Геометрия и алгебра

Geometry and algebra

УДК 519.719.2

СОВЕРШЕННАЯ ВЕРИФИКАЦИЯ МОДУЛЯРНОЙ СХЕМЫ

Г. В. МАТВЕЕВ[1)]***, В. В. МАТУЛИС***[1)]

[1)]*Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь*

Схемы разделения секрета используются для распределения секретного значения среди группы пользователей таким образом, что только разрешенные подмножества пользователей могут правильно восстановить секрет. Изучаемая нами модулярная схема разделения секрета основывается на китайской теореме об остатках. В этой схеме секреты $s(x)$, $S(x)$, $s_1(x), \ldots, s_k(x)$ определяются следующим образом: $s(x) = S(x) \bmod m(x)$, $s_i(x) = S(x) \bmod m_i(x)$, $i = 1, 2, \ldots, k$. Все секреты $s(x)$, $S(x)$, $s_1(x), \ldots, s_k(x)$ и модули $m(x)$, $m_1(x), \ldots, m_k(x)$ являются элементами кольца полиномов $F_p[x]$, а восстановление секрета $s(x)$ осуществляется путем применения упомянутой китайской теоремы об остатках. Под верификацией любой схемы разделения секрета понимают протокол проверки участниками их частичных секретов и (или) протокол проверки законности действий дилера. В работе предлагаются способы совершенной верификации модулярной схемы разделения секрета. Это означает, что в результате верификации никто из участников и неразрешенные подмножества участников не получают никакой информации о секрете $s(x)$, кроме априорной. Представлены два способа верификации. Первый способ – более простой, он основан на предположении о честности дилера. Если дилер нечестный, то верификация является более сложной. Оба способа основываются на одной работе Дж. Бенало и обобщают протокол, предложенный ранее М. Васьковским и Г. Матвеевым в двух направлениях. Во-первых, верифицируется общая, а не только пороговая структура доступа, а во-вторых, дилер не обязательно честный. Ранее Н. Шенец нашел условие совершенности модулярной схемы разделения секрета. Таким образом, при соблюдении этого условия совершенными являются и указанная схема, и протокол ее верификации.

Ключевые слова: полиномиальная модулярная схема; теория разделения секрета; верификация; секрет; частичный секрет; конечное поле.

Образец цитирования:
Матвеев ГВ, Матулис ВВ. Совершенная верификация модулярной схемы. *Журнал Белорусского государственного университета. Математика. Информатика.* 2018;2:4–9.

For citation:
Matveev GV, Matulis VV. Perfect verification of modular scheme. *Journal of the Belarusian State University. Mathematics and Informatics.* 2018;2:4–9. Russian.

Авторы:
Геннадий Васильевич Матвеев – доцент кафедры высшей математики факультета прикладной математики и информатики.
Владислав Вячеславович Матулис – магистрант кафедры высшей математики факультета прикладной математики и информатики. Научный руководитель – Г. В. Матвеев.

Authors:
Gennadii V. Matveev, associate professor at the department of higher mathematics, faculty of applied mathematics and informatics.
matveev@bsu.by
Vladislav V. Matulis, master's degree student at the department of higher mathematics, faculty of applied mathematics and informatics.
uladzislau.matulis@yandex.by

PERFECT VERIFICATION OF MODULAR SCHEME

***G. V. MATVEEV*[a], *V. V. MATULIS*[a]**

[a]*Belarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus*
Corresponding author: V. V. Matulis (uladzislau.matulis@yandex.by)

