— Для проверки результата необходимо проверить доказательства всех участников, а также правильность сложения администраций.

Конфиденциальность голосующего сохраняется, если хотя бы одна администрация является честной. Проверяемость результатов достигается благодаря доказательствам с нулевым разглашением. Взлом схемы подразумевает собой решение задачи M-SIS или M-LWE.

Заключение

Разработана постквантовая схема электронного голосования на основе решёток для любого количества кандидатов. В схеме участвует множество администраций, конфиденциальность каждого голоса сохраняется до тех пор, пока хотя бы одна администрация остаётся честной. Проверить финальный результат голосования может любой участник, так как для этого необходимо проверить опубликованные голосующими и администрациями доказательства. Безопасность предложенной схемы основывается на сложности решения задач M-SIS и M-LWE.

ЛИТЕРАТУРА

1. *Del Pino R., Lyubashevsky V., Neven G., and Seiler G.* Practical quantum-safe voting from lattices // Proc. ACM SIGSAC Conf. Comput. Commun. Security. 2017. P. 1565–1581.
2. *Langlois A.and Stehlé D.* Worst-case to average-case reductions for module lattices // Des. Codes Cryptogr. 2015. V. 75. P. 565–599.
3. *Lyubashevsky V. and Seiler G.* Short, invertible elements in partially splitting cyclotomic rings and applications to lattice-based zero-knowledge proofs // LNCS. 2018. V. 10820. P. 204–224.
4. *Baum C., Damgård I., Lyubashevsky V., et al.* More efficient commitments from structured lattice assumptions // LNCS. 2018. V. 11035. P. 368–385.
5. *Baum C., Bootle J., Cerulli A., et al.* Sub-linear lattice-based zero-knowledge arguments for arithmetic circuits // LNCS. 2018. V. 10992. P. 669–699.
6. *Attema T., Lyubashevsky V., and Seiler G.* Practical product proofs for lattice commitments // LNCS. 2020. V. 12171. P. 470–499.
7. *Esgin M., Nguyen N., and Seiler G.* Practical exact proofs from lattices: New techniques to exploit fully-splitting rings // Adv. Cryptology — ASIACRYPT 2020. P. 259–288.

УДК 519.7 DOI 10.17223/2226308X/14/22

ОБ ARX-ПОДОБНЫХ ШИФРСИСТЕМАХ НА БАЗЕ РАЗЛИЧНЫХ КОДИРОВОК НЕАБЕЛЕВЫХ РЕГУЛЯРНЫХ 2-ГРУПП С ЦИКЛИЧЕСКОЙ ПОДГРУППОЙ ИНДЕКСА 2

Б. А. Погорелов, М. А. Пудовкина

В большинстве блочных шифрсистем операции наложения ключа описываются с помощью преобразований из аддитивной группы векторного пространства $(V_m, +)$ над полем GF(2), аддитивной группы $(\mathbb{Z}_{2^m}, +)$ кольца вычетов $\mathbb{Z}_{2^m}$, либо их комбинации. В шифрсистемах типа ARX одновременно используются преобразования трёх типов, где дополнительно введена операция циклического сдвига. В работе обсуждается возможность использования для этих целей неабелевых групп. Рассматриваются подстановочные свойства неабелевых 2-групп с циклической подгруппой индекса 2, т. е. близких к подстановочному представлению группы $(\mathbb{Z}_{2^m}, +)$ и перспективных с точки зрения синтеза блочных шифрсистем. С целью сокращения числа различных групп, используемых в одной шифрсистеме,

целесообразно вместе с группой применять различные её вариации (естественные кодировки элементов, правые и левые регулярные представления). Описываются свойства групп, порождённых такими вариациями, включая условия их imprимитивности, а также совпадения с симметрической группой.

