A New Threshold Scheme Via Plücker Coordinates [1]

Wang Mingsheng Feng Dengguo Wang Guilin
State Key Laboratory of Information Security
Institute of Software, Chinese Academy of Sciences
Beijing 100080, P.O.Box Beijing 8718
e-mail: wangmsh@ercist.iscas.ac.cn

Abstract Plücker coordinates is an important concept in pure mathematics. In our recent paper [15], we obtained a general framework for constructing secret sharing schemes. In this paper, we will give a concrete scheme which is a particular case of our basic strategy. This scheme has a simple structure and easily to operate.

Key Words Cryptology, Secret sharing scheme, Plücker coordinates.

1 Introduction

The ideal of threshold scheme was independently introduced by Blakely [1] and Shamir [9]. Since then, many research papers have appeared, for example [2], [3], [5], [6], [7], [8], [10], [11], [12], [13], [14] etc. A (t, n) threshold scheme is designed to divide secret K into "shares" $K_1, K_2, \cdots, K_n$ such that

(i) knowledge of any t shares is sufficient to derive K.

(ii) knowledge of any $t-1$ shares provides no any information about K.

In our recent paper[15], we have proposed a new strategy based on Plücker coordinates which can be used as giving new explanation for several well-known threshold schemes, for example, Shamir's secret sharing scheme, Blakely's scheme and Karnin-Greene-Hellman threshold scheme.

In this paper, we propose a new scheme by using Plücker coordinates which is a geometric scheme.

First, we explain the concepts of plücker coordinates in the section 2, then we propose our threshold scheme in section 3, and in section 4, we discuss its security properties.

2 Plücker Coordinates

In this section, we give some mathematics preparations which will be needed in our discussions. Some of them are standard results but they are included here for sake of completeness and to fix the notation.

[1]This research is supported by 973 project (G1999035802) and State Key Laboratory of Information Security

Let V be a N dimensional vector space over a field k. Let $\epsilon_1, \epsilon_2, \cdots, \epsilon_N$ be the standard basis of V and let W be a t-dimensional subspace with basis $w_1, \cdots, w_t$. Suppose that

$$w_p = \sum_{j=1}^{N} a_{jp}\epsilon_j, \quad p = 1, \cdots, t$$

and

$$\pi(i) = \pi(i_1, \cdots, i_t) = det(a_{i_j p})$$

for $i = (i_1, \cdots, i_t)$ with $1 \leq i_j \leq N$.

Notice that $\pi(i)$ are uniquely determined by the $\pi(i_1, \cdots, i_t)$ with $1 \leq i_1 < i_2 < i_t \leq N$.

Let $(\pi(i)) = (\pi(1, 2, \cdots, t), \pi(1, \cdots, t-1, t+1), \cdots, \pi(N-t+1, \cdots, N))$.

Note that we arrange the coordinates of $(\pi(i))$ in lexicographic ordering of $i = (i_1, \cdots, i_t)$.

Also, if $w'_p, p = 1, \cdots, t$ is another basis of W with

$$w'_p = \sum_{s=1}^{t} b_{sp} w_s$$

and

$$w'_p = \sum_{j=1}^{N} a'_{jp}\epsilon_j$$

then

$$a'_{jp} = \sum_{s=1}^{t} b_{sp} a_{js}$$

with $det(b_{sp}) \neq 0$ and $\pi'(i) = det(b_{sp})\pi(i)$for all $i = (i_1, i_2, \cdots, i_t)$. where $\pi'(i) = \pi'(i_1, \cdots, i_t) = det(a'_{i_j p})$.

Let $\mathbb{P}^m$ be a projective space over the field F_p. Namely, a point $\eta \in \mathbb{P}^m$ is given by $m+1$ elements $(\eta_0 : \eta_1 : \cdots : \eta_m)$ of the field F_p, not all equal to 0; and two points $(\xi_0 : \xi_1 : \cdots : \xi_m)$ and $(\eta_0 : \eta_1 : \cdots : \eta_m)$ are considered to be equal in $\mathbb{P}^m$ if and only if there exists $\lambda \neq 0$ such that $\eta_i = \lambda\xi_i$ for $i = 0, 1, \cdots, m$. Any set $(\xi_0 : \xi_1 : \cdots : \xi_m)$ defining the points ξ is called a set of homogeneous coordinates for ξ.

Hence, for every $t-$ dimensional subspace W of V, we can uniquely determine a point $(\pi(i))$ in $\mathbb{P}^m$, $m = \binom{N}{t} - 1$, which depends on W alone and not on the choice of basis.