Secret sharing schemes are used to distribute a secret value among a group of users so that only authorized set of them can reconstruct the original secret correctly. The modular secret sharing scheme (MSSS) we are studying is based on the Chinese Remainder Theorem. In this scheme the secrets $s(x)$, $S(x)$, $s_1(x), \ldots, s_k(x)$ are defined as follows $s(x) = S(x) \bmod m(x)$, $s_i(x) = S(x) \bmod m_i(x)$, $i = 1, 2, \ldots, k$. All the secrets and moduli are chosen from polynomial ring $F_p[x]$, and the reconstruction of secret $s(x)$ is carried out by applying the above-mentioned Chinese Remainder Theorem. The verification of any secret sharing scheme is understood as the protocol of verification by the participants of their partial secrets and (or) the protocol for verifying the legitimacy of the actions of the dealer. In this paper, we introduce a perfect verification protocol of MSSS. It means that none information leaks under distribution and verification. Two verification protocols are introduced in this paper. The first one is simpler and it depends on assumption about dealer honesty. If there is no such assumption verification is more complex. Both protocols are based on one work by J. Benalo and generalize the protocol proposed earlier by M. Vaskovsky and G. Matveev in two ways. First, the general, not only the threshold access structure is verified, and secondly, the dealer is not necessarily honest. Earlier, N. Shenets found the perfection condition of MSSS. Thus, if these conditions are met, both the MSSS and its verification protocol are perfect.

Key words: polynomial modular scheme; secret sharing; verification; secret; partial secret; finite field.

Постановка общей задачи

Схемы разделения секрета относятся к числу важных криптографических протоколов, использующихся в системах электронного голосования [1], шифрования на основе атрибутов [2] и в распределенных конфиденциальных вычислениях [3].

Схема разделения секрета решает следующую задачу. Пусть имеется некоторая важная информация (секрет) s и множество $I = \{1, 2, \ldots, k\}$ пользователей. Требуется сообщить каждому пользователю i некоторую информацию s_i (частичный секрет) таким образом, чтобы только заранее определенные группы участников могли, объединяя свои частичные секреты, восстановить секрет s, а для остальных групп эта задача являлась бы трудноразрешимой. Как правило, под этим понимается, что задача восстановления секрета неразрешенной группой участников должна быть эквивалентна полному перебору.

Дадим точное определение разрешенных и запрещенных подмножеств.

Определение. Под структурой доступа Γ понимают монотонное семейство подмножеств, т. е. предполагается, что для его элементов выполняется условие

$$A \in \Gamma,\ A \subset B \subset I \Rightarrow B \in \Gamma.$$

Эти подмножества называют разрешенными, а остальные – запрещенными.

Структура доступа, когда разрешенными считаются подмножества A с условием $|A| \geq t$, называется пороговой, а число t, $1 \leq t \leq k$, – ее порогом.

Алгоритмы распределения частичных секретов и восстановления исходного секрета называют схемой разделения секрета. Они, в частности, должны обеспечивать правильное восстановление секрета разрешенными группами участников.

Схему разделения секрета называют:

• совершенной, если запрещенное множество участников не получает никакой информации о секрете, кроме априорной;

• идеальной, если ключи всех участников и ключ s имеют один и тот же размер. Иногда условие идеальности включает и совершенность схемы.

Под верификацией схемы разделения секрета понимают протоколы проверки частичных секретов и (или) протокол проверки честности дилера и отдельных участников.

Протокол верификации будем называть совершенным, если его реализация не нарушает совершенность исходной схемы. Отметим, что предложенные ранее [4–6] протоколы верификации не являются таковыми.

Цель настоящего исследования – построение совершенного протокола верификации модулярного разделения секрета. Таким образом, оно является продолжением работы [5], в которой намечен подход к решению рассматриваемой задачи.

Модулярные схемы разделения секрета

В основе модулярных схем разделения секрета лежит деление полиномов с остатком в кольце полиномов $F_q[x]$ над конечным полем F_q.

