УДК 519.719.2

ВЕРИФИКАЦИЯ МОДУЛЯРНОГО РАЗДЕЛЕНИЯ СЕКРЕТА

М. М. ВАСЬКОВСКИЙ [1)]***, Г. В. МАТВЕЕВ*** [1)]

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

Построены схемы верификации модулярного разделения секрета. Верификация с участием доверенной стороны осуществляется с помощью внешнего устройства, в которое можно загрузить произвольный многочлен $S(x)$, и при вводе $x_0 \in F_{p^n}$ оно выдает значение $\xi S(x_0)$, где ξ – равномерно распределенная случайная величина, принимающая значения из F_{p^n}. Показано, что данное устройство позволяет каждому пользователю верифицировать его секрет. Полиномиальная верификация модулярной схемы основана на верификации делимости $g(x) \mid f(x)$ в кольце $Z[x]$. При такой верификации разглашается лишь значение $S(x)$ в некоторой неизвестной посторонним точке $x = l$. Верификация модулярной схемы по Бенало дает возможность каждому из участников убедиться в том, что все частичные секреты в совокупности являются консистентными, т. е. любая разрешенная группа участников может правильно восстановить секрет $S(x)$. Никакой информации о секрете $S(x)$, кроме априорной, не разглашается. Предложенные протоколы могут быть безопасно использованы для схем над произвольными конечными полями без дополнительных ограничений на мощность поля.

Ключевые слова: полиномиальная модулярная схема; секрет; частичный секрет; конечное поле.

VERIFICATION OF MODULAR SECRET SHARING

M. M. VASKOUSKI [a]***, G. V. MATVEEV*** [a]

[a]*Belarusian State University, Niezaliežnasci Avenue, 4, 220030, Minsk, Belarus*
Corresponding author: M. M. Vaskouski (vaskovskii_m@mail.ru)

In the present paper new scheme of secret verification are constructed. Verification with trusted party participation is conducted with help of an external device, which takes an arbitrary polynomial $S(x)$, input element $x_0 \in F_{p^n}$ and returns a value $\xi S(x_0)$, where ξ is an F_{p^n} – valued uniformly distributed random variable. It is shown that using of such device allows any user to verify his secret. Polynomial verification scheme is based on verification of divisibility $g(x) \mid f(x)$ in the ring $Z[x]$. Only a value of polynomial $S(x)$ in unknown point $x = l$ is disclosed at the proposed verification method. Benaloh's verification of the modular scheme allows any shareholder to ensure in consistency of all partial secrets, i. e. any legal group of shareholders can restore the secret $S(x)$ correctly. None information about the secret $S(x)$, excepting a prior information, is disclosed. The proposed protocols can be used safely for schemes over arbitrary finite fields without additional restrictions on a size of a filed.

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

Образец цитирования:
Васьковский М. М., Матвеев Г. В. Верификация модулярного разделения секрета // Журн. Белорус. гос. ун-та. Математика. Информатика. 2017. № 2. С. 17–22.

For citation:
Vaskouski M. M., Matveev G. V. Verification of modular secret sharing. *J. Belarus. State Univ. Math. Inform.* 2017. No. 2. P. 17–22 (in Russ.).

Авторы:
Максим Михайлович Васьковский – кандидат физико-математических наук, доцент; доцент кафедры высшей математики факультета прикладной математики и информатики.
Геннадий Васильевич Матвеев – кандидат физико-математических наук, доцент; доцент кафедры высшей математики факультета прикладной математики и информатики.

