Efficient Multi-Point Local Decoding of Reed-Muller Codes via Interleaved Codex

Ronald Cramer, Chaoping Xing, and Chen Yuan

***Abstract*— Reed-Muller codes are among the most important classes of locally correctable codes. Currently local decoding of Reed-Muller codes is based on decoding on lines or quadratic curves to recover one single coordinate. To recover multiple coordinates simultaneously, the naive way is to repeat the local decoding for recovery of a single coordinate. This decoding algorithm might be more expensive, i.e., require higher query complexity. In this paper, we focus on Reed-Muller codes with usual parameter regime, namely, the total degree of evaluation polynomials is $d = \Theta(q)$, where q is the code alphabet size (in fact, d can be as big as $q/4$ in our setting). By introducing a novel variation of codex, i.e., interleaved codex (the concept of codex has been used for arithmetic secret sharing), we are able to locally recover arbitrarily large number k of coordinates of a Reed-Muller code simultaneously with error probability $\exp(-\Omega(k))$ at the cost of querying merely $O(q^2k)$ coordinates. It turns out that our local decoding of Reed-Muller codes shows (*perhaps surprisingly*) that accessing k locations is in fact cheaper than repeating the procedure for accessing a single location for k times. Precisely speaking, to get the same success probability by repeating the local decoding algorithm of a single coordinate, one has to query $\Omega(qk^2)$ coordinates. Thus, the query complexity of our local decoding is smaller for $k = \Omega(q)$. If we impose the same query complexity constraint on both algorithm, our local decoding algorithm yields smaller error probability when $k = \Omega(q^q)$. In addition, our local decoding is efficient, i.e., the decoding complexity is $\mathrm{Poly}(k, q)$. Construction of an interleaved codex is based on concatenation of a codex with a multiplication friendly pair, while the main tool to realize codex is based on algebraic function fields (or more precisely, algebraic geometry codes).**

***Index Terms*— Block codes, Reed-Muller codes, Local decoding.**

I. Introduction

IN TRANSMISSION of information over noisy channels or data storage, people are often interested in a portion of data. Thus, one needs to decode only this portion of data instead of the whole data set. However, classical error-correcting codes are generally designed to recover the whole information. Thus, this new application give rise to a special class of error-correcting codes, i.e., locally decodable (correctable) codes.

Although locally decodable (correctable) codes have been studied for about two decades, Reed-Muller codes and their variants are still among the most important classes of locally correctable codes. Therefore, the local decoding of Reed-Muller codes plays significant role in this topic. There are various decodings of Reed-Muller codes such as local decoding, list decoding or local list decoding in the literature [1], [4], [12], [17], [23], [24]. Among these decodings, there are basically two local decoding methods, i.e., decoding on lines and quadratic curves. Though decoding on quadratic curves can be generalized to decoding on high-degree curves, it does not appear in the literature. Almost all locally correctable codes including Reed-Muller codes focus on the recovery of one single coordinate [1], [3], [12], [17], [19], [20], [22], [27]. To recover multiple coordinates simultaneously, the naive way is to repeat these local decodings of single coordinate. However, this idea loses its attraction when one attempts to recover a large number of coordinates (see Subsection 1.5 below).

The current local decoding of Reed-Muller codes is based on decoding on lines or curves, i.e., randomly choose a line or a curve passing through a given point, then reduce it to the Reed-Solomon code decoding. Actually, in the PCP literature, one considers the projection of a codeword to a low-degree curve instead of line [21]. However, the decoding algorithm is eventually reduced to the decoding of Reed-Solomon codes again. Therefore, for a fixed alphabet size, one cannot read and decode as many coordinates as one wishes. Instead, one has to run a decoding algorithm multiple times which results in the increase of the error probability.

The main reason why the above local decoding of multiple points requires higher query complexity is due to the decoding of Reed-Solomon codes. A natural and promising alternative is to replace Reed-Solomon codes with algebraic geometry codes in the local decoding of multiple coordinates. Similar to the decoding of Reed-Solomon codes, we also want that our algebraic geometry codes have as much randomness as possible. The randomness of local decoding based on algebraic geometry code turns out to be closely related to the dual distance of this code. In this sense, one can locally recover multiple

Manuscript received May 18, 2018; revised August 19, 2019; accepted August 21, 2019. Date of publication September 3, 2019; date of current version December 23, 2019. R. Cramer and C. Yuan was supported by European Research Council (ECR) Advanced Grants (ADG) under Grant 74079 (ALGSTRONGCRYPTO).

R. Cramer is with the CWI, 1098XG Amsterdam, The Netherlands, and also with the Mathematical Institute, Leiden University, 2333CA Leiden, The Netherlands (e-mail: Ronald.Cramer@cwi.nl).

C. Xing is with the School of Electronics, Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: xingcp@sjtu.edu.cn).

C. Yuan is with CWI, 1098XG Amsterdam, The Netherlands (e-mail: Chen.Yuan@cwi.nl).

Communicated by A. Rudra, Associate Editor for Complexity.

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2019.2939135

coordinates of a Reed-Muller codeword simultaneously as long as there exists a good algebraic geometry code or a codex. Here, we use the concept codex [7] to capture the property we need in the local decoding. The construction of codex is through algebraic curves over finite fields (or more precisely algebraic geometry codes). As algebraic function fields with many rational places are usually defined over $\mathbb{F}_{q^2}$, the codex built from these function fields are also defined over $\mathbb{F}_{q^2}$. To overcome this obstacle, we present the concept interleaved codex. The interleaved codex is a concatenation of codex over $\mathbb{F}_{q^2}$ with a multiplication friendly pair that was first introduced in [10] to study multiplication of elements in extension fields of $\mathbb{F}_q$. Here, we refer to the term concatenation because one can treat the multiplication friendly pair as an inner code with multiplicative property and codex as an outer code. To our surprise, even for the Reed-Muller code defined over base field $\mathbb{F}_q$ with a square q, this concatenation technique leads to a local decoding algorithm with significantly larger decoding radius than applying the codex directly. We will see this in Section 4. Essentially our local decoding of multiple coordinates is based on the decoding of algebraic geometry codes which generalizes local decoding based on Reed-Solomon codes. However, this generalization is by no means trivial. In fact, several sophisticated algebraic tools are used to achieve our local decoding goal.

In this paper, we consider local decoding of Reed-Muller codes with the usual parameter regime, i.e., $d = \Theta(q)$, where q is the code alphabet size (in fact, d can be as big as $q/4$ in our setting). As a main consequence of our local decoding, we are able to locally recover arbitrarily large number k coordinates of a Reed-Muller code simultaneously with error probability $\exp(-\Omega(k))$ at the cost of querying merely $O(q^2k)$ coordinates. This is not achievable by all other existing local decodings of Reed-Muller codes. For instance, to get the same success probability from repetition of local decoding for recovery of a single coordinate, one has to query $\Omega(qk^2)$ coordinates. Thus, the query complexity of our local decoding is smaller for $k = \Omega(q)$. Furthermore, our local decoding is efficient, i.e., the decoding complexity is $\mathrm{Poly}(k, q)$. Our local decoding also works for the recovery of one single coordinate as well. In this case, there is a trade-off between code dimension and success probability.

In the literature, there is a construction of locally decodable (correctable) codes via algebraic function fields (or algebraic curves) with large automorphism groups [3], [14]. However, usage of algebraic curves in this paper is not for purpose of constructing locally correctable codes, but for local decoding of Reed-Muller codes.

A. Locally Correctable Codes

To better state our result, let us introduce locally correctable codes first.

Definition 1.1: A subset C of $\mathbb{F}_q^N$ is called a q-ary (r, δ, ϵ)-locally correctable code of length N if there exists a randomized algorithm $\mathcal{A}$ such that (i) for any $i \in [N]$ and $\mathbf{c} \in C$, $\mathbf{y} \in \mathbb{F}_q^N$ with $\mathrm{wt}_H(\mathbf{c}, \mathbf{y}) \le \delta N$, one has $\Pr[\mathcal{A}^{\mathbf{y}}(i) = c_i] \ge 1-\epsilon$, where the probability is taken over random coin tosses of the algorithm $\mathcal{A}$ (note that c_i stands for the i-th coordinate of $\mathbf{c}$ and $\mathcal{A}^{\mathbf{y}}(i)$ stands for the output of $\mathcal{A}$ from $\mathbf{y}$ for the position at i); (ii) $\mathcal{A}$ makes at most r queries to $\mathbf{y}$.

The above definition is only for recovery of one single coordinate (or point). We can generalize it to a locally correctable code with recovery of multiple coordinates (or points).

Definition 1.2: A subset C of $\mathbb{F}_q^N$ is called a q-ary $(k; r, \delta, \epsilon)$-locally correctable code of length N if there exists a randomized algorithm $\mathcal{A}$ such that (i) for any $S \subseteq [N]$ with $|S| \le k$, and $\mathbf{c} \in C$, $\mathbf{y} \in \mathbb{F}_q^N$ with $\mathrm{wt}_H(\mathbf{c}, \mathbf{y}) \le \delta N$, one has $\Pr[\mathcal{A}^{\mathbf{y}}(S) = \mathbf{c}_S] \ge 1 - \epsilon$, where the probability is taken over random coin tosses of the algorithm $\mathcal{A}$ (note that $\mathbf{c}_S$ stands for the projection of $\mathbf{c}$ to S and $\mathcal{A}^{\mathbf{y}}(S)$ stands for the output of $\mathcal{A}$ from $\mathbf{y}$ for the positions at S); (ii) $\mathcal{A}$ makes at most r queries to $\mathbf{y}$.

Thus, a $(1; r, \delta, \epsilon)$-locally correctable code is an (r, δ, ϵ)-locally correctable code.

B. Reed-Muller Codes

We denote by $\mathbf{x}$ the variable vector $(x_1, \dots, x_m)$. The multivariate polynomial ring $\mathbb{F}_q[x_1, \dots, x_m]$ is denoted by $\mathbb{F}_q[\mathbf{x}]$. For a vector $I = (e_1, \dots, e_m) \in \mathbb{Z}^m_{\ge 0}$, we denote by $\mathbf{x}^I$ the monomial $\prod_{i=1}^m x_i^{e_i}$. Thus, we can write a polynomial of total degree at most d by $f(\mathbf{x}) = \sum_{\mathrm{wt}_L(I) \le d} a_I \mathbf{x}^I$, where $a_I \in \mathbb{F}_q$ and $\mathrm{wt}_L(I) = \sum_{i=1}^m e_i$ is the Lee weight. A polynomial in $\mathbb{F}_q[\mathbf{x}]$ is called a degree-d polynomial if its total degree is at most d. In the setting throughout the paper, we assume that $d < q$.

