УДК 519.719.2

РАЗДЕЛЕНИЕ СЕКРЕТА В КОЛЬЦАХ МНОГОЧЛЕНОВ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ С ИСПОЛЬЗОВАНИЕМ КИТАЙСКОЙ ТЕОРЕМЫ ОБ ОСТАТКАХ

Г. В. МАТВЕЕВ[1)]

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

Обобщено разделение целочисленного секрета, использующего алгоритм китайской теоремы об остатках на случай кольца многочленов от нескольких переменных над конечным полем. Для генерации частичных секретов вместо целочисленных модулей применяются идеалы и их базисы Грёбнера. Этот подход предложен нами ранее. В настоящей работе показано, что любую пороговую структуру доступа можно реализовать идеально. Это является одним из преимуществ предлагаемого подхода. В кольце целых чисел никакую структуру доступа нельзя осуществить идеально, поскольку частичные секреты всех участников имеют различные размеры.

Ключевые слова: китайская теорема об остатках; разделение секрета; равноостаточные идеалы; эквипроективные множества.

Благодарность. Автор выражает благодарность Т. Галибус и Н. Шенецу за их ценные замечания, а также В. Матулису за помощь при подготовке рукописи к печати.

CHINESE REMAINDER THEOREM SECRET SHARING IN MULTIVARIATE POLYNOMIALS

G. V. MATVEEV[a]

[a]*Belarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus*

This paper deals with a generalization of the secret sharing using Chinese remainder theorem over the integers to multivariate polynomials over a finite field. We work with the ideals and their Gröbner bases instead of integer moduli. Therefore, the proposed method is called GB secret sharing. It was initially presented in our previous paper. Now we prove that any threshold structure has ideal GB realization. In a generic threshold modular scheme in ring of integers the sizes of the share space and the secret space are not equal. So, the scheme is not ideal and our generalization of modular secret sharing to the multivariate polynomial ring is more secure.

Keywords: Chinese remainder theorem; secret sharing; equiresidual ideals; equiprojectable sets.

Acknowledgements. I thank T. Galibus and N. Shenets for their valuable comments. I also want to thank to V. Matulis for his help in preparation the paper.

Образец цитирования:
Матвеев ГВ. Разделение секрета в кольцах многочленов от нескольких переменных с использованием китайской теоремы об остатках. *Журнал Белорусского государственного университета. Математика. Информатика.* 2019;3:129–133 (на англ.).
https://doi.org/10.33581/2520-6508-2019-3-129-133

For citation:
Matveev GV. Chinese remainder theorem secret sharing in multivariate polynomials. *Journal of the Belarusian State University. Mathematics and Informatics.* 2019;3:129–133.
https://doi.org/10.33581/2520-6508-2019-3-129-133

Автор:
Геннадий Васильевич Матвеев – кандидат физико-математических наук; доцент кафедры высшей математики факультета прикладной математики и информатики.

Author:
Gennadii V. Matveev, PhD (physics and mathematics); associate professor at the department of higher mathematics, faculty of applied mathematics and informatics.
matveev@bsu.by
https://orcid.org/0000-0002-1372-0117

CC BY NC

Introduction

Secret sharing enables a group of l participants to share a secret. Each of them is provided a share. The sharing scheme has a threshold t if any t-subset of participants with t out of l shares enables the secret to be recovered.

The basic idea of the modular secret sharing is as follows. Let $s \in \mathbb{Z}$ be the secret value, and let the residue $s_i = s \bmod m_i$, where m_i is the public key, be the share of the i participant. It is necessary to choose the secret s and moduli m_i so that only the authorized groups of participants can compute the secret. For more details, see [1]. However, in a generic (t, l)-threshold modular scheme in $\mathbb{Z}$, the sizes of the share space and the secret space are not equal. So, the scheme is not ideal.

In this paper, the modular constructions in the ring of integers are transformed into the modular constructions in the multivariate polynomial ring $F_q[x]$, where $x = (x_1, x_2, \ldots, x_n)$. We prove that any threshold structure has the ideal GB realization. So, our generalization of modular secret sharing to the multivariate polynomial ring is more secure.

The modular secret sharing in the ring $F_q[x]$ is based on the following facts:

• first, given a monomial ordering, we can compute the residue of a secret polynomial $s(x) \in F_q[x]$ modulo any zero-dimensional ideal;

• second, there is the CRT-algorithm for computing the secret [2].

Our approach can be generalized to other commutative rings with the effective Gröbner basis theory. We studied the univariate case and its verification protocols in our previous papers [3–6]. GB secret sharing was presented in [7].

