# The Limits of $t$-Private Share Conversion

Bar Alon*
alonbar08@gmail.com

September 13, 2026

**Abstract**

Private information retrieval (PIR) protocols allow a user to retrieve an entry from a database held by several servers without revealing any information about the index to any individual server. State-of-the-art information-theoretic PIR protocols are based on a combination of matching vectors over the ring $\mathbb{Z}_m$ and decoding polynomials (Efremenko, SICOMP 2012; Dvir and Gopi, STOC 2015; Ghasemi, Kopparty, and Sudan, STOC 2025). Decoding polynomials are sparse polynomials over a field $\mathbb{F}_q$, where $q$ is a prime power coprime to $m$, that evaluate to a nonzero value at 1 and to 0 on a certain set of inputs determined by $m$.

The properties of decoding polynomials were abstracted by Beimel, Ishai, Kushilevitz, and Orlov (CCC 2012) through the notion of share conversions. Share conversions allow a set of parties to locally convert a secret shared under one scheme into a related secret shared under another scheme. They constructed a share conversion from $\mathbb{Z}_m$ to $\mathbb{F}_q$ for various values of $m$ and prime-powers $q$. More recent PIR protocols by Dvir and Gopi and by Ghasemi et al. were abstracted by Alon, Beimel, and Lasri (TCC 2025). The share conversion they considered transforms shares from the ring $\mathbb{Z}_m$ to a finite field $\mathbb{F}_q$, where $q$ is a prime-power coprime to $m$.

We observe that if the initial conversion is based on a $t$-private secret-sharing scheme, then the resulting PIR protocol of Alon et al. is also $t$-private: no set of $t$ servers learns any information about the user's index. We call such share conversions $t$-private share conversions. Moreover, the resulting PIR protocol could potentially achieve communication complexity better than that of the best-known $t$-private PIR protocols, due to Woodruff and Yekhanin (CCC 2005) and Barkol, Ishai, and Weinreb (APPROX-RANDOM 2007). This raises the natural question of whether $t$-private share conversions exist.

We show that there is no $t$-private share conversion from $\mathbb{Z}_m$ to $\mathbb{F}_q$ when $t \geq 2$ and $q$ is coprime to $m$. As a result, the PIR framework of Alon et al. cannot be instantiated in a way that yields a $t$-private PIR protocol. We further generalize the result to conversions whose output is in the ring $\mathbb{Z}_{m'}$.

## 1 Introduction

Private information retrieval (PIR) protocols allow a user holding an index $i \in [N]$ to obtain the $i^{\text{th}}$ entry of a database $D \in \{0,1\}^N$ held by 2 or more servers, using a single round, and without revealing any information about $i$ to any single server. A trivial solution is for one server to send the entire database $D$ to the user, incurring communication complexity $N$; however, protocols with

*School of Electrical Engineering, Tel-Aviv University, Tel-Aviv, Israel. Research supported by Israel Science Foundation (ISF) grant no. 2805/21 and by the European Union (ERC-2022-ADG) under grant agreement no.101097959 NFITSC.

better communication complexity are known if the database is held by at least 2 servers. PIR protocols were introduced by Chor, Goldreich, Kushilevitz, and Sudan [12]. They found many applications including the construction of secure multiparty protocols [20, 9], locally decodable codes [23], and they inspired constructions of conditional disclosure of secrets [25, 26].

PIR protocols have been studied in a long line of work [2, 21, 5, 7, 29, 4, 24, 30, 22, 15, 11, 14, 18, 1, 19]. This line of work culminated in the seminal work of Dvir and Gopi [14], who constructed a 2-server PIR protocol with communication complexity $2^{\tilde{O}(\sqrt{\log N})}$. More recently, Ghasemi et al. [18] constructed a 3-server PIR protocol with communication complexity $2^{\tilde{O}(\sqrt[3]{\log N})}$. Very recently, Gupte and Ragavan [19] showed that under a number-theoretic assumption, there is $k$-server PIR protocol with communication complexity $2^{\tilde{O}(\sqrt[k]{\log N})}$. This bound was proved to be optimal in the Efremenko [15] paradigm of "matching vectors + decoding polynomials" [17, 6].

Beimel, Ishai, Kushilevitz, and Orlov [8] generalized the notion of decoding polynomials to share conversions. Informally, share conversions allow parties to locally convert shares of a secret from one sharing scheme to shares of a related secret under another sharing scheme. They observed that decoding polynomials imply share conversions, and showed that a $k$-party share conversion implies a $k$-server PIR protocol. They further constructed share conversion from $\mathbb{Z}_m$ to $\mathbb{F}_q$ for certain values of $m$ and prime-powers $q$.

A recent work by Alon et al. [1] showed that the PIR protocols of [14, 18, 19] can also be abstracted using share conversions.[1] We observe that the privacy of the resulting PIR protocol directly relates to the privacy of the starting secret-sharing scheme. Specifically, if the share conversion starts from a $t$-private sharing scheme, then the resulting PIR protocol of [1] would be $t$-private, i.e., no set of $t$ servers learns any information on the user's index $i$. Moreover, if the share conversion is "sufficiently good", then the resulting PIR protocol would have communication complexity that is comparable to the 1-private setting, and potentially improving on the best known $t$-private PIR protocols [29, 4].

In more detail, the $k$-server $t$-private protocol of Woodruff and Yekhanin [29] has communication complexity

$$\frac{k^2}{t} \cdot \log k \cdot N^{1/\lfloor (2k-1)/t \rfloor}.$$

The compiler of Barkol et al. [4] transforms a $k$-server 1-private PIR protocol with complexity $c$ into a $k^t$-server $t$-private PIR protocol with complexity $\max(tc, c^t)$.[2] For example, applying this compiler to the recent protocol of Gupte and Ragavan [19] results in a $k^t$-server $t$-private protocol with communication complexity

$$2^{\tilde{O}(t \cdot \sqrt[k]{\log N})}.$$

When $t$ is small relative to $k$, this gives a better protocol than [29].

In this paper, we ask whether the PIR protocol of Alon et al. [1] can be instantiated with a share conversion from a $t$-private secret-sharing scheme. More precisely, we ask:

*Is there a share conversion from a $t$-private secret-sharing scheme that can be used to instantiate the PIR protocol of Alon et al. [1]?*

[1] The share conversion required in [1] satisfies a different set of constraints than that of [8]; however, they showed they are equivalent.

[2] If the 1-private PIR protocol has query length $c_q$ and answer length $c_a$, then the compiled $t$-private protocol has query length $O(tc_q)$ and answer length $O(c_a^t)$.

To the best of our knowledge, all PIR-motivated share conversions considered in the prior literature start from 1-private secret-sharing schemes. We therefore focus on $t \geq 2$.

### 1.1 Our Results

We answer the above question negatively, showing that there are no share conversions of the type required by Alon et al. [1]. Specifically, for every $t \geq 2$ and every number of servers $k \in \mathbb{N}$, no $t$-private secret-sharing scheme admits a share conversion satisfying the requirements of Alon et al. [1]. We first describe these requirements.

**Definition 1.1** ($S$-share conversion, informal)**.** *Let $m \in \mathbb{N}$ and let $q$ be prime-power $q$ coprime to $m$. For a set $S \subseteq \mathbb{Z}_m \setminus \{1\}$, an $S$-share conversion is a collection of $k$ functions $C_1, \ldots, C_k$, where $C_i$ is applied to the share of the $i^{th}$ party, such that the following hold.*

- *The share conversion maps shares of a linear secret-sharing scheme[3] over $\mathbb{Z}_m$ to shares over a finite field $\mathbb{F}_q$.*
- *Shares of the secret $1 \in \mathbb{Z}_m$ are converted into additive shares of some nonzero value in $\mathbb{F}_q$.*
- *Shares of any secret in $S$ are converted into additive shares of 0.*

The PIR protocol of [1] uses $S_{\mathrm{can},m}$-share conversions, where $m = p_1 \cdot p_2 \cdots p_r$ is the product of $r$ distinct primes and

$$S_{\mathrm{can},m} = \{s \in \mathbb{Z}_m \setminus \{1\} : s \bmod p_i \in \{0,1\} \text{ for all } i \in [r]\}.$$

**Impossibility of $t$-private share conversion to fields.** Our main result is the impossibility of $t$-private $S$-share conversion for any nonempty $S \subseteq \mathbb{Z}_m \setminus \{1\}$ and every $t \geq 2$. Stated differently, if one secret in $\mathbb{Z}_m$ is required to be converted to additive shares of 0 in $\mathbb{F}_q$, then such a conversion is impossible. Note that this holds for $S_{\mathrm{can},m}$ in particular.

**Theorem 1.2** (Informal)**.** *Let $k, m \in \mathbb{N}$, let $t \geq 2$, and let $q$ be a prime-power coprime to $m$. Then for every nonempty $S \subseteq \mathbb{Z}_m \setminus \{1\}$, there is no $t$-private $S$-share conversion from $\mathbb{Z}_m$ to $\mathbb{F}_q$.*

As a corollary, the PIR protocol of [1] cannot yield a $t$-private PIR protocol, whenever $t \geq 2$.