Definition 1.3: The Reed-Muller code $\mathrm{RM}(q, d, m)$ is defined by $\{(f(\mathbf{u}))_{\mathbf{u} \in \mathbb{F}_q^m} : f(\mathbf{x}) \in \mathbb{F}_q[\mathbf{x}];\ \deg(f(\mathbf{x})) \le d\}$, where $\deg(f(\mathbf{x}))$ denotes the total degree of $f(\mathbf{x})$.

The dimension of the Reed-Muller code $\mathrm{RM}(q, d, m)$ is $\binom{m+d}{d}$. Currently, the two most popular parameter regimes for locally decoding Reed-Muller codes are either constant d or $d \le \sigma q$ for some constant $0 < \sigma < 1$. In this paper, we focus on the latter case.

C. Known Results

The simplest local decodings of Reed-Muller codes is called decoding on lines [27, Proposition 2.5]. The decoding on line can be generalized to decoding on quadratic curves [27, Proposition 2.6]. Both decodings are very special cases of our codex decoding where a Reed-Solomon code with pairwise independent variables is used (see Example 4.1(i) and (ii)).

Proposition 1.4: Let $0 < \sigma, \delta < 1$ be positive real. Let m and d be positive integers. Let q be a prime power.

(i) If $d \le \sigma(q-1) - 1$, then the Reed-Muller code $\mathrm{RM}(q, d, m)$ is $(q-1, \delta, 2\delta/(1-\sigma))$-locally correctable for all positive real with $\delta < \frac{1-\sigma}{2}$.

(ii) If $d \le \sigma(q-1) - 1$, then the Reed-Muller code $\mathrm{RM}(q, d, m)$ is $\left(q-1, \delta, \epsilon = O\left(\frac{\gamma_{\sigma,\delta}}{q}\right)\right)$-locally correctable for all positive real with $\delta < \frac{1-2\sigma}{2}$, where $\gamma_{\sigma,\delta} = \frac{\delta-\delta^2}{1-2\sigma-2\delta}$.

The purpose of (ii) in Proposition 1.4 is to increase the success probability of local decoding. As σ, δ are constant and q is usually large, Proposition 1.4(ii) gives much better success probability at the cost of a slightly smaller local decoding radius.

Although it does not appear in the literature, generalization of local decoding on quadratic curves is quite straightforward in the following way. Assume that $f(\mathbf{u})_{\mathbf{u}\in\mathbb{F}_q^m}$ is transmitted and we want to recover $f(\mathbf{w})$ at position $\mathbf{w}$. Choose t independently random vectors $\mathbf{v}_1, \ldots, \mathbf{v}_t$ and consider the degree t curve $\mathbf{w} + \sum_{i=1}^t x^i \mathbf{v}_i$. By using the error probability bound for t-wise independence (see Lemma 2.12), we obtain the result on local decoding using higher degree curves (see Example 4.1(iii)).

D. Our Results

This paper mainly focuses on multiple point local decoding although single point local decoding is considered as well.

For local decoding to recover multiple coordinates, we only state the result based on the Garcia-Stichtenoth tower though all three classes of codes, namely Reed-Solomon codes, Hermitian codes and algebraic geometry codes from the Garcia-Stichtenoth tower are discussed in this paper. We refer to Theorem 4.7(i)-(iv) for local decoding of recovering multiple coordinates based on Reed-Solomon and Hermitian codes.

Theorem 1.5: Let q be a prime power. Let $d > 1, m, k$ be positive integers. Let δ, σ be two reals in (0, 1) with $\delta < \frac{1-4\sigma}{2}$ and $d < \sigma q$. Then the Reed-Muller code $\mathrm{RM}(q, d, m)$ is $\left(k; q^2 k, \delta, O\left(\left(\frac{\mu_{\delta,\sigma}}{\sqrt{q}}\right)^k\right)\right)$-locally correctable, where $\mu_{\delta,\sigma} = \frac{\sqrt{8}}{1-4\sigma-2\delta}$ (note that k can be arbitrarily large). Furthermore, the decoding algorithm is efficient, i.e., the decoding time complexity is $\mathrm{Poly}(k, q)$.

E. Comparison

Let us compare our results given in Subsection I-D with the known results (or those derived from the known results).

(i) To obtain a k-multiple point local decoding from the single point decoding given in Proposition 1.4(ii), one can repeat local decoding k times to get a $(k; qk, \delta, \epsilon)$-locally correctable code with $\epsilon = O_{\sigma,\delta}\left(\frac{k}{q}\right)$. Therefore, this method does not work when $k > q$.

(ii) The other way is to first repeat local decoding to correct $f(\mathbf{u})$ at the same point $\mathbf{u}$ to increase probability, and then repeat the above procedure to correct multiple points with meaningful probability. Let us analyze this decoding idea in detail. To increase decoding success probability of the local decoding in Proposition 1.4(ii), we can repeat local correction of $f(\mathbf{u})$ at $\mathbf{u}$ for s times. Denote by Y_i a binary random variable such that $Y_i = 1$ if the local decoding algorithm outputs a wrong answer in the i-th round and $Y_i = 0$ otherwise. It follows from Proposition 1.4(ii) that $\Pr[Y_i = 1] = b = O\left(\frac{\gamma_{\sigma,\delta}}{q}\right)$. Thus, we have

$$\Pr\left[\sum_{i=1}^{s} Y_i \geq \frac{s}{2}\right] = \sum_{i\geq s/2} \binom{s}{i} b^i (1-b)^{s-i}$$
$$= O\left(\left(\frac{4\gamma_{\sigma,\delta}}{q}\right)^{s/2}\right). \quad \text{(I.1)}$$

Therefore, we conclude that the Reed-Muller code $\mathrm{RM}(q, d, m)$ is (qs, δ, ϵ')-locally correctable, where ϵ' is given in (I.1). By repeating the above decoding procedure to correct k points, we can also conclude that the Reed-Muller code $\mathrm{RM}(q, d, m)$ is $(k; kqs, \delta, k\epsilon')$-locally correctable.

(iii) The k-multiple point local decodings in Theorem 1.5 does not impose any constraint on the size of k. This means that we can recover k coordinates simultaneously with a high probability no matter how large k is. Meanwhile, the number of queries is $O(q^2 k)$. To the best of our knowledge, this is by no means possible for any other known local decoding.

  (a) By repeating the local decoding described in (ii), to correct k points with the same success probability $1 - O\left(\left(\frac{\mu_{\sigma,\delta}}{\sqrt{q}}\right)^k\right)$ as in Theorem 1.5, s in (I.1) has to be $\Omega(k)$. The decoding algorithm discussed in the above (ii) then requires the query complexity $\Omega(qk^2)$. Therefore, for $k = \Omega(q)$, our local decoding of Reed-Muller codes in Theorem 1.5 with query complexity $O(q^2 k)$ is cheaper than repeating the procedure for accessing a single location for k times.

  (b) Even for an unfair comparison, namely, in order to get a meaningful success probability $> \frac{2}{3}$ by repeating local decoding of a single location for s times, s in (I.1) has to be $\Omega(\log k / \log q)$. Thus, the decoding algorithm discussed in the above (ii) requires the query complexity $\Omega(qk \log k / \log q)$. In this case, our local decoding of Reed-Muller codes in Theorem 1.5 is still cheaper than repeating the procedure for accessing a single location for k times if $k = \Omega(q^q)$. This parameter regime is meaningful when the Reed-Muller code is defined over a fixed finite field and its message polynomial has $\geq q$ variables.

F. Our Techniques

Let $f(\mathbf{x})$ be a degree d m-variate polynomial. The codeword of Reed-Muller code associated with $f(\mathbf{x})$ is $(f(\mathbf{u}))_{\mathbf{u}\in\mathbb{F}_q^m}$, i.e., the evaluation of $f(\mathbf{x})$ at each point in $\mathbb{F}_q^m$. We want to recover $f(\mathbf{w})$ at the point $\mathbf{w} = (w_1, \ldots, w_m)$. In the curve decoding, one replaces $(x_1, \ldots, x_m)$ by $\mathbf{w} + \lambda\mathbf{u}_1 + \lambda^2\mathbf{u}_2$ for some random vectors $\mathbf{u}_1 = (u_{11}, \ldots, u_{1m}), \mathbf{u}_2 = (u_{21}, \ldots, u_{2m}) \in \mathbb{F}_q^m$ (i.e., replace x_i by $w_i + u_{1i}\lambda + u_{2i}\lambda^2$ for $i = 1, 2, \ldots, m$). Then the function $f(\mathbf{w} + \lambda\mathbf{u}_1 + \lambda^2\mathbf{u}_2)$ becomes a univariate polynomial of degree at most $2d$. Thus, one can decode it via Reed-Solomon codes. In the curve decoding, we can let $g(\lambda) = \mathbf{w} + \lambda\mathbf{u}_1 + \lambda^2\mathbf{u}_2$ pass through two given coordinates. Meanwhile, $g(\lambda)$ is still a random curve since we need three coordinates to fix it. That means we can make use of high-degree curve to achieve both multiple-point decoding and low error probability as long as the decoding radius is still beyond the error rate. The degree of this curve can also be interpreted as the dual distance of the Reed-Solomon code. This observation leads to the local decoding algorithm based on algebraic geometry code.

Let us replace x_i with z_i for some function z_i in some Riemann-Roch space $\mathcal{L}(G)$ with an effective divisor G of an algebraic curve with many rational points. Then $f(z_1, \ldots, z_m)$ becomes a function in the Riemann-Roch space $\mathcal{L}(dG)$ and thus one can recover the function $f(z_1, \ldots, z_m)$ by using decoding of algebraic geometry codes. If we want to recover $f(\mathbf{w}_i)$ for $i = 1, 2, \ldots, k$, we can simply take some rational points $Q_1, \ldots, Q_k$ on this curve such that $(z_1(Q_i), \ldots, z_m(Q_i))$ are equal to $\mathbf{w}_i$ for all $1 \le i \le k$. Assume that the dual distance of this algebraic geometry codes is t. Then, we can recover $k < t$ given coordinates $\mathbf{w}_i$ for $1 \le i \le k$ and use the rest of $t-k$ coordinates to reduce the error probability. A direct generalization requires us to go deeply into the details of algebraic geometry codes. Thus, we introduce the concept codex in [6], [7]. The function of codex serves all the purposes of local decoding without knowing what happens inside, i.e., (i) a codex has high randomness and uniformity; (ii) a codex provides independent variables that are needed in local decoding of Reed-Muller codes; (iii) a codex also allows correction of errors.

