = u \oplus M$$
$$A = \sigma(u) \oplus \sigma(s')$$
$$c_0 = h(\sigma \parallel Hu'^T)$$
$$c_1 = h(\sigma(u'))$$
$$c_2 = h(A) = h(\sigma(u' \oplus s))$$

$$r_0 = \sigma, \quad r_1 = u', \quad b = 0$$
$$r_0 = \sigma, \quad r_1 = \sigma^{-1}(A) = u' \oplus s, \quad b = 1$$
$$r_0 = \sigma(u'), \quad r_1 = \sigma(s') \oplus \sigma(M) = \sigma(s), \quad b = 2$$

Модифицированная схема

Применение дифференциальных атак

РусКрипто

$$u' = u \oplus M$$
$$r_1 = u' \oplus s, \quad b = 1$$

$$wt(s) = wt\big((u \oplus M) \oplus (u' \oplus s)\big) = |wt(u \oplus M) - wt(u' \oplus s)| \sim |T_1 - T_2|$$

Вес ключа – открытая информация, но нужно складывать все биты за одну операцию, а не по «машинным словам».

Применение дифференциальных атак

РусКрипто

$$c_1 = h\big(\sigma(u)\big)$$
$$c_2 = h\big(\sigma(u \oplus s)\big)$$

$$wt(\sigma(s)) = wt(\sigma(u) \oplus \sigma(u \oplus s)) = \big|wt\big(\sigma(u)\big) - wt\big(\sigma(u \oplus s)\big)\big| \sim |T_1 - T_2|$$

Перестановку проводят побитово, поэтому злоумышленник увидит пики в $|T_1 - T_2|$, соответствующие единичным битам секретного ключа. Применив σ^{-1}, он извлекает ключ.

Защита перестановок

$$y_{\psi(i)} = x_{\sigma(\psi(i))} \quad \forall i = \overline{1,n}$$

x – перемешиваемый вектор

y – результирующий вектор ($y = \sigma(x)$)

σ – раскрываемая перестановка

ψ – нераскрываемая перестановка

РусКрипто

Стратегии противника

РусКрипто

$\hat{b} = 0$ $t = \{0,1\}^n$: $wt(t) = \omega$	$\hat{b} = 1$ $t = \{0,1\}^n$: $wt(t) = \omega$	$\hat{b} = 2$ $t = \{0,1\}^n$: $Ht^T = y$
$c_0 = h(\sigma \parallel H(u \oplus t)^T \oplus y)$ $c_1 = h(\sigma(u))$ $c_2 = h(\sigma(u \oplus t))$	$c_0 = h(\sigma \parallel Hu^T)$ $c_1 = h(\sigma(u))$ $c_2 = h(\sigma(u \oplus t))$	$c_0 = h(\sigma \parallel Hu^T)$ $c_1 = h(\sigma(u))$ $c_2 = h(\sigma(u \oplus t))$
$r_0 = \sigma, \quad r_1 = u \oplus t, \quad b = 1$ $r_0 = \sigma(u), \; r_1 = \sigma(t), \quad b = 2$	$r_0 = \sigma, \quad r_1 = u, \quad b = 0$ $r_0 = \sigma(u), \; r_1 = \sigma(t), \quad b = 2$	$r_0 = \sigma, \quad r_1 = u, \quad b = 0$ $r_0 = \sigma, \quad r_1 = u \oplus \mathrm{t}, \quad b = 1$

Stern J. A new identification scheme based on syndrome decoding // Advances in Cryptology — CRYPTO' 93 / под ред. D. R. Stinson. — Berlin, Heidelberg : Springer Berlin Heidelberg, 1994. — С. 13—21.

Определения машин Тьюринга

РусКрипто

$A = (A_1, A_2)$

$A(u, \sigma, y, b, \hat{b}, s)$:

1. $(c_0, c_1, c_2, r_0', r_1', r_0'', r_1'') \leftarrow A_1(u, \sigma, y, \hat{b}, s)$
2. $(r_0, r_1) \leftarrow A_2(b, \hat{b}, r_0', r_1', r_0'', r_1'')$
3. Вернуть $(c_0, c_1, c_2, r_0, r_1)$.

$\hat{b}$ — выбор стратегии противника

r_0', r_1', r_0'', r_1'' — наборы ответов противника, соответствующие выбранной им стратегии

Определения машин Тьюринга

РусКрипто

$B = (B_1, B_2)$

$B(u, \sigma, y, b, \hat{b}, s', M)$:

1. $(c_0, c_1, c_2, r_0', r_1', r_0'', r_1'') \leftarrow B_1(u, \sigma, y, \hat{b}, s', M)$
2. $(r_0, r_1) \leftarrow B_2(b, \hat{b}, r_0', r_1', r_0'', r_1'')$
3. Вернуть $(c_0, c_1, c_2, r_0, r_1)$.

$\hat{b}$ — выбор стратегии противника

r_0', r_1', r_0'', r_1'' — наборы ответов противника, соответствующие выбранной им стратегии

Сравнение стойкости версий протокола

РусКрипто

Утверждение: Время работы машин A и B совпадает.

Доказательство.

$$A\left(u, \sigma, y, b, \hat{b}, s\right) = B\left(u, \sigma, y, b, \hat{b}, s, 0\right)$$
$$B\left(u, \sigma, y, b, \hat{b}, s', M\right) = A\left(u \oplus M, \sigma, y, b, \hat{b}, s' \oplus M\right)$$

Определения машин Тьюринга

РусКрипто

$$SC_1: \quad T_1 \to s$$
$$SC_2: \quad (T_1, T_2) \to (s', M)$$

T_1, T_2 — измеренные трассы

T_{SC_1}, T_{SC_2} — время работы машин в тактах.

$\hat{A}(u, \sigma, y, b, \hat{b}, T_1)$:

1. $s \leftarrow SC_1(T_1)$
2. $(c_0, c_1, c_2, r_0, r_1) \leftarrow A(u, \sigma, y, b, \hat{b}, s)$
3. Вернуть $(c_0, c_1, c_2, r_0, r_1)$.

$\hat{B}(u, \sigma, y, b, \hat{b}, T_1, T_2)$:

1. $(s', M) \leftarrow SC_2(T_1, T_2)$
2. $(c_0, c_1, c_2, r_0, r_1) \leftarrow B(u, \sigma, y, b, \hat{b}, s', M)$
3. Вернуть $(c_0, c_1, c_2, r_0, r_1)$.

Сравнение стойкости версий протокола

РусКрипто

Утверждение: Время работы машины $\hat{A}$ меньше времени работы $\hat{B}$.

Доказательство.

$$\begin{cases} T_{\hat{A}} = T_{SC_1} + T_A \\ T_{\hat{B}} = T_{SC_2} + T_B \\ T_A = T_B \\ T_{SC_1} < T_{SC_2} \end{cases} \Rightarrow T_{\hat{A}} < T_{\hat{B}}$$

Выводы

РусКрипто

- Одного метода защиты недостаточно. Их нужно комбинировать.
- При разработке криптографических схем стоит учитывать атаки по побочным каналам заранее, чтобы схемы были стойкими к ним по построению.
- Предложенные изменения позволяют повысить стойкость к этим атакам реализации схемы подписи Шиповник.

РусКрипто

Смирнов Дмитрий Константинович: Smirnov.DK@infotecs.ru
Чижов Иван Владимирович: ichizhov@cs.msu.ru

СПАСИБО ЗА ВНИМАНИЕ