**Corollary 1.3.** *For all $t \geq 2$ and $k \in \mathbb{N}$, there is no instantiation of the $k$-server PIR protocol of [1] that is $t$-private.*

It is important to note that Corollary 1.3 *does not* rule out the existence of $t$-private PIR protocols with communication complexity comparable to the 1-private setting. Our impossibility only applies to the share conversion relation underlying the framework of Alon et al. [1]; it does not rule out other approaches to constructing more efficient $t$-private PIR protocols.

[3] A secret-sharing scheme is called linear if it can be described as a linear mapping of the secret and the coordinates of the random string.

**Impossibility of $t$-private share conversion to rings.** We further study $S_{\mathrm{can},m}$-share conversion in the more general setting considered by Beimel et al. [8]. The setting generalizes the previous setting in two ways. First, the output of the conversion is in a ring $\mathbb{Z}_{m'}$, where $m'$ is not necessarily a prime-power. Note that since the requirements from the conversion only involves addition, share conversion to $\mathbb{Z}_{m'}$ is well-defined. Second, we allow $m'$ to have common prime factors with $m$. We prove that if $m$ has a prime factor that $m'$ does not have, then there is no $t$-private $S_{\mathrm{can},m}$-share conversion from $\mathbb{Z}_m$ to $\mathbb{Z}_{m'}$.

**Theorem 1.4** (Informal)**.** *Let $k \in \mathbb{N}$, let $t \geq 2$, and let $m, m' \in \mathbb{N}$ be such that there exists a prime $p$ such that $p \mid m$ and $p \nmid m'$. Then there is no $t$-private $S_{\mathrm{can},m}$-share conversion from $\mathbb{Z}_m$ to $\mathbb{Z}_{m'}$.*

We leave open the case where there is no such prime $p$. Note that in particular, there is no $t$-private $S_{\mathrm{can},m}$-share conversion from $\mathbb{Z}_{p_1 p_2}$ to $\mathbb{Z}_{p_1}$. This is in contrast to the 1-private setting, where such share conversion do exists in the 3-party setting for certain primes [8, 28, 27].

**Characterization of $t$-private share conversion in a field.** Using Theorem 1.4, we can completely characterize when a $t$-private $S_{\mathrm{can},m}$-share conversion to a field $\mathbb{F}_{p^\ell}$ exists.

**Corollary 1.5.** *Let $k, m, \ell \in \mathbb{N}$, let $t \geq 2$, and let $p$ be a prime. Then there exists a $t$-private $S_{\mathrm{can},m}$-share conversion from $\mathbb{Z}_m$ to $\mathbb{F}_{p^\ell}$ if and only if $m = p^e$ for some $e \geq 1$.*

We prove that the positive direction follows from the trivial conversion: the starting sharing scheme is the additive $k$-out-of-$k$ secret-sharing scheme, and each $C_i(r_i)$ outputs $r_i \bmod p$. See Theorem 3.7 for the formal statement and proof.

## 1.2 Our Techniques

We next provide an overview of our proofs. In Section 1.2.1 we prove Theorem 1.2, showing there is no $t$-private share conversion from $\mathbb{Z}_m$ to $\mathbb{F}_q$, whenever $q$ is coprime to $m$. Then, in Section 1.2.2, we consider the setting where the conversion is in a ring $\mathbb{Z}_{m'}$. For the entirety of the section, we assume the following without loss of generality.

- The linear scheme from which the conversion starts is a $t$-private CNF scheme. This is because $t$-private CNF secret sharing can be locally converted to any other $t$-private linear secret-sharing scheme [13, 8].
- Since $t$-private CNF can be locally converted to 2-private CNF, it suffices to consider the case $t = 2$.

### 1.2.1 Impossibility of Conversions to a Field

Fix $k, m \in \mathbb{N}$, $t \geq 2$ and a prime-power $q$ coprime to $m$. We assume that $m \mid q - 1$. This is without loss of generality, since otherwise, by Euler's theorem, we can embed $\mathbb{F}_q$ into an extension field $\mathbb{F}_{q^\ell}$ such that $m \mid q^\ell - 1$. We then analyze share conversions whose output is in the copy of $\mathbb{F}_q$ inside $\mathbb{F}_{q^\ell}$.

Let us first recall the definition of 2-private CNF secret sharing. A secret $s \in \mathbb{Z}_m$ is shared among $k$ parties as follows:

1. For every $i \neq j \in [k]$ such that $\{i, j\} \neq \{1, 2\}$, sample $r_{\{i,j\}} \leftarrow \mathbb{Z}_m$.

2. Set
$$r_{\{1,2\}} = s - \sum_{\substack{i \neq j \in [k]: \\ \{i,j\} \neq \{1,2\}}} r_{\{i,j\}}.$$

3. The share of party $i$ consists of all $r_{\{j,j'\}}$ such that $j, j' \neq i$.

We denote the CNF randomness by $\mathbf{r} = (r_{\{i,j\}})_{i \neq j \in [k]}$, and the $i^{\text{th}}$ share by $\mathbf{r}_{-i}$.

Now, fix a nonempty $S \subseteq \mathbb{Z}_m \setminus \{1\}$ and assume toward a contradiction that there is an $S$-share conversion. Then there are functions $(C_i)_{i \in [k]}$, where $C_i : \mathbb{Z}_m^{\binom{k-1}{2}} \to \mathbb{F}_q$ for every $i \in [k]$, satisfying the following properties:

- For every $\mathbf{r} \in \mathbb{Z}_m^{\binom{k}{2}}$ whose entries sum to a value in $S$, $\sum_{i=1}^k C_i(\mathbf{r}_{-i}) = 0$.
- For every $\mathbf{r} \in \mathbb{Z}_m^{\binom{k}{2}}$ whose entries sum to 1 in $\mathbb{Z}_m$, $\sum_{i=1}^k C_i(\mathbf{r}_{-i}) \neq 0$.

For each secret $s \in \mathbb{Z}_m$ consider the following matrix $\mathbf{C}_s$: Its rows are indexed by CNF randomness $\mathbf{r} \in \mathbb{Z}_m^{\binom{k}{2}}$, its columns are indexed by the servers $i \in [k]$, and its corresponding entries are
$$\mathbf{C}_s(\mathbf{r}, i) = \begin{cases} C_i(\mathbf{r}_{-i}) & \text{if } \sum_{i \neq j \in [k]} r_{\{i,j\}} = s \\ 0 & \text{otherwise.} \end{cases}$$
In other words, if $\mathbf{r}$ is a possible CNF randomness for sharing $s$, then $\mathbf{C}_s(\mathbf{r}, i)$ is the converted share output by the $i^{\text{th}}$ party; otherwise, the entry is 0. Now, fix a secret $s \in S$. Then
$$\mathbf{C}_s \cdot \mathbf{1} = \mathbf{0},$$
where $\mathbf{1}$ and $\mathbf{0}$ are the all-one and all-zero vectors, respectively. On the other hand, every entry in $\mathbf{C}_1 \cdot \mathbf{1}$ is nonzero. To obtain a contradiction, we show that there exists a matrix $\mathbf{M}$ such that[4]
$$\mathbf{M} \cdot \mathbf{C}_s = \mathbf{C}_1. \tag{1}$$

At a high level, we construct $\mathbf{M}$ by moving to the Fourier basis, where $\mathbf{M}$ becomes an appropriate diagonal matrix. We next provide details. Since $m \mid q - 1$, there is an $m^{\text{th}}$ primitive root of unity $\omega \in \mathbb{F}_q$. Consider the (unnormalized) Fourier transform matrix $\mathcal{F}$ defined by $\mathcal{F}(\mathbf{a}, \mathbf{r}) = \omega^{\langle \mathbf{a}, \mathbf{r} \rangle}$ for all $\mathbf{a}, \mathbf{r} \in \mathbb{Z}_m^{\binom{k}{2}}$. We show that for every $\tilde{s} \in \mathbb{Z}_m$, each row $\mathbf{a}$ of $\mathcal{F} \cdot \mathbf{C}_{\tilde{s}}$ can be written as a scalar $\omega^{b \cdot \tilde{s}}$ multiplied by a row vector $\mathbf{v}_{\mathbf{a}}$, where $b$ depends only on $\mathbf{a}$, while $\mathbf{v}_{\mathbf{a}}$ is independent of $\tilde{s}$. We refer to Lemma 3.2 for the proof of this statement. Thus, multiplying $\mathcal{F} \cdot \mathbf{C}_s$ on the left by a diagonal matrix $\mathbf{D}$ whose diagonal entries are of the form $\omega^{b(1-s)}$, yields $\mathcal{F} \cdot \mathbf{C}_1$. Since $\mathcal{F}$ is invertible, we can take $\mathbf{M} = \mathcal{F}^{-1} \cdot \mathbf{D} \cdot \mathcal{F}$. This proves Equation (1), contradicting $\mathbf{C}_s \cdot \mathbf{1} = \mathbf{0}$ and the fact that every entry of $\mathbf{C}_1 \cdot \mathbf{1}$ is nonzero.

[4] In fact, the proof shows that if all sharings of some secret $s \in \mathbb{Z}_m$ are converted to additive sharing of 0 in $\mathbb{F}_q$, then *all* sharings (in particular, shares of 1) are converted to additive sharing of 0.