Authors:
Maksim Vaskouski, PhD (physics and mathematics), docent; associate professor at the department of higher mathematics, faculty of applied mathematics and computer sciences.
vaskovskii_m@mail.ru
Gennadii Matveev, PhD (physics and mathematics), docent; associate professor at the department of higher mathematics, faculty of applied mathematics and computer sciences.
matveev@bsu.by

Постановка задачи

Схемы разделения секрета (СРС) являются составной частью многих криптографических протоколов. Разделение секрета применяется для совместных конфиденциальных вычислений [1], шифрования на основе атрибутов [2] и электронного защищенного голосования [3]. Важной задачей в разделении секрета является построение таких схем, с помощью которых пользователи могут проверить корректность секрета и тем самым не допустить обмана со стороны остальных участников и дилера. Такие схемы строятся на основе протоколов с нулевым разглашением [4]. В схемах верифицируемого разделения секрета (СВРС) дилер распределяет информацию о секретном значении среди участников таким образом, что для честных пользователей гарантируется получение ими значения секрета, а для нечестных – невозможность восстановить секрет.

Преимущество полиномиальных схем модулярного разделения секрета заключается в их теоретико-информационной криптостойкости: полиномиальная модулярная схема является в общем случае совершенной, а в пороговом – идеальной [5]. Еще одно преимущество этих схем по сравнению с целочисленными – их расширенные возможности по генерации параметров: в качестве исходного используется поле F_p, а количество параметров зависит от степеней полиномов в $F_p[x]$, что позволяет строить сколько угодно схем даже для небольших простых p. В связи с этим верификация полиномиальной модулярной схемы – актуальная задача, состоящая в построении протокола верификации, пригодного для любой модулярной пороговой СРС. Заметим, что [6] является пороговой СРС в полиномиальном кольце $F_2[x]$. Решение этой задачи лишь для больших простых p было получено в работе [7], где верификация полиномиальной схемы основана на вычислительной сложности задачи дискретного логарифмирования в полях большой мощности.

В отличие от [7] в настоящей работе построены протоколы верификации полиномиальной модулярной схемы, основанные на свойствах делимости многочленов с целыми коэффициентами и умножении параметров схемы на подходящие случайные величины, что позволяет безопасно использовать данные схемы в произвольных конечных полях без ограничений числа элементов поля.

Пороговая модулярная схема разделения секрета в кольце $F_p[x]$

Пороговая полиномиальная модулярная СРС была предложена в работе [8] как обобщение классической схемы Шамира [9] и схемы Асмуса – Блюма [10]. Данная схема позволяет разделить секретное значение $s(x) \in F_p[x]$. Промежуточный секрет $S(x)$ (t, k)-пороговой модулярной полиномиальной схемы выбирается так, что $\deg S(x) < tn$, где t – порог; n – общая степень модулей участников. Разделение секрета можно начать с генерации значения $S(x)$.

Фаза дилера (алгоритм разделения):

1) случайным образом выбирается промежуточное значение секрета $S(x) \in F_p[x]$ с условием

$$\deg S(x) < tn;$$

2) случайным образом выбираются попарно различные неприводимые $m_i(x)$, $i = 1, \ldots, k$, и $p(x)$ с ограничением $\deg m_i(x) = \deg p(x) = n$. В работе [8] указан способ выбора параметров t, k, n, p;

3) дилером публикуются $m_i(x)$, $p(x)$, а $s(x) = S(x) \bmod p(x)$ назначается в качестве секрета схемы;

4) дилером по секретным каналам отправляются частичные секреты участников: $s_i(x) = S(x) \bmod m_i(x)$.

5) дополнительно, для ускорения вычислений на фазе восстановления секрета, дилером заранее вычисляются и публикуются следующие значения:

$$M_A(x) = \prod_{j=i_1}^{i_t} m_j(x),$$

где $A = \{i_1, \ldots, i_t\}$ – подмножество t участников; $M_{A\setminus\{i\}} = \dfrac{M_A(x)}{m_i(x)}$; $M'_{A,i} = \left(\dfrac{M_A(x)}{m_i(x)}\right)^{-1} \bmod m_i(x)$, $\forall i \in A$.