Ключевые слова: *ARX-шифрсистемы, примитивные группы, группа диэдра, группа обобщённых кватернионов, полудиэдральная группа, модулярная максимально-циклическая группа.*

В раундовых преобразованиях большинства блочных шифрсистем обычно используются преобразования из аддитивной группы $(V_m, +)$ m-мерного векторного пространства V_m над полем GF(2), реже — из аддитивной группы $(\mathbb{Z}_{2^m}, +)$ кольца вычетов $\mathbb{Z}_{2^m}$. В ряде шифрсистем используются комбинации таких групп (IDEA, SAFER), действующих параллельно или последовательно. Ещё один класс составляют ARX-шифрсистемы (Addition-Rotation-Xor). Они реализуются с помощью большого числа простых преобразований соответственно из подстановочных представлений групп $(\mathbb{Z}_{2^m}, +)$, $(V_m, +)$ и циклического сдвига координат. Известными представителями ARX-шифрсистем являются TEA, XTEA [1], RC5 [2], RC6 [3], SIMON, SPECK [4].

Естественным развитием этого подхода представляется рассмотрение неабелевых групп, «ближайших» к указанным, а также различных подстановочных представлений таких групп, в том числе связанных с различными кодировками элементов группы. Ранее в работах авторов описаны подстановочные свойства групп с циклической подгруппой индекса 2 [5], классы преобразований на указанных группах [6, 7], а также рассмотрены вопросы марковости [8].

Из теоремы 12.5.1 [9] следует, что неабелевыми группами порядка 2^m с циклической подгруппой индекса 2 являются только четыре группы, удовлетворяющие следующим порождающим соотношениям:

— группа диэдра D_{2^m}, $m \geqslant 3$,

$$a^{2^{m-1}} = e, \quad u^2 = e, \quad ua = a^{-1}u;$$

— обобщённая группа кватернионов Q_{2^m}, $m \geqslant 3$,

$$a^{2^{m-1}} = e, \quad u^2 = a^{2^{m-2}}, \quad ua = a^{-1}u;$$

— модулярная максимально-циклическая группа M_{2^m}, $m \geqslant 4$,

$$a^{2^{m-1}} = e, \quad u^2 = e, \quad ua = a^{1+2^{m-2}}u;$$

— полудиэдральная группа SD_{2^m}, $m \geqslant 4$,

$$a^{2^{m-1}} = e, \quad u^2 = e, \quad ua = a^{-1+2^{m-2}}u.$$

Обозначим через H_m одну из четырёх групп: $H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, SD_{2^m}\}$. Элементы группы H_m будем записывать как $u^{\varepsilon_1}a^{\varepsilon_2}$, где $\varepsilon_1 \in \{0, 1\}$; $\varepsilon_2 \in \{0, \ldots, 2^{m-1} - 1\}$. Пусть $\varphi_{rr} : H_m \to S(H_m)$, $\varphi_{lr} : H_m \to S(H_m)$ — соответственно правое и левое регулярные подстановочные представления, заданные для всех $i \in \{0, \ldots, 2^{m-1} - 1\}$, $x \in H_m$ условиями

$$\varphi_{rr}\left(a^i\right) : x \mapsto xa^i, \quad \varphi_{rr}\left(ua^i\right) : x \mapsto xua^i,$$
$$\varphi_{lr}\left(a^i\right) : x \mapsto a^{-i}x, \quad \varphi_{lr}\left(ua^i\right) : x \mapsto (ua^i)^{-1}x.$$

Пусть $\mathbb{Z}_{2^m}^+, V_m^+$ — правые подстановочные представления аддитивных групп кольца $\mathbb{Z}_{2^m}$ и m-мерного векторного пространства V_m над полем GF(2).

Напомним (см., например, [10]), что транзитивная группа подстановок $G \leqslant S(X)$ называется импримитивной, если существует сохраняемое G нетривиальное разбиение $\mathbf{W}$ множества X на равномощные блоки, т. е.

$$g(W) = \{g(\alpha) | \alpha \in W\} \in \mathbf{W} \text{ для всех } g \in G, W \in \mathbf{W}.$$

