entropy

MDPI

Article

New Bounds and a Generalization for Share Conversion for 3-Server PIR

Anat Paskin-Cherniavsky * and Olga Nissenbaum

Computer Science Department, Ariel University, Ariel 40700, Israel; olga@nissenbaum.ru
* Correspondence: anatpc@ariel.ac.il

Abstract: Private Information Retrieval (PIR) protocols, which allow the client to obtain data from servers without revealing its request, have many applications such as anonymous communication, media streaming, blockchain security, advertisement, etc. Multi-server PIR protocols, where the database is replicated among the non-colluding servers, provide high efficiency in the information-theoretic setting. Beimel et al. in CCC 12' (further referred to as BIKO) put forward a paradigm for constructing multi-server PIR, capturing several previous constructions for $k \geq 3$ servers, as well as improving the best-known share complexity for 3-server PIR. A key component there is a share conversion scheme from corresponding linear three-party secret sharing schemes with respect to a certain type of "modified universal" relation. In a useful particular instantiation of the paradigm, they used a share conversion from $(2,3)$-CNF over $\mathbb{Z}_m$ to three-additive sharing over $\mathbb{Z}_p^\beta$ for primes p_1, p_2, p where $p_1 \neq p_2$ and $m = p_1 \cdot p_2$, and the relation is modified universal relation C_{S_m}. They reduced the question of the existence of the share conversion for a triple (p_1, p_2, p) to the (in)solvability of a certain linear system over $\mathbb{Z}_p$, and provided an efficient (in $m, \log p$) construction of such a sharing scheme. Unfortunately, the size of the system is $\Theta(m^2)$ which entails the infeasibility of a direct solution for big m's in practice. Paskin-Cherniavsky and Schmerler in 2019 proved the existence of the conversion for the case of odd p_1, p_2 when $p = p_1$, obtaining in this way infinitely many parameters for which the conversion exists, but also for infinitely many of them it remained open. In this work, using some algebraic techniques from the work of Paskin-Cherniavsky and Schmerler, we prove the existence of the conversion for even m's in case $p = 2$ (we computed β in this case) and the absence of the conversion for even m's in case $p > 2$. This does not improve the concrete efficiency of 3-server PIR; however, our result is promising in a broader context of constructing PIR through composition techniques with $k \geq 3$ servers, using the relation C_{S_m} where m has more than two prime divisors. Another our suggestion about 3-server PIR is that it's possible to achieve a shorter server's response using the relation $C_{S'_m}$ for extended $S'_m \supset S_m$. By computer search, in BIKO framework we found several such sets for small m's which result in share conversion from $(2,3)$-CNF over $\mathbb{Z}_m$ to 3-additive secret sharing over $\mathbb{Z}_p^{\beta'}$, where $\beta' > 0$ is several times less than β, which implies several times shorter server's response. We also suggest that such extended sets S'_m can result in better PIR due to the potential existence of matching vector families with the higher Vapnik-Chervonenkis dimension.

Keywords: PIR; Share conversion; CNF secret sharing; communication complexity

Citation: Paskin-Cherniavsky, A.; Nissenbaum, O. New Bounds and a Generalization for Share Conversion for 3-Server PIR. *Entropy* **2022**, *24*, 497. https://doi.org/10.3390/e24040497

Academic Editor: Boris Ryabko

Received: 6 February 2022
Accepted: 29 March 2022
Published: 1 April 2022

1. Introduction

1.1. Private Information Retrieval

Private Information Retrieval (PIR) protocols allow the client to fetch items from the server's database without disclosing to the server which item was requested. A main challenge in constructing PIR protocols is minimizing the communication complexity. The idea of PIR was introduced by Chor et al. [1], together with the 2-server PIR protocol having the communication complexity $O(n^{1/3})$ for the dataset size n. PIR has a wide variety of applications such as anonymous communication [2,3], privacy-preserving media

streaming [4], blockchain security [5,6], personalized advertisement [7], location and contact discovery [8–10], etc.

The naive approach to PIR is just to make the server send all the items in the database to the client: we stress that PIR cares only about the privacy of the client's request but not about the privacy of the server. However, it entails a huge communication complexity equal to the size of the database. To shorten the communication complexity and still keep the privacy of the request, there are two main approaches to construct PIR:

- Historically, the first type of PIR was **a Multi-Server PIR** [1], where the database is replicated for $k \geq 2$ non-colluding servers. The client secret-shares its request, and servers locally compute the secret-shared response and send it back to the client. The client recovers the item from the shares of response. Multi-Server PIR protocols, such as [11–14] are relatively efficient in information-theoretic settings. The requirement of the replicated database kept by the non-colluding parties is restrictive; however, there is a space for such a PIR, preferably in blockchain databases, cloud services, multi-server enterprise ecosystems where a small number of servers (but not all) are likely to be compromised.
- **Single-Server PIR** protocols work in a computational setting and are built on the basis of homomorphic encryption (FHE, AHE, or SHE). The starting point in single-server PIR is the AHE-based protocol of Kushilevitz and Ostrovski [15]. The early single-server PIR constructions were both computationally and communicationally low efficient, although recently significant progress was made which allow speaking about the practically suitable one-server PIR solutions [16–19]. For instance, the OnionPIR protocol from SHE [16] achieves a 64 KB request and 128 KB response in the online phase of the protocol (and the same in the offline phase) for all the realistic database sizes.

On the high level, for both approaches, the database is represented as a function (usually, a polynomial) f such that for any key x and the correspondent value (a record) y holds $y = f(x)$. Then, the client has to send the request x to the server (servers) in a way that preserves its privacy. For the Single-Server PIR, it means that x is sent encrypted, in the Multi-Server paradigm, x is secret-shared. Encryption or secret sharing has to be homomorphic so that the server (servers) could compute the function $f(x)$ under the encryption/secret-sharing and send the encrypted or secret-shared response y back to the client.

In a 2-server computationally-secure PIR of Gilboa and Ishai [20], the request is shared as a DPF (Distributed Point Function) and has a polylog length. In this case, to compute the shares of the response, only additive operations are needed (DPF sharing is homomorphic in respect of them). However, in the information-theoretic setting, which is the focus of this work, it is still unclear how to construct *efficient* in terms of communication and computation PIR with the secret sharing which is homomorphic in respect of any number of additions and multiplications.

Currently, 3 generations of information-theoretic PIR protocols exist: the first generation originated from the work of Chor et al [1] is based on Reed-Muller codes and have communication complexity $n^{1/\Theta(k)}$, in the second from Beimel et al. [21] they restated some of the previous results in a more arithmetic language, in terms of polynomials, and also considered a certain encoding of the inputs and element-wise secret sharing the encoding, which resulted in $n^{O(k)}$ communication complexity. The third generation from works of Efremenko [11] followed by [22–26], Yekhanin [12], Beimel et al. [13], Dvir and Gopi [14] is based on matching vectors and is the most computationally efficient line of protocols with the complexity $n^{o(1)}$ for database size n. In all the 3rd generation schemes, but [14], as was demonstrated by Beimel et al. [13], in fact, the combination of two secret-sharing schemes is utilized, both linear in different groups, and a *share conversion* with respect to some relation, allowing to locally perform some non-linear operation over the shares (apart from the case of the identity relation).

1.2. Share Conversion

Suppose that there is some number of parties, each holding a share of a secret s which was created by a secret-sharing scheme Sh_1. **The share conversion** is defined as a process of a local computation performed by those parties based only on their shares and outputting the new shares of the secret s' in a different scheme Sh_2 so that there is some predefined relation between s and s'. A systematic study of share conversion was started by Cramer et al. [27] by considering the case $s = s'$ for two arbitrary linear secret sharing systems over different fields.

Let us consider an easy illustrative example: for the function $f(x) = x_1 \cdot x_2$ over the ring R', and for the conversion's relation $s' = s^2$, for the input $x = (x_1, x_2)$ shared in a linear scheme over the ring R, it is possible to compute $f(x)$ in the following circuit: first, according to the linear property of the first scheme, servers locally compute shares of $x_3 = x_1 + x_2$, then convert shares of x_1, x_2 and x_3 to shares of x_1^2, x_2^2 and x_3^2 over R', and finally obtain shares of the response $y = 2^{-1}(x_3^2 - x_1^2 - x_2^2)$.

This approach, however, leaves room for improvement, as such a conversion usually increases the size of the request and response in PIR, because the conversion is a local operation and therefore it is not a trivial issue: to evaluate the circuit which computes some succinct function $f(x)$ which represents the database, the client forms its request as a proper input to this circuit. In addition, not any circuit is possible to compute within the existing secret sharing and conversion schemes, which means that we are bound to only certain kinds of the circuit families and, depending on the VC-dimension of these families of those certain function families, the proper representation of request might be much larger than the size of the database. Recall that the notion of the VC-dimension was introduced by V. Vapnik and A. Chervonenkis in [28]. Informally, for the boolean function family $\mathcal{F}$, where each $f \in \mathcal{F} : D \to \{0,1\}$, VC-dimension $VC(\mathcal{F})$ is the size of the largest $I \subset D$ such that the set $\left\{ f|_I \,\middle|\, f \in \mathcal{F} \right\}$ of restrictions of functions from $\mathcal{F}$ contains all the possible boolean functions over I. The higher $VC(\mathcal{F})$ relative to $|D|$, the more efficient PIR can be built. For a precise definition, see [13].

Using homomorphic properties of secret sharing schemes to perform MPC on shared values is a widely used technique in information-theoretic MPC, initiated by the seminal work of [29]. Indeed, in order to (semi honestly) securely evaluate an algebraic circuit, the parties share their input with Shamir secret sharing. Then, linear combinations can be homomorphically evaluated 'for free' via local computation on the shares so that additions can be performed repeatedly any number of times. Multiplications can also be performed, however, multiplying two shared values results in a value shared according to Shamir with the doubled degree. This limits the depth of a circuit computable with (even) 1-privacy if we require that the only communication round will be sending shares for the final reconstruction. This idea transfers to PIR, where inputs come from a single party, so they may also be conveniently preprocessed by it via arbitrarily complex functions (which is not always possible for inputs distributed among multiple parties). For instance, for 3-server PIR, degree-2 polynomials can be locally evaluated if Shamir secret sharing was used. As degree-2 polynomials (over a field) in n variables have non-trivially high VC dimension (n^2), this allows for encoding each input via a vector of $O(2^{n/2})$ entries and using the appropriate share conversion. For k-server PIR, different kinds of share conversion may enable us to evaluate a family of shallow circuits that both have high VC dimension and suitable secret sharing with share conversion, allowing us to locally evaluate them. In particular, note that a share conversion for a suitable relation, rather than a function suffice to evaluate circuits of that type.

1.3. BIKO Framework

In [13], Beimel, Ishai, Kushilevitz, and Orlov (BIKO) interpret the state of the art 3-server PIR schemes as using share conversion from a (variant) of Shamir secret sharing over a certain ring R_m for small composite m, applied to circuits stemming from MV codes [30] $\{u_1, \ldots, u_h\}, \{v_1, \ldots, u_h\}$ with a bounded set $S \cup \{0\}$ of $< u_i, u_j >$ values, for

some $S \subseteq \mathbb{Z}_m \setminus \{0\}$. It has the property that $< u_i, v_i >= 0$, while $< u_j, v_i >$ for $j \neq i$ is in S. We refer to such codes as S-bounded MV codes. They manage to get improved complexity of the resulting PIR, by using conversions from CNF secret sharing rather than from Shamir over certain small R_m, for which a conversion from Shamir for that relation does not exist (the (t,k)-CNF is a threshold secret sharing scheme introduced in [31]; see Section 2.2 for a detailed description). Specifically, they obtained conversions from $(2,3)$-CNF over $\mathbb{Z}_m$ to the additive secret sharing scheme over $\mathbb{Z}_p^\beta$ for the following relation $C_S = \left\{(0,s') | s' \in \mathbb{Z}_p^\beta \setminus \{0\}\right\} \cup \left\{(s,0) | s \in S \setminus \{0\}\right\} \cup \left(\mathbb{Z}_m \setminus \left\{S \cup \{0\}\right\}\right) \times \mathbb{Z}_p^\beta$. They work with the so-called *canonical* set $S = S_m = \left\{x \in \mathbb{Z}_m | \forall i \ x \text{ is either 0 or 1 mod} p_i^{e_i}\right\} \setminus \{0\}$, where $m = \prod_{i=1}^k p_i^{e_i}$ is the decomposition of m into prime factors. This is a useful choice, due to the existence of good S_m-bounded MV codes over composite moduli m. Their approach is motivated by the existence of conversions for CNF to additive (roughly, that CNF can be converted to "any" scheme, and any scheme can be converted to additive), they use Sh_1 as CNF over a certain ring, and Sh_2 as additive over another ring. This relation (although not a function) suffices to evaluate the required type of circuits, arising from the MV family. There is a potential tradeoff here between the best MV codes that exist over a certain ring R, and the size (more generally, the identity) of the set S that can be achieved. On a high level:

1. The smaller S is, the easier it is to find a suitable share conversion (required to evaluate functions in the circuit family induced by the MV code).
2. The larger S is, the easier it is to find an MV code resulting in a family of circuits with high VC dimension. The communication complexity of the resulting PIR decreases with the VC dimension of the set (and eventually, the size of the shallow circuit to evaluate).

The concrete parameters of both constructions used so far for 3-server PIR (in their most efficient variants) follow from the following Theorem 7, and instantiations of it via known constructions of MV codes and share conversion schemes.

On a very high level, these PIR protocols consist of three steps and is shown in Construction 1.

Construction 1: BIKO Framework [13]

1 Let $f : \{0,1\}^{log(n)} \to \{0,1\}$ denote the server's database. The client preprocesses its input $x \in \{0,1\}^{log(n)}$ into a vector $v_x \in R^h$ for a (constant) ring R, where $\{v_x\}_x$ is a set of vectors of an S-bounded MV code. It shares the vector coordinate-wise among the k servers via some $(2,k)$-private secret sharing scheme Sh_1 (so no single server learns anything about the secret).

