How to Correct Errors in Multi-Server PIR

Kaoru Kurosawa

Ibaraki University,
kaoru.kurosawa.kk@vc.ibaraki.ac.jp

Abstract. Suppose that there exist a user and ℓ servers $S_1, ..., S_\ell$. Each server S_j holds a copy of a database $\mathbf{x} = (x_1, \ldots, x_n) \in \{0,1\}^n$, and the user holds a secret index $i_0 \in \{1, \ldots, n\}$. A b error correcting ℓ server PIR (Private Information Retrieval) scheme allows a user to retrieve x_{i_0} correctly even if and b or less servers return false answers while each server learns no information on i_0 in the information theoretic sense. Although there exists such a scheme with the total communication cost $O(n^{1/(2k-1)} \times k\ell \log \ell)$ where $k = \ell - 2b$, the decoding algorithm is very inefficient.
In this paper, we show an efficient decoding algorithm for this b error correcting ℓ server PIR scheme. It runs in time $O(\ell^3)$.

keywords. Private Information Retrieval, information theoretic, error correcting

1 Introduction

Private information retrieval (PIR) was introduced by Chor, Kushilevitz, Goldreich and Sudan [9]. In this model, a server S holds a database $\mathbf{x} = (x_1, \ldots, x_n) \in \{0,1\}^n$, and a user holds a secret index $i_0 \in \{1, \ldots, n\}$. The user should be able to retrieve x_{i_0} without revealing no information on i_0 to the server S. A trivial solution is that S sends the entire $\mathbf{x}$ to the user. Can the user obtain x_{i_0} with less than n bits of communication ?

Unfortunately, Chor et al. [9] showed that n bits are required in the information theoretic setting. (In what follows, we consider information theoretic setting.) To get around this, they considered an ℓ server PIR scheme such that each server S_j has a copy of the database $\mathbf{x}$, where the ℓ servers do not communicate each other. In particular, they showed a two server protocol whose total communication cost is $O(n^{1/3})$. [1] The ℓ server PIR schemes have been improved further by [1, 3, 4, 22, 13, 16, 7, 11].

Beimel and Stahl [5] considered what can be done if some of the servers break down. In a (k, ℓ) robust PIR schemes, the user can retrieve x_{i_0} if

[1] i.e., the total number of bits communicated between the user and the servers.

k out of ℓ servers respond. Woodruff and Yekhanin [21] showed a (k, ℓ) robust PIR scheme whose total communication cost is

$$O(n^{1/(2k-1)} \times k\ell \log \ell).$$

Currently this is the best known (k, ℓ) robust PIR scheme.

Beimel and Stahl [5] also considered what can be done if some of the servers return false answers. A b-error correcting ℓ server PIR scheme is a (ℓ, ℓ) robust PIR scheme with the additional property such that the user can compute x_{i_0} correctly even if b (or less) servers return false answers. They [5] showed that a (k, ℓ) robust PIR scheme can be used as a b error correcting ℓ server PIR scheme if

$$\ell \geq k + 2b.$$

However, their generic decoding algorithm is very inefficient as they mentioned in [5, page 314].

To summarize, although there exists a b error correcting ℓ server PIR scheme with the total communication cost $O(n^{1/(2k-1)} \times k\ell \log \ell)$ [5, 21], where $k = \ell - 2b$, the decoding algorithm [5] is very inefficient.

In this paper, we show an efficient decoding algorithm for the above b error correcting ℓ server PIR scheme. The running time is $O(\ell^3)$. We achieve this by extending Berlekamp-Welch decoding algorithm [6] for Reed-Solomon codes to our problem. While a codeword is defined by using a polynomial $f(x)$ in a Reed-Solomon code, it is defined by using $(f(x), f'(x))$ in the b error correcting ℓ server PIR scheme. This is the difficulty which we must overcome.

A ℓ server PIR scheme is said to be t-private if any coalition of t servers learn no information on i_0. Woodruff and Yekhanin [21] showed a t-private (k, k) robust PIR scheme with the total communication cost $O(n^{\lfloor (2k-1)/t \rfloor} \times k\ell/t \ \log \ell)$. It is easily generalized to a t-private (k, ℓ) robust PIR scheme, and the latter can be used as a t-private b error correcting ℓ server PIR scheme if $\ell \geq k + 2b$ [5]. Our decoding algorithm can be applied to this scheme too.

