О ВЫСОКОСКОРОСТНОМ АСИММЕТРИЧНОМ ШИФРОВАНИИ НА ОТКРЫТОМ КЛЮЧЕ НА БАЗЕ WHITE-BOX-КРИПТОГРАФИИ

Щелкунов Д.А., к.т.н., КФ МГТУ имени Н.Э. Баумана, кафедра ЭИУ6-КФ; компания «Рекрипт»

Чиликов А.А., к.ф.-м.н., МГТУ имени Н.Э. Баумана, кафедра ИУ-8; МФТИ, факультет инноваций и высоких технологий, лаборатория продвинутой комбинаторики и сетевых приложений; Passware, Research Department

Проблемы асимметричной криптографии

- Медленна
- Ресурсоёмка (требует больших вычислительных ресурсов)
- Спроектирована, в основном, для подписи
- Постквантовый мир?

White-box-криптография

- Набор техник, позволяющих преобразовать симметричный блочный шифр в асимметричный посредством сокрытия ключа в реализации алгоритма шифрования (white-box-реализация)
- По сути — разновидность обфускации
- Преимущество — высокая скорость шифрования\расшифрования
- Преимущество — низкая ресурсоёмкость (низкие требования к вычислительным ресурсам)
- Стойких white-box-реализаций общеизвестных симметричных шифров на текущий момент не существует

Предыдущие исследования

1. S. Chow, P. Eisen, H. Johnson, P.C. van Oorschot, A White-Box DES Implementation for DRM Applications, 2002.

2. S. Chow, P. Eisen, H. Johnson, P.C. van Oorschot, White Box Cryptography and an AES Implementation, 2002.

3. Julien Bringer, Herve Chabanne, Emmanuelle Dottax, White Box Cryptography: Another Attempt, 2006.

4. Hamilton E. Link, William D. Neumann, Clarifying Obfuscation: Improving the Security of White-Box Encoding.

5. B. Wyseur, "White-Box Cryptography," PhD thesis, Katholieke Universiteit Leuven, B. Preneel (promotor), 169+32 pages, 2009. URL: http://www.cosic.esat.kuleuven.be/publications/thesis-152.pdf

6. Щелкунов Д.А. О практическом применении White-Box криптографии., // Международная конференция РусКрипто, 2009.

8. Щелкунов Д.А. White-Box криптография, обфускация и защита ПО. Основные направления развития., // Международная конференция РусКрипто, 2010.

9. Dmitry Schelkunov. White-Box Cryptography and SPN ciphers. LRC method. URL: http://eprint.iacr.org/2010/419

10. Joppe W. Bos and Charles Hubain and Wil Michiels and Philippe Teuwen, Differential Computation Analysis: Hiding your White-Box Designs is Not Enough, Cryptology ePrint Archive: Report 2015/753

11. Bogdanov, A., Isobe, T., Tischhauser, E.: Towards practical whitebox cryptography: optimizing efficiency and space hardness. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10031, pp. 126-158. Springer, Heidelberg (2016)

12. Bogdanov, A., Isobe, T.: White-box cryptography revisited: space-hard ciphers. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 1058-1069. ACM (2015)

13. Fouque, P.A., Karpman, P., Kirchner, P., Minaud, B.: Efficient and provable whitebox primitives. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10031, pp. 159-188. Springer, Heidelberg (2016).

14. Gilbert, H.: On White-Box Cryptography. invited talk, Fast Software Encryption 2016 (2016). http://fse.rub.de/slides/wbc_fse2016_hg_2pp.pdf

15. Delerabl´ee, C., Lepoint, T., Paillier, P., Rivain, M.: White-box security notions for symmetric encryption schemes. In: Lange, T., Lauter, K., Lison˘ek, P. (eds.) SAC 2013. LNCS, vol. 8282, pp. 247-264, Springer, Heidelberg (2014).

16. Щелкунов Д.А. Асимметричный SPN-шифр на базе white-box-криптографии и хаотических отображений., // Международная конференция РусКрипто, 2017.