The paper is organized as follows. In the second section we construct the special zero-dimensional ideals of $F_q[x]$. They provide the security of the proposed scheme. Our construction is based on the triangular ideals' characterization (see [8]). In the third section, we present ideal threshold schemes in the ring $F_q[x]$.

Equiresidual ideals

The results of this section are essentially inspired by the concept of equiprojectivity (see [8]). Following their notation, we say that an ideal of $F_q[x]$ is a triangular ideal if it admits a separable triangular set of generators. Throughout the paper, we consider the Gröbner bases in the ring $F_q[x]$, where $x = (x_1, x_2, \ldots, x_n)$, $x_1 < x_2 < \ldots < x_n$.

Let I be a triangular zero-dimensional ideal of $F_q[x]$. It has the reduced Gröbner basis $\{f_1, f_2, \ldots, f_n\}$:

$$f_i = x_i^{d_i} + a_{i,\,d_i-1}x_i^{d_i-1} + \ldots + a_{i,1}x_i + a_{i,0},\ a_{i,\,d_i-1}, \ldots, a_{i,1}, a_{i,0} \in F_q[x_1, x_2, \ldots, x_{i-1}],$$

and its zero-set $V(I)$ in the algebraic closure of F_q is equiprojectable (see theorem 4.5 in [8]). In this case, the vector of fiber cardinalities is defined as

$$FC(I) = \left(\operatorname{card}\pi_1^{-1}(M), \operatorname{card}\pi_2^{-1}(M), \ldots, \operatorname{card}\pi_{n-1}^{-1}(M)\right) = (d_2 \cdots d_n, d_3 \cdots d_n, \ldots, d_n),$$

where $\pi_i(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\alpha_1, \alpha_2, \ldots, \alpha_i)$ (see [8, p. 640]). $FC(I)$ does not depend on the choice of the point $M \in V(I)$.

The set of all reduced terms modulo I is denoted by $RT(I)$. The set of all reduced polynomials is denoted by $RP(I)$. Let

$$D(I) = (d_1, d_2, \ldots, d_n),\ d = d_1 d_2 \cdots d_n.$$

Definition 1. We say that zero-dimensional ideals $I_1, I_2, \ldots, I_l$ are equiresidual if

$$RT(I_1) = RT(I_2) = \ldots = RT(I_l).$$

In this case, it is convenient to use the notation:

$$RT(I_1) = RT(I_2) = \ldots = RT(I_l) = RT_1.$$

Obviously, zero-dimensional triangular ideals $I_1, I_2, \ldots, I_l$ are equiresidual if and only if (*ER condition*)

$$D(I_1) = D(I_2) = \ldots = D(I_l).$$

Remark 1. Let I be a zero-dimensional triangular ideal I. According to theorem 4.5 in [8], $d_2, \ldots, d_n$ (not d_1) are uniquely determined by $FC(I)$. It will be used in the proof of theorem 2.

Definition 2. We say that zero-dimensional ideals are strongly equiresidual if

$$RT\left(I_{i_1} I_{i_2} \cdots I_{i_k}\right) = RT\left(I_{j_1} I_{j_2} \cdots I_{j_k}\right),$$

where $1 \le i_1 < i_2 < \ldots < i_k \le l$, $1 \le j_1 < j_2 < \ldots < j_k \le l$, for each $k \in [1, l]$.

Obviously, we have

$$RT\left(I_{i_1} I_{i_2} \cdots I_{i_k}\right) = RT\left(I_{j_1} I_{j_2} \cdots I_{j_k}\right) \Leftrightarrow RP\left(I_{i_1} I_{i_2} \cdots I_{i_k}\right) = RP\left(I_{j_1} I_{j_2} \cdots I_{j_k}\right).$$

In this case, it is convenient to introduce a simpler notation:

$$RT_k = RT\left(I_{i_1} I_{i_2} \cdots I_{i_k}\right),\ RP_k = RP\left(I_{i_1} I_{i_2} \cdots I_{i_k}\right),\ 1 \le i_1 < i_2 < \ldots < i_k \le l.$$

Definition 3. (SDNI condition.) We say that zero-sets $V(I_1)$ and $V(I_2)$ strongly don't intersect if

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \in V(I_1),\ (\beta_1, \beta_2, \ldots, \beta_n) \in V(I_2) \Rightarrow \alpha_i \ne \beta_j,\ 1 \le i,\ j \le n.$$

Remark 2. The motivation of SDNI is to provide the following property of ER zero-dimensional triangular ideals I_1, I_2:

$$FC(I_1) = FC(I_2) = FC(I_1 I_2).$$

Theorem 1. *Let zero-dimensional triangular ideals $I_1, I_2, \ldots, I_k$ satisfy ER and SDNI conditions. Then their product $I = I_1 I_2 \cdots I_k$ is a triangular ideal.*

P r o o f. ER implies:

$$FC(I_1) = FC(I_2) = \ldots = FC(I_k).$$

SDNI implies that $V(I)$ is equiprojectable with

$$FC(I) = FC(I_j),\ \text{for each}\ j \in [1, k].$$

It follows from theorem 4.5 in [8] that I is a triangular ideal. The theorem 1 is proved.