On the other hand, as far as we know, the only way to construct codex is through algebraic curves with many rational points (or more precisely algebraic geometry codes). We introduce three classes of curves, i.e., projective line, Hermitian curve and the Garcia-Stichtenoth tower, to construction of codex and realize our local decoding. Since a good asymptotic tower is usually defined over $\mathbb{F}_{q^2}$, the codex built from such a tower is also defined over $\mathbb{F}_{q^2}$. Thus, we have to reduce the field size from q^2 to q. Our technique to achieve this reduction is concatenation of codex via multiplication friendly pairs. The multiplication friendly pairs that we employ are simply from Reed-Solomon codes. As for error probability, we make use of the error probability bound for t-wise linearly independent variables given in [2].

G. Organization

The paper is organized as follows. In Section 2, we introduce some preliminaries including definitions of codex and interleaved codex, a construction of codex through algebraic geometry codes, construction of interleaved codex, error probability bounds and introduction to Hermitian curves the Garcia-Stichenoth tower. Our local decoding algorithms of Reed-Muller codes through codex and interleaved codex are presented in Section 3. Finally we apply various codices to decoding algorithms in Section 3 to obtain our main results in Section 4.

II. Preliminaries

A. Codex

The concept of codex was first introduced in [6], [7], [9] for the purpose of arithmetic secret sharing. A special case of codex in this paper was implicitly introduced in [5], [8].

Let $\mathbb{F}_q$ be a finite field of q elements. $\mathbb{F}_q^*$ denotes the multiplicative group of $\mathbb{F}_q$. Let n, t, d, r be positive integers with $d \ge 2$ and $1 \le t < r \le n$. Vectors in the $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$ are denoted in boldface. If $\mathbf{u} \in \mathbb{F}_q^n$, its coordinates are denoted as $(u_i)_{i=1}^n$. Define $\mathbf{1} = (1, \ldots, 1) \in \mathbb{F}_q^n$. The standard inner-product on $\mathbb{F}_q^n$ is denoted $\langle \cdot, \cdot \rangle$. If $A \subset \{1, \ldots, n\}$ is non-empty, π_A denotes projection of $\mathbb{F}_q^n$ onto the A-indexed coordinates, i.e., $\pi_A(\mathbf{u}) = (u_i)_{i \in A}$ for all $\mathbf{u} \in \mathbb{F}_q^n$.

Definition 2.1: For $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, $\mathbf{u} * \mathbf{v}$ denotes the vector $(u_1 v_1, \ldots, u_n v_n) \in \mathbb{F}_q^n$. For an $\mathbb{F}_q$-linear code $C \subset \mathbb{F}_q^n$, the $\mathbb{F}_q$-linear code $C^{*d} \subset \mathbb{F}_q^n$, the *$d$-th power of C*, is defined as the $\mathbb{F}_q$-linear subspace generated by all terms of the form $\mathbf{c}_1 * \cdots * \mathbf{c}_d$ with $\mathbf{c}_1, \ldots, \mathbf{c}_d \in C$.

Note that if $\mathbf{1} \in C$, then $C = C^{*1} \subset C^{*2} \subset \ldots \subset C^{*d}$.

Consider the following special case of an arithmetic secret sharing scheme (SSS for short) which, in turn, is a special case of an arithmetic codex [7].

Definition 2.2: An $(n, t, d, r; \mathbb{F}_q^k/\mathbb{F}_q)$-codex is a pair (C, ψ) such that the following conditions are satisfied:

(i) $C \subset \mathbb{F}_q^n$ is an $\mathbb{F}_q$-linear code and $\psi : C \longrightarrow \mathbb{F}_q^k$ is a surjective $\mathbb{F}_q$-linear map.

(ii) It is *unital*, i.e., $\mathbf{1} \in C$ and $\psi(\mathbf{1}) = \mathbf{1}$.

(iii) (*t-privacy with uniformity*) For each $A \subset \{1, \ldots, n\}$ with $|A| = t$, the projection map

$$\mathrm{proj}_{\psi,A} : C \longrightarrow \mathbb{F}_q^k \times \mathbb{F}_q^t, \quad \mathbf{c} \mapsto (\psi(\mathbf{c}), \mathrm{proj}_A(\mathbf{c}))$$

is surjective, where $\mathrm{proj}_A(\mathbf{c})$ is the projection of $\mathbf{c}$ at A.

(iv) (*(d, r)-product reconstruction*) The map ψ extends uniquely to an $\mathbb{F}_q$-linear map $\psi : C^{*d} \longrightarrow \mathbb{F}_q^k$ such that the following holds.

(a) ψ satisfies the multiplicative relation

$$\psi(\mathbf{c}_1 * \cdots * \mathbf{c}_d) = \psi(\mathbf{c}_1) * \cdots * \psi(\mathbf{c}_d) \in \mathbb{F}_q^k,$$

for all $\mathbf{c}_1, \ldots, \mathbf{c}_d \in C$.

(b) C^{*d} has minimum distance at least $n-r+1$. Thus, ψ is r-wise determined, i.e., $\psi(\mathbf{z}) = \mathbf{0}$, for all $\mathbf{z} \in C^{*d}$ with $\mathrm{proj}_B(\mathbf{z}) = \mathbf{0}$ for some $B \subset \{1, \ldots, n\}$ with $|B| = r$.

Remark 2.3: (i) *Uniqueness* of ψ in (iv) is not required separately, as it is implied by existence. Also note that, in fact, $\psi(\mathbf{c}_1 * \cdots * \mathbf{c}_{d'}) = \psi(\mathbf{c}_1) * \cdots * \psi(\mathbf{c}_{d'})$ for all $\mathbf{c}_1, \ldots, \mathbf{c}_{d'} \in C$ and all integers d' with $1 \le d' \le d$.

(ii) Given the above codex, we can define an arithmetic SSS, where each coordinate of $\mathbf{c}$ is a share and $\psi(\mathbf{c})$ is the secret (please refer to [7] for the details).

For the purpose of our local decoding, we have to introduce a variant of the above codex, i.e., interleaved codex.

Definition 2.4: An $(n, \ell, t, d, r; \mathbb{F}_q^k/\mathbb{F}_q)$-interleaved codex is a pair (C, φ) such that the following conditions are satisfied:

(i) $C \subset \mathbb{F}_q^{n\ell}$ is an $\mathbb{F}_q$-linear code and $\varphi : C \longrightarrow \mathbb{F}_q^k$ is a surjective $\mathbb{F}_q$-vector space morphism.

(ii) It is *unital*, i.e., $\mathbf{1} \in C$ and $\varphi(\mathbf{1}) = \mathbf{1}$.

(iii) (*weak t-privacy with uniformity*) Let the coordinate of C be indexed by pairs $(i, j) \in [n] \times [\ell]$, i.e., every codeword is written as $(c_{ij})_{1 \le i \le n; 1 \le j \le \ell}$. Then for each $1 \le j \le \ell$ and each $A \subset \{(1, j), \ldots, (n, j)\}$ with $|A| = t$, the projection map

$$\mathrm{proj}_{\varphi,A} : C \longrightarrow \mathbb{F}_q^k \times \mathbb{F}_q^t, \quad \mathbf{c} \mapsto (\varphi(\mathbf{c}), \mathrm{proj}_A(\mathbf{c}))$$

is surjective.

(iv) (*(d,r)-product reconstruction*) The map φ extends uniquely to an $\mathbb{F}_q$-linear map $\varphi : C^{*d} \longrightarrow \mathbb{F}_q^k$ such that the following holds.

(a) φ satisfies the multiplicative relation

$$\varphi(\mathbf{c}_1 * \cdots * \mathbf{c}_d) = \varphi(\mathbf{c}_1) * \cdots * \varphi(\mathbf{c}_d) \in \mathbb{F}_q^k,$$

for all $\mathbf{c}_1, \ldots, \mathbf{c}_d \in C$.

(b) C^{*d} has minimum distance at least $n-r+1$. Thus, φ is r-wise determined, i.e., $\varphi(\mathbf{z}) = \mathbf{0}$, for all $\mathbf{z} \in C^{*d}$ with $\mathrm{proj}_B(\mathbf{z}) = \mathbf{0}$ for some $B \subset [n] \times [\ell]$ with $|B| = r$.

B. A Construction of Codex

As far as we know, the only way to construct codex with $t = \Omega(n)$ is through algebraic geometry codes. In this subsection, we briefly introduce algebraic geometry codes and show how to construct codex.

For the convenience of reader, we start with some definitions and notations. The reader may refer to [25], [26].

An *algebraic function field* over $\mathbb{F}_q$ in one variable is a field extension $F \supset \mathbb{F}_q$ such that F is a finite algebraic extension of $\mathbb{F}_q(x)$ for some $x \in F$ that is transcendental over $\mathbb{F}_q$. It is assumed that $\mathbb{F}_q$ is its full field of constants, i.e., $\bar{\mathbb{F}}_q \cap F = \mathbb{F}_q$.

Let $\mathbb{P}_F$ denote the set of places of F. A divisor is a formal sum $G = \sum_{P \in \mathbb{P}_F} a_P P$, where a_P are integers and are equal to zero except for finitely many P. For a divisor G of F, we define the Riemann-Roch space by $\mathcal{L}(G) := \{f \in F^* : \mathrm{div}(f) + G \geq 0\} \cup \{0\}$. Then $\mathcal{L}(G)$ is a finite dimensional space over $\mathbb{F}_q$ and its dimension $\dim_{\mathbb{F}_q}(\mathcal{L}(G))$ is determined by the Riemann-Roch theorem which gives

$$\dim_{\mathbb{F}_q} \mathcal{L}(G) = \deg(G) + 1 - g(F) + \ell(K - G),$$

where K is a canonical divisor of degree $2g(F) - 2$, and $g(F)$ is the genus of F. Therefore, we always have that $\dim_{\mathbb{F}_q}(\mathcal{L}(G)) \geq \deg(G) + 1 - g(F)$ and the quality holds if $\deg(G) \geq 2g(F) - 1$.

