A New Secret Sharing Scheme Based on Polynomials over Finite Fields

Selda Çalkavur, Patrick Solé, Alexis Bonnecaze

mathematics

MDPI

Article

A New Secret Sharing Scheme Based on Polynomials over Finite Fields

Selda Çalkavur [1], Patrick Solé [2,*] and Alexis Bonnecaze [2]

[1] Math Department,Math Department, Kocaeli University, 41135 Kocaeli , Turkey
[2] CNRS, Aix Marseille University, Centrale Marseilles, I2M, 13009 Marseilles , France
* Correspondence: sole@enst.fr (P.S.)

Received: 12 June 2020; Accepted: 20 July 2020; Published: date

Abstract: In this paper, we examine a secret sharing scheme based on polynomials over finite fields. In the presented scheme, the shares can be used for the reconstruction of the secret using polynomial multiplication. This scheme is both ideal and perfect.

Keywords: Ideal secret sharing; polynomial; finite field

1. Introduction

Secret sharing schemes were first proposed by Blakley [1] and Shamir [2] in 1979. They represent an important cryptographic primitive that is still used in many security network protocols or for secure multi-party computations. A secret sharing scheme involves a *dealer* who holds a secret. This dealer distributes pieces of its secret (called *shares*) to a set of participants (also called *users*) in order that each party holds a share of that secret. Some subsets of participants can reconstruct the secret while some cannot. The groups which can reconstruct the secret are called *qualified* (or sometimes authorized), and the other groups are called *rejected*.

Threshold secret sharing scheme is one of the important class of secret sharing schemes. The main concept of (t, n)- threshold secret sharing scheme is that t out of n participants can retrieve the secret, but $(t-1)$ cannot. Shamir and Blakley's schemes are threshold schemes. Shamir's scheme was based on polynomial interpolation and Blakley used the hyperplane geometry to solve the secret sharing problem.

Pedersen [3] proves the Shamir scheme: The n shares (one for each shareholder) can be confirmed by the n shareowners. Moreover, several authors have investigated the general secret sharing schemes [4–10].

It is well known that polynomials play an important role in the development of the theory of algebraic structure of finite fields. Sun and Shieh [11] presented a polynomial-based secret sharing scheme. They used the Diffie-Hellman's principle to construct their scheme. Hwang and Chang [12] also employed polynomials to construct their secret sharing scheme.

In this paper, we present a secret sharing scheme based on polynomials over $GF(q)$, exploiting the structure of field extension of degree $d+1$. For concreteness, we give some numerical examples. We prove that the scheme is both ideal and perfect. We give conditions on q and d to thwhart passive attacks.

The material is organized as follows. The next section gives some necessary information about algebraic topics. In Section 3 we construct our secret sharing scheme and explain its security. Section 4 concludes our work.

2. Polynomials over Finite Fields

Polynomials over finite fields form an important class of finite rings which is heavily used in cryptography. We start by recalling some background helpful when working with polynomials.

Definition 1 ([13]). *Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a non-zero polynomial of degree n over an arbitrary field $GF(q)$, q being a prime. Then a_n is said to be the leading coefficient of $f(x)$ and a_0 is the constant term.*

In fact, the polynomials we consider belong to the field F of q^{d+1} elements, d being an arbitrary positive integer. To define F, we need to consider an irreducible polynomial $Q \in GF(q)[x]$ of degree $d+1$ and set $F = GF(q)[x]/(Q(x))$. Therefore, the protocol uses the operations (addition and multiplication) of the field F. In the sequel, we use indifferently the notations P or $P(x)$ as an element of the field.

3. The Scheme

In this section, we present a secret sharing scheme based on operations in the field F. The secret space and the sharing space are both equal to $GF(q^{d+1})^*$, the non-zero polynomials of degree d over $GF(q)$.

The secret, denoted s, is a polynomial of degree d over $GF(q)$, and as a polynomial, it can also be denoted $s(x)$. The protocol uses a trusted dealer T to deliver the shares of the secret s to the m participants.

The setup is as follows:

1. The shares, denoted $P_i(x)$, are randomly chosen by T.
2. T chooses a primitive irreducible polynomial Q of degree $d+1$, then computes the product of the m shares modulo $Q(x)$:
$$P(x) = \prod_{i=1}^{m} P_i(x) \mod Q(x).$$
Thus, $P(x)$ is of degree $\leq d$.
3. T computes the polynomial $D(x)$ such that $D(x) = s(x) - P(x)$ and makes public $Q(x)$ and $D(x)$.
4. The dealer sends the share $P_i(x)$, using a channel which preserves confidentiality, to user i for $(1 \leq i \leq m)$.

