PAPER *Special Section on Foundations of Computer Science*

Improved Constructions for Query-Efficient Locally Decodable Codes of Subexponential Length*

Toshiya ITOH[†a)], ***Member and*** **Yasuhiro SUZUKI**[††b)], ***Nonmember***

SUMMARY A (k, δ, ε)-locally decodable code $C : \mathbf{F}_q^n \to \mathbf{F}_q^N$ is an error-correcting code that encodes $\vec{x} = (x_1, x_2, \ldots, x_n) \in \mathbf{F}_q^n$ to $C(\vec{x}) \in \mathbf{F}_q^N$ and has the following property: For any $\vec{y} \in \mathbf{F}_q^N$ such that $d(\vec{y}, C(\vec{x})) \leq \delta N$ and each $1 \leq i \leq n$, the symbol x_i of $\vec{x}$ can be recovered with probability at least $1 - \varepsilon$ by a randomized decoding algorithm looking at only k coordinates of $\vec{y}$. The efficiency of a (k, δ, ε)-locally decodable code $C : \mathbf{F}_q^n \to \mathbf{F}_q^N$ is measured by the code length N and the number k of queries. For a k-query locally decodable code $C : \mathbf{F}_q^n \to \mathbf{F}_q^N$, the code length N was conjectured to be exponential of n, i.e., $N = \exp(n^{\Omega(1)})$, however, this was disproved. Yekhanin [In Proc. of STOC, 2007] showed that there exists a 3-query locally decodable code $C : \mathbf{F}_2^n \to \mathbf{F}_2^N$ such that $N = \exp(n^{1/\log\log n})$ assuming that infinitely many Mersenne primes exist. For a 3-query locally decodable code $C : \mathbf{F}_q^n \to \mathbf{F}_q^N$, Efremenko [ECCC Report No.69, 2008] further reduced the code length to $N = \exp(n^{O((\log\log n/\log n)^{1/2})})$, and in general showed that for any integer $r > 1$, there exists a 2^r-query locally decodable code $C : \mathbf{F}_q^n \to \mathbf{F}_q^N$ such that $N = \exp(n^{O((\log\log n/\log n)^{1-1/r})})$. In this paper, we will present improved constructions for query-efficient locally decodable codes by introducing a technique of "composition of locally decodable codes," and show that for any integer $r > 5$, there exists a $9 \cdot 2^{r-4}$-query locally decodable code $C : \mathbf{F}_q^n \to \mathbf{F}_q^N$ such that $N = \exp(n^{O((\log\log n/\log n)^{1-1/r})})$.

key words: *locally decodable codes, S-matching vectors, S-decoding polynomials, perfectly smooth decoders, private information retrieval*

1. Introduction

Conventional error-correcting codes $C : \mathbf{F}_q^n \to \mathbf{F}_q^N$ allow one to encode $\vec{x} = (x_1, x_2, \ldots, x_n) \in \mathbf{F}_q^n$ to $C(\vec{x}) \in \mathbf{F}_q^N$ and have the following property: For any $\vec{y} \in \mathbf{F}_q^N$ such that $d(\vec{y}, C(\vec{x})) \leq \delta N$, the original message $\vec{x}$ can be recovered by looking at entire coordinates of $\vec{y}$. If one is interested in recovering a single symbol x_i of $\vec{x}$, more efficient schemes are possible. Such schemes are known as *locally decodable codes* $C : \mathbf{F}_q^n \to \mathbf{F}_q^N$ that allow recovery of any single symbol x_i of $\vec{x} \in \mathbf{F}_q^n$ by looking at only k randomly chosen coordinates of $\vec{y} \in \mathbf{F}_q^N$ such that $d(\vec{y}, C(\vec{x})) \leq \delta N$. Informally, a (k, δ, ε)-locally decodable code $C : \mathbf{F}_q^n \to \mathbf{F}_q^N$ is an error-correcting code that encodes $\vec{x} = (x_1, x_2, \ldots, x_n) \in \mathbf{F}_q^n$ to $C(\vec{x}) \in \mathbf{F}_q^N$ and has the following property: For any $\vec{y} \in \mathbf{F}_q^N$ such that $d(\vec{y}, C(\vec{x})) \leq \delta N$ and each $1 \leq i \leq n$, the symbol x_i of $\vec{x}$ can be recovered with probability at least $1 - \varepsilon$ by a randomized decoding algorithm looking at only k coordinates of $\vec{y}$.

1.1 Known Results

From theoretical and practical point of view, we are interested in designing a (k, δ, ε)-locally decodable code $C : \mathbf{F}_q^n \to \mathbf{F}_q^N$ with as shorter N as possible and as smaller k as possible. The notion of locally decodable codes was considered in several contexts [2], [17], [19], and Katz and Trevisan [15] were the first to provide a formal definition of locally decodable codes and prove lower bounds for the code length. Gasarch [8] and Goldreich [9] conjectured that for a k-query locally decodable code $C : \mathbf{F}_q^n \to \mathbf{F}_q^N$ with $k > 1$, the length N is unavoidable to be the exponential in n, i.e., $N = \exp(n^{\Omega(1)})$. In Table 1, we summarize the known results on the length for k-query locally decodable codes.

Yekhanin [24], [25] improved the upper bound for the length of 3-query locally decodable codes to $N = \exp(n^{1/32582657})$ and disproved the conjecture [8], [9] on the length of 3-query locally decodable codes, i.e., $N = \exp(n^{O(1/\log\log n)})$ for infinitely many n's if there exist infinitely many Mersenne primes. Very recently, Efremenko [7, Theorem 3.8] improved much further the upper bound for the length of 3-query locally decodable codes to $N = \exp(n^{O((\log\log n/\log n)^{1/2})})$ by introducing the notions of S-matching vectors [7, Definition 3.1] and S-decoding polynomials [7, Definition 3.4] — this reduces the length of 3-query locally decodable codes and removes the unproven assumption that infinitely many Mersenne primes exist. For any $k > 2$, Efremenko [7, Theorem 3.6] also disproved the conjecture [8], [9] on the length of k-query locally decodable codes (with no unproven assumption), and showed that for any integer $r > 1$, there exists a 2^r-query locally decodable code of length $N = \exp(n^{O((\log\log n/\log n)^{1-1/r})})$. For notational simplicity, we use $N(r)$ to denote the code length as a function of $r > 1$, i.e.,

$$N(r) = \exp\left(n^{O\left((\log\log n/\log n)^{1-1/r}\right)}\right).$$

1.2 Main Result

In this paper, we present improved constructions for a query-efficient locally decodable code, and show that for any $r > 5$,

Manuscript received March 3, 2009.

Manuscript revised June 2, 2009.

[†]The author is with the Global Scientific Information and Computing Center (GSIC), Tokyo Institute of Technology, Tokyo, 152–8550 Japan.

[††]The author is with the Department of Information Processing, Tokyo Institute of Technology, Tokyo, 152–8550 Japan.

[*]This research was supported in part by JSPS Global COE program "Computationism as a Foundation for the Sciences."

a) E-mail: titoh@dac.gsic.titech.ac.jp

b) E-mail: suzuki@dac.gsic.titech.ac.jp

DOI: 10.1587/transinf.E93.D.263

Table 1 Known results on the code length.