Выбор параметров и генерация секретов осуществляются таким образом. Сначала выбирается вспомогательный секрет $S(x) \in F_q[x]$ и модули (открытые ключи участников) $m_1(x), m_2(x), \ldots, m_k(x) \in F_q[x]$ и один дополнительный модуль (общий открытый ключ) $m(x)$. Хранимым секретом считается остаток от деления $S(x)$ на $m(x)$: $s(x) = S(x) \bmod m(x)$. Аналогично определяются частичные секреты (закрытые ключи участников) $s_i(x) = S(x) \bmod m_i(x)$, $i = 1, 2, \ldots, k$.

Восстановление секрета $S(x)$ группой участников $1, 2, \ldots, l$, $l \le k$, осуществляется решением системы сравнений

$$\begin{cases} S(x) \equiv s_1(x) \left(\bmod m_1(x)\right), \\ S(x) \equiv s_2(x) \left(\bmod m_2(x)\right), \\ \qquad \ldots \\ S(x) \equiv s_l(x) \left(\bmod m_l(x)\right), \end{cases} \tag{1}$$

а затем находится хранимый секрет $s(x) = S(x) \bmod m(x)$.

В [7] указано, как с помощью специального подбора секрета $S(x)$ и модулей $m_1(x), m_2(x), \ldots, m_k(x)$ можно реализовать любую структуру доступа, и показано, что пороговую структуру доступа можно реализовать и совершенно, и идеально. Эти построения опираются на тот факт, что в кольцах $F_q[x]$ имеются большие семейства попарно взаимно простых многочленов одинаковой степени. Установлено, что такие многочлены $m_1(x), m_2(x), \ldots, m_k(x)$ пригодны для реализации любой (t, k)-пороговой схемы, $1 \le t \le k$, и дано описание максимального по числу элементов такого семейства. Существуют и более простые способы строить достаточно большие семейства попарно взаимно простых многочленов одной и той же степени.

Для разделения секрета в произвольной структуре доступа положим

$$M_2 = \min_{A \in \Gamma} \deg \text{НОК}\left(m_i(x),\ i \in A\right),$$

$$M_1 = \max_{A \notin \Gamma} \deg \text{НОК}\left(m_i(x),\ i \in A\right).$$

Реализация корректна лишь в случае $M_2 > M_1$.

В [8] получен следующий критерий совершенности модулярной реализации общей структуры доступа.

Теорема 1. *Модулярная реализация структуры доступа будет совершенной тогда и только тогда, когда:*

1) $\text{НОД}\left(m(x),\ m_i(x)\right) = 1,\ i = 1, 2, \ldots, k;$

2) $\deg m_0(x) \le M_2 - M_1$.

Далее исследуются модулярные схемы, удовлетворяющие условиям теоремы 1.

Совершенная верификация модулярных схем разделения секрета

Сначала рассмотрим следующую задачу верификации для модулярных схем. Пусть после фазы разделения секрета участники хотят удостовериться в правильности полученных частичных секретов $s_i(x)$ и тем самым в том, что они правильно восстанавливают значение секрета. Дополнительно накладывается требование, чтобы в результате такой проверки никто из участников не извлек никакой дополнительной информации о секрете.

Пусть $A \subset I$ – некоторое подмножество участников. Обозначим через $S_A(x)$ полученное ими решение системы (1), а через $s_A(x)$ – остаток от деления многочлена $S_A(x)$ на многочлен $m(x)$,

$$s_A(x) = S_A(x) \bmod m(x).$$

При корректной реализации модулярной схемы выполнено условие

$$\forall A \in \Gamma,\ s_A(x) = s(x).$$

Проверить это участники не могут – ведь настоящий секрет $s(x)$ им неизвестен. Следуя Дж. Бенало [3], будем проверять более слабые условия:

$$\forall A, B \in \Gamma,\ s_A(x) = s_B(x). \tag{2}$$

Это означает, что все допустимые подмножества участников, восстанавливая секрет, получают одно и то же значение.