The reconstruction phase is as follows:
The m users pool their shares to compute $P(x) = \prod_{i=1}^{m} P_i(x) \mod Q(x)$ then $s(x) = D(x) + P(x)$.

Example 1. *Suppose that $q = 2$, $d = 2$, $m = 3$, $Q(x) = x^3 + x + 1$, and $F = GF(2)[x]/(Q(x))$. Take the shares as*
$$P_1(x) = x^2 + 1, P_2(x) = x^2 + x + 1, P_3(x) = x^2 + x$$
and the secret as $s(x) = x^2 + x + 1$.

The dealer T calculates $P(x)$ in the field F.

$$\begin{aligned} P(x) = \prod_{i=1}^{3} P_i(x) &= P_1(x).P_2(x).P_3(x) \\ &= x^6 + x^4 + x^3 + x \\ &= x. \end{aligned}$$

Then T makes public $D(x) = s(x) + P(x)$. Please note that the characteristic of the field is 2, hence subtraction and addition are the same. The calculation of $D(x)$ in this example gives

$$D(x) = (x^2 + x + 1) + (x)$$

$$D(x) = x^2 + 1.$$

The reconstruction phase is as follows. The m participants pool their shares to obtain $P(x)$, and then add the public value $D(x)$

$$s(x) = P(x) + D(x)$$
$$s(x) = x^2 + x + 1.$$

Example 2. *Suppose that* $q = 3$, $d = 3$, $m = 4$, $Q(x) = x^4 + 2 * x^3 + 2$, *and* $F = GF(3)[x]/(Q(x))$. *Take the shares as*

$$P_1(x) = x^3 + 2x^2, P_2(x) = x^3 + x + 1,$$
$$P_3(x) = x^3 + 2x, P_4(x) = x^3 + x^2 + 2$$

and the secret $s(x) = x^3 + x^2 + 1$.

$$P(x) = \prod_{i=1}^{4} P_i(x) = P_1(x).P_2(x).P_3(x).P_4(x)$$
$$= x^{12} + 2x^{10} + x^7 + 2x^3 = 1$$

The dealer makes public

$$D(x) = s(x) - P(x)$$
$$= (x^3 + x^2 + 1) - 1$$
$$= x^3 + x^2.$$

The reconstruction phase gives

$$s(x) = P(x) + D(x)$$
$$= x^3 + x^2 + 1.$$

3.1. Properties and Security

In a secret sharing scheme, a large number of participants may increase the security. We can explain this situation using the information rate ρ [14]. This parameter is an important parameter determining the security and the efficiency of a secret sharing scheme.

Proposition 1. *The size of the secret is* $\log_q(q^{d+1} - 1)$.

Proof. The secret space consists of the non-zero polynomials of degree d over $GF(q)$ and the number of these polynomials is $q^{d+1} - 1$. Therefore, the secret can be written using $d + 1$ elements of $\mathbb{F}_q$. □

In our scheme, the size of a share is exactly equal to the size of the secret. The information rate is

$$\rho = \frac{\log_q(q^{d+1} - 1)}{\log_q(q^{d+1} - 1)} = 1.$$

We recall that if the size of the shares of all participants are less than or equal to the size of the secret, then the secret sharing scheme is said to be ideal [15]. Therefore, we have the following theorem:

Theorem 1. *The constructed scheme is ideal.*

For the property of perfect privacy, we have to show [16] that every rejected set cannot learn anything about the secret (in the information theoretic sense) from their shares. In terms of entropy function, it means that the entropy of the secret knowing the shares of any rejected set is equal to the

entropy of the secret. In fact, the security of our scheme relies on the equation $s(x) = D(x) + P(x)$. Since $P(x)$ is a product of random polynomials, it can also be considered to be random. Moreover, s, D and P are of same size. This equation is therefore the same as the one of One Time Pad which has a perfect secrecy. It means that knowing D, an adversary cannot know any information about the secret. Moreover, an adversary who knows strictly less than m shares gets no information about the secret.