	Upper Bound		Lower Bound	
2-Query	$\exp(O(n))$	[14]	$\exp(\Omega(n))$	[14]
3-Query	$\exp\left(n^{1/2}\right)$	[4]	$\tilde{\Omega}\left(n^2\right)$	[14], [22]
k-Query	$\exp\left(n^{O(\log\log k)/k\log k}\right)$	[5]	$\tilde{\Omega}\left(n^{1+1/(\lceil k/2\rceil-1)}\right)$	[14], [22]

there exists a $9 \cdot 2^{r-4}$-query locally decodable code $C : \mathbf{F}_q^n \to \mathbf{F}_q^N$ of length $N(r)$. Our construction of $9 \cdot 2^{r-4}$-query locally decodable codes is partially based on the construction due to Efremenko [7]. To reduce the number of queries, we introduce a technique of "composition of locally decodable codes." In fact, we show that for a k_1-query locally decodable code C_1 of length $N(r_1)$ and a k_2-query locally decodable code C_2 of length $N(r_2)$, there exists a k_1k_2-query locally decodable code C of length $N(r_1 + r_2)$.

In this paper, we find a 3-query locally decodable code C_{IS} of length $N(2)$ by an exhaustive search. By applying our technique of "composition of locally decodable codes" to the 3-query locally decodable code C_{E} [7, Theorem 3.8] of length $N(2)$, the 3-query locally decodable code C_{IS} of length $N(2)$, and the 2^{r-4}-query locally decodable code [7, Theorem 3.6] of length $N(r-4)$ for any integer $r > 5$, we can construct a $9 \cdot 2^{r-4}$-query locally decodable code C of length $N(r)$.

1.3 Application of Locally Decodable Codes

Locally decodable codes have many applications in complexity theory and cryptography (see, e.g., [8], [20]). In particular, locally decodable codes are closely related to designing efficient private information retrieval. Informally, a k-server private information retrieval is a protocol that consists of k databases $\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_k$ with identical data $\vec{x} = (x_1, x_2, \ldots, x_n)$ and a user $\mathcal{U}$, where each database $\mathcal{D}_j$ does not communicate to any other database $\mathcal{D}_h$, and allows the user $\mathcal{U}$ to retrieve x_i of $\vec{x}$, while any of the k databases $\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_k$ learns nothing about i. Private information retrieval was introduced by Chor et al. [6], and the efficiency of a k-server private information retrieval is measured by its communication complexity $C_k(n)$, i.e., the total amount of bits exchanged between $\mathcal{U}$ and $\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_k$. Trevisan [20] observed that any k-query locally decodable code with perfectly smooth decoders can be transformed into a k-server private information retrieval. For further details on k-server private information retrieval, see, e.g., [1], [3], [4], [10], [12]–[14], [16], [18], [23].

In Table 2, we summarize the known results on the communication complexity $C_k(n)$ for k-server private information retrieval. In particular, Efremenko [7, Theorem 3.6] recently showed that a communication-efficient k-server private information retrieval exists for a specific $k > 1$, i.e., for any $r > 1$, there exists a 2^r-server private information retrieval such that $C_{2^r}(n) = n^{O((\log\log n/\log n)^{1-1/r})}$, and in particular, there exists a 3-server private information retrieval such that $C_3(n) = n^{O((\log\log n/\log n)^{1/2})}$.

2. Preliminaries

2.1 Locally Decodable Codes

Let $\mathbf{F}_q$ be a finite field of q elements and $d(\vec{x}, \vec{y})$ be the Hamming distance of $\vec{x} = (x_1, x_2, \ldots, x_n) \in \mathbf{F}_q^n$ and $\vec{y} = (y_1, y_2, \ldots, y_n) \in \mathbf{F}_q^n$, i.e., the number of indices such that $x_i \neq y_i$. For any pair of integers $a \leq b$, we use $[a, b]$ to denote the set $\{a, a+1, \ldots, b\}$, and for any integer $m > 1$, let $\mathbf{Z}_m = \{0, 1, \ldots, m-1\}$ and $\mathbf{Z}_m^* = \{z \in \mathbf{Z}_m : \gcd(z, m) = 1\}$.

Definition 2.1 [15]**:** *We say that $C : \mathbf{F}_q^n \to \mathbf{F}_q^N$ is a (k, δ, ε)-*locally decodable code *if for each $i \in [1, n]$, there exists a randomized algorithm $D_i : \mathbf{F}_q^N \to \mathbf{F}_q$ such that* (1) *for any $\vec{x} = (x_1, x_2, \ldots, x_n) \in \mathbf{F}_q^n$ and any $\vec{y} \in \mathbf{F}_q^N$,* $\Pr[D_i(\vec{y}) = x_i] \geq 1 - \varepsilon$ *if $d(C(\vec{x}), \vec{y}) \leq \delta N$*; (2) *the algorithm D_i makes at most k queries to $\vec{y}$.*

We say that a (k, δ, ε)-locally decodable code $C : \mathbf{F}_q^n \to \mathbf{F}_q^N$ is *linear* if C is linear over $\mathbf{F}_q$ and is *nonadaptive* if the decoding algorithm D_i makes all its queries simultaneously. In this paper, we deal with only linear and nonadaptive (k, δ, ε)-locally decodable codes.

Definition 2.2 [20]**:** *We say that $C : \mathbf{F}_q^n \to \mathbf{F}_q^N$ has a* perfectly smooth decoder $\mathcal{D} = \{D_i\}_{i \in [1,n]}$ *if for each $\vec{x} \in \mathbf{F}_q^n$ and each $i \in [1, n]$,* $\Pr[D_i(C(\vec{x})) = x_i] = 1$*, and each query made by the randomized decoding algorithm D_i is uniformly distributed over* $[1, N]$.

Trevisan [20] observed that for a code $C : \mathbf{F}_q^n \to \mathbf{F}_q^N$, if C has a perfectly smooth decoder and makes at most k queries, then C is a $(k, \delta, k\delta)$-locally decodable code. In the rest of this paper, we consider only locally decodable codes with perfectly smooth decoders and we use a term "k-query locally decodable codes" instead of a term (k, δ, ε)-locally decodable codes.

2.2 S-Matching Vectors

For any pair of vectors $\vec{x} = (x_1, x_2, \ldots, x_h) \in \mathbf{Z}_m^h$ and $\vec{y} = (y_1, y_2, \ldots, y_h) \in \mathbf{Z}_m^h$, we use $\langle \vec{x}, \vec{y} \rangle_m$ to denote the *inner product* of $\vec{x}$ and $\vec{y}$ modulo m, i.e.,

$$\langle \vec{x}, \vec{y} \rangle_m \equiv \sum_{j=1}^{h} x_j y_j \pmod{m}.$$

Definition 2.3 [7]**:** *Let $\mathcal{U} = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_t\}$ be a family of vectors, where $\vec{u}_i \in \mathbf{Z}_m^h$, and let $S \subseteq \mathbf{Z}_m \setminus \{0\}$. We say that a family $\mathcal{U} = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_t\}$ of vectors is S-*matching *if it*

Table 2 Known results on the communication complexity.

	Upper Bound		Lower Bound	
1-Server	$n + 1$	[6]	n	[6]
2-Server	$n^{1/3}$	[6], [11]	$5 \log n$	[21]
3-Server	$n^{O((\log\log n/\log n)^{1/2})}$	[7]	—	
4-Server	$n^{1/7.87}$	[5]	—	
k-Server	$n^{O(\log\log k/k \log k)}$	[5]	—	

satisfies the following: (1) *for each* $i \in [1, t]$, $\langle \vec{u}_i, \vec{u}_i \rangle_m = 0$; (2) *for each* $i, j \in [1, t]$ *such that* $i \neq j$, $\langle \vec{u}_i, \vec{u}_j \rangle_m \in S$.