### 1.2.2 Impossibility of Conversions to a Ring

We next prove the impossibility of $t$-private $S_{\text{can},m}$-share conversions that map to the ring $\mathbb{Z}_{m'}$, assuming there exists a prime $p$ that divides $m$ but not $m'$.

Assume that such a conversion $(C_i)_{i\in[k]}$ exists. First note that if $m$ and $m'$ do not share any common prime factor, then for every prime-power $q \mid m'$, by projecting the output of every $C_i$ to $\mathbb{Z}_q$, we can apply the argument from the finite field case (specifically Equation (1)) to conclude that the conversion maps all sharings to additive shares of 0 in $\mathbb{Z}_q$. Since this is true for every $q$ that divides $m'$, this is true in $\mathbb{Z}_{m'}$ and we reach a contradiction.

Assume now that $m$ and $m'$ do share a common prime factor $\tilde{p}$, and let $e$ and $e'$ be the maximal exponents such that $\tilde{p}^e \mid m$ and $\tilde{p}^{e'} \mid m'$. Let $q = \tilde{p}^e$ and $q' = \tilde{p}^{e'}$. Our idea is to construct a new share conversion where the powers of $\tilde{p}$ are removed. That is, we construct a share conversion from $\mathbb{Z}_{m/q}$ to $\mathbb{Z}_{m'/q'}$. This can generalized to allow us to remove all common prime factors.

There is one subtlety in the case where every prime factor of $m'$ is also a prime factor of $m$. In this case, before applying the inductive argument, we first choose a prime $p' \nmid m, m'$ and embed the output of the share conversion in $\mathbb{Z}_{m'p'} \cong \mathbb{Z}_{m'} \times \mathbb{Z}_{p'}$ so that the second coordinate of the output of every $C_i$ is 0. That is, we define $C'_i(\mathbf{r}_{-i})$ to output the unique value (given by the CRT) such that

$$C'_i(\mathbf{r}_{-i}) \equiv C_i(\mathbf{r}_{-i}) \pmod{m'} \quad \text{and} \quad C'_i(\mathbf{r}_{-i}) \equiv 0 \pmod{p'}.$$

Then $(C'_i)_{i\in[k]}$ is an $S_{\text{can},m}$-share conversion from $\mathbb{Z}_m$ to $\mathbb{Z}_{m'p'}$. The inductive argument can now be applied to $m$ and $m'p'$.

To finish the proof, we construct the $S_{\text{can},m/q}$-share conversion from $\mathbb{Z}_{m/q}$ to $\mathbb{Z}_{m'/q'}$. We do it in two steps. In the first step, we construct a share conversion from $\mathbb{Z}_{m/q}$ to $\mathbb{Z}_{m'}$. The idea is to have all the parties think of the secret $s' \in \mathbb{Z}_{m/q}$ as the unique value (from the CRT) $s \in \mathbb{Z}_m$ that satisfies

$$s \equiv s' \pmod{m/q} \quad \text{and} \quad s \equiv 1 \pmod{q}.$$

This can be done by viewing the CNF randomness $r_{\{1,2\}}$ as $1 \pmod q$, and viewing every other $r_{\mathcal{T}}$ as $0 \pmod q$. Note that if $s' \in S_{\text{can},m/q}$ then $s \in S_{\text{can},m}$, and if $s' = 1$ in $\mathbb{Z}_{m/q}$ then $s = 1$ in $\mathbb{Z}_m$. Let $(C''_i)_{i\in[k]}$ denote the resulting share conversion from $\mathbb{Z}_{m/q}$ to $\mathbb{Z}_{m'}$.

In the second step, we use Equation (1) to show there is a share conversion from $\mathbb{Z}_{m/q}$ to $\mathbb{Z}_{m'/q'}$. Since $\gcd(q', m'/q') = 1$, by the Chinese remainder theorem, we may write $\mathbb{Z}_{m'}$ as $\mathbb{Z}_{m'/q'} \times \mathbb{Z}_{q'}$. Since $q' \nmid m/q$, by Equation (1), the second coordinate of

$$\sum_{i=1}^{k} C''_i(\mathbf{r}_{-i})$$

is 0 for all $\mathbf{r} \in \mathbb{Z}_{m/q}^{\binom{k}{2}}$. Thus, projecting each $C''_i$ to its first coordinate results in a share conversion from $\mathbb{Z}_{m/q}$ to $\mathbb{Z}_{m'/q'}$.

## 1.3 Related Works

**1-private PIR.** PIR protocols were introduced by Chor et al. [12]. They showed that there is no single-server PIR protocol with communication complexity $o(N)$. They further constructed a $k$-server PIR protocol with communication complexity $N^{1/k}$. The best known PIR protocols follow

the Efremenko [15] paradigm. He constructed a 3-server 1-private PIR protocol with query length $2^{\tilde{O}(\sqrt{\log N})}$ and $2^r$-server 1-private PIR protocols with query length $2^{\tilde{O}(\sqrt[r]{\log N})}$; the answer length in these protocols is $O(1)$. Dvir and Gopi [14] broke the $N^{1/3}$ barrier in the 2-server setting. They constructed a 2-server PIR protocol with complexity $2^{\tilde{O}(\sqrt{\log N})}$. Recently, Ghasemi, Kopparty, and Sudan [18] constructed a 3-server PIR protocol with complexity $2^{\tilde{O}(\sqrt[3]{\log N})}$. Very recently, Gupte and Ragavan [19] showed that under a number-theoretic assumption, there is $k$-server PIR protocol with communication complexity $2^{\tilde{O}(\sqrt[k]{\log N})}$. They further empirically verified the construction for all $k \leq 15$.

**$t$-private PIR.** $t$-private PIR protocols were constructed in [12, 2, 20, 5, 7, 29]. In particular, Woodruff and Yekhanin [29] presented a $t$-private $k$-server PIR with communication complexity $\frac{k^2}{t} \cdot \log k \cdot N^{1/\lfloor (2k-1)/t \rfloor}$. Barkol, Ishai, and Weinreb [4] presented a general transformation from 1-private PIR protocols to $t$-private PIR protocol. Specifically, given a 1-private $k$-server PIR protocol with query length $c_q$ and answer length $c_a$, they constructed a $t$-private $k^t$-server PIR protocol with query length $O(tc_q)$ and answer length $O(c_a^t)$.

**Share conversion.** Share conversions were introduced by Cramer et al. [13]. They considered the setting of converting sharing of a secret in one scheme to sharing of the *same* secret under another scheme. They showed that CNF secret sharing can be converted to any other linear secret-sharing scheme. Recently, Ben-David et al. [10] initiated a systematic study of such share conversion and established several impossibility results, including results for share conversions from one field to another. Note that their conversion relation preserves the secret and the access structure, whereas the PIR-induced conversion studied in this paper maps a prescribed set of secrets to additive shares satisfying a specified relation. Our result therefore addresses a different conversion problem and is incomparable to that of [10].

Beimel et al. [8] were the first to consider the general notion of share conversions, where the conversion maps to a possibly different (but related) secret. They defined the requirements from share conversion that are applicable to PIR protocols and showed that decoding polynomials are a special case of such share conversions. They further constructed 3-party share conversions from $\mathbb{Z}_m$ to $\mathbb{F}_q$ for various values of $m$ and prime-powers $q$. Paskin-Cherniavsky and Schmerler [28] generalized the results of [8], showing there is a 3-party share conversion from $\mathbb{Z}_{p_1 p_2}$ to $\mathbb{F}_{p_1}$, where $p_1$ and $p_2$ are distinct odd primes. Paskin-Cherniavsky and Nissenbaum [27] showed a conversion when $p_1 = 2$, and proved there is no share conversion if $p_2 = 2$.

Share conversions where $q$ is coprime to $m$ was studied in relation to sparse decoding polynomials [15, 22, 11, 3, 17, 6, 19]. A $k$-sparse decoding polynomial has $k$ nonzero coefficients, and it implies $k$-party share conversion [8]. Efremenko [15] found the first non-trivial 3-sparse decoding polynomial using a computer search. Itoh and Suzuki [22], Chee et al. [11], Gupte and Ragavan [19] gave analytic results on the existence of non-trivial decoding polynomials, with [19] constructing decoding polynomials with optimal sparsity under a number-theoretic assumption. Note that the share conversion implied by decoding polynomials is 1-private.

Ghasemi and Kopparty [17] studied decoding polynomials, by considering the Fourier coefficients of certain functions over the Boolean hypercube embedded in $\mathbb{Z}_m$. They showed that if $m = p_1 \cdot p_2 \cdots p_r$ is the product of $r$ primes, then for a $k$-sparse decoding polynomial to exists it must be the case where $r < k$. Beimel and Lasri [6] showed that when $q$ is coprime to $m$, 1-private $k$-party

share conversions are equivalent to $k$-sparse decoding polynomials. In particular, there is no share conversion with better parameters than the construction of Gupte and Ragavan [19].

# 2 Preliminaries

## 2.1 Notations

For $n \in \mathbb{N}$ we let $[n] = \{1, 2 \dots n\}$ and for $k \in [n]$ we let $\binom{[n]}{k} = \{\mathcal{T} \subseteq [n] : |\mathcal{T}| = k\}$. For a vector $\mathbf{v}$ of dimension $n$, we write $v_i$ for its $i^{\text{th}}$ component. For a randomized function (or an algorithm) $f$ we write $f(x)$ to denote the random variable induced by the function on input $x$, and write $f(x; r)$ to denote the value when the randomness of $f$ is fixed to $r$.

