On the Access Structures of Hyperelliptic Secret Sharing Schemes

Lei Li and Siman Yang

Abstract. In this paper we partially determine the access structures of algebraic-geometric secret sharing schemes from one point algebraic-geometric codes associated with a hyperelliptic curve of any genus. Our result includes the access structures of elliptic secret sharing schemes as a special case.

1. Introduction

Secret sharing, which was independently invented by Shamir [**Sh**] and Blakley [**B**], is an important cryptographic primitive. A secret sharing scheme is a method to distribute a secret value among a group of participants in such a way that only the qualified subsets of participants can recover the secret with their shares. The family of the qualified subsets is the access structure of the scheme. One of the main open problems in secret sharing is the characterization of the access structures of ideal secret sharing schemes. Messey first used error-correcting codes to construct linear secret sharing schemes [**M1**][**M2**]. Chen and Cramer [**CC**] proposed secret sharing schemes based on algebraic-geometric codes as a natural generalization of Shamir's scheme. However, their schemes are so called ramp schemes in the sense that any subset with fewer than t_1 players is not in the access structure and any subset with at least t_2 players is in the access structure. The number $t_2 - t_1$ called the threshold gap, is known to be at most $2g$, where g is the genus of the underlying curve, for an algebraic-geometric sharing scheme. Generally speaking, whether a subset of t elements with $t_1 \leq t < t_2$ is a qualified set or not is unknown. The access structures of elliptic sharing schemes were recently completely determined in [**CLX**].

In this paper, we extend the method of [**CLX**] and partially determine the access structures of the algebraic-geometric secret sharing schemes from one point algebraic-geometric codes associated with a hyperelliptic curve of any genus by employing a property of the reduced divisor on the Jacobian of a hyperelliptic curve. Our result includes the access structures of elliptic secret sharing schemes as a special case.

1991 *Mathematics Subject Classification.* Primary 94A62; Secondary 11G20.

Key words and phrases. secret sharing, access structure, algebraic-geometric code, hyperelliptic curve.

The research of the second author was supported in part by the National Natural Science Foundation of China Grant #10801050.

2. Preliminaries

Let $\mathbb{F}_q$ be a finite field of q elements and $\mathbf{C}$ be a linear $[n+1, k, d]$ code over $\mathbb{F}_q$ with code length $n+1$, dimension k and minimum Hamming distance d. Let G be a generator matrix of $\mathbf{C}$ such that no column of G is a zero vector. Suppose a dealer P_0 shares a secret $s \in \mathbb{F}_q$ among players $\mathbf{P} = \{P_1,\ P_2, \ldots,\ P_n\}$ in the following way: Choose a $\mathbf{u} \in \mathbb{F}_q^k$ randomly such that $s =< \mathbf{u}, \mathbf{g}_0 >$, where $< *, * >$ is the usual inner product of vectors and $\mathbf{g}_0$ is the 0th column of G. The dealer calculates the codeword $\mathbf{c} = \mathbf{u}G = (c_0, c_1, \ldots, c_n)$ with $c_0 = s$ and gives the player P_i the value c_i as his share. From a lemma in [**M1**] and [**M2**], $\{P_{i_1},\ P_{i_2}, \ldots,\ P_{i_t}\}$ is a qualified subset if and only if there is a codeword $\mathbf{v} = (1, 0, \ldots, v_{i_1}, \ldots, v_{i_t}, \ldots, 0) \in \mathbf{C}^{\perp}$ where $\mathbf{C}^{\perp}$ is the dual code of $\mathbf{C}$.