Let k, t, n be positive integers. Suppose $Q_1, \ldots, Q_k, P_1 \ldots, P_n$ are distinct rational places of a function field F and denote by $\mathcal{Q}$ and $\mathcal{P}$ the set $\{Q_1, \ldots, Q_k\}$ and $\{P_1, \ldots, P_n\}$, respectively. Let G be a divisor of F such that $\mathrm{Supp}(G) \cap (\mathcal{P} \cup \mathcal{Q}) = \emptyset$. We define an algebraic geometry code of length $k+n$ as follows

$$C(G; \mathcal{Q}+\mathcal{P}) = \{(f(Q_1), \ldots, f(Q_k), f(P_1), \ldots, f(P_n) : f \in \mathcal{L}(G))\} \subseteq \mathbb{F}_q^k \times \mathbb{F}_q^n.$$

We also denote by $C(G; \mathcal{P})$ the code obtained from $C(G; \mathcal{Q}+\mathcal{P})$ by puncturing the first k positions.

Proposition 2.5: Let F be a function field of genus $g(F)$ with two disjoint sets $\mathcal{Q} = \{Q_1, \ldots, Q_k\}$ and $\mathcal{P} = \{P_1, \ldots, P_n\}$ of rational places. Let $t \geq 1, d \geq 2, r \geq 1$ satisfy $n \geq r > d(2g(F)+k+t-1)$. For a positive divisor G with $\deg(G) = 2g(F)+k+t-1$ and $\mathrm{Supp}(G) \cap (\mathcal{P} \cup \mathcal{Q}) = \emptyset$, let C be the code $C(G; \mathcal{P})$ and define the map ψ from C to $\mathbb{F}_q^k$ given by $(f(P_1), \ldots, f(P_n)) \mapsto (f(Q_1), \ldots, f(Q_k))$ (note that the function f is uniquely determined by $(f(P_1), \ldots, f(P_n))$). Then (C, ψ) is an $(n, t, d, r; \mathbb{F}_q^k/\mathbb{F}_q)$-codex.

PROOF. It is clear that ψ is $\mathbb{F}_q$-linear and unital. To prove that ψ is a surjective, we consider the kernel of ψ. The kernel clearly has dimension $\dim_{\mathbb{F}_q}(\mathcal{L}(G - \sum_{i=1}^k Q_i))$ which is equal to $\deg(\mathcal{L}(G)) - k - g(F) + 1$ by the Riemann-Roch Theorem. Thus, the image of ψ has dimension $\dim_{\mathbb{F}_q}(G) - (\deg(G) - k - g(F) + 1) = k$. This implies that ψ is surjective. As $\deg(G) - (t+k) = 2g(F) - 1$, one can show t-privacy with uniformity in the same way.

Finally, we verify that it is (d,r)-product reconstruction. For a function $f \in \mathcal{L}(G) \subseteq F$, we denote by $\mathbf{b}_f$ and $\mathbf{c}_f$ the words $(f(Q_1), \ldots, f(Q_k))$ and $(f(P_1), \ldots, f(P_n))$, respectively. Thus, one has $\psi(\mathbf{c}_f) = \mathbf{b}_f$ for any $f \in \mathcal{L}(G)$. Furthermore, for d codewords $\mathbf{c}_{f_1} * \cdots * \mathbf{c}_{f_d}$ in $C(G, \mathcal{P})$ we have $\psi(\mathbf{c}_{f_1} * \cdots * \mathbf{c}_{f_d}) = \psi(\mathbf{c}_{f_1 \cdots f_d}) = \mathbf{b}_{f_1 \cdots f_d} = \mathbf{b}_{f_1} * \cdots * \mathbf{b}_{f_d} = \psi(\mathbf{c}_{f_1}) * \cdots * \psi(\mathbf{c}_{f_d})$. Now for $\mathbf{z} \in C^{*d}$, we have $\mathbf{z} \in C(dG, \mathcal{P})$. Thus, there exists a function $h \in \mathcal{L}(dG)$ such that $\mathbf{z} = \mathbf{c}_h$. If $\pi_B(\mathbf{z}) = 0$, i.e., $h \in \mathcal{L}(dG - \sum_{i \in B} P_i)$, then we must have $h = 0$ since $d \deg(G) < r = |B|$. Hence, $\psi(\mathbf{z}) = \mathbf{0}$. This completes the proof. $\triangle$

Example 2.6: Consider the rational function field $F = \mathbb{F}_q(x)$, then $g(F) = 0$. Let $\mathcal{Q}$ and $\mathcal{P}$ be the set $\{0\}$ and $\mathbb{F}_q \setminus \{0\}$. In this case, $k = 1$ and $n = q - 1$.

(i) Choose $t = 1$, then for any $1 < d < r \leq q-1$, there exists is a $(q-1, 1, d, r; \mathbb{F}_q/\mathbb{F}_q)$-codex.

(ii) Choose $t = 2$, then for any $1 < 2d < r \leq q-1$, there exists is a $(q-1, 2, d, r; \mathbb{F}_q/\mathbb{F}_q)$-codex.

C. Concatenation of Codex

As algebraic function fields with many rational places are usually defined over $\mathbb{F}_{q^2}$, the codex constructed from function fields in the previous subsection is defined over $\mathbb{F}_{q^2}$ as well. Thus, we have to reduce the field size form q^2 to q through concatenation. In order to concatenate codex over $\mathbb{F}_{q^2}$, we need to introduce the following multiplication friendly pair. Multiplication friendly pairs were first introduced by D.V. Chudnovsky and G.V. Chudnovsky [10] as bilinear multiplication algorithms to study multiplication complexity in extension fields. In fact, a multiplication friendly pair is a special codex. The reader may refer to [9] for details.

Definition 2.7: A pair (π, ϕ) is called a $(d,k,m)_q$-multiplication friendly pair if π is an $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q^m$ and ϕ is an $\mathbb{F}_q$-linear map from $\mathbb{F}_q^m$ to $\mathbb{F}_{q^k}$ such that $\pi(1) = (1, \ldots, 1)$ and $\phi(\pi(\alpha_1) * \cdots * \pi(\alpha_d)) = \alpha_1 \cdots \alpha_d$ for all $\alpha_i \in \mathbb{F}_q$. A $(2,k,m)_q$-multiplication friendly pair is also called a bilinear multiplication friendly pair.

It is well known that, for a multiplication friendly pair (π, ϕ), the map π is injective (see [15, Lemma 3.1] for instance). Furthermore, by using Reed-Solomon codes, one can construct the following multiplication friendly pair (see [15, Lemma 3,2 and Example 3.3]).

Lemma 2.8: If $k \geq 2$ and $q > d(k-1)$, then there exists a $(d,k,q)_q$-multiplication friendly pair (π, ϕ) such that $(\pi(\mathbb{F}_{q^k}))^{*d}$ is a q-ary linear code of length m and relative minimum distance at least $1 - d(k-1)/q$.

In fact, this multiplication friendly pair (π, ϕ) is obtained from a $[q, d, q-d+1]$ Reed-Solomon code. Now, we proceed to concatenate a codex over $\mathbb{F}_{q^2}$ with a multiplication friendly pair given in Lemma 2.8. Note that the concatenated codex, if we disregard the multiplicative property, is merely a concatenation of two codes.

Proposition 2.9: Given an $(n, t, d, r; \mathbb{F}_{q^2}^k/\mathbb{F}_{q^2})$-codex, one can construct an $(n, q, t, d, dn + qr; \mathbb{F}_{q^2}^k/\mathbb{F}_{q^2})$-interleaved codex in time $\mathrm{Poly}(n, q)$.

PROOF. Let (C, ψ) be an $(n, t, d, r; \mathbb{F}_{q^2}^k/\mathbb{F}_{q^2})$-codex. By Lemma 2.8, we have a $(d, 2, q)_q$-multiplication friendly pair (π, ϕ). This multiplication friendly pair is obtained via a $[q, 2, q-1]$ Reed-Solomon code. We extend π to an $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^2}^s$ to $\mathbb{F}_q^{qs}$ by defining $\pi(v_1, \ldots, v_s) = (\pi(v_1), \ldots, \pi(v_s))$ for every $s \geq 1$. Then it is clear that π is injective on $\mathbb{F}_{q^2}^s$.

Put $C_1 = \pi(\psi^{-1}(\mathbb{F}_q^k)) \subseteq \mathbb{F}_q^{qn}$. Then $\pi^{-1}(C_1) = \psi^{-1}(\mathbb{F}_q^k)$ since π is injective. For a codeword $\mathbf{c} = (c_1, \ldots, c_n) \in C$, we denote $\pi(c_i)$ by $(c_{i,1}, \ldots, c_{i,q})$. Thus, a codeword $\pi(\mathbf{c})$ of C_1 has coordinates indexed by pairs $(i, j) \in [n] \times [q]$.

Consider the maps

$$C_1 = \pi(\psi^{-1}(\mathbb{F}_q^k)) \xrightarrow{\pi^{-1}} \psi^{-1}(\mathbb{F}_q^k) \xrightarrow{\psi} \mathbb{F}_q^k.$$

Let φ be the composition map $\psi \circ \pi^{-1}$. Then it is clear that φ is an $\mathbb{F}_q$-linear map from C_1 to $\mathbb{F}_q^k$. We claim that the pair (C_1, φ) is the interleaved codex with desired parameters.

It is clear that φ is surjective.

As π maps 1 to the all-one vector of length q and the all-one vector of length n belongs to C, we conclude that the all-one vector $\mathbf{1}$ of length qn belongs to C_1. From the definition of φ, we clearly have $\varphi(\mathbf{1}) = \mathbf{1}$.

To show t-weak privacy, let $(\mathbf{u}, \mathbf{v})$ be a vector of $\mathbb{F}_q^k \times \mathbb{F}_q^t$. Then there is a vector $\mathbf{v}' \in \mathbb{F}_{q^2}^t$ such that $\mathrm{proj}_j \circ \pi(\mathbf{v}') = \mathbf{v}$, where proj_j is the projection map of $\mathbb{F}_q^q$ at position j. Let $\mathbf{b} \in C$ such that $(\psi(\mathbf{b}), \mathrm{proj}_B(\mathbf{b})) = (\mathbf{u}, \mathbf{v}')$ with $B = \{1 \leq i \leq n : (i, j) \in A\}$. Then $\mathbf{b}$ belongs to $\psi^{-1}(\mathbb{F}_q^k)$. Now it is easy to verify that $(\varphi(\mathbf{c}), \mathrm{proj}_A(\mathbf{c})) = (\mathbf{u}, \mathbf{v})$, where $\mathbf{c} = \pi(\mathbf{b})$.

