Access Structures of Elliptic Secret Sharing Schemes

Hao Chen, San Ling, and Chaoping Xing

Abstract—It is a central problem in secret sharing to understand the access structures of secret sharing schemes. In Chen and Kramer, secret sharing schemes from algebraic-geometric codes and their applications in secure multiparty computation were proposed and studied. For any given finite field $GF(q)$, these secret sharing schemes are ideal ramp secret sharing schemes and allow arbitrarily many players. In this correspondence, we give the access structures explicitly for the elliptic secret sharing schemes from algebraic-geometric (AG) codes associated with elliptic curves. Based on higher degree rational points on elliptic curves, we also construct some nonideal secret sharing schemes with weighted threshold structures.

Index Terms—Access structure, algebraic-geometric (AG) code, elliptic curve, secret sharing scheme.

I. INTRODUCTION AND PRELIMINARIES

In a secret sharing scheme among the set of players $P = \{P_1, \ldots, P_n\}$, a dealer $D_0$, not in $P$, has a secret $s \in K$ and distributes shares $s_i \in K_i$ of the secret among the players in $P$ such that only the qualified subsets of players can reconstruct the secret from their shares. Here, $K$ denotes the set of secrets and $K_i$ denotes the set of shares for player $P_i$. If the information rate is 1, it is an ideal $\{k, n\}$-threshold scheme if the access structure consists of the subsets of at least $k$ elements in the set $P$. This is, among the $n$ players any subset of at least $k$ players can reconstruct the secret. The first secret sharing scheme given independently by Blakley [4] and Shamir [17] in 1979 was a threshold secret sharing scheme. The existence of perfect secret sharing schemes with arbitrary given access structures was proved in [3] and [10]. If the information rate is 1, the secret sharing scheme is called ideal. It is a long standing problem to characterize the access structures of ideal secret sharing schemes (see [5]).

In a weighted threshold secret sharing scheme, each player $i$ is given a weight $w_i > 0$, a subset $\{i_1, \ldots, i_t\}$ of players is qualified if and only if $w_{i_1} + \cdots + w_{i_t} \geq T$, where $T$ is a threshold value. Weighted threshold secret sharing schemes have been considered in the introductory paper [17] of Shamir and studied in [1], [2], [6], [14], [15]. We will show that algebraic curves over finite fields form a natural resource to construct weighted threshold secret sharing schemes.

The approach of secret sharing based on error-correcting codes was studied in [11]–[13]. Actually Shamir’s $(k,n)$-threshold scheme is just the secret sharing scheme based on the famous Reed–Solomon (RS) code. Let $C$ be a linear error-correcting $[n+1, k, d]$ code over a finite field $GF(q)$ with code length $n+1$, dimension $k$ and minimum Hamming distance $d$. Let $G = \{g_{ab}\}_{0 \leq a, b \leq n}$ be a generator matrix of $C$ such that no column of $G$ is 0. Suppose $s$ is a given secret value in $GF(q)$ of the dealer $D_0$ and the secret is shared among $P = \{P_1, \ldots, P_n\}$, the set of $n$ players. Let $g_0 = (g_{00}, \ldots, g_{0n})^T$ be the $0$th column of $G$. Choose a $u = (u_0, \ldots, u_k) \in GF(q)^k$ randomly such that $s = \sum a_i u_i$. We have the codeword $c = (c_0, \ldots, c_n) \in GF(q)^n$. It is clear that $c_0 = s$ is the secret. The dealer $D_0$ then gives the $i$th player $P_i$ the value $c_i$ as the share of $P_i$, for $i = 1, \ldots, n$. This is an ideal perfect secret sharing scheme. In this secret sharing scheme, the error-correcting code $C$ is assumed to be known to every player and the dealer. We refer to [11], [12], and [13] for the following Lemma.

Lemma 1: (cf. [11], [12], and [13]). Let $C$ be a linear code of length $n+1$ with generator matrix $G$. Suppose the dual of $C$, i.e., $C^\perp = \{v = (v_0, \ldots, v_n) : GV^T = 0\}$, has no codeword of Hamming weight 1. In the above secret sharing scheme based on the error-correcting code $C$, for any positive integer $m$, $(P_1, \ldots, P_m)$ can reconstruct the secret if and only if there is a codeword $v = (1, 0, \ldots, v_{i}, 0, \ldots, 0)$ in $C^\perp$.