Let X be an algebraic curve defined over $\mathbb{F}_q$ of genus g, $\mathbf{D} = \{P_0,\ P_1, \ldots,\ P_n\}$ be a subset of $X(\mathbb{F}_q)$, and G be an $\mathbb{F}_q$-rational divisor of X with $\mathrm{supp}(G) \cap \mathbf{D} = \emptyset$. The functional algebraic-geometric code $C_L(D, G) \subseteq \mathbb{F}_q^{n+1}$ is defined as the evaluations of $L(G)$ at the points in the set $\mathbf{D}$, where $L(G)$ is the linear space of all rational functions with divisor not smaller than $-G$, i.e., $L(G) = \{f : (f) + G \geq 0\} \bigcup \{0\}$. The residual algebraic-geometric code $C_\Omega(D, G) \subseteq \mathbb{F}_q^{n+1}$ is defined as the evaluations of $\Omega(G)$ at the points in the set D, where $\Omega(G)$ is the linear space of all differentials with divisor not smaller than G, i.e., $\Omega(G) = \{\omega : (\omega) \geq G\}$. It is well known that $C_L(D, G)$ and $C_\Omega(D, G)$ are dual codes. For more details, readers may consult [**St**] and [**TV**].

A genus g hyperelliptic curve defined over $\mathbb{F}_q$ with one point at infinity (denoted by O) is a curve with an affine model $X :\ y^2 + h(x)y = f(x)$, where $h(x), f(x) \in \mathbb{F}_q[x]$, $f(x)$ is a monic polynomial of degree $2g + 1$ and $h(x)$ is a polynomial of degree at most g. It is assumed that there is no singular point on $X(\overline{\mathbb{F}}_q)$, i.e., there is no solution $(x, y) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ which simultaneously satisfy $y^2 + h(x)y = f(x)$, $2y + h(x) = 0$ and $h'(x)y - f'(x) = 0$. The canonical involution of X is defined by $P = (x, y) \mapsto \tilde{P} = (x, -y - h(x))$. If $P = O$ then define $\tilde{P} = O$. A reduced divisor is of the form $D = \sum m_i P_i$ such that $m_i \geq 0$, $\sum m_i \leq g$, and P_i's are finite points such that when $P_i \in supp(D)$ then $\tilde{P}_i \notin supp(D)$, unless $P_i = \tilde{P}_i$, in which case $m_i = 1$. In hyperelliptic setting, a reduced divisor can be expressed in Mumford representation. Using *Cantor's algorithm* [**C**], two reduced divisors can be added efficiently [**MWZ**]. Note that there is not a group law on the points of a hyperelliptic curve; instead we use the divisor class group of the curve, called Jacobian. The Jacobian of X is defined by $\mathbb{J}_X = \mathbb{D}_X^0/\mathbb{P}_X$, where $\mathbb{D}_X^0$ (resp. $\mathbb{P}_X$) denotes the group of degree 0 divisors (resp. principal divisors). Its $\mathbb{F}_q$-rational part is denoted by $\mathbb{J}_X(\mathbb{F}_q)$. If two divisors D_1 and D_2 are linearly equivalent then write $D_1 \sim D_2$. Let $P_0 = (x_0, y_0) \in X(\overline{\mathbb{F}}_q)$ and $u(x) = (x - x_0)$ is a function on X, then $\mathrm{div}(u(x)) = P_0 + \tilde{P}_0 - 2O$ (cf [**G**]), i.e., $P_0 - O \sim -(\tilde{P}_0 - O)$. Each element of the jacobian has a unique representative of the form $D - nO$, where D is reduced.

3. The Access Structures of Hyperelliptic Secret Sharing Scheme

In this section we will give an characterization to determine explicitly whether a set of shares with size in $[n - \deg(G), n - \deg(G) + g]$ is qualified for the secret sharing schemes from the algebraic-geometric codes $C = C_\Omega(D, G)$ associated with a genus g hyperelliptic curve.