2 The servers use linear homomorphism properties of Sh_1, Sh_2, which are homomorphic over certain finite groups, to locally evaluate (an encoding of) f on the shared v. More concretely,

$$f(v) = \sum_{\{i|f(i)=1\}} f_i(v)$$

where $f_i(v) =< u_i, v >$. In some more detail, each $< u_i, v >$ uses linear homomorphism of Sh_1, then a share conversion from Sh_1 to Sh_2 relatively to C_S, applied to each share of $f_i(v)$, and finally linear homomorphism of Sh_2 is applied to evaluate $\sum_i f_i(v)$ on the resulting shares. The share conversion is required to transform $< v_i, v >$ for $v_i = v$ into a non-zero value, and $< u_j, v >$ for $v_j \neq v$ into 0's, making the sum non-zero iff. $f(v) = 1$. Then each server sends its share to the client.

3 The client recovers the output using linear homomorphism of Sh_2, and post-processing the value.

The correctness of the scheme is easy to verify.

For a 3-server PIR, Ref. [13] provides the technique for the constructing the conversion (it such a conversion exists) from (2,3)-CNF to the additive secret sharing and obtains results for some special cases. Utilizing the results of Beimel et al., Paskin-Cherniavsky and Schmerler in [32] proved that there is a share conversion from (2,3)-CNF over $\mathbb{Z}_m$ to 3-additive secret sharing over $\mathbb{Z}_p$, if $m = p_1 p_2$, for distinct odd primes p_1 and p_2, one of which is equal to p. Thereby they found infinitely many cases when conversion falling into the BIKO framework exists.

Theorem 1 ([13,32]). *Let $m = p_1 \cdot p_2$, where p_1, p_2 are distinct primes, and p is a prime. Then, there exists a share conversion from $(2,3)$-CNF to additive over $\mathbb{Z}_p^\beta$ for the relation C_{S_m} for some β in the following cases:*

1. *$p_1, p_2 \neq 2$, and $p \in \{p_1, p_2\}$*
2. *$p_1 = 2, p_2 \in \{3,5,7\}$ and $p = 2$.*

For other cases of $m = p_1 \cdot p_2$ and p, however, the existence of the conversion was neither confirmed nor disproved. The constant β in Theorem 1 seems to grow with m, but due to the techniques used, it has not been proven for any infinite family of parameters.

Remark 1. *However, not all the 3rd generation information-theoretic PIR protocols fall into the BIKO framework. For instance, the work of [14] could be viewed as a certain generalization of it. This beautiful work surprisingly manages to carry over "3rd generation" PIR communication complexity previously achieved for 3 or more servers, to the 2-server setting, resolving a long standing open problem, thereby illustrating the limitations of the BIKO framework, providing evidence that generalizing it in certain directions can be instrumental in the context of PIR. In some more detail, [14]'s PIR has a bilinear, rather than linear reconstruction in Sh_2, and the step corresponding to share conversion can not be cleanly viewed as a share conversion from Sh_1 to Sh_2 according to C_S (or in fact any) relation. In particular, the client essentially uses a 2-out-of-3 sharing scheme to make the share conversion work, with himself holding one of the shares.*

1.4. Our Contribution

Obtaining another infinite class of conversions from (2,3)-CNF.

Following the BIKO framework [13] and utilizing some results of [32], we prove that:

Theorem 2 (Main result, informal)**.**

- *There exists a share conversion from (2,3)-CNF over $\mathbb{Z}_{2q}$ to 3-additive secret-sharing scheme over $\mathbb{Z}_2^{(q-1)(q-2)}$ for any odd prime q.*
- *There is no conversion from (2,3)-CNF over $\mathbb{Z}_{2q}$ to $\mathbb{Z}_p^\beta$ for any odd primes q and p (including the case $q = p$) and any $\beta > 0$.*

In this way, we prove the existence of the conversion for infinitely many cases, and also for infinitely many cases we prove a conversion does not exist. Together with [32] for m's which are products of two primes, it leaves open only the question of the conversion in the case when $m = p_1 p_2$, where p_1 and p_2 are both odd and not equal to p.

Note also that for considered cases, we managed to compute the parameter β which determines the server's response size. We prove that β in Theorem 7 is indeed the best for $m = 6$ among $m = p_1 p_2$ where $p_1 = 2$. More concretely, one of our contributions is the precise value of β for share conversion with respect to relation $C_{S_{2q}}$. Previous techniques did not allow to compute β, as they traded generality that could allow computing β for some additional simplicity—using a single row in $M_{\not\equiv}$ to understand the rank difference $\beta = rank(M_{\equiv,\not\equiv}) - rank(M_{\equiv})$.

Computing and improving server reply size.

Another somewhat surprising observation we made is that we may sometimes increase S beyond S_m so that a conversion from $(2,3)$-CNF over $\mathbb{Z}_m$ to $\mathbb{Z}_q^\beta$ (for the same m, q as before) still exists. This may have two possible implications. A direct implication that we observed experimentally for several values of m, is that the rank difference β sometimes goes down, but not all the way to 0. Thus, if the share conversion still exists, as follows from the BIKO technique, β may decrease, leading to the reduced size of the server's response. We checked this fact for some small m's by computer search and obtained positive results, which is presented in Section 4. Indeed, we obtained smaller β supplementing S_m up to S'_m by additional values. We informally sum the result of the computer search in the following theorem.

Theorem 3. *There exists a share conversion from (2,3)-CNF over $\mathbb{Z}_m$ to 3-additive secret-sharing scheme over $\mathbb{Z}_p^{\beta'}$ with respect to the relation $C_{S'_m}$, refining β, where:*

- $m = 14$, $p = 2$, $S'_m = S_m \cup \{3\}$ *and* $S'_m = S_m \cup \{5\}$, $\beta = 30$, $\beta' = 6$;
- $m = 15$, $p = 3$, $S'_m = S_m \cup \{11\}$ $\beta = 24$, $\beta' = 12$;
- $m = 21$, $p = 3$, $S'_m = S_m \cup \{8\}$, $\beta = 60$, $\beta' = 30$;
- $m = 33$, $p = 3$, $S'_m = S_m \cup \{23\}$, $\beta = 180$, $\beta' = 90$;
- $m = 15$, $p = 5$, $S'_m = S_m \cup$ (*any non-empty subset of* $\{4, 7, 13\}$), $\beta = 8$, $\beta' = 2$;
- $m = 35$, $p = 5$, $S'_m = S_m \cup$ (*any non-empty subset of* $\{8, 22, 29\}$), $\beta = 120$, $\beta' = 30$;
- $m = 21$, $p = 7$, $S'_m = S_m \cup$ (*any non-empty subset of* $\{4, 10, 13, 16, 19\}$), $\beta = 12$, $\beta' = 2$;
- $m = 35$, $p = 7$, $S'_m = S_m \cup$ (*any non-empty subset of* $\{6, 11, 16, 26, 31\}$), $\beta = 72$, $\beta' = 12$.

This result may also be viewed as evidence that canonical sets S_m for m with a larger number r of prime factors may potentially have share conversions for C_{S_m} for (significantly) smaller than $2^r - 1$ number of servers (as we have conversions for $2^r - 1$ servers but S larger than S_m, where the resulting linear system has much more rows than columns). This direction is interesting to explore, initiating a systematic search for share conversions with server sets as small as possible, resulting in PIR with share complexity polynomial in MV codeword length for m which is a factor of r primes.

In addition to our two main contributions, **we identify a few minor errors** in [13,32]. Nevertheless, these errors do not affect the correctness of any of their main contributions.

- We recalculated some computer search results of [13] (BIKO) as they come in contradiction with the theoretical result of Paskin-Cherniavsky and Schmerler. In particular, [13] showed the absence of the conversion for $m = 35$, $p = 7$, while [32] proved that the conversion for this case exists. In addition, we obtained numerical results for cases $m = 22$, 26, 33 which were not considered in BIKO. Our numerical results given in Section 4 confirm both our theoretical result for $p_1 = 2$ and the conclusion of [32].
- We corrected some calculation mistakes made in previous work [32]. The corrigenda are shown in Appendix A.

1.5. Instantiations of BIKO and Future Directions of Our Work

Almost all third-generation PIR protocols falling in a BIKO framework, utilize the conversion from Shamir secret sharing instead of CNF. The existence of the conversion from Shamir secret sharing scheme implies the existence of conversion from CNF, but not vice versa [13].

The following theorem by V. Grolmusz generalizes a similar instance of the theorem for 3-servers in [13], to put our work in a broader context. It states the size of the MV families depending on the constant m which has an impact on the complexity of the PIR protocols based on them.

Theorem 4 ([30]). *Let $m = \prod_{i=1}^{r} p_i$ where the p_i's are distinct constant primes, and $r > 1$ is constant. Then there exists an MV code family $C \subseteq \mathbb{Z}_m^h$ of size $|C| = \exp\left(\frac{c \log^r(h)}{\log\log(h)^{(r-1)}}\right)$ which is S_m-bounded. Here $c \leq p_r^{-r}$, where p_r is the largest prime.*

In fact, the construction in Theorem 4 generalizes to any m with r distinct prime divisors.

Next, we outline some parameters for which suitable share conversions leading to (3rd generation) PIR via the BIKO framework and MV codes from Theorem 4 exist. Note that Theorems 5 and 6 were initially stated in terms of conversion from Shamir secret sharing, but a corresponding conversion from CNF is implied.

Theorem 5 ([11,26]). *For each $r \geq 2$, there exists a number m with r distinct prime divisors $p_1 \leq \ldots \leq p_r$, with $p_r \geq 73$, for which there exists a share conversion from $(2, 3/4 \cdot 2^r)$-CNF over $\mathbb{Z}_m$ to $3/4 \cdot 2^r$-additive over $\mathbb{Z}_2^\beta$ for some $\beta < m$, and relation C_{S_m}. Furthermore, such a conversion exists for every m of the form $2^t - 1$ with r distinct prime divisors, if the number of parties, $3/4 \cdot 2^r$, is replaced by 2^r.*

In a nutshell, the above result is obtained by [26] via a composition technique applied to [11]'s result for 3-server and 2^r-server PIR. The reduction in the number of parties from 2^r to $3/4 \cdot 2^r$ for m with r prime distinct divisors follows from the (somewhat surprising) 3-party conversion for $r = 2$ and $m = 73 \cdot 7$.

In [23], the authors found 50 additional such 3-party conversions for $m = p_1 \cdot p_2$ (which need to satisfy a certain condition), leading to further improvements in the number of parties as a function of r. Note, that for all m found in [23], $p_r \geq 73$ are large, so the constant in Theorem 1 grows fast with r.

Theorem 6 ([23]). *For each $r \geq 104$, there exists a share conversion from $(2, (3/4)^{51} \cdot 2^r)$-CNF over $\mathbb{Z}_m$ to $(3/4)^{51} \cdot 2^r$-additive over $\mathbb{Z}_2^\beta$ for some $\beta < m$, and relation C_{S_m}. For each $r < 104$, there exists a share conversion from $(2, 3^{\lceil r/2 \rceil})$-CNF over $\mathbb{Z}_m$ to $3^{\lceil r/2 \rceil}$-additive over $\mathbb{Z}_2^\beta$ for some $\beta < m$, and relation C_{S_m}.*

Note that for the above instantiations, "descending" from [11], m must be odd.

Theorem 7 (Implicit in [13]). *Let $m \in \mathbb{N}$, $\{0\} \subseteq S \subseteq \mathbb{Z}_m$, and C an S-bounded MV code family $\{C_h\}$ of vectors in $\mathbb{Z}_m^h$. Assume also there exists share conversion from $(2, k)$-CNF over $\mathbb{Z}_m$ to $\mathbb{Z}_p^\beta$ for some constant β, for the relation C_S. Then there exists a k-server PIR family for databases of size $n = |C_h|$ with client's message of size $\lceil h \log(m) \rceil$ and server's message of size $\lceil \beta \log p \rceil$.*

From Theorems 6 and 7 follows

Corollary 7. *Let $r \geq 3$. Then there exists some $m = \prod_{i=1}^{r} p_i^{e_i}$ where $p_1 < \ldots < p_r$ are primes where $m | (2^\beta - 1)$ for some β. Then a $3/4 \cdot 2^r$-server PIR with client communication complexity of $O(2^{2p_r \cdot \log^{1/r}(n) \log\log^{1-1/r}(n)})$ and (each) server's communication complexity $\beta \log(p)$, for some $\beta \leq m$ exists. For $r \geq 104$, this improves to $(3/4)^{51} 2^r$ servers, and $3^{\lceil r/2 \rceil}$ servers for $r < 104$.*

We note that among the known m's in the Corollary above for $r = 2$, $p_r \geq 73$ and grows particularly fast with r for $r \geq 104$ if $(3/4)^{51} 2^r$ servers (instead of $3/4 \cdot 2^r$) exist.

Instantiating Theorem 7 with Theorem 4 for MV-code construction, and either Theorem 1, we obtain the best known concrete efficiency of 3-server PIR, with $2^{6\sqrt{\log(n)\log\log(n)}}$ communication complexity. On the other hand, for more than polynomially improved communication complexity and a larger number of servers, the best result is obtained by instantiating the share conversion via Theorem 5.