Рассмотрим два произвольных подмножества допустимых участников A, $B \in \Gamma$. Нетрудно показать, что

$$P\{s_A(x) = s_B(x) \mid S_A(x) \neq S_B(x)\} = \frac{q^{-n} - q^{-M_2}}{1 - q^{-M_2}},$$

где $n = \deg m(x)$. Это значение не превосходит априорной вероятности угадывания секрета, поэтому можно считать его пренебрежимо малым. Тогда условие (2) можно заменить следующим:

$$\forall A, B \in \Gamma, S_A(x) = S_B(x). \quad (3)$$

Более того, верификация $S(x)$ сильнее верификации $s(x)$. По этой причине далее рассматривается верификация $S(x)$.

Теорема 2. *Условие (3) равносильно тому, что решение системы (1) множеством всех участников имеет степень, меньшую M_2, т. е.* $\deg S_1(x) < M_2$.

Доказательство.

Необходимость. По условию (3) все значения $S_A(x)$, $\forall A \in \Gamma$, равны. Обозначим это значение через $S'(x)$. Пусть $B \in \Gamma$ – допустимое подмножество участников, таких что $\text{НОК}(\{m_i(x), i \in B\}) = M_2$. Тогда $S_1(x) = S'(x) = S_B(x)$, но $\deg S_B(x) < M_2$.

Достаточность. Пусть $\deg S_1(x) < M_2$. Тогда для любого $A \in \Gamma$ верно

$$\deg \text{НОК}(\{m_i(x), i \in A\}) \geq M_2.$$

Поэтому и поскольку $A \subset I$, получаем, что для любого $A \in \Gamma$ выполнено $S_A(x) < S_1(x)$.

Замечание. Ясно, что если реализация схемы корректна и все частичные секреты правильные, то $S_1(x) = S(x)$.

Задача свелась к проверке степени многочлена $S_1(x)$. В то же время публично восстанавливать $S_1(x)$ для такой проверки нельзя, так как это приведет к разглашению секрета $s(x)$. Далее нам потребуется одно простое свойство степени многочлена.

Утверждение. Условие $\deg(P(x) + Q(x)) < l$ равносильно одному из следующих: либо $\deg P(x) < l$ и $\deg Q(x) < l$, либо $\deg P(x) \geq l$ и $\deg Q(x) \geq l$.

Именно это утверждение лежит в основе двух предлагаемых ниже протоколов верификации, охватывающих случаи честного и нечестного дилера.

Случай честного дилера. Если дилер является доверенным лицом, то для верификации может быть использован следующий протокол.

Протокол 1.

1. Дилер генерирует случайный многочлен $S'(x)$ степени меньше M_2, $S'(x) < M_2$.
2. Дилер сообщает каждому участнику значение $s'_i(x) = S'(x) \bmod m_i(x)$, $i = 1, 2, \ldots, k$.
3. Каждый участник публикует значение $p_i(x) = (s_i(x) + s'_i(x)) \bmod m_i(x)$, $i = 1, 2, \ldots, k$.
4. Участники совместно находят решение $P(x)$ системы сравнений относительно $p_i(x)$, $P(x) = S_1(x) + S'(x)$.
5. Участники проверяют степень полученного решения $P(x)$: $\deg P(x) < M_2$.

Если все участники честные, алгоритм решает поставленную задачу полностью. Если же предположить, что есть злоумышленник, который выдает себя за участника i, то вероятность того, что он угадает многочлен $p_i(x)$ и таким образом будет верифицирован, невелика, например, в пороговом случае она равна $1/q^n$, где n – степень многочлена $m_i(x)$.

Предложенный протокол верификации является совершенным: значения $p_i(x)$, $i = 1, 2, \ldots, k$, не несут никакой дополнительной информации о значениях частичных секретов $s_i(x)$, а восстанавливаемое по ним значение $P(x)$ не содержит дополнительной информации о промежуточном секрете $S(x)$.

Случай нечестного дилера. Если дилер не является доверенным лицом, то протокол 1 не будет надежным. Опишем, каким образом он может быть нарушен.