Let $m = p_1 p_2 \cdots p_r$ be a product of $r > 1$ distinct primes. Define $S_m \subseteq \mathbf{Z}_m \setminus \{0\}$ as follows: For each $s \in \mathbf{Z}_m \setminus \{0\}$, if either $s \equiv 0 \pmod{p_i}$ or $s \equiv 1 \pmod{p_i}$ for each $i \in [1, r]$, then $s \in S_m$. We refer to S_m as the *canonical* set of the integer $m = p_1 p_2 \cdots p_r$.

For each integer $t \in [1, 2^r - 1]$, we use $\mathrm{bin}(t) = (t_{r-1}, t_{r-2}, \ldots, t_0) \in \{0, 1\}^r$ to denote the binary representation of t, i.e., $t = t_{r-1} \cdot 2^{r-1} + t_{r-2} \cdot 2^{r-2} + \cdots + t_0 \cdot 2^0$, and define $s_t \in [1, m - 1]$ to be an integer such that $s_t \equiv t_{i-1} \pmod{p_i}$ for each $i \in [1, r]$. From the definition of $S_m \subseteq Z_m \setminus \{0\}$, it follows that $S_m = \{s_1, s_2. \ldots, s_{2^r - 1}\}$, where $s_0 = 0$ and $s_{2^r - 1} = 1$.

Lemma 2.1 [7, Corollary 3.3]**:** *Let* $m = p_1 p_2 \cdots p_r$ *be a product of* $r > 1$ *distinct primes and let* S_m *be the canonical set of* m*. Then there exists* $c = c(m) > 0$ *such that for any integer* $h > 0$, *there exists a family* $\mathcal{U} = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_t\}$ *of* S_m*-matching vectors such that* $\vec{u}_i \in \{0, 1\}^h \subseteq \mathbf{Z}_m^h$ *and*

$$t \geq \exp\left(c \frac{(\log h)^r}{(\log\log h)^{r-1}}\right).$$

Remark 2.1: *Let* $m = p_1 p_2 \cdots p_r$ *be a product of* $r > 1$ *distinct primes and* S_m *be the canonical set of* m*. As in the proof of* [7, Theorem 3.6], *it suffices to take*

$$h = n^{O((\log\log n/\log n)^{1-1/r})} \tag{1}$$

to define a family $\mathcal{U} = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n\}$ *of* S_m*-matching vectors for any integer* $n > 1$, *where* $\vec{u}_i \in \mathbf{Z}_m^h$.

2.3 S-Decoding Polynomials

To construct a (k, δ, ε)-locally decodable codes of short length, the following lemma is useful.

Lemma 2.2: *For an odd integer* $m > 1$, *let* $t \in [1, m - 1]$ *be the minimum integer such that* $2^t \equiv 1 \pmod{m}$*. Then there exist an element* $\gamma \in \mathbf{F}_{2^t}$ *of order* m, *i.e.,* $\gamma^m = 1$ *and* $\gamma^i \neq 1$ *for each* $i \in [1, m - 1]$.

The lemma above is a slightly stronger result of [7, Fact 2.4] and can be shown in a way similar to [7, Fact 2.4].

Let $m = p_1 p_2 \cdots p_r$ be a product of $r > 1$ distinct odd primes and $\gamma \in \mathbf{F}_{2^t}$ be an element given by Lemma 2.2. Efremenko [7] introduced a notion of S-decoding polynomials, which plays a crucial role to construct a query-efficient locally decodable code.

Definition 2.4 [7, Definition 3.4]**:** *For any* $S \subseteq \mathbf{Z}_m \setminus \{0\}$, *we say that* $P(x) \in \mathbf{F}_{2^t}[x]$ *is an* S-decoding polynomial *if it satisfies the following*: (1) $P(\gamma^s) = 0$ *for each* $s \in S$; (2) $P(\gamma^0) = 1$.

Efremenko [7] showed that there exists an S-decoding polynomial with a few monomials.

Lemma 2.3 [7, Claim 3.1]**:** *For a product* m *of* $r > 1$ *distinct odd primes and a canonical set* S_m *of* m, *there exists an* S_m*-decoding polynomial* $P_m(x)$ *over* $\mathbf{F}_{2^t}$ *with at most* $|S_m| + 1$ *monomials.*

Remark 2.2: *The number of monomials of an* S_m*-decoding polynomial is closely related to the number of queries of the corresponding locally decodable code. In fact, the number of monomials of an* S_m*-decoding polynomial is* k *iff the number of queries of the corresponding locally decodable code is* k.

From the definition of the canonical set S_m of a product $m = p_1 p_2 \cdots p_r$ of $r > 1$ distinct odd primes, it is obvious that $|S_m| = 2^r - 1$. Thus from Lemma 2.3, we immediately have the following lemma:

Lemma 2.4 [7]**:** *Let* $m = p_1 p_2 \cdots p_r$ *be a product of* $r > 1$ *distinct odd primes. Then there exists an* S_m*-decoding polynomial* $P_m(x)$ *with at most* 2^r *monomials.*

3. Known Construction

We describe the construction of (k, δ, ε)-locally decodable codes given by Efremenko [7].

Let $m = p_1 p_2 \cdots p_r$ be a product of $r > 1$ distinct odd primes, $\gamma \in \mathbf{F}_{2^t}$ be an element determined by Lemma 2.2 and $P_m(x) = a_0 + a_1 x^{b_1} + \cdots + a_{k-1} x^{b_{k-1}} \in \mathbf{F}_{2^t}[x]$ be an S_m-decoding polynomial, where S_m is the canonical set of m. For an integer $n > 1$, we take $h = n^{O((\log\log n/\log n)^{1-1/r})}$ as we have mentioned in Remark 2.1, and we construct a family $\mathcal{U} = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n\}$ of S_m-matching vectors, where $\vec{u}_i \in \mathbf{Z}_m^h$ for each $i \in [1, n]$.

In the following, we present encoding and decoding procedures by Efremenko [7], which are used in our constructions for query-efficient locally decodable codes.

3.1 Encoding

For each $i \in [1, n]$, let $\vec{e}_i \in \mathbf{F}_{2^t}^n$ be the ith unit vector. Define

```
Input:  A vector $\vec{y} \in \mathbf{F}_{2^t}^N$.
Step 1: Choose $\vec{v} \in \mathbf{Z}_m^h$ uniformly at random.
Step 2: Query $\vec{y}(\vec{v}), \vec{y}(\vec{v} + b_1\vec{u}_i), \ldots, \vec{y}(\vec{v} + b_{k-1}\vec{u}_i) \in \mathbf{F}_{2^t}$, where $\vec{y}(\vec{z})$ denotes the symbol of $\vec{y} \in \mathbf{F}_{2^t}^N$ indexed by $\vec{z} \in \mathbf{Z}_m^h$.
Step 3: Output $z_i = \gamma^{-\langle \vec{u}_i, \vec{v} \rangle_m}\{a_0 \cdot \vec{y}(\vec{v}) + a_1 \cdot \vec{y}(\vec{v} + b_1\vec{u}_i) \cdots + a_{k-1} \cdot \vec{y}(\vec{v} + b_{k-1}\vec{u}_i)\}$.
```

Fig. 1 Decoding algorithm D_i.

a code $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$ as follows: For any message $\vec{x} = (x_1, x_2, \ldots, x_n) \in \mathbf{F}_{2^t}^n$, let $C(\vec{x}) = x_1 C(\vec{e}_1) + x_2 C(\vec{e}_2) + \cdots + x_n C(\vec{e}_n)$, where for each $i \in [1, n]$,

$$C(\vec{e}_i) = \left(\gamma^{\langle \vec{u}_i, \vec{z} \rangle_m}\right)_{\vec{z} \in \mathbf{Z}_m^h}. \qquad (2)$$

Thus the code length of C is given by $N = m^h$, i.e., $N = N(r) = \exp(n^{O((\log\log n/\log n)^{1-1/r})})$.