The following is a well-known fact.

**Fact 2.1.** *Let $m \in \mathbb{Z}$, let $q$ be a prime-power such that $m \mid q - 1$. Then $\mathbb{F}_q$ contains an $m$-th primitive root of unity $\omega$. Moreover, for every $a \in \mathbb{Z}_m$,*

$$\sum_{s \in \mathbb{Z}_m} \omega^{as} = \begin{cases} m & \text{if } a = 0 \\ 0 & \text{otherwise,} \end{cases}$$

*where the summation is in $\mathbb{F}_q$.*

## 2.2 Secret Sharing

A $(t+1)$-out-of-$k$ secret-sharing scheme defines a way to distribute shares to parties, such that any set of $t+1$ parties can reconstruct the secret, while any set of (at most) $t$ parties learn nothing about it. The formal definition is given as follows.

**Definition 2.2** (Threshold secret-sharing schemes)**.** *Let $k \in \mathbb{N}$ and let $t \in [k-1]$. A $(t+1)$-out-of-$k$ secret-sharing scheme $\Pi$ over a set of parties $\mathcal{P} = \{\mathsf{P}_1, \dots, \mathsf{P}_k\}$ with domain of secrets $\mathcal{S}$ and domain of random strings $\mathcal{R}$ is a mapping from $\mathcal{S} \times \mathcal{R}$ to a set of $k$-tuples $\mathcal{S}_1 \times \mathcal{S}_2 \times \cdots \times \mathcal{S}_k$ (the set $\mathcal{S}_j$ is called the domain of shares of $\mathsf{P}_j$). A dealer distributes a secret $s \in \mathcal{S}$ according to $\Pi$ by first sampling a random string $r \leftarrow \mathcal{R}$, computing a vector of shares $\Pi(s; r) = (\mathsf{sh}_1, \dots, \mathsf{sh}_k)$, and privately communicating each share $\mathsf{sh}_j$ to party $\mathsf{P}_j$. For a set $A \subseteq \{\mathsf{P}_1, \dots, \mathsf{P}_k\}$, we denote $\Pi_A(s; r)$ as the restriction of $\Pi(s; r)$ to its $A$-entries (i.e., the shares of the parties in $A$).*

*The scheme $\Pi$ must satisfy the following two requirements:*

**Correctness.** *The secret $s$ can be reconstructed by any set of $t+1$ parties. That is, for any set $A = \{\mathsf{P}_{i_1}, \mathsf{P}_{i_2}, \dots, \mathsf{P}_{i_{t+1}}\}$, there exists a reconstruction function $\mathsf{Rec}_A : \mathcal{S}_{i_1} \times \cdots \times \mathcal{S}_{i_{t+1}} \to \mathcal{S}$ such that $\mathsf{Rec}_A(\Pi_A(s; r)) = s$ for every secret $s \in \mathcal{S}$ and every random string $r \in \mathcal{R}$.*

**Security.** *Every set of at most $t$ parties cannot learn anything about the secret from its shares. Formally, for any set $B \in \binom{[k]}{t}$, every two secrets $s_1, s_2 \in \mathcal{S}$, and for a uniformly distributed $r \leftarrow \mathcal{R}$, the distributions $\Pi_B(s_1; r)$ and $\Pi_B(s_2; r)$ are identically distributed.*

*When $k$ is clear from context, we will sometimes refer to a $(t+1)$-out-of-$k$ scheme as $t$-private.*

**Definition 2.3** (Linear secret-sharing schemes over $\mathbb{Z}_m$ [16])**.** *Let $m \in \mathbb{N}$. A* linear secret-sharing scheme *over $\mathbb{Z}_m$ is defined a pair $(\mathbf{M}, \rho)$, where $\mathbf{M}$ is an $n \times b$ matrix over the ring $\mathbb{Z}_m$, and $\rho : [n] \to \mathcal{P}$ labels each row of $\mathbf{M}$ by a party $\mathsf{P}_i \in \mathcal{P}$. For every $i \in [k]$ we let $\mathbf{M}_i$ denote the restriction of $\mathbf{M}$ to the rows labeled by $\mathsf{P}_i$. A sharing of a secret $s \in \mathbb{Z}_m$ is done as follows:*

1. *Sample* $r_1, \ldots, r_{b-1} \leftarrow \mathbb{Z}_m$ *independently.*
2. *Set* $r_b = s - \sum_{i=1}^{b-1} r_i$ *and let* $\mathbf{r} = (r_1, \ldots, r_b)$.
3. *The share of* $\mathsf{P}_j$ *is* $\mathsf{sh}_j := \mathbf{M}_j \cdot \mathbf{r}$.

We next recall the linear secret-sharing schemes that will be used in this paper.

**Definition 2.4** (Additive secret sharing)**.** *In an* additive secret-sharing scheme *over* $\mathbb{Z}_m$*, a secret* $s \in \mathbb{Z}_m$ *is shared as follows:*

1. *For every* $i \in [k-1]$*, sample* $r_i \leftarrow \mathbb{Z}_m$.
2. *Set* $r_k = s - \sum_{i=1}^{k-1} r_i$.
3. *The share of* $\mathsf{P}_j$ *is* $\mathsf{sh}_j := r_j$.

*We denote this scheme by* $\Pi_{(k,\mathbb{Z}_m)\text{-add}}$*. When* $m$ *and* $k$ *are clear from context we write* $\Pi_{\text{add}}$ *for brevity.*

**Definition 2.5** (CNF secret sharing)**.** *In a* $(t+1)$*-out-of-*$k$ CNF scheme *over* $\mathbb{Z}_m$*, a secret* $s \in \mathbb{Z}_m$ *is shared as follows:*

1. *For every subset* $\mathcal{T} \in \binom{[k]}{t} \setminus \{[t]\}$*, sample* $r_{\mathcal{T}} \leftarrow \mathbb{Z}_m$.
2. *Set* $r_{\{1,2,\ldots,t\}} = s - \sum_{\mathcal{T} \in \binom{[k]}{t}} r_{\mathcal{T}}$.
3. *The share of* $\mathsf{P}_j$ *is* $\mathsf{sh}_j := (r_{\mathcal{T}})_{\mathcal{T} \not\ni j}$.

*We denote this scheme by* $\Pi_{(t,k,\mathbb{Z}_m)\text{-CNF}}$*. When* $m$ *and* $k$ *are clear from context we write* $\Pi_{t\text{-CNF}}$ *for brevity.*

## 2.3 Share Conversion

We next present the definition of share conversion from a $k$-party secret-sharing scheme over $\mathbb{Z}_m$ to additive sharing over $\mathbb{Z}_{m'}$. In such share conversions, the parties are given shares of a secret $s \in \mathbb{Z}_m$, and each party locally computes a function of its share to produce new shares of a related secret $s' \in \mathbb{Z}_{m'}$.[5]

**Definition 2.6** (Share conversion [8, 1])**.** *Let* $m, m', k \in \mathbb{N}$*, let* $\Pi$ *be a* $k$*-party sharing over* $\mathbb{Z}_m$*, and let* $S \subseteq \mathbb{Z}_m \setminus \{1\}$*. A* $k$-party $(\Pi, S, m, m')$-share conversion *is a collection of* $k$ *functions* $(C_i)_{i \in [k]}$*, where* $C_i : \mathbb{Z}_m^{\ell_i} \to \mathbb{Z}_{m'}$ *for every* $i \in [k]$ *and* $\ell_i \in \mathbb{N}$ *is the number of elements in the* $i^{th}$ *share, such that the following hold.*

- *If* $\mathsf{sh}_1, \ldots, \mathsf{sh}_k = \Pi(1; r)$ *for some* $r$*, then* $C_1(\mathsf{sh}_1) + \ldots + C_k(\mathsf{sh}_k) \neq 0$.

[5] Originally, the definition considered in [8, 1] viewed the output of the conversion as a value in a finite field. However, since the requirements from the conversion involves only addition, the definition readily generalizes. Beimel et al. [8] further considered a broader definition of a share conversion with respect to a relation $R \subseteq \mathbb{Z}_m \times \mathbb{Z}_{m'}$ in which $k$ parties hold shares of a secret $s$ given by a secret-sharing scheme over $\mathbb{Z}_m$ and each party locally computes a share of a secret $s' \in \mathbb{Z}_{m'}$ such that $(s, s') \in R$. We only consider the specific relation that is used for PIR protocols [1].

- *If* $\mathsf{sh}_1, \ldots, \mathsf{sh}_k = \Pi(s; r)$ *for some* $r$ *and* $s \in S$*, then* $C_1(\mathsf{sh}_1) + \ldots + C_k(\mathsf{sh}_k) = 0$.

*We say that there is a* $k$*-party* $t$*-private* $(S, m, m')$*-share conversion, if there exists a* linear $(t+1)$*-out-of-*$k$ *secret-sharing scheme* $\Pi$*, for which there is a* $k$*-party* $(\Pi, S, m, m')$*-share conversion.*

We next describe the set $S$ which is used in the best-known PIR construction.