We denote by $(\pi_W(i))$ the unique point in $\mathbb{P}^m$ determined by W.

Thus, we have a well-defined map P of the set of all $t-$dimensional subspace of V into $\mathbb{P}^m$ given by

$$P(W) = (\pi_W(i))$$

where $i = (i_1, \cdots, i_t), \quad 1 \leq i_1 < \cdots < i_t \leq N$.

The $\pi_W(i)$ are called the plücker coordinates of W. Note that for two different basis of W, $\pi_W(i)$ are different, but they are equal up to a non-zero constant multiple.

Now, let $\mathbb{A}_i^m = \{(\eta_0, \eta_1, \cdots, \eta_m) \in \mathbb{P}^m | \eta_i \neq 0\}$. Then $\mathbb{P}^m = \bigcup_{i=0}^m \mathbb{A}_i^m$. Points of $\mathbb{A}_i^m$ can be put in one-to-one correspondence with the points of an N-dimensional affine space by setting $\alpha_j = \frac{\eta_j}{\eta_i}$ for $j = 0, 1, \cdots, m$, and sending $\eta \in \mathbb{A}_i^m$ to

$(\alpha_0, \cdots, \alpha_{i-1}, \alpha_{i+1}, \cdots, \alpha_m) \in \mathbb{A}^m$.

Thus, for any $t-$dimensional subspace W of V, if $(\pi_W(i)) \in \mathbb{A}_j^m$ for some j, then $(\pi_w(i))$ has a unique affine coordinate in $\mathbb{A}_j^m$.

We can describe $(\pi_W(i))$ in terms of exterior product.

In fact, Let $v_1, \cdots, v_t$ be a basis of W, and A be a $n \times t$ matrix such that:

$$(v_1, \cdots, v_t) = (\epsilon_1, \cdots, \epsilon_n) \cdot A$$

Then, it is easily to prove that

$$v_1 \wedge v_2 \cdots \wedge v_t = \sum_i det\,[A|i]\, e_{i_1} \wedge \cdots \wedge e_{i_t}$$

where $det\,[A|i]$ denote the determinant of the $t \times t$ minor from the $i_1, \cdots, i_t$ rows and $1, \cdots, t$ columns, and $i = (i_1, \cdots, i_t)$. Hence $\pi_W(i) = det\,[A|i]$ with $i = (i_1, \cdots, i_t)$, $1 \leq i_1 < \cdots < i_t \leq n$.

3 Scheme

In this section, We will describe a secret sharing scheme based on the plücker coordinates.

Now, assume that n is the total number of "shares" need to be constructed and t is the threshold value such that any t shares they jointly hold can be used to derive the secret K.

Let V be a $t+1$ dimensional vector space over a prime field F_p. First, we describe a basic strategy as follows:

A basic strategy:

The secret generation center generates n vectors $s_i \in V$ such that any t vectors generate the same vector subspace W of V, $1 \leq i \leq n$. Assume that secret K is concealed by the Plucker coordinates of W. The n shares are given by s_i.

In the following, we will propose a new scheme which is a particular example of the basic strategy.

3.1 A new scheme

In this part, We will point out that a concrete scheme can be constructed by using Plücker coordinates.

Let V be a $t+1$-dimensional vector space over a prime field F_p. Without loss of generality, we can assume $V = {F_p}^{t+1}$. Suppose the center wants to share a secret $K \in F_p$, then a new scheme can be constructed as follows:

Descriptions of the scheme.

(i) The secret generation center randomly selects t linear independent (column) vectors $v_1, \cdots, v_t \in V$. Let $A = (v_1, \cdots, v_t)$ be $t+1 \times t$ matrix. Without loss of generality, we can assume that $a = det\,[A|12\cdots t] \neq 0$, and compute $b = det\,[A|23\cdots tt+1]$. We use L to denote the line determined by (a, b) and $(0, 0)$ in the plane $\mathbb{A}^2$.

(ii) Let K be a secret needed to be shared. The center randomly selects a line L' from the plane $\mathbb{A}^2$ such that the first coordinate of the intersection point of L and L' is K. (We will provide an algorithm for choosing line L' later.)

(iii) The center selects randomly a $t \times n$ matrix B such that any t rows are linearly independent and computes $s_1, \cdots, s_n$ as follows:

$$(s_1, s_2, \cdots, s_n) = (v_1, v_2, \cdots, v_t) \cdot B$$

(iv) For $1 \leq i \leq n$, the center gives secretly shares s_i to P_i, and announces L'.