Secret sharing schemes based on algebraic-geometric codes were proposed in [7] as a natural generalization of Shamir’s scheme. They are so called ramp secret sharing schemes in the sense that any subset of $P$ with fewer than $t_1$ players is not in the access structure and any subset of $P$ with at least $t_2$ players is in the access structure, for some $t_1 < t_2$. Generally speaking we do not know whether a set with $t$ elements, where $t_1 < t < t_2$, is qualified or not. This kind of secret sharing schemes based on AG codes allows arbitrarily many players for a constant-size base field $GF(q)$. Moreover the gap $t_2 - t_1$ is bounded by the intrinsic invariant $2g$ ($g$ is the genus) of the curve. In this correspondence we give explicitly the access structures of these schemes from AG codes when the underlying curves are elliptic curves (elliptic secret sharing schemes). By using higher degree rational points on elliptic curves, we also construct some weighted threshold secret sharing schemes.

II. ACCESS STRUCTURES OF ELLIPTIC SECRET SHARING SCHEMES

In this section, we obtain the access structures of elliptic secret sharing schemes. We shall first recall some basic facts about algebraic-geometric (AG) codes. For more details, the reader may refer to [18]–[20].

Let $X$ be an absolutely irreducible, projective and smooth curve defined over $GF(q)$ with genus $g$. $D = \{P_0, \ldots, P_n\}$ be a set of $GF(q)$-rational points of $X$ and $G$ be a $GF(q)$-rational divisor satisfying $\sum_{P_i \in D} \omega_i = 0$. Let $L(G) = \{f : (f + G) \geq 0\}$ be the linear space (over $GF(q)$) of all rational functions with divisor not smaller than $-G$, and $\Omega (B) = \{\omega : (\omega + B) \geq 0\}$ be the linear space of all differentials with divisor not smaller than $B$. Then the functional AG (algebraic-geometric) code $C_L(G, D)$ is $GF(q)^{n+1}$ and residual AG (algebraic-geometric) code $C_{\Omega}(D, G)$ is $GF(q)^{n+1}$ are defined as the evaluations of $L(G)$ and $\Omega (B)$, respectively, at the points in the set $D$. $C_{\Omega}(D, G)$ is an $[n + 1, k = \dim L(G) - \dim (L(G - D)), n + k - \deg (G)]$ code over $GF(q)$ and $C_L(D, G)$ is an $[n + 1, k = \dim (\Omega (G - D)) - \deg (\Omega (G)), d \geq \deg (G) - 2g + 2]$ code over $GF(q)$. It is also known that $C_L(D, G)$ and $C_{\Omega}(D, G)$ are dual codes.

Using $C = C_{\Omega}(D, G)$, secret sharing schemes based on AG codes were constructed in [7]. From the results in [7], it is known that in the
case of elliptic secret sharing schemes, i.e., where $X = E$ is an elliptic curve and the genus $g = 1$, every subset with at least $n - \deg(G) + 2$ elements is qualified and every subset with fewer than $n - \deg(G)$ elements is unqualified. In the following result, we determine explicitly which sets with $n - \deg(G)$ or $n - \deg(G) + 1$ elements are qualified.

In general, any qualified set is said to be minimal if none of its proper subsets is also a qualified set.

We also note that, when $X = E$ is an elliptic curve over $GF(q)$, the set of $GF(q)$-rational points on $E$, denoted by $E(GF(q))$, forms a finite abelian group with zero element $O$.

**Theorem 1:** Let $E$ be an elliptic curve over $GF(q)$. Let $D \subseteq \{P_0, P_1, \ldots, P_n\}$ be a subset of $E(GF(q))$ of $n + 1$ nonzero elements and let $G = mO$. Consider the elliptic secret sharing scheme obtained from $E$ with the set of players $P = \{P_1, \ldots, P_n\}$.

Let $A = \{P_1, \ldots, P_m\}$ be a subset of $P$ with $t$ elements, and let $B$ be the element in $E(GF(q))$ such that the group sum of $B$ and $P_1, \ldots, P_m$ in $E(GF(q))$ is $O$. If $A^- = \{P \in A\}$ is a minimal qualified subset for the secret sharing scheme from $C_R(D, G)$, then $t \leq m$.

Furthermore, we have the following:

1) when $t = m$, $A^-$ is a minimal qualified subset if and only if $B = O$;

2) when $t = m - 1$, $A^-$ is a minimal qualified subset if and only if $B$ is not in $D$ or $B$ is in the set $A$;

3) any subset of $P$ of more than $n - m + 2$ elements is qualified.

