Утверждение 1. Пусть в некоторой неодноэлементной связной компоненте графа эквивалентности ключей шифра существует цикл нечётной длины. Тогда данный шифр минимален по включению.

Таким образом, в работе предложен графовый подход к исследованию и описанию совершенных шифров, их аналогов и обобщений. В рамках предлагаемого подхода доказано утверждение (достаточное условие минимальности шифра по включению), которое может служить основой для дальнейших обобщений; приведены примеры, иллюстрирующие эффективность подхода. Полученные результаты могут быть применены и для изучения почти совершенных шифров.

ЛИТЕРАТУРА

1. *Шеннон К.* Теория связи в секретных системах // Работы по теории информации и кибернетике. М.: Наука, 1963. С. 333–402.
2. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2001.
3. *Зубов А. Ю.* Совершенные шифры. М.: Гелиос АРВ, 2003.
4. *Зубов А. Ю.* Почти совершенные шифры и коды аутентификации // Прикладная дискретная математика. 2011. № 4(14). С. 28–33.
5. *Зубов А. Ю.* О понятии ε-совершенного шифра // Прикладная дискретная математика. 2016. № 3(33). С. 45–52.
6. *Медведева Н. В., Титов С. С.* Аналоги теоремы Шеннона для эндоморфных неминимальных шифров // Прикладная дискретная математика. Приложение. 2016. № 9. С. 62–65.
7. *Медведева Н. В., Титов С. С.* Описание неэндоморфных максимальных совершенных шифров с двумя шифрвеличинами // Прикладная дискретная математика. 2015. № 4 (30). С. 43–55.
8. *Медведева Н. В., Титов С. С.* Геометрическая модель совершенных шифров с тремя шифрвеличинами // Прикладная дискретная математика. Приложение. 2019. № 12. С. 113–116.
9. *Медведева Н. В., Титов С. С.* Конструкции неэндоморфных совершенных шифров // Прикладная дискретная математика. Приложение. 2020. № 13. С. 51–54.

УДК 512.55+003.26 DOI 10.17223/2226308X/14/21

ПОСТКВАНТОВОЕ ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ НА ОСНОВЕ РЕШЁТОК ПРИ УЧАСТИИ НЕСКОЛЬКИХ КАНДИДАТОВ

Д. А. Набоков

В последние годы появляется множество эффективных криптографических схем на основе решёток, среди которых стоит отметить (полностью) гомоморфное шифрование и протокол конфиденциального вычисления. Такие схемы на решётках интересны тем, что являются стойкими к атакам квантового компьютера. В работе реализована схема электронного голосования, эффективно поддерживающая нескольких кандидатов, за которых можно голосовать. Возможны два варианта голосования: голос за единственного кандидата или голоса для любого подмножества кандидатов. В схеме присутствует множество администраций, конфиденциальность голосов сохраняется в случае, когда хотя бы одна администрация остаётся честной. Схема направлена на соблюдение конфиденциальности голосов и проверямости результатов; для соблюдения других часто рассматриваемых свойств безопасности электронного голосования используются различные предположения,

например, что у каждой администрации есть открытые ключи всех допущенных к голосованию лиц. В основе устройства схемы лежат доказательства с нулевым разглашением и схема обязательства с гомоморфными по сложению свойствами. Благодаря доказательствам с нулевым разглашением, проверить результаты голосования может любой участник схемы.

Ключевые слова: *решётки, электронное голосование, схема обязательства, доказательство с нулевым разглашением, амортизированное доказательство открытия.*

Введение

В работе [1] представлена схема электронного голосования, безопасность которой основана на сложности задач на решётках: M-SIS и M-LWE [2]. Считается, что эти задачи являются сложными как для классического, так и для квантового компьютера, то есть получившаяся схема является постквантовой. Предложенная в [1] схема обеспечивает конфиденциальность голоса и проверяемость результатов, в качестве голоса выступает значение из $\{0,1\}$, то есть голосование производится за одного кандидата. Авторы предлагают способ расширения схемы при участии в голосовании нескольких кандидатов, однако их способ неэффективен.