Theorem 2. *For any integer $l > 0$ there exist strongly equiresidual ideals $I_1, I_2, \ldots, I_l$ of $F_q[x]$.*

P r o o f. If $n = 1$ and $f_1(x),\ f_2(x), \ldots, f_l(x)$ are pairwise different of given degree m then the ideals $\langle f_1(x)\rangle$, $\langle f_2(x)\rangle, \ldots, \langle f_l(x)\rangle$ are strongly equiresidual and $RT_k = \left\{1, x, \ldots, x^{km-1}\right\}$.

In general case pick triangular $I_1, I_2, \ldots, I_l$ under ER and SDNI conditions. According to theorem 1 the product $I = I_1 I_2 \cdots I_k$, $k \le l$, is triangular. Let us calculate $D(I)$. According to CRT, there is a ring isomorphism:

$$F_q[x]/I \cong F_q[x]/I_1 \times F_q[x]/I_2 \times \ldots \times F_q[x]/I_k.$$

Hence,

$$\left|F_q[x]/I\right| = k\left|RP_1\right|.$$

It is the first observation. Secondly,

$$D(I_1) = \ldots = D(I_k) = (d_1, d_2, \ldots, d_n),\ FC(I_1) = \ldots = FC(I_k) = FC(I)$$

implies

$$D(I) = (d_1', d_2, \ldots, d_n).$$

In summary, $d_1' = kd_1$, and

$$D(I) = (kd_1, d_2, \ldots, d_n).$$

The same holds for each product $I_{j_1} I_{j_2} \cdots I_{j_k}$, $1 \le j_1 < j_2 < \ldots < j_k \le l$. The theorem 2 is proved.

Remark 3. Ideals of symmetric relations are strongly equiresidual ideals if their separable polynomials are pairwise coprime and of the same degree (see [8]).

Ideal threshold schemes

We propose the following generalization of Asmuth – Bloom (t, l)-threshold scheme [1]. Pick strongly equiresidual ideals $I_0, I_1, \ldots, I_l$. Let $S(x)$ be a uniformly distributed intermediate secret value, $S(x) \in RP_t$. We identify $RP\left(I_{i_1} I_{i_2} \cdots I_{i_k}\right) = RP_k$ with $F_q[x]/I_{i_1} I_{i_2} \cdots I_{i_k}$. Then we define the secret $s(x)$ and the shares $s_i(x)$, $i = 1, 2, \ldots, l$, as follows:

$$s(x) = S(x) \bmod I_0,\ s_i(x) = S(x) \bmod I_i.$$

Hence, the common space of the secret and secret shares is

$$RP(I_0) = \ldots = RP(I_l) = F_q[x]/I_0 = RP_1.$$

That's why the proposed modular scheme is potentially ideal. The space of $S(x)$ is RP_t.

If k shares $k \geq t$ are known, we uniquely determine $S(x)$ using the CRT-algorithm [2], as $S(x) \in RP_t$. After that we evaluate $s(x)$.

We will use below the following simple fact.

It is well-known that the image of a function $s = f(S)$ has the uniform distribution if the cardinalities of all fibres $f^{-1}(s)$ are the same (*EP condition*).

Theorem 3. *The generalized (t, l)-threshold Asmuth – Bloom scheme with strongly equiresidual ideals is ideal.*

P r o o f. We only need to prove the perfectness. The proof is based on the following ring isomorphism:

$$S(x) \in RP_t = F_q[x]/I_0 I_1 \cdots I_{t-1} \cong F_q[x]/I_0 \times F_q[x]/I_1 \times \ldots \times F_q[x]/I_{t-1}.$$

Therefore, we may put

$$S(x) = \left(s(x), s_1(x), \ldots, s_{t-1}(x)\right).$$

The secret $s(x)$ is the projection of $S(x)$ onto the first component, and the cardinality of every fibre is equal to

$$\left|F_q[x]/I_1\right|\left|F_q[x]/I_2\right| \cdots \left|F_q[x]/I_{t-1}\right|.$$

As $\dim_{F_q} F_q[x]/I_i = d = d_1 d_2 \cdots d_n$, then all cardinalities of the fibers are equal to $q^{d(t-1)}$. Hence, $s(x)$ is uniformly distributed on RP_1.