Now, we move to proof of the multiplication property. Note that ϕ is equal to π^{-1} when restricted to $\pi(\mathbb{F}_{q^2})$. Thus, we can extend π^{-1} to a map from $\mathbb{F}_q^{qn}$ to $\mathbb{F}_{q^2}^n$ via replacement of π^{-1} by ϕ. Thus, φ is equal to $\psi \circ \phi$ on C_1. Hence, φ can be extended to a map from C_1^{*d} to $\mathbb{F}_q^k$.

For d vectors $\pi(\mathbf{c}_1), \ldots, \pi(\mathbf{c}_d) \in C_1$ with $\mathbf{c}_i \in \psi^{-1}(\mathbb{F}_q^k) \subset C$, we have

$$\begin{aligned}
& \varphi(\pi(\mathbf{c}_1) * \cdots * \pi(\mathbf{c}_d)) \\
= \; & (\psi \circ \phi)(\pi(\mathbf{c}_1) * \cdots * \pi(\mathbf{c}_d)) \\
= \; & \psi(\mathbf{c}_1 * \cdots * \mathbf{c}_d) = \psi(\mathbf{c}_1) * \cdots * \psi(\mathbf{c}_d) \\
= \; & (\psi \circ \phi(\pi(\mathbf{c}_1))) * \cdots * (\psi \circ \phi(\pi(\mathbf{c}_d))) \\
= \; & \varphi(\pi(\mathbf{c}_1)) * \cdots * \varphi(\pi(\mathbf{c}_d)).
\end{aligned}$$

Finally, note that C_1 is the concatenated code of C with a $[q, 2, q-1]$-Reed-Solomon code. Since C^{*d} has minimum distance at least $n-r+1$ and $\pi(\mathbb{F}_{q^2})^{*d}$ has minimum distance at least $q-d$, we conclude that the minimum distance of C_1^{*d} is at least $(n-r+1)(q-d) \geq qn - (dn+qr) + 1$. The proof is completed. △

D. A Property of Codex

Let (C, ψ) be an $(n, t, d, r, \mathbb{F}_{q^2}^k/\mathbb{F}_{q^2})$-codex. Let (C_1, φ) be the interleaved codex constructed from (C, ψ) in Proposition 2.9. Let m be a positive integer. For each integer $e \geq 1$ and each polynomial $f(\mathbf{x}) \in \mathbb{F}_q[x_1, \ldots, x_m]$ with $\deg(f(\mathbf{x})) \leq d$. Define the map $f^{(e)} : \mathbb{F}_q^{e \times m} \longrightarrow \mathbb{F}_q^e$; $(\mathbf{u}_1, \ldots, \mathbf{u}_m) \mapsto (f(u_{1j}, \ldots, u_{mj}))_{i=1}^e$, where u_{ij} denotes the j-th coordinate of $\mathbf{u}_i$ $(i = 1, \ldots, m, j = 1, \ldots, r)$. Note that $f(u_1, \ldots, u_m) = f^{(1)}(u_1, \ldots, u_m)$.

For codewords $\mathbf{c}_1, \ldots, \mathbf{c_m} \in C \subseteq \mathbb{F}_q^n$, we have

$$\begin{aligned}
& f^{(n)}(\mathbf{c}_1, \ldots, \mathbf{c}_m) \\
= \; & (f(c_{11}, \ldots, c_{m1}), \ldots, f(c_{1n}, \ldots, c_{mn})) \\
= \; & (\cdots, \sum_{\mathrm{wt}_L(I) \leq d} a_I \mathbf{c}_{(j)}^I, \cdots) \\
= \; & \sum_{\mathrm{wt}_L(I) \leq d} a_I (\cdots, \mathbf{c}_{(j)}^I, \cdots),
\end{aligned}$$

where $\mathbf{c}_{(j)}^I := \prod_{i=1}^m c_{ij}{}^{e_i}$ for $I = (e_1, e_2, \ldots, e_m)$. This implies that $f^{(n)}(\mathbf{c}_1, \ldots, \mathbf{c}_m) \in C^{*d}$. Furthermore, we have

$$\begin{aligned}
& \psi(f^{(n)}(\mathbf{c}_1, \ldots, \mathbf{c}_m)) \\
= \; & \sum_{\mathrm{wt}_L(I) \leq d} a_I \psi(\cdots, \mathbf{c}_{(j)}^I, \cdots) \\
= \; & f^{(k)}(\psi(\mathbf{c}_1), \ldots, \psi(\mathbf{c}_m))
\end{aligned} \tag{II.1}$$

and

$$\begin{aligned}
& \varphi(f^{(n)}(\mathbf{c}_1, \ldots, \mathbf{c}_m)) \\
= \; & \sum_{\mathrm{wt}_L(I) \leq d} a_I \varphi(\cdots, \mathbf{c}_{(j)}^I, \cdots) \\
= \; & f^{(k)}(\varphi(\mathbf{c}_1), \ldots, \varphi(\mathbf{c}_m)).
\end{aligned} \tag{II.2}$$

E. Bounds on Error Probability

In this subsection, we investigate the sum of t-wise independent variables that will be used in local decoding of Reed-Muller codes. For our purpose, let us consider binary random variables that take values either 0 or 1.

Definition 2.10: Binary random variables $X_1, X_2, \ldots, X_n$ are said to be *t-wise independent* if for any $a_1, a_2, \ldots, a_t \in \{0, 1\}$ and any t indices $1 \leq i_1 < i_2 < \cdots < i_t \leq n$, one has $\Pr[X_{i_1} = a_1, \ldots, X_{i_t} = a_t] = \prod_{i=1}^t \Pr[X_{i_i} = a_i]$.

We are going to bound the deviation from the mean of the sum $X = X_1 + \cdots + X_n$. Let us first consider the case $t = 2$ where Chebyshev's inequality is employed.

Lemma 2.11: Let $X_1, \ldots, X_n$ be pairwise independent binary random variables taking values in $\{0, 1\}$ and satisfy $\Pr(X_i = 1) = \delta$ for all $1 \leq i \leq n$. Then, for any $A > 0$, $\Pr[|X - \delta n| \geq A] \leq \frac{(\delta - \delta^2)n}{A^2}$.

PROOF. Define $X = \sum_{i=1}^n X_i$. By linearity of expectation, $\mathrm{E}[X] = \sum_{i=1}^n \mathrm{E}[X_i] = \delta n$. Since the X_i's are pairwise independent, linearity of variance holds here as well. This implies

$$\mathrm{Var}(X) = \sum_{i=1}^M \mathrm{Var}[X_i] = \sum_{i=1}^n (\mathrm{E}[X_i^2] - \mathrm{E}[X_i]^2) = (\delta - \delta^2)n.$$

Then by Chebyshev's Inequality, we have

$$\text{Prob}[|X - \text{E}[X]| \geq A] \leq \frac{\text{Var}(X)}{A^2} = \frac{(\delta - \delta^2)n}{A^2}.$$

This completes the proof. △

For $t \geq 4$, we have the following *Second t-wise Independence Tail Inequality*.

Lemma 2.12: (see [2]) Let $t \geq 4$ be an even integer. Suppose $X_1, \ldots, X_n$ are t-wise independent random variables over $\{0, 1\}$. Let $X := \sum_{i=1}^n X_i$ and define $\mu := E[X]$ as the expectation of the sum. Then, for any $A > 0$, $Pr[|X - \mu| \geq A] \leq 8\left(\frac{t\mu+t^2}{A^2}\right)^{t/2}$.

F. Two Classes of Function Fields

In this subsection, we introduce two classes of algebraic curves (or equivalently function fields) that will be used to construct our codex in Section III, namely Hermitian curves and the Garcia-Stichtenoth tower. The reader may refer to [11] and [25, Sections 6.4 and 7.2] for the detail.

For a function F of genus $g(F)$ over $\mathbb{F}_{q^2}$, the number $N(F)$ of rational places of F is upper bounded by the Hasse-Weil bound $q+1+2g(F)q$. F is called maximal if $N(F)$ achieves the Hasse-Weil bound, i.e., $N(F) = q + 1 + 2g(F)q$. One of maximal function fields is called the Hermitian function field. It is defined over $\mathbb{F}_{q^2}$ and its equation is given by

$$y^q + y = x^{q+1}.$$

The function field of this curve is $F = \mathbb{F}_{q^2}(x, y)$. There are totally $q^3 + 1$ rational places for this function field. One of them is the point "at infinity", denoted by ∞. The other places are given by $(\alpha, \beta) \in \mathbb{F}_{q^2}^2$ satisfying $\beta^q + \beta = \alpha^{q+1}$. These are called "finite" rational places. The genus of this function field is $g(F) = q(q - 1)/2$.

The other class of function fields is also defined over $\mathbb{F}_{q^2}$. It is asymptotically optimal and recursively defined by the following equations

$$x_{i+1}^q + x_{i+1} = \frac{x_i^q}{1 + x_i^{q-1}}, \quad i = 1, 2 \ldots$$

with x_1 being a transcendental element over $\mathbb{F}_q$. The function field $\mathbb{F}_q(x_1, x_2, \ldots, x_e)$ is denoted by F_e. The genus $g_e := g(F_e)$ is at most q^e. There is one place over the pole of x_1 called "point at infinity". Furthermore, for each element $\alpha \in \mathbb{F}_{q^2} \setminus \{\alpha \in \mathbb{F}_{q^2} : \alpha^q + \alpha = 0\}$, there are exactly q^{e-1} places over it. This implies the number $N(F_e)$ of rational places of F_e is at least $q^e(q-1)+1$. Thus, one has $\lim_{e\to\infty} N(F_e)/g(F_e) \geq q-1$. On the other hand, the Vlăduţ-Drinfeld bound [26] says $\lim_{e\to\infty} N(F_e)/g(F_e) \leq q - 1$. Therefore, this function field matches the upper bound.

III. Local Decoding of Reed-Muller Codes

In this section, we focus on the local decoding of Reed-Muller code aiming to recover multiple coordinates simultaneously. Let $\text{RM}(q, d, m)$ be the q-ary Reed-Muller code. We denote by $\mathbf{a}_f$ the codeword of $\text{RM}(q, d, m)$ generated by the polynomial $f(\mathbf{x})$. Let $N = q^m$ and $\delta \in (0, 1)$. Suppose $\mathbf{a}_f$ is transmitted and there are at most δN error positions, i.e., there exists a vector $\mathbf{b} \in \mathbb{F}_q^N$ with $\text{wt}_\text{H}(\mathbf{b}) \leq \delta N$ such that the received word is $\tilde{\mathbf{a}} := \mathbf{a}_f + \mathbf{b} \in \mathbb{F}_q^N$.