Настоящая работа посвящена эффективному расширению постквантовой схемы электронного голосования из [1] для нескольких кандидатов. В связи с этим модель безопасности схемы и доказательство безопасности аналогичны оригинальной. Основные отличия заключаются в следующем:

— В качестве голоса выступает вектор $\mathbf{v} \in \{0,1\}^{N_c}$ (N_c — количество кандидатов), для которого можно потребовать, чтобы его вес был равен единице. Основной сложностью такого расширения схемы для нескольких кандидатов является возможность доказательства, что голос в отправляемом бюллетене правильно сформирован.

— Так как голос уже не элемент из $\{0,1\}$, то для данной схемы разработано новое доказательство корректности голоса в публикуемом бюллетене, именуемое в дальнейшем `VProof`. Соответственно, доказательство OR-proof заменено на `VProof`.

— Используется более эффективное амортизированное доказательство открытия.

В основе схемы лежат такие криптографические конструкции, как доказательства с нулевым разглашением и схема обязательства (commitment scheme).

1. Криптографические конструкции

В эффективных криптографических схемах на решётках вычисления обычно проводятся в кольце $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^d+1)$ для простого q и целого d, являющегося степенью двойки.

Для различных q, d многочлен $X^d + 1$ может разлагаться в кольце $\mathbb{Z}_q$ на произведение многочленов меньшей степени. Пусть $l|d$ и $q - 1 \equiv 2l \mod 4l$, тогда, согласно [3, Theorem 2.3],

$$X^d + 1 = \prod_{i \in \mathbb{Z}_{2l}^*} (X^{d/l} - \zeta^i),$$

где $X^{d/l} - \zeta^i$ является неприводимым над $\mathbb{Z}_q$ многочленом, а ζ^i пробегает все $2l$ корней из единицы. В $\mathbb{Z}_q$ не существует элементов, порядок которых больше $2l$.

Подобное разложение позволяет работать с многочленами аналогично Китайской Теореме об остатках. Определим такое отображение NTT, которое переводит многочлен $m \in \mathcal{R}_q$ в набор многочленов $\mathrm{NTT}(m) = (\check{m}_0, \ldots, \check{m}_{l-1})$, где

$$\check{m}_i = m \bmod (X^{d/l} - \zeta^{2i+1}).$$

Многочлены $\check{m}_0, \ldots, \check{m}_{l-1}$ будем называть NTT-коэффициентами m. Вектор $\mathbf{v}$ можно разбить на блоки из l коэффициентов и представить его в виде многочленов $m_1, \ldots, m_{\lceil N_c/l \rceil} \in \mathcal{R}_q$, таких, что NTT-коэффициенты m_i являются i-м блоком вектора $\mathbf{v}$ (последний блок дополняется нулями). В таком представлении NTT-коэффициентами являются многочлены нулевой степени.

Определение 1 [4]. Для открытой случайной матрицы $B_0 \in \mathcal{R}_q^{\varkappa \times (\varkappa+\lambda+n)}$ и открытых случайных векторов $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathcal{R}_q^{\varkappa+\lambda+n}$, а также секретного короткого вектора $\mathbf{r} \leftarrow \chi^{(\varkappa+\lambda+n)d}$ из распределения шума χ обязательством к сообщениям $m_1, \ldots, m_n \in \mathcal{R}_q$ является

$$\begin{aligned} \mathbf{t}_0 &= B_0\mathbf{r}, \\ t_1 &= \langle \mathbf{b}_1, \mathbf{r} \rangle + m_1, \\ &\ldots \\ t_n &= \langle \mathbf{b}_n, \mathbf{r} \rangle + m_n, \end{aligned}$$

где размер открытых векторов и матрицы зависит от количества сообщений n и параметров $\varkappa$ и λ, от которых зависит сложность задач M-SIS и M-LWE соответственно (стоит отметить, что сложность зависит и от других параметров, например d и χ).

Чтобы открыть данное обязательство, достаточно опубликовать вектор $\mathbf{r}$, для которого выполняется равенство $\mathbf{t}_0 = B_0\mathbf{r}$. Сообщения m_i находятся как $t_i - \langle \mathbf{b}_1, \mathbf{r} \rangle$. Задача нахождения m_i из обязательства сводится к задаче M-LWE, задача получения другого открытия r^* — к M-SIS. Наиболее эффективные схемы получаются при таком выборе параметров, что обе задачи имеют примерно одинаковую стойкость.