Our concrete result does not improve communication complexity for 3-server PIR, which is essentially optimal for conversion from $\mathbb{Z}_6$ by [13] as stated in Theorem 1. However,

the technical tools developed may help understand the existence of share conversions for even m with a larger number of prime factors, with better the communication complexity of PIR and the larger number of servers. Due to the generality of BIKO's framework, converting from CNF, one could hopefully get improved efficiency of communication complexity relatively to the number of servers. In particular, as noted above, the instantiation of BIKO as in [11] does not yield PIR protocols with even m, and the known values of m have large maximal factors and lead to PIR with high constants in the exponent. By a direct corollary from Theorems 4 and 5 similar to Corollary 7, we get a 6-server PIR with communication complexity $O\left(2^{146\cdot\log^{1/3}(n)\log\log^{2/3}(n)}\right)$. Using the BIKO framework instantiated Theorem 5—the 'furthermore' part, for 8-server PIR we obtain a complexity of $O\left(2^{34\cdot\log^{1/3}(n)\log\log^{2/3}(n)}\right)$, by using $m = 255 = 3\cdot 5\cdot 17 = 2^8 - 1$, and instantiating Theorem 4 with $m = 255$. Thus, as far as we know, no PIR with complexity better than $O\left(2^{146\cdot\log^{1/3}(n)\log\log^{2/3}(n)}\right)$ (best known 6-server PIR) exists for 7 servers. We conjecture that a 7-server PIR with much improved constants exists, by using share conversion from $(2,7)$-CNF with parameters generalizing the conversions we obtained for $m = 2\cdot p_2$.

Conjecture 1. *A share conversion from $(2,7)$-CNF over $\mathbb{Z}_{30}$ to $\mathbb{Z}_2^\beta$ for some constant β exists, implying a 7-server PIR for $O\left(2^{10\cdot\log^{1/3}(n)\log\log^{2/3}(n)}\right)$.*

We hope to be able to verify the conjecture more easily by generalizing the insights we have for the existence of a share conversion for $m = 2\cdot p_2$ to a share conversion to $m = 2\cdot 15$ (more generally, for $2\cdot c$ for some composite c), and the fact that in this case of p_1, the analysis turned out to be rather simple. Another reason to hope we can manage with 7 servers is that $M_{\equiv}$ is in that case, has a form similar to the 3-server case considered in present work (unless, for example, 6-server case). See Section 1.6 for more details.

A broader goal is improving the number of servers one can tolerate for PIR with CC corresponding to MV codes over $\mathbb{Z}_m$ with r prime factors. While [26] show how to achieve $(3/4)^{51}2^r$ servers for an infinite number of r's and corresponding m's, and $3^{r/2}$-server PIR for finitely many r's, it would be interesting to improve Theorem 6 to get share conversion for $3^{r/2}$-server PIR for all r. Our hope is to devise a composition theorem along the lines of [26], composing 'gadgets' of conversions from $(2,3)$-CNF over $\mathbb{Z}_m$ for coprime composite m's. As we already have such conversions for infinitely many pairwise coprime m's via Theorem 1, we only need a suitable composition theorem. In fact, it is not hard to show, that if we had conversions for coprime m_1, m_2 respectively, both to $\mathbb{Z}_p^\beta$ for the same p, say $\mathbb{Z}_2^\beta$, we would obtain the result. In particular, it is strictly easier to prove the existence of conversion from $\mathbb{Z}_{p_1p_2}$ to $\mathbb{Z}_2^\beta$ for some β depending on p_1, p_2 for infinitely many coprime $p_{2i+1}\cdot p_{2i+2}$'s (as the 51 known cases based on Mersenne-style primes in [26] are a special case). To summarize, to complete this direction, we only need to find a conversion from $(2,3)$-CNF over $\mathbb{Z}_{m_i}$ to $\mathbb{Z}_2^{\beta_i}$ for infinitely many coprimes m_i's of the form $m_i = p_1\cdot p_2$ where p_1, p_2 are distinct primes. This seems to require only moderate extension on the (linear algebraic) toolbox conversions from $(2,3)$-CNF that has been laid out in the seminal work of [13] and subsequently in [32].

A more ambitious still direction (which we expect to be more technically involved) is expected to lead to dramatic improvements in the number of servers, bringing it down from exponential to linear in r. It relies on the following composition lemma, which is not hard to prove (see full version for details).

Lemma 1. *Let $m_1 = 2m_1'$, $m_2 = 2m_2'$, where m_1', $m_2' > 1$ are odd coprime integers. Assume there exists a share conversion from $(2,k)$-CNF over $\mathbb{Z}_{m_1}$ to (t_1,k)-CNF over $\mathbb{Z}_2^{\beta_1}$ for the relation S_{m_1} (and an analogous conversion exists for m_2). Then there exists a share conversion from $(2,k)$-CNF over $\mathbb{Z}_{2m_1'm_2'}$ to (t_1+t_2+1,k)-CNF over $\mathbb{Z}_2^{max(\beta_1,\beta_2)}$ for $C_{S_{2m_1'm_2'}}$.*

Remark 2. *More generally, slightly optimizing parameters, relatively to iteratively applying Lemma 1 for two m_i's, for any $r \geq 2$, and $m_1, \ldots, m_r$ as above, we obtain a share conversion from $(2,k)$-CNF over $\mathbb{Z}_{2\prod_{i=1}^{r} m_i'}$ to $(1+\sum_{i=1}^{r} t_i, k)$-CNF over $\mathbb{Z}_2^{max(\beta_1,\ldots,\beta_r)}$ for the relations $C_{S_{2\prod_{i=1}^{r} m_i'}}$.*

Assume a conversion generalizing our result from Theorem A1 for 3 servers to more servers, while keeping the conversion to a scheme (t,k)-CNF for sufficiently small t. Such a scheme has enough redundancy to support multiplications over the resulting field $\mathbb{F}_{2^\beta}$ unlike (k,k)-additive, which has none (if needed, the field characteristic 2 may be replaced with some other prime, generalizing Theorem 1 instead). Then we can obtain PIR with linear server complexity $k = O(r)$, using Theorem 4, and applying Lemma 1 $r-1$ times. More precisely, we have:

Corollary 7. *Assume there exists a (global) constant t, such that for all sufficiently large k, the following holds. For infinitely many m_i's of the form $m_i = 2p_i$ where all p_i are odd distinct primes, there exists a share conversion from $(2,k)$-CNF to (t,k)-CNF over $\mathbb{Z}_2^{\beta_i}$ for the relation C_{m_i}. Then, for all sufficiently large r, there exists a $k = t(r-1)+1$-server PIR with communication complexity $2^{O(\log^{1/r}(n)\log\log^{1-1/r}(n))}$.*

1.6. Our Techniques

As described above, one of the main contributions of [13] was an instantiation of the framework for designing PIR protocols, which reduces the question of the existence of a three-server PIR protocol to the existence of a share conversion for certain parameters p_1, p_2, p, and certain linear sharing schemes over Abelian rings R, R' determined by the parameters.

BIKO provides the criteria of the share conversion existence in the case when $m = p_1p_2$ for distinct primes p_1 and p_2 and the set $S_m = \{s_1, s_2, 1\}$, where $s_1 \mod p_1 = 0$, $s_1 \mod p_2 = 1$, $s_2 \mod p_1 = 1$, $s_2 \mod p_2 = 0$. Namely, they prove that for such m and S_m, the share conversion from (2,3)-CNF over $\mathbb{Z}_m$ to 3-additive scheme over $\mathbb{Z}_p^\beta$ exists if and only if $rank(M_{\equiv,\not\equiv}) - rank(M_\equiv) = \beta > 0$, where the rank is computed over $\mathbb{F}_p$. The matrices $M_\equiv$ and $M_{\equiv,\not\equiv}$ are matrices over $\mathbb{Z}_p$ with $3m^2$ columns and $3m^2$ and $4m^2$ rows respectively which are constructed from some specific system of equations and inequalities. Beimel et al. in [13] did not provide the general solution for this system; however, they proved existence and nonexistence of the conversion for some special cases.

While the solvability of a system can be verified efficiently for a concrete instance, it does not provide a simple condition for characterizing triples (p_1, p_2, p) for which solutions exist. Moreover, the size of the matrix $M_{\equiv,\not\equiv}$ in this system is $4m^2 \times 3m^2$ which makes the numerical solution for big m's heavy in practice (though asymptotically efficient). Before [32], where the solvability of the system for the case odd primes p_1 and p_2, if one of them equals to p was proven, even the question of whether an infinite set of such triples exists remained open.

Our concrete goal in this work is to better understand the case of $m = p_1p_2$, motivated by understanding the technical foundations of the broader problem for m which is a product of $r > 2$ distinct primes (see Section 1.5 for details). We proceed using the BIKO characterization above. Concretely, for parameters $m = p_1p_2$ and p, this reduces to calculating the quantity $rank(M_{\equiv,\not\equiv}) - rank(M_\equiv) = \beta$, where the rank is computed over $\mathbb{Z}_p$.

In [32], the case $p_1 = p$ for odd p_1 and p_2 was explored. To simplify the technical task, the authors of [32] rely on the observation from [13] that $\beta > 0$ iff $M_\equiv$ does not span $v_{\not\equiv}$ for *any* row $v_{\not\equiv}$ of $M_{\not\equiv}$. Thus, they replace $M_{\not\equiv}$ with some $v_{\not\equiv}$ as above, and work with that (forgoing the goal of understanding the particular value of β). Then, they proceed by bringing the matrix $M_{\equiv,\not\equiv}$ to a more convenient form by performing a sequence of carefully tailored elimination steps on the rows of the matrix $M_{\equiv,\not\equiv}$. The sequence of eliminations is based on a observing a 3-leveled structure of the matrix of the matrix $M_{\equiv,\not\equiv}$,

and working on blocks of decreasing coarseness as the elimination process progresses. It also involves a change of basis at some point, to make the matrix's structure nicer for understanding. That is, rewriting the matrix so that the set of columns corresponds to a new basis—here we even manage to get fewer vectors in, as it suffices to include a set of vectors which is guaranteed to span $M_{\equiv,\not\equiv}$. However, the resulting matrix after that process remains too complex to check whether $\beta > 0$ for all parameters. The analysis up to that point (resulting in some matrix $A_{inter} = (A'_{inter}, v'_{\not\equiv})$ to analyze) is oblivious to the particular parameters except for not looking at even m (not because it was particularly hard, but rather out of a decision to limit the scope of the paper at what was already achieved). To obtain their partial result for some of the parameters, the authors then reduce the matrix's rows modulo a certain vector subspace (formally, multiplied it from the right by a certain square matrix L with non-trivial left kernel). Clearly, it holds that if $rank(A_{inter}L) - rank(A'L) > 0$, then $rank(A_{inter}) - rank(A') > 0$ as well (implying the existence of a share conversion), but not necessarily the other way around. The matrix $A_{inter}L$ turns out to be sufficiently simple to analyze, and for p which is either p_1 or p_2, the resulting rank difference is non-zero. However, we do not yet understand other parameters, for which $rank(A_{inter}) - rank(A') = 0$, or the case of even m. Also, due to the first simplification, the concrete value of β is not found, and thus the concrete answer complexity of the resulting PIR as implied by Theorem 8 remains unknown.

Our current paper considers the case where $p_1 = 2$. We proceed by a quite straightforward generalization of [32]'s elimination process up until producing the matrix A_{inter}, except that we do not make the simplification of keeping a single row out of $M_{\not\equiv}$, but rather keep the entire matrix. The main divergence from [32] is that we do not perform the reduction modulo a subspace, but are able to directly check whether $rank(A_{inter}) - rank(A') > 0$, and furthermore to compute the exact value of β. This is made possible, as the case where $p_1 = 2$ turns out to be particularly simple, and we managed to successfully analyze it directly (for all p_2, p). The other cases (when m is odd, and p is not equal to p_1 or p_2) remain open.

2. Preliminaries

2.1. Some Notation

Parameters of the secret sharing schemes. Throughout this paper, we fix the notation for p_1, p_2 and p being prime numbers such that $p_1 \neq p_2$, and $m = p_1 \cdot p_2$ are the parameters of the secret sharing schemes and conversion. Later, considering the corner case $p_1 = 2$ in Section 3.4, we introduce the odd prime number q to set $p_2 = q$.

Matrices and block-matrices. In this paper, we will consider matrices and block-matrices over a finite field $\mathbb{F} = \mathbb{Z}_p$. Those matrices are defined for 3 levels. The level-2 ("big") block-matrices we denote by letter A with correspondent indexes. The elements of level-2 matrices are level-1 block-matrices which we denote by the letter R with a lower index equal to the upper index of its "host" A. The level-0 "small" matrices are square matrices, initially having the size $m \times m$. For them, we use distinct letters.

For entry i, j of some matrix X, we use the standard notation of $X[i, j]$. Addressing the elements of level-2 and level-1 matrices, we address their blocks. Such, $A^1[i, j]$ denotes the block in the ith row and jth column of A^1. For level-0 matrices, we address the particular elements of this matrix. More generally, for a matrix $X \in \mathbb{F}^{u \times v}$, for the subsets $R \subseteq [v]$ of rows and $C \subseteq [u]$ of columns, $X[R, C]$ denotes the sub-matrix with rows (or block-rows) restricted to R and columns (or block-columns) restricted to C. Those rows and columns are ordered in the original order in X. As special cases, using a single index i instead of R (C) refers to a single row (column). A "$\cdot$" instead of R (C) stands for $[u]$ ($[v]$). Most of the time, index arithmetic will be done modulo the matrices' number of (block-)rows and columns (we will however state this explicitly).

When we consider the case $p_1 = 2$ in Section 3.4, the level-1 matrices R^i_j's are quite small and have only 2 level-0 blocks. Therefore, we omit the level-1 and address to level-0 blocks as to the entries of level-2 matrices $A^{(k),\ell}$.

Some concrete matrices and vectors. By the letter I, we denote the $m \times m$ identity matrix. If the identity matrix has a different size, we write this size down in the lower index. For instance, I_q is a $q \times q$ identity matrix. By $a^{b\times c}$ we denote a $b \times c$ matrix with all elements equal to a. In case when $a = 0$ and the size of this zero-block is clear from the context, we omit $b \times c$ and write 0 instead of $0^{b\times c}$. By a^b we denote the row of a's of the length b. For example, 1^m means the m-long string of 1's.