**Proof:** Applying Lemma 1 with $C = C_{R}(D, G)$, it follows that if $A^-$ is a minimal qualified subset if and only if we can find a function $f \in L(G)$ whose zero locus in $P$ is the set $A$ and $f(P_0) \neq 0$, i.e., the set $A^-$ is a minimal qualified subset if and only if we can find an effective $GF(q)$-rational divisor $D$ of degree $\deg(G) - \deg(G) (A)$ such that the elements of supp(U) are either outside of $D$ or in $A$, and the divisor $A + U$ is linearly equivalent to the divisor $G$ (here, we have identified the set $A$ with the divisor $P_1 + \cdots + P_t$). The minimum Hamming weight of $C_{R}(D, G)$ is at least $n + 1 - t$. Thus, if $A^-$ is a minimal qualified subset, then $t \leq m$.

The following fact is useful for the rest of the proof: for any $t$ points $W_1, \ldots, W_t$ in $E(GF(q))$, the divisor $W_1 + \cdots + W_t - tO$ is linearly equivalent to the divisor $W - O$, where $W$ is the group sum of $W_1, \ldots, W_t$ in $E(GF(q))$ (see [9]).

Suppose $t = m$. If $B = O$, then the group sum of $P_1, \ldots, P_m$ in $E(GF(q))$ is $O$, so the divisor $P_1 + \cdots + P_m = mO$, which therefore implies that the group sum of $P_1, \ldots, P_m$ in $E(GF(q))$ is $O$, i.e., $B = O$. (This proves 1).

Next suppose $t = m - 1$. If $\{P_1, \ldots, P_{m-1}\}$ is a minimal qualified subset, then there exists a function $f \in L(G)$ such that the divisor of $f$ is $P_1 + \cdots + P_{m-1} - O$, which implies that the group sum of $P_1, \ldots, P_{m-1}$ in $E(GF(q))$ is $O$, i.e., $B = O$. (This proves 2).

If $A$ is a subset of $P$ such that $\{|A| \leq m - 2\}$, the divisor $G - A$ has its degree $\deg(G - A) \geq 2$ (we have again identified the set $A$ with the divisor $P_1 + \cdots + P_t$). Hence the corresponding linear system has no base point (see [9]). We can find a function in $L(G - A)$ such that it is not zero at $P_0$, thus we have a codeword in $C_{R}(D, G)$ which is not zero at $P_0$ and zero at all points of $A$. This implies that $A^-$ is a qualified subset. The statement 3) is proved.

**Example 1:** Let $E$ be the elliptic curve $y^2 + y = x^3$ defined over $GF(4)$. This is the Hermitian curve over $GF(4)$, it has nine rational points and $E(GF(q))$ is isomorphic to $Z_3 \oplus Z_3$. We take $G = 3O$, where $O$ is the zero element in the group $E(GF(4))$. Let $P_0$ be the rational point on $E$ corresponding to $(i, j)$ in $Z_3 \oplus Z_3$, with $P_0 = O$. Let $D = \{P_0, P_0, \ldots, P_2\} = E(GF(4)) \setminus \{P_0\}$ and $P = \{P_0, \ldots, P_2\} = D \setminus \{P_0\}$.

1) In the case where $A$ has three elements, by Theorem 1, 1), $A^-$ is a minimal qualified subset if and only if the sum of the three elements in $E(GF(q))$ is $O$. By determining all the three-element subsets of $P$ whose elements sum to $O$, it follows that the minimal qualified subsets of four elements are: $\{P_{0}, P_{1}, P_{2}\}$, $\{P_{0}, P_{0}, P_{2}\}$, $\{P_{1}, P_{0}, P_{1}\}$, $\{P_{0}, P_{2}, P_{2}\}$, $\{P_{2}, P_{2}, P_{2}\}$.

2) In the case where $A$ has two elements, say $A = \{U, V\} \subseteq P$, $B$ has to be $O$ or $U$ or $V$. Then $U + V = O$ or $2U = O$ or $2V = O$. However, $U$ and $V$ have been chosen to be distinct. Thus the minimal qualified subsets of five elements are $\{P_{1}, P_{2}\}$, $\{P_{1}, P_{3}\}$, $\{P_{2}, P_{2}\}$.