Схема обладает важным гомоморфным свойством: при сложении обязательств получается обязательство к сообщению, равному сумме исходных сообщений, однако в этом случае используется вектор $\mathbf{r}$ с бóльшими коэффициентами, из-за чего стойкость одной из задач ниже. То есть параметры в этом случае необходимо выбрать так, чтобы как исходное обязательство, так и их сумма были безопасными. Соответственно при суммировании большого числа обязательств схема может стать неэффективной.

Иногда возникает необходимость доказать, что опубликовавший обязательство действительно может предоставить короткий $\mathbf{r}$ (не опубликовывая его), которое открывает обязательство. Такое доказательство называется доказательством открытия (opening proof).

Определение 2. Амортизированным доказательством открытия для обязательств $(\mathbf{t}_0 \| t_1 \| \ldots \| t_n)_i$, $i = 1, \ldots, p$, является протокол между доказывающим и проверяющим, в результате которого проверяющий убеждается, что доказывающий знает $\mathbf{r}_i^*$, такие, что $\bar{c}\mathbf{t}_{0,i} = B_0\mathbf{r}_i^*$ для короткого обратимого многочлена $\bar{c}$ и вектора $\mathbf{r}_i^*$ с несколько бóльшими по сравнению с $\mathbf{r}_i$ коэффициентами.

В результате амортизированного доказательства открытия доказывается более слабое относительно желаемого утверждение. Выбирать параметры необходимо так, чтобы найти такие $\mathbf{r}_i^*$ было трудно. Так как для всех обязательств используется один и тот же фиксированный многочлен $\bar{c}$, эти обязательства можно гомоморфно складывать. В работе используется амортизированное доказательство открытия из [5, Section 3], которое является более эффективным по сравнению с используемым в [1].

Доказательство `VProof`, позволяющее доказать, что голос является правильно сформированным в предоставленном обязательстве, реализуется на основе доказательства произведения [6] и доказательства неструктурированной линейной связи (unstructured linear relation) [7].

Доказательство произведения для обязательства к сообщениям m_1, m_2, m_3 направлено на доказательство $m_1 \cdot m_2 = m_3$. Модифицируем его таким образом, чтобы доказывать $m_i(m_i - 1) = 0$ (эта модификация достаточно простая и не влияет на безопасность доказательства, однако конкретные детали опустим). При умножении многочленов из $\mathcal{R}_q$ их NTT-коэффициенты умножаются покоординатно. В итоге для каждого NTT-коэффициента $\check{m}$ выполняется

$$\check{m}(\check{m} - 1) = 0 \pmod{X^{d/l} - \zeta^j},$$

а так как $X^{d/l} - \zeta^j$ является неприводимым многочленом, то $\check{m}$ равняется либо 0, либо 1. В итоге для обязательства можно доказать, что NTT-коэффициенты его сообщений являются двоичной строкой. Так как вектор $\mathbf{v}$ дополняется нулями до кратности l, то для m_n уравнение изменяется на $m_n(m_n - m') = 0$, где NTT-коэффициенты m' сначала единицы, а потом нули, причём количество нулей равно $l - (N_c \mod l)$. То есть в итоге доказывается принадлежность NTT-коэффициентов $\{0, 1\}^{N_c}$.

С помощью доказательства неструктурированной линейной связи для открытой матрицы $A \in \mathbb{Z}_q^{\alpha \times nl}$ и открытого вектора $\mathbf{u} \in \mathbb{Z}_q^{\alpha}$ можно доказать $A\mathbf{v} = \mathbf{u}$. Нас интересует случай $\alpha = 1$, $A = (1 \dots 1)$, $\mathbf{u} = (1)$, то есть сумма коэффициентов вектора $\mathbf{v}$ должна быть равна единице.

Доказательство `VProof` можно воспринимать как одновременное применение этих двух доказательств. Стоит заметить, что доказательство неструктурированной линейной связи используется для классического понимания голосования, то есть выбор ровно одного кандидата из многих. Это доказательство можно опустить, тогда правильным голосом будет считаться голос за любое подмножество кандидатов. Или можно в качестве A и $\mathbf{u}$ брать более сложные конструкции для обеспечения каких-то нетривиальных требований на голоса.

Доказательства произведения и неструктурированной линейной связи в оригинальных работах представлены как интерактивные протоколы, для которых доказаны свойства корректности и полноты, а также нулевого разглашения, если проверяющий является честным. Приведём (неформальную) теорему о свойствах интерактивного протокола для `VProof`.