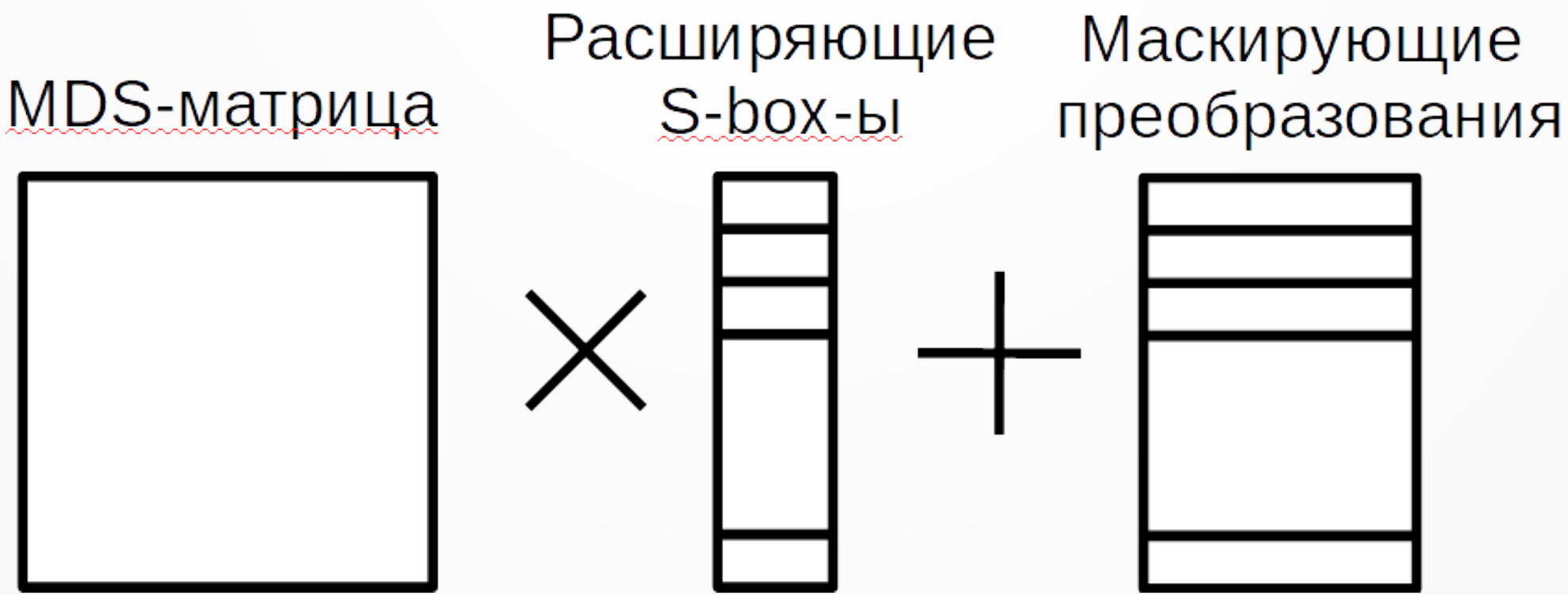
17. Чиликов А.А., Анализ стойкости криптосистемы EVHEN 1., // VIII Юбилейная Всероссийская Научно-Техническая Конференция «Безопасные информационные технологии», 2017.

18. Щелкунов Д.А., Чиликов А.А. EVHEN 2.0. Высокоскоростное асимметричное шифрование на публичном ключе., // VIII Юбилейная Всероссийская Научно-Техническая Конференция «Безопасные информационные технологии», 2017.

Основная проблема white-box-реализаций

- Попытка «упаковать» в таблицы существующие алгоритмы симметричного шифрования
- Биективность преобразований
- White-box-преобразования применяются по отношению к одному раунду

Наш подход


MDS-матрица
Расширяющие S-box-ы
Маскирующие преобразования

Обозначения

$s_i(x_i): x_i^{(t)} \to z_i^{(k)}$ - инъективное таблично заданное нелинейное преобразование,
где t и k соответственно размерности входного и выходного векторов

$F_i^j(x): x_i^{(k)} \to (\beta_i^j)^{(h)}$ также задаётся таблично. $k < h \le \frac{1}{2} v$

$q + m$ - сумма двух полиномов над $GF(2)$, результат которой - вектор размерности v над $GF(2)$

$q \cdot m$ - произведение двух полиномов над $GF(2)$,
результат которого - вектор размерности v над $GF(2)$

M_i^j - квадратная обратимая матрица размерности $k \times k$ над $GF(2)$

$M \times a$ - умножение квадратной обратимой матрицы M размерности $k \times k$
на вектор a размерности k над $GF(2)$

Задача

$$\begin{cases} y_0^i(x_i) = M_0^i \times s_i(x_i) + \lambda_0 \cdot F_0^i(x_i) \\ \dots \\ y_{n-1}^i(x_i) = M_{n-1}^i \times s_i(x_i) + \lambda_{n-1} \cdot F_{n-1}^i(x_i) \end{cases} \quad (1)$$