1.1 Related Works

Goldberg [14] and Devet et al. [12] considered the case where the user retrieves a block instead of each x_i. For example, a block is $(x_1, \ldots, x_{\sqrt{n}})$. The size of each block is $\sqrt{nw}$ for some w in their schemes. Hence the total communication cost is at least $\Omega(\sqrt{n})$.

Sun et al. [19, 20] and Banawan et al. [2] considered the case where the size of x_i is very large, and hence only the download cost is of interest (but not the upload cost).

In the computatioanl setting, PIR has been studied by [8, 17, 10, 18, 15].

2 Preliminaries

2.1 PIR

In the model of (k, ℓ) robust PIR schemes, there exist ℓ servers $S_1, ..., S_\ell$ such that each server S_j has a copy of a database $\mathbf{x} = (x_1, \ldots, x_n) \in \{0,1\}^n$. The user should be able to retrieve x_{i_0} if k servers respond while any server S_j should learn no information on i_0 in the information theoretic sense.

Definition 1. A (k, ℓ) robust PIR scheme consists of three algorithms $(\mathcal{Q}, \mathcal{A}, \mathcal{C})$ as follows.

1. The user U runs $\mathcal{Q}(n, i_0)$ to generate ℓ queries $(q_1, ..., q_\ell)$ together with an auxiliary information aux.
2. He sends q_j to server S_j for $j = 1, \ldots, \ell$.
3. Each server S_j returns $a_j = \mathcal{R}_0(j, \mathbf{x}, q_j)$ to U, where $\mathbf{x} = (x_1, \ldots, x_n) \in \{0,1\}^n$ is a copy of a database.
4. Upon receiving (at least) k answers $a_{j_1}, \ldots, a_{j_k}$ from servers, U runs

$$\mathcal{C}((j_1, a_{j_1}), ..., (j_k, a_{j_k}), aux)$$

to compute x_{i_0}.

It must satisfy the following requirements.

- Correctness :
  For any n, $\mathbf{x} \in \{0,1\}^n$, $i_0 \in \{1, \ldots, n\}$ and $\{j_1, \ldots, j_k\} \subset \{1, \ldots, \ell\}$, it holds that
  $$\mathcal{C}((j_1, a_{j_1}), ..., (j_k, a_{j_k}), aux) = x_{i_0}$$
  if $(q_1, ..., q_\ell)$ and $(a_1, ..., a_\ell)$ are computed from n, $\mathbf{x} \in \{0,1\}^n$ and $i_0 \in \{1, \ldots, n\}$.
- Privacy :
  Any server learns no information on i_0. Formally, for any $i_1, i_2 \in \{1, \ldots, n\}$, q_j generated by $\mathcal{Q}(n, i_1)$ and q_j generated by $\mathcal{Q}(n, i_2)$ are identically distributed for $j = 1, \ldots, \ell$.

Definition 2. A b-error correcting ℓ server PIR scheme is a (ℓ, ℓ) robust PIR scheme with the additional property such that the user can compute x_{i_0} correctly even if b (or less) answers among $(a_1, \ldots, a_\ell)$ are false.

Definition 3. The total communication cost of a (k, ℓ) robust PIR scheme is the number of bits communicated between the user U and the ℓ servers $S_1, ..., S_\ell$.

The total communication cost of a b-error correcting ℓ server PIR scheme is defined similarly.

.

2.2 Technical Lemma

Woodruff and Yekhanin [21] proved the following lemma.

