Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 186 (2007) 43–48
www.elsevier.com/locate/entcs

Generalized Mignotte's Sequences Over Polynomial Rings

Tatyana Galibus[1]

Department of Mathematical Modelling and Data Analysis
Belarusian State University
Minsk, Belarus

Genadii Matveev[2]

Department of Higher Mathematics
Belarusian State University
Minsk, Belarus

Abstract

This paper introduces the generalization of Mignotte modular secret sharing over the polynomial rings. Mignotte proposed threshold secret sharing over the ring of integers. We extend his method for the ring of polynomials which is Euclidean as well and therefore allowing to use the Chinese Remainder Theorem. In particular, we prove that any access structure can be realized within this modular approach. Further, we put the bounds on the number of participants of such secret sharing scheme with the moduli of the same degree. And finally we estimate the information rate of the new scheme.

Keywords: Access structure, Chinese Remainder Theorem, co-prime polynomials, Euclidean ring, Mignotte secret sharing, modular secret sharing, shares, threshold.

1 Introduction

The concept of secret sharing as a mathematical method of splitting the secret value into shares so that only authorized subsets of shares could restore it was initially introduced by Shamir [8]. Later, Asmuth, Bloom [1] and Mignotte [6] independently devised the modular approach in secret sharing based on the Chinese Remainder Theorem in the ring of integers. Also, Asmuth and Bloom proposed to use Euclidean rings other than the ring of integers. All mentioned methods deal with the threshold secret sharing i.e. all subsets of not less than k participants out of t can compute the secret.

[1] Email: galibus@bsu.by
[2] Email: matveev@bsu.by

doi:10.1016/j.entcs.2006.12.044

Recently, it was noticed that some other access structures different from the threshold ones can be realized modularly by means of so called generalized Mignotte sequences introduced by Iftene [4]. In particular, he proposed the modular realization for so called compartmented secret sharing.

In this paper we present Mignotte secret sharing over the polynomial ring $F_q[x]$ where F_q is the Galois field of prime order q. We show that it can be used to realize any given access structure. In fact, we construct the corresponding Mignotte sequence. Further, we consider Mignotte sequences of polynomials of equal degrees being the closest possible moduli. This property is substantial for the secret sharing (see, for example, [3]). We put the upper bound on the length of such sequence i.e. the number of participants of secret sharing scheme with the equal moduli.

And finally, we estimate the information rate of the new secret sharing scheme in the most important case of $q = 2$.

2 Polynomial Modular Realization of the General Access Structures

Mignotte introduced his method for the threshold secret sharing. Let us give some more general definitions. Let $P = \{x_1, x_2, ..., x_t\}$ be a set of participants of the secret sharing scheme. We say that $A \subset P$ is authorized if participants from A can compute the secret. Let Γ be a set of all authorized subsets in P. Also, let Γ be monotone that is $A \in \Gamma, A \subset B \Rightarrow B \in \Gamma$. Then we say that Γ is an access structure over P. In particular, threshold access structure is defined by $\Gamma = \{B \subset P || B| \geq k\}$. The compartmented access structure realized modularly by Iftene is $\Gamma = \{A \subset P || A| \geq K, |A \cap C_j| \geq k_j, j = \overline{1,m}\}$ where K is the global threshold, $C_1, C_2, ..., C_m$ is the partition of P into compartments and $k_1, k_2, ..., k_m$ is the set of corresponding compartment thresholds.

The base of the modular secret sharing is the Chinese Remainder Theorem over $\mathbb{Z}$ which holds true over $F_q[x]$ as well. Thus, we can construct the similar Mignotte scheme for the polynomials. It is well-known that if the system of congruences

$$S(x) \equiv s_1(x)(\text{mod } m_1(x)), ..., S(x) \equiv s_k(x)(\text{mod } m_k(x))$$

over $F_q[x]$ is solvable then it has the single solution modulo $\text{LCM}(m_1(x), ..., m_k(x))$. As a rule the residue class representative of minimal degree is chosen for such solution.

Now let every participant $x_i \in P$ possess some monic polynomial $m_i(x) \in F_q[x]$. We denote the least common multiple of the moduli $m_i(x)$ for the arbitrary subset $A \in P$ as $[m_i(x); i \in A]$. Let the degree of secret $S(x)$ be chosen from some interval (M_1, M_2), $M_1 < \deg S(x) < M_2$ where $M_1, M_2 \in \mathbb{N}$ and the shares $s_i(x)$ are defined by $s_i(x) \equiv S(x)(\text{mod} m_i(x))$.

Definition 2.1 We say that access structure Γ has Mignotte realization over the ring $F_q[x]$ if there exist polynomials $m_i(x), i = \overline{1,t}$ such that

$$\deg [m_i, i \in A] > M_2 \text{ for } A \in \Gamma, \ \deg [m_i, i \in A] < M_1 \text{ for } A \notin \Gamma \quad (1)$$

We also say that the sequence of polynomials $m_i(x)$ is a generalized polynomial Mignotte sequence for the access structure Γ.