Recovery of the secret K

(i) When participants $P_{i_1}, P_{i_2}, \cdots, P_{i_t}$ want to determine the secret K, they can form the matrix $S = (s_{i_1}, s_{i_2}, \cdots, s_{i_t})$, and compute $c = \pi_W(1, 2, \cdots, t)$, $d = \pi_W(2, 3, \cdots, t+1)$. Thus parametric equation of the line L_1 determined by (c, d) and $(0, 0)$ is $x = ct, y = dt$. (Note that $L = L_1$)

(ii) They compute the intersection point of L' and L. Hence K can be obtained.

3.2 Correctness discussions of the new scheme

Now, we must prove that our scheme is feasible. we first provide an algorithm for choosing the line L' in the step (ii) of the scheme.

First, we note that a simple lemma:

Lemma 1 Let parametric equaton of line L be $x = at, y = bt$ with $a \neq 0$. Let L' be another line with its parametric equation $x = b_1 t + c_1, y = b_2 t + c_2$ such that L and L' have only a uniqe intersection point. Then K is the first coordinate of the intersection point of L and L' if and only if $c_1 = K - b_1 t_2$ and $c_2 = b(\frac{K}{a}) - b_2 t_2$ for some t_2.

With the above lemma 1, we can state an algorithm for choosing the Line L' in the step (ii) of the scheme as follows:

(i) Let the parametric equation of line L be $x = at, y = bt$ with $a \neq 0$. we randomly select b_1 and b_2 such that $ab_2 - bb_1 \neq 0$.

(ii) We randomly select a $t_2 \in F_p$, and set $c_1 = K - b_1 t_2$, $c_2 = b(\frac{K}{a}) - b_2 t_2$.

(iii) Setting parametric equation of L' as follows: $x = b_1 t + c_1$, $y = b_2 t + c_2$.

Now, correctness of the scheme is implied by the following lemma 2:

Lemma 2 Let L be the line in the step (i) of the scheme, and L_1 be the line in the first step of recovery phrase. Then $L = L_1$.

Proof. Correctness of the Lemma 2 comes from basic properties of Plücker coordinates.

4 Security discussion of the Scheme

Now, we will prove that our scheme can meet security requirements specified in the section 1.

(i) Any t participants can compute the value of K, but no group of $t-1$ participants can do so.

Let participants $P_1, P_2, \cdots, P_t$ want to recover the secret K, then they can form a $n+1 \times t$ matrix $S = (s_{i_1}, s_{i_2}, \cdots, s_{i_t})$. Let $W = \text{Span}\ (v_1, \cdots, v_n)$. They can compute the homogeneous coordinates of $(\pi_W(i))$: $\pi_W(j) = det[S|j]$, where $j = (j_1, \cdots, j_t)$ and $1 \leq j_1 < \cdots < j_t \leq n$.

In fact,

$$c = \pi_W(1, 2, \cdots, t) = det[S|12 \cdots t] = a \cdot f$$

and

$$d = \pi_W(2, 3, \cdots, t+1) = det[S|23 \cdots t+1] = b \cdot f$$

where f is a non-zero constant.

Hence the line determined by (a,b) and (0,0) is same as the line determined by (c,d) and (0,0). So K can be obtained. This establishes that any group of t participants will be able to derive the secret K in this scheme.

(ii) If a group of $t-1$ participants attempt to recover K, they will obtain $t-1$ vectors. In order to compute $(\pi_W(i))$, they must hypothesize a vector $s \in {F_p}^{t+1}$ so that s and other $t-1$ vectors linearly independent over F_p. Hence, for every hypothesized value s, there is a unique point in $\mathbb{P}^m$. Hence, no value of the key can be ruled, and thus a group of $t-1$ participants can obtain no information about the key.

5 An example

In the following, we will give an example to explain this scheme.

Example 1 Let $p = 17$, and $V = {F_p}^4$, and $t = 3, n = 5$. We will propose a $(3, 5)$ threshold scheme.

(i) The center selects randomly 3 linearly independent column vectors $v_1 = (1, 7, 11, 15)^t$, $v_2 = (2, 8, 3, 14)^t$, $v_3 = (16, 2, 7, 6)^t$. It is easily to compute $\pi_W((1, 2, 3)) =$

12, and $\pi_W((2,3,4)) = 4$, where 't' denotes transpose of a row vector and W=Span (v_1, v_2, v_3).