**Definition 2.7** ($S_{\mathrm{can},m}$)**.** *Let* $m = q_1 \cdot q_2 \cdots q_r$*, where* $q_1, \ldots, q_r$ *are pairwise coprime prime-powers. Define the set*

$$S_{\mathrm{can},m} = \{s \in \mathbb{Z}_m \setminus \{1\} : s \bmod q_i \in \{0, 1\} \text{ for all } i \in [r]\}.$$

Beimel et al. [8] showed that a $t$-private CNF secret sharing over rings[6] is maximal among all $t$-private linear schemes, in the sense that it can be locally converted to any other $t$-private linear secret-sharing scheme. Moreover, a $t$-private CNF sharing can be converted to a 2-private CNF sharing. Thus, we have the following.

**Theorem 2.8** ([13, 8])**.** *If there is a* $k$*-party* $t$*-private* $(S, m, m')$*-share conversion, then there exists a* $k$*-party* $(\Pi_{(2,k,\mathbb{Z}_m)\text{-CNF}}, S, m, m')$*-share conversion.*

# 3 Impossibility of $t$-Private Share Conversion

In this section, we prove our impossibility results. In Section 3.1, we prove the impossibility of a $t$-private share conversion from $\mathbb{Z}_m$ to $\mathbb{F}_q$ whenever $q$ is coprime to $m$. This result hold even under weaker requirements than what is required for PIR protocols. Then, in Section 3.2, we focus on $S_{\mathrm{can}}$-share conversions from $\mathbb{Z}_m$ to a ring $\mathbb{Z}_{m'}$, and show that $t$-privacy is impossible for many choices of $m$ and $m'$. Finally, in Section 3.3, we characterize when a $t$-private $S_{\mathrm{can}}$-share conversion to a field exists.

## 3.1 Impossibility of $t$-Private Share Conversion in a Field

Our main result is the impossibility of a $t$-private share conversion from $\mathbb{Z}_m$ to $\mathbb{F}_q$ whenever $q$ is coprime to $m$.

**Theorem 3.1.** *Let* $m, k \in \mathbb{N}$*, let* $q$ *be prime-power coprime to* $m$*, let* $2 \le t \le k-1$*, and let* $S \subseteq \mathbb{Z}_m \setminus \{1\}$ *be a nonempty set. Then there is no* $k$*-party* $t$*-private* $(S, m, q)$*-share conversion.*

*Proof.* The theorem will follow immediately from the following lemma, which roughly states that if the functions $(C_i)_{i\in[k]}$ are share conversions from a CNF scheme that map all sharings of some fixed secret $s \in \mathbb{Z}_m$ to additive sharing of 0 (in $\mathbb{F}_q$), then they map *all* sharings to additive sharing of 0. By Theorem 2.8, it will suffice to state the lemma for $t = 2$. We use the following notations: For CNF randomness $\mathbf{r} = (r_{\mathcal{T}})_{\mathcal{T}\in\binom{[k]}{2}} \in \mathbb{Z}_m^{\binom{k}{2}}$ and an index $i \in [k]$, we let $\mathbf{r}_{-i} = (r_{\mathcal{T}})_{\mathcal{T}\not\ni i}$, and let $\mathbf{r}_i = (r_{\mathcal{T}})_{\mathcal{T}\ni i}$.

**Lemma 3.2.** *Let* $m, k \in \mathbb{N}$*, let* $q$ *be prime-power coprime to* $m$*, and let* $(C_i)_{i\in[k]}$ *be functions, where* $C_i : \mathbb{Z}_m^{\binom{k-1}{2}} \to \mathbb{Z}_q$*. Assume there exists* $s \in \mathbb{Z}_m$ *such that* $\sum_{i=1}^k C_i(\mathbf{r}_{-i}) = 0$ *for all* $\mathbf{r} = (r_{\mathcal{T}})_{\mathcal{T}\in\binom{[k]}{2}} \in \mathbb{Z}_m^{\binom{k}{2}}$ *satisfying* $\sum_{\mathcal{T}\in\binom{[k]}{2}} r_{\mathcal{T}} = s$*. Then* $\sum_{i=1}^k C_i(\mathbf{r}_{-i}) = 0$ *for all* $\mathbf{r} \in \mathbb{Z}_m^{\binom{k}{2}}$.

[6] This was originally proved by Cramer et al. [13] over fields.

*Proof.* In the following, let $\mathsf{sum} : \bigcup_{\ell\in\mathbb{N}} \mathbb{Z}_m^\ell \to \mathbb{Z}_m$ be defined as $\mathsf{sum}(r_1,\ldots,r_\ell) = \sum_{i=1}^{\ell} r_i$, and we let $K = \binom{k}{2}$, let $K' = \binom{k-1}{2}$, and let $M = m^K$. Since $q$ is a prime-power, we may view the set $\mathbb{Z}_q$ as a field $\mathbb{F}_q$. We first give a sufficient condition to prove the statement. For a secret $s \in \mathbb{Z}_m$, let $\mathbf{C}_s \in \mathbb{F}_q^{M\times k}$ be defined as $\mathbf{C}_s(\mathbf{r}, i) = C_i(\mathbf{r}_{-i})$ if $\mathsf{sum}(\mathbf{r}) = s$, and $\mathbf{C}_i(\mathbf{r}, i) = 0$ otherwise. Then it suffices to prove the following: for every $s, s' \in \mathbb{Z}_m$, there exists a matrix $\mathbf{M}_{s,s'} \in \mathbb{F}_q^{M,M}$ such that

$$\mathbf{M}_{s,s'} \cdot \mathbf{C}_s = \mathbf{C}_{s'}. \tag{2}$$

Fix $s, s' \in \mathbb{Z}_m$. Let $\mathcal{R} = \{\mathbf{r} \in \mathbb{Z}_m^K : \mathsf{sum}(\mathbf{r}) = s\}$ denote the set of randomness for CNF shares of $s$, and for every CNF share $\mathbf{r}_{-i} \in \mathbb{Z}_m^{K'}$ let $\mathcal{R}(\mathbf{r}_{-i}) = \left\{\mathbf{r}_i \in \mathbb{Z}_m^{k-1} : \mathsf{sum}(\mathbf{r}_i) + \mathsf{sum}(\mathbf{r}_{-i}) = s\right\}$ denote the set of randomness that complete $\mathbf{r}_{-i}$ to CNF shares of $s$. Finally, we assume that $m \mid q-1$. This is without loss of generality since by Euler's theorem, there exists $\ell$ such that $m \mid q^\ell - 1$, and we can view the output of each $C_i$ as in $\mathbb{F}_{q^\ell}$ instead of $\mathbb{F}_q$.

Since $m \mid q-1$, there exists an $m^{\text{th}}$ primitive root of unity $\omega \in \mathbb{F}_q$. Let $\mathcal{F} \in \mathbb{F}_q^{M\times M}$ be the (unnormalized) Fourier transform matrix, defined as $\mathcal{F}(\mathbf{a}, \mathbf{r}) = \omega^{\langle \mathbf{a},\mathbf{r}\rangle}$ for all $\mathbf{a}, \mathbf{r} \in \mathbb{Z}_m^K$. Then

$$(\mathcal{F}\cdot\mathbf{C}_s)(\mathbf{a}, i) = \sum_{\mathbf{r}\in\mathcal{R}} \omega^{\langle \mathbf{a},\mathbf{r}\rangle} \cdot C_i(\mathbf{r}_{-i}) = \sum_{\mathbf{r}_{-i}\in\mathbb{Z}_m^{K'}} C_i(\mathbf{r}_{-i}) \cdot \omega^{\langle \mathbf{a}_{-i},\mathbf{r}_{-i}\rangle} \cdot \sum_{\mathbf{r}_i\in\mathcal{R}(\mathbf{r}_{-i})} \omega^{\langle \mathbf{a}_i,\mathbf{r}_i\rangle}.$$

The following claim uses Fact 2.1 to simplify the last term in the sum.