λ_j - произвольно выбранные полиномы степени h

$$t \le k < h \le \frac{1}{2} v \quad (2)$$

$y_0^i(x_i), y_1^i(x_i) \dots y_{n-1}^{i_i}(x)$ в (1) заданы таблично

При правильно выбранных параметрах и неизвестности $s_i(x_i)$ и $F_j^i(x_i)$,
а также полиномов λ_j, сложность восстановления линейной зависимости между $y_0^i(x_i), y_1^i(x_i) \dots y_{n-1}^{i_i}(x)$, замаскированной суммами с произведениями $\lambda_j \cdot F_j^i(x_i)$ составляет $O(2^v)$

Если параметры известны

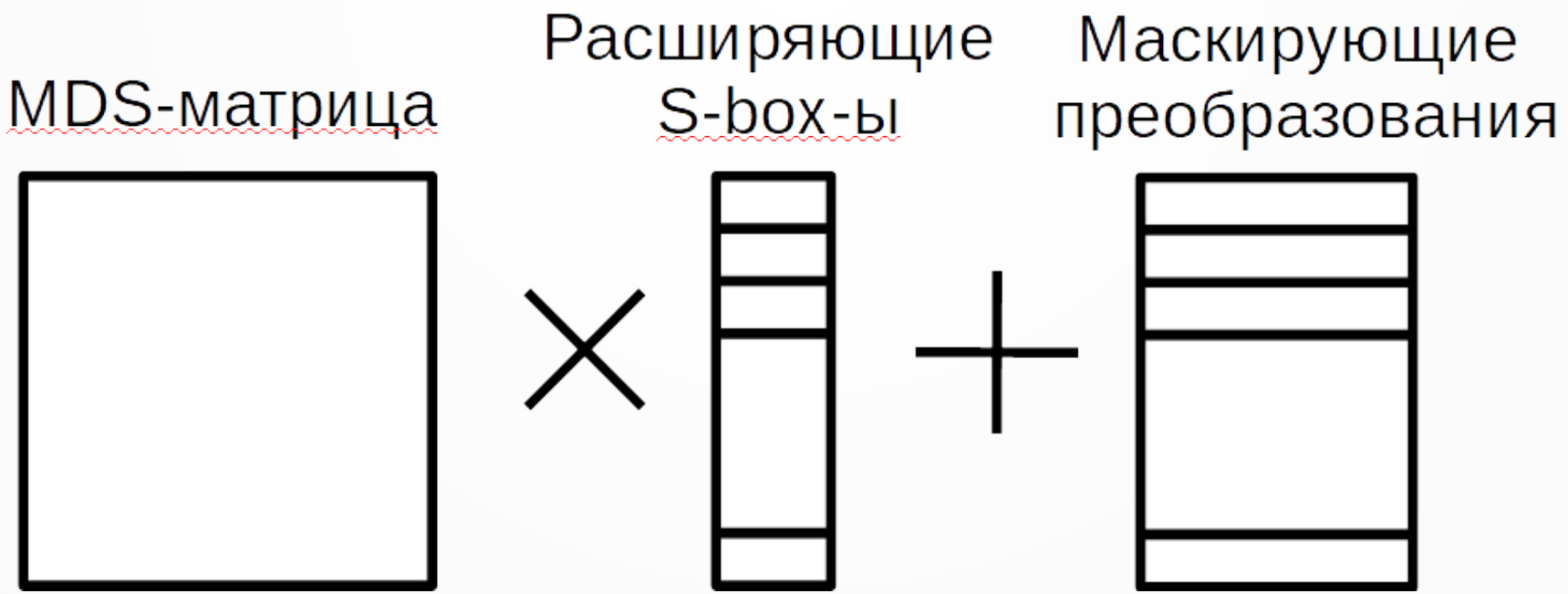
$$\begin{cases} y_0^i(x_i) = M_0^i \times s_i(x_i) + \lambda_0 \cdot F_0^i(x_i) \\ \dots \\ y_{n-1}^i(x_i) = M_{n-1}^i \times s_i(x_i) + \lambda_{n-1} \cdot F_{n-1}^i(x_i) \end{cases} \quad (1) \qquad t \le k < h \le \frac{1}{2} v \quad (2)$$

Пусть $s_i(x_i)$ в (1) известны. Зная значения $M_j^i \times s_i(x_i) + \lambda_j \cdot F_j^i(x_i)$, возможно вычислить значения младших k бит произведений $\lambda_j \cdot F_j^i(x_i)$. А следовательно, восстановить скрытую с помощью сумм с этими произведениями линейную зависимомть между $y_0^i(x_i), y_1^i(x_i) \dots y_{n-1}^{i_i}(x)$ с точностью до линейной части.