3.2 Decoding

For each $i \in [1, n]$, a randomized decoding algorithm $D_i : \mathbf{F}_{2^t}^N \to \mathbf{F}_{2^t}$ is described in Fig. 1.

Lemma 3.1 [7, Lemma 3.5]**:** *The decoding algorithm $\mathcal{D} = \{D_i\}_{i \in [1,n]}$ is a perfectly smooth decoder.*

From Lemmas 2.1 and 2.4, we have the following result:

Theorem 3.1 [7, Theorem 3.6]**:** *For any integer $n > 1$ and any integer $r > 1$, there exists a 2^r-query locally decodable code $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$ of length $N(r)$.*

4. Query-Efficient Locally Decodable Codes

In this section, we present constructions for query-efficient locally decodable codes of short length. A key idea of our construction is to generate a k_1k_2-locally decodable code by composing a k_1-locally decodable code and a k_2-locally decodable code (see Theorem 4.1).

4.1 How to Reduce the Number of Queries

By setting $r = 2$ in Theorem 3.1, it is immediate to see that for any integer $n > 1$, there exists a 4-query locally decodable code $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$ of length $N(2)$.

Efremenko [7] found a surprising example: Let $m = 511 = 2^9 - 1 = 7 \cdot 73$ and $S_{511} = \{147, 365, 1\}$. For the integer $m = 511$, determine a finite field $\mathbf{F}_{2^t}$ and an element $\gamma \in \mathbf{F}_{2^t}$ of order $m = 511$ by Lemma 2.2. Indeed, the finite field $\mathbf{F}_{2^t}$ is $\mathbf{F}_{2^9} = \mathbf{F}_2[\gamma]/(\gamma^9 + \gamma^4 + 1)$ and $\gamma \in \mathbf{F}_{2^9}$ is an element of order 511.

Fact 4.1 [7, Example 3.7]**:** *For the integer $m = 511$, there exists an S_{511}-decoding polynomial $P_{511}(x) = \gamma^{423} \cdot x^{65} + \gamma^{257} \cdot x^{12} + \gamma^{342}$ with 3 monomials, which implies that for any $n > 1$, there exists a 3-query locally decodable code $C_{\mathrm{E}} : \mathbf{F}_{2^9}^n \to \mathbf{F}_{2^9}^N$ of length $N = N(2)$.*

The result above for the integer $m = 511$ is special. For an odd integer $m = 15 = 2^4 - 1 = 3 \cdot 5$, let $S_{15} = \{6, 10, 1\}$ and by Lemma 2.2, take the finite field $\mathbf{F}_{2^t}$ to be $\mathbf{F}_{2^4} = \mathbf{F}_2[\gamma]/(\gamma^4 + \gamma + 1)$ and the element $\gamma \in \mathbf{F}_{2^4}$ of order 15. By an exhaustive search, we verify that for the integer $m = 15$, there does not exist an S_{15}-decoding polynomial with less than 4 monomials. On the other hand, it is not the case for an odd integer $m = 2047 = 2^{11} - 1 = 23 \cdot 89$. Let $S_{2047} = \{713, 1335, 1\}$ be the canonical set of the integer $m = 2047$ and by Lemma 2.2, take the finite field $\mathbf{F}_{2^t}$ to be $\mathbf{F}_{2^{11}} = \mathbf{F}_2[\gamma]/(\gamma^{11} + \gamma^2 + 1)$ and the element $\gamma \in \mathbf{F}_{2^{11}}$ of order 2047.

Fact 4.2: *For the integer $m = 2047 = 2^{11} - 1 = 23 \cdot 89$, there exists an S_{2047}-decoding polynomial $P_{2047}(x) = \gamma^{1485} \cdot x^{29} + \gamma^{694} \cdot x^{27} + \gamma^{118}$ with 3 monomials, which implies that for any $n > 1$, there exists a 3-query locally decodable code $C_{\mathrm{IS}} : \mathbf{F}_{2^{11}}^n \to \mathbf{F}_{2^{11}}^N$ of length $N = N(2)$.*

From these observations, we see that it is impossible for every odd integer $m = p_1p_2$ to have an S_m-decoding polynomial with less than 4 monomials. Thus for an odd integer $m = p_1p_2 \cdots p_r$, we need to find structural properties of S_m-decoding polynomials to reduce the number of queries to less than 2^r.

4.2 Technical Lemmas

Let $m_1 = p_1p_2 \cdots p_r$ be a product of $r > 1$ distinct odd primes and $m_2 = q_1q_2 \cdots q_\ell$ be a product of $\ell > 1$ distinct odd primes. In the rest of this paper, assume that $\gcd(m_1, m_2) = 1$, and let $m = m_1m_2$ be a product of $r + \ell > 2$ distinct odd primes. From Lemma 2.2, we know that (1) for the odd integer m_1, there exist a finite field $\mathbf{F}_{2^{t_1}}$ with $t_1 \in [1, m_1 - 1]$ and an element $\gamma_1 \in \mathbf{F}_{2^{t_1}}$ of order m_1; (2) for the odd integer m_2, there exist a finite field $\mathbf{F}_{2^{t_2}}$ with $t_2 \in [1, m_2 - 1]$ and an element $\gamma_2 \in \mathbf{F}_{2^{t_2}}$ of order m_2; (3) for the odd integer $m = m_1m_2$, there exist a finite field $\mathbf{F}_{2^t}$ with $t \in [1, m - 1]$ and an element $\gamma \in \mathbf{F}_{2^t}$ of order m. The following lemmas are crucial for our construction.

Lemma 4.1: *For the finite fields $\mathbf{F}_{2^{t_1}}$, $\mathbf{F}_{2^{t_2}}$, and $\mathbf{F}_{2^t}$, the following holds: (1) $\mathbf{F}_{2^{t_1}}$ is a subfield of $\mathbf{F}_{2^t}$; (2) $\mathbf{F}_{2^{t_2}}$ is a subfield of $\mathbf{F}_{2^t}$; (3) $t = \mathrm{lcm}(t_1, t_2)$.*

Proof: For the statement (1), it is easy to see that $\mathbf{F}_{2^{t_1}}$ is a subfield of $\mathbf{F}_{2^t}$ iff t is divisible by t_1. From Lemma 2.2, we note that $t_1 \in [1, m_1 - 1]$ is the minimum integer with $2^{t_1} \equiv 1 \pmod{m_1}$ and $t \in [1, m - 1]$ is the minimum integer with $2^t \equiv 1 \pmod{m}$. Assume that t is not divisible by t_1, i.e., there exist $Q \geq 0$ and $0 < \rho < t_1$ such that $t = Qt_1 + \rho$. Since $m = m_1 m_2$, we have that $2^t \equiv 1 \pmod{m_1}$. From the fact that $2^{t_1} \equiv 1 \pmod{m_1}$, it follows that

$$1 \equiv 2^t \equiv 2^{Qt_1+\rho} \equiv (2^{t_1})^Q \cdot 2^\rho \equiv 2^\rho \pmod{m_1}.$$

This contradicts the fact that $t_1 \in [1, m_1 - 1]$ is the minimum integer with $2^{t_1} \equiv 1 \pmod{m_1}$. So t is divisible by t_1, which completes the proof of the statement (1). The proof of the statement (2) is analogous to that of the statement (1). The statement (3) follows from the statements (1) and (2) and the fact that $t \in [1, m - 1]$ is the minimum integer with $2^t \equiv 1 \pmod{m}$. ■