Фаза участников (алгоритм восстановления): участники из подмножества A обмениваются своими частичными секретами $s_i(x)$, $i \in A$, и находят значение секрета $s(x)$:

$$u_i = s_i M'_{A,i} M_{A\setminus\{i\}}, \ \forall i \in A,$$

$$S(x) = \sum_{i \in A} u_i \bmod M_A,$$

$$s(x) = S(x) \bmod p(x).$$

Верификация с участием доверенной стороны

Рассмотрим подход к проверке условия $s_i(x) = S(x) \bmod m_i(x)$ для каждого участника в отдельности. Не нарушая общности, будем считать, что $s_i(x) \equiv 0$, а многочлен $m_i(x)$ сепарабельный. Если $m_i(x)$ неприводимый, то достаточно проверить, что хотя бы один корень $\beta_j \in F_{p^n}$ многочлена $m_i(x)$ является корнем многочлена $S(x)$. В общем случае проверка необходима всем корням β_j многочлена $m_i(x)$.

Предлагаемый способ заключается в следующем. Будем считать, что, кроме дилера B и законного участника A_i, имеется внешнее устройство C, в которое можно загрузить произвольный многочлен (в нашем случае $S(x)$), и данное устройство при вводе $x_0 \in F_{p^n}$ выдает значение $\xi S(x_0)$, где ξ – равномерно распределенная случайная величина, принимающая значения из F_{p^n}. Очевидно, что это устройство позволяет проверить пользователю A_i, является ли элемент $x_0 \in F_{p^n}$ корнем загруженного многочлена $S(x)$, но при этом за счет случайности ξ не позволяет восстановить сам многочлен $S(x)$ по значениям $(x_0, \xi S(x_0))$. Очевидно, что проверка условия $\xi S(x_0) = 0$, проведенная по всем корням β_j многочлена $m_i(x)$, даст однозначный ответ на вопрос о делимости $m_i(x) \mid S(x)$.

Полиномиальная верификация модулярной схемы

Ниже предлагается верификация схемы на основе верификации полиномиального деления. Ранее этот способ был применен нами для верификации схемы Шамира. В его основе лежит следующая теорема, обобщающая [11, теорема].

Теорема. *Пусть* $f(x)$, $g(x)$ *– многочлены с целыми коэффициентами,* $\deg f \geq \deg g$, *причем старший коэффициент* $g(x)$ *равен 1. Тогда условие* $\dfrac{f(x)}{g(x)}$ *равносильно условию* $\dfrac{f(l)}{g(l)}$, *где* $l \geq l_0(f, g) = \left(H_g + H_f \left(H_g + 1\right)^{\deg f - \deg g + 1}\right)\deg g + 1$; H_g, H_f *– высоты многочленов* $g(x)$ *и* $f(x)$ *соответственно.*

Доказательство. Предположим, что существуют такие многочлены $f(x) = a_m x^m + \ldots + a_1 x + a_0$; $g(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$ с целыми коэффициентами, что $f(x) = q(x)g(x) + r(x)$, $\deg f \geq \deg g$, $r(x) \neq 0$ (так как старший коэффициент многочлена $g(x)$ равен 1, то $r(x) \in Z[x]$), и такое $l \geq l_0(f, g)$, что выполняется условие $g(l) \mid f(l)$. Оценим высоту H_r многочлена $r(x)$. На первом шаге деления с остатком $f(x)$ на $g(x)$ получаем неполное частное $a_m x^{m-n}$, затем снова делим многочлен $mf_1(x) = f(x) - a_m x^{m-n} g(x)$ на $g(x)$. Видно, что $H_{f_1} \leq H_f + H_f H_g$. На следующем шаге получаем в остатке многочлен $f_2(x) = f_1(x) - \alpha x^{m-n-1} g(x)$, где α – старший коэффициент многочлена $f_1(x)$, т. е. имеем $H_{f_2} \leq H_{f_1} + H_{f_1} H_g$. Таким образом, по индукции получаем, что $H_r \leq H_f \left(H_g + 1\right)^{\deg f - \deg g + 1}$. Ввиду того, что $l > H_r + 1$; $l > H_g + 1$, l не является корнем ни $g(x)$, ни $r(x)$. Поскольку $g(l) \mid f(l)$ и $r(l) \neq 0$, $g(l) \neq 0$, то $g(l) \mid r(l)$ и $|r(l)| \geq |g(l)|$. Из неравенств $H_r \leq H_f \left(H_g + 1\right)^{\deg f - \deg g + 1}$ и $l \geq \left(H_g + H_f \left(H_g + 1\right)^{\deg f - \deg g + 1}\right)\deg g + 1$ вытекает, что $l > \left(H_r + H_g\right)\deg g$. Тогда получаем $|g(l)| \geq l^{\deg g} - l^{\deg g - 1} H_g \deg g > l^{\deg g - 1} H_r \deg g \geq |r(l)|$, что противоречит неравенству $|r(l)| \geq |g(l)|$.