This definition generalizes Mignotte's one which was introduced only for the threshold access structures and pairwise co-prime moduli [6] and extends the definition of generalized Mignotte sequences of integers introduced by Iftene [4].

It is evident that under the given conditions any authorized subset $A \in \Gamma$ can compute the secret solving the system of congruences $S(x) \equiv s_i(x)(\mod\ m_i(x)),\ i \in A$ as well as any other subset cannot.

Theorem 2.2 *Any arbitrary access structure possesses Mignotte modular realization over the ring $F_q[x]$.*

Proof. Let us initially choose the polynomials $m_1(x), m_2(x), ..., m_t(x)$ equal to 1. Now we shall consider some maximal unauthorized subset $A \notin \Gamma$ (with respect to the inclusion i.e. such subset that no other unauthorized subset contains it). All moduli not belonging to participants from A we multiply by some irreducible monic $p_1(x) \in F_q[x]$. As we can choose $p_1(x)$ of any degree then after multiplying we can obtain the following condition fulfilled: $\deg [m_i(x), i \in A] < \deg [m_i(x), i \in B]$, for any authorized subset B. This condition holds true if we choose some other maximal unauthorized subset and perform the same operation for the irreducible monic $p_2(x) \neq p_1(x)$. Thus, having repeated the operation for all maximal unauthorized subsets we finally derive the realization of the given access structure Γ.

To conclude the proof it remains to choose the secret $S(x)$ so that $M_1 \leq \deg S(x) < M_2$ where M_1 is the maximal degree of LCM of the moduli belonging to unauthorized subsets and M_2 is the minimal degree of LCM of the moduli belonging to authorized subsets.

□

We note that it is more convenient to use the pairwise co-prime polynomials instead of irreducible ones. In the most cases the degrees of the resulting polynomials in 2.2 are less for the co-prime polynomials.

3 Generalized Mignotte Sequences in the Ring $F_q[x]$

We shall now show that using the ring $F_q[x]$ allows us to construct Mignotte sequences with better opportunities. In this ring we may choose moduli of the same degree i.e. ones with equal Euclidean norms. The only condition is that moduli should be co-prime.

Remark 3.1 Let $m_1(x), m_2(x), ..., m_t(x)$ be the set of pairwise co-prime polynomials of the same degree n. It can be easily verified that this set is a Mignotte sequence realizing all threshold access structures of t participants: $(1, t), (2, t), ..., (t, t)$. The value of threshold depends upon the degree of the secret. In fact, the degree secret can be chosen from any numeric interval: $(n, 2n), (2n, 3n), ..., ((t-1)n, tn)$. Moreover, this set of polynomials can be used for the generation of the generalized

Mignotte sequence for any access structure with no more than t maximal unauthorized subsets.

Irreducible polynomials are obviously co-prime. Let the number of monic irreducible polynomials of degree n in $F_q[x]$ be $N_q(n)$. The well-known formula for $N_q(n)$ is

$$N_q(n) = \frac{1}{n}\sum_{d|n}\mu(d)q^{\frac{n}{d}} \tag{2}$$

where $\mu(d)$ is a Möbius function [5]. Let us denote the maximal number of monic pairwise co-prime polynomials from $F_q[x]$ of the fixed degree n by $C_q(n)$. We shall now evaluate the value of $C_q(n)$ but first we need a technical result. We can not give a reference to the following lemma so we give a proof of it.

Lemma 3.2 *The function $N_q(n)$ is strictly increasing on n for any natural q and n except for the cases $q = 2, 3$ when it is strictly increasing starting from $n = 2$.*

Proof. It follows from (2) that

$$N_q(n) \geq \frac{1}{n}(q^n - \frac{q^n - q}{q-1}), N_q(n) \leq \frac{1}{n}(q^n + \frac{q^n - q}{q-1})$$

Therefore

$$N_q(n+1) - N_q(n) \geq \frac{1}{n(n+1)(q-1)}(q^{n+1}(nq - 3n - 1) + (2n+1)q) > 0$$

for every $q > 3$ as $nq > 3n - 1$. The rest cases need more precise estimations for $N_q(n)$:

$$N_q(n) \geq \frac{1}{n}(q^n - \frac{q^{[\frac{n}{2}]+1} - q}{q-1}), N_q(n) \leq \frac{1}{n}(q^n + \frac{q^{[\frac{n}{2}]+1} - q}{q-1})$$

If $q = 2$ then

$$N_2(n+1) - N_2(n) \geq \frac{1}{n(n+1)}((n-1)2^n - n2^{[\frac{n+1}{2}]+1} - (n+1)2^{[\frac{n}{2}]+1} + 2n + 2) > 0$$

starting from $n = 5$. For $1 < n < 5$ the formula also holds true, it can be verified by the simple evaluation. The case of $q = 3$ is similar. □