THEOREM 3.1. *Let X be a hyperelliptic curve over $\mathbb{F}_q$ of genus g. Let $\boldsymbol{D} = \{P_0,\ P_1, \ldots,\ P_n\}$ be any given subset of finite elements of $X(\mathbb{F}_q)$ and let $G = mO$. Consider the hyperelliptic secret sharing scheme obtained from X with the set of players $\boldsymbol{P} = \{P_1,\ P_2, \ldots,\ P_n\}$.*

Let $\boldsymbol{A} = \{P_{i_1}, P_{i_2}, \ldots, P_{i_t}\}$ be a subset of $\boldsymbol{P}$ with t elements. Let the group sum of $\tilde{P}_{i_1} - O$, $\tilde{P}_{i_2} - O$, $\cdots$, $\tilde{P}_{i_t} - O$ in $\mathbb{J}_X(\mathbb{F}_q)$ is a reduced divisor $B - kO$ with $B = Q_1 + Q_2 + \cdots + Q_k$ (where the same point can appear more than once and $k \leq g$). Let $\boldsymbol{A}^c := \boldsymbol{P} \setminus \boldsymbol{A}$ and Γ is the access structure of the secret sharing scheme from $\boldsymbol{C} = C_\Omega(D, G)$ associated with X, then we have the following:

1) If $\#\boldsymbol{A}^c \leq n - m - 1$ (i.e. $t \geq m + 1$), then $\boldsymbol{A}^c \notin \Gamma$;

2) If $\#\boldsymbol{A}^c \geq n - m + 2g$ (i.e. $t \leq m - 2g$), then $\boldsymbol{A}^c \in \Gamma$;

3) When $n - m \leq \#\boldsymbol{A}^c \leq n - m + g$ (i.e. $m - g \leq t \leq m$), if $\boldsymbol{A}^c$ is a minimal[1] *qualified subset, then $supp(B) \cap \boldsymbol{D} \subset \boldsymbol{A}$ and $deg(B) \leq m - t$ (i.e. $k \leq m - t$), and conversely, if $supp(B) \cap \boldsymbol{D} \subset \boldsymbol{A}$ and $deg(B) \leq m - t$, then $\boldsymbol{A}^c$ is a qualified subset.*

PROOF. The divisor B can be calculated by *Cantor's algorithm*. The first and second part follow from the general result on the algebraic geometric secret sharing scheme. For completeness the details are given below.

1) Assume $\mathbf{A}^c$ is a qualified subset, that is equal to say there is a codeword $(1,\ v_1,\ v_2, \ldots, v_n) \in C_L(D, G)$ with $v_{i_1} = v_{i_2} = \cdots = v_{i_t} = 0$. Then there exists $f \in L(G),\ s.t.,\ f(P_0) \neq 0,\ f(P_{i_1}) = \cdots = f(P_{i_t}) = 0$. As G is of degree $m < t$, it is impossible for a function of $L(G)$ to have more than m zeros.

2) If $\#\mathbf{A}^c \geq n - m + 2g$, then $\deg(G - \mathbf{A}) \geq 2g$. By the Riemann-Roch theorem, $L(G - \mathbf{A} - P_0) \neq L(G - \mathbf{A})$ (here we identify the set $\mathbf{A}$ with the divisor $P_{i_1} + P_{i_2} + \cdots + P_{i_t}$). Hence there exists a function $f \in L(G - \mathbf{A}) \setminus L(G - \mathbf{A} - P_0)$ which corresponds to a codeword $(1,\ v_1,\ v_2, \ldots, v_n) \in C_L(D, G)$ with $v_{i_1} = v_{i_2} = \cdots = v_{i_t} = 0$. This proves 2).

3) Suppose $m - g \leq t \leq m$. If $\mathbf{A}^c$ is a minimal qualified subset of $\mathbf{P}$, there is a function $f \in L(G)$ such that $f(P_{i_1}) = \cdots = f(P_{i_t}) = 0$ and $f(P) \neq 0$ for $P \in \mathbf{P} \setminus \mathbf{A}$. Suppose that $\mathrm{div}(f) = P_{i_1} + \cdots + P_{i_t} + Q'_1 + \cdots + Q'_{k'} - (t + k')O$, where $Q'_j \notin \mathbf{P} \setminus \mathbf{A}$ and $k' \leq m - t \leq g$. Thus we have: $Q'_1 + \cdots + Q'_{k'} \sim -P_{i_1} - \cdots - P_{i_t} + (t + k')O$ and $Q_1 + \cdots + Q_k \sim \tilde{P}_{i_1} + \tilde{P}_{i_2} + \cdots + \tilde{P}_{i_t} - (t - k)O$, which imply that $Q_1 + \cdots + Q_k - kO \sim Q'_1 + \cdots + Q'_{k'} - k'O$.