**Claim 3.3.** *For every $i \in [k]$ and every $\mathbf{r}_{-i} \in \mathbb{Z}_m^{K'}$,*

$$\sum_{\mathbf{r}_i\in\mathcal{R}(\mathbf{r}_{-i})} \omega^{\langle \mathbf{a}_i,\mathbf{r}_i\rangle} = \begin{cases} m^{k-2}\cdot\omega^{b\cdot s}\cdot\omega^{-b\cdot\mathsf{sum}(\mathbf{r}_{-i})} & \text{if } \exists b\in\mathbb{Z}_m \text{ s.t. } \mathbf{a}_i = b\cdot\mathbf{1}_{k-1} \\ 0 & \text{otherwise.}\end{cases}$$

*Proof.* For simplicity we assume $i = 1$. The general case is handled similarly. Fix $\mathbf{r}_{-1} \in \mathbb{Z}_m^{K'}$ and compute

$$\begin{aligned}
\sum_{\mathbf{r}_1\in\mathcal{R}(\mathbf{r}_{-1})} \omega^{\langle \mathbf{a}_1,\mathbf{r}_1\rangle} &= \sum_{(r_{\{1,2\}},\ldots,r_{\{1,k\}})\in\mathcal{R}(\mathbf{r}_{-1})} \omega^{a_{\{1,2\}}\cdot r_{\{1,2\}}} \cdot \prod_{j=3}^{k} \omega^{a_{\{1,j\}}\cdot r_{\{1,j\}}} \\
&= \sum_{r_{\{1,3\}},\ldots,r_{\{1,k\}}\in\mathbb{Z}_m} \omega^{a_{\{1,2\}}\cdot(s-\mathsf{sum}(\mathbf{r}_{-i})-r_{\{1,3\}}-\ldots-r_{\{1,k\}})} \prod_{j=3}^{k} \omega^{a_{\{1,j\}}\cdot r_{\{1,j\}}} \\
&= \omega^{a_{\{1,2\}}\cdot s}\cdot\omega^{-a_{\{1,2\}}\cdot\mathsf{sum}(\mathbf{r}_{-i})} \cdot \sum_{r_{\{1,3\}},\ldots,r_{\{1,k-1\}}\in\mathbb{Z}_m} \prod_{j=3}^{k} \omega^{(a_{\{1,j\}}-a_{\{1,2\}})\cdot r_{\{1,j\}}} \\
&= \omega^{a_{\{1,2\}}\cdot s}\cdot\omega^{-a_{\{1,2\}}\cdot\mathsf{sum}(\mathbf{r}_{-i})} \cdot \prod_{j=3}^{k} \sum_{r_{\{1,j\}}\in\mathbb{Z}_m} \omega^{(a_{\{1,j\}}-a_{\{1,2\}})\cdot r_{\{1,j\}}}.
\end{aligned}$$

The claim now follows from Fact 2.1, which implies that for every $j \in \{3, 4, \ldots, k\}$,

$$\sum_{r_{\{1,j\}}\in\mathbb{Z}_m} \omega^{(a_{\{1,j\}}-a_{\{1,2\}})\cdot r_{\{1,j\}}} = \begin{cases} m & \text{if } a_{\{1,j\}} = a_{\{1,2\}} \\ 0 & \text{otherwise.}\end{cases}$$

□

Equation (2) will follow from the observation that the value $b$ in Claim 3.3 is independent of $i$. In other words, every row of $\mathcal{F} \cdot \mathbf{C}_s$ can be written as the product of $\omega^{-b \cdot s}$ for some $b \in \mathbb{Z}_m$, and a row vector that is *independent* of $s$. For $\mathbf{a} \in \mathbb{Z}_m^K$, let

$$\mathcal{I}(\mathbf{a}) = \{i \in [k] : \exists b_i \in \mathbb{Z}_m \text{ s.t } \mathbf{a}_i = b_i \cdot \mathbf{1}_{k-1}\}.$$

Observe that if $i, j \in \mathcal{I}(\mathbf{a})$, then $b_i = a_{i,j} = b_j$. Therefore, by Claim 3.3, for every $\mathbf{a} \in \mathbb{Z}_m^K$ there exists $b \in \mathbb{Z}_m$ such that for all $i \in [k]$,

$$(\mathcal{F} \cdot \mathbf{C}_s)(\mathbf{a}, i) = \begin{cases} m^{k-2} \cdot \omega^{b \cdot s} \cdot \sum_{\mathbf{r}_{-i} \in \mathbb{Z}_m^{K'}} C_i(\mathbf{r}_{-i}) \cdot \omega^{\langle \mathbf{a}_{-i}, \mathbf{r}_{-i} \rangle} \cdot \omega^{-b \cdot \mathsf{sum}(\mathbf{r}_{-i})} & \text{if } i \in \mathcal{I}(\mathbf{a}) \\ 0 & \text{otherwise.} \end{cases}$$

Similarly, for $s'$,

$$(\mathcal{F} \cdot \mathbf{C}_{s'})(\mathbf{a}, i) = \begin{cases} m^{k-2} \cdot \omega^{b \cdot s'} \cdot \sum_{\mathbf{r}_{-i} \in \mathbb{Z}_m^{K'}} C_i(\mathbf{r}_{-i}) \cdot \omega^{\langle \mathbf{a}_{-i}, \mathbf{r}_{-i} \rangle} \cdot \omega^{-b \cdot \mathsf{sum}(\mathbf{r}_{-i})} & \text{if } i \in \mathcal{I}(\mathbf{a}) \\ 0 & \text{otherwise.} \end{cases}$$

We are now ready to define $\mathbf{M}_{s,s'}$. Let $\mathbf{D}_{s,s'} \in \mathbb{Z}_m^{M,M}$ be the diagonal matrix whose diagonal is given by $\mathbf{D}_{s,s'}(\mathbf{a}, \mathbf{a}) = \omega^{b(s'-s)}$, where $b = 0$ if $\mathcal{I}(\mathbf{a}) = \emptyset$, and otherwise, $b = a_{\{i,j\}}$ where $\{i, j\}$ is the lexicographically smallest set such that $\{i, j\} \cap \mathcal{I}(\mathbf{a}) \neq \emptyset$. Then $\mathbf{D}_{s,s'} \cdot \mathcal{F} \cdot \mathbf{C}_s = \mathcal{F} \cdot \mathbf{C}_{s'}$. Since $\mathcal{F}$ is the Fourier transform matrix, it is invertible. Then we can define $\mathbf{M}_{s,s'}$ as

$$\mathbf{M}_{s,s'} = \mathcal{F}^{-1} \cdot \mathbf{D}_{s,s'} \cdot \mathcal{F}.$$

Equation (2) follows. □

Now, assume towards contradiction that there exists a $k$-party $t$-private $(S, m, q)$-share conversion. Then by Theorem 2.8 there exists a $k$-party $(\Pi_{2\text{-CNF}}, S, m, q)$-share conversion. Fix $s \in S$. Then all CNF sharings of $s$ are mapped to additive sharing of 0 in $\mathbb{F}_q$. By Lemma 3.2, all CNF sharings are mapped to additive sharing of 0 in $\mathbb{F}_q$, in particular, this is true for sharings of 1, which is a contradiction. □

### 3.2 Impossibility of $t$-Private Share Conversion in a Ring

In this section, we show the impossibility of a $t$-private $S_{\text{can},m}$-share conversion from $\mathbb{Z}_m$ to the ring $\mathbb{Z}_{m'}$, assuming $m$ has a prime factor that $m'$ does not have. For a natural number $n$ we let $\mathcal{P}(n)$ denote the set of all prime factors of $n$.

**Theorem 3.4.** *Let $k \in \mathbb{N}$, let $2 \leq t \leq k-1$, and let $m, m' \in \mathbb{N}$ be such that $\mathcal{P}(m) \not\subseteq \mathcal{P}(m')$, i.e., there exists a prime $p$ that divides $m$ but not $m'$. Then there is no $k$-party $t$-private $(S_{\text{can},m}, m, m')$-share conversion.*

*Proof.* To prove the theorem, we use Lemma 3.2 and the following lemma, which will allow us to remove the common prime factors of $m$ and $m'$, and reduce the proof to the case of share conversions to fields.

**Lemma 3.5.** *Let $m, m', k, n, n' \in \mathbb{N}$ such that $\mathcal{P}(n) = \mathcal{P}(n')$ and both are co-prime to $m$ and $m'$. If there is a $k$-party $(\Pi_{2\text{-CNF}}, S_{\text{can},mn}, mn, m'n')$-share conversion, then there is a $k$-party $(\Pi_{2\text{-CNF}}, S_{\text{can},m}, m, m')$-share conversion.*

*Proof.* The proof is done in two steps: In the first step, we use the assumed share conversion to construct a $k$-party $(\Pi_{2\text{-CNF}}, S_{\text{can},m}, m, m'n')$-share conversion. In the second step, we use Lemma 3.2 to argue the existence of a $k$-party $(\Pi_{2\text{-CNF}}, S_{\text{can},m}, m, m')$-share conversion.

**First Step.** Let $(C_i)_{i\in[k]}$ denote the share conversion from $\mathbb{Z}_{mn}$ to $\mathbb{Z}_{m'n'}$. We first define a share conversion $(C'_i)_{i\in[k]}$ from $\mathbb{Z}_m$ to $\mathbb{Z}_{m'n'}$. The idea is to have all the parties think of the secret $s' \in \mathbb{Z}_m$ as the unique value (from the CRT) $s \in \mathbb{Z}_{mn}$ that satisfies

$$s \equiv s' \pmod{m} \quad \text{and} \quad s \equiv 1 \pmod{n}.$$

Such $s$ exists since $\gcd(m,n) = 1$. This will be done by viewing the CNF randomness $r_{\{1,2\}}$ as 1 (mod $n$), and viewing every other $r_{\mathcal{T}}$ as 0 (mod $n$). Formally, define the functions $(C'_i)_{i\in[k]}$, where $C'_i : \mathbb{Z}_m^{\binom{k-1}{2}} \to \mathbb{Z}_{m'n'}$ for every $i \in [k]$, as follows: on input $(r'_{\mathcal{T}})_{\mathcal{T}\not\ni i} \in \mathbb{Z}_m^{\binom{k-1}{2}}$, consider the vector $(r_{\mathcal{T}})_{\mathcal{T}\not\ni i} \in \mathbb{Z}_{mn}^{\binom{k-1}{2}}$, where $r_{\mathcal{T}}$ is defined as the unique value satisfying

$$r_{\mathcal{T}} \equiv r'_{\mathcal{T}} \pmod{m} \quad \text{and} \quad r_{\mathcal{T}} \equiv \begin{cases} 1 \pmod{n} & \text{if } \mathcal{T} = \{1,2\} \\ 0 \pmod{n} & \text{otherwise.} \end{cases}$$