What happens if a group of $k < t$ participants attempt to compute $s(x)$? Let $I_1, I_2, \ldots, I_k$ be their moduli and $s_1(x), \ldots, s_k(x)$ be their shares. In this case, $S(x)$ is uniformly distributed on the direct product

$$RP_1 \times s_1(x) \times \ldots \times s_k(x) \times \ldots \times (RP_1) \subset RP_t.$$

The map $S(x) \to s(x)$ is EP with $q^{d(t-k-1)}$ being the cardinality of the fibres. Hence, our scheme is perfect.

Example. Shamir's scheme [9] is a particular case of the proposed scheme, which we can see as follows. Take the univariate case and consider different polynomials of degree 1: $x - x_0, x - x_1, x - x_2, \ldots, x - x_l$. The ideals generated by these polynomials are strongly equiresidual. Now if one goes over the construction in theorem 3, one would first construct polynomial of degree at most t. Now taking this polynomial modulo $x - x_i$ is exactly evaluating it in x_i.

Remark 4. The ideals of symmetric relations are suitable for the construction of the ideal secret sharing in the general case $n \geq 1$.

Conclusion

Ideal threshold modular secret sharing schemes in the multivariate polynomial ring over a finite field are presented. The existence of the strongly residual ideals is proved.

Библиографические ссылки

1. Asmuth C, Bloom J. A modular approach to key safeguarding. *IEEE Transactions on Information Theory.* 1983;29(2):208–210. DOI: 10.1109/TIT.1983.1056651.

2. Becker T, Weispfenning V. *Gröbner Bases. A Computational Approach to Commutative Algebra.* New York: Springer-Verlag; 1993. 576 p. (Graduate Texts in Mathematics; volume 141). DOI: 10.1007/978-1-4612-0913-3.

3. Galibus T, Matveev G, Shenets N. Some structural and security properties of the modular secret sharing. In: *Symbolic and Numeric Algorithms for Scientific Computing, 2008. SYNASC 2008. 10th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing; 2008 September 26–29; Timisoara, Romania.* Los Alamitos: IEEE Computer Society Press; 2009. p. 197–200. DOI: 10.1109/SYNASC.2008.14.

4. Galibus T, Matveev G. Generalized mignotte's sequences over polynomial rings. *Electronic Notes in Theoretical Computer Science.* 2007;186(14):43–48. DOI: 10.1016/j.entcs.2006.12.044.

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

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

7. Galibus T, Matveev G. Finite Fields. Gröbner Bases and Modular Secret Sharing. *Journal of Discrete Mathematical Sciences and Cryptography.* 2012;15(6):339–348. DOI: 10.1080/09720529.2012.10698386.

8. Aubry P, Valibouze A. Using galois ideals for computing relative resolvents. *Journal of Symbolic Computations.* 2000;30(6): 635–651. DOI: 10.1006/jsco.2000.0376.

9. Shamir A. How to share a secret. *Communications of the ACM.* 1979;22(11):612–613. DOI: 10.1145/359168.359176.

References

1. Asmuth C, Bloom J. A modular approach to key safeguarding. *IEEE Transactions on Information Theory.* 1983;29(2):208–210. DOI: 10.1109/TIT.1983.1056651.

2. Becker T, Weispfenning V. *Gröbner Bases. A Computational Approach to Commutative Algebra.* New York: Springer-Verlag; 1993. 576 p. (Graduate Texts in Mathematics; volume 141). DOI: 10.1007/978-1-4612-0913-3.

3. Galibus T, Matveev G, Shenets N. Some structural and security properties of the modular secret sharing. In: *Symbolic and Numeric Algorithms for Scientific Computing, 2008. SYNASC 2008. 10th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing; 2008 September 26–29; Timisoara, Romania.* Los Alamitos: IEEE Computer Society Press; 2009. p. 197–200. DOI: 10.1109/SYNASC.2008.14.

4. Galibus T, Matveev G. Generalized mignotte's sequences over polynomial rings. *Electronic Notes in Theoretical Computer Science.* 2007;186(14):43–48. DOI: 10.1016/j.entcs.2006.12.044.

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

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

7. Galibus T, Matveev G. Finite Fields. Gröbner Bases and Modular Secret Sharing. *Journal of Discrete Mathematical Sciences and Cryptography.* 2012;15(6):339–348. DOI: 10.1080/09720529.2012.10698386.

8. Aubry P, Valibouze A. Using galois ideals for computing relative resolvents. *Journal of Symbolic Computations.* 2000;30(6): 635–651. DOI: 10.1006/jsco.2000.0376.

9. Shamir A. How to share a secret. *Communications of the ACM.* 1979;22(11):612–613. DOI: 10.1145/359168.359176.

Received by editorial board 23.08.2019.