Если в (1) известны преобразования $F_j^i(x_i)$, то несложно выделить соответствующие им произведения $M_j^i \times s_i(x_i)$ из сумм $M_j^i \times s_i(x_i) + \lambda_j \cdot F_j^i(x_i)$ посредством редукции по модулю $F_j^i(x_i)$. А следовательно, восстановить скрытую линейную зависимомть между $y_0^i(x_i), y_1^i(x_i) \dots y_{n-1}^{i_i}(x)$ с точностью до линейной части.

Аналогичное можно сказать и про λ_j.

Шифрование



$$\begin{bmatrix} M_0^0 \times s_0(x_0) + \lambda_0 \cdot F_0^0(x_0) \\ \dots \\ M_{n-1}^0 \times s_0(x_0) + \lambda_{n-1} \cdot F_{n-1}^0(x_0) \end{bmatrix} + \dots + \begin{bmatrix} M_0^{n-1} \times s_{n-1}(x_{n-1}) + \lambda_0 \cdot F_0^{n-1}(x_{n-1}) \\ \dots \\ M_{n-1}^{n-1} \times s_{n-1}(x_{n-1}) + \lambda_{n-1} \cdot F_{n-1}^{n-1}(x_{n-1}) \end{bmatrix} \quad (3)$$

Шифрование

$$\begin{bmatrix} M_0^0 \times s_0(x_0) + \lambda_0 \cdot F_0^0(x_0) \\ \dots \\ M_{n-1}^0 \times s_0(x_0) + \lambda_{n-1} \cdot F_{n-1}^0(x_0) \end{bmatrix} + \dots + \begin{bmatrix} M_0^{n-1} \times s_{n-1}(x_{n-1}) + \lambda_0 \cdot F_0^{n-1}(x_{n-1}) \\ \dots \\ M_{n-1}^{n-1} \times s_{n-1}(x_{n-1}) + \lambda_{n-1} \cdot F_{n-1}^{n-1}(x_{n-1}) \end{bmatrix} \quad (3)$$

$$T_0(x_0) \qquad\qquad T_{n-1}(x_{n-1})$$

$T_i(x_i)$ - вектор размерности n, каждый элемент которого - вектор размерности v

Множество всех $T_i(x_i)$ - открытый ключ

Выбор параметров

Для корневой стойкости 128 бит выбираем общую длину блока = 256 бит.

Идеальное решение — невыполнение линейных комбинаций следующего вида:

$$\exists a_i^j \neq 0, a_i^j \in GF(2), \sum_{j=0}^{t-1} \sum_{i=0}^{n-1} a_i^j \cdot s_i(x_i^j) = 0 \qquad (4)$$

$$\exists a_i^j \neq 0, a_i^j \in GF(2), \sum_{i=0,\, j=0}^{n-1} a_i^j \cdot F_i^j(x_i) = 0 \qquad (5)$$

Если (5) не выполняется, то множество значений функций $F_i^j(x_i)$ должно быть базисом векторного пространства размерностью $2^{(t \cdot n)^2}$, что при $n = 64$ и $t = 4$ составляет 2^{65536}.

Выбор параметров

Пусть при некторых коэффициентах a_i^j (4) выполняется. Тогда возможно получить следующее:

$$\sum_{j=0}^{t-1}\sum_{i=0}^{n-1} a_i^j \cdot (\lambda_c \cdot F_c^j(x_i^j)) = \alpha_c \qquad (6),$$

где c - некоторое фиксированное число - номер выражения в сумме (3). Из (6) получаем:

$$\lambda_c \cdot \sum_{j=0}^{t-1}\sum_{i=0}^{n-1} a_i^j \cdot F_c^j(x_i^j) = \alpha_c \qquad (7)$$

Факторизовав α_c, мы получим λ_c. Вычислив все λ_c для $c = 0 \ldots n-1$, атакующий способен демаскировать T-box-ы из суммы (3), что даст ему возможность восстановить MDS-матрицу с точностью до линейной части...