Lemma 3.3 *For any natural n*

$$C_q(n) = \sum_{i=1}^{[\frac{n}{2}]} N_q(i) + N_q(n). \tag{3}$$

Proof. Any polynomial of degree n contains irreducible divisor of degree less than or equal to $[\frac{n}{2}]$. So $C_q(n)$ does not exceed the sum (3). Now we consider any reducible polynomial from the above set $f_1(x)f_2(x)$. As $\deg f_1(x)f_2(x) = n$, $\deg f_1(x) = l < [\frac{n}{2}]$ then $\deg f_2(x) = n - l$. The existence of the additional polynomial $f_2(x)$ follows from the condition $N_q(l) \leq N_q(n-l)$ (true for $l < n-l$ as it obviously follows from the lemma (3.2)). So the upper boundary on the number of polynomials is accessible in this case. □

Theorem 3.4 *Let the polynomials used for the generalized Mignotte sequence generation possess the same degree n. Then this sequence allows to construct the modular Mignotte realization in $F_q[x]$ of any (k,t)-threshold access structure where*

$$t \leq C_q(n).$$

Also, this sequence allows to construct the modular Mignotte realization in $F_q[x]$ of any general access structure over the set of t participants where

$$t \leq log_2 C_q(n).$$

Proof. The boundary on the number of participants of the threshold secret sharing scheme follows from the previous lemma. To realize the arbitrary structure according to the theorem (2.2) we need no more than 2^t different pairwise co-prime moduli for multiplications (number of all subsets of t participants). □

And finally let us estimate the information rate of the constructed secret sharing scheme. Information rate is defined as the quotient of dividing the length of the secret by the maximal length of the share (in bits).We consider the most important case of $q = 2$.

Theorem 3.5 *The information rate of any polynomial Mignotte secret sharing scheme over $F_2[x]$ exceeds $1/2$.*

Proof. Let the degrees of Mignotte's sequence polynomials be n. The maximal degree of the LCM of polynomials belonging to unauthorized subset is kn where k is the corresponding number of multiplications for the moduli of the given subset. Therefore the degree of the secret is chosen from the interval $[kn, (k+1)n]$. The degrees of shares do not exceed kn. The estimation of the information rate ρ is:

$$\rho = \frac{kn}{\log_2\left(2^{kn+n} - 2^{kn}\right)} > \frac{kn}{\log_2\left(2^{kn}2^n\right)} = \frac{kn}{kn+n} > \frac{1}{2},\ k, n \in \mathbb{N}$$

□

Another well-known secret sharing scheme for the general access structures based on the monotone circuit construction was devised by Benaloh and Leichter [2]. It has the same estimation of the lower boundary on the information rate as it was shown in [9]. We do not investigate perfectness of the constructed Mignotte's secret sharing scheme in this paper. The perfectness can be measured as the quantity of information or the logarithm of the difference between the general entropy of the secret value and conditional one. In the case of basic Mignotte's scheme this estimation is not very good. However, it is possible to construct the Asmuth-Bloom polynomial secret sharing scheme over $F_q[x]$ i.e. choose the secret value modulo $p(x)$ where $p(x)$ is an additional modulus. In this case the quantity of information as well as the information rate can have a good estimation i.e. the scheme is close to the perfect an ideal one. It is a common approach to use the co-prime moduli as close as possible to achieve the best estimation of perfectness and ideality [3]. In the case of polynomials the above estimations can be considerably improved because we take the moduli of the equal degrees which is not possible for numbers. This

research is a subject of our further work. In fact, we managed to conclude this research after the conference. We have proved that the polynomial modular scheme is perfect and ideal using the technique of Quisquater, Preneel and Vanderwalle [7]. These authors revisited the security of the modular scheme in the ring of integers and showed that it is only asymptotically secure.

4 Acknowledgements

We thank the anonymous referees of the ICS workshop for their valuable comments that helped to find and correct the inaccuracies and unclear questions. Also, we thank N. Shenets for helping us to improve the proof of lemma 3.3.

References

[1] Asmuth, C.A., and J. Bloom, *A modular approach to key safeguarding*, IEEE Transactions on Information Theory. **29** (1983), 156–169.

[2] Benaloh, J., and J. Leichter, *Generalized secret sharing and monotone functions*, Lecture Notes in Computer Science. **403** (1990), 27–36.

[3] Goldreich, O., D. Ron and M. Sudan, *Chinese remaindering with errors*, IEEE Transactions on Information Theory. **46** (2000), 1330–1338.

[4] Iftene, S., *Compartmented secret sharing based on the CRT*, Cryptology ePrint Archive **408** (2005), URL: http://eprint.iacr.org/2005/408.pdf

[5] Lidl, R., and H. Niderraiter, "Finite fields," Cambridge University Press, Cambridge, UK, 1985.

[6] Mignotte, M., *How to share a secret*, Lecture Notes in Computer Science. **149** (1983), 371–375.

[7] Quisquater, M., Preneel, B., Vandewalle, J., *On the Security of the Threshold Scheme Based on the Chinese Remainder Theorem*, Lecture Notes in Computer Science. **2274** (2002), 199-210.

[8] Shamir, A., *How to share a secret*, Communications of the ACM. **22** (1979), 612–613.

[9] Stinson, D.R., "Cryptography: theory and practice," CRC Press, Boca Raton, Florida, 1995.