Algebraic Geometric Secret Sharing Schemes over Large Fields Are Asymptotically Threshold

Fan Peng, Hao Chen and Chang-An Zhao

Abstract

In Chen-Cramer Crypto 2006 paper [7] algebraic geometric secret sharing schemes were proposed such that the "Fundamental Theorem in Information-Theoretically Secure Multiparty Computation" by Ben-Or, Goldwasser and Wigderson [3] and Chaum, Crépeau and Damgård [6] can be established over constant-size base finite fields. These algebraic geometric secret sharing schemes defined by a curve of genus g over a constant size finite field $\mathbf{F}_q$ is quasi-threshold in the following sense, any subset of $u \leq T-1$ players (non qualified) has no information of the secret and any subset of $u \geq T+2g$ players (qualified) can reconstruct the secret. It is natural to ask that how far from the threshold these quasi-threshold secret sharing schemes are? How many subsets of $u \in [T, T+2g-1]$ players can recover the secret or have no information of the secret?

In this paper it is proved that almost all subsets of $u \in [T, T+g-1]$ players have no information of the secret and almost all subsets of $u \in [T+g, T+2g-1]$ players can reconstruct the secret when the size q goes to the infinity and the genus satisfies $\lim \frac{g}{\sqrt{q}} = 0$. Then algebraic geometric secret sharing schemes over large finite fields are asymptotically threshold in this case. We also analyze the case when the size q of the base field is fixed and the genus goes to the infinity.

Index Terms

Algebraic geometric secret sharing, Quasi-threshold, Threshold, Algebraic-Geometry codes.

F. Peng is with College of Mathematics and Statistics, Guangxi Normal University, Guilin, China. (E-mail: pengfan@gxnu.edu.cn.

H. Chen is with College of Information Science and Technology/College of Cyber Security, Jinan University, Guangzhou, Guangdong Province, 510632, China. E-mail: haochen@jnu.edu.cn

C.-A, Zhao is with School of Mathematics, Sun Yat-sen University, Guangzhou 510275, P.R.China and with Guangdong Key Laboratory of Information Security, Guangzhou 510006, P.R. China. (E-mail: zhaochan3@mail.sysu.edu.cn)

I. Introduction

A. Linear secret sharing schemes (LSSS) and applications

Let K be a finite field. A K-linear secret sharing scheme (LSSS)$\{K, V_1, ..., V_m, u\}$ on a set of participants $\mathcal{P} = \{P_1, ..., P_m\}$ is defined as a sequence of subspaces $\{V_1, ..., V_m\}$ of K^e, where $V_i \subset K^e$ and u is a given vector in K^e. A subset A of $\mathcal{P}$ is qualified if u is in the subspace of K^e spanned by the $\{V_i\}_{i \in A}$. For any secret value $s \in K$, choose a random linear mapping $\phi : K^e \to K$ such that $\phi(u) = x$, $\{\phi(e_1^i), ..., \phi(e_{dimV_i}^i)\}$ is the share of the participant P_i, where $e_1^i, ..., e_{dimV_i}^i$ is a base of $V_i \subset K^e$. Only the qualified subsets of $\mathcal{P}$ can reconstruct the secret from their shares. The access structure, $\Gamma \subset 2^{\mathcal{P}}$, of a secret-sharing scheme is the family of all qualified subsets of $\mathcal{P}$. The adversary structure Γ^c is the family consisting of all subsets of $\mathcal{P}$ not in Γ. The minimum access structure $\min \Gamma \subset 2^{\mathcal{P}}$ is defined to be the set of all minimum elements in Γ (here we use the natural order relation $S_1 < S_2$ if and only if $S_1 \subset S_2$ on $2^{\mathcal{P}}$). We call a secret-sharing scheme a (k, m)-threshold scheme if the access structure consists of all the subsets of $\mathcal{P}$ with k or more elements, where the cardinality of $\mathcal{P}$ is m. The first secrets-sharing scheme was proposed independently by Shamir [32] and Blakley [2] in 1979, and is in fact a threshold secret-sharing scheme. The existence of secret-sharing schemes with arbitrary given access structures was proved in [1]. The complexity of the K-LSSS is defined to be $\lambda(\Gamma) = \Sigma_{i=1}^m \dim_K(V_i)$. When the complexity is m, the LSSS is called ideal. One of the main open problems in secrete sharing is the characterization of the access structures of ideal secret sharing schemes [4].

Let $\{K, V_1, ..., V_m, u\}$ be an LSSS over K, denote $v = u \otimes u \in K^{e^2}$ and $V_i' = V_i \otimes V_i \in K^{e^2}$ for $i = 1, ..., m$. This LSSS is said to have multiplicative property if v is in the linear subspace of K^{e^2} spanned by all $\{V_i'\}_{i=1,...,m}$. This is equivalent to the following fact : for any given two secrets x (with shares $c_i \in K^{dimV_i}$ for $i = 1, ...m$) and y(with shares $d_i \in K^{dimV_i}$ for $i = 1, ..., m$), the product xy is in the linear span with coefficients in K of $c_i d_i$ (here the product can be understood as a bilinear mapping $K^{dimV_i} \otimes K^{dimV_i} \to K^{dimV_i}$). It is said to have strongly multiplicative property if the v is in the linear subspace spanned by $\{V_i'\}_{i \in \mathbf{P} - B}$ where B is any subset of $\mathcal{P}$ in the adversary structure.

For an adversary structure Γ^c on $\mathcal{P}$, it is said that Γ^c is Q_2 if $A \bigcup B \neq \mathcal{P}$ for any $A, B \in \Gamma^c$, and Γ^c is Q_3 if $A \bigcup B \bigcup C \neq \mathcal{P}$ for any $A, B, C \in \Gamma^c$. One of the key results in [10] is a method to construct, from any LSSS with a Q_2 access structure Γ, a multiplicative LSSS Γ' with the same access structure and double complexity, that is $\lambda(\Gamma') \leq 2\lambda(\Gamma)$ can be constructed. K-MLSSSs with Q_2 and Q_3 access structures are closely related to secure multi-party computation. It is known that any strongly multiplicative LSSS can be efficiently transformed into a polynomial complexity error-free multi-party computation protocol computing any arithmetic circuit. This protocol is information-theoretically secure against the adaptive and active Γ^c adversary. For details of secure multi-party computation and its relation with linear secret sharing schemes, the reader is referred to [10], [11].

The approach of secret sharing based on error-correcting codes was studied in [8], [26]–[28]. It is a special form of the above LSSS. Actually it was realized that Shamir's (k, n)-threshold scheme is just the secret sharing scheme based on the famous Reed-Solomon code in 1979 paper [28].

We recall the construction of LSSS from error-correcting codes in [8]. Let C be a q-ary $[n+1, k, d]$-code, let $G = (\mathrm{g}_0, \mathrm{g}_1, \cdots, \mathrm{g}_n)$ be a generator matrix for C. We give a construction for a secret sharing scheme for $\mathcal{P} = \{P_1, \cdots, P_n\}$ as follows:

(1) Let the generator matrix G be publicly known to everyone in the system.

(2) To share a secret $s \in \mathbb{F}_q$, the dealer randomly selects a vector

$$\mathrm{r} = (r_1, r_2, \cdots, r_k) \in \mathbb{F}_q^k$$

such that $s = \mathrm{r} \cdot \mathrm{g}_0$.

(3) Each participant P_i receives a share $s_i = \mathrm{r} \cdot \mathrm{g}_i$, for $i = 1, \cdots, n$.

We have the codeword $\mathrm{c} = (s, s_1, \cdots, s_n) = \mathrm{r}G$. This is an ideal perfect secret sharing scheme. We refer to [26], [27] and [28] for the following Lemma.

Lemma 1: Let C be a linear code of length $(n+1)$ with generator matrix G. Suppose the dual of C, i.e., $\mathrm{C}^{\perp} = \{\mathrm{v} = (v_0, v_1, \cdots, v_n) | G\mathrm{v}^T = 0\}$, 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, $\{P_{i_1}, \cdots, P_{i_m}\}$ can reconstruct the secret if and only if there is a codeword $\mathrm{v} = (1, 0, \cdots, v_{i_1}, \cdots, v_{i_m}, \cdots, 0) \in \mathrm{C}^{\perp}$, i.e., the support of the codeword $\mathrm{supp(v)} \subseteq \{0, i_1, \cdots, i_m\}$.