If $Q'_i \neq \tilde{Q'}_j$ for any $1 \leq i, j \leq k'$, then $B = Q'_1 + \cdots + Q'_{k'}$ due to the uniqueness of the reduced form. Clearly, we have $supp(B) \cap \mathbf{D} \subset \mathbf{A}$ and $\deg(B) \leq k' \leq m - t$ as $Q'_j \notin \mathbf{P} \setminus \mathbf{A}$. Otherwise we may assume there exists $Q'_i = \tilde{Q'}_j$ for some $1 \leq i, j \leq k'$, then B is linearly equivalent to $Q'_1 + \cdots + Q'_{k'} - Q'_i - Q'_j + 2O$. Continue this process till we reach the reduced form of B with support included in $\{Q'_1, \cdots, Q'_{k'}\}$. Again, we have $supp(B) \cap \mathbf{D} \subset \mathbf{A}$ and $\deg(B) \leq k' \leq m - t$.

Conversely, assume $\mathrm{supp}(B) \cap \mathbf{D} \subset \mathbf{A}$ and $\deg(B) \leq m - t$. As the divisor $P_{i_1} + P_{i_2} + \cdots + P_{i_t} + Q_1 + Q_2 + \cdots + Q_k$ is linearly equivalent to $(t + k)O$, there exists a function $f \in L((t + k)O) \subset L(G)$ with $\mathrm{div}(f) = P_{i_1} + P_{i_2} + \cdots + P_{i_t} + Q_1 + Q_2 + \cdots + Q_k - (t + k)O$ and $f(P_0) \neq 0$. This implies that there exists a codeword $(1, v_1, \ldots, v_n) \in C_L(D, G)$ with $v_{i_1} = \cdots = v_{i_t} = 0$. Hence $\mathbf{A}^c$ is a qualified subset. □

[1] A qualified set is said to be minimal if none of its proper subsets is qualified.

REMARK 3.2. The characterization of hyperelliptic sharing scheme is not complete as it is still unclear for the sets of shares with size in $[n-m+g+1, n-m+2g-1$. The underlying reason lies in that uniqueness of reduced divisors does not extend to semi-reduced divisors of degree at most $2g$ in the setting of hyperelliptic curves. It looks like a complete characterization of hyperelliptic sharing scheme is not practical and helpful.

REMARK 3.3. From the main theorem whether a subset $\mathbf{A}$ is a qualified set can be determined unless $n - m + g + 1 \leq \#\mathbf{A}^c \leq n - m + 2g - 1$. Thus the access structure of an elliptic secret sharing scheme ($g = 1$ hyperelliptic curve) is completely determined. Therefore we re-discovered the result in [**CLX**].

We illustrate the theorem by completely determine the access structure of the following hyperelliptic sharing scheme.

EXAMPLE 3.4. Let X be the hyperelliptic curve $y^2 + y = x^5 + x^3 + x$ of genus 2 defined over $\mathbb{F}_5$, which has six rational points $P_0 = (0, 0)$, $P_1 = (0, 4)$, $P_2 = (2, 1)$, $P_3 = (2, 3)$, $P_4 = (4, 1)$, $P_5 = (4, 3)$ and an infinite point O. Let $\mathbf{D} = \{P_0, P_1, \ldots, P_5\}$, $\mathbf{P} = \{P_1, \ldots, P_5\}$, $G = 3O$. Consider the hyperelliptic secret sharing scheme obtained from $C_\Omega(D, G)$.

1) In the case where $\mathbf{A}$ has at least four elements (i.e., $\mathbf{A}^c$ has at most one element), then $\mathbf{A}^c$ is not a qualified subset from 1).