Lemma 1. *Suppose that (y_i, u_i) are given for $i = 1, \ldots, s$, where $y_i \in \mathbb{F}_p$ and $u_i \in \mathbb{F}_p$. Then there exists at most one polynomial $f(\lambda)$ over $\mathbb{F}_p$ of degree $\leq 2s - 1$ such that $f(i) = y_i$ and $f'(i) = u_i$ for $i = 1, \ldots, s$.*

3 Robust PIR of Woodruff and Yekhanin

Let

$$\mathbf{x} = (x_1, \ldots, x_n) \in \{0, 1\}^n$$

be a database. Woodruff and Yekhanin [21] showed a (k, ℓ) robust PIR scheme such that the total communication cost is

$$O(n^{1/(2k-1)} \times k\ell \log \ell).$$

In their (k, k)-robust PIR scheme, the user somehow obtains $(f(i), f'(i))$ from a server S_i for $i = 1, \ldots, k$, where $f(\lambda)$ is a polynomial of degree $2k - 1$ such that $f(0) = x_{i_0}$. He then reconstruct $f(\lambda)$ from

$$(f(1), f'(1)), \ldots, (f(k), f'(k)).$$

3.1 (k, k)-robust PIR scheme

For a given (n, k), consider m such that

$$\binom{m}{2k-1} \geq n. \tag{1}$$

There exists such m which also satisfies [21]

$$m = O(kn^{1/(2k-1)}). \tag{2}$$

Then we can consider an injection

$$E : \{1, \ldots, n\} \to \{0,1\}^m$$

such that each $E(i)$ has the Hamming weight $2k-1$.

Let p be a prime such that $k < p \le 2k$. For a database $\mathbf{x} = (x_1, \ldots, x_n) \in \{0,1\}^n$, define a function $F : \mathbb{F}_p^m \to \mathbb{F}_p$ by

$$F(z_1, \ldots, z_m) = x_1 \cdot (\prod_{E(1)_j=1} z_j) + \ldots + x_n \cdot (\prod_{E(n)_j=1} z_j) \tag{3}$$

where $E(i)_j$ is the jth coordinate of $E(i) \in \{0,1\}^m$.

For example, let $n = m = 4$ and $2k-1 = 3$. Define E as

$$E(1) = (1110), E(2) = (1101), E(3) = (1011), E(4) = (0111).$$

Then

$$F(z_1, \ldots, z_4) = x_1(z_1z_2z_3) + x_2(z_1z_2z_4) + x_3(z_1z_3z_4) + x_4(z_2z_3z_4).$$

(A1) The degree of $F(z_1, \ldots, z_m)$ is $2k-1$ because each $E(i)$ has the Hamming weight $2k-1$.

(A2) For each i, it holds that $F(E(i)) = x_i$.

Their (k,k)-robust PIR scheme is as follows.

1. The user chooses $\mathbf{V} = (v_1, \ldots, v_m) \in \mathbb{F}_p^m$ randomly.
2. For $i = 1, \ldots, k$, he sends

   $$\mathbf{Q}_i = E(i_0) + i \cdot \mathbf{V} \in \mathbb{F}_p^m$$

   to a server S_i, where i_0 is the secret index of the user.
3. For $i = 1, \ldots, k$, S_i returns $y_i \in \mathbb{F}_p$ and $\mathbf{B}_i \in \mathbb{F}_p^m$ such that

   $$y_i = F(\mathbf{Q}_i)$$
   $$\mathbf{B}_i = (F_{z_1}(\mathbf{Q}_i), \ldots, F_{z_m}(\mathbf{Q}_i))$$

   to the user, where F is defined by eq.(3) and F_z is the partial derivative of F by z.

Now define

$$f(\lambda) = F(E(i_0) + \lambda \mathbf{V}). \tag{4}$$

Then the degree of $f(\lambda)$ is $2k-1$ from (A1). Therefore $f(\lambda)$ is written as

$$f(\lambda) = a_0 + a_1\lambda + \ldots + a_{2k-1}\lambda^{2k-1}. \tag{5}$$

Further it holds that

$$f(i) = y_i, \tag{6}$$

$$f'(i) = \mathbf{B}_i \cdot \mathbf{V}^T \tag{7}$$

for $i = 1, \ldots, k$. (Eq.(7) is obtained by using the chain rule.) The above equations give $2k$ linear equation in $(a_0, \ldots, a_{2k-1})$.

The user computes $(a_0, \ldots, a_{2k-1})$ by solving this set of equations. Finally the user obtains x_{i_0} from

$$x_{i_0} = F(E(i_0)) = f(0) = a_0.$$

See (A2).