B. Algebraic geometric secret sharing schemes over a constant-size field

Secret sharing schemes proposed in [7] can be thought as a natural generalization of Shamir's scheme by applying algebraic-geometric codes in the above construction. In Shamir's scheme the number of players has to be upper bounded by the size of the base field. In algebraic geometric secret sharing schemes this restriction can be removed with quasi-threshold access structures instead of threshold access structures . These LSSS from algebraic curves are quasi-threshold in the following sense, any subset of $u \leq T-1$ players (non qualified) has no information of the secret and any subset of $u \geq T+2g$ players (qualified) can reconstruct the secret, where g is the genus of the curve on which the secret sharing is defined. Algebraic geometric secret sharing schemes have a remarkable application in the "Fundamental Theorem in Information-Theoretically Secure Multiparty Computation" by Ben-Or, Goldwasser and Wigderson [3] and Chaum, Crépeau and Damgård [6]. The communication complexity in the above fundamental protocols is saved with a $\log(n)$ factor and the information-theoretically secure multiparty computation can be established over a constant-size field $\mathbb{F}_q$ with a decreasing corruption tolerance by a small $\frac{1}{\sqrt{q}-1}$-fraction (see [11], [12]). The asymptotical result in [7] plays a central role in [19] about communication-efficient zero knowledge for circuit satisfiability, two-party computation [13], [14], [21], OT combiners [17] and correlation extractors [20]. We refer to [11] page 342 for its impact in secure multiparty computation and other fields of cryptography.

Let $\mathbb{F}_q$ be a given finite field with q elements, C be a smooth projective absolutely irreducible curve defined over $\mathbb{F}_q$ with the genus g, and $C(\mathbb{F}_q)$ be the set of $(\mathbb{F}_q)$ rational points of C. $\{Q, P_0, P_1, \cdots, P_n\}$ is a subset of $C(\mathbb{F}_q)$, and $G = mQ$. D is the divisor $P_0 + P_1 + \cdots + P_n$. Let $L(G) = \{f \in \mathcal{M}_C \big| \mathrm{div}(f) + G \geq 0\}$ with dimension denoted by $l(G)$, and let $\Omega(G-D) = \{\omega \in \Omega_C \big| \mathrm{div}(\omega) \geq G - D\}$ with dimension denoted by $i(G-D)$.

We can define algebraic geometry codes

$$C_L(D,G) = \{(f(P_0), f(P_1), \cdots, f(P_n)) \big| f \in L(G)\},$$

and

$$C_\Omega(D,G) = \{(\mathrm{res}_{P_0}(\omega), \mathrm{res}_{P_1}, (\omega) \cdots, \mathrm{res}_{P_n}(\omega)) \big| \omega \in \Omega(G-D)\}.$$

Assume $2g-2 < \deg G = m < n+1$, then $l(G) = m-g+1$ and $i(G-D) = n-m+g$ by the Riemann-Roch theorem. The first one is a linear $[n+1,k,d]$ code, and the second one is the dual $[n+1, n+1-k, d^\perp]$ code, where $k = m-g+1, d \geq n+1-m$, and $d^\perp \geq m-2g+2$.

Applying Massey's construction as follows.

(1) To share a secrete $s \in \mathbb{F}_q$, the dealer randomly select an element $\omega \in \Omega(G-D)$ such that $\mathrm{res}_{P_0}(\omega) = s$.

(2) The share of the participant is $s_i = \text{res}_{P_i}(\omega) \in \mathbb{F}_q$, for $1 \le i \le n$.

Note that, in (1) of the construction above, due to Riemann-Roch theorem, we have $i(G-D)-i(G-D+P_0) = 1$. Thus there exists a non-zero rational differential $\omega \in \Omega(G-D)\backslash\Omega(G-D+P_0)$ such that $\text{res}_{P_0}(\omega) = s$. Then we have a codeword $(s, s_1, \cdots, s_n) \in C_\Omega(D, G)$. Let $\mathcal{A} = \{P_{i_1}, \cdots, P_{i_t}\} \subset \mathcal{P}$ and $P_\mathcal{A} = \sum_{P\in\mathcal{A}} P$, then the complement $\mathcal{A}^c = \mathcal{P} \setminus \mathcal{A}$ is qualified if and only if there exists a rational function $f \in L(G)$ such that $f(P_0) \neq 0$, and $f(P) = 0$, for $P \in \mathcal{A}$, i.e. $f \in L(G - P_\mathcal{A})$ with $f(P_0) \neq 0$. So we have following three cases.

(1) When $t \le m - 2g$, since $\deg(G - P_\mathcal{A}) \ge 2g$, so the linear system $L(G - P_\mathcal{A})$ is base point free [18]. Then there is a function f with the above property, thus $\mathcal{A}^c$ is qualified.

(2) When $t > m$, since $\deg(G - P_\mathcal{A}) < 0$, so $L(G - P_\mathcal{A}) = \emptyset$, thus $\mathcal{A}^c$ is unqualified.

(3) When $m - 2g < t \le m$, it's hard to determine $\mathcal{A}^c$ is qualified or unqualified.

In [9] access structures of LSSS from elliptic curves were completely determined.

Theorem 1 (Chen, Lin, Xing): Let E be an elliptic curve over $\mathbb{F}_q$, and let $\{P_0, \cdots, P_n\}$ be a subset of $E(\mathbb{F}_q)$ of $n + 1$ nonzero elements. Let $D = P_0 + \cdots + P_n$ and $G = mO$. Consider the elliptic secret sharing scheme obtained from E with the set of players $\mathcal{P} = \{P_1, \cdots, P_n\}$.

Let $\mathcal{A} = \{P_{i_1}, \cdots, P_{i_t}\}$ be a subset of $\mathcal{P}$ with t elements, and let B be the element in $E(\mathbb{F}_q)$ such that the group sum of B and $\{P_{i_1}, \cdots, P_{i_t}\}$ in $E(\mathbb{F}_q)$ is O. If $\mathcal{A}^c \overset{\text{def}}{=} \mathcal{P} \setminus \mathcal{A}$ is a minimal qualified subset for the secret sharing scheme from $C_\Omega(D, G)$, then $t \le m$ Furthermore, we have the following:

1) when $t = m, \mathcal{A}^c$ is a minimal qualified subset if and only if $B = O$.

2) when $t = m - 1, \mathcal{A}^c$ is a minimal qualified subset if and only if $B \notin \{P_0, \cdots, P_n\}$ or $B \in \mathcal{A}$.

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

II. Main result and open question

A. Main result

In this paper we will discuss the access structures of algebraic geometric secret sharing schemes when q tends to the infinity and the genus satisfies $\lim \frac{g}{\sqrt{q}} = 0$. Roughly speaking quasi-threshold algebraic geometric schemes approach to the threshold secret sharing in this case.

The access structures of elliptic curve secret sharing schemes are determined completely in [9], by applying the finite Abelian group structure of $E(\mathbb{F}_q)$. We will analyze elliptic curves and higher genus curves cases when the order of the ground field q tends to the infinity. In the elliptic curve case, because the set of the rational points $E(\mathbb{F}_q)$ forms a finite Abelian group, we reduce the problem to the counting of the number $N(t, B, \mathcal{P})$ of the set

$$\left\{\mathcal{A} \in \binom{\mathcal{P}}{t} \,\middle|\, \bigoplus_{P\in\mathcal{A}} P = B\right\},$$

where $\mathcal{P} \subset \mathfrak{G}$ is a subset in N element Abelian group $(\mathfrak{G}, \oplus)$ with the cardinality n, $\binom{\mathcal{P}}{t}$ is the set of all subset of $\mathcal{P}$ of the cardinality t, and B is an arbitrary element in $\mathfrak{G}$.

This problem has been extensively studied in [23]–[25]. By Lemma (3), the asymptotic formula $N(t, B, \mathcal{P})$ has a main term $\binom{n}{t}/N$ and an error term $\binom{M}{t}$. Under our assumptions, we have $M < \delta' n$, where $\delta' < 1$, so the error term is much smaller than the main term, as $q \to \infty$, then our result follows.