Пусть

$$Q(x) = q_0 + q_1 x + \ldots + q_m x^m,\ P(x) = p_0 + p_1 x + \ldots + p_n x^n \in F_q[x].$$

Обозначим через $R_l[P(x)]$ семейство многочленов:

$$R_l[P(x)] = \{Q(x) \in F_q[x] : \deg Q(x) = \deg P(x), q_i + p_i = 0,\ i = l, \ldots, \deg P(x)\}.$$

Тогда для любого многочлена $Q(x)$ из семейства $R_l[P(x)]$ верно: $\deg(Q(x) + P(x)) < l$.

Предположим, что условие теоремы 2 не выполняется, т. е. $\deg S_1(x) \geq M_2$. В таком случае нечестный дилер в качестве контрольного многочлена $S'(x)$ может взять не случайный многочлен степени меньше M_2, а любой многочлен из $R_{M_2}\left[P(x)\right]$. Тогда $\deg\left(S_1(x)+S'(x)\right) < M_2$ при $\deg S_1(x) \geq M_2$, что приведет к нарушению протокола. В самом деле, участники не могут знать наверняка, что степень контрольного многочлена $S'(x)$ действительно меньше M_2. Если же они захотят восстановить многочлен $S'(x)$, его больше не имеет смысла использовать для верификации, поскольку при известных $S'(x)$ и $S_1(x)+S'(x)$ можно однозначно восстановить $S_1(x)$.

Предлагается следующий способ предотвратить эти действия злоумышленника. Пусть согласно протоколу дилер генерирует не один многочлен, а достаточно много. Тогда участники могут случайным образом разбить их на два непересекающихся подмножества. Многочлены одного из них восстанавливаются непосредственно, чтобы участники могли точно проверить их степень. Для каждого многочлена из другого подмножества выполняется раунд протокола 1.

Протокол 2.

1. Дилер генерирует большое количество N случайных многочленов $S'_j(x), j = 1, 2, \ldots, N, \deg S'_j(x) < M_2$.

2. Каждый из этих многочленов распределяется среди участников, т. е. каждый участник получает $s'_{ij}(x) = S'_j(x) \bmod m_i(x)$, $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, N$.

3. Участники выбирают случайное подмножество $M \subset \{1, 2, \ldots, N\}$ индексов многочленов, которые будут восстанавливаться непосредственно.

4. Участники восстанавливают многочлены $S'_j(x)$ путем публикации соответствующих значений частичных секретов $s'_{ij}(x) = S'_j(x) \bmod m_i(x)$, $i = 1, 2, \ldots, k, j \in M$.

5. Участники проверяют степени восстановленных многочленов, т. е. условие $\deg S'_j(x) < M_2$, $j \in M$. Если это не так, верификация завершается и считается не пройденной.

6. Участники восстанавливают многочлены $s_1(x) + S'_j(x)$ путем публикации $\left(s_i(x) + s'_{ij}(x)\right) \bmod m_i(x)$, $i = 1, 2, \ldots, k$, $j \notin M$.

7. Участники проверяют условие $\deg\left(S_1(x) + S'_j(x)\right) < M_2$ для восстановленных многочленов.

Теперь, если секрет $S_1(x)$ неправильный, дилеру сложнее скрыть этот факт. Для этого ему нужно угадать, каким будет множество M. Тогда в качестве многочленов с номерами из M дилер должен предоставить любые многочлены степени меньше M_2, а все остальные – любые многочлены из $R_{M_2}\left[P(x)\right]$. Если M выбирается случайным образом из всех подмножеств множества $\{1, 2, \ldots, N\}$, вероятность успеха дилера равна $1/2^N$, т. е. за счет выбора N может быть сделана достаточно малой.