For the finite field $\mathbf{F}_{2^{t_1}}$ and the element $\gamma \in \mathbf{F}_{2^t}$ determined by Lemma 4.1, the following claims hold:

Claim 4.1: *For every $d \in \mathbf{Z}^*_{m_1}$, $\gamma^{dm_2} \in \mathbf{F}_{2^{t_1}}$ is an element of order m_1.*

Proof: Since $2^{t_1} \equiv 1 \pmod{m_1}$, there exists $Q \geq 1$ such that $2^{t_1} - 1 = Qm_1$. From the fact that the order of $\gamma \in \mathbf{F}_{2^t}$ is $m = m_1 m_2$, we have that for every $d \in \mathbf{Z}^*_{m_1}$,

$$\left(\gamma^{dm_2}\right)^{2^{t_1}-1} = \left(\gamma^{dm_2}\right)^{Qm_1} = (\gamma^m)^{Qd} = 1,$$

which implies that $\gamma^{dm_2} \in \mathbf{F}_{2^{t_1}}$. Assume by contradiction that there exists a $d \in \mathbf{Z}^*_{m_1}$ such that the order of γ^{dm_2} is $0 < \ell < m_1$, i.e., $(\gamma^{dm_2})^\ell = \gamma^{d\ell m_2} = 1$. Since the order of $\gamma \in \mathbf{F}_{2^t}$ is m, we have that $d\ell m_2$ is divisible by $m = m_1 m_2$, which implies that $d\ell$ is divisible by m_1. From the fact that $d \in \mathbf{Z}^*_{m_1}$, i.e., $\gcd(d, m_1) = 1$, it follows that ℓ is divisible by m_1, which contradicts the assumption that $0 < \ell < m_1$. ■

Claim 4.2: *In the finite field $\mathbf{F}_{2^{t_1}}$, there exist exactly $|\mathbf{Z}^*_{m_1}|$ elements of order m_1.*

Proof: For an element $g \in \mathbf{F}_{2^{t_1}}$ of order $2^{t_1} - 1$, we have that $\alpha = g^{(2^{t_1}-1)/m_1} \in \mathbf{F}_{2^{t_1}}$ is an element of order m_1. So the m_1 elements $\alpha^0, \alpha^1, \ldots, \alpha^{m_1-1}$ are the set of all elements that satisfies $x^{m_1} = 1$. It is immediate to see that for each $j \in \mathbf{Z}_{m_1}$, the order of α^j is $m_1 / \gcd(j, m_1)$. This implies that in the finite field $\mathbf{F}_{2^{t_1}}$, there exist exactly $|\mathbf{Z}^*_{m_1}|$ elements of order m_1. ■

In a way similar to the proofs of Claims 4.1 and 4.2, we can show the following claims for the finite field $\mathbf{F}_{2^{t_2}}$ and the element $\gamma \in \mathbf{F}_{2^t}$ determined by Lemma 2.2.

Claim 4.3: *For every $d \in \mathbf{Z}^*_{m_2}$, $\gamma^{dm_1} \in \mathbf{F}_{2^{t_2}}$ is an element of order m_2.*

Claim 4.4: *In the finite field $\mathbf{F}_{2^{t_2}}$, there exist exactly $|\mathbf{Z}^*_{m_2}|$ elements of order m_2.*

From Claims 4.1, 4.2, 4.3, and 4.4, we can immediately show the following lemma:

Lemma 4.2: *For the elements $\gamma_1 \in \mathbf{F}_{2^{t_1}}$, $\gamma_2 \in \mathbf{F}_{2^{t_2}}$, and $\gamma \in \mathbf{F}_{2^t}$, the following holds: (1) there exists $d_1 \in \mathbf{Z}^*_{m_1}$ such that $\gamma_1 = \gamma^{d_1 m_2}$; (2) there exists $d_2 \in \mathbf{Z}^*_{m_2}$ such that $\gamma_2 = \gamma^{d_2 m_1}$.*

Proof: The statement (1) immediately follows from Claims 4.1 and 4.2 and the statement (2) immediately follows from Claims 4.3 and 4.4. ■

Let $S_{m_1} = \{s^1_1, s^1_2, \ldots, s^1_{2^r-1}\}$ be the canonical set of m_1, $S_{m_2} = \{s^2_1, s^2_2, \ldots, s^2_{2^\ell-1}\}$ be the canonical set of m_2, and $S_m = \{s_1, s_2, \ldots, s_{2^{r+\ell}-1}\}$ be the canonical set of $m = m_1 m_2$. Let $s^1_0 = s^2_0 = s_0 = 0$.

Lemma 4.3: *For the sets S_{m_1}, S_{m_2}, and S_m, the following holds: For any $s \in S_m \cup \{0\}$, (1) $s \in S_m$ iff there exist $s^1_{i_1} \in S_{m_1} \cup \{0\}$ and $s^2_{i_2} \in S_{m_2} \cup \{0\}$ such that $s \equiv s^1_{i_1} \pmod{m_1}$, $s \equiv s^2_{i_2} \pmod{m_2}$, and either $s^1_{i_1} \neq 0$ or $s^2_{i_2} \neq 0$; (2) $s = 0$ iff $s \equiv 0 \pmod{m_1}$ and $s \equiv 0 \pmod{m_2}$.*

Proof: It follows from the definitions of S_{m_1}, S_{m_2}, and S_m and the Chinese Remainder Theorem. ■

4.3 Composition of Locally Decodable Codes

The following lemma is essential to construct query-efficient locally decodable codes.

Lemma 4.4 (Composition Lemma)**:** *For a product m_1 of $r > 1$ distinct odd primes, let $P_{m_1}(x) \in \mathbf{F}_{2^{t_1}}[x]$ be an S_{m_1}-decoding polynomial with k_1 monomials, and for a product m_2 of $\ell > 1$ distinct odd primes, let $P_{m_2}(x) \in \mathbf{F}_{2^{t_2}}[x]$ be an S_{m_2}-decoding polynomial with k_2 monomials. If $\gcd(m_1, m_2) = 1$, then we can construct an S_m-decoding polynomial $P_m(x) \in \mathbf{F}_{2^t}[x]$ with $k_1 k_2$ monomials from $P_{m_1}(x)$ and $P_{m_2}(x)$.*

Proof: For $d_1 \in \mathbf{Z}^*_{m_1}$ given by Lemma 4.2-(1) and $d_2 \in \mathbf{Z}^*_{m_2}$ given by Lemma 4.2-(2), let

$$P_m(x) = P_{m_1}(x^{d_1 m_2}) \cdot P_{m_2}(x^{d_2 m_1}) \in \mathbf{F}_{2^t}[x],$$

which is a polynomial with $k = k_1 k_2$ monomials. From Definition 2.4, we have that $P_m(1) = P_{m_1}(1) \cdot P_{m_2}(1) = 1$. From Lemma 4.2, it is immediate that

$$\begin{aligned} P_m(\gamma^s) &= P_{m_1}\left(\gamma^{d_1 m_2 s}\right) \cdot P_{m_2}\left(\gamma^{d_2 m_1 s}\right) \\ &= P_{m_1}(\gamma_1^s) \cdot P_{m_2}(\gamma_2^s). \end{aligned}$$