Выбор параметров

$$\lambda_c \cdot \sum_{j=0}^{t-1} \sum_{i=0}^{n-1} a_i^j \cdot F_c^j(x_i^j) = \alpha_c \quad (7)$$

Факторизовав α_c, мы получим λ_c. Вычислив все λ_c для $c = 0 \ldots n-1$, атакующий способен демаскировать T-box-ы из суммы (3), что даст ему возможность восстановить MDS-матрицу с точностью до линейной части...

НО!

Атакующий должен иметь возможность убедиться, что (4) выполняется. Иначе вместо (7) он получит следующее:

$$\lambda_c \cdot \left(\sum_{j=0}^{t-1} \sum_{i=0}^{n-1} a_i^j \cdot F_c^j(x_i^j)\right) + e_c = \alpha_c \quad (8),$$

где e_c - неизвестная ошибка. Факторизовав (8), получим $\hat{\lambda}_c$. Чтобы убедиться, что $\lambda_c = \hat{\lambda}_c$, необходимо убедиться, является ли редуцированный по модулю $\hat{\lambda}_c$ c-й элемент T-box-а помноженным на некоторую матрицу M_i^j s-box-ом, для чего необходимо вычислить $\hat{\lambda}_{c+1 \pmod n}$ и проверить наличие линейной зависимости между элементами с номерами c и $c+1 \pmod n$.

Сложность при n=64, k=16, t=4 составляет $2^{n \cdot k \cdot t} = 2^{4096}$

Выбор параметров

$$\exists a_i^j \neq 0, a_i^j \in GF(2), \sum_{i=0, j=0}^{n-1} a_i^j \cdot F_i^j(x_i) = 0 \qquad (5)$$

Пусть (5) выполняется для каких-либо a_i^j. Предположим, удалось получить следующее:

$$\sum_{i=0, j=0}^{n-1} a_i^j \cdot T_i^j(x_j) = d^{(k)} \qquad (9),$$

где $T_i^j(x_j) = M_i^j \times s_j(x_j) + \lambda_i \cdot F_i^j(x_j)$, $d^{(k)}$ - вектор размерности k (старшие $v-k$ бит $=0$).

$$\sum_{i=0, j=0}^{n-1} a_i^j \cdot (M_i^j \times s_j(x_j) + \lambda_i \cdot F_i^j(x_j)) = d^{(k)} \qquad (10)$$

$$\sum_{i=0, j=0}^{n-1} a_i^j \cdot (M_i^j \times s_j(x_j) + low_k(\lambda_i \cdot F_i^j(x_j)) + high_k(\lambda_i \cdot F_i^j(x_j))) = d^{(k)} \qquad (11),$$

где $low_k(\lambda_i \cdot F_i^j(x_j))$ - вектор размерности v, младшие k бит которого совпадают с младшими k битами $\lambda_i \cdot F_i^j(x_j)$, а остальные $v-k=0$, а $high_k(\lambda_i \cdot F_i^j(x_j))$ - вектор размерности v, младшие k бит которого равны 0, а старшие $v-k$ совпадают с аналогичными из $\lambda_i \cdot F_i^j(x_j)$.

Выбор параметров

$$\exists a_i^j \neq 0, a_i^j \in GF(2), \sum_{i=0, j=0}^{n-1} a_i^j \cdot F_i^j(x_i) = 0 \qquad (5)$$

$$\sum_{i=0, j=0}^{n-1} a_i^j \cdot \left(M_i^j \times s_j(x_j) + low_k(\lambda_i \cdot F_i^j(x_j)) + high_k(\lambda_i \cdot F_i^j(x_j)) \right) = d^{(k)} \qquad (11)$$

Очевидно, что из (11) не следует (5)

И более строго:

$$\sum_{i=0}^{t-1} a_i \cdot \left(M_0^0 \times s_0(i) + low_k(\lambda_0 \cdot F_0^0(i)) + high_k(\lambda_0 \cdot F_0^0(i)) \right) = d^{(k)} \qquad (12)$$

Очевидно, что из (12) - частный случай (11)