By $\mathbf{e}_i$ we denote the unity vector. The length of this vector is, as a rule, clear from the context, or it is specified in the accompanying text. The lower index specifies the position of 1 in this vector. In Section 2.5 and subsequently in Section 3.2, when we construct matrices in the basis $B = B_1 \cup B_2$, the unity vectors have double indexes $\mathbf{e}_{b,c}$. As explained in Section 2.5, there is the telescopic indexing system, and this double index points to the single position in the vector.

Concatenation and circular shifts over matrices. For matrices X, Y with the same number of columns, $(X;Y)$ denotes the matrix comprised by concatenating Y below X. For matrices X, Y with the same number of rows, we denote by $(X|Y)$ the matrix obtained by concatenating Y to the right of X.

In Section 3.4, we obtain the set of circularly shifted matrices. By $X^{<<k}$ we denote the matrix X with the circular left shift by k positions.

2.2. Secret Sharing Schemes

A *secret sharing scheme* is defined by pair of algorithms $Sh = (\mathsf{Share}, \mathsf{Dec})$. The randomized algorithm Share randomly splits a secret message $s \in S$ into an n-tuple of shares, $(s_1, \ldots, s_n)$. The deterministic algorithm Dec reconstructs s from some allowed (*qualified*) subset of the shares. The set of all the qualified sets is called an *access structure* of the secret-sharing scheme. We say that Sh is t-private, and has a threshold access structure if any t shares jointly reveal no information about the secret s.

We say that Sh is linear over some finite Abelian ring G if $S \subseteq G$ and each share s_i is obtained by applying a linear function over G to the vector $(s, r_1, \ldots, r_\ell) \in G^{\ell+1}$, where $r_1, \ldots, r_\ell$ are random and independent elements of G. A useful property of such schemes is that they allow evaluating locally linear functions of the shares such that additions and multiplications by the constant from G. In this work, we consider two types of linear secret sharing schemes:

- **Additive secret sharing:** the algorithm Share splits $s \in G$ into n random ring elements that add up to s; the algorithm Dec reconstructs s by adding up all the shares. This scheme is $(n-1)$-private. Within the limits of this work, we consider a 3-additive scheme, where $n = 3$.
- **CNF secret sharing:** the algorithm Share first splits $s \in G$ into $\binom{n}{t}$ additive shares s_T, each labeled by a distinct set $T \in \binom{[n]}{t}$, and then lets each share s_i be the subset of s_T apart from $i \in T$. For (2,3)-CNF we consider in this work, each of 3 parties obtains 2 additive shares out of 3, such that if additive shares of s are (a, b, c), then $s_1 = (b, c)$, $s_2 = (a, c)$, and $s_3 = (a, b)$. This scheme is 1-private, as any two parties can sum their shares up to calculate the secret s.

  See [33] for a survey on secret sharing.

2.3. Share Conversion

We recall the definition of (generalized) share conversion schemes as considered in our paper. Our definition is exactly the definition in [13], in turn, adopted from previous work.

Definition 1 ([13]). *Let Sh_1 and Sh_2 be two n-party secret-sharing schemes over the domains of secrets S_1 and S_2, respectively, and let $C \subseteq S_1 \times S_2$ be a relation such that, for every $a \in S_1$, there exists at least one $b \in S_2$ such that $(a, b) \in C$. A share conversion scheme* $\mathsf{convert}(s_1, \ldots, s_n)$ *from Sh_1 to Sh_2 with respect to relation C is specified by (deterministic) local conversion functions $g_1, \ldots, g_n$ such that: If $(s_1, \ldots s_n)$ is a valid sharing for some secret s in Sh_1, then $g_1(s_1), \ldots g_n(s_n)$ is a valid sharing for some secret s' in Sh_2 such that $(s, s') \in C$.*

For a pair of Abelian groups G_1, G_2 (When G_1, G_2 are rings, we consider G_1, G_2 as groups with respect to the "$+$" operation of the rings), we define the relation C_S as in [13].

Definition 2 (The relation C_S [13]). *Let G_1 and G_2 be finite Abelian groups, and let $S \subseteq G_1 \setminus \{0\}$. The relation C_S converts $s = 0 \in G_1$ to any nonzero $s' \in G_2$ and every $s \in S$ to $s' = 0$. There is no requirement when $s \notin S \cup 0$. Formally,*

$$C_S = \{(s,0)|s \in S\} \cup \{(0,s') : s' \in G_2 \setminus \{0\}\} \cup \{(s,s')|s \notin S \cup \{0\}, s' \in G_2\}$$

Given $m = p_1 \cdot p_2$, where $p_1 \neq p_2$ are primes and p is a prime, we consider pairs of rings $G_1 = \mathbb{Z}_m, G_2 = \mathbb{Z}_p^\beta$. We denote the set a relation C_{S_m} in this work is built with as $S_m = \{x \in G_1 | \forall i \in [2], x \mod p_i \in \{0,1\}\} \setminus \{0\}$. I.e., $S_m = \{(0,1)_{\mathbb{Z}_m}, (1,0)_{\mathbb{Z}_m}, (1,1)_{\mathbb{Z}_m}\}$, where $(a,b)_{\mathbb{Z}_m}$ means the element of $\mathbb{Z}_m$ which has the remainder a modulo p_1, and b modulo p_2. For $S = S_m$, we refer to S_m as the *canonical relation* for $\mathbb{Z}_m$.

2.4. The Characterization of BIKO.

In Beimel et al. [13], Sh_1 is a 3-additive secret sharing scheme over $\mathbb{Z}_m$, and Sh_2 is (2,3)-CNF sharing over $\mathbb{Z}_p^\beta$. The conversion with respect to relation C_{S_m} from Sh_1 to Sh_2 is considered. In [13], is proven that such a conversion exists iff a certain condition is satisfied by the matrix $M_{\equiv,\not\equiv}$ over $\mathbb{Z}_p$.

In matrix $M_{\equiv,\not\equiv}$, the rows are indexed by triples $(a,b,c) \in \mathbb{Z}_m^3$, corresponding to $(2,3)$-CNF sharings of some $s \in S_m \cup \{0\}$. The rows corresponding to $s \neq 0$ (i.e., to $s \in S_m$) form the upper part of the matrix, denoted by $M_\equiv$, and the rows corresponding to $s = 0$ form the lower part, denoted by $M_{\not\equiv}$. In this way, $M_{\equiv,\not\equiv} = (M_\equiv; M_{\not\equiv})$. The columns of $M_{\equiv,\not\equiv}$ are indexed by values in $[3] \times \mathbb{Z}_m \times \mathbb{Z}_m$. Intuitively, an index (i,x,y) of a column corresponds to share s_i (of ith server) of the $(2,3)$-CNF scheme being equal to (x,y). Rows are indexes by triples $(a,b,c) = (s-b-c,b,c)$. There are m possible values for a, b and c, and 4 possible values for s. For a given b and c, and for a given s there is only one possible value of $s-b-c$, hence we replace the first index by simply s, and the matrix has $4m^2$ rows. The row indexed by (s,b,c) has 1 in the column (i,x,y), if the 3-additive shares $(s-b-c,b,c)$ are agree with CNF-shares, and 0 otherwise. Thus, there are 1's in cells $[(s,b,c);(1,b,c)]$, $[(s,b,c);(2,s-b-c,c)]$ and $[(s,b,c);(3,s-b-c,b)]$, and 0's elsewhere in this row.

The work in [13] provided a quantitative lower bound on β, depending on the degree difference between $M_\equiv$ and $M_{\not\equiv}$.

Theorem 8 (Theorem 4.5 [13]). *Let $\beta = rank_{\mathbb{F}_p}(M_{\equiv,\not\equiv}) - rank_{\mathbb{F}_p}(M_\equiv)$. Then, we have:*

- *If $\beta = 0$, then there is no conversion from $(2,3)$-CNF sharing over $\mathbb{Z}_m$ to additive sharing over $\mathbb{Z}_p^\kappa$ with respect to C_{S_m}, for every $\kappa > 0$.*
- *If $\beta > 0$, then there is a conversion from $(2,3)$-CNF sharing over $\mathbb{Z}_m$ to additive sharing over $\mathbb{Z}_p^\beta$ with respect to C_{S_m}. Furthermore, in this case, every row v of $M_{\not\equiv}$ is not spanned by the rows of $M_\equiv$.*

Theorem 8 provides a full characterization via a condition that given (p_1, p_2, p) can be verified in polynomial time in $(p_1, p_2, \log(p))$. More precisely, the size of our matrix $M_{\equiv,\not\equiv}$ is $4m^2 \times 3m^2$, so verifying the condition amounts to solving a set of linear equations, which naïvely takes about $O(m^6)$ time, or slightly better using improved algorithms for matrix multiplication, and the running time cannot be better than $\tilde{\Omega}(m^4)$ using generic matrix multiplication algorithms. Thus, the complexity of verification grows very fast with m, becoming essentially infeasible for p_1, p_2 circa 50.

2.5. Our Starting Point—The Result of Paskin-Cherniavsky and Schmerler

The work [32] is made within BIKO's setting. Starting with the matrix $M_{\equiv,\not\equiv}$ they performed the sequence of elimination steps, according to the following lemma.

Lemma 2. *Let A denote a matrix in $\mathbb{Z}_p^{v\times u}$, and let $b = A[v,[u]]$. Let $I_1 \subseteq [v-1], I_2 \subseteq [u]$ denote non-empty sets of rows and columns, respectively. A' is obtained from A by a sequence of row operations on A, so that $A'[I_1,I_2]$ is a basis of $A'[[v],I_2]$, and the rest of the rows in $A'[I_1,I_2]$ are zero. Let $b' = A'[v,[u]]$. Then, $Rows(A'[[v]\setminus I_1,[u]\setminus I_2])$ span $b'[[u]\setminus I_2]$ iff $Rows(A[[v-1],[u]])$ span b.*

In fact, the result of [32] is the proof of the existence of the conversion for finite rings $G_1 = \mathbb{Z}_{p_1p_2}$ to $G_2 = \mathbb{Z}_{p_1}^{\beta}$ with distinct odd p_1 and p_2, for which it was enough to prove that the first row of $M_{\not\equiv}$ is not spanned by $M_{\equiv}$. Therefore, the matrix considered in [32] contained the full matrix $M_{\equiv}$ and the single row from $M_{\not\equiv}$. (As in our work we solve the problem for 2 sets of parameters proving both positive and negative results, we consider the full $M_{\equiv,\not\equiv}$ matrix.) After two elimination steps which cut the matrix $M_{\equiv}$ to $m+m^2$ rows, and the permutation of columns, they introduced a new basis $B = B_1 \cup B_2$, where

$$\begin{aligned} B_1 &= \{-\mathbf{e}_{b,i} + \mathbf{e}_{b,i+1} \mid b \in \mathbb{Z}_m,\ i \in \{0,\ldots,p_2-2\}\},\\ B_2 &= \left\{\mathbf{e}_{b,i+j\cdot(1,0)_{\mathbb{Z}_m}} - \mathbf{e}_{b,i+(j+1)\cdot(1,0)_{\mathbb{Z}_m}} \mid b \in \mathbb{Z}_m,\ i \in \mathbb{Z}_{p_2}, j \in \mathbb{Z}_{p_1}\setminus\{p_1-1\}\right\}, \end{aligned} \tag{1}$$

where $\mathbf{e}_{x,y}$ is a vector of length m^2 having 1 in the position indexed by (x,y) and 0's elsewhere. Indexes x and y are taken modulo m.

In this new basis, the matrix $M_{\equiv,\not\equiv}$ has the block structure and is separated into 3 "types" (layers): Type-1 and Type-2 layers compose $M_{\equiv}$, and Type-3 is $M_{\not\equiv}$ after several elimination steps and basis change. For the Type-1 matrix, the basic block is the m-component vector $(1,\ldots,1)$ and $p_1\times(p_1-1)$ block matrices R_1^2 and R_1^3 made from m-long vectors:

$$R_1^2 = \begin{array}{c|cccccc} & 0 & 1 & \cdots & p_1-3 & p_1-2\\ \hline 0 & & & & & \\ 1 & (1,\ldots,1) & & & & \\ 2 & (1,\ldots,1) & (1,\ldots,1) & & & \\ \vdots & (1,\ldots,1) & (1,\ldots,1) & \ddots & & \\ p_1-2 & (1,\ldots,1) & (1,\ldots,1) & \cdots & (1,\ldots,1) & \\ p_1-1 & (1,\ldots,1) & (1,\ldots,1) & \cdots & (1,\ldots,1) & (1,\ldots,1) \end{array}, \tag{2}$$

$$R_1^3 = \begin{array}{c|cccccccc} & 0 & \cdots & & (p_2-1) \mod p_1 & \cdots & p_1-2\\ \hline 0 & (1,\ldots,1) & \cdots & (1,\ldots,1) & (1,\ldots,1) & & \\ \vdots & \vdots & & \vdots & \vdots & \ddots & \\ -p_2 \mod p_1 & (1,\ldots,1) & \cdots & (1,\ldots,1) & (1,\ldots,1) & & (1,\ldots,1)\\ & & & & & & \\ & (1,\ldots,1) & & & & & \\ \vdots & \vdots & \ddots & & & & \\ p_1-1 & (1,\ldots,1) & \cdots & (1,\ldots,1) & & & \end{array}. \tag{3}$$

Basic $m\times m$ blocks of Type-2 are identity matrix I, and

$$T_2 = \begin{array}{c|cccccccc} & 0 & \cdots & (1,0)_{\mathbb{Z}_m}-2 & (1,0)_{\mathbb{Z}_m}-1 & (1,0)_{\mathbb{Z}_m} & \cdots & m-1\\ \hline 0 & 1 & \cdots & 1 & 1 & & & \\ & & 1 & \cdots & 1 & 1 & & \\ \vdots & & & \ddots & \ddots & \ddots & \ddots & \\ m-1 & 1 & \cdots & 1 & & & & 1 \end{array}. \tag{4}$$