Приведенную теорему можно применить для верификации делимости $g(x) \mid f(x)$ в кольце $Z[x]$:

1) дилер публикует $f(l)$, $l \geq l_0$;

2) пользователь проверяет делимость $g(l) \mid f(l)$.

При такой верификации разглашается лишь значение многочлена в некоторой неизвестной посторонним точке $x = l$.

Распространим эту верификацию на случай кольца многочленов $F_p[x]$. Будем верифицировать деление $f(x) = g(x)q(x)$.

Сначала построим инъективное отображение φ поля разложения $F_p[x]$ многочлена $f(x)$ в кольцо целых чисел Z. Выберем неприводимый многочлен $h(x) \in F_p[x]$ степени k. Поскольку $F_{p^k} \cong \frac{F_p[x]}{h(x)}$, то элементы поля F_{p^k} будем рассматривать как многочлены $r(x) = \sum_{i=0}^{k-1} a_i x^i \left(\mathrm{mod}\, h(x)\right)$. Каждому такому многочлену поставим в соответствие целое число $\sum_{i=0}^{k-1} a_i p^i$, рассматривая $a_i \in Z_p$ как наименьший неотрицательный вычет по модулю p. Построенное таким образом отображение обозначим через φ. Имеется эффективный алгоритм обращения φ: выбранное целое число $a \in \left[0,\ p^k\right)$ представляется в системе счисления по основанию p, т. е. $a = \sum_{i=0}^{k-1} a_i p^i$, тогда $\varphi^{-1}(a) = \sum_{i=0}^{k-1} a_i x^i \left(\mathrm{mod}\, h(x)\right)$.

Преобразуем затем многочлены $g(x) \in F_p[x]$ и $f(x) \in F_p[x]$ в целочисленный многочлены $\overline{g}(x)$ и $\overline{f}(x)$, полагая, что

$$\overline{g}(x) = \left(x - \varphi(\alpha_1)\right)\left(x - \varphi(\alpha_2)\right) \cdot \ldots \cdot \left(x - \varphi(\alpha_s)\right),$$

$$\overline{f}(x) = \left(x - \varphi(\beta_1)\right)\left(x - \varphi(\beta_2)\right) \cdot \ldots \cdot \left(x - \varphi(\beta_m)\right),$$

где $\alpha_1, \alpha_2, \ldots, \alpha_s \in F_{p^k}$ – все корни многочлена $g(x)$; $\beta_1, \beta_2, \ldots, \beta_m \in F_{p^k}$ – все корни многочлена $f(x)$.

Очевидно, что делимость $f(x) = g(x)q(x)$ в кольце $F_p[x]$ равносильна делимости $\overline{g}(x) \,|\, \overline{f}(x)$.

Поэтому верификация частичного секрета $s_i(x) = S(x) \bmod m_i(x)$ сводится к верификации делимости в кольце $Z[x]$: $\overline{m}_l(x) \,|\, \overline{S(x) - s_l(x)}$ (с этой целью можно применить приведенную выше теорему).

Перейдем к верификации схемы с порогом t и k.