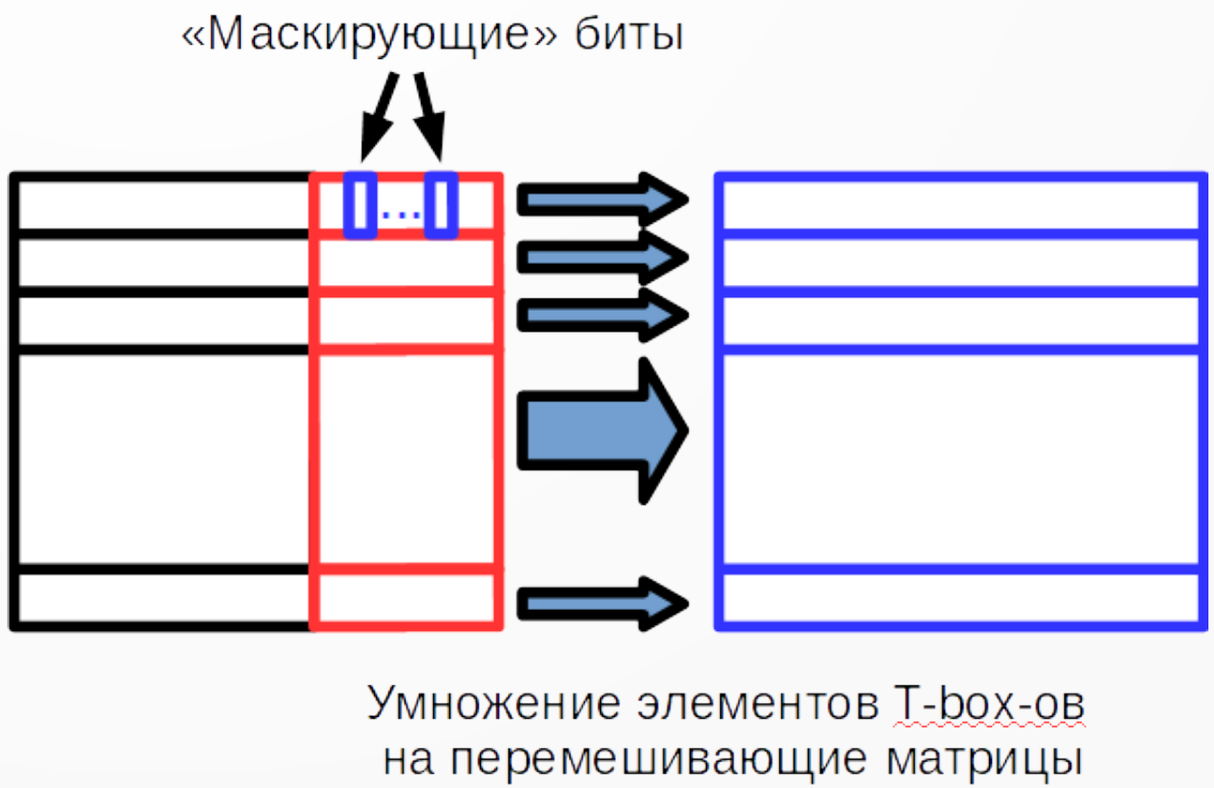
Нахождение маленького вектора $d^{(k)}$ не несёт практического смысла!

Выбор параметров

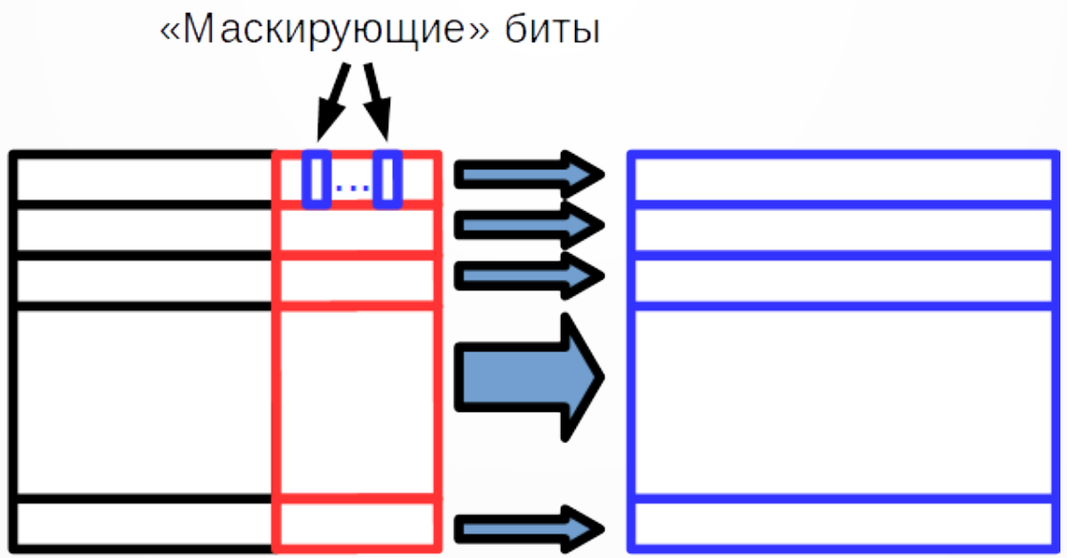
$$\nabla c \in [0 \ldots n-1], \sum_{j=0}^{t-1} a^j \cdot s_c\left(x_c^j\right) = 0 \Rightarrow a^j = 0,\ j \in [0, t-1] \qquad (13)$$