3) The subsets of $P$ with six elements and the set $P$ are qualified. The subsets in 1) and 2) are the minimal qualified subsets.

The main result Theorem 1 can help us to construct some ideal access structures, which can be realized by ideal perfect secret sharing schemes from elliptic curves.

Let $H$ be a finite group which is $E(GF(q))$ for some elliptic curve $E$ defined over $GF(q)$, such that the group order $|H|$ is an odd number. It is known that any cyclic group of $p$ elements, where $p$ is an odd prime, is an example of such a group (see [16], [18]). Let $P = H \setminus \{O, W\}$ be the set of $|H| - 2$ players, where $O$ is the zero element of $H$ and $W$ is any nonzero element in $H$. We define an access structure $F$ on $P$ as follows. Any subset of $P$ with fewer than $|H| - 4$ elements is not in $F$; any subset, other than $\{-W\}$, with at least $|H| - 3$ elements is in $F$; and there are $|H| - 3)/2$ subsets, of the form $\{a, -a\}$, with $|H| - 4$ elements in $F$, where $a$ runs over all elements in $P \setminus \{-W\}$. From Theorem 1 we have the following result.

**Corollary 1:** The above access structure can be realized by an ideal perfect secret sharing scheme from an elliptic curve.

**Proof:** We take an elliptic curve $E$ such that $E(GF(q)) = H$. Let $G = 2O$, $D$ be the set $H - 4$ nonzero elements in $E(GF(q))$ and any nonzero element $W$ in $D$ be the dealer. Using Theorem 1, 2), if $A = \{a\}$ is such that $A^-$ is qualified, then we must have 2$n = O$, which implies that $a = O$ since $|H|$ is an odd number. This is a contradiction since $A \subseteq P$ means that $a \neq O$. Hence, we only have minimal qualified subsets with $|H| - 4$ elements.

**III. WEIGHTED THRESHOLD SECRET SHARING SCHEMES FROM ELLIPTIC CURVES**

In this section, we construct weighted threshold secret sharing schemes from higher degree rational points on algebraic curves. The constructed secret sharing schemes are not ideal in general. Let $X$ be an absolutely irreducible, projective and smooth curve defined over $GF(q)$ with genus $g = D = \{P_1, \ldots, P_n\}$, where $P_i$ is a $GF(q^i)$-rational point on $X$ (in other words, $\deg(P_i) = t_i$, that is, there exist $t_i$ conjugate $GF(q^i)$-rational points $P_i, \delta(P_i), \ldots, \delta^{t_i-1}(P_i)$ on $X$, where $\delta$ is the Frobenius automorphism of $X$). We assume that $t_0 = 1$ and for any two distinct $i < j \in [1, \ldots, n]$ there exists no positive integer $s$ such that $\delta^s(P_i) = P_j$. Let $G$ be a $GF(q)$-rational
divisor of degree $m$ satisfying $\supp(G) \cap D = \emptyset$. We further assume $2g = 2 < \deg(G) < \sum_i \deg(P_i)$.

The secret sharing scheme (over $GF(q)$) is constructed as follows. For any secret value $s \in GF(q)$, we take a function $f \in L(G)$ randomly such that $f(P_0) = s$. For any player $P_i$, we have $t_i$ conjugate points $P_i, \delta_i(P_i), \ldots, \delta_i^{t_i-1}(P_i)$ of $P_i$ on $X$. We take a normal basis $\alpha_0 = \beta, \alpha_1 = \beta^2, \ldots, \alpha_{t_i-1} = \beta^{t_i-1}$ of the field $GF(q^{t_i})$ over $GF(p)$. If $f(P_i) = a_0 \alpha_0 + \cdots + a_{t_i-1} \alpha_{t_i-1}$, then the coordinate vector of $f(\delta_i^{j}(P_i))$ with respect to the basis $\alpha_0, \ldots, \alpha_{t_i-1}$, is just a cyclic shift of $(a_0, \ldots, a_{t_i-1})$. The share of this player $P_i$ is the vector $(a_0, \ldots, a_{t_i-1})$, and the weight assigned to the player $P_i$ is $w(P_i) = \deg(P_i)$. From the following result this is a weighted ramp secret sharing scheme over $GF(q)$ with information rate $1/\max\{w(P_i), \ldots, w(P_n)\}$.