Группа $G_m = \left\langle V_m^+,\ \mathbb{Z}_{2^m}^+ \right\rangle$ импримитивна с r-й системой импримитивности $\mathbf{W}^{(r,m)} = \left\{ W_0^{(r,m)}, \ldots, W_{2^r-1}^{(r,m)} \right\}$, где

$$\left| W_t^{(r,m)} \right| = 2^{m-r},$$

$$W_t^{(r,m)} = \left\{ j \in \{0, \ldots, 2^m - 1\} : j \equiv t \pmod{2^r} \right\},\ t = 0, \ldots, 2^r - 1,\ r = 0, \ldots, m.$$

Группа G_m возникает в связи с разными криптографическими приложениями. Её строение описано, например, в [11, 12]. Максимальной подгруппой в S_{2^m}, сохраняющей каждое разбиение $\mathbf{W}^{(0,m)}, \mathbf{W}^{(1,m)}, \ldots, \mathbf{W}^{(m,m)}$, является силовская 2-подгруппа $P_m \in \mathrm{Syl}_2\left(S_{2^m}\right)$, описываемая операцией сплетения $P_m = P_2 \wr P_{m-1}$ и содержащая G_m.

Возможны различные способы задания отображения $v : H_m \to \{0, \ldots, 2^m - 1\}$, кодирующего элементы группы H_m целыми числами из множества $\{0, \ldots, 2^m - 1\}$, которые удобны для использования в криптографических приложениях.

Для $c \in \{rr, lr\}$ отображению v сопоставим естественное изоморфное вложение $\tilde{v} : \varphi_c(H_m) \to S_{2^m}$, такое, что элементу $b \in \varphi_c(H_m)$ ставится в соответствие подстановка $\tilde{v}(b) \in S(\{0, \ldots, 2^m - 1\})$, заданная условием

$$\tilde{v}(b) : v(a) \mapsto v(b(a)) \text{ для всех } a \in H_m.$$

Тем самым каждому элементу $a \in H_m$ и его образу $b(a) \in H_m$ сопоставляются соответственно элементы $v(a), v(b(a)) \in \{0, \ldots, 2^m - 1\}$, которые однозначно задают подстановку $\tilde{v}(b)$ на $\{0, \ldots, 2^m - 1\}$. Далее отображение v будем называть *кодировкой*.

Напомним [10], что у импримитивной группы существуют нетривиальные естественные (подстановочные) гомоморфизмы. Кроме того, импримитивность группы, порождённой криптографическими преобразованиями, в частности раундовыми функциями, может привести к уязвимости шифрсистемы относительно метода гомоморфизмов [13, 14]). В связи с этим описание кодировок v, для которых группы, порождённые комбинациями групп $\tilde{v}(\varphi_{rr}(H_m))$, $\tilde{v}(\varphi_{lr}(H_m))$ и $\mathbb{Z}_{2^m}^+$, являются примитивными, представляет интерес с точки зрения криптографических приложений, включая синтез ARX-шифрсистем и их вариаций.

Пусть $c \in \{lr, rr\}$. В данной работе приведены необходимые и достаточные условия на отображение v, при которых справедливо включение $\tilde{v}(\varphi_c(H_m)) \leqslant P_m$ или равенство $\left\langle \mathbb{Z}_{2^m}^+, \tilde{v}\left(\varphi_c(H_m)\right) \right\rangle = S_{2^m}$. Для преобразования обращения $s \in H_m$, $s : \alpha \mapsto \alpha^{-1}$, и регулярного представления $\tilde{v}(\varphi_c(H_m))$ получены необходимые и достаточные условия справедливости включения $\langle \tilde{v}(s), \tilde{v}(\varphi_c(H_m)) \rangle \leqslant P_m$.