(Privacy) For any i, $\mathbf{Q}_i = E(i_0) + i \cdot \mathbf{V}$ is random because $\mathbf{V}$ is randomly chosen. Therefore any sever S_i learns no information on i_0.

(Communication Cost) The user sends $\mathbf{Q}_i \in \mathbb{F}_p^m$ to each sever S_i, and S_i returns $(y_i, \mathbf{B}_i) \in \mathbb{F}_p^{m+1}$. Since $m = O(kn^{1/(2k-1)})$ and $p \leq 2k$, the total communication cost is given by

$$O(n^{1/(2k-1)} \times k^2 \log k).$$

3.2 (k, ℓ)-robust PIR

Let p be a prime such that $\ell < p \leq 2\ell$. Then the above scheme is easily generalized to a (k, ℓ)-robust PIR scheme. In step 2 and 3, just replace "$i = 1, \ldots, k$" with "$i = 1, \ldots, \ell$".

The total communication cost is given by

$$O(n^{1/(2k-1)} \times k\ell \log \ell).$$

4 Error Correcting PIR of Beimel and Stahl

Beimel and Stahl [5] showed that a robust PIR scheme can be used as an error correcting PIR.

Proposition 1. *A (k, ℓ) robust PIR scheme is also a b error correcting ℓ server PIR if*

$$\ell \geq k + 2b.$$

Their generic decoding algorithm is as follows.

1. For each subset B of servers such that $|B| = k$, compute x_{i_0} by running the (k, ℓ) robust PIR scheme.
2. Find the largest A such that for every $B \subset A$ such that $|B| = k$, the user reconstructs the same value of x_{i_0}.
3. Output this value as the value of x_{i_0}.

This algorithm is, however, very inefficient because $\binom{\ell}{k}$ is very large in general, as Beimel and Stahl mentioned in [5, page 314].

From Proposition 1 [5], the (k, ℓ) robust PIR scheme of Woodruff and Yekhanin [21] is also a b error correcting ℓ server PIR scheme if $\ell \geq k + 2b$. However, the decoding algorithm is very inefficient as shown above.

For this b error correcting ℓ server PIR scheme we can consider a variant of the decoding algorithm such as follows.

1. For each subset **BAD** of servers such that $|\mathbf{BAD}| = b$, check if the user reconstructs the same value of x_{i_0} for every $B \subset A \setminus \mathbf{BAD}$ such that $|B| = k$.
2. If the check succeeds, then output this value as the value of x_{i_0}.

Still it is very inefficient because $\binom{\ell}{b}$ is very large in general.

To summarize, although there exists a b error correcting ℓ server PIR scheme with the total communication cost $O(n^{1/(2k-1)} \times k\ell \log \ell)$ [5, 21], where $k = \ell - 2b$, the decoding algorithm [5] is very inefficient.

5 Proposed Decoding Algorithm

In this section, we show an efficient decoding algorithm for the above b error correcting ℓ server PIR scheme. The running time is $O(\ell^3)$.

We achieve this by extending Berlekamp-Welch decoding algorithm [6] for Reed-Solomon codes to our problem. While a codeword is defined by using a polynomial $f(x)$ in a Reed-Solomon code, it is defined by using $(f(x), f'(x))$ in the b error correcting ℓ server PIR scheme. This is the difficulty which we must overcome.

5.1 Berlekamp-Welch Algorithm

Consider a Reed Solomon code of length ℓ with dimension k over $\mathbb{F}_p$. A codeword is given by

$$\mathbf{c} = (f(1), \ldots, f(\ell))$$

for some polynomial $f(\lambda)$ of degree at most $k-1$. Let

$$\mathbf{r} = (r_1, \ldots, r_\ell)$$

be the received vector which includes at most b errors, where

$$\ell \geq 2b + k. \tag{8}$$

Note that $r_i = f(i)$ if r_i has no error.