Bigger blocks composed from them have the size $p_1 \times (p_1 - 1)$ "small" $m \times m$ blocks:

$$R_2^1 = \begin{array}{c|cccc} & 0 & 1 & \cdots & p_1-2 \\ \hline 0 & I & & & \\ 1 & & I & & \\ \vdots & & & \ddots & \\ p_1-2 & & & & I \\ p_1-1 & -I & -I & \cdots & -I \end{array}; \tag{5}$$

$$R_2^2 = \begin{array}{c|cccccc} & 0 & 1 & \cdots & p_1-3 & p_1-2 \\ \hline 0 & & & & & \\ 1 & T_2 & & & & \\ 2 & T_2 & T_2 & & & \\ \vdots & T_2 & T_2 & \ddots & & \\ p_1-2 & T_2 & T_2 & \cdots & T_2 & \\ p_1-1 & T_2 & T_2 & \cdots & T_2 & T_2 \end{array}; \tag{6}$$

$$R_2^3 = \begin{array}{c|cccccccc} & 0 & \cdots & & (p_2-1) \mod p_1 & p_2 \mod p_1 & \cdots & p_1-2 \\ \hline 0 & T_2 & \cdots & T_2 & T_2 & & & \\ 1 & T_2 & \cdots & T_2 & T_2 & T_2 & & \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \ddots & \\ -p_2 \mod p_1 & T_2 & \cdots & T_2 & T_2 & T_2 & & T_2 \\ & & & & & & & \\ & T_2 & & & & & & \\ \vdots & \vdots & \ddots & & & & & \\ p_1-1 & T_2 & \cdots & T_2 & & & & \end{array}; \tag{7}$$

$$R_2^4 = \begin{array}{c|cccc} & 0 & 1 & \cdots & p_1-2 \\ \hline 0 & I & & & \\ 1 & -I & I & & \\ \vdots & \vdots & & \ddots & \\ p_1-2 & -I & & & I \\ p_1-1 & -2I & -I & \cdots & -I \end{array}. \tag{8}$$

The matrix $M_{\equiv}$ is brought to the form $(A^1; A^2)$, where each of matrices A^1 and A^2 are block matrices having the left and right parts (In [32], the matrices we are talking about have the additional upper index (6), which is omitted here. Thus, $A^i = A^{(6),i} = (A^{(6),L,i}|A^{(6),R,i})$ for $i \in 1, 2$):

$$(A^1; A^2), \quad A^1 = (A^{L,1}|A^{R,1}), \quad A^2 = (A^{L,2}|A^{R,2}), \tag{9}$$

where

$$A^{L,1} = \begin{array}{c|c} 0 & L_1^0 \\ 1 & L_1^1 \\ \vdots & \vdots \\ p_2-2 & L_1^{p_2-2} \\ p_2-1 & 0 \end{array}, L_1^i = \begin{array}{c|ccccccc} & 0 & 1 & \cdots & i & \cdots & p_2-2 \\ \hline 0 & & & & (1,\ldots,1) & & \\ 1 & & & & & & \\ \vdots & & & & & & \\ p_1-2 & & & & & & \\ p_1-1 & & & & & & \end{array}$$

$$A^{R,1} = \begin{array}{c|cccccc} & 0 & 1 & 2 & \cdots & p_2-2 & p_2-1 \\ \hline 0 & R_1^2 & -R_1^2 & & & & \\ 1 & & R_1^2 & -R_1^2 & & & \\ \vdots & & & & \ddots & & \\ p_2-2 & & & & & R_1^2 & -R_1^2 \\ p_2-1 & R_1^2-R_1^3 & & & & & \end{array}, \tag{10}$$

$$A^{L,2} = \begin{array}{c|c} 0 & L_2^0 \\ 1 & L_2^1 \\ \vdots & \vdots \\ p_2-2 & L_2^{p_2-2} \\ p_2-1 & 0 \end{array}, \quad L_2^i = \begin{array}{c|cccccc} & 0 & 1 & \cdots & i & \cdots & p_2-2 \\ \hline 0 & & & & T_2 & & \\ 1 & & & & & & \\ \vdots & & & & & & \\ p_1-2 & & & & & & \\ p_1-1 & & & & & & \end{array},$$

$$A^{R,2} = \begin{array}{c|ccccccc} & 0 & 1 & 2 & \cdots & p_2-2 & p_2-1 \\ \hline 0 & R_2^4+R_2^2 & -R_2^2 & & & & \\ 1 & & R_2^4+R_2^2 & -R_2^2 & & & \\ \vdots & & & & \ddots & & \\ p_2-2 & & & & & R_2^4+R_2^2 & -R_2^2 \\ p_2-1 & R_2^1+R_2^2-R_2^3 & R_2^1 & \cdots & & R_2^1 & R_2^1 \end{array}. \tag{11}$$

We remark that the appearance of $A^{R,1}$ and $A^{R,2}$ are slightly different from those in the work of Paskin-Cherniavsky and Schmerler. The difference is in $p_2 - 1$'st block-row and comes from the computational mistake made in [32] while changing the basis to B. We correct this mistake and bring the corrigendum in Appendix A.

In [32], only the first row from the Type-3 layer was constructed. For our purposes of obtaining β, we need the full Type-3 matrix. Therefore, we write here down the general formula for Type-3 rows taken from [32], and we use it in our next work to construct the entire Type-3 matrix in the basis B:

$$\mathbf{e}_{(B,C)} - \mathbf{e}_{(B,C+(0,1)_{\mathbb{Z}_m})} - \sum_{k=0}^{(-1,0)_{\mathbb{Z}_m}} (\mathbf{e}_{B+k,C} - \mathbf{e}_{B+k,C+1}), \quad \text{where} \quad B,\ C \in \mathbb{Z}_m. \tag{12}$$

3. Our Result

3.1. Starting Point and Main Technical Tool

Our goal is to compute the difference between ranks of matrices $M_{\equiv}$ and $M_{\equiv,\not\equiv}$. We start from the matrix $M_{\equiv}$ brought to the form (9) and we also construct the result of initial elimination steps over the matrix $M_{\not\equiv}$ from (12), obtained in [32]. We continue the process of elimination using Lemma 2 considering the case $m = 2q$, where q is an odd prime number.

3.2. Construction of Type-3 matrix

First, as we need to compute the rank of the matrix $M_{\equiv,\not\equiv}$, it is not enough to consider only a single row from the Type-3 matrix (which is the result of the sequence of elimination steps over $M_{\not\equiv}$. Therefore, our first step is to reconstruct this matrix from (12) and to perform initial elimination steps similar to those were made over matrix A^2 in [32] to bring it to the form (11).

To be consistent, we denote the initial Type-3 matrix as $A^{(-1),3}$, the intermediate result of the inner elimination steps over this matrix as $A^{(0),3}$, and the final result (on the same stage as (9)) as A^3. Next we describe the process of obtaining Type-3 matrix from (12). Recall that each of matrices A is separated in the left and right parts, where the left part contains indexes of vectors from basis B_1, and right—from B_2. Each row of $A^{(-1),3}$ is indexed by

i, j, b such that the largest blocks are indexed by $i \in \mathbb{Z}_{p_2}$, and contains blocks indexes by $j \in \mathbb{Z}_{p_1}$. The smallest blocks indexed by $b \in \mathbb{Z}_m$ are, in turn, parts of middle-size blocks.

First, rewrite (12) as

$$\begin{aligned} \mathbf{e}_{(B,C)} - \mathbf{e}_{(B,C+(0,1)_{\mathbb{Z}_m})} - \mathbf{e}_{(B,C)} + \mathbf{e}_{(B,C+1)} - \sum_{k=1}^{(-1,0)_{\mathbb{Z}_m}} (\mathbf{e}_{B+k,C} - \mathbf{e}_{B+k,C+1}) = \\ = \mathbf{e}_{(B,C+1)} - \mathbf{e}_{(B,C+1-(1,0)_{\mathbb{Z}_m})} - \sum_{k=1}^{(-1,0)_{\mathbb{Z}_m}} (\mathbf{e}_{B+k,C} - \mathbf{e}_{B+k,C+1}). \end{aligned} \tag{13}$$

- Consider the case when $i \neq p_2 - 1$, $j \neq 0$. Each row indexed by (i, j, b) is determined by (13), where $B = b$, $C = i + j(1,0)_{\mathbb{Z}_m}$. Then the first two terms in (13) are

$$\mathbf{e}_{B,C+1} - \mathbf{e}_{B,C+1-(1,0)_{\mathbb{Z}_m}} = \mathbf{e}_{b,(i+1)+j(1,0)_{\mathbb{Z}_m}} - \mathbf{e}_{B,(i+1)+(j-1)(1,0)_{\mathbb{Z}_m}} = B_2[(i+1),(j-1),b]. \tag{14}$$

The term in the sum in (13) is

$$\begin{aligned} \mathbf{e}_{B+k,C} - \mathbf{e}_{B+k,C+1} = \mathbf{e}_{b+k,i} - \mathbf{e}_{b+k,i} + \mathbf{e}_{b+k,i+(1,0)_{\mathbb{Z}_m}} - \ldots + \mathbf{e}_{b+k,i+j(1,0)_{\mathbb{Z}_m}} - \\ - \mathbf{e}_{b+k,i+1} + \mathbf{e}_{b+k,i+1} - \mathbf{e}_{b+k,i+1+(1,0)_{\mathbb{Z}_m}} - \ldots - \mathbf{e}_{b+k,i+1+j(1,0)_{\mathbb{Z}_m}} = \\ = B_1[i,(b+k)] + \sum_{\ell=0}^{j-1} (B_2[i,\ell,b+k] - B_2[(i+1),\ell,b+k]). \end{aligned} \tag{15}$$

- When $j = 0$, $i \neq p_2 - 1$ the sum in (15) turns to 0. As for (14), the first two terms in (13) are:

$$\mathbf{e}_{B,C+1} - \mathbf{e}_{B,C+1-(1,0)_{\mathbb{Z}_m}} = \mathbf{e}_{b,i+1} - \mathbf{e}_{B,i-(1,0)_{\mathbb{Z}_m}} = -\sum_{\ell=0}^{p_1-2} B_2[(i+1),\ell,b]. \tag{16}$$

- When $j \neq 0$, $i = p_2 - 1$, the first two terms of (13) are the same as in (14). The only difference is the sum of terms:

$$\begin{aligned} \mathbf{e}_{B+k,C} - \mathbf{e}_{B+k,C+1} = \mathbf{e}_{b+k,(p_2-1)+j(1,0)_{\mathbb{Z}_m}} - \mathbf{e}_{b+k,p_2+j(1,0)_{\mathbb{Z}_m}} = \\ = -\mathbf{e}_{b+k,0} + \mathbf{e}_{b+k,p_2-1} - \sum_{\ell=0}^{p_2-1+j} (\mathbf{e}_{b+k,\ell(1,0)_{\mathbb{Z}_m}} - \mathbf{e}_{b+k,(\ell+1)(1,0)_{\mathbb{Z}_m}}) + \\ + \sum_{\ell=0}^{j-1} (\mathbf{e}_{b+k,(p_2-1)+\ell(1,0)_{\mathbb{Z}_m}} - \mathbf{e}_{b+k,(p_2-1)+(\ell+1)(1,0)_{\mathbb{Z}_m}}) = \\ = -\sum_{\ell=0}^{p_2-2} B_1[\ell,b+k] - \sum_{\ell=0}^{p_2-1+j} B_2[0,\ell,b+k] + \sum_{\ell=0}^{j-1} B_2[(p_2-1),\ell,b+k]. \end{aligned} \tag{17}$$

- Finally, for $i = p_2 - 1$, $j = 0$, the first two terms in (13) are according (16), and the terms in sum are as in (17), except from the term $\sum_{\ell=0}^{j-1} B_2[(p_2-1),\ell,b+k]$, i.e.,

$$-\sum_{\ell=0}^{p_2-2} B_1[\ell,b+k] - \sum_{\ell=0}^{p_2-1+j} B_2[0,\ell,b+k]. \tag{18}$$

Substituting expressions (14)–(18) to (13) for appropriate i, j, b, we obtain the matrix which has the structure similar to A^2:

$$A^{(-1),3} = \left(A^{(-1),L,3} | A^{(-1),R,3} \right), \tag{19}$$

where

$$A^{(-1),L,3} = \begin{array}{c|c} 0 & L_3^{(-1),0} \\ 1 & L_3^{(-1),1} \\ \vdots & \vdots \\ p_2-2 & L_3^{(-1),p_2-2} \\ p_2-1 & -\sum_{i=0}^{p_2-2} L_3^{(-1),i} \end{array}, \quad L_3^{(-1),i} = \begin{array}{c|cccccc} & 0 & 1 & \cdots & i & \cdots & p_2-2 \\ 0 & & & & T_3 & & \\ 1 & & & & T_3 & & \\ \vdots & & & & & & \\ p_1-2 & & & & T_3 & & \\ p_1-1 & & & & T_3 & & \end{array},$$

$$A^{(-1),R,3} = \begin{array}{c|cccccc} & 0 & 1 & 2 & \cdots & p_2-2 & p_2-1 \\ 0 & R_3^2 & R_3^1-R_3^2 & & & & \\ 1 & & R_3^2 & R_3^1-R_3^2 & & & \\ \vdots & & & & \ddots & & \\ p_2-2 & & & & & R_3^2 & R_3^1-R_3^2 \\ p_2-1 & R_3^4-R_3^3 & & & & & R_3^2 \end{array}.$$