The same method is used for higher genus curve case with a more complicated technique. The finite Abelian group is replaced by the Jacobian variety $\mathrm{Jac}(C)(\mathbb{F}_q)$ over $\mathbb{F}_q$. In Theorem 4 (or the main result below) by the using of the Abel-Jacobi map we express the proportion of the qualified subsets by $\sum_{a\in\ominus W_{m-t}} N(t, a, \mathcal{P}) \Big/ \binom{n}{t}$. Further in $(\star)$, it can be bounded by

$$\frac{\left|\ominus W_{m-t}(\mathbb{F}_q)\right|}{\binom{n}{t}} \left\{ \frac{\binom{n}{t}}{h_q(C)} + \binom{M}{t} \right\},$$

where $W_d = \phi_d(\mathrm{Sym}^d C)$ is the image of symmetric product of the curve under the d-th Abelian-Jacobi mapping ϕ_d in $\mathrm{Jac}(C)$ and $h_q(C) = |\mathrm{Jac}(C)(\mathbb{F}_q)|$. By Weil bounds for character sums, we also have $M < \delta' n$, where $\delta' < 1$. $h_q(C)$ have the classical Hasse-Weil bound, and $\left|\ominus W_{m-t}(\mathbb{F}_q)\right|$ can be bounded by Proposition 1. When $q \to \infty$, all these bounds fit together to obtain our result.

Let $\mathbb{F}_q$ be a finite field with q elements, C be a smooth projective absolutely irreducible curve defined over $\mathbb{F}_q$ with the genus g, and $C(\mathbb{F}_q)$ be the set of $(\mathbb{F}_q)$ rational points of C. $\{Q, P_0, P_1, \cdots, P_n\}$ is a subset of $C(\mathbb{F}_q)$, $D = P_0 + P_1 + \cdots + P_n$, and $G = mQ$. for some Q not in *supp*(D). The set of players is $\mathcal{P} = \{P_1, \ldots, P_n\}$. The following is our main result in this paper.

Main Result. We assume that $q \to \infty$ and $\lim_{q\to\infty} \frac{g}{\sqrt{q}} = 0$. Suppose that $m = \delta n$, where δ is a constant between 0 and $\frac{2}{3}$, m and n go to the infinity as q tends to infinity. Suppose that $\left|C(\mathbb{F}_q)\right| - \left|\mathcal{P}\right|$ is bounded by a constant c as q tends to infinity. Then

I) when $0 \le m - t < g$, the proportion of the qualified subsets approaches to zero;

II) when $g \le m - t < 2g$, the proportion of the qualified subsets approaches to 1.

.

B. Open question

When the size of the base field is fixed and the genus goes to the infinity the situation would be quite different. In the above proof of Theorem 4, the range of cardinalities of unknown subsets is $[T, T+2g-1]$. The size of this range is $2g$. Because $\lim \frac{g}{\sqrt{q}} = 0$, and $n \sim \left|C(\mathbb{F}_q)\right| \sim q$, then $\lim \frac{2g}{n} = 0$. On the other hand, if we fixed q, and consider a maximal tower $\mathcal{C} = \{C_i\}$ over $\mathbb{F}_q$, which means that $\lim\limits_{i\to\infty} g(C_i) = \infty$ and $\lim\limits_{i\to\infty} \frac{|C_i(\mathbb{F}_q)|}{g(C_i)} = \sqrt{q} - 1$. When q is a square, this can be achieved [16]. Because $\left|C_i(\mathbb{F}_q)\right| - \left|\mathcal{P}\right| < c$, so the limit is $\lim \frac{2g}{n} \approx \frac{2}{\sqrt{q}-1}$, In this case, the Weil bound $\Phi(\mathcal{P}) \le (2g-2)\sqrt{q} + c \sim (2\frac{n}{\sqrt{q}-1} - 2)\sqrt{q} \sim 2\frac{\sqrt{q}}{\sqrt{q}-1}n$ is weaker than the trivial bound $\Phi(\mathcal{P}) \le n$. By this trivial bound, we have $M > n$, so $\binom{n}{t} < \binom{M}{t}$. The estimate about $(\star)$ fails. We refer to [5] for some results on the threshold gap of secret sharing. It seems that in the case q is fixed and the genus goes to the infinity algebraic secret sharing schemes over a fixed base field are not asymptotically threshold.

III. Technical tools

In this section for $x \in \mathbb{R}$, we denote $(x)_0 = 1$ and $(x)_t = x(x-1)\cdots(x-t+1)$ for $t \in \mathbb{Z}^+$. For $t \in \mathbb{N}$, $\binom{x}{t} \overset{\text{def}}{=} \frac{(x)_t}{t!}$.

A. Li-Wan's sieve

We recall the sieving formula discovered by Li and Wan [23]. Roughly speaking, this formula significantly improves the classical inclusion-exclusion sieve for distinct coordinate counting problems. We cite it here without proof, and there are many interesting applications of this new sieve method [23]–[25].

Let $\mathcal{P}$ be a finite set, and $\mathcal{P}^t$ denotes the Cartesian product of t copies of $\mathcal{P}$. Let X be a subset of $\mathcal{P}^t$. Define $\bar{X} = \{x = (x_1, x_2, \cdots, x_t) \in X | x_i \ne x_j, i \ne j\}$, Let $f(x_1, x_2, \cdots, x_t)$ be a complex valued function defined over X and

$$F = \sum_{x \in \bar{X}} f(x_1, x_2, \cdots, x_t).$$

Let S_t be the symmetric group on $\{1, 2, \cdots, t\}$. Each permutation $\tau \in S_t$ factorizes uniquely as a product of disjoint cycles and each fixed point is viewed as a trivial cycle of length 1. Two permutations in S_t are conjugate if and only if they have the same type of cycle structure (up to the order). For $\tau \in S_t$, define the sign of τ to be $\text{sign}(\tau) = (-1)^{(t-l(\tau))}$, where $l(\tau)$ is the number of cycles of τ including the trivial cycles. For a permutation $\tau = (i_1 i_2 \cdots i_{a_1})(j_1 j_2 \cdots j_{a_2}) \cdots (l_1 l_2 \cdots l_{a_s})$ with $1 \le a_i, 1 \le i \le s$, define

$$X_\tau = \{(x_1, \cdots, x_t) \in X, x_{i_1} = \cdots = x_{i_{a_1}}, \cdots, x_{l_1} = \cdots = x_{l_{a_s}}\}.$$

For $\tau \in S_t$, define $F_\tau = \sum_{x \in X_\tau} f(x_1, x_2, \cdots, x_t)$. Now we can state Li-Wan's sieve formula.

Theorem 2: Let F and F_τ be defined as above. Then

$$F = \sum_{\tau \in S_t} \text{sign}(\tau) F_\tau. \tag{1}$$

Note that the symmetric group S_t acts on $\mathcal{P}^t$ naturally by permuting coordinates, That is,for $\tau \in S_t$ and $x = (x_1, x_2 \cdots, x_t) \in \mathcal{P}^t$, we have $\tau \circ x = (x_{\tau(1)}, x_{\tau(2)}, \cdots, x_{\tau(t)})$. A subset $X \subset \mathcal{P}^t$ is said to be symmetric if for any $x \in X$ and any $\tau \in S_t, \tau \circ x \in X$.

For $\tau \in S_t$, denote by $\bar{\tau}$ the conjugacy class determined by τ and it can also be viewed as the set of permutations conjugate to τ. Conversely, for one given conjugacy class $\bar{\tau} \in C_t$, denote by τ a representative permutation of this class. For convenience we usually identify these two symbols.

In particular, if X is symmetric and f is a symmetric function under the action of S_t, we then have the following simpler formula than (1).

Corollary 1: Let C_t be the set of conjugacy classes of S_t. If X is symmetric and f is symmetric, then

$$F = \sum_{\tau \in C_t} \text{sign}(\tau) C(\tau) F_\tau, \tag{2}$$

where $C(\tau)$ is the number of permutations conjugate to τ.