Now Berlekamp-Welch decoding algorithm works as follows. Since the number of errors is at most b, there exists a monic polynomial $R_1(\lambda)$ of degree b such that $R_1(i) = 0$ if $r_i \neq f(i)$. Then it holds that

$$R_1(i)f(i) = R_1(i)r_i$$

for $i = 1, \ldots, \ell$. Let $R_0(\lambda) = R_1(\lambda)f(\lambda)$. Then we have

$$R_0(i) = R_1(i)r_i \tag{9}$$

for $i = 1, \ldots, \ell$. $R_0(\lambda)$ has $b + k$ unknown coefficients and $R_1(\lambda)$ has b unknown coefficients. Hence there are $(b + k) + b = k + 2b$ unknowns in total. On the other hand, eq.(9) gives ℓ linear equation in these unknowns.

Therefore we can obtain $R_0(\lambda)$ and $R_1(\lambda)$ by solving this set of linear equations, and can find $f(\lambda) = R_0(\lambda)/R_1(\lambda)$.

5.2 Proposed Decoding Algorithm

We show an efficient decoding algorithm for the b error correcting ℓ server PIR scheme. Fix (b, ℓ) and k such that

$$\ell \geq k + 2b. \tag{10}$$

See Proposition 1 for eq.(10).

Consider the (k, ℓ) robust PIR scheme of Woodruff and Yekhanin [21]. If all servers are honest, then the user obtains

$$\mathbf{c} = (c_1, \ldots, c_\ell)$$

such that

$$c_i = (f(i), f'(i))$$

for $i = 1, \ldots, \ell$ from eq.(6) and eq.(7), where

$$\deg f(\lambda) = 2k - 1. \tag{11}$$

See Sec.3.1.

Suppose that b or less servers return false answers. Then the user obtains

$$\mathbf{c}' = (c'_1, \ldots, c'_\ell)$$

which includes b or less errors. Let

$$c'_i = (\hat{y}_i, \hat{u}_i)$$

for $i = 1, \ldots, \ell$. Note that

$$(\hat{y}_i, \hat{u}_i) = (f(i), f'(i))$$

if c'_i has no error.

Now consider two polynomials $R_0(\lambda)$ and $R_1(\lambda)$ over $\mathbb{F}_p$ with the following properties:

(P1) $\deg R_0(\lambda) \leq 2k - 1 + 2b$.
(P2) $R_1(\lambda)$ is a monic polynomial with $\deg R_1(\lambda) = 2b$.
(P3) $R_0(i) - \hat{y}_i R_1(i) = 0$ for $i = 1, \ldots, \ell$.
(P4) $R'_0(i) - \hat{u}_i R_1(i) - \hat{y}_i R'_1(i) = 0$ for $i = 1, \ldots, \ell$.

Theorem 1. *There exist such polynomials $R_0(\lambda)$ and $R_1(\lambda)$.*

Proof. Define

$$\mathbf{BAD} = \{i \mid (\hat{y}_i, \hat{u}_i) \neq (f(i), f'(i))\}.$$

Then $c = |\mathbf{BAD}| \leq b$. Let

$$B(z) = z^{b-c} \prod_{i \in \mathbf{BAD}} (z - i).$$

Let

$$\begin{aligned} R_1(\lambda) &= B(\lambda)^2, \\ R_0(\lambda) &= f(\lambda) R_1(\lambda) = f(\lambda) B(\lambda)^2. \end{aligned}$$

Then it is easy to see that (P1) and (P2) are satisfied. Further

$$\begin{aligned}
R_0(i) - \hat{y}_i R_1(i) &= f(i)B(i)^2 - \hat{y}_i B(i)^2 \\
&= (f(i) - \hat{y}_i)B(i)^2 \\
&= 0
\end{aligned}$$

because $B(i) = 0$ if $f(i) \neq \hat{y}_i$. Also

$$\begin{aligned}
&R_0'(i) - \hat{u}_i R_1(i) - \hat{y}_i R_1'(i) \\
&= f'(i)R_1(i) + f(i)R_1'(i) - \hat{u}_i R_1(i) - \hat{y}_i R_1'(i) \\
&= (f'(i) - \hat{u}_i)R_1(i) + (f(i) - \hat{y}_i)R_1'(i) \\
&= (f'(i) - \hat{u}_i)B(i)^2 + 2(f(i) - \hat{y}_i)B(i)B'(i) \\
&= 0
\end{aligned}$$

because $B(i) = 0$ if $(f(i), f'(i)) \neq (\hat{y}_i, \hat{u}_i)$. Therefore (P3) and (P4) are satisfied. □