(ii) Suppose a secret $K = 11$ need to be shared. The center selects a line L' from the plane $\mathbb{A}^2$ such that the first coordinate of the intersection point of L and L' is 11. For example, choosing L' with its parametric equation $x = 3t, y = 2t - \frac{11}{3}$, and announcing L'.

(iii)The center compute

$$(s_1, s_2, \cdots, s_5) = (v_1, v_2, v_3) \cdot B$$

where

$$B = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 4 & 7 & 9 & 11 \\ 2^2 & 4^2 & 7^2 & 9^2 & 11^2 \end{bmatrix}$$

Hence

$$\begin{aligned} s_1 &= (1, 14, 11, -1)^t \\ s_2 &= (10, 3, -1, -3)^t \\ s_3 &= (0, 8, 1, -1)^t \\ s_4 &= (5, 5, 0, 4)^t \\ s_5 &= (4, 14, 7, 11)^t \end{aligned}$$

(iv) The center gives s_i to P_i, $i = 1, \cdots, 5$.

Suppose participants P_1, P_2, P_3 want to determine K. They form a 5×3 matrix $C = (s_1, s_2, s_3)$ as follows:

$$C = \begin{bmatrix} 1 & 10 & 0 \\ 14 & 3 & 8 \\ 11 & -1 & 1 \\ -1 & -3 & -1 \end{bmatrix}$$

They compute $\pi_W((1,2,3)) = det\,[C|123] = 3$, and $\pi_W((2,3,4)) = det\,[C|234] = 1$, So they get the parametric equation of the line L is $x = 3t, y = t$, hence they obtain the secret $K = 11$ by solving the following equations

$$\begin{cases} 3t_1 &= 3t_2 \\ t_1 &= 2t_2 - \frac{11}{3} \end{cases}$$

In fact, $K = 3t_1$.

6 Conclusion

In this paper, we propose a new method for constructing threshold schemes by using plucker coordinates. After a general strategy is proposed, we give a concrete scheme which is a particular case. This scheme has a simple structure and easily to operate. We will further study possible applications of plücker coordinates in other papers.

References

[**1**] G. R. Blakley. Safeguarding cryptographic keys. AFIPS conference proceedings, 48, 313-317, 1979.

[**2**] E. F. Brickell. Some ideal secret sharing scheme. Journal of combinatorial mathematics and combinatorial computing 9, 105-113, 1989.

[**3**] E. F. Brickell and D. M. Davenport, On the classification of ideal secret sharing schemes, Journal of Cryptology, Vol. 4 (1991), 121-134.

[**4**] L. Gong and D. L. Wheeler, A Matrix key-distribution scheme, Journal of Cryptology, Vol. 2 (1990), 51-59.

[**5**] C. S. Laih, L. Harn, J. Lee and T. Hwang. Dynamic threshold scheme based on the definition of cross-product in an N-dimensional linear space. Crypto'89, Lecture notes in computer science 435, 286-297. Springer-verlag, 1990.

[**6**] S. C. Kothari. Generalized linear threshold scheme. Advances in Cryptography: Proceedings of CRYPTO'84 , Springer-Verlag, 1985, 231-241.

[**7**] E. D. Karnin, J. W. Greene and M.E. Hellman. On sharing secret system. IEEE Transactions on Information Theory, Vol 29,35-41,1983.

[**8**] T. Matsumoto. Incidence structure for key sharing, Advance in Cryptology: ASIACRYPT'94, Lecture Notes in Computer Science, 917, 342-353, 1995.

[**9**] A. Shamir. How to share a secret. Communications of the ACM, Vol 22, No. 11, 612-613,1979.

[**10**] D. R. Stinson. Cryptography theory and practice. CRC press, Inc., Boca Raton, 1995.

[**11**] D. R. Stinson. On some methods for unconditionally secure key distribution and broadcast encryption. Designs, Codes and Cryptography, Vol. 12, 215-243 (1997).

[**12**] D. R. Stinson. An explication of secret sharing scheme, Designs, Codes and Cryptography, Vol. 4, 177-191 (1992).

[**13**] G. J. Simmons (ed). Contemporary Cryptology, The science of information integrity. IEEE Press, 1992.

[**14**] B. Schneier. Applied cryptography: Protocol, Algorithm, and Source code in C. John Wiley & Sons, Inc. (1996).

[**15**] M. Wang, D. Feng and G. Wang. Threshold Schemes Based on Plucker Coordinates. Submitted.