In other words, $\tilde{\mathbf{a}}$ is a corruption of the codeword $\mathbf{a}_f$ by an error vector $\mathbf{b}$ of relative Hamming weight at most δ. Assume that we are going to recover $\mathbf{a}_f$ at positions $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k \in \mathbb{F}_q^m$. Write $\tilde{\mathbf{a}} = (\tilde{a}_\mathbf{u})_{\mathbf{u}\in\mathbb{F}_q^m}$ and $\mathbf{w}_i = (w_{i,1}, w_{i,2}, \ldots, w_{i,m})$ for $i = 1, 2, \ldots, k$.

A. Direct Decoding With Codex

We first introduce a local decoding with codex.

Algorithm 1 Local Decoding Algorithm With Codex

1. Choose an $(n, t, d, \sigma n, \mathbb{F}_q^k/\mathbb{F}_q)$-codex $\mathcal{C} = (C, \psi)$ with a real $0 < \sigma < 1$;
2. For $i = 1, \ldots, m$, select $\mathbf{c}_i \in C \subset \mathbb{F}_q^n$ uniformly at random (and independently of everything else) such that $\psi(\mathbf{c}_i) = (w_{1,i}, \ldots, w_{k,i})$;
3. Query $\tilde{\mathbf{a}} = (\tilde{a}_\mathbf{u})_{\mathbf{u}\in\mathbb{F}_q^m}$ at positions $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n \in \mathbb{F}_q^m$, where $\mathbf{v}_j$ denotes collection of the j-th coordinate of the codewords $\mathbf{c}_1, \ldots, \mathbf{c}_m$;
4. Find a codeword $(z_1, z_2, \ldots, z_n) \in C^{*d}$ such that the Hamming distance between $(z_1, z_2, \ldots, z_n) \in C^{*d}$ and $(\tilde{a}_{\mathbf{v}_1}, \ldots, \tilde{a}_{\mathbf{v}_n})$ is at most $(n - \sigma n)/2$.
5. If no such a codeword $(z_1, z_2, \ldots, z_n)$ in Step 4 is found, output "fail". Otherwise, output $(f(\mathbf{w}_1), f(\mathbf{w}_2), \ldots, f(\mathbf{w}_k)) = \psi(z_1, z_2, \ldots, z_n)$.

Now, we analyze the above algorithm.

First, $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are t-wise independent and uniformly random distributed in $\mathbb{F}_q^m$ by Definition 2.2(iii).

Suppose that a codeword $(z_1, z_2, \ldots, z_n) \in C^{*d}$ is found such that the Hamming distance between $(z_1, z_2, \ldots, z_n) \in C^{*d}$ and $(\tilde{a}_{\mathbf{v}_1}, \ldots, \tilde{a}_{\mathbf{v}_n})$ is at most $(n-\sigma n)/2$. Then by Definition 2.2(iv)(b), we have $(f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n)) = (z_1, z_2, \ldots, z_n)$ as long as the Hamming distance between $(f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n))$ and $(\tilde{a}_{\mathbf{v}_1}, \ldots, \tilde{a}_{\mathbf{v}_n})$ is at most $(n - \sigma n)/2$.

By Subsection II-D, it holds that $f^{(n)}(\mathbf{c}_1, \ldots, \mathbf{c}_m) = (f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n)) \in C^{*d}$ and $f^{(k)}(\psi(\mathbf{c}_1), \ldots, \psi(\mathbf{c}_m)) = (f(\mathbf{w}_1), \ldots, f(\mathbf{w}_k))$. Thus, we can recover $(f(\mathbf{w}_1), \ldots, f(\mathbf{w}_k))$ as follows.

$$\begin{aligned}(f(\mathbf{w}_1), \ldots, f(\mathbf{w}_k)) &= f^{(k)}(\psi(\mathbf{c}_1), \ldots, \psi(\mathbf{c}_m)) \\ &= \psi(f^{(n)}(\mathbf{c}_1, \ldots, \mathbf{c}_m)) = \psi(f(\mathbf{v}_1), \ldots, f(\mathbf{v}_n)) \\ &= \psi(z_1, z_2, \ldots, z_n).\end{aligned}$$

The second equality is due to (II.1). Now the probability of successfully recovering $(f(\mathbf{w}_1), \ldots, f(\mathbf{w}_k))$ is equal to the probability of successfully finding a codeword $(z_1, z_2, \ldots, z_n)$ such that the Hamming distance between $(\tilde{a}_{\mathbf{v}_1}, \ldots, \tilde{a}_{\mathbf{v}_n})$ and $(z_1, z_2, \ldots, z_n)$ is at most $(n - \sigma n)/2$. This probability is at least the probability that there are at most $(n-\sigma n)/2$ corrupted positions for $\mathbf{a}_f$ among $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$.

Denote by E the set of coordinates $\mathbf{u}$ such that $\mathbf{b}_\mathbf{u} \neq 0$. For $j = 1, \ldots, n$, define the binary random variable X_j such that $X_j = 1$ if $\mathbf{v}_j \in E$ and $X_j = 0$ otherwise. Then $X_1, \ldots, X_n$ are

t-wise independent and $\mathrm{Prob}(X_j = 1) = \delta$ for $j = 1, \ldots, n$. Put $X = \sum_{i=1}^{n} X_i$.

Since the minimum distance of C^{*d} is at least $(n - \sigma n) + 1$, one can correctly recover $\psi(z_1, z_2, \ldots, z_n)$ from $(\tilde{a}_{\mathbf{v}_1}, \ldots, \tilde{a}_{\mathbf{v}_n})$ if $|E \cap \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}| \le (n - \sigma n)/2$.

Thus, by the above identity it implies that one can correctly recover $(f(\mathbf{w}_1), \ldots, f(\mathbf{w}_k))$ with probability at least $1 - \Pr(X \le (n - \sigma n)/2)$ by querying $\tilde{\mathbf{a}} = (\tilde{a}_{\mathbf{u}})_{\mathbf{u} \in \mathbb{F}_q^m}$, at coordinates $\mathbf{v}_1, \ldots, \mathbf{v}_n$.

Summarizing the above analysis, we get the following local decoding of Reed-Muller codes.

Theorem 3.1: If there exists an $(n, t, d, \sigma n, \mathbb{F}_q^k/\mathbb{F}_q)$-codex (C, ψ) with a real $0 < \sigma < 1$, then the Reed-Muller code $\mathrm{RM}(q, d, m)$ is an $(k; n, \delta, \epsilon)$-locally decodable code with $\epsilon = \Pr(X > (n - \sigma n)/2)$, where X is defined above. Furthermore, the local decoding complexity is $\mathrm{Poly}(n, k, q)$ if the codex can be constructed in time $\mathrm{Poly}(n, k, q)$ and decoding time of the code C^{*d} is $\mathrm{Poly}(n, q)$.

B. Decoding With Interleaved Codex

Now we introduce a local decoding with interleaved codex. We start with a codex over $\mathbb{F}_{q^2}$ and assume that $d \le \sigma q$ with $\sigma < 1$.

Algorithm 2 Local Decoding Algorithm With Interleaved Codex

1. Choose an $(n, t, d, \rho n, \mathbb{F}_{q^2}^k/\mathbb{F}_{q^2})$-codex $\mathcal{C} = (C, \psi)$ with a real $0 < \rho < 1 - \sigma$ and let $(C_1, \varphi = \psi \circ \phi)$ be the interleaved codex obtained by concatenating codex (C, ψ) in Proposition 2.9 with multiplication friendly pair (π, ϕ);
2. For $i = 1, \ldots, m$, select $\mathbf{c}_i \in C \subset \mathbb{F}_{q^2}^n$ uniformly at random (and independently of everything else) such that $\varphi(\pi(\mathbf{c}_i)) = (w_{1,i}, \ldots, w_{k,i})$;
3. Query $\tilde{\mathbf{a}} = (\tilde{a}_{\mathbf{u}})_{\mathbf{u} \in \mathbb{F}_q^m}$ at positions $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{qn} \in \mathbb{F}_q^m$, where $\mathbf{v}_j$ denotes collection of the j-th coordinate of the codewords $\pi(\mathbf{c}_1), \ldots, \pi(\mathbf{c}_m)$;
4. Find a codeword $\mathbf{z} \in C_1^{*d}$ such that the Hamming distance between $\mathbf{z}$ and $(\tilde{a}_{\mathbf{v}_1}, \ldots, \tilde{a}_{\mathbf{v}_{qn}})$ is at most $(1 - \sigma - \rho)qn/2$.
5. If no such a codeword $\mathbf{z}$ in Step 4 is found, output "fail". Otherwise, output $(f(\mathbf{w}_1), f(\mathbf{w}_2), \ldots, f(\mathbf{w}_k)) = \varphi(\mathbf{z})$.

Analysis of the above algorithm is similar to that of Algorithm 1. Let us discuss probability only.

Note that C_1 is a concatenated code. The outer code is C which is defined over $\mathbb{F}_{q^2}$ and the inner code is a Reed-Solomon code. Thus, $(\tilde{a}_{\mathbf{v}_1}, \ldots, \tilde{a}_{\mathbf{v}_{qn}})$ can be partitioned into n blocks $(\tilde{\mathbf{a}}_1, \ldots, \tilde{\mathbf{a}}_n)$, each with length q. Write $\tilde{\mathbf{a}}_i = (\tilde{a}_{i,1}, \ldots, \tilde{a}_{i,q})$ be the i-th block. Denote by $X_{i,j}$ for $(i, j) \in [n] \times [q]$ be the random variable such that $X_{i,j} = 1$ if $\tilde{a}_{i,j}$ is corrupted, and $X_{i,j} = 0$ otherwise. Then $\Pr[X_{i,j} = 1] = \delta$ follows from the fact that there is δ fraction of corrupted positions. By t-weak privacy of the pair (C_1, φ), it is clear that the random variables $X_{1,j}, X_{2,j}, \ldots, X_{n,j}$ are t-wise independent. Let $X_i = \sum_{j=1}^{n} X_{j,i}$. In Lemma 2.12, put $A = (1 - \sigma - \rho)n/2 - \delta n$, we obtain

$$\Pr[X_i > \frac{(1 - \sigma - \rho)n}{2}] \le 8(\frac{4t\delta n + 4t^2}{(1 - \sigma - \rho - 2\delta)^2 n^2})^{t/2}.$$

By the union bound, we have

$$\Pr[\exists i : X_i > \frac{(1 - \sigma - \rho)n}{2}] \le 8q(\frac{4t\delta n + 4t^2}{(1 - \sigma - \rho - 2\delta)^2 n^2})^{t/2}.$$

Thus, we have

$$\begin{aligned} & \Pr[\sum_{i=1}^{q} X_i > \frac{(1 - \sigma - \rho)qn}{2}] \\ \le\ & \Pr[\exists i : X_i > \frac{(1 - \sigma - \rho)n}{2}] \\ \le\ & 8q(\frac{4t\delta n + 4t^2}{(1 - \sigma - \rho - 2\delta)^2 n^2})^{t/2}. \end{aligned} \tag{III.1}$$

C_1^{*d} is a concatenated code and it has minimum distance at least $qn - dn - \sigma qn + 1 = qn(1 - \sigma - \rho) + 1$. By [18], we know that a concatenated code can be efficiently decoded up to half of minimum distance. This completes analysis of Algorithm 2.