For the purpose of evaluating the above summation, we need a combinatorial formulas. A permutation $\tau \in S_t$ is said to be of type $(c_1, c_2, \cdots, c_t)$ if τ has exactly c_i cycles of length i. Note that $\sum_{i=1}^t i c_i = t$. As we know, two permutations in S_t are conjugate if and only if they have the same type of cycle structure. Let $N(c_1, c_2, \cdots, c_t)$ be the number of permutations in S_t of type $(c_1, c_2, \cdots, c_t)$ and it is well known that

$$N(c_1, c_2, \cdots, c_t) = \frac{t!}{1^{c_1} c_1! 2^{c_2} c_2! \cdots t^{c_t} c_t!}.$$

Lemma 2: Define the generating function

$$C_t(q_1, q_2, \cdots, q_t) = \sum_{\sum_{i=1}^t ic_i = t} N(c_1, c_2, \cdots, c_t) q_1^{c_1} q_2^{c_2} \cdots q_t^{c_t},$$

and set $q_1 = q_2 = \cdots = q_k = q$, then we have

$$\begin{aligned} C_t(q, q, \cdots, q) &= \sum_{\sum ic_i = t} N(c_1, c_2, \cdots, c_t) q^{c_1} q^{c_2} \cdots q^{c_t} \\ &= (q + t - 1)_t. \end{aligned}$$

If we set $q_i = q$ for $d \mid i$ and $q_i = s$ for $d \nmid i$, then

$$\begin{aligned} & C_t(\overbrace{s, \cdots, s}^{d-1}, q, \overbrace{s, \cdots, s}^{d-1}, q, \cdots) \\ = & \textstyle\sum_{\sum ic_i = t} N(c_1, c_2, \cdots, c_t) s^{c_1} s^{c_2} \cdots q^{c_d} s^{c_{d+1}} \cdots \\ = & t! \textstyle\sum_{i=0}^{\lfloor t/d \rfloor} \binom{\frac{q-s}{d} + i - 1}{\frac{q-s}{d} - 1} \binom{s+t-di-1}{s-1} \\ \leq & t! \binom{s+t+(q-s)/d-1}{t}. \end{aligned}$$

Let $(\mathfrak{G}, \oplus)$ be a finite Abelian group with order $\left|\mathfrak{G}\right| = N$, and let $\mathcal{P} \subset \mathfrak{G}$ be a nonempty subset of cardinality n. $\binom{\mathcal{P}}{t}$ denotes the set of all t-subsets of $\mathcal{P}$, then $\left|\binom{\mathcal{P}}{t}\right| = \binom{n}{t}$. For $B \in \mathfrak{G}$, let

$$\mathfrak{N}(t, B, \mathcal{P}) = \left\{ \mathcal{A} \in \binom{\mathcal{P}}{t} \middle| \bigoplus_{P \in \mathcal{A}} P = B \right\},$$

and

$$N(t, B, \mathcal{P}) = \left|\mathfrak{N}(t, B, \mathcal{P})\right|.$$

$\hat{\mathfrak{G}}$ is the group of additive characters of $\mathfrak{G}$ with trivial character χ_0. Note that $\hat{\mathfrak{G}}$ is isomorphic to $\mathfrak{G}$. Denote the partial character sum $s_\chi(\mathcal{P}) = \sum_{a \in \mathcal{P}} \chi(a)$ and the amplitude $\Phi(\mathcal{P}) = \max_{\chi \in \hat{\mathfrak{G}}, \chi \neq \chi_0} |s_\chi(\mathcal{P})|$.

For our application, the estimate $N(t, B, \mathcal{P})$ is crucial, when $\mathfrak{G} = \mathrm{Jac}(C)(\mathbb{F}_q)$, which is the rational points of the Jacobian variety of an algebraic curve. In [23]–[25] the authors gave estimates for some special finite Abelian groups. We use their method to give an estimate for a general finite Abelian group.

Lemma 3: Let $N(t, B, \mathcal{P})$ be defined as above. Then

$$\left| N(t, B, \mathcal{P}) - \frac{\binom{n}{t}}{N} \right| \leq \binom{M}{t}, \tag{3}$$

where M is defined as $M = \max\left\{ \Phi(\mathcal{P}) + t - 1, \frac{n + \Phi(\mathcal{P})}{2}, \frac{n - \Phi(\mathcal{P})}{3} + \Phi(\mathcal{P}) + t - 1 \right\}$.

Proof. Let $X = \mathcal{P}^t$ be the Cartesian product of t copies of $\mathcal{P}$, and $\bar{X} = \{x = (x_1, x_2 \cdots, x_t) \in \mathcal{P}^t | x_i \neq x_j, i \neq j\}$. It is clear that $\left|X\right| = n^t$ and $\left|\bar{X}\right| = (n)_t$. Then

$$\begin{aligned} t!N(t,B,\mathcal{P}) &= N^{-1} \sum_{x\in\bar{X}} \sum_{\chi\in\hat{\mathfrak{G}}} \chi(x_1 + x_2 + \cdots + x_t - B) \\ &= \frac{(n)_t}{N} + N^{-1} \sum_{\chi\neq\chi_0} \sum_{x\in\bar{X}} \chi(x_1)\chi(x_2)\cdots\chi(x_t)\chi^{-1}(B) \\ &= \frac{(n)_t}{N} + N^{-1} \sum_{\chi\neq\chi_0} \chi^{-1}(B) \sum_{x\in\bar{X}} \prod_{i=1}^{t} \chi(x_i). \end{aligned}$$

For $\chi \neq \chi_0$, let $f_\chi(x) = f_\chi(x_1, x_2 \cdots, x_t) = \prod_{i=1}^t \chi(x_i)$, and for $\tau \in S_t$ let

$$F_\tau(\chi) = \sum_{x\in X_\tau} f_\chi(x) = \sum_{x\in X_\tau} \prod_{i=1}^{t} \chi(x_i).$$

Obviously X and $f_\chi(x_1, x_2 \cdots, x_t)$ are symmetric. Applying (2),

$$t!N(t,B,\mathcal{P}) = \frac{(n)_t}{N} + N^{-1} \sum_{\chi\neq\chi_0} \chi^{-1}(B) \sum_{\tau\in C_t} \mathrm{sign}(\tau)C(\tau)F_\tau(\chi).$$

Assume τ is of type $(c_1, c_2, \cdots, c_t)$, without loss of generality, we can write

$$\tau = (1)(2)\cdots(c_1)((c_1+1)(c_1+2))\cdots((c_1+2c_2-1)(c_1+2c_2))\cdots.$$

One can check that

$$X_\tau = \left\{(x_1, \cdots, x_t) \in \mathcal{P}^t \middle| x_{c_1+1} = x_{c_1+2}, \cdots, x_{c_1+2c_2-1} = x_{c_1+2c_2}, \cdots \right\}.$$

Then we have

$$\begin{aligned} F_\tau(\chi) &= \sum_{x\in X_\tau} \prod_{i=1}^{t} \chi(x_i) \\ &= \sum_{x\in X_\tau} \prod_{i=1}^{c_1} \chi(x_i) \prod_{i=1}^{c_2} \chi^2(x_{c_1+2i}) \cdots \prod_{i=1}^{c_t} \chi^t(x_{c_1+2c_2+\cdots ti}) \\ &= \prod_{i=1}^{t} (\sum_{a\in\mathcal{P}} \chi^i(a))^{c_i} \\ &= n^{\sum c_i m_i(\chi)} s_\chi(\mathcal{P})^{\sum c_i(1-m_i(\chi))}, \end{aligned}$$

where $m_i(\chi) = 1$ if $\chi^i = 1$ and otherwise $m_i(\chi) = 0$.