Then $C'_i$ is defined as

$$C'_i\left((r'_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) = C_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right).$$

Now, if $\sum_{\mathcal{T}\in\binom{[k]}{2}} r'_{\mathcal{T}} \in S_{\text{can},m}$, where summation is over $\mathbb{Z}_m$, then $\sum_{\mathcal{T}\in\binom{[k]}{2}} r_{\mathcal{T}} \in S_{\text{can},mn}$ over $\mathbb{Z}_{mn}$. Thus,

$$\sum_{i=1}^{k} C'_i\left((r'_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) = \sum_{i=1}^{k} C_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) = 0.$$

Similarly, if $\sum_{\mathcal{T}\in\binom{[k]}{2}} r'_{\mathcal{T}} = 1$ in $\mathbb{Z}_m$, then $\sum_{\mathcal{T}\in\binom{[k]}{2}} r_{\mathcal{T}} = 1$ in $\mathbb{Z}_{mn}$. Therefore,

$$\sum_{i=1}^{k} C'_i\left((r'_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) = \sum_{i=1}^{k} C_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) \neq 0.$$

We conclude that $(C'_i)_{i\in[k]}$ form a share conversion from $\mathbb{Z}_m$ to $\mathbb{Z}_{m'n'}$.

**Second Step.** We now move to the second step of the proof. Let $n' = q_1 \cdot q_2 \cdots q_\ell$, where each $q_j$ is a prime-power, be the factorization of $n'$. We show that for every $j \in [\ell]$, projecting the functions $(C'_i)_{i\in[k]}$ to $\mathbb{Z}_{q_j}$ results in share conversion that map every sharing to additive shares of 0. We then conclude that projecting them to $\mathbb{Z}_{m'}$ results in the desired $(\Pi_{2\text{-CNF}}, S_{\text{can},m}, m, m')$-share conversion.

Fix $j \in [\ell]$ and consider the functions $(C''_i)_{i\in[k]}$ from $\mathbb{Z}_m^{\binom{k-1}{2}}$ to $\mathbb{Z}_{q_j}$ defined as

$$C''_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) = C'_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) \bmod q_j$$

for every $i \in [k]$ and $(r_{\mathcal{T}})_{\mathcal{T}\not\ni i} \in \mathbb{Z}_m^{\binom{k-1}{2}}$. Since $(C'_i)_{i\in[k]}$ form a share conversion from $\mathbb{Z}_m$ to $\mathbb{Z}_{m'n'}$, the functions $(C''_i)_{i\in[k]}$ map every sharing of $0 \in \mathbb{Z}_m$ to additive sharing of $0 \in \mathbb{Z}_{q_j}$. Since $\gcd(q_j, m) =$

$\gcd(n', m) = 1$, by Lemma 3.2, these functions convert every sharing to additive sharing of 0, i.e.,

$$\sum_{i=1}^{k} C'_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) \equiv 0 \pmod{q_j}, \tag{3}$$

for all $(r_{\mathcal{T}})_{\mathcal{T}\in\binom{[k]}{2}} \in \mathbb{Z}_m^{\binom{k}{2}}$.

We can now show the existence of a share conversion from $\mathbb{Z}_m$ to $\mathbb{Z}_{m'}$. Define the functions $(\widetilde{C}_i)_{i\in[k]}$ from $\mathbb{Z}_m^{\binom{k-1}{2}}$ to $\mathbb{Z}_{m'}$ as

$$\widetilde{C}_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) = C'_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) \bmod m'$$

for every $i \in [k]$ and $(r_{\mathcal{T}})_{\mathcal{T}\not\ni i} \in \mathbb{Z}_m^{\binom{k-1}{2}}$. If $\sum_{\mathcal{T}\in\binom{[k]}{2}} r_{\mathcal{T}} \in S_{\text{can},m}$, then

$$\sum_{i=1}^{k} \widetilde{C}_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) = \sum_{i=1}^{k} C'_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) \bmod m' = 0.$$

On the other hand, if $\sum_{\mathcal{T}\in\binom{[k]}{2}} r_{\mathcal{T}} = 1$ in $\mathbb{Z}_m$, then

$$\sum_{i=1}^{k} \widetilde{C}_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) = \sum_{i=1}^{k} C'_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) \bmod m' \neq 0,$$

where the last transition follows from Equation (3), the fact that the sum is not 0 in $\mathbb{Z}_{m'n'}$, and since $\gcd(m', n') = 1$. We conclude that $(\widetilde{C}_i)_{i\in[k]}$ form a share conversion from $\mathbb{Z}_m$ to $\mathbb{Z}_{m'}$. □

The following claim states that we can add new prime factors to $m'$ while retaining the existence of a share conversion.

**Claim 3.6.** *Let $m, m', k \in \mathbb{N}$ and let $q'$ be a prime-power coprime to $m'$. If there is a $k$-party $(\Pi_{2\text{-CNF}}, S_{\text{can},m}, m, m')$-share conversion, then there is a $k$-party $(\Pi_{2\text{-CNF}}, S_{\text{can},m}, m, m'q')$-share conversion.*

*Proof.* Let $(C_i)_{i\in[k]}$ be the assumed $k$-party $(\Pi_{2\text{-CNF}}, S_{\text{can},m}, m, m')$-share conversion. Define the functions $(C'_i)_{i\in[k]}$, where each $C'_i : \mathbb{Z}_m^{\binom{k-1}{2}} \to \mathbb{Z}_{m'q'}$ is defined as follows: On input $(r_{\mathcal{T}})_{\mathcal{T}\not\ni i} \in \mathbb{Z}_m^{\binom{k-1}{2}}$, output the unique value in $\mathbb{Z}_{m'q'}$ satisfying

$$C'_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) \equiv C_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) \pmod{m'} \quad \text{and} \quad C'_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) \equiv 0 \pmod{q'}.$$

Then

$$\sum_{i=1}^{k} C'_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) = 0 \iff \sum_{i=1}^{k} C_i\left((r_{\mathcal{T}})_{\mathcal{T}\not\ni i}\right) = 0,$$

where summation on the left is in $\mathbb{Z}_{m'q'}$, and summation of the right is in $\mathbb{Z}_{m'}$. Therefore, $(C'_i)_{i\in[k]}$ is a $k$-party $(\Pi_{2\text{-CNF}}, S_{\text{can},m}, m, m'q')$-share conversion. □

We show that there is no $k$-party $t$-private $(S_{\text{can},m}, m, m')$-share conversion. By Theorem 2.8, it suffices to prove that there is no $k$-party $(\Pi_{\text{2- CNF}}, S_{\text{can},m}, m, m')$-share conversion. Assume towards a contradiction that such a share conversion exists. Let $p'$ be a prime-number coprime to both $m$ and $m'$. By Claim 3.6, there is a $k$-party $(\Pi_{\text{2- CNF}}, S_{\text{can},m}, m, m'p')$-share conversion.

If $\gcd(m, m'p') > 1$, there exists $n$ and $n'$ such that $\mathcal{P}(n) = \mathcal{P}(n')$ and are both coprime to both $m$ and $m'$. Write $m = \bar{m}n$ and $m' = \bar{m}'n'p'$, where $n$ and $n'$ are coprime to $\bar{m}$ and $\bar{m}'$, respectively. Then $\bar{m}$ and $\bar{m}'$ are coprime and Lemma 3.5 yields a $k$-party $(\Pi_{\text{2- CNF}}, S_{\text{can},\bar{m}}, \bar{m}, \bar{m}'p')$-share conversion.

Now, for every prime-power $q$ that appears in the factorization of $m'p'$, consider the projection of the outputs of the conversion to $\mathbb{Z}_q$. Since $q \nmid m$, Lemma 3.2 implies that the conversion maps every sharing to additive shares of 0 in $\mathbb{Z}_q$. This implies that all shares are mapped to additive sharing of 0 in $\mathbb{Z}_{m'p'}$, resulting in a contradiction. □

### 3.3 Characterization of $t$-Private Share Conversion in a Field

We now characterize when a $t$-private share conversion from $\mathbb{Z}_m$ to $\mathbb{F}_q$ exists. We show that a conversion exists if and only if $m$ and $q$ are prime-powers of the same prime.