Библиографические ссылки

1. Cramer R, Damgård I, Nielsen JB. Multiparty Computation from Threshold Homomorphic Encryption. In: Pfitzmann B, editor. *Advances in Cryptology – EUROCRYPT 2001*. Berlin, Heidelberg: Springer; 2001. p. 280–300. (Lecture Notes in Computer Science; volume 2045). DOI: 10.1007/3-540-44987-6_18.

2. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. *Proceedings of 2007 IEEE Symposium on Security and Privacy*. 2007 May 20–23; Berkeley, California, USA. Los Alamitos, California: IEEE Computer Society; 2007. p. 321–334.

3. Benaloh JC. Secret sharing homomorphisms: keeping shares of a secret secret (extended abstract). In: Odlyzko AM, editor. *Advances in Cryptology – CRYPTO'86.* Berlin, Heidelberg: Springer; 1987. p. 251–260. (Lecture Notes in Computer Science; volume 263). DOI: 10.1007/3-540-47721-7_19.

4. Галибус ТВ, Матвеев ГВ. Верификация параметров модулярного разделения секрета. *Вестник БГУ. Серия 1, Физика. Математика. Информатика.* 2015;1:76–79.

5. Васьковский ММ, Матвеев ГВ. Верификация модулярного разделения секрета. *Журнал Белорусского государственного университета. Математика. Информатика*. 2017;2:17–22.

6. Галибус ТВ. Верификация полиномиального модулярного разделения секрета над двоичным полем. *Вестник Брестского государственного технического университета. Серия 1, Физика, математика, информатика.* 2014;5:26–27.

7. Galibus T, Matveev G. Generalized Mignotte's sequences over polynomial rings. *Electronic Notes Theoretical Computer Science*. 2007;186:43–48. DOI: 10.1016/j.entcs.2006.12.044.

8. Шенец НН. Об информационном уровне модулярных схем разделения секрета. *Доклады Национальной академии наук Беларуси. Серия физико-математических наук.* 2010;54(6):9–12.

References

1. Cramer R, Damgård I, Nielsen JB. Multiparty Computation from Threshold Homomorphic Encryption. In: Pfitzmann B, editor. *Advances in Cryptology – EUROCRYPT 2001*. Berlin, Heidelberg: Springer; 2001. p. 280–300. (Lecture Notes in Computer Science; volume 2045). DOI: 10.1007/3-540-44987-6_18.

2. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. *Proceedings of 2007 IEEE Symposium on Security and Privacy*. 2007 May 20–23; Berkeley, California, USA. Los Alamitos, California: IEEE Computer Society; 2007. p. 321–334.

3. Benaloh JC. Secret sharing homomorphisms: keeping shares of a secret secret (extended abstract). In: Odlyzko AM, editor. *Advances in Cryptology – CRYPTO'86.* Berlin, Heidelberg: Springer; 1987. p. 251–260. (Lecture Notes in Computer Science; volume 263). DOI: 10.1007/3-540-47721-7_19.

4. Galibus TV, Matveev GV. Verification of the modular secret sharing parameters. *Vestnik BGU. Seriya 1, Fizika. Matematika. Informatika*. 2015;1:76–79. Russian.

5. Vaskouski MM, Matveev GV. Verification of modular secret sharing. *Journal of the Belarusian State University. Matematics and Informatics*. 2017;2:17–22. Russian.

6. Galibus TV. Verification of modular secret sharing over a binary field. *Vestnik Brestskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya 1, Fizika, matematika, informatika*. 2014;5:26–27. Russian.

7. Galibus T, Matveev G. Generalized Mignotte's sequences over polynomial rings. *Electronic Notes Theoretical Computer Science.* 2007;186:43–48. DOI: 10.1016/j.entcs.2006.12.044.

8. Shenets NN. On the information level of modular secret sharing schemes. *Doklady Natsional'noi akademii nauk Belarusi. Seriya fiziko-matematicheskikh nauk*. 2010;54(6):9–12. Russian.

Статья поступила в редколлегию 15.12.2017.
Received by editorial board 15.12.2017.