Now suppose $\mathrm{ord}(\chi) = d$ with $d \mid N$. Note that $C(\tau) = N(c_1, c_2, \ldots, c_t)$. In the case $3 \le d \le t$ since $|s_\chi(\mathcal{P})| \le \Phi(\mathcal{P})$, applying Lemma 2, we have

$$\begin{aligned}&\sum_{\tau \in C_t} \mathrm{sign}(\tau) C(\tau) F_\tau(\chi) \\ &\le \sum_{\tau \in C_t} C(\tau) n^{\sum c_i m_i(\chi)} \Phi(\mathcal{P})^{\sum c_i (1 - m_i(\chi))} \\ &\le t! \binom{\frac{n - \Phi(\mathcal{P})}{d} + \Phi(\mathcal{P}) + t - 1}{t}.\end{aligned}$$

In the case $d = 2$, it can also be prooved that [25]

$$\sum_{\tau \in C_t} \mathrm{sign}(\tau) C(\tau) F_\tau(\chi) \le t! \binom{\frac{n + \Phi(\mathcal{P})}{2}}{t}.$$

Similarly, if $\mathrm{ord}(\chi) > t$, then

$$\sum_{\tau \in C_t} \mathrm{sign}(\tau) C(\tau) F_\tau(\chi) \le t! \binom{\Phi(\mathcal{P}) + t - 1}{t}.$$

Let T be the set of characters which have order greater than t. Summing over all nontrivial characters, we obtain

$$\begin{aligned}\left| N(t, B, \mathcal{P}) - \frac{\binom{n}{t}}{N} \right| \le \frac{|T|}{N} \binom{\Phi(\mathcal{P}) + t - 1}{t} + \frac{\pi(2)}{N} \binom{\frac{n + \Phi(\mathcal{P})}{2}}{t} \\ + \frac{1}{N} \sum_{2 < d \le t} \pi(d) \binom{\frac{n - \Phi(\mathcal{P})}{d} + \Phi(\mathcal{P}) + t - 1}{t},\end{aligned}$$

where $\pi(d)$ is the number of characters in $\widehat{\mathfrak{G}}$ of order d. The sequence $\{\frac{n - \Phi(\mathcal{P})}{d} + \Phi(\mathcal{P}) + t - 1\}_{d > 2}$, is decreasing. So let

$$M = \max\left\{\Phi(\mathcal{P}) + t - 1, \frac{n + \Phi(\mathcal{P})}{2}, \frac{n - \Phi(\mathcal{P})}{3} + \Phi(\mathcal{P}) + t - 1\right\},$$

we have the inequality.

□

B. Abel-Jacobi Map

Let $C/\mathbb{F}_q$ be a smooth projective curve of genus g over the finite field $\mathbb{F}_q$. The divisor class group of C is defined to be the quotient group $\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{Prin}(C)$, where $\mathrm{Prin}(C)$ is the subgroup consisting of all principal divisors. For a divisor $D \in \mathrm{Div}(C)$, the corresponding element in the factor group $\mathrm{Pic}(C)$ is denoted by $[D]$, the divisor class of D.

We have the degree zero divisor class subgroup $\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{Prin}(C)$. Assume that C has a $\mathbb{F}_q$-rational point Q, it is well known that there exists an Abelian variety $\mathrm{Jac}(C)/\mathbb{F}_q$ of dimension g with the property that for every extension field $k/\mathbb{F}_q$, there is a naturally isomorphism

$$\mathrm{Jac}(C)(k) \longrightarrow \mathrm{Pic}^0(C)(k).$$

Moreover, the so-called Abel-Jacobi map $\phi_1 : C/\mathbb{F}_q \to \mathrm{Jac}(C)/\mathbb{F}_q$ given by

$$\phi_1 : \quad P \mapsto [P - Q]$$

is a morphism of algebraic varieties over $\mathbb{F}_q$.

Let $\mathrm{Sym}^d C$ denote the d-th symmetric product of C, and let $\mathrm{Div}^d_+(C)$ denote the set of the effective rational divisors of degree d. Then $\mathrm{Sym}^d C(\mathbb{F}_q)$ can be identified with $\mathrm{Div}^d_+(C)$, And let $A_d \stackrel{\mathrm{def}}{=} |\mathrm{Div}^d_+(C)| = |\mathrm{Sym}^d C(\mathbb{F}_q)|$. We can further define the d-th Abel-Jacobi map $\phi_d : \mathrm{Sym}^d C \to \mathrm{Jac}(C)$ by

$$\phi_d : \quad D_1 + \cdots + D_h \mapsto [D_1 + \cdots + D_h - dQ],$$

where $D_1, \cdots, D_h$ are closed points of $C/\mathbb{F}_q$, with $\sum_{i=1}^h \deg(D_i) = d$. Let $W_d = \phi_d(\mathrm{Sym}^d C)$ denote the image of ϕ_d in $\mathrm{Jac}(C)$.

The Abel-Jacobi Theorem says that $\phi_1 : C \to W_1$ is an isomorphism, $\phi_d : \mathrm{Sym}^d C \to W_d$ are birational morphisms, for $2 \le d \le g$, and $W_g = \mathrm{Jac}(C)$. Let $h_q(C) = |\mathrm{Jac}(C)(\mathbb{F}_q)|$, then there is Hasse-Weil bound for $\mathrm{Jac}(C)$ [30], [34]

$$(\sqrt{q} - 1)^{2g} \le h_q(C) \le (\sqrt{q} + 1)^{2g}. \tag{4}$$

We have the following estimates (For details please refer to [30], Lemma 5.3.4) as well.

Proposition 1: Let $C/\mathbb{F}_q$ be an algebraic curve of genus $g \ge 1$. Then for any integers $d \ge 0$ we have

$$A_d \le \frac{h_q(C)}{q^{g-d}} \left(\frac{2gq^{1/2}}{q^{1/2} - 1} - \frac{q}{q-1} \right).$$

Consequently, we have

$$\left|W_d(\mathbb{F}_q)\right| \le A_d \le \frac{h_q(C)}{q^{g-d}} \left(\frac{2gq^{1/2}}{q^{1/2} - 1} - \frac{q}{q-1} \right), \tag{5}$$

for $1 \le d \le g - 1$.

C. Character Sums on Curve

$\mathrm{Jac}(C)(\mathbb{F}_q)$ is a finite Abelian group. Let $\chi : \mathrm{Jac}(C)(\mathbb{F}_q) \to \mathbb{C}^*$ be a character. Via Abel-Jacobi map $\phi_1 : \quad P \mapsto [P - Q]$, one can consider character sum on curve C, let

$$s_\chi = \sum_{P \in C(\mathbb{F}_q)} \chi([P - Q]).$$

If χ is trivial, we have Hasse-Weil bound

$$\left| s_\chi - q \right| \leq 2gq^{\frac{1}{2}}.$$

If χ is nontrivial, we have the following Weil bounds for character sums (For details please refer to [22], proposition 9.1.3 and [31], chapter 9).

Proposition 2: Suppose χ is a nontrivial character of $\mathrm{Jac}(C)(\mathbb{F}_q)$, then

$$|s_\chi| \leq (2g - 2)q^{\frac{1}{2}}. \tag{6}$$

IV. AGLSSS over large fields are asymptotically threshold

In this section we consider the case of secret sharing schemes from elliptic curves when $q \to \infty$ at first, since in this case Theorem 1 can be used to count qualified and unqualified sets directly.

Let $E/\mathbb{F}_q$ be an elliptic curve, and let $C/\mathbb{F}_q$ be an algebraic curve of genus g at least 2. In this section we let the Abelian group $\mathfrak{G}$ be equal to $E(\mathbb{F}_q)$ and $\mathrm{Jac}(C)(\mathbb{F}_q)$ separately. $\oplus$ and $\ominus$ denote additive and minus operator in the group.

A. Elliptic curve case

Let $\mathfrak{G} = E(\mathbb{F}_q)$ with zero element O. As in Theorem 1, $\{P_0, \cdots, P_n\}$ are a subset of $E(\mathbb{F}_q)$ of $n + 1$ nonzero distinct elements. $D = P_0 + \cdots + P_n$ and $G = mO$ are divisors of E. We have the secret sharing scheme from $C_\Omega(D, G)$, with the set of players $\mathcal{P} = \{P_1, \cdots, P_n\}$. Then we have the following result.

Theorem 3: Suppose that $m = \delta n$, where δ is a constant between 0 and $\frac{2}{3}$. As $q \to \infty$, we assume that n and m all approach to infinity, and $\left|\mathfrak{G}\right| - \left|\mathcal{P}\right|$ is bounded by a constant c. Then
I) when $t = m$, the proportion of the qualified subsets approaches to $zero$;
II) when $t = m - 1$, the proportion of the qualified subsets approaches to 1.