Теорема 1. Интерактивный протокол для доказательства `VProof` обладает следующими свойствами:

— Полнота (Completeness): честный доказывающий убеждает честного проверяющего с вероятностью, близкой к единице.
— Корректность (Soundness): существует извлекатель знания (knowledge extractor), который, имея доступ к детерминированному доказывающему $\mathcal{P}^*$, представленному в виде чёрного ящика с возможностью перемотки, либо выдаёт открытие обязательства к сообщению m^*, являющемуся корректным голосом, либо решение задачи M-SIS.
— Нулевое разглашение с честным проверяющим (honest verifier zero-knowldge): существует симулятор, который способен симулировать успешные взаимодействия между доказывающим и проверяющим. Способность различать реальное взаимодействие от симулированного сводится к решению задачи M-LWE.

Свойство нулевого разглашения применяется только в случае честного проверяющего, это ограничение можно нивелировать, преобразовав интерактивный протокол в неинтерактивный с помощью замены проверяющего на случайный оракул.

Строгая формулировка теоремы 1, а также её доказательство аналогичны работам [6, 7].

2. Набросок схемы электронного голосования

В данной работе разработана схема электронного голосования со множеством голосующих, администраций (authority) и кандидатов. В наброске мы опишем схему для $n = 1$. Схема легко расширяется для большего числа сообщений, но усложняется индексация.

Чтобы опубликовать бюллетень, голосующий i делает следующее:

— Пусть $m_i \in \mathcal{R}_q$ — сообщение, являющееся правильным голосом.

— Голосующий разделяет голос между N_a администрациями: $x_i^{(1)}, \ldots, x_i^{(N_a)} \leftarrow\!\!\$\, \mathcal{R}_q$: $\sum\limits_{j=1}^{N_a} x_i^{(j)} = m_i$.

— Голосующий создаёт N_a обязательств к $x_i^{(j)}$ с секретными векторами $\mathbf{r}_i^{(j)} \leftarrow \leftarrow \chi^{(\varkappa+\lambda+1)d}$.

— Используя `VProof`, он доказывает, что обязательство к m_i для секретного вектора $\sum\limits_{j=1}^{N_a} \mathbf{r}_i^{(j)}$ содержит в себе корректный голос.

— Голосующий зашифровывает $\mathbf{r}_i^{(j)}$ с помощью открытого ключа j-й администрации и публикует его вместе со всеми обязательствами и доказательством.

Сумма всех случайных многочленов $x_i^{(j)}$ является финальным результатом голосования. Эта сумма находится по частям: каждая j-я администрация находит сумму $\sum\limits_i x_i^{(j)}$ и публикует промежуточную сумму.

Порядок действий каждой администрации:

— Администрация расшифровывает все секретные векторы пользователей, предназначенных для неё.

— Амортизированно доказывает открытие обязательств для этих секретных векторов.

— Администрация находит сумму этих обязательств и сумму соответствующих секретных векторов и публикует эти суммы вместе с амортизированным доказательством открытия.

При сложении обязательств коэффициенты секретного вектора растут, что снижает безопасность схемы и может привести к неэффективному выбору параметров. Для решения этой проблемы вводится параметр u. Администрация может складывать не более u обязательств. Так как администрация знает все сообщения, она может создать новое обязательство (со «свежим» секретным вектором) к сообщению, являющемуся суммой сообщений в этих u обязательствах. Дальше необходимо доказать, что сообщение в свежем обязательстве корректно, для этого используется доказательство открытия к нулю для обязательства, равного разности свежего обязательства и сумме u старых. Доказательство открытия к нулю показывает, помимо $\bar{c}\mathbf{t}_0 = B_0\mathbf{r}^*$, ещё $\bar{c}t_1 = \langle \mathbf{b}_1, \mathbf{r}^* \rangle$, то есть в этом обязательстве нулевое сообщение.

В итоге u старых обязательств заменяются на одно новое. Этот процесс можно продолжать сколько угодно, пока не останется u или меньше обязательств.

Порядок действий для подведения результатов голосования и его проверки:

— Для вычисления результата голосования необходимо сложить промежуточные суммы всех администраций.

— 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,