From Lemma 4.3, it follows that for any $s \in S_m$, there exist $s^1_{i_1} \in S_{m_1} \cup \{0\}$ and $s^2_{i_2} \in S_{m_2} \cup \{0\}$ such that $s \equiv s^1_{i_1} \pmod{m_1}$, $s \equiv s^2_{i_2} \pmod{m_2}$, and either $s^1_{i_1} \neq 0$ or $s^2_{i_2} \neq 0$. Recall that the order of $\gamma_1 \in \mathbf{F}_{2^{t_1}}$ is m_1; the order of $\gamma_2 \in \mathbf{F}_{2^{t_2}}$ is m_2; $P_{m_1}(x)$ is an S_{m_1}-decoding polynomial; $P_{m_2}(x)$ is an S_{m_2}-decoding polynomial. Then

$$\begin{aligned} & P_{m_1}\left(\gamma_1^s\right) = P_{m_1}\left(\gamma_1^{s^1_{i_1}}\right) = 0 \\ & \bigvee P_{m_2}\left(\gamma_2^s\right) = P_{m_2}\left(\gamma_1^{s^2_{i_2}}\right) = 0, \end{aligned}$$

which implies that $P_m(\gamma^s) = 0$ for any $s \in S_m$. ■

From Lemma 4.4, we have the following theorem on the constructions of locally decodable codes:

Theorem 4.1: *For a product m_1 of $r > 1$ distinct odd primes, let $C_1 : \mathbf{F}_{2^{t_1}}^n \to \mathbf{F}_{2^{t_1}}^{N_1}$ be a locally decodable code of length $N_1 = N(r)$ that has an S_{m_1}-decoding polynomial $P_{m_1}(x) \in \mathbf{F}_{2^{t_1}}[x]$ with k_1 monomials, and for a product m_2 of $\ell > 1$ distinct odd primes, let $C_2 : \mathbf{F}_{2^{t_2}}^n \to \mathbf{F}_{2^{t_2}}^{N_2}$ be a locally decodable code of length $N_2 = N(\ell)$ that has an S_{m_2}-decoding polynomial $P_{m_2}(x) \in \mathbf{F}_{2^{t_2}}[x]$ with k_2 monomials. If $\gcd(m_1, m_2) = 1$, then we can construct a locally decodable code $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$ of length $N = N(r + \ell)$ that has an S_m-decoding polynomial $P_m(x) \in \mathbf{F}_{2^t}[x]$ with k_1k_2 monomials.*

Proof: For $m = m_1m_2$ and $h > 0$ given by (1), define $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$ as follows: For $\vec{x} = (x_1, x_2, \ldots, x_n) \in \mathbf{F}_{2^t}^n$, let $C(\vec{x}) = x_1C(\vec{e}_1) + x_2C(\vec{e}_2) + \cdots + x_nC(\vec{e}_n)$, where for each $i \in [1, n]$, $C(\vec{e}_i)$ is given by (2). Thus we have that $N = m^h = N(r + \ell)$. From Lemma 4.4, let

$$\begin{aligned} P_m(x) &= P_{m_1}(x^{d_1m_2}) \cdot P_{m_2}(x^{d_2m_1}) \\ &= a_0 + a_1x^{b_1} + \cdots + a_{k-1}x^{k-1} \end{aligned}$$

be an S_m-decoding polynomial with $k = k_1k_2$ monomials. For each $i \in [1, n]$, a randomized decoding algorithm D_i can be defined exactly the same as Fig. 1. For each $i \in [1, n]$, we have that

$$\begin{aligned} D_i(C(\vec{x})) &= D_i\left(\sum_{j=1}^{n} x_jC(\vec{e}_j)\right) \\ &= \sum_{j=1}^{n} x_jD_i(C(\vec{e}_j)). \end{aligned}$$

For each $i \in [1, n]$ and each $j \in [1, n] \setminus \{i\}$, it suffices to show that $\Pr[D_i(C(\vec{e}_i)) = 1] = 1$ and $\Pr[D_i(C(\vec{e}_j)) = 0] = 1$. From (2) and Lemma 4.4, it follows that for k queries $\vec{v}, \vec{v} + b_1\vec{u}_i, \ldots, \vec{v} + b_{k-1}\vec{u}_i \in Z_m^h$,

$$\begin{aligned} &D_i(C(\vec{e}_i)) \\ &= \gamma^{-\langle\vec{u}_i,\vec{v}\rangle_m} \cdot \Big(a_0\gamma^{\langle\vec{u}_i,\vec{v}\rangle_m} + a_1\gamma^{\langle\vec{u}_i,\vec{v}+b_1\vec{u}_i\rangle_m} \\ &\quad + \cdots + a_{k-1}\gamma^{\langle\vec{u}_i,\vec{v}+b_{k-1}\vec{u}_i\rangle_m}\Big) \\ &= \gamma^{-\langle\vec{u}_i,\vec{v}\rangle_m} \cdot \Big(a_0\gamma^{\langle\vec{u}_i,\vec{v}\rangle_m} + a_1\gamma^{\langle\vec{u}_i,\vec{v}\rangle_m}\gamma^{b_1\langle\vec{u}_i,\vec{u}_i\rangle_m} \\ &\quad + \cdots + a_{k-1}\gamma^{\langle\vec{u}_i,\vec{v}\rangle_m}\gamma^{b_{k-1}\langle\vec{u}_i,\vec{u}_i\rangle_m}\Big) \\ &= a_0 + a_1\gamma^{b_1\langle\vec{u}_i,\vec{u}_i\rangle_m} + \cdots + a_{k-1}\gamma^{b_{k-1}\langle\vec{u}_i,\vec{u}_i\rangle_m} \\ &= P_m\left(\gamma^{\langle\vec{u}_i,\vec{u}_i\rangle_m}\right) = P_m(1) = 1; \\ &D_i(C(\vec{e}_j)) \\ &= \gamma^{-\langle\vec{u}_i,\vec{v}\rangle_m} \cdot \Big(a_0\gamma^{\langle\vec{u}_j,\vec{v}\rangle_m} + a_1\gamma^{\langle\vec{u}_j,\vec{v}+b_1\vec{u}_i\rangle_m} \\ &\quad + \cdots + a_{k-1}\gamma^{\langle\vec{u}_j,\vec{v}+b_{k-1}\vec{u}_i\rangle_m}\Big) \\ &= \gamma^{-\langle\vec{u}_i,\vec{v}\rangle_m} \cdot \Big(a_0\gamma^{\langle\vec{u}_j,\vec{v}\rangle_m} + a_1\gamma^{\langle\vec{u}_j,\vec{v}\rangle_m}\gamma^{b_1\langle\vec{u}_i,\vec{u}_j\rangle_m} \\ &\quad + \cdots + a_{k-1}\gamma^{\langle\vec{u}_j,\vec{v}\rangle_m}\gamma^{b_{k-1}\langle\vec{u}_i,\vec{u}_j\rangle_m}\Big) \end{aligned}$$

$$\begin{aligned} &= \gamma^{-\langle\vec{u}_i,\vec{v}\rangle_m} \cdot \gamma^{\langle\vec{u}_j,\vec{v}\rangle_m} \cdot \Big(a_0 + a_1\gamma^{b_1\langle\vec{u}_i,\vec{u}_j\rangle_m} \\ &\quad + \cdots + a_{k-1}\gamma^{b_{k-1}\langle\vec{u}_i,\vec{u}_j\rangle_m}\Big). \\ &= \gamma^{-\langle\vec{u}_i,\vec{v}\rangle_m} \cdot \gamma^{\langle\vec{u}_j,\vec{v}\rangle_m} \cdot P_m\left(\gamma^{\langle\vec{u}_i,\vec{u}_j\rangle_m}\right) = 0. \end{aligned}$$