Proof. Note that $\mathcal{P}$ is the set of players $\{P_1, \cdots, P_n\}$. Recall that $\binom{\mathcal{P}}{t}$ denotes the set of all t-subsets of $\mathcal{P}$.

Let $\mathcal{A} \in \binom{\mathcal{P}}{t}$ be a subset of $\mathcal{P}$ with cardinality t. Then $\mathcal{A}^c = \mathcal{P} \setminus \mathcal{A}$ is a qualified subset if and only if we can find a rational function $f \in L(G)$ such that $f(P_0) \neq 0$ and $f(P) = 0$ for all $P \in \mathcal{A}$.

Now we divide into two sub-cases for completing the whole proof of the theorem.

I) Suppose $t = m$. Because f is a nonzero element of $L(G)$ with the divisor $G = mO$, it has at most m distinct zeros. It follows from the assumption $t = m$ that the divisor of the function f should be

$$\mathrm{div}(f) = \sum_{P \in \mathcal{A}} P - mO.$$

The existence of such a function f is equivalent to saying (see Theorem 11.2 of [35])

$$\bigoplus_{P \in \mathcal{A}} P = O.$$

Namely $\mathcal{A} \in \mathfrak{N}(t, O, \mathcal{P})$. For our purpose, we now give an estimate for the value $\Phi(\mathcal{P})$. According to the basic properties of group characters, we have

$$\sum_{g \in \mathfrak{G}} \chi(g) = 0$$

for a nontrivial character χ. This implies that

$$\sum_{g \in \mathcal{P}} \chi(g) = -\sum_{g \in \mathfrak{G} - \mathcal{P}} (g)$$

and so

$$\Phi(\mathcal{P}) = \Phi(\mathfrak{G} - \mathcal{P}) \leq \left|\mathfrak{G} - \mathcal{P}\right| = \left|\mathfrak{G}\right| - \left|\mathcal{P}\right| \leq c,$$

if $\left|\mathfrak{G}\right| - \left|\mathcal{P}\right|$ is bounded by a constant c. Now let $n \to \infty$, if $t < \frac{1}{6}n$, then $M = \frac{n+\Phi(\mathcal{P})}{2}$; if $\frac{1}{6}n \leq t = m < \frac{2}{3}n$, then $M = \frac{n-\Phi(\mathcal{P})}{3} + \Phi(\mathcal{P}) + t - 1$. in a word, $M < \delta' n$, where $0 < \delta' < 1$. It follows from Lemma 3 that

$$\begin{aligned} \frac{N(t, O, \mathcal{P})}{\binom{n}{t}} &\leq \frac{1}{N} + \frac{\binom{M}{t}}{\binom{n}{t}} \\ &\leq \frac{1}{N} + \frac{\binom{\delta' n}{t}}{\binom{n}{t}} \\ &= \frac{1}{N} + \frac{(\delta' n)(\delta' n - 1) \cdots (\delta' n - t + 1)}{n(n-1) \cdots (n-t+1)}. \end{aligned}$$

Since

$$1 > \delta' = \frac{\delta' n}{n} > \frac{\delta' n - 1}{n - 1} > \cdots > \frac{\delta' n - t + 1}{n - t + 1},$$

it follows that $\lim\limits_{q\to\infty} \frac{(\delta' n)(\delta' n-1)\cdots(\delta' n-t+1)}{n(n-1)\cdots(n-t+1)} = 0$. Note that $\lim\limits_{q\to\infty} \frac{1}{N} = 0$. Hence we have

$$\lim_{q\to\infty} \frac{N(t,O,\mathcal{P})}{\binom{n}{t}} = 0.$$

This means that the proportion of the qualified subsets approaches to *zero* if $t = m$.

II) Suppose $t = m-1$. For the same reason, the divisor of the function f should satisfy

$$\operatorname{div}(f) = \sum_{P\in\mathcal{A}} P + P' - mO,$$

where $P' \in E(\mathbb{F}_q)$ and $P' \neq P_0$. Similarly, the existence of the function f is equivalent to

$$\bigoplus_{P\in\mathcal{A}} P = \ominus P' \neq P_0.$$

That is to say, $\mathcal{A} \notin \mathfrak{N}(t,(\ominus P_0),\mathcal{P})$. Similarly, one can show that

$$\lim_{q\to\infty} \frac{N(t,(\ominus P_0),\mathcal{P})}{\binom{n}{t}} = 0.$$

This implies that the proportion of the qualified subsets which is equal to $1 - \frac{N(t,(\ominus P_0),\mathcal{P})}{\binom{n}{t}}$ approaches to 1 if q and m tend to infinity and $t = m-1$. This completes the whole proof of Theorem 3.

□

B. General curve case

Let $C/\mathbb{F}_q$ be an algebraic curve of genus g. Let $\{Q, P_0, P_1, \cdots, P_n\}$ be a subset of $C(\mathbb{F}_q)$, and let $D = P_0 + \cdots + P_n$ and $G = mQ$. We have the secret sharing scheme from $C_\Omega(D,G)$, with the set of players $\mathcal{P} = \{P_1, \cdots, P_n\}$. In this section, we will consider the asymptotic access structures of that algebraic geometric secret sharing schemes as $q \to \infty$.

We denote $\mathfrak{G} = \operatorname{Jac}(C)(\mathbb{F}_q)$ in this subsection. Because Abel-Jacobi map $\phi_1 : C \to \operatorname{Jac}(C)$, is an embedding. For a subset $\mathcal{S} \subset C(\mathbb{F}_q)$, the symbol $\mathcal{S}$ sometimes denotes its image $\phi_1(\mathcal{S}) \subset \operatorname{Jac}(C)(\mathbb{F}_q)$ by abuse of notation. By Hasse-Weil bound we have $q - 2gq^{1/2} \leq \left|C(\mathbb{F}_q)\right| \leq q + 2gq^{1/2}$. If the genus g satisfies $\lim\limits_{q\to\infty} \frac{g}{\sqrt{q}} = 0$, then $\left|C(\mathbb{F}_q)\right| \sim q$. Thus $\left|C(\mathbb{F}_q)\right|$ and $h_q(C) = \left|\operatorname{Jac}(C)(\mathbb{F}_q)\right| \geq (q^{1/2}-1)^{2g}$ both approach to infinity as q tends to infinity. We prove the following result.

Theorem 4: We assume that $q \to \infty$ and $\lim\limits_{q\to\infty} \frac{g}{\sqrt{q}} = 0$. Suppose that $m = \delta n$, where δ is a constant between 0 and $\frac{2}{3}$, m and n go to the infinity as q tends to infinity. Suppose that $\left|C(\mathbb{F}_q)\right| - \left|\mathcal{P}\right|$ is bounded by a constant c as q tends to infinity. Then

I) when $0 \leq m - t < g$, the proportion of the qualified subsets approaches to zero;

II) when $g \leq m - t < 2g$, the proportion of the qualified subsets approaches to 1.

Proof. For any $\mathcal{A} \in \binom{\mathcal{P}}{t}$, let $\mathcal{A}^c = \mathcal{P} \setminus \mathcal{A}$ and $P_{\mathcal{A}} = \sum_{P \in \mathcal{A}} P \in \mathrm{Div}_+^t(C)$. Then $\mathcal{A}^c$ is a qualified subset if and only if we can find a rational function $f \in L(G)$ such that $\mathcal{A}$ is contained in the zero locus of f and $f(P_0) \neq 0$, i.e. $f \in L(G - P_{\mathcal{A}}) \setminus L(G - P_{\mathcal{A}} - P_0)$. And by the Riemann-Roch Theorem [33], we have the following equivalent condition for $\mathcal{A}^c$ qualified

$$\begin{cases} l(G - P_{\mathcal{A}}) > 0, & (a) \\ L(K_C - G + P_{\mathcal{A}}) = L(K_C - G + P_{\mathcal{A}} + P_0), & (b) \end{cases}$$

where $l(G - P_{\mathcal{A}}) = \dim(L(G - P_{\mathcal{A}}))$, and K_C is the canonical divisor of C.