Here block matrices R_3^2 and R_3^3 are of the same form as R_2^2 (6) and R_2^3 (7) respectively, where the blocks T_2 are replaced with the blocks T_3:

$$T_3 = \begin{array}{c|cccccccccc} & 0 & 1 & 2 & \cdots & (0,1)_{\mathbb{Z}_m}-2 & (0,1)_{\mathbb{Z}_m}-1 & (0,1)_{\mathbb{Z}_m} & \cdots & m-1 \\ 0 & & 1 & 1 & \cdots & 1 & 1 & & & \\ & & & 1 & \cdots & 1 & 1 & 1 & & \\ \vdots & & & & \ddots & \ddots & \ddots & \ddots & & \\ m-1 & 1 & 1 & 1 & \cdots & 1 & & & & \end{array}. \tag{20}$$

The matrix R_3^1 is similar to R_2^1, but with the opposite sign, and permuted rows:

$$R_3^1 = \begin{array}{c|cccc} & 0 & 1 & \cdots & p_1-2 \\ 0 & I & I & \cdots & I \\ 1 & -I & & & \\ 2 & & -I & & \\ \vdots & & & \ddots & \\ p_1-1 & & & & -I \end{array}. \tag{21}$$

The matrix R_3^4 can be obtained from R_3^1 with the circular permutation of rows:

$$R_3^4 = \begin{array}{c|cccccccc} & 0 & \cdots & & (p_2-1) \mod p_1 & p_2 \mod p_1 & \cdots & p_1-2 \\ 0 & & & & -I & & & \\ 1 & & & & & -I & & \\ \vdots & & & & & & \ddots & \\ -p_2 \mod p_1 & & & & & & & -I \\ & I & \cdots & I & I & I & \cdots & I \\ & -I & & & & & & \\ \vdots & & \ddots & & & & & \\ p_1-1 & & & -I & & & & \end{array}. \tag{22}$$

3.3. Elimination Steps in Type-3 Matrix

Following the way in [32] for elimination steps in A^2, we first sum the block-rows in (19) with ordinal numbers from 0 to p_1-2 to the last block-row. The resulting matrix $A^{(0),3}$ equals $A^{(-1),3}$ except the last row, where $A^{(0),L,3}[p_2-1,\cdot]$ is 0-block, and

$$A^{(0),R,3}[p_2-1,\cdot] = \begin{pmatrix} R_3^2+R_3^4-R_3^3 & | & R_3^1 & | & \ldots & | & R_3^1 \end{pmatrix}.$$

The second elimination step is an inner step in every block-row except from the last one (as those block-rows are the same in $A^{(-1),3}$ and $A^{(0),3}$, we can say that this step is performed over (19)). Namely, in any level-2 block-row $A^{(0),3}[i,\cdot]$ where $i \in \{0,...,p_1-2\}$, we subtract the level-1 block-row with the ordinal number 0 from all other sub-rows in this block-row. As a result, $A^3 = \left(A^{L,3}|A^{R,3}\right)$, where the left-side matrix takes the form

$$A^{L,3} = \begin{array}{|c|c|}\hline 0 & L_3^0 \\ \hline 1 & L_3^1 \\ \hline \vdots & \vdots \\ \hline p_2-2 & L_3^{p_2-2} \\ \hline p_2-1 & 0 \\ \hline \end{array}, \quad L_3^i = \begin{array}{|c|c|c|c|c|c|c|}\hline & 0 & 1 & \cdots & i & \cdots & p_2-2 \\ \hline 0 & & & & T_3 & & \\ \hline 1 & & & & & & \\ \hline \vdots & & & & & & \\ \hline p_1-2 & & & & & & \\ \hline p_1-1 & & & & & & \\ \hline \end{array}, \tag{23}$$

and the right-side matrix is

$$A^{R,3} = \begin{array}{|c|c|c|c|c|c|c|}\hline & 0 & 1 & 2 & \cdots & p_2-2 & p_2-1 \\ \hline 0 & R_3^2 & R_3^5-R_3^2 & & & & \\ \hline 1 & & R_3^2 & R_3^5-R_3^2 & & & \\ \hline \vdots & & & & \ddots & & \\ \hline p_2-2 & & & & & R_3^2 & R_3^5-R_3^2 \\ \hline p_2-1 & R_3^2+R_3^4-R_3^3 & R_3^1 & \cdots & R_3^1 & R_3^1 & R_3^1 \\ \hline \end{array}, \tag{24}$$

where

$$R_3^5 = \begin{array}{|c|c|c|c|c|}\hline & 0 & 1 & \cdots & p_1-2 \\ \hline 0 & I & I & \cdots & I \\ \hline 1 & -2I & -I & \cdots & -I \\ \hline 2 & -I & -2I & \cdots & -I \\ \hline \vdots & \vdots & \vdots & \ddots & \vdots \\ \hline p_1-1 & -I & -I & \cdots & -2I \\ \hline \end{array}. \tag{25}$$

3.4. The Case of the Even m ($p_1 = 2$, $p_2 = q$)

In this section, we consider the case $p_1 = 2$, $p_2 > 2$ for both $p = 2$ and $p > 2$ (including the case $p_2 = p$). We obtain the feasibility results and, moreover, in the case of $p = 2$ when the conversion from (2,3)-CNF over $\mathbb{Z}_{2p_2}$ to three-additive secret sharing over $\mathbb{Z}_2^\beta$ (as we prove) exists, we also compute β. We adopt the following *notation* in this section: $p_2 = q > 2$, and p are prime numbers, and $m = 2q$ (later we split this case into subcases $p = 2$ and $p > 2$). Our starting point is the block matrix $A = \left(A^2; A^1; A^3\right)$ over $\mathbb{Z}_p$, where A^1 and A^2 are described in (9), and A^3 in (23) and (24).

We next consider the matrices in the case when $m = 2q$, where q is an odd prime number. Below we write down the block matrices completing the matrix A. Each of the following matrices contains two square $m \times m$ blocks:

$$\begin{gathered} R_2^1 = R_3^1 = R_3^4 = \begin{pmatrix} I \\ -I \end{pmatrix}; \quad R_2^4 = R_3^5 = \begin{pmatrix} I \\ -2I \end{pmatrix}; \\ R_2^2 = \begin{pmatrix} 0 \\ T_2 \end{pmatrix}; \quad R_2^3 = \begin{pmatrix} T_2 \\ 0 \end{pmatrix}; \quad R_3^2 = \begin{pmatrix} 0 \\ T_3 \end{pmatrix}; \quad R_3^3 = \begin{pmatrix} T_3 \\ 0 \end{pmatrix}. \end{gathered} \tag{26}$$

We would like to remind that $1^m = (1,...,1)$ is an m-element vector of 1's, also 1^q is the q-element vector of 1's. I is a $m \times m$ identity matrix, and I_q is a $q \times q$ identity matrix.

Taking into account (26), the block matrix $A = \left(A^2; A^1; A^3\right)$ according to (9), (23) and (24) is the following:

$$A^2 = \left(\begin{array}{cccc||cccccc} T_2 & & & & I & & & & & \\ & & & & T_2-2I & -T_2 & & & & \\ & T_2 & & & & I & & & & \\ & & & & & T_2-2I & -T_2 & & & \\ & & \ddots & & & & & \ddots & & \\ & & & T_2 & & & & & I & \\ & & & & & & & & T_2-2I & -T_2 \\ & & & & I-T_2 & I & I & \cdots & I & I \\ & & & & T_2-I & -I & -I & \cdots & -I & -I \end{array}\right) \tag{27}$$

$$A^1 = \left(\begin{array}{cccc||cccccc} 1^m & & & & & & & & & \\ & & & & 1^m & -1^m & & & & \\ & 1^m & & & & & & & & \\ & & & & & 1^m & -1^m & & & \\ & & \ddots & & & & & \ddots & & \\ & & & 1^m & & & & & & \\ & & & & & & & & 1^m & -1^m \\ & & & & -1^m & & & & & \\ & & & & & & & & & 1^m \end{array}\right) \tag{28}$$

$$A^3 = \left(\begin{array}{cccc||cccccc} T_3 & & & & & I & & & & \\ & & & & T_3 & -(T_3+2I) & & & & \\ & T_3 & & & & & I & & & \\ & & & & & T_3 & -(T_3+2I) & & & \\ & & \ddots & & & & & \ddots & & \\ & & & T_3 & & & & & I & \\ & & & & & & & & T_3 & -(T_3+2I) \\ & & & & -(T_3+I) & I & I & \cdots & I & I \\ & & & & T_3+I & -I & -I & \cdots & -I & -I \end{array}\right) \tag{29}$$

The left-side and the right-side matrices are divided by the double vertical line. All the subsequent matrices which we will obtain from A will have the additional upper indexes: $A^{(i)} = \left(A^{(i),2}; A^{(i),1}; A^{(i),3}\right)$, where i is the ordinal number of the matrix in the sequence of transformation steps. Within the limits of this section, we consider matrices $A^{(\cdot),\ell}$ as if they have level-0 blocks as the entries, and we, therefore, address to level-0 blocks as to the entries of level-2 matrices $A^{(\cdot),\ell}$.

First of all, we subtract A^2 from A^3 and rewrite all the matrices such that first go all the block-rows for $i < p_2 - 1$, $j = 0$, and then the block-rows for $i < p_2 - 1$, $j = 1$ and two last block-rows remain where they were before.

Matrices T_2 and T_3 depend on values $(0,1)_{\mathbb{Z}_m} = q+1$ and $(1,0)_{\mathbb{Z}_m} = q$. We introduce the new block $T = T_3 - T_2$ and note that with respect to (26),

$$T = T_3 - T_2 = \left(\begin{array}{c|c} -I_q & I_q \\ \hline I_q & -I_q \end{array}\right), \qquad T + 2I = \left(\begin{array}{c|c} I_q & I_q \\ \hline I_q & I_q \end{array}\right). \tag{30}$$

$$A^{(1),2} = \left(\begin{array}{c|c|c|c||c|c|c|c|c|c} T_2 & & & & I & & & & & \\ \hline & T_2 & & & & I & & & & \\ \hline & & \ddots & & & & & \ddots & & \\ \hline & & & T_2 & & & & & I & \\ \hline & & & & T_2-2I & -T_2 & & & & \\ \hline & & & & & T_2-2I & -T_2 & & & \\ \hline & & & & & & \ddots & \ddots & & \\ \hline & & & & & & & & T_2-2I & -T_2 \\ \hline & & & & I-T_2 & I & I & \cdots & I & I \\ \hline & & & & T_2-I & -I & -I & \cdots & -I & -I \end{array}\right) \tag{31}$$

$$A^{(1),1} = \left(\begin{array}{c|c|c|c||c|c|c|c|c|c} 1^m & & & & & & & & & \\ \hline & 1^m & & & & & & & & \\ \hline & & \ddots & & & & & & & \\ \hline & & & 1^m & & & & & & \\ \hline & & & & 1^m & -1^m & & & & \\ \hline & & & & & 1^m & -1^m & & & \\ \hline & & & & & & \ddots & \ddots & & \\ \hline & & & & & & & & 1^m & -1^m \\ \hline & & & & -1^m & & & & & \\ \hline & & & & & & & & & 1^m \end{array}\right) \tag{32}$$

$$A^{(1),3} = \left(\begin{array}{c|c|c|c||c|c|c|c|c|c} T & & & & -I & I & & & & \\ \hline & T & & & & -I & I & & & \\ \hline & & \ddots & & & & & \ddots & & \\ \hline & & & T & & & & & -I & I \\ \hline & & & & T+2I & -(T+2I) & & & & \\ \hline & & & & & T+2I & -(T+2I) & & & \\ \hline & & & & & & \ddots & \ddots & & \\ \hline & & & & & & & & T+2I & -(T+2I) \\ \hline & & & & -(T+2I) & & & & & \\ \hline & & & & T+2I & & & & & \end{array}\right) \tag{33}$$

We note that the last block-row in $A^{(1),2}$ is the same as the previous one up to sign. The same observation we can make about $A^{(1),3}$.

3.4.1. Internal Transformations in Matrices on the Level-2

We made some quite obvious steps inside each of the matrices $A^{(1),\cdot}$ to reach a more comfortable form. In $A^{(1),2}$ we eliminate the last block-row. In addition, we add all the block-rows from $A^{(1),2}[i]$ for $i \in \{q-1, ..., 2q-3\}$ to block-row $A^{(1),2}[2q-2]$ and change the sign of this row. The resulting matrix is

$$A^{(2),2} = \left(\begin{array}{c|c|c|c||c|c|c|c|c|c} T_2 & & & & I & & & & & \\ \hline & T_2 & & & & I & & & & \\ \hline & & \ddots & & & & & \ddots & & \\ \hline & & & T_2 & & & & & I & \\ \hline & & & & T_2-2I & -T_2 & & & & \\ \hline & & & & & T_2-2I & -T_2 & & & \\ \hline & & & & & & \ddots & \ddots & & \\ \hline & & & & & & & & T_2-2I & -T_2 \\ \hline & & & & I & I & I & \cdots & I & T_2-I \end{array}\right) \tag{34}$$

In $A^{(1),1}$, we change the sign of the pre-last row, move it to the position $p_2 - 1 = q - 1$ and make telescopic elimination by the following sequence of steps: starting with the row $i = q$, we subtract the previous row from ith, then change the sign of the ith row. Then we increment i by 1. We repeat this algorithm up to the last row of this matrix. Note, that the last row turns to 0, so we eliminate it from the matrix. The result is the matrix with $(2q - 1)$ rows:

$$A^{(2),1} = \left(\begin{array}{c|c|c|c||c|c|c|c|c} 1^m & & & & & & & & \\ \hline & 1^m & & & & & & & \\ \hline & & \ddots & & & & & & \\ \hline & & & 1^m & & & & & \\ \hline & & & & 1^m & & & & \\ \hline & & & & & 1^m & & & \\ \hline & & & & & & \ddots & & \\ \hline & & & & & & & 1^m & \\ \hline & & & & & & & & 1^m \end{array}\right) \tag{35}$$

The same transformation we perform in $A^{(2),3}$, working with block-rows instead of rows. The result is the following matrix with $(2q - 1)$ block-rows:

$$A^{(2),3} = \left(\begin{array}{c|c|c|c||c|c|c|c|c} T & & & & -I & I & & & \\ \hline & T & & & & -I & I & & \\ \hline & & \ddots & & & & \ddots & & \\ \hline & & & T & & & & -I & I \\ \hline & & & & T+2I & & & & \\ \hline & & & & & T+2I & & & \\ \hline & & & & & & \ddots & & \\ \hline & & & & & & & T+2I & \\ \hline & & & & & & & & T+2I \end{array}\right) \tag{36}$$

3.4.2. Resolution of the Level-0 Blocks in $A^{(2),3}$

Consider the block-rows of the appearance $\left(\begin{array}{c|c|c} \cdots & T+2I & \cdots \end{array}\right)$ in (36). According (30), it equals to the matrix $\left(\begin{array}{c|c|c} \cdots & (I_q|I_q) & \cdots \\ \cdots & (I_q|I_q) & \cdots \end{array}\right)$, where first q rows are the same as q last ones, and those q rows can be eliminated from the matrix. According to our notation, the $q \times m$-block equal to the concatenation of two I_q's is denoted as $(I_q|I_q)$. The rows we just considered belong to the local basis of $A^{(2),3}$.