Thus $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$ is a locally decodable code of length $N = N(r + \ell)$ that has an S_m-decoding polynomial $P_m(x) \in \mathbf{F}_{2^t}[x]$ with k_1k_2 monomials. ■

From Theorem 4.1 and Remark 2.2, we can derive the following corollaries on the constructions of query-efficient locally decodable codes:

Corollary 4.1: *For any integer $n > 1$ and any integer $r > 3$, there exists a $3 \cdot 2^{r-2}$-query locally decodable code $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$ of length $N(r)$.*

Proof: As given in Fact 4.1, Efremenko [7, Example 3.7] showed that for an odd integer $m_1 = 511 = 2^9 - 1 = 7 \cdot 73$, there exists a 3-query locally decodable code $C_{\mathrm{E}} : \mathbf{F}_{2^{t_1}}^n \to \mathbf{F}_{2^{t_1}}^{N_1}$ of length $N_1 = N(2)$ that has an S_{m_1}-decoding polynomial $P_{m_1}(x) \in \mathbf{F}_{2^{t_1}}[x]$ with 3 monomials. Efremenko [7, Theorem 3.6] also derived that for a product m' of $\ell > 1$ distinct odd primes, there exists a 2^ℓ-query locally decodable code $C' : \mathbf{F}_{2^{t'}}^n \to \mathbf{F}_{2^{t'}}^{N'}$ of length $N' = N(\ell)$ that has an $S_{m'}$-decoding polynomial $P_{m'}(x) \in \mathbf{F}_{2^{t'}}[x]$ with 2^ℓ monomials. For any integer $r > 3$, we take a product m_2 of $r - 2$ distinct odd primes such that $\gcd(m_1, m_2) = 1$ and construct a 2^{r-2}-query locally decodable code $C_2 : \mathbf{F}_{2^{t_2}}^n \to \mathbf{F}_{2^{t_2}}^{N_2}$ of length $N_2 = N(r - 2)$ that has an S_{m_2}-decoding polynomial $P_{m_2}(x)$ with 2^{r-2} monomials. Applying Theorem 4.1 to the 3-query locally decodable code C_{E} and the 2^{r-2}-query locally decodable code C_2, we can construct a $3 \cdot 2^{r-2}$-query locally decodable code $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$ of length $N(r)$ that has an S_m-decoding polynomial $P_m(x) \in \mathbf{F}_{2^t}[x]$ with $3 \cdot 2^{r-2}$ monomials. ■

Corollary 4.2: *For any integer $n > 1$ and any integer $r > 5$, there exists a $9 \cdot 2^{r-4}$-query locally decodable code $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$ of length $N(r)$.*

Proof: For any integer $r > 5$, take a product m_1 of $r - 4$ distinct odd primes such that $\gcd(m_1, 511 \cdot 2047) = 1$. Then there exists a 2^{r-4}-query locally decodable code $C_1 : \mathbf{F}_{2^{t_1}}^n \to \mathbf{F}_{2^{t_1}}^{N_1}$ of length $N_1 = N(r - 4)$ that has an S_{m_1}-decoding polynomial $P_{m_1}(x)$ with 2^{r-4} monomials. Applying Theorem 4.1 to the 3-query locally decodable code C_{E} given in Fact 4.1, the 3-query locally decodable code C_{IS} given in Fact 4.2, and the 2^{r-4}-query locally decodable code C_1, we can construct a $9 \cdot 2^{r-4}$-query locally decodable code $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$ of length $N(r)$ that has an S_m-decoding polynomial $P_m(x) \in \mathbf{F}_{2^t}[x]$ with $9 \cdot 2^{r-4}$ monomials. ■

5. Concluding Remarks

In this paper, we have shown the Composition Theorem that constructs a k_1k_2-query locally decodable code by composing a k_1-query locally decodable code and a k_2-query locally decodable code (see Theorem 4.1). As the application of Theorem 4.1, we have also shown that (Corollary 4.1) for any integer $r > 3$, there exists a $3 \cdot 2^{r-2}$-query locally decodable code $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$ of length $N(r)$ and (Corollary 4.2) for any integer $r > 5$, there exists a $9 \cdot 2^{r-4}$-query locally decodable code $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$ of length $N(r)$.

For perfectly smooth decoders, we can immediately modify Theorem 4.1 as follows:

Theorem 5.1: *For a product m_1 of $r > 1$ distinct odd primes, let $C_1 : \mathbf{F}_{2^{t_1}}^n \to \mathbf{F}_{2^{t_1}}^{N_1}$ be a k_1-query locally decodable code of length $N_1 = N(r)$ that has a perfectly smooth decoder $\mathcal{D}_1$ and an S_{m_1}-decoding polynomial $P_{m_1}(x) \in \mathbf{F}_{2^{t_1}}[x]$ with k_1 monomials, and for a product m_2 of $\ell > 1$ distinct odd primes, let $C_2 : \mathbf{F}_{2^{t_2}}^n \to \mathbf{F}_{2^{t_2}}^{N_2}$ be a k_2-query locally decodable code of length $N_2 = N(\ell)$ that has a perfectly smooth decoder $\mathcal{D}_2$ and an S_{m_2}-decoding polynomial $P_{m_2}(x) \in \mathbf{F}_{2^{t_2}}[x]$ with k_2 monomials. If $\gcd(m_1, m_2) = 1$, then we can construct a k_1k_2-query locally decodable code $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$ of length $N = N(r + \ell)$ that has a perfectly smooth decoder $\mathcal{D}$ and an S_m-decoding polynomial $P_m(x) \in \mathbf{F}_{2^t}[x]$ with k_1k_2 monomials.*

From Theorem 5.1 and Corollaries 4.1 and 4.2, we can transform k-query locally decodable codes with perfectly smooth decoders to communication-efficient k-server private information retrieval [20].

Theorem 5.2: *For any integer $n > 1$ and any integer $r > 3$, there exists a $3 \cdot 2^{r-2}$-server private information retrieval with the communication complexity*

$$C_k(n) = n^{O\left(\left(\log\log n/\log n\right)^{1-1/r}\right)},$$

and for any integer $n > 1$ and any integer $r > 5$, there exists a $9 \cdot 2^{r-4}$-server private information retrieval with the communication complexity

$$C_k(n) = n^{O\left(\left(\log\log n/\log n\right)^{1-1/r}\right)},$$

At present, we know only 3-query locally decodable codes $C_{\mathrm{E}} : \mathbf{F}_{2^9}^n \to \mathbf{F}_{2^9}^N$ of length $N = N(2)$ for an add integer $m_1 = 511 = 2^9 - 1 = 7 \cdot 73$ [7, Example 3.7] and $C_{\mathrm{IS}} : \mathbf{F}_{2^{11}}^n \to \mathbf{F}_{2^{11}}^N$ of length $N = N(2)$ for an odd integer $m_2 = 2047 = 2^{11} - 1 = 23 \cdot 89$ (see Fact 4.2). Let $\mathcal{M}_r$ be a set of integers, each of which is a product of $r > 1$ distinct odd primes.

From Composition Theorem (see Theorem 4.1), we have that if there exist $m_1, m_2, \ldots, m_\ell \in \mathcal{M}_2$ such that $\gcd(m_i, m_j) = 1$ for each $1 \le i < j \le \ell$ and each $m_i \in \mathcal{M}_2$ generates a 3-query locally decodable code $C_i : \mathbf{F}_{2^{t_i}}^n \to \mathbf{F}_{2^{t_i}}^{N_i}$ of length $N_i = N(2)$ that has an S_{m_i}-decoding polynomial $P_{m_i}(x) \in \mathbf{F}_{2^{t_i}}[x]$ with 3 monomials, then for the integer $m = m_1 m_2 \cdots m_\ell$, we can construct a 3^ℓ-query locally decodable code $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$ of length $N = N(2\ell)$ that has an S_m-decoding polynomial $P_m(x) \in \mathbf{F}_{2^t}[x]$ with 3^ℓ monomials. For integers less than 2048, however, we do know only such integers $m_1 = 511 \in \mathcal{M}_2$ and $m_2 = 2047 \in \mathcal{M}_2$.