Theorem 2. *We can find $R_0(\lambda)$ and $R_1(\lambda)$ which satisfy (P1) $\sim$ (P4) in time $O(\ell^3)$.*

Proof. From (P1) and (P2), the number of unknown coefficients of $R_0(\lambda)$ and $R_1(\lambda)$ are given by

$$2k + 2b + 2b = 2(k + 2b).$$

On the other hand, (P3) and (P4) give

$$2\ell \geq 2(k + 2b)$$

linear equations involving them. (See eq.(10).) Further there exists a solution for this set of linear equations from Theorem 1. Hence we can find a solution in time $O(\ell^3)$.

Consequently we can find $R_0(\lambda)$ and $R_1(\lambda)$ which satisfy (P1) $\sim$ (P4) in time $O(\ell^3)$.

□

Theorem 3. *It holds that*

$$f(\lambda) = R_0(\lambda)/R_1(\lambda)$$

for any $R_0(\lambda)$ and $R_1(\lambda)$ which satisfy (P1) $\sim$ (P4),

Proof. Let
$$Q(\lambda) = R_0(\lambda) - f(\lambda)R_1(\lambda).$$
Then
$$Q'(\lambda) = R_0'(\lambda) - f'(\lambda)R_1(\lambda) - f(\lambda)R_1'(\lambda).$$
Since there are at most b errors, there exist
$$\ell - b \geq k + 2b - b = k + b (= s)$$
points such that $\hat{y}_i = f(i)$ and $\hat{u}_i = f'(i)$. For these $k+b$ points, we have
$$\begin{aligned} Q(i) &= R_0(i) - f(i)R_1(i) \\ &= R_0(i) - \hat{y}_i R_1(i) \\ &= 0 \end{aligned}$$
and
$$\begin{aligned} Q'(i) &= R_0'(i) - f'(i)R_1(i) - f(i)R_1'(i) \\ &= R_0'(i) - \hat{u}_i R_1(i) - \hat{y}_i R_1'(i) \\ &= 0 \end{aligned}$$
from (P3) and (P4). On the other hand,
$$\begin{aligned} \deg Q(\lambda) &\leq \max(\deg R_0(\lambda), \deg f(\lambda) + \deg R_1(\lambda)) \\ &= 2(k+b) - 1 (= 2s - 1) \end{aligned}$$
This means that $Q(\lambda) = 0$ from Lemma 1. Therefore we have $f(\lambda) = R_0(\lambda)/R_1(\lambda)$.

□

Our decoding algorithm of the user is given as follows.

1. The user obtains $(\hat{y}_i, \hat{u}_i)$ from the answer of a server S_i for $i = 1, \ldots, \ell$.
2. He computes two polynomials $R_0(\lambda)$ and $R_1(\lambda)$ which satisfy (P1) $\sim$ (P4) in time $O(\ell^3)$. See Theorem 2.
3. He computes $f(\lambda) = R_0(\lambda)/R_1(\lambda)$. See Theorem 3.
4. Finally he computes $x_{i_0} = f(0)$.

It runs in time $O(\ell^3)$.

6 Extension to t-Private PIR Scheme

A ℓ server PIR scheme is said to be t-private if any coalition of t servers learn no information on i_0. Woodruff and Yekhanin [21] showed a t-private (k, k) robust PIR scheme with the total communication cost $O(n^{\lfloor (2k-1)/t \rfloor} \times k\ell/t \;\log \ell)$ such as follows.

Let $d = \lfloor (2k-1)/t \rfloor$. For a given n, consider m such that

$$\binom{m}{d} \geq n. \tag{12}$$

There exists such m which also satisfies [21]

$$m = O(dn^{1/d}). \tag{13}$$

1. The user chooses $\mathbf{V}_1, \ldots, \mathbf{V}_t \in \mathbb{F}_p^m$ randomly.
2. For $i = 1, \ldots, k$, the user sends

$$Q_i = E(i_0) + i \cdot \mathbf{V}_1 + \ldots + i^t \cdot \mathbf{V}_t$$

   to the server S_i.