Теорема 1. Пусть $m \geqslant 4$, $H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, SD_{2^m}\}$, биективные отображения $v_d^{(m)} : H_m \to \{0, 1, \ldots, 2^m - 1\}$, $d \in \{1, 2, 3\}$, заданы условиями:

$$v_1^{(m)} : x \mapsto \begin{cases} 2i, & \text{если } x = a^i, \\ 2i + 1, & \text{если } x = ua^i, \end{cases}$$

$$v_2^{(m)} : x \mapsto \begin{cases} i, & \text{если } x = a^i, \\ i + 2^{m-1}, & \text{если } x = ua^i, \end{cases}$$

$$v_3^{(m)} : x \mapsto \begin{cases} i, & \text{если } x = a^i, \\ 2^m - i - 1, & \text{если } x = ua^i, \end{cases}$$

где $x \in H_m$, $i \in \{0, 1, \ldots, 2^{m-1} - 1\}$. Тогда имеют место следующие свойства:

1) Для $\varphi_{rr}(H_m)$

$$\tilde{v}_1^{(m)}(\varphi_{rr}(H_m)) \leqslant P_m,$$
$$\left\langle \tilde{v}_1^{(m)}(s), \tilde{v}_1^{(m)}(\varphi_{rr}(H_m)) \right\rangle \leqslant P_m \text{ для } H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, SD_{2^m}\},$$
$$\tilde{v}_2^{(m)}(\varphi_{rr}(H_m)) \leqslant P_m \text{ для } H_m \in \{D_{2^m}, M_{2^m}\}.$$

Кроме того,

а) $\left\langle \mathbb{Z}_{2^m}^+, \tilde{v}_2^{(m)}(\varphi_{rr}(H_m)) \right\rangle = S_{2^m}$ для каждой $H_m \in \{Q_{2^m}, SD_{2^m}\}$;

б) $\left\langle \mathbb{Z}_{2^m}^+, \tilde{v}_2^{(m)}(\varphi_{rr}(H_m)) \right\rangle = S_{2^m}$, $\left\langle \mathbb{Z}_{2^m}^+, \tilde{v}_3^{(m)}(\varphi_{rr}(H_m)) \right\rangle = S_{2^m}$ для каждой $H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, SD_{2^m}\}$.

2) Для $\varphi_{lr}(H_m)$

$$\tilde{v}_1^{(m)}(\varphi_{lr}(H_m)) \leqslant P_m,$$
$$\left\langle \tilde{v}_1^{(m)}(s), \tilde{v}_1^{(m)}(\varphi_{lr}(H_m)) \right\rangle \leqslant P_m \text{ для } H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, SD_{2^m}\},$$
$$\tilde{v}_2^{(m)}(\varphi_{lr}(H_m)) \leqslant P_m \text{ для } H_m = M_{2^m},$$
$$\tilde{v}_3^{(m)}(\varphi_{lr}(H_m)) \leqslant P_m \text{ для } H_m \in \{D_{2^m}, SD_{2^m}\}.$$

Кроме того,

а) $\left\langle \mathbb{Z}_{2^m}^+, \tilde{v}_2^{(m)}(\varphi_{lr}(H_m)) \right\rangle = S_{2^m}$ для каждой $H_m \in \{D_{2^m}, Q_{2^m}, SD_{2^m}\}$;

б) $\left\langle \mathbb{Z}_{2^m}^+, \tilde{v}_3^{(m)}(\varphi_{lr}(H_m)) \right\rangle = S_{2^m}$ для каждой $H_m \in \{M_{2^m}, Q_{2^m}\}$.

Заметим, что группа $\mathbb{Z}_{2^m}^+$ порождена полным циклом $(0, \ldots, 2^m - 1)$. При доказательстве теоремы 1 использовано свойство, что примитивная группа, содержащая полный 2^m-цикл, изоморфна симметрической группе S_{2^m} или естественному подстановочному представлению степени 2^m проективной группы $PGL(2, p)$, $p = 2^m - 1$ — простое число [15].