**Theorem 2:** Let $w(P_i) = \deg(P_i) = t_i$. The secret sharing scheme over $GF(q)$ as above has the following properties.
1. Any subset $\mathbf{A}$ of $\{P_1, \ldots, P_n\}$ satisfying $\sum_{i \in \mathbf{A}} \deg(P_i) \leq \deg(G) - 2q$ is not qualified.
2. Any subset $\mathbf{A}$ of $\{P_1, \ldots, P_n\}$ satisfying $\sum_{i \in \mathbf{A}} \deg(P_i) \geq \deg(G) + 1$ is qualified.

**Proof:** Similar to Proposition 1 of [7], a subset $\mathbf{A}$ of $\{P_1, \ldots, P_n\}$ is not in the access structure if and only if $L(G - P_{\mathbf{A}} - \sum_{i \in \mathbf{A}} \alpha_i P_i)$ is a proper subspace of $L(G - \sum_{i \in \mathbf{A}} \alpha_i P_i)$. The statements 1) and 2) follow directly.

Suppose there are $n_i$ degree $t_i$, $GF(q^{t_i})$-rational points in the set $D$ of players where $i = 1, \ldots, n$, then a subset with $m_1$ players of weight $t_1, \ldots, m_n$ players of weight $t_n$, is qualified if $t_1 m_1 + \cdots + t_n m_n \geq \deg(G) + 1$. If $gcd(t_1, \ldots, t_n) > 1$ then the larger gap value 2g in Theorem 2, we have a weighted threshold secret sharing scheme with the threshold value $T = \deg(G) + 1$. In the case of elliptic secret sharing schemes, the gap is 2, so we can construct weighted threshold secret sharing schemes from elliptic curves by choosing suitable $t_1, \ldots, t_n$ easily.

**Example 2:** Let $E$ be the super-singular elliptic curve $y^2 + y = x^3$ defined over $GF(2)$. We take $t_0 = 1, t_1 = p_1, t_2 = p_2, \ldots$ where $p_1, q_1, q_2$ are distinct odd prime numbers satisfying $p < q_1 < q_2$. There are exactly $2^{p_1-1} - 1 + 2^{q_1} + 2$ degree $p_1$ rational points on $E$ and $2^{p_1} = 2^{q_1} + 2 + 2^{q_2} + 2$ degree $p_2$ points on $E$. In fact, for any odd $r$, there are $2^{p_1} + 1$ $GF(2)$-rational points of $E$, among which $(0, 0, 0)$ and the point at infinity $O$ are rational over $GF(2)$. Let $G = mO$ be a $GF(2)$-rational divisor on $E$, and $D$ be the set $\{P_0, P_1, \ldots, P_{N_1}, Q_1, \ldots, Q_{N_2}\}$ where $P_0$ is a nonzero $GF(2)$-rational point on $E$, $N_1 = (2^{p_1-1} - 2^{q_1} + 2)/(p_1q_2)$, $N_2 = (2^{p_1-1} - 2^{q_1} + 2)/(p_1q_2)$, $P_1, \ldots, P_{N_1}$ are $N_1$ nonconjugate rational points of degree $p_1$ on $E$ and $Q_1, \ldots, Q_{N_2}$ are $N_2$ nonconjugate rational points of degree $p_2$ on $E$. Thus, we have the following result.

**Corollary 2:** Let $p < q_1 < q_2$ be distinct odd primes. We have a two-weight weighted threshold secret sharing scheme of information rate $1/(p_2q_2)$ among $(2^{p_1} - 2^{q_1} + 2)/(p_1q_2)$ players. There are $(2^{p_1} - 2^{q_1} + 2)/(p_1q_2)$ players (called Class I) with weight $p_1$, and $(2^{p_1} - 2^{q_1} + 2)/(p_1q_2)$ players (called Class II) with weight $p_2$. A subset with $x$ Class I players and $y$ Class II players is qualified if and only if $pq_1x + p_2q_2y \geq m + 1$.

**IV. CONCLUSION**

In this correspondence, we have determined the explicit access structures of the ideal linear secret sharing schemes based on AG codes associated with elliptic curves. Weighted threshold secret sharing schemes based on higher degree rational points on elliptic curves were constructed. This demonstrates that elliptic curves form an important resource in the theory of secret sharing.

**ACKNOWLEDGMENT**

The authors would like to thank the anonymous referees for helpful comments that helped improve the organization and exposition of this correspondence.

**REFERENCES**