Выбираем $t = 4, k = 16, v = 34$

Увеличим размер элемента T-box-а до 64-х бит:



Дополнительная защита



Умножение элементов T-box-ов
на перемешивающие матрицы

$$\left[\begin{array}{l} L_0 \times Ex_0^0\left(M_0^0 \times s_0(x_0) + \lambda_0 \cdot F_0^0(x_0)\right) \\ L_1 \times Ex_1^0\left(M_1^0 \times s_0(x_0) + \lambda_1 \cdot F_1^0(x_0)\right) \\ \ldots \\ L_{n-1} \times Ex_{n-1}^0\left(M_{n-1}^0 \times s_0(x_0) + \lambda_{n-1} \cdot F_{n-1}^0(x_0)\right) \end{array}\right] + \ldots + \left[\begin{array}{l} L_0 \times Ex_0^{n-1}\left(M_0^{n-1} \times s_{n-1}(x_{n-1}) + \lambda_0 \cdot F_0^{n-1}(x_{n-1})\right) \\ L_1 \times Ex_1^{n-1}\left(M_1^{n-1} \times s_{n-1}(x_{n-1}) + \lambda_1 \cdot F_1^{n-1}(x_{n-1})\right) \\ \ldots \\ L_{n-1} \times Ex_{n-1}^{n-1}\left(M_{n-1}^{n-1} \times s_{n-1}(x_{n-1}) + \lambda_{n-1} \cdot F_{n-1}^{n-1}(x_{n-1})\right) \end{array}\right] \quad (14)$$

Шифрование

$$\begin{bmatrix} L_0 \times Ex_0^0\left(M_0^0 \times s_0(x_0) + \lambda_0 \cdot F_0^0(x_0)\right) \\ L_1 \times Ex_1^0\left(M_1^0 \times s_0(x_0) + \lambda_1 \cdot F_1^0(x_0)\right) \\ \dots \\ L_{n-1} \times Ex_{n-1}^0\left(M_{n-1}^0 \times s_0(x_0) + \lambda_{n-1} \cdot F_{n-1}^0(x_0)\right) \end{bmatrix} + \dots + \begin{bmatrix} L_0 \times Ex_0^{n-1}\left(M_0^{n-1} \times s_{n-1}(x_{n-1}) + \lambda_0 \cdot F_0^{n-1}(x_{n-1})\right) \\ L_1 \times Ex_1^{n-1}\left(M_1^{n-1} \times s_{n-1}(x_{n-1}) + \lambda_1 \cdot F_1^{n-1}(x_{n-1})\right) \\ \dots \\ L_{n-1} \times Ex_{n-1}^{n-1}\left(M_{n-1}^{n-1} \times s_{n-1}(x_{n-1}) + \lambda_{n-1} \cdot F_{n-1}^{n-1}(x_{n-1})\right) \end{bmatrix} \quad (14)$$

$$T_0(x_0) \qquad T_{n-1}(x_{n-1})$$

$Ex_i(x): x^{(v)} \to y^{(l)}$ - добавление маскирующих бит

$Dex_i(x): x^{(l)} \to y^{(v)}$ - извлечение информационных бит

$L_i^{l \times l}$ - обратимая матрица над $GF(2), l = 64$

$T_i(x_i)$ - вектор размерности n, каждый элемент которого - вектор размерности v

Множество всех $T_i(x_i)$ - открытый ключ

Расшифрование

$$\begin{cases} \hat{z}_0 = L_0 \times Ex_0\left(\left(M_0^0 \times s_0(x_0) + \ldots + M_0^{n-1} \times s_{n-1}(x_{n-1})\right) + \lambda_0 \cdot \left(F_0^0(x_0) + \ldots + F_0^{n-1}(x_{n-1})\right)\right) \\ \ldots \\ \hat{z_{n-1}} = L_{n-1} \times Ex_{n-1}\left(\left(M_{n-1}^0 \times s_0(x_0) + \ldots + M_{n-1}^{n-1} \times s_{n-1}(x_{n-1})\right) + \lambda_{n-1} \cdot \left(F_{n-1}^0(x_0) + \ldots + F_{n-1}^{n-1}(x_{n-1})\right)\right) \end{cases} \quad (15)$$