Summarizing the above analysis, we obtain the following local decoding of Reed-Muller codes.

Theorem 3.2: Let $d \le \sigma q$. If there exists an $(n, t, d, \rho n, \mathbb{F}_{q^2}^k/\mathbb{F}_{q^2})$-codex (C, ψ) with a real $0 < \rho < 1 - \sigma$, then the Reed-Muller code $\mathrm{RM}(q, d, m)$ is a $(k; n, \delta, \epsilon)$-locally decodable code with ϵ upper bounded by (III.1). Furthermore, the local decoding complexity is $\mathrm{Poly}(n, k, q)$ if the codex can be constructed in time $\mathrm{Poly}(n, k, q)$ and decoding time of the code C_1^{*d} is $\mathrm{Poly}(n, q)$, where C_1 is the concatenated code defined in Subsection II-C.

IV. The Main Results

In this section, we apply various codex constructed from the rational function fields, Hermitian function fields and function fields in the Garcia-Stichtenoth tower to obtain our main results by using Theorems 3.1 or 3.2.

A. Single Point Decoding

In this subsection, we consider local decoding to recover only a single coordinate via codex from Reed-Muller codes.

Example 4.1: For the rational function field $F = \mathbb{F}_q(x)$, we have $g(F) = 0$. Let $\mathcal{Q}$ and $\mathcal{P}$ be the set $\{0\}$ and $\mathbb{F}_q \setminus \{0\}$. In this case, $k = 1$ and $n = q - 1$.

(i) Choose $t = 1$, then for any real $0 < \sigma < 1$ and $1 < d \le \sigma(q-1)+1$, there exists is a $(q-1, 1, d, \sigma(q-1); \mathbb{F}_q/\mathbb{F}_q)$-codex. By Markov's inequality the probability that $(1 - \sigma)(q - 1)/2$ or more of the queries go to corrupted locations is at most $2\delta/(1-\sigma)$. Thus, the Reed-Muller code $\mathrm{RM}(q, d, m)$ is a $(q - 1, \delta, 2\delta/(1 - \sigma))$-locally correctable code by Theorem 3.1. This is exactly the same decoding given in [27, Proposition 2.5].

(ii) Choose $t = 2$, then for any real $0 < \sigma < 1$ and $1 < d \le \sigma(q - 1) - 1$, there exists is a

$(q-1, 2, d, 2\sigma(q-1); \mathbb{F}_q/\mathbb{F}_q)$-codex. In Lemma 2.11, let A be $(1-2\sigma)(q-1)/2 - \delta(q-1)$, we obtain

$$\begin{aligned}\epsilon &= \Pr[X > (1-2\sigma)(q-1)/2] \\ &\le \frac{(\delta-\delta^2)(q-1)}{((1-2\sigma)(q-1)/2-\delta(q-1))^2} \\ &= \frac{4(\delta-\delta^2)}{(1-2\sigma-2\delta)^2} \times \frac{1}{q-1}. \qquad \text{(IV.1)}\end{aligned}$$

Thus, by Theorem 3.1, the Reed-Muller code $\mathrm{RM}(q, d, m)$ is a $(q-1, \delta, \epsilon)$-locally correctable code with ϵ given in (IV.1). This is exactly the same decoding on curves given in [27, Proposition 2.6].

(iii) Let $t \ge 4$. For any real $0 < \sigma \le 1$ and $1 < d \le \sigma(q-1)/t - 1/t$, there exists is a $(q-1, t, d, \sigma(q-1); \mathbb{F}_q/\mathbb{F}_q)$-codex. It is clear that the expectation of X is $\mu = \delta(q-1)$. In Lemma 2.12, put $A = (1-\sigma)(q-1)/2 - \delta(q-1)$, by Lemma 2.12 we obtain

$$\begin{aligned}\epsilon &= \Pr[X > (1-\sigma)(q-1)/2] \\ &\le 8\left(\frac{4t\delta(q-1)+4t^2}{(1-\sigma-2\delta)^2(q-1)^2}\right)^{t/2}. \qquad \text{(IV.2)}\end{aligned}$$

Thus, by Theorem 3.1, the Reed-Muller code $\mathrm{RM}(q, d, m)$ is an $(q-1, \delta, \epsilon)$-locally decodable code with ϵ given in (IV.2). It is easy to see from (IV.2) that $\epsilon \le 8\left(\frac{\lambda_{\sigma,\delta} t}{\sqrt{q}}\right)^t$, where $\lambda_{\sigma,\delta} = \frac{\sqrt{8}}{1-\sigma-2\delta}$.

Remark 4.2: For sufficiently large q, by choice of a suitable t, local decoding in Example 4.1(iii) gives much better probability than those in Example 4.1(i) and (ii).

In the rest of this subsection we are going to apply Algorithm 2 and concatenated codex from algebraic geometry codes over $\mathbb{F}_{q^2}$ to get local decoding of Reed-Muller codes. We first consider decoding using codex from the Hermitian function field.

Theorem 4.3: For any real $0 < \sigma, \delta \le 1$ and integers $4 \le t \le q$, $d > 1$ satisfying $\sigma < (1-2\delta)/2$ and $d \le \sigma q$, the Reed-Muller code $\mathrm{RM}(q, d, m)$ is a $\left(q(q^3-1), \delta, \epsilon\right)$-locally correctable code with $\epsilon \le 8q\left(\frac{\nu_{\sigma,\delta} t}{\sqrt{q^3-1}}\right)^t$, where $\nu_{\sigma,\delta} = \frac{\sqrt{8}}{1-2\sigma-2\delta}$.

Proof. Consider the Hermitian function field over $\mathbb{F}_{q^2}$ defined in Subsection II-F. Let $\mathcal{Q} = \{(0,0)\}$ and let $\mathcal{P}$ be the set consisting of all "finite" points except for $(0,0)$. Then for any real $0 < \sigma \le 1$ and integers $4 \le t \le q$, $d > 1$ satisfying $d \le \sigma q$, there exists a $(q^3-1, t, d, \sigma(q^3-1), \mathbb{F}_{q^2}/\mathbb{F}_{q^2})$-codex. Applying Algorithm 2 and (III.1), we conclude that the Reed-Muller code $\mathrm{RM}(q, d, m)$ is a $(q(q^3-1), \delta, \epsilon)$-locally correctable code with

$$\begin{aligned}\epsilon &\le 8q\left(\frac{4t\delta(q^3-1)+4t^2}{(1-2\sigma-2\delta)^2(q^3-1)^2}\right)^{t/2} \\ &\le 8q\left(\frac{\nu_{\sigma,\delta} t}{\sqrt{q^3-1}}\right)^t.\end{aligned}$$

The desired result follows. △

Finally, we apply Algorithm 2 and concatenated codex from the Garcia-Stichtenoth tower.

Theorem 4.4: Let q be a square prime power and let $e \ge 2$. Fix reals $0 < \sigma, \delta \le 1$. If integers $4 \le t \le q^e$, $d > 1$ satisfy $\sigma < (1-2\delta)/4$ and $d \le \sigma q$, then the Reed-Muller code $\mathrm{RM}(q, d, m)$ is an (qn, δ, ϵ)-locally detectable code with $\epsilon \le 8q\left(\frac{4t\delta n+4t^2}{(1-4\sigma-2\delta)^2 n^2}\right)^{t/2}$, where $n = q^e(q-1)-1$. Furthermore, the local decoding complexity is $\mathrm{Poly}(n, q)$

Proof. Consider the function field F_e in the Garcia-Stichtenoth tower over $\mathbb{F}_{q^2}$ defined in Subsection II-F. Then $N(F_e) \ge q^e(q-1)$ and $g(F_e) \le q^e$. Let $\mathcal{Q}$ be a single "finite" rational place set and let $\mathcal{P}$ be the set consisting of other $n = q^e(q-1)-1$ "finite" rational place. Then $d(2g(F)+1+t-1) < \rho n < n$ and hence by Proposition 2.5, there exists an $(n, t, d, \rho n, \mathbb{F}_{q^2}/\mathbb{F}_{q^2})$-codex, where $\rho = 3\sigma$. Applying the local decoding Algorithm 2 in Subsection III-B gives the desired result.

Since the codex is constructed from the Garcia-Stichtenoth tower and the code C_1^{*d} is an algebraic geometry code based on this tower, the result on decoding complexity follows. △

By taking $t = n/q = q^{e-1}(q-1)$ in Theorem 4.4, we obtain the results on local decoding of single coordinate.

Corollary 4.5: Let q be a prime power. Let $d > 1, t, m$ be positive integers. Let δ, σ be two reals in $(0,1)$ with $\delta < \frac{1-4\sigma}{2}$. Then the Reed-Muller code $\mathrm{RM}(q, d, m)$ with $d \le \sigma q$ is $\left(q^2 t, \delta, O\left(\left(\frac{\mu_{\delta,\sigma}}{\sqrt{q}}\right)^t\right)\right)$-locally correctable, where $\mu_{\delta,\sigma} = \frac{\sqrt{8}}{1-4\sigma-2\delta}$ (note that t can be arbitrarily large).

Remark 4.6: One might question that our performance of single-point decoding does not even match the local decoding algorithm based on Reed-Solomon codes, i.e., repeating decoding in Proposition 1.4 multiple times. However, as we know in our next subsection, this algorithm can also be used to recover multiple points at the cost of almost the same query complexity as in the single-point decoding. The key point behind this phenomenon is that our algebraic geometry code has very large dual distance, which can both pass through many given coordinates and generate t-wise independent variables for very large t at the same time.

B. Multiple-Point Local Decoding of Reed-Muller Codes

In this subsection, we analyze local decoding of Reed-Muller codes to recover multiple coordinates simultaneously. Again we apply Reed-Solomon codes, Hermtian codes and algebraic geometry codes based on the Garcia-Stichtenoth tower, respectively. The proofs are almost identical with those in the previous subsection except for replacing $\mathcal{Q}$ of a single point set by a k-point set. We state the results without proof below.