Для этого требуется инъективное отображение поля разложения многочлена $\prod_{i-1}^{k} \left(S(x) - s_i(x)\right)$ в кольцо целых чисел. Аналогично черта будет применяться для обозначения образов элементов поля и многочленов.

Каждый в отдельности частичный секрет можно верифицировать путем проверки делимости $\overline{m}_l(x) \,|\, \overline{S(x) - s_l(x)}$ в кольце $Z[x]$. При этом дилер публикует целые числа $\overline{S(l) - s_l(l)}$, $i = 1, 2, \ldots, k$, которые можно использовать для атаки на ключи $s_i(x)$.

Чтобы предотвратить эту атаку, дилер может поступить следующим образом:

1) выбрать число $l \in Z[x]$, достаточное для верификации всех условий $\overline{m}_l(x) \,|\, \overline{S(x) - s_l(x)}$, $i = 1, 2, \ldots, k$;

2) подобрать и опубликовать в открытом доступе систему попарно взаимно простых чисел $q_1, q_2, \ldots, q_s$ таких, что

$$q_i^{|\overline{s}_i(l)|} > \left|\overline{s}_i(l)\overline{S(l) - s_l(l)}\right|,\ i = 1, 2, \ldots, k;$$

3) разместить в открытом доступе число G такое, что

$$G \equiv \overline{s}_i(l)\overline{S(l) - s_l(l)} \left(\mathrm{mod}\, q_i^{|\overline{s}_i(l)|}\right),\ i = 1, 2, \ldots, k.$$

Для того чтобы законному участнику проверить свой частичный секрет s_i, нужно:

1) вычислить $G_i = G\left(\mathrm{mod}\, q_i^{|\overline{s}_i(l)|}\right)$. В этом случае он находит $\overline{s}_i(l)\overline{S(l) - s_l(l)}$;

2) проверить, будет ли целым число $Q_i = \dfrac{G_i}{\overline{s}_i(l)}$. Если нет, то секрет не является достоверным. Иначе перейти к шагу 3;

3) если $Q_i = \overline{S(l) - s_l(l)}$ целое, то проверить условие $\overline{m}_l(l) \big| Q_i$ (шаг выполняется только для достоверных секретов).

Верификация модулярной схемы по Бенало

Этот способ верификации дает возможность каждому из k участников убедиться в том, что все частичные секреты в совокупности являются t-консистентными, т. е. любые t из k участников смогут правильно восстановить секрет $S(x)$. Обоснование протокола Бенало дано в работе [3]. Никакой информации о секрете $S(x)$, кроме априорной $\deg S(x) \le tn$, не разглашается. Приведем интерактивное доказательство.

1. Дилер генерирует полином $S(x)$ и распределяет частичные секреты $s_i(x)$, …, $s_{i_m}(x)$.
2. Дилер генерирует большое число l случайных полиномов степени не выше tn.
3. Участник случайным образом выбирает $m < l$ полиномов.
4. Дилер раскрывает участнику частичные секреты полиномов $S_i(x)$, …, $S_{i_m}(x)$, а также частичные секреты сумм $S(x) + \sum_{j=m+1}^{l} S_j(x)$, образованных с участием оставшихся полиномов.
5. Участник, пользуясь китайской теоремой об остатках (CRT), устанавливает, что все полиномы $S(x) + \sum_{j=m+1}^{l} S_j(x)$ имеют степени не выше tn.