**Theorem 3.7.** *Let $k, m, \ell \in \mathbb{N}$, let $2 \leq t \leq k-1$, and let $p$ be a prime. Then there exists a $k$-party $t$-private $(S_{\text{can},m}, m, p^\ell)$-share conversion if and only if $m = p^e$ for some $e \geq 1$.*

*Proof.* If $m$ is not a power of $p$, then by Theorem 3.4 there is no such share conversion. For the positive direction, we show a conversion from the additive scheme, namely, we show there is a $k$-party $(\Pi_{\text{add}}, S_{\text{can},p^e}, p^e, p^\ell)$. Note that this suffices since $\Pi_{\text{add}}$ has $k-1$ privacy. First, observe that $S_{\text{can},p^e} = \{0\}$. Next, define $(C_i)_{i\in[k]}$, where $C_i : \mathbb{Z}_{p^e} \to \mathbb{F}_{p^\ell}$ for every $i \in [k]$, as

$$C_i(r_i) = r_i \bmod p.$$

Fix $(r_i)_{i\in[k]} \in \mathbb{Z}_{p^e}^k$. For every $i \in [k]$, write $r_i = a_i \cdot p + b_i$, where $0 \leq b_i < p$. Then

$$\sum_{i=1}^{k} C_i(r_i) = \sum_{i=1}^{k} (r_i \bmod p) = \sum_{i=1}^{k} b_i,$$

where summation is in $\mathbb{F}_{p^\ell}$. Therefore, if $\sum_{i=1}^{k} r_i = a \cdot p^e$ for some $a \in \mathbb{N}$, i.e., the sum is in $S_{\text{can},p^e}$, then

$$\sum_{i=1}^{k} C_i(r_i) \equiv \sum_{i=1}^{k} b_i \equiv a \cdot p^e - p \cdot \sum_{i=1}^{k} a_i \equiv 0 \pmod{p}.$$

On the other hand, if $\sum_{i=1}^{k} r_i = a \cdot p^e + 1$ for some $a \in \mathbb{N}$, then

$$\sum_{i=1}^{k} C_i(r_i) \equiv \sum_{i=1}^{k} b_i \equiv a \cdot p^e + 1 - p \cdot \sum_{i=1}^{k} a_i \equiv 1 \pmod{p}.$$

□


## Acknowledgments

We thank Amos Beimel, Eran Omri, and Anat Paskin-Cherniavsky for useful conversations.

## References


[1] B. Alon, A. Beimel, and O. Lasri. Simplified PIR and CDS protocols and improved linear secret-sharing schemes. In B. Applebaum and H. R. Lin, editors, *Theory of Cryptography - 23rd International Conference, TCC 2025, Aarhus, Denmark, December 1-5, 2025, Proceedings, Part II*, volume 16269 of *Lecture Notes in Computer Science*, pages 365–398. Springer, 2025.

[2] A. Ambainis. Upper bound on the communication complexity of private information retrieval. In P. Degano, R. Gorrieri, and A. Marchetti-Spaccamela, editors, *Automata, Languages and Programming*, pages 401–407, Berlin, Heidelberg, 1997. Springer Berlin Heidelberg.

[3] H. Amran. Constructing multi-servers private information retrieval protocols. Master's thesis, Ben-Gurion University, 2016.

[4] O. Barkol, Y. Ishai, and E. Weinreb. On locally decodable codes, self-correctable codes, and $t$ -private PIR. In M. Charikar, K. Jansen, O. Reingold, and J. D. P. Rolim, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, 10th International Workshop, APPROX 2007, and 11th International Workshop, RANDOM 2007, Princeton, NJ, USA, August 20-22, 2007, Proceedings*, volume 4627 of *Lecture Notes in Computer Science*, pages 311–325. Springer, 2007.

[5] A. Beimel and Y. Ishai. Information-theoretic private information retrieval: A unified construction. In F. Orejas, P. G. Spirakis, and J. van Leeuwen, editors, *Automata, Languages and Programming, 28th International Colloquium, ICALP 2001, Crete, Greece, July 8-12, 2001, Proceedings*, volume 2076 of *Lecture Notes in Computer Science*, pages 912–926. Springer, 2001.

[6] A. Beimel and O. Lasri. Private information retrieval: Share conversions vs decoding polynomials. In N. Heninger and M. Rosulek, editors, *Advances in Cryptology – CRYPTO 2026*, pages 544–575, Cham, 2026. Springer Nature Switzerland.

[7] A. Beimel, Y. Ishai, and E. Kushilevitz. General constructions for information-theoretic private information retrieval. *Journal of Computer and System Sciences*, 71(2):213–247, 2005.

[8] A. Beimel, Y. Ishai, E. Kushilevitz, and I. Orlov. Share conversion and private information retrieval. In *Proceedings of the 27th Conference on Computational Complexity, CCC 2012*, pages 258–268, 2012. doi: 10.1109/CCC.2012.23.

[9] A. Beimel, Y. Ishai, R. Kumaresan, and E. Kushilevitz. On the cryptographic complexity of the worst functions. In Y. Lindell, editor, *TCC 2014*, volume 8349 of *Lecture Notes in Computer Science*, pages 317–342. Springer, 2014.

[10] T. Ben-David, V. Narayanan, O. Nissenbaum, and A. Paskin-Cherniavsky. New results in share conversion, with applications to evolving access structures. In N. Gilboa, editor, *6th Conference on Information-Theoretic Cryptography, ITC 2025, University of California, Santa Barbara, CA, USA, August 16-17, 2025*, volume 343 of *LIPIcs*, pages 11:1–11:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2025.

[11] Y. M. Chee, T. Feng, S. Ling, H. Wang, and L. F. Zhang. Query-efficient locally decodable codes of subexponential length. *Computational Complexity*, 22(1):159–189, 2013.

[12] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan. Private information retrieval. In *Proceedings of the 36th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 41–51, 1995. Journal version: *J. of the ACM*, 45:965–981, 1998.

[13] R. Cramer, I. Damgård, and Y. Ishai. Share conversion, pseudorandom secret-sharing and applications to secure computation. In J. Kilian, editor, *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005, Proceedings*, volume 3378 of *Lecture Notes in Computer Science*, pages 342–362. Springer, 2005.

[14] Z. Dvir and S. Gopi. 2-server PIR with subpolynomial communication. *J. ACM*, 63(4):39:1–39:15, 2016. doi: 10.1145/2968443. URL https://doi.org/10.1145/2968443.

[15] K. Efremenko. 3-query locally decodable codes of subexponential length. *SIAM J. Comput.*, 41(6):1694–1703, 2012.

[16] S. Fehr. Span programs over rings and how to share a secret from a module. Master's thesis, ETH Zurich, Institute for Theoretical Computer Science, 1998.

[17] F. Ghasemi and S. Kopparty. Fourier sparsity of delta functions and matching vector pirs. In S. Saraf, editor, *17th Innovations in Theoretical Computer Science Conference, ITCS 2026, Bocconi University, Milan, Italy, January 27-30, 2026*, volume 362 of *LIPIcs*, pages 68:1–68:22. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2026.

[18] F. Ghasemi, S. Kopparty, and M. Sudan. Improved PIR schemes using matching vectors and derivatives. In M. Koucký and N. Bansal, editors, *Proceedings of the 57th Annual ACM Symposium on Theory of Computing, STOC 2025, Prague, Czechia, June 23-27, 2025*, pages 1648–1656. ACM, 2025.

[19] A. Gupte and S. Ragavan. Exponentially fewer-server PIR from sparser $s$-decoding polynomials. Cryptology ePrint Archive, Paper 2026/1515, 2026. URL https://eprint.iacr.org/2026/1515.

[20] Y. Ishai and E. Kushilevitz. Improved upper bounds on information-theoretic private information retrieval (extended abstract). In J. S. Vitter, L. L. Larmore, and F. T. Leighton, editors, *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing*, pages 79–88. ACM, 1999.

[21] T. Itoh. Efficient private information retrieval. *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, E82-A(1):11–20, 1999.

[22] T. Itoh and Y. Suzuki. Improved constructions for query-efficient locally decodable codes of subexponential length. *IEICE Transactions on Information and Systems*, E93-D(2):263–270, 2010. ISSN 1745-1361. doi: 10.1587/transinf.e93.d.263. URL http://dx.doi.org/10.1587/transinf.E93.D.263.

[23] J. Katz and L. Trevisan. On the efficiency of local decoding procedures for error-correcting codes. In F. F. Yao and E. M. Luks, editors, *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pages 80–86. ACM, 2000.

[24] K. S. Kedlaya and S. Yekhanin. Locally decodable codes from nice subsets of finite fields and prime factors of Mersenne numbers. Technical Report TR07-040, Electronic Colloquium on Computational Complexity, 2007.

[25] T. Liu, V. Vaikuntanathan, and H. Wee. Conditional disclosure of secrets via non-linear reconstruction. In J. Katz and H. Shacham, editors, *Advances in Cryptology - CRYPTO 2017, Part I*, volume 10401 of *Lecture Notes in Computer Science*, pages 758–790. Springer, 2017.

[26] T. Liu, V. Vaikuntanathan, and H. Wee. Towards breaking the exponential barrier for general secret sharing. In *EUROCRYPT 2018*, volume 10820 of *LNCS*, pages 567–596, 2018.

[27] A. Paskin-Cherniavsky and O. Nissenbaum. New bounds and a generalization for share conversion for 3-server PIR. *Entropy*, 24(4):497, 2022.

[28] A. Paskin-Cherniavsky and L. Schmerler. On share conversions for private information retrieval. *Entropy*, 21(9):826, 2019.

[29] D. P. Woodruff and S. Yekhanin. A geometric approach to information-theoretic private information retrieval. In *20th Annual IEEE Conference on Computational Complexity (CCC 2005), 11-15 June 2005, San Jose, CA, USA*, pages 275–284. IEEE Computer Society, 2005.

[30] S. Yekhanin. Towards 3-query locally decodable codes of subexponential length. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing (STOC)*, pages 266–274, 2007.