I) Suppose $0 \leq m - t < g$. If $\mathcal{A}^c$ is qualified, then

$$l(G - P_{\mathcal{A}}) > 0,$$

by the condition (a). We choose a nonzero element $f \in L(G - P_{\mathcal{A}})$, and let $D_{\mathcal{A}} = G - P_{\mathcal{A}} + \mathrm{div}(f) \geq 0$ which is an effective divisor of C, with $\deg(D_{\mathcal{A}}) = m - t$.

Consider the following map $\binom{\mathcal{P}}{t} \hookrightarrow \mathrm{Div}_+^t(C) \to \mathrm{Jac}(C)$ given by

$$\mathcal{A} \mapsto P_{\mathcal{A}} \overset{\phi_t}{\mapsto} [P_{\mathcal{A}} - tQ].$$

Because $D_{\mathcal{A}}$ is linearly equivalent to $G - P_{\mathcal{A}}$, we have the divisor class equality

$$[D_{\mathcal{A}}] = [G - P_{\mathcal{A}}]$$

in the Jacobian group $\mathrm{Jac}(C)$. It follows from $G = mQ$ that

$$[D_{\mathcal{A}} - (m - t)Q] = [G - P_{\mathcal{A}} - (m - t)Q] = \ominus[P_{\mathcal{A}} - tQ].$$

Thus

$$\phi_t(P_{\mathcal{A}}) = \ominus\phi_{m-t}(D_{\mathcal{A}}) \in \ominus W_{m-t},$$

where $\ominus W_{m-t}$ denotes the set that contains all negative elements in W_{m-t}.

Now we get

$$\mathcal{A} \in \bigcup_{a \in \ominus W_{m-t}} \phi_t^{-1}(a) \cap \binom{\mathcal{P}}{t} = \bigcup_{a \in \ominus W_{m-t}} \mathfrak{N}(t, a, \mathcal{P})$$

by the definition of $\mathfrak{N}(t, a, \mathcal{P})$.

For our purpose, we give an estimate for $\Phi(\mathcal{P})$. By Proposition 2, for a nontrivial character χ, we have

$$\Phi(\mathcal{P}) = \Phi(C(\mathbb{F}_q) - (C(\mathbb{F}_q)\backslash\mathcal{P})) \leq \Phi(C(\mathbb{F}_q)) + \Phi(C(\mathbb{F}_q)\backslash\mathcal{P})) \leq (2g - 2)q^{\frac{1}{2}} + c$$

if $\left|C(\mathbb{F}_q)\right| - \left|\mathcal{P}\right|$ is bounded by a constant c. Since $\lim_{q\to\infty} \frac{(2g-2)\sqrt{q}}{n} = 0$. In Lemma 3, as the elliptic curve case, we have $M < \delta' n$, where $\delta' < 1$.

We are now in a position to show that the proportion of the qualified subsets tends to *zero* , i.e., the ratio

$$\sum_{a\in\ominus W_{m-t}} N(t,a,\mathcal{P}) \Big/ \binom{n}{t} \to 0,$$

as q tends to infinity

On basis of (3), (4) and (5) one has

$$\begin{aligned}
&\frac{\sum\limits_{a\in\ominus W_{m-t}} N(t,a,\mathcal{P})}{\binom{n}{t}} \\
\leq\ & \frac{\left|\ominus W_{m-t}(\mathbb{F}_q)\right|}{\binom{n}{t}} \left\{ \frac{\binom{n}{t}}{h_q(C)} + \binom{M}{t} \right\} \\
<\ & \frac{\left|W_{m-t}(\mathbb{F}_q)\right|}{h_q(C)} + \left|W_{m-t}(\mathbb{F}_q)\right| \frac{(\delta' n)_t}{(n)_t} \\
\leq\ & \frac{1}{q^{(g-(m-t))}} \left(\frac{2gq^{1/2}}{q^{1/2}-1} - \frac{q}{q-1} \right) + \\
& \frac{h_q(C)}{q^{(g-(m-t))}} \left(\frac{2gq^{1/2}}{q^{1/2}-1} - \frac{q}{q-1} \right) \prod_{i=0}^{t-1} \frac{\delta' n - i}{n-i} \\
\leq\ & \frac{1}{q} \left(\frac{2gq^{1/2}}{q^{1/2}-1} - \frac{q}{q-1} \right) + \\
& \frac{(q^{1/2}+1)^{2g}}{q} \left(\frac{2gq^{1/2}}{q^{1/2}-1} - \frac{q}{q-1} \right) \prod_{i=0}^{t-1} \frac{\delta' n - i}{n-i}, \quad (\star)
\end{aligned}$$

where $n \sim q$ and $t \sim \delta q$.

When $q \to \infty$, we have $\frac{1}{q}\left(\frac{2gq^{1/2}}{q^{1/2}-1} - \frac{q}{q-1}\right) \to 0$, since $\lim_{q\to\infty} \frac{g}{\sqrt{q}} = 0$. And $\frac{\delta' n - i}{n-i} < \delta' < 1$, this implies that

$$\prod_{i=0}^{t-1} \frac{\delta' n - i}{n-i} \leq \delta'^{\delta q}.$$

Consequently

$$\begin{aligned}
& \ln \left\{\frac{(q^{1/2}+1)^{2g}}{q}\left(\frac{2gq^{1/2}}{q^{1/2}-1}-\frac{q}{q-1}\right)\prod_{i=0}^{t-1}\frac{\delta' n-i}{n-i}\right\} \\
\leq \quad & 2g\ln(q^{1/2}+1)-\ln q+\ln\left(\frac{2gq^{1/2}}{q^{1/2}-1}-\frac{q}{q-1}\right)+(\delta\ln\delta')q \\
\to \quad & -\infty,
\end{aligned}$$

as q tends to infinity. Thus $(\star)$ approaches to *zero*. The conclusion follows.

II) Suppose $g \leq m-t < 2g$. By the Riemann-Roch Theorem, we have

$$l(G-P_{\mathcal{A}}) \geq \deg(G-P_{\mathcal{A}})+1-g = m-t+1-g > 0.$$

This means that Condition (a) always holds. It follows from the Condition (b) that the set $\mathcal{A}^c$ is unqualified if and only if the set $L(K_C-G+P_{\mathcal{A}})$ is a proper subset of $L(K_C-G+P_{\mathcal{A}}+P_0)$, i.e.,

$$L(K_C-G+P_{\mathcal{A}}) \subsetneq L(K_C-G+P_{\mathcal{A}}+P_0).$$

Let us choose a nonzero element $f \in L(K_C-G+P_{\mathcal{A}}+P_0)\setminus L(K_C-G+P_{\mathcal{A}})$, and let $D_{\mathcal{A}}^K = K_C-G+P_{\mathcal{A}}+P_0+\mathrm{div}(f) \geq 0$ which is an effective divisor of C, with degree $s=\deg(D_{\mathcal{A}}^K)=2g-1-(m-t)$, and $0 \leq s \leq g-1$. This fact will play a vital role in the proof.

In a similar manner, we consider the following map $\binom{\mathcal{P}}{t} \hookrightarrow \mathrm{Div}_+^t(C) \to \mathrm{Jac}(C)$ given by

$$\mathcal{A} \mapsto P_{\mathcal{A}} \stackrel{\phi_t}{\mapsto} [P_{\mathcal{A}}-tQ].$$

Because $D_{\mathcal{A}}^K$ is linearly equivalent to $K_C-G+P_{\mathcal{A}}+P_0$, by definition, $[D_{\mathcal{A}}^K]=[K_C-G+P_{\mathcal{A}}+P_0]$, then

$$\begin{aligned}
[D_{\mathcal{A}}^K-sQ] &= [K_C-G+P_{\mathcal{A}}+P_0-sQ] \\
&= [K_C+P_0-(2g-1)Q]\oplus[P_{\mathcal{A}}-tQ].
\end{aligned}$$

Thus

$$\begin{aligned}
\phi_t(P_{\mathcal{A}}) &= \phi_s(D_{\mathcal{A}}^K)\ominus[K_C+P_0-(2g-1)Q] \\
&\in \phi_s(C_s)\ominus[K_C+P_0-(2g-1)Q]=\widetilde{W}_s,
\end{aligned}$$

where $\widetilde{W}_s$ is the translation of W_s by the element $\ominus[K_C + P_0 - (2g-1)Q]$.