Thus the following problems are both of theoretical interest and of practical importance.

(1) Find integers $m \in \mathcal{M}_2 \setminus \{511, 2047\}$ that generate a 3-query locally decodable code $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$, i.e., the code C has an S_m-decoding polynomial $P(x) \in \mathbf{F}_{2^t}[x]$ with 3 monomials.

(2) For any integer $r > 3$, find an integer $m \in \mathcal{M}_r$ that generate a k-query locally decodable code $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$ that has an S_m-decoding polynomial $P(x) \in \mathbf{F}_{2^t}[x]$ with $k < 3 \cdot 2^{r-2}$ monomials.

(3) For any integer $r > 5$, find an integer $m \in \mathcal{M}_r$ that generate a k-query locally decodable code $C : \mathbf{F}_{2^t}^n \to \mathbf{F}_{2^t}^N$ that has an S_m-decoding polynomial $P(x) \in \mathbf{F}_{2^t}[x]$ with $k < 9 \cdot 2^{r-4}$ monomials.

Acknowledgments

The authors would like to thank Osamu Watanabe for his insightful discussions for the earlier version of the paper. The authors also wish to thank anonymous referees for their valuable comments on the paper.

References

[1] A. Ambainis, "Upper bound on the communication complexity of private information retrieval," Proc. 24th International Colloquium on Automata, Languages, and Programming, Lect. Notes Comput. Sci., vol.1256, pp.401–407, 1997.

[2] L. Babai, L. Fortnow, L. Levin, and M. Szegedy, "Checking computation in polylogarithmic time," Proc. 23rd Annual ACM Symposium on Theory of Computing, pp.21–31, 1991.

[3] A. Beimel, L. Fortnow, and W. Gasarch, "A tight lower bound for restricted PIR protocols," Comoutat. Comlex., vol.15, pp.82–91, 2006.

[4] A. Beimel, Y. Ishai, and E. Kushilevitz, "General constructions for information-theoretic private information retrieval," J. Comput. Syst. Sci., vol.71, no.2, pp.213–247, 2005.

[5] A. Beimel, Y. Ishai, E. Kushilevitz, and F. Raymond, "Breaking the $O(n^{\frac{1}{2k-1}})$ barrier for information-theoretic private information retrieval," Proc. 43rd IEEE Annual Symposium on Foundations of Computer Science, pp.261–270, 2002.

[6] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," Proc. 36th IEEE Annual Symposium on Foundations of Computer Science, pp.41–51, 1995.

[7] K. Efremenko, "3-query locally decodable codes of subexponential length," Electronic Colloquium on Computational Complexity, Report no.69, 2008.

[8] W. Gasarch, "A survey on private information retrieval," Bull, EATCS 82, pp.72–107, 2004.

[9] O. Goldreich, "Short locally testable codes and proofs," Electronic Colloquium on Computational Complexity, Report no.14, 2005.

[10] O. Goldreich, H. Karloff, L.J. Schulman, and L. Trevisan, "Lower bounds for linear locally decodable codes and private information retrieval," Proc. 17th IEEE Annual Conference on Computational Complexity, pp.175–183, 2002.

[11] Y. Ishai and E. Kushilevitz, "Improved upper bounds on information-theoretic private information retrieval," Proc. 31st Annual ACM Symposium on Theory of Computing, pp.79–88, 1999.

[12] T. Itoh, "Efficient private information retrieval," IEICE Trans. Fundamentals, vol.E82-A, no.1, pp.11–20, Jan. 1999.

[13] T. Itoh, “On lower bound for the communication complexity of private information retrieval,” IEICE Trans. Fundamentals, vol.E84-A, no.1, pp.157–164, Jan. 2001.

[14] I. Kerenidis and R. de Wolf, “Exponential lower bound for 2-query locally decodable code via a quantum argument,” Proc. 35th Annual ACM Symposium on Theory of Computing, pp.106–115, 2003.

[15] J. Katz and L. Trevisan, “On the efficiency of locally decoding procedures for error-correcting codes,” Proc. 32nd Annual ACM Symposium on Theory of Computing, pp.80–86, 2000.

[16] E. Mann, Private Access to Distributed Information. Master’s Thesis, Technion – Israel Institute of Technology, Haifa, Israel, 1998.

[17] A. Polisgchuk and D. Spielman, “Nearly-linear size holographic proofs,” Proc. 26th Annual ACM Symposium on Theory of Computing, pp.194–203, 1994.

[18] A. Razborov and S. Yekhanin, “An $\Omega(n^{1/3})$ lower bounds for bilinear group based private information retrieval,” Proc. 47th Annual IEEE Symposium on Foundations of Computer Science, pp.739–748, 2006.

[19] M. Sudan, Efficient Checking of Polynomials and Proofs and the Hardness of Approximation Problems, Ph.D. Thesis, University of California at Berkeley, 1992.

[20] R. Trevisan, “Some applications of coding theory in computational complexity,” Quad. Matemat. 13, Electronic Colloquium on Computational Complexity, Report no.43, pp.347–424, 2004.

[21] S. Wehner and R. de Wolf, “Improved lower bound for locally decodable codes and private information retrieval,” Proc. 32nd International Colloquium on Automata, Languages, and Programming, Lect. Notes Comput. Sci., vol.3580, pp.1424–1436, 1997.

[22] D. Woodruff, “New lower bounds for general locally decodable codes,” Electronic Colloquium on Computational Complexity, Report no.6, 2007.

[23] D. Woodruff and S. Yekhanin, “A geometric approach to information theoretic private information retrieval,” SIAM J. Comput., vol.37, no.4, pp.1046–1056, 2007.

[24] S. Yekhanin, “Towards 3-query locally decodable codes of subexponential length,” Proc. 39th Annual ACM Symposium on Theory of Computing, pp.266–274, 2007.

[25] S. Yekhanin, “Towards 3-query locally decodable codes of subexponential length,” J. ACM, vol.55, no.1, pp.1–16, 2008.

Toshiya Itoh was born in Urawa, Japan, in 1959. He received the B.E., M.E., and Dr. Eng. degree in electronic engineering in 1982, 1984, and 1988, respectively from Tokyo Institute of Technology, Tokyo, Japan. From 1985 to 1990, he was an Assistant Professor in the Department of Electrical and Electronic Engineering at Tokyo Institute of Technology, and from 1990 to 1992, he was a Lecturer in the Department of Information Processing at Tokyo Institute of Technology. From 1992 to 2001, he was an Associate Professor in the Department of Information Processing at Tokyo Institute of Technology, and since 2001, he has been a Professor in the Global Scientific Information and Computing Center at Tokyo Institute of Technology. His current interests are discrete algorithms, combinatorics, and complexity theory. Dr. Itoh is a member of the Information Processing Society of Japan, the Association for Computing Machinery, and LA.

Yasuhiro Suzuki was born in Iwata, Japan, in 1984. He received the B.E. degree in 2009 from Tokyo Institute of Technology, and since 2009, he has been a master course student in the Department of Information Processing at Tokyo Institute of Technology. His current research interests are discrete algorithms, approximation algorithms, and complexity theory.