The rest is the same as in Sec.3.1. A t-private (k, ℓ) robust PIR scheme is obtained similarly.

Beimel and Stahl [5] showed that a t-private (k, ℓ) robust PIR scheme can be used as a t-private b error correcting ℓ server PIR scheme if $\ell \geq k + 2b$. Now it is easy to see that our decoding algorithm can also be applied to this scheme.

References

1. Andris Ambainis. 1997. Upper bound on communication complexity of private information retrieval. In ICALP ’ 97. 401?407.
2. Karim A. Banawan, Sennur Ulukus: Private information retrieval from Byzantine and colluding databases. Allerton 2017: 1091-1098
3. Amos Beimel and Yuval Ishai. 2001. Information-theoretic private information retrieval: A unified construction. In ICALP ’ 97. 912?926.
4. Amos Beimel, Yuval Ishai, Eyal Kushilevitz, and Jean-Franc?ois Raymond. 2002. Breaking the O(n1/(2k- 1)) barrier for information-theoretic private information retrieval. In FOCS ’ 02. 261?270.
5. Amos Beimel, Yoav Stahl: Robust Information-Theoretic Private Information Retrieval. J. Cryptology 20(3): 295-321 (2007)
6. `https://en.wikipedia.org/wiki/Berlekamp%E2%80%93Welch_algorithm`
7. Yeow Meng Chee, Tao Feng, San Ling, Huaxiong Wang, and Liang Feng Zhang. 2013. Query-efficient locally decodable codes of subexponential length. Computational Complexity 22, 1, 159?189.

8. B. Chor and N. Gilboa, Comput. Private Information Retrieval, STOC 1997.
9. Benny Chor, Eyal Kushilevitz, Oded Goldreich, Madhu Sudan: Private Information Retrieval. J. ACM 45(6): 965-981 (1998)
10. C. Cachin, S. Micali, M. Stadler, Computational Private Information Retrieval with Polylogarithmic Communication, Eurocrypt 1999.
11. Zeev Dvir, Sivakanth Gopi: 2-Server PIR with Subpolynomial Communication. J. ACM 63(4): 39:1-39:15 (2016)
12. Casey Devet, Ian Goldberg, Nadia Heninger: Optimally Robust Private Information Retrieval. USENIX Security Symposium 2012: 269-283
13. Klim Efremenko. 2012. 3-query locally decodable codes of subexponential length. SIAM Journal on Computing 41, 6, 1694?1703.
14. Ian Goldberg: Improving the Robustness of Private Information Retrieval. IEEE Symposium on Security and Privacy 2007: 131-148
15. Craig Gentry, Zulfikar Ramzan: Single-Database Private Information Retrieval with Constant Communication Rate. ICALP 2005: 803-815
16. Toshiya Itoh and Yasuhiro Suzuki. 2010. Improved constructions for query-efficient locally decodable codes of subexponential length. IEICE Transactions 93-D, 2, 263?270.
17. E. Kushilevits and R. Ostrovsky, Replication is not needed: single database, computationally private information Retrieval. FOCS 1997.
18. Helger Lipmaa: An Oblivious Transfer Protocol with Log-Squared Communication. ISC 2005: 314-328
19. Hua Sun, Syed Ali Jafar: The Capacity of Private Information Retrieval. IEEE Trans. Information Theory 63(7): 4075-4088 (2017)
20. Hua Sun, Syed Ali Jafar: The Capacity of Robust Private Information Retrieval With Colluding Databases. IEEE Trans. Information Theory 64(4): 2361-2370 (2018)
21. David Woodruff, Sergey Yekhanin: A Geometric Approach to Information-Theoretic Private Information Retrieval. SIAM J. Comput. 37(4): 1046-1056 (2007)
22. Sergey Yekhanin. 2008. Towards 3-query locally decodable codes of subexponential length. Journal of the ACM 55, 1.