Namely, $\mathcal{A}^c$ is a qualified subset if and only if

$$\mathcal{A} \notin \bigcup_{a\in\widetilde{W}_s} \phi_t^{-1}(a) \cap \binom{\mathcal{P}}{t} = \bigcup_{a\in\widetilde{W}_s} \mathfrak{N}(t,a,\mathcal{P}).$$

Since $s \leq g-1$, similarly one can show that

$$\lim_{q\to\infty} \frac{\sum_{a\in\widetilde{W}_s} N(t,a,\mathcal{P})}{\binom{n}{t}} = 0.$$

So the proportion of the qualified subsets approaches to 1 as q tends to infinity. This completes the whole proof of the theorem.

$\square$

V. Conclusion

Algebraic geometric secret sharing schemes have been widely used in two-party secure computation, secure multiparty computation, communication-efficient zero-knowledge of circuit satisfiability, correlation extractors and OT-combiners since the publication of [7]. In many cases when Shamir's threshold secret sharing scheme is replaced by algebraic geometric secret sharing schemes the base field can be constant-size and communication complexity can be saved by a $logn$ factor. Thus it is quite important to answer the question how far from threshold these quasi-threshold algebraic geometric secret sharing schemes are. We showed that when the size q of the base field goes to the infinity and $\lim \frac{g}{\sqrt{q}} = 0$, algebraic geometric secret sharing schemes are asymptotically threshold. It would be interesting to know asymptotic situation of algebraic geometric secret sharing schemes in the case that the size q of base field is fixed and the genus of curves goes to the infinity. In particular are algebraic geometric secret sharing schemes asymptotically threshold in this case?

References

[1] J. Benaloh and J. Leichter, Generalized secret sharing and monotone functions, in: Advances in Cryptology – Crypto' 88, Lecture Notes in Computer Science, vol. 403, Springer, Heidelberg, 1989, pp. 25–35.

[2] G. R. Blakley, Safeguarding cryptographic key, Proceedings of the 1979 AFIPS National Computer Conference (Monval, NJ, USA), AFIPS Press, pp. 313-317, 1979.

[3] M. Ben-Or, S. Goldwaser and A. Wigderson, Completeness theorems for noncryptographic fault-tolerant distributed computation (extended abstract), Proceedings of the 20th Annual ACM STOC, 1988, 1-10, 1988.

[4] E. F. Brickell, Some ideal secret sharing schemes, Advances in Cryptology-Eurocrypt 89, ser. Lecture Notes in Computer Science, Heidelberg, Germany: Springer, vol. 434, pp. 468-475, 1990.

[5] I. Cascudo, R. Cramer and C. Xing, Bounds on the threshold gap in secret sharing and its applications, IEEE Transactions on Information Theory, vol. 59, no.9, 5600-5612, 2013.

[6] D. Chaum, C. Crépeau and Damgård, Multiparty unconditionally secure protocols (extended abstract), Proceedings of the 20th Annual ACM STOC, 1988, 11-19, 1988.

[7] H. Chen and R. Cramer, Algebraic geometric secret sharing schemes and secure multi-party computation over small fields, Proc. Crypto 2006, pp. 521-536, 2006.

[8] H.Chen, R. Cramer, S.Goldwasser, R.de Haan and V.Vaikuntanathan, Secure computation from random error-correcting codes, Proceedings of the Eurocrypt 2007, 291-310, 2007.

[9] H. Chen, S. Ling, C. Xing, Access Structures of Elliptic Secret Sharing Schemes, IEEE Transactions on Information Theory, vol. 54, no. 2, pp. 850-852, 2008.

[10] R. Cramer, I. Damgård and U. Maurer, General secure multi-party computation from any linear secret-sharing scheme, in: Advances in Cryptology – Eurocrypt 2000, Lecture Notes in Computer Science, vol. 1807, Springer, Heidelberg, pp. 316–334.

[11] R. Cramer, I. B. Damgård, and J. B. Nielsen, Secure Multiparty Computation and Secret Sharing, Cambridge University Press, 2015.

[12] R. Cramer, The arithmetic codex: Theory and applications, invited talk in Eurocrypt 2011.

[13] I. Damgård, Y. Ishai and M. KrØigaard, Perfect secure multiparty computation and the computational overhead of cryptography, Proceedings of Eurocrypt 2010, 445-465, 2010.

[14] I. Damgård and S. Zakarias, Constant-overhead secure computation of Boolean circuits using preprocessing, Proceedings of TCC 2013, 621-641, 2013.

[15] G. Frey and T. Lange, Background on Curves and Jacobians, Handbook of elliptic and hyperelliptic curve cryptography, Chap. 4 (H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, eds.), Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006.

[16] A. Garcia and H. Stichtenoth, A tower of Artin-Schreier extension of function fields attaining Drinfeld-Vladut bound, Invent. Math. 121(1) (1995), pp. 211-222.

[17] D. Harnik, Y. Ishai, E. Kushilevitz and J. B. Nielsen, OT-combiners via secure multiparty computation, Proceedings of TCC 2008, 393-411, 2009.

[18] R. Hartshorne, Algebraic Geometry, Springer, New York, 1977.

[19] Y. Ishai, E. Kushilevitz, R. Ostrovsky and A. Sahai, Zero-knowledge from secure multiparty computation, Proceedings of STOC 2007, 21-30, 2007.

[20] Y. Ishai, E. Kushilevitz, R. Ostrovsky and A. Sahai, Extracting correlations, Proceedings of FOCS 2009, 261-270, 2009.

[21] Y. Ishai, M. Prabhakaran and A. Sahai, Founding cryptography on oblivious transfer efficiently, Proceedings of Crypto 2008, 572-591, 2008.

[22] N. M. Katz, Twisted L-Functions and Monodromy, Annals of Mathematics Studies, vol. 150, Princeton University Press, Princeton, NJ, 2005.

[23] J. Li and D. Wan, Counting subset sums of finite abelian groups, Journal of Combinatorial Theory, Series A, vol. 119, no. 1, pp. 170-182, 2012.

[24] J. Li and D. Wan, Counting polynomial subset sums, Ramanujan J. 47, pp. 67-84, 2018.

[25] J. Li, D. Wan, J. Zhang, On the minimum distance of elliptic curve codes, Proceedings of the IEEE International Symposium on Information Theory (ISIT), pp. 2391-2395, 2015.

[26] J. L. Massey, Minimal codewords and secret sharing, Proc. 6th Joint Swedish-Russian Worksh. Inf. Theory, Molle, Sweden, Aug. 22-27, pp. 269-279, 1993.

[27] J. L. Massey, Some applications of coding theory in cryptography, Codes and Ciphers: Cryptography and Coding IV, P. G. Farrell, Ed. Essex, U.K.: Formara, pp. 33-47, 1995.

[28] R. J. McEliece and D. V. Sarwate, On sharing secrets and Reed-Solomon codes, Commun. ACM, vol. 22, no. 11, pp. 612-613, Nov. 1979.

[29] J. S. Milne, Jacobian varieties, Arithmetic Geometry, Chap. VII (G. Cornell and J. H. Silverman, eds.), Springer-Verlag, New York, 1986.

[30] H. Niederreiter and C. Xing, Algebraic Geometry in Coding Theory and Cryptography, Princeton Univ. Press, Princeton, NJ, 2009.

[31] M. Rosen, Number Theory in Function Fields, Graduate Texts in Mathematics, vol. 210, Springer, 2002.

[32] A. Shamir, How to share a secret, Commun. ACM 22, no. 11, 612-613, 1979.

[33] H. Stichtenoth, Algebraic function fields and codes. Graduate Texts in Mathematics, Vol. 254, Springer, 2009.

[34] M. Tsfasman, S. Vlăduț, D. Nogin, Algebraic Geometric Codes: Basic Notions, Math. Surveys Monogr., vol. 139, Amer. Math. Soc., Providence, RI, 2007.

[35] L. C. Washington. Elliptic curves: number theory and cryptography. 2nd edition, Chapman and Hall/CRC, 2008.