So this scheme has the property of perfect privacy [15] and it has a secure access structure. Moreover, the scheme is robust against passive adversaries. It means that if all the participants follow the protocol honestly, no attacker can retrieve the secret with a probability greater than $1/(q^{d+1} - 1)$. Indeed, suppose that $m - 1$ users collude, pool their shares, and try to guess the share of order m picking a random element of F^*. The probability of success of such an attack is $\frac{1}{(q^{d+1}-1)}$. More generally if r users with $r < m - 1$ try to mount an attack, with less information than $m - 1$ users, the probability of success of that attack will be strictly less than the above quantity.

Remark 1. *This scheme is not a $(m, m)-$ threshold secret sharing scheme since the factorization in the field is not unique. Suppose, for example, that a share is equal to the product of all the shares. In this case, this share is theoretically able to recover the secret. This fact means that there is no predefined threshold to recover the secret from the shares, but it does not affect the security of the scheme.*

It is also easy to see that the scheme is not monotone since the authorized coalition is unique.

4. Conclusions

In this paper, we have studied a new secret sharing scheme based on polynomial multiplications over $GF(q)$. We have determined its access structure and computed its information rate. Our scheme is ideal and secure against passive attacks. Our scheme could be used in embedded systems because multiplications in a field are easily optimized and therefore the computational costs are lower than schemes using interpolation.

Author Contributions: Investigation, P.S., A.B.; and supervision S.Ç. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Blakley, G.R. Safeguarding Cryptographic Keys. In Proceedings of the 1979 International Workshop on Managing Requirements Knowledge (MARK), New York, NY, USA, 4–7 June 1979; pp. 313–317.
2. Shamir, A. How to share a secret. *Comm. ACM* **1979**, *22*, 612–613.
3. Pedersen, T.P. Distributed provers with applications to undeniable signatures. In *Lecture Notes in Computer Science 547, Advances in Cryptology-Eurocrypt'91*; Davies, D.W., Ed.; Springer-Verlag: Berlin, Germany, 1991; pp. 221–238.
4. Ding, C.; Kohel, D.; Ling, S. Secret sharing with a class of ternary codes. *Theor. Comp. Sci.* **2000**, *246*, 285–298.
5. Karnin, E.D.; Greene, J.W.; Hellman, M.E. On secret sharing systems. *IEEE Trans. Inf. Theory* **1983**, *29*, 35–41.
6. Massey, J.L. Minimal codewords and secret sharing. In Proceedings of the 6th Joint Swedish-Russian on Information Theory, Mölle, Sweden, 22–27 August 1993; pp. 276–279.
7. Eliece, R.J.M.; Sarwate, D.V. On sharing secrets and reed-solomon codes. *Commun. Assoc. Comp. Mach.* **1981**, *24*, 583–584.
8. Okada, K.; Kurosawa, K. MDS Secret Sharing Scheme Secure Against Cheaters. *IEEE Trans. Inf. Theory* **2000**, *46*, 1078–1081.
9. Piepryzk, J.; Zhang, X.M. Ideal Threshold Schemes from MDS Codes. In *Information Security and Cryptology-Proc. of ICISC 2002 (Lecture Notes in Computer Science)*; Springer-Verlag: Berlin, Germany, 2003; Volume 1172, pp. 67–78.

10. Renvall, A.; Ding, C. The access structure of some secret sharing schemes. In *Information Security and Privacy (Lecture Notes in Computer Science)*; Springer-Verlag: Berlin, Germany, 1996; Volume 1172, pp. 67–78.
11. Sun, H.-M.; Shieh, S.-P. Construction of dynamic threshold schemes. *Electron. Lett.* **1994**, *30*, 2023–2026.
12. Hwang, S.; Chang, C. A dynamic secret sharing scheme with cheater detection. In *Lecture Notes in Computer Science 1172, ACISP'96*; Springer-Verlag: Berlin, Germany, 1993; pp. 136–146.
13. Lidl, R.; Niederreiter, H. *"Finite Fields", Encyclopedia of Mathematics and Its Applications*; University of London: London, UK, 1983; Volume 20.
14. Padro, C. Robust vector space secret sharing schemes. *Inf. Process. Lett.* **1998**, *68*, 107–111 .
15. Yılmaz, R. Some Ideal Secret Sharing Schemes. Master's Thesis, Bilkent University, Ankara, Turkey, 2010.
16. Beimel, A. Secret-sharing schemes: a survey. In *International Conference on Coding and Cryptology*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 11–46.