2) In the case where $\mathbf{A}$ has three elements (i.e., $\mathbf{A}^c$ has two elements), $\mathbf{A}^c$ is a minimal qualified subset if and only if B is the zero element from 3). Direct calculation gives the minimal qualified subsets of two elements are: $\{P_2, P_3\}$, $\{P_4, P_5\}$.

3) In the case where $\mathbf{A}$ has two elements (i.e., $\mathbf{A}^c$ has there elements), direct calculation shows that candidates satisfying $\mathrm{supp}(B) \cap \mathbf{D} \subset \mathbf{A}$ and $\deg(B) \leq 1$ are: $\mathbf{A}^c = \{P_2, P_3, P_4\}$, $\{P_2, P_3, P_5\}$, $\{P_2, P_4, P_5\}$ or $\{P_3, P_4, P_5\}$, we have $\mathrm{supp}(B) \cap \mathbf{D} \subset \mathbf{A}$ and $\deg(B) \leq 1$. From 2), all of them are qualified subsets, but not minimal qualified subsets.

4) In the case where $\mathbf{A}$ has one element (i.e., $\mathbf{A}^c$ has four elements), the only subset satisfying $\mathrm{supp}(B) \cap \mathbf{D} \subset \mathbf{A}$ and $\deg(B) \leq 2$ is $\mathbf{A}^c = \{P_2, P_3, P_4, P_5\}$, which is not a minimal qualified subset.

Combining the above results, the access structure of the secret sharing scheme is $\{\{P_2, P_3\}, \{P_4, P_5\}\}$.

4. Conclusion

In this paper, we partially determined the access structure of the secret sharing schemes from algebraic-geometric codes associated with a hyperelliptic curve of arbitrary genus. Our result includes the elliptic secret sharing schemes [**CLX**] as a special case.

References

[B] G. R. Blakley, *Safeguarding cryptographic keys*, In Proc. NCC AFIPS, 1979, pp. 313–317.

[C] D. G. Cantor, *Computing in the jacobian of a hyperelliptic curve*, Math. Comp. 48, 1987, pp. 95–101.

[CC] H. Chen, R. Cramer, *Algebraic geometric secret sharing schemes and secure multi-party computation over small fields*, In: Advances in Cryptology, CRYPTO 2006, pp. 521–536.

[CLX] H. Chen, S. Ling, C. P. Xing, *Access structures of elliptic secret sharing schemes*, IEEE Trans. Inf. Theory, vol. 54, no. 2, 2008, pp. 850–852.

[G] S. D. Galbraith, *Mathematics of Public Key Cryptography*, Available at http://www.isg.rhul.ac.uk/ s̃dg/crypto-book/.

[M1] J. L. Massey, *Minimal codewords and secret sharing*, In Proc. 6th Joint Swedish-Russian Worksh. Inf. Theory, 1993, pp.269–279.

[M2] J. L. Massey, *Some applications of coding theory in cryptography*, In Codes and Ciphers: Crytography and Coding IV, 1995, pp. 33–47.

[MWZ] A. Menezes, Y.-H. Wu, R. Zuccherato, *An elementary introduction to hyperelliptic curves*, In: *Algebraic aspects of cryptography*, by N. Koblitz, Springer-Verlag, 1997, pp. 155–178.

[Sh] A. Shamir, *How to share a secret*, Commun. ACM, vol. 22, 1979, pp. 612–613.

[St] H. Stichtenoth, *Algebraic Function Fields and Codes*, Berlin, Germany: Springer, 1993.

[TV] M. A. Tsfasman, S. G. Vladut, *Algebraic-Geometric Codes*, Dordrecht, Germany: Kluwer, 1999.

Department of Mathematics, East China Normal University, Shanghai 200241, P.R.China
E-mail address: lileiat163@163.com

Department of Mathematics, East China Normal University, Shanghai 200241, P.R.China
E-mail address: smyang@math.ecnu.edu.cn