Библиографические ссылки

1. *Cramer R., Damgard I., Nielsen J.* Multiparty Computation from Threshold Homomorphic Encryption // Lect. Notes Comput. Sci. 2001. Vol. 2045. P. 280 –300.
2. *Bethencourt J., Sahai A., Waters B.* Ciphertext-policy attribute-based encryption // Proceedings of IEEE Symposium on Security and Privacy. Berkley, 2007. P. 321–334.
3. *Benaloh J.* Secret sharing homomorphisms: keeping shares of a secret // Lect. Notes Comput. Sci. 1987. Vol. 263. P. 251–260.
4. *Blum M., Feldman P., Micali S.* Non Interactive Zero-Knowledge and Its Applications // Proceedings of the 20th ACM Symposium on Theory of Computing. New York, 1988. P. 103–112.
5. *Galibus T., Matveev G., Shenets N.* Some structural and security properties of the modular secret sharing // Proceedings of SYNASC'08 : IEEE Comp. soc. press (Timisoara, 26–29 Sept., 2008). Timisoara, 2008. P. 197–200.
6. Информационные технологии и безопасность. Алгоритмы разделения секрета : СТБ 34.101.60–2011. Введ. 01.07.2011.
7. *Галибус Т. В., Матвеев Г. В.* Верификация параметров модулярного разделения секрета // Вестн. БГУ. Сер. 1, Физика. Математика. Информатика. 2015. № 1. С. 76–79.
8. *Galibus T., Matveev G.* Generalized Mignotte Sequences in Polynomial Rings // ENTCS. 2007. Vol. 186. P. 43–48.
9. *Shamir A.* How to share a secret // Commun. ACM. 1979. Vol. 22, № 11. P. 612–613.
10. *Asmuth C. A., Bloom J.* A modular approach to key safeguarding // IEEE Trans. Inf. Theory. 1983. Vol. 29, issue 2. P. 208–210.
11. *Васьковский М. М., Матвеев Г. В.* Полиномиальная верификация схемы Шамира // Информационные системы и технологии : Междунар. конгр. по информатике (Минск, 24–27 окт. 2016 г.). Минск, 2016. С. 431–433.

References

1. Cramer R., Damgard I., Nielsen J. Multiparty Computation from Threshold Homomorphic Encryption // Lect. notes comput. sci. 2001. Vol. 2045. P. 280–300.
2. Bethencourt J., Sahai A., Waters B. Ciphertext-policy attribute-based encryption. *Proceedings of IEEE Symposium on Security and Privacy.* Berkley, 2007. P. 321–334.
3. Benaloh J. Secret sharing homomorphisms: keeping shares of a secret. *Lect. Notes Comput. Sci.* 1987. Vol. 263. P. 251–260.
4. Blum M., Feldman P., Micali S. Non Interactive Zero-Knowledge and Its Applications. *Proceedings of the 20th ACM Symposium on Theory of Computing.* New York, 1988. P. 103–112. DOI: 10.1145/62212.62222.

5. Galibus T., Matveev G., Shenets N. Some structural and security properties of the modular secret sharing. *Proceedings of SYNASC'08* : IEEE Comp. soc. press (Timisoara, 26–29 Sept., 2008). Timisoara, 2008. P. 197–200.

6. Informatsionnye tekhnologii i bezopasnost'. Algoritmy razdeleniya sekreta : STB 34.101.60–2011. Introd. 01.07.2011 (in Russ.).

7. Galibus T. V., Matveev G. V. Verification of the modular secret sharing parameters. *Vestnik BGU. Ser. 1, Fiz. Mat. Inform.* 2015. No. 1. P. 76–79 (in Russ.).

8. Galibus T., Matveev G. Generalized Mignotte Sequences in Polynomial Rings. *ENTCS.* 2007. Vol. 186. P. 43–48.

9. Shamir A. How to share a secret. *Commun. ACM.* 1979. Vol. 22, No. 11. P. 612–613.

10. Asmuth C. A., Bloom J. A modular approach to key safeguarding. *IEEE Trans. Inf. Theory.* 1983. Vol. 29, issue 2. P. 208–210. DOI: 10.1109/TIT.1983.1056651.

11. Vaskouski M. M., Matveev G. V. [Polynomial verifications of the shamir scheme]. *Information Systems and Technologies* : Int. cong. comput. sci. (Minsk, 24–27 Oct., 2016). Minsk, 2016. P. 431–433 (in Russ.).

Статья поступила в редколлегию 20.03.2017.
Received by editorial board 20.03.2017.