Умножаем каждый l-битный элемент результата на соответствующую ему матрицу, обратную L_i и применяем соответствующие $Dex_i(x): x^{(l)} \rightarrow y^{(v)}$:

$$\begin{cases} \hat{z}_0 = \left(M_0^0 \times s_0(x_0) + \ldots + M_0^{n-1} \times s_{n-1}(x_{n-1})\right) + \lambda_0 \cdot \left(F_0^0(x_0) + \ldots + F_0^{n-1}(x_{n-1})\right) \\ \hat{z}_1 = \left(M_1^0 \times s_0(x_0) + \ldots + M_1^{n-1} \times s_{n-1}(x_{n-1})\right) + \lambda_1 \cdot \left(F_1^0(x_0) + \ldots + F_1^{n-1}(x_{n-1})\right) \\ \ldots \\ \hat{z_{n-1}} = \left(M_{n-1}^0 \times s_0(x_0) + \ldots + M_{n-1}^{n-1} \times s_{n-1}(x_{n-1})\right) + \lambda_{n-1} \cdot \left(F_{n-1}^0(x_0) + \ldots + F_{n-1}^{n-1}(x_{n-1})\right) \end{cases} \quad (16)$$

Редуцируем каждую из строк системы (16) по модулю соответствующего λ_i

Расшифрование

Редуцируем каждую из строк системы (16) по модулю соответствующего λ_i:

$$\begin{cases} \acute{z}_0 = M_0^0 \times s_0(x_0) + \ldots + M_0^{n-1} \times s_{n-1}(x_{n-1}) \\ \acute{z}_1 = M_1^0 \times s_0(x_0) + \ldots + M_1^{n-1} \times s_{n-1}(x_{n-1}) \\ \ldots \\ z'_{n-1} = M_{n-1}^0 \times s_0(x_0) + \ldots + M_{n-1}^{n-1} \times s_{n-1}(x_{n-1}) \end{cases} \quad (17) \qquad \acute{Z} = M \times S(x) \quad (18)$$

Умножив (18) на матрицу, обратную матрице M, получим:

$$\begin{cases} z_0 = s_0(x_0) \\ z_1 = s_1(x_1) \\ \ldots \\ z_{n-1} = s_{n-1}(x_{n-1}) \end{cases} \quad (19)$$

Применим к (19) $g_i(s_i(x_i) = z_i) : s_i(x_i)^{(k)} \rightarrow x_i^{(t)}$ и получим исходные $x_0, x_{1,\ldots}, x_{n-1}$.

Параметры

Сложность шифрования: $O(N)$

Сложность расшифрования: $O(N^3)$

Размер открытого ключа: 4 Мб

Декларируемая стойкость: 128 бит

Операции, используемые при шифровании: выборка из памяти, сложение по модулю 2, запись в память

Шифрование на открытом ключе в режиме реального времени - «на лету»!

Расшифрование тоже очень быстро и нересурсоёмко!

Применение

- Телеметрия
- Управление цифровыми правами (DRM):
  - Формирование случайной последовательности
  - Шифрование её на открытом ключе
  - Отправка результата удалённому ресурсу
  - Удалённый ресурс расшифровывает полученные данные на секретном ключе и возвращает результат
  - Если полученный результат совпадает с исходной случайной последовательностью, проверка пройдена

А что подпись?

- Работа ведётся
- Промежуточный результат: метод коллизий
  - У проверяющего два открытых ключа (два набора разных T-box-ов)
  - Обладатель секретного ключа считает хэш-сумму сообщения, которое хочет отправить (1-я последовательность)
  - Обладатель секретного ключа формирует последовательность большего размера (2-я последовательность)
  - Если результат шифрования 1-й последовательности на 1-ом ключе совпадает с результатом шифрования 2-й последовательности на 2-м, проверка считается пройденной

Щелкунов Д.А., к.т.н., КФ МГТУ имени Н.Э. Баумана, кафедра ЭИУ6-КФ; компания «Рекрипт»
d.schelkunov@gmail.com; schelkunov@re-crypt.com

Чиликов А.А., к.ф.-м.н., МГТУ имени Н.Э. Баумана, кафедра ИУ-8; МФТИ, факультет инноваций и высоких технологий, лаборатория продвинутой комбинаторики и сетевых приложений; Passware, Research Department; Москва
chilikov@passware.com