Theorem 4.7: Let q be a prime power. Let $d > 1, t, m, k$ be positive integers. Let δ, σ be two reals in $(0,1)$ with $\delta < \frac{1-\sigma}{2}$.

(i) **(Reed-Solomon code with $t = 1$)** If $k + n \le q$ and $d < \frac{\sigma n}{k}$, then the Reed-Muller code $\mathrm{RM}(q, d, m)$ is an $(k; n, \delta, \epsilon)$-locally decodable code with $\epsilon = \frac{2\delta}{1-\sigma}$.

(ii) **(Reed-Solomon code with $t = 2$)** If $k + n \le q$ and $d < \frac{\sigma n}{k+2}$, then the Reed-Muller code $\mathrm{RM}(q, d, m)$ is an $(k; n, \delta, \epsilon)$-locally decodable code with $\epsilon = \frac{\delta-\delta^2}{(1-\sigma-2\delta)^2} \times \frac{1}{n}$.

(iii) **(Reed-Solomon code with** $t \geq 4$) If $k+n \leq q$ and $d < \frac{\sigma n}{k+t}$, then the Reed-Muller code $\mathrm{RM}(q,d,m)$ is an $(k;n,\delta,\epsilon)$-locally decodable code with $\epsilon = 8\left(\frac{4t\delta n+4t^2}{(1-\sigma-2\delta)^2}\right)^{t/2} \times \left(\frac{1}{n}\right)^t$.

(iv) **(Hermitian code with** $t \geq 4$) If $k+n \leq q^3$ and $d < \sigma q$, then the Reed-Muller code $\mathrm{RM}(q,d,m)$ is an $(k;qn,\delta,\epsilon)$-locally decodable code with $\epsilon = 8\left(\frac{4t\delta n+4t^2}{(1-\sigma-\rho-2\delta)^2}\right)^{t/2} \times \left(\frac{1}{n}\right)^t$, where $\rho = (k+t+q^2-q)/q^2$.

(v) **(GS tower code with** $t \geq 4$) Let $e \geq 2$. If $t \leq n$ and $k \leq n$, $k+n \leq q^e(q-1)$ and $d < \sigma n$, then the Reed-Muller code $\mathrm{RM}(q,d,m)$ is an $(k;qn,\delta,\epsilon)$-locally decodable code with $\epsilon = 8q\left(\frac{4t\delta+4t^2}{(1-\sigma-\rho-2\delta)^2}\right)^{t/2} \times \left(\frac{1}{n}\right)^t$, where $\rho = (2q^{e+1}+qk+qt)/n$. Furthermore, the local decoding complexity is $\mathrm{Poly}(n,k,q)$

Note that we applied Algorithm 1 for the first three local decodings in Theorem 4.7, while Algorithm 2 is employed for the last two local decodings in Theorem 4.7.

Proof of Theorem 1.5: Taking $n \approx \frac{2q}{2q+1} \times q^e(q-1)$ and $k = t = \lfloor n/(2q) \rfloor$, we obtain Theorem 1.5 from Theorem 4.7(v).

Remark 4.8: The interleaved codex is obtained via concatenation of codex with multiplication friendly pair, i.e., we treat multiplication friendly pair as an inner code with multiplicative property and codex as an outer code. To improve the performance of our interleaved codex, we must find codex with better parameters. The current known construction of codex is via algebraic geometry codes. As we know, the asymptotic behaviour of algebraic geometry codes must obey the celebrated Vlăduţ-Drinfeld bound [26]. The codex we employ already reaches this bound.

References

[1] N. Alon, T. Kaufman, M. Krivelevich, S. Litsyn, and D. Ron, "Testing Reed–Müller codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 11, pp. 4032–4039, Nov. 2005.

[2] M. Bellare and J. Rompel, "Randomness-efficient oblivious sampling," in *Proc. FOCS*, Nov. 1994, pp. 276–287.

[3] E. Ben-Sasson, A. Gabizon, Y. Kaplan, S. Kopparty, and S. Saraf, "A new family of locally correctable codes based on degree-lifted algebraic geometry codes," in *Proc. STOC*, 2013, pp. 833–842.

[4] A. Bhowmick and S. Lovett, "The list decoding radius for Reed–Müller codes over small fields," in *Proc. STOC*, 2015, pp. 277–285.

[5] H. Chen and R. Cramer, "Algebraic geometric secret sharing schemes and secure multi-party computations over small fields," in *Proc. CRYPTO*, 2006, pp. 521–536.

[6] R. Cramer, "The arithmetic codex: Theory and applications," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 6632. Berlin, Germany: Springer, 2011, p. 1.

[7] I. Cascudo, R. Cramer, and C. Xing, "The arithmetic codex," in *Proc. Inf. Theory Workshop*, Sep. 2012, pp. 75–79.

[8] R. Cramer, I. Damgård, and U. M. Maurer, "General secure multi-party Computation from any linear secret-sharing scheme," in *Proc. EUROCRYPT*, 2000, pp. 316–334.

[9] R. Cramer, I. Damgård, and I. Nielsen, *Secure Multiparty Computation and Secret Sharing*. Cambridge, U.K.: Cambridge Univ. Press, 2015.

[10] D. V. Chudnovsky and G. V. Chudnovsky, "Algebraic complexities and algebraic curves over finite fields," *Proc. Nat. Acad. Sci. USA*, vol. 84, no. 7, pp. 1739–1743, Apr. 1987.

[11] A. Garcia and H. Stichtenoth, "A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound," *Inventiones Math.*, vol. 121, no. 1, pp. 211–222, 1995.

[12] P. Gopalan, "A Fourier-analytic approach to Reed–Müller decoding," in *Proc. FOCS*, 2010, pp. 685–694.

[13] P. Gopalan, A. R. Klivans, and D. Zuckerman, "List-decoding Reed–Müller codes over small fields," in *Proc. STOC*, 2008, pp. 265–274.

[14] A. Guo, "High-rate locally correctable codes via lifting," 2014, *arXiv:1304.1202*. [Online]. Available: https://arxiv.org/abs/1304.1202

[15] V. Guruswami and C. Xing, "Hitting sets for low-degree polynomials with optimal density," in *Proc. IEEE 29th Conf. Comput. Complex. (CCC)*, Jun. 2014, pp. 161–168.

[16] A. Guo, S. Kopparty, and M. Sudan, "New affine-invariant codes from lifting," in *Proc. ITCS*, 2013, pp. 529–540.

[17] V. Guruswami, L. Jin and C. Xing, "Efficiently list-decodable punctured Reed–Müller codes," *IEEE Trans. Inf. Theory*, vol. 63, no. 7, pp. 4317–4324, Jul. 2017.

[18] G. D. Forney, "Generalized minimum distance decoding," *IEEE Trans. Inf. Theory*, vol. 12, no. 2, pp. 125–131, Apr. 1966.

[19] S. Hoory, N. Linial, and A. Wigderson, "Expander graphs and their applications," *Bull. AMS*, vol. 43, no. 4, pp. 439–561, 2006.

[20] S. Kopparty, S. Saraf, and S. Yekhanin, "High-rate codes with sublinear-time decoding," *J. ACM*, vol. 61, no. 5, p. 28, 2014.

[21] D. Moshkovitz and R. Raz, "Sub-constant error probabilistically checkable proof of almost-linear size," *Comput. Complex.*, vol. 19, no. 3, pp. 367–422, 2010.

[22] O. Meir, "Locally correctable and testable codes approaching the singleton bound," in *Proc. Electron. Colloq. Comput. Complex. (ECCC)*, vol. 21, 2014, p. 107.

[23] R. Pellikaan and X.-W. Wu, "List decoding of q-ary Reed–Müller codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 4, pp. 679–682, Apr. 2004.

[24] R. Saptharishi, A. Shpilka, and B. L. Volk, "Efficiently decoding Reed-Müller codes from random errors," 2015, *arXiv:1503.09092*. [Online]. Available: http://arxiv.org/abs/1503.09092

[25] H. Stictenoth, *Algebraic Function Fields and Codes*. Berlin, Germany: Springer, 2009.

[26] M. A. Tsfasman and S. G. Vladut, *Algebraic-Geometric Codes*. Dordrecht, The Netherlands: Kluwer, 1991.

[27] S. Yekhanin, "Locally decodable codes," *Found. Trends Theor. Comput. Sci.*, vol. 6, no. 3, pp. 139–255, 2012.

Ronald Cramer received the MSc degree (mathematics) from Leiden University, the Netherlands, in 1992 and the PhD degree (cryptology) from the University of Amsterdam, the Netherlands, in 1997. Since June 1, 2004, he has been the head (and founder) of the Cryptology Group at CWI in Amsterdam. CWI is the Dutch national research center for mathematics and computer science in the Netherlands. Also since June 1, 2004, he has been Full Professor at the Mathematical Institute, Leiden University. Prior to that he held research positions at ETH Zurich, Switzerland and at Aarhus University, Denmark. He is Fellow of the International Association for Cryptologic Research (IACR) and he is Member of the Royal Netherlands Academy of Sciences (KNAW), both since 2013. Cramer's research area is cryptology, including applications of coding theory, algebraic number theory and algebraic geometry.

Chaoping Xing received his PhD degree in 1990 from University of Science and Technology of China. From 1990 to 1993 he was a lecturer and associate professor in the same university. He joined University of Essen, Germany as an Alexander von Humboldt fellow from 1993 to 1995. After this he spent most time in Institute of Information Processing, Austrian Academy of Sciences until 1998. From March of 1998 to November of 2007, he was working in National University of Singapore as an assitant/associate/full professor. December of 2007 to August of 2019, he was working in Nanyang Technological University as a full professor. Since September 2019, he has been with Shanghai Jiaotong University as a chair professor. Dr. Xing has been working on the areas of coding theory, cryptography, algebraic curves over finite fields and quasi-Monte Carlo methods, etc.

Chen Yuan received his B.S degree in mathematics in 2008 and Ph.D degree in computer science in 2013, both from Fudan University. He received his Ph.D degree in mathematics in 2018 from Nanyang Technological University. He used to work as a research fellow at the Division of Mathematical Sciences, Nanyang Technological University, Singapore from September of 2017 to March of 2018. Since April of 2018, he joined the Cryptology group in Centrum Wiskunde & Informatica as a postdoctoral researcher. His research interests include coding theory and its application in cryptography and theoretical computer science.