Then we consider the block-rows $\left(\begin{array}{c|c|c|c|c} \cdots & T & \cdots & -I & I & \cdots \end{array}\right)$ in (36). Subtracting from this block-row the basis vectors from two corresponding block-rows $\left(\begin{array}{c|c|c} \cdots & (I_q|I_q) & \cdots \end{array}\right)$ and taking into account (30), we transform it to:

$$\left(\begin{array}{c|c|c|c|c|c} \cdots & (-I_q| \quad I_q) & \cdots & (0| \quad I_q) & (0|-I_q) & \cdots \\ \cdots & (\quad I_q|-I_q) & \cdots & (0|-I_q) & (0| \quad I_q) & \cdots \end{array}\right).$$

Again, the first q rows in this block-row can be crossed out from the matrix, as they are the same as q following ones up to the sign. Then the resulting matrix contains only $q(2q - 1)$ rows of the local basis:

$$A^{(3),3} = \left(\begin{array}{c|c|c|c||c|c|c|c|c} (I_q|-I_q) & & & & (0|-I_q) & (0|I_q) & & & \\ \hline & (I_q|-I_q) & & & & (0|-I_q) & (0|I_q) & & \\ \hline & & \ddots & & & & \ddots & \ddots & \\ \hline & & & (I_q|-I_q) & & & & (0|-I_q) & (0|I_q) \\ \hline & & & & (I_q|I_q) & & & & \\ \hline & & & & & (I_q|I_q) & & & \\ \hline & & & & & & \ddots & & \\ \hline & & & & & & & (I_q|I_q) & \\ \hline & & & & & & & & (I_q|I_q) \end{array}\right) \tag{37}$$

3.4.3. Resolution of the Level-0 Blocks in $(A^{(2),2}; A^{(2),1})$

First, we consider block-rows of appearance $(\ \cdots \mid T_2 \mid \cdots \mid I \mid \cdots\ )$ in $A^{(2),2}$ (Equation (34)). For each $j > q$, $T_2[j] = T_2[0] + T_2[q] - T[j-q]$, hence we can bring all the $T_2[j]$ to 0 by the inner linear operations of rows in the block-row, which result in the following appearance of the block-row under the consideration:

$$\left(\begin{array}{c|c|c|c|c} \cdots & T'_2 & \cdots & (I_{q+1}|0) & \cdots \\ \hline \cdots & 0 & \cdots & (J|J) & \cdots \end{array}\right), \tag{38}$$

where $T'_2 = T_2[\{0,...,q\},\cdot]$, and J is a $(q-1)\times q$-size matrix:

$$J = \left(\begin{array}{c|c|c|c|c} -1 & 1 & 0 & \cdots & 0 \\ \hline -1 & 0 & 1 & \cdots & 0 \\ \hline \vdots & & & \ddots & \\ \hline -1 & 0 & 0 & \cdots & 1 \end{array}\right). \tag{39}$$

The set of all the upper block-rows as in (38) is in the echelon form and belongs to the basis of our matrix. Now, we pay attention to $q-1$ first rows in $A^{(2),1}$ (Equation (35)), taking into account that $1^m = T'_2[0] + T'_2[q]$. Subtracting the correspondent rows of $A^{(2),2}$ from $A^{(2),1}$, we bring the rows of the appearance $A^{(2),1}[i,\cdot] = (\ \cdots \mid 1^m \mid \cdots \parallel \cdots\ )$ to the form $(\ 0 \parallel \cdots \mid (-\mathbf{e}_0|-\mathbf{e}_0) \mid \cdots\ )$. Considering this resulting row together with the second block-row from (38), we can see that those are easily transformable to the form $(\ 0 \parallel \cdots \mid (I_q|I_q) \mid \cdots\ )$. As block-rows of the appearance $(\ 0 \parallel \cdots \mid (I_q|I_q) \mid \cdots\ )$ are composed from transformed rows of both matrices $A^{(2),2}$ and $A^{(2),1}$, we denote this merged matrix of $q-1$ block-rows as $A^{(3),1\&2}_{q-1}$:

$$A^{(3),1\&2}_{q-1} = \left(\begin{array}{c|c|c|c||c|c|c|c|c} & & & & (I_q|I_q) & & & & \\ \hline & & & & & (I_q|I_q) & & & \\ \hline & & & & & & \ddots & & \\ \hline & & & & & & & (I_q|I_q) & \end{array}\right). \tag{40}$$

This matrix is in the left echelon form and thus consisted from the basis vectors of $M_{\equiv,\not\equiv}$.

In addition, we consider the last block-row of $A^{(2),2}$, namely, $(\ 0 \parallel I \mid I \mid \cdots \mid I \mid T_2 - I\ )$ and subtract from there all the correspondent basis vectors of (40). Each block I then turns to $\left(\begin{array}{c|c} 0 & -I_q \\ \hline 0 & I_q \end{array}\right)$. Adding the upper half of the resulting block-row to the lower (and changing the sign of the upper one), we get $\left(\begin{array}{c\|c|c|c|c|c} 0 & (0|I_q) & (0|I_q) & \cdots & (0|I_q) & (I-T_2)[\{0,...,q-1\},\cdot] \\ \hline 0 & 0 & 0 & \cdots & 0 & (1^{q\times q} - I_q | 1^{q\times q} - I_q) \end{array}\right)$. We subtract the last row of $A^{(2),1}$ from each of last q rows of this block-row. Then these last q rows come to the form $(\ 0 \parallel \cdots \mid (I_q|I_q)\ )$, and we append them to (40) to complete the matrix $A^{(3),1\&2}$. Then, subtracting the appropriate rows of the block $(I_q|I_q)$ from

the block $(I - T_2)[0, ..., q-1]$, we transform it to the form $(0^{q\times q}|I_q - N)$, where N is a q-dimension matrix

$$N = \left(\begin{array}{c|c|c|c|c|c} 1 & -1 & -1 & \cdots & -1 & -1 \\ \hline 1 & 1 & -1 & \cdots & -1 & -1 \\ \hline 1 & 1 & 1 & \cdots & -1 & -1 \\ \hline \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \hline 1 & 1 & 1 & \cdots & 1 & 1 \end{array}\right). \tag{41}$$

Finally, we consider the block-rows in $A^{(2),2}$ in (34) of the appearance $\left(\begin{array}{c||c|c|c} 0 & \cdots & T_2 - 2I & -T_2 \end{array}\cdots\right)$. Let us consider the result of the elimination the basis $(I_q|I_q)$ from the block

$$T_2 - 2I = \left(\begin{array}{c|c|c|c|c|c|c|c|c|c} -1 & 1 & 1 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 \\ \hline 0 & -1 & 1 & \cdots & 1 & 1 & 0 & 0 & \cdots & 0 \\ \hline & & \ddots & \ddots & \ddots & \ddots & \ddots & & & \\ \hline 0 & 0 & 0 & \cdots & -1 & 1 & 1 & 1 & \cdots & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 & -1 & 1 & 1 & \cdots & 1 \\ \hline 1 & 0 & 0 & \cdots & 0 & 0 & -1 & 1 & \cdots & 1 \\ \hline \ddots & \ddots & & & & & & \ddots & \ddots & \ddots \\ \hline 1 & 1 & 1 & \cdots & 0 & 0 & 0 & 0 & \cdots & -1 \end{array}\right). \tag{42}$$

The result of the elimination is $\left(\begin{array}{c|c} 0 & N \\ \hline 0 & -N \end{array}\right)$. For the block $-T_2$, the result of the elimination is $\left(\begin{array}{c|c} 0 & 2I_q - N \\ \hline 0 & N - 2I_q \end{array}\right)$. Thus, each block-row under the consideration turns to the following q-row block-row $\left(\begin{array}{c||c|c|c} 0 & \cdots & (0|N) & (0|2I_q - N) \end{array}\cdots\right)$.

Thus, the result of all the transformations over $\left(A^{(2),2}; A^{(2),1}\right)$ above is $\left(A^{(3),2}; A^{(3),1\&2}\right)$, where

$$A^{(3),2} = \left(\begin{array}{c|c|c|c||c|c|c|c|c|c} T_2' & & & & (I_{q+1}|0) & & & & & \\ \hline & T_2' & & & & (I_{q+1}|0) & & & & \\ \hline & & \ddots & & & & & \ddots & & \\ \hline & & & T_2' & & & & & (I_{q+1}|0) & \\ \hline & & & & (0|N) & (0|2I_q - N) & & & & \\ \hline & & & & & (0|N) & (0|2I_q - N) & & & \\ \hline & & & & & & \ddots & \ddots & & \\ \hline & & & & & & & & (0|N) & (0|2I_q - N) \\ \hline & & & & (0|I_q) & (0|I_q) & (0|I_q) & \cdots & (0|I_q) & (0|I_q - N) \end{array}\right)$$

$$A^{(3),1\&2} = \left(\begin{array}{c|c|c|c||c|c|c|c} & & & & (I_q|I_q) & & & \\ \hline & & & & & (I_q|I_q) & & \\ \hline & & & & & & \ddots & \\ \hline & & & & & & & (I_q|I_q) \end{array}\right). \tag{43}$$

We note, that all the rows of $A^{(2),1}$ in (35) of the appearance $\left(\begin{array}{c||c|c|c} 0 & \cdots & 1^m & \cdots \end{array}\right)$ are spanned by $A^{(3),1\&2}$ as the row's sums over the correspondent block-row.

3.4.4. Resolution of the $A^{(3),1\&2}$ Basis

To apply Lemma 2, it is necessary to subtract vectors of basis $A^{(3),1\&2}$ from the first $(q-1)$ block-rows of $A^{(3),2}$. The matrix $A^{(3),3}$ contains exactly the same block-rows as $A^{(3),1\&2}$ which can be simply crossed out.

Subtracting block $(I_q|I_q)$ from block $(I_{q+1}|0)$, we obtain the latest in form $\left(\begin{array}{c|c} 0 & -I_q \\ \hline 0 & \mathbf{e}_0 \end{array}\right)$. We denote the $(q+1)\times q$ block $\left(\begin{array}{c} -I_q \\ \hline \mathbf{e}_0 \end{array}\right)$ as $(-I'_{q+1})$. Then, after applying Lemma 2 to remove the basis $A^{(3),1\&2}$ and corresponding columns, we obtain the matrix

$$A^{(4)} = \left(A^{(4),2}; A^{(4),3}\right),$$

where

$$A^{(4),2} = \left(\begin{array}{cccc||cccccc} T'_2 & & & & -I'_{q+1} & & & & & \\ & T'_2 & & & & -I'_{q+1} & & & & \\ & & \ddots & & & & & \ddots & & \\ & & & T'_2 & & & & & -I'_{q+1} & \\ & & & & N & 2I_q - N & & & & \\ & & & & & N & 2I_q - N & & & \\ & & & & & & \ddots & \ddots & & \\ & & & & & & & & N & 2I_q - N \\ & & & & I_q & I_q & I_q & \cdots & I_q & I_q - N \end{array}\right) \tag{44}$$

$$A^{(4),3} = \left(\begin{array}{cccc||ccccc} (I_q| - I_q) & & & & -I_q & I_q & & & \\ & (I_q| - I_q) & & & & -I_q & I_q & & \\ & & \ddots & & & & \ddots & & \\ & & & (I_q| - I_q) & & & & -I_q & I_q \end{array}\right)$$

3.4.5. Elimination of the Left-Side Matrices

We note that each row in block $(I_q| - I_q)$ is spanned by the rows of T'_2, namely, $(I_q| - I_q)[j] = T'_2[j] - T'_2[j+1]$ $(j \in \{0, ..., q-1\})$. Subtracting the correspondent rows of $A^{(4),2}$ from $A^{(4),3}$, and applying Lemma 2, we obtain

$$A^{(5),2} = \left(\begin{array}{cccccc} N & 2I_q - N & & & & \\ & N & 2I_q - N & & & \\ & & \ddots & \ddots & & \\ & & & & N & 2I_q - N \\ I_q & I_q & I_q & \cdots & I_q & I_q - N \end{array}\right)$$

$$A^{(5),3} = \left(\begin{array}{ccccc} -I'_q & I_q & & & \\ & -I'_q & I_q & & \\ & & \ddots & & \\ & & & -I'_q & I_q \end{array}\right), \text{ where } I'_q = \left(\begin{array}{ccccc} & 1 & & \cdots & \\ & & 1 & \cdots & \\ & & & \ddots & \\ & & & \cdots & 1 \\ -1 & & & \cdots & \end{array}\right). \tag{45}$$

Here, the left side is crossed out, and matrix $A^{(5)} = \left(A^{(5),2}; A^{(5),3}\right)$ is the matrix of $q \times q$ level-0 blocks.