ЛИТЕРАТУРА

1. *Wheeler D. J. and Needham R. M.* TEA, a Tiny Encryption Algorithm // LNCS. 1995. V. 1008. P. 363–366.
2. *Rivest R. L.* The RC5 encryption algorithm // LNCS. 1995. V. 1008. P. 86–96.
3. *Rivest R. L., Robshaw M. J. B., Sidney R., and Yin Y. L.* The RC6 Block Cipher. V1.1, AES Proposal. 1998. `http://www.rsa.com/rsalabs/aes`.
4. *Beaulieu R., Shors D., Smith J., et al.* The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive. 2013. `https://eprint.iacr.org/2013/404`.
5. *Погорелов Б. А., Пудовкина М. А.* Подстановочные представления неабелевых 2-групп с циклической подгруппой индекса 2 // Матем. вопр. криптогр. 2021. Т. 12. (в печати)

6. *Погорелов Б. А., Пудовкина М. А.* Вариации ортоморфизмов и псевдоадамаровых преобразований на неабелевой группе // Прикладная дискретная математика. Приложение. 2019. № 12. С. 24–27.
7. *Погорелов Б. А., Пудовкина М. А.* О классе степенных кусочно-аффинных подстановок на неабелевой группе порядка 2^m, обладающей циклической подгруппой индекса два // Прикладная дискретная математика. Приложение. 2019. № 12. С. 27–29.
8. *Погорелов Б. А., Пудовкина М. А.* Неабелевость группы наложения ключа и свойство $\otimes_{\mathbf{W}}$-марковости алгоритмов блочного шифрования // Матем. вопр. криптогр. 2020. Т. 11. № 4. С. 3–22.
9. *Холл М.* Теория групп. М.: ИЛ, 1962. 468 с.
10. *Dixon J. D. and Mortimer B.* Permutation Groups. Berlin: Springer Verlag, 1996. 346 p.
11. *Grossman E.* Group Theoretic Remark on Cryptographic System Based on Two Types of Additions. Math. Sc. Dept. IBM Watson res. Center Yorktown Heights, 1974.
12. *Погорелов Б. А., Пудовкина М. А.* Надгруппы аддитивных регулярных групп порядка 2^m кольца вычетов и векторного пространства // Дискретная математика. 2015. Т. 27. № 3. С. 74–94.
13. *Бабаш А. В., Шанкин Г. П.* Криптография. М.: СОЛОН-Р, 2002. 512 с.
14. *Paterson K. G.* Imprimitive permutation groups and trapdoors in iterated block ciphers // LNCS. 1999. V. 1636. P. 201–214.
15. *Погорелов Б. А.* Примитивные группы подстановок, содержащие 2^m-цикл // Алгебра и логика. 1980. Т. 19. № 2. С. 236–247.

УДК 519.7 DOI 10.17223/2226308X/14/23

ПОРОЖДЕНИЕ ДОПОЛНИТЕЛЬНЫХ ОГРАНИЧЕНИЙ В ЗАДАЧАХ АЛГЕБРАИЧЕСКОГО КРИПТОАНАЛИЗА ПРИ ПОМОЩИ SAT-ОРАКУЛОВ[1]

А. А. Семёнов, К. В. Антонов, И. А. Грибанова

Описывается новая техника, предназначенная для дополнения исходной системы ограничений в задаче алгебраического криптоанализа новыми ограничениями. Порождаемые ограничения могут иметь форму линейных уравнений над полем из двух элементов в случае, если задача криптоанализа сведена к квадратичной системе над GF(2). Если же рассматриваемая задача сведена к SAT, то порождаемые ограничения имеют вид эквивалентностей или единичных резольвент. Для обеих ситуаций мы показываем, что порождаемые ограничения могут снижать оценки трудоёмкости криптоанализа.

Ключевые слова: *алгебраический криптоанализ, проблема булевой выполнимости (SAT), квадратичные системы уравнений над GF(2), SAT-оракул.*

1. Предварительные результаты

Везде далее под термином «ограничение» понимается либо линейное уравнение над GF(2), либо дизъюнкт. Рассматривается задача обращения функции вида

$$f : \{0,1\}^n \to \{0,1\}^m, \tag{1}$$

заданной некоторым алгоритмом A_f: то есть требуется, зная A_f и произвольное $\gamma \in \in \operatorname{Range} f \subseteq \{0,1\}^m$, найти такое $\alpha \in \{0,1\}^n$, что $f(\alpha) = \gamma$.

[1]Грибанова И. А. поддержана стипендией Президента РФ (СП-3545.2019.5).