3.4.6. Resolution of N and $2I_q - N$ Blocks

Up to this moment, we performed transformations in matrices without connection to any particular modulus. Considering blocks N and $2I_q - N$ in $A^{(5),2}$ (Equation (45)), we can see two different situations taking into account the prime modulus $p = 2$ or $p > 2$:

- In the case of $p > 2$, each N defined in (41) can be transformed to I_q by the linear transformation steps such as additions of rows, multiplications by (-1) and 2^{-1} (which exists due to the fact that p is odd). Applying the same transformations to the adjacent block $2I_q - N$, we turn it into $-I_q^*$, where

$$I_q^* = \left(\begin{array}{c|c|c|c|c} & & \cdots & & -1 \\ \hline 1 & & \cdots & & \\ \hline & 1 & \cdots & & \\ \hline & & \ddots & & \\ \hline & & \cdots & 1 & \end{array}\right). \tag{46}$$

- In the case of $p = 2$, each block-row of the appearance $\left(\begin{array}{c|c|c|c} \cdots & N & 2I_q - N & \cdots \end{array}\right)$ in (45) contains q equal rows $\left(\begin{array}{c|c|c|c} \cdots & 1^q & 1^q & \cdots \end{array}\right)$.
  According to the dichotomy above, we next consider two cases.

3.4.7. Case $p_1 = 2$, $p_2 = q$, $p > 2$

As described in the previous subsection, we start from matrix $A^{(6)} = \left(A^{(6),2}; A^{(6),3}\right)$, where

$$A^{(6),2} = \left(\begin{array}{c|c|c|c|c|c} I_q & -I_q^* & & & & \\ \hline & I_q & -I_q^* & & & \\ \hline & & \ddots & \ddots & & \\ \hline & & & & I_q & -I_q^* \\ \hline I_q & I_q & I_q & \cdots & I_q & I_q - N \end{array}\right); \quad A^{(6),3} = \left(\begin{array}{c|c|c|c|c} -I_q' & I_q & & & \\ \hline & -I_q' & I_q & & \\ \hline & & \ddots & & \\ \hline & & & -I_q' & I_q \end{array}\right).$$

Performing inside each block-row of $A^{(6),3}$ two operations: multiplication rows at indexes from 0 to $q-1$ by (-1), and circular permutation of rows, we transform $A^{(6),3}$ to the form

$$A^{(7),3} = \left(\begin{array}{c|c|c|c|c|c} I_q & -I_q^* & & & & \\ \hline & I_q & -I_q^* & & & \\ \hline & & \ddots & \ddots & & \\ \hline & & & & I_q & -I_q^* \end{array}\right),$$

which is obviously spanned by rows of $A^{(6),2}$, and therefore $rank(M_{\equiv,\not\equiv}) = rank(M_{\equiv})$.

Theorem 9. *Assume $m = 2q$, and p, q are odd prime numbers. Then there is no share conversion from (2,3)-CNF over $\mathbb{Z}_{2q}$ to three-additive secret-sharing scheme over $\mathbb{Z}_p^\beta$ for any β.*

Proof. The proof follows from Theorem 8 and the fact that $rank(M_{\equiv,\not\equiv}) = rank(M_{\equiv})$. □

3.4.8. Case $p_1 = 2$, $p_2 = q$, $p = 2$

Here, we start from matrix $A^{(6)} = \left(A^{(6),2}; A^{(6),3}\right)$, where

$$A^{(6),2} = \left(\begin{array}{c|c|c|c|c|c} 1^q & 1^q & & & & \\ \hline & 1^q & 1^q & & & \\ \hline & & \ddots & \ddots & & \\ \hline & & & & 1^q & 1^q \\ \hline I_q & I_q & I_q & \cdots & I_q & I_q \oplus N \end{array}\right); \quad A^{(6),3} = \left(\begin{array}{c|c|c|c|c|c} I_q' & I_q & & & & \\ \hline & I_q' & I_q & & & \\ \hline & & \ddots & \ddots & & \\ \hline & & & & I_q' & I_q \end{array}\right).$$

Performing the same permutation of rows in each block-row in $A^{(6),3}$ as for the case $p > 2$, we obtain block-rows in form $\left(\begin{array}{c|c|c|c} \cdots & I_q & I_q^{<<1} & \cdots \end{array}\right)$, where $I_q^{<<k}$ according to

our notation is the result of the left k-bit circular shift in I_q. We remark that $I_q^{<<k_1} I_q^{<<k_2} = I_q^{<<(k_1+k_2) \mod q}$. Subtracting the last block-row of $A^{(6),2}$ from the first block-row of $A^{(6),3}$, we obtain

$$A^{(7),3}[0] = \left(\begin{array}{c|c|c|c|c} 0 & I_q \oplus I_q^{<<1} & I_q & \cdots & I_q & I_q \oplus N \end{array} \right).$$

The matrix $I_q \oplus I_q^{<<1}$ is an invertible matrix, hence it is the linear transformation matrix. We subtract the row $(I_q \oplus I_q^{<<1})A^{(7),3}[1]$ from $A^{(7),3}[0]$ to obtain

$$A^{(7),3}[0] = \left(\begin{array}{c|c|c|c|c|c} 0 & 0 & I_q \oplus (I_q \oplus I_q^{<<1})I_q^{<<1} & \cdots & I_q & I_q \oplus N \end{array} \right).$$

We stress, that $I_q \oplus (I_q \oplus I_q^{<<1})I_q^{<<1} = I_q \oplus I_q^{<<1} \oplus I_q^{<<2}$. Then we similarly subtract the 3rd block-row multiplied by the 3rd element of the first block-row, then 4th, and so on. As a result, the first block-row takes the form:

$$A^{(7),3}[0] = \left(\begin{array}{c|c|c|c|c|c} 0 & 0 & 0 & \cdots & 0 & I_q \oplus N \oplus I_q^{<<1} \oplus I_q^{<<2} \oplus \cdots \oplus I_q^{<<(q-1)} \end{array} \right).$$

Taking into account that $\bigoplus_{k=0}^{q-1} I_q^{<<k} = 1^{q \times q} = N$, the first block-row of $A^{(7),3}[0]$ equals zero and can be crossed out of the matrix.

Now, we make some elimination steps to bring matrix $A^{(6),2}$ to the echelon form (such that all the rows there are basis rows). For this, we subtract all the rows with even ordinal numbers from the first row of the last block-row. The resulting last block-row in $A^{(6),2}$ turns to $\left(\begin{array}{c|c|c|c|c} K & K & \cdots & K & K \oplus N \end{array} \right)$, where

$$K = \left(\begin{array}{c|c|c|c|c} 0 & 1 & 1 & \cdots & 1 \\ \hline 0 & 1 & 0 & \cdots & 0 \\ \hline 0 & 0 & 1 & \cdots & 0 \\ \hline & & & \ddots & \\ \hline 0 & 0 & 0 & \cdots & 1 \end{array} \right), \quad K \oplus N = \left(\begin{array}{c|c|c|c|c} 1 & 0 & 0 & \cdots & 0 \\ \hline 1 & 0 & 1 & \cdots & 1 \\ \hline 1 & 1 & 0 & \cdots & 1 \\ \hline & & & \ddots & \\ \hline 1 & 1 & 1 & \cdots & 0 \end{array} \right) \tag{47}$$

In both blocks K and $K \oplus N$, the first row is spanned by others (as their sum), thus the first row of this block-row can be crossed out. The remaining rows in this block-row are basis vectors, which do not span $A^{(7),3}$, and thus, according to Lemma 2 can be thrown out the next consideration (together with the first row which also does not span $A^{(7),3}$). Then $A^{(7)} = \left(A^{(7),2}; A^{(7),3} \right)$, where

$$A^{(7),2} = \left(\begin{array}{c|c|c|c|c|c|c} & 1^q & 1^q & & & & \\ \hline & & 1^q & 1^q & & & \\ \hline & & & & \ddots & & \\ \hline & & & & & 1^q & 1^q \end{array} \right); \quad A^{(7),3} = \left(\begin{array}{c|c|c|c|c|c|c} & I_q & I_q^{<<1} & & & & \\ \hline & & I_q & I_q^{<<1} & & & \\ \hline & & & & \ddots & & \\ \hline & & & & & I_q & I_q^{<<1} \end{array} \right).$$

Matrix $A^{(7),3}$ contains $(q-2)$ block-rows with q rows each. We make the last elimination step by subtracting each row of $A^{(7),2}$ from the first row of the correspondent block-row of $A^{(7),2}$. Then each block I_q turns to K, and each $I_q^{<<1}$ turns to $K^{<<1}$, where the first row is the sum of others. Hence, each block-row in $A^{(7),3}$ loses the first row, and the rest of them are not spanned by the basis vectors of $A^{(7),2}$. Thereby, there are $(q-2)$ block-rows with $(q-1)$ rows each, and $rank(M_{\equiv,\not\equiv}) - rank(M_{\equiv}) = (q-1)(q-2)$.

Theorem 10. *Assume $m = 2q$, where q is an odd prime number. Then there exists a share conversion from (2,3)-CNF over $\mathbb{Z}_{2q}$ to a three-additive secret-sharing scheme over $\mathbb{Z}_2^{(q-1)(q-2)}$.*

Proof. The proof follows from Theorem 8 and $rank(M_{\equiv,\not\equiv}) - rank(M_{\equiv}) = (q-1)(q-2)$. □

4. Computer Search Results on the Set S_m and the Extended Set S'_m.

Table 4 in the work of Beimel et al. [13] reports ranks of the matrices $M_{\equiv}$ and $M_{\equiv,\not\equiv}$ for $m = 6, 10, 14, 15, 21, 35$ and $p = 2, 5, 7, 11$. Unfortunately, some of the data there go against the proven properties of those matrices. For instance, in [32] it was proven that there exists a share conversion in case $m = p_1 \cdot p_2$ and $p = p_1$, where p_1 and p_2 are distinct odd primes. At the same time, Table 4 in [13] shows that for the case $m = 5 \cdot 7$ it holds that $rank(M_{\equiv}) = rank(M_{\equiv,\not\equiv})$ over $\mathbb{Z}_7$, which means the absence of the conversion. Moreover, $rank(M_{\equiv})$ cannot be less than m^2, since the matrix $M_{\equiv}$ has an identity block matrix of the size $m^2 \times m^2$ in the upper left corner. However, for case $m = 35$ in Table 4 in [13], this rank appears to be less. Therefore, we recalculated this table (also by computer search) in Tables 1 and 2 to correct the result of [13] as well as to check the soundness of our derivations.

Table 1. Rank of $M_{\equiv}$ and difference between ranks $M_{\equiv}$ and $M_{\equiv,\not\equiv}$ ($rank(M_{\equiv})$; β) for some even m over different $\mathbb{Z}_p$.

m	$2 \cdot 3 = 6$	$2 \cdot 5 = 10$	$2 \cdot 7 = 14$	$2 \cdot 11 = 22$	$2 \cdot 13 = 26$
S_m	$\{1, 3, 4\}$	$\{1, 5, 6\}$	$\{1, 7, 8\}$	$\{1, 11, 12\}$	$\{1, 13, 14\}$
$p = 2$	87 ; 2	247 ; 12	487 ; 30	1207 ; 90	1687 ; 132
$p = 3$	89 ; 0	259 ; 0	517 ; 0	1297 ; 0	1819 ; 0
$p = 5$	89 ; 0	259 ; 0	517 ; 0	1297 ; 0	1819 ; 0
$p = 7$	89 ; 0	259 ; 0	517 ; 0	1297 ; 0	1819 ; 0

The results in Table 1 confirm our conclusions. Indeed, for the case of $m = 2q$ there is a conversion if and only if the modulus of the group is 2, and in this case $\beta = (q-1)(q-2)$. Table 2 is relevant to the result of [32]. For the case of odd $m = p_1 \cdot p_2$, there is a conversion if the modulus of the group p equals either p_1 or p_2.

Table 2. Rank of $M_{\equiv}$ and difference between ranks $M_{\equiv}$ and $M_{\equiv,\not\equiv}$ ($rank(M_{\equiv})$; β) for some odd m over different $\mathbb{Z}_p$.

m	$3 \cdot 5 = 15$	$3 \cdot 7 = 21$	$3 \cdot 11 = 33$	$5 \cdot 7 = 35$
S_m	$\{1, 6, 10\}$	$\{1, 7, 15\}$	$\{1, 12, 22\}$	$\{1, 15, 21\}$
$p = 2$	617 ; 0	1229 ; 0	3077 ; 0	3529 ; 0
$p = 3$	593 ; 24	1169 ; 60	2897 ; 180	3529 ; 0
$p = 5$	609 ; 8	1229 ; 0	3077 ; 0	3409 ; 120
$p = 7$	617 ; 0	1217 ; 12	3077 ; 0	3457 ; 72

In this paper, as well as in [32], only the case of the set S_m of size 3 was considered. However, as we noted in the Introduction, the larger sets if the conversion for them exists, could result in MV families with higher VC dimension and hence in better PIR. For cases when the conversion exists in respect to the relation C_{S_m}, we also decided to check the extended sets S'_m, trying different additional values from $\mathbb{Z}_m$ and checking the ranks of $M_{\equiv}$ and $M_{\equiv,\not\equiv}$.

For even m, we only tested possible extensions for S_m modulo 2 (because if there is no conversion for a set S_m, then there is no conversion for any extended set). Of all the cases in Table 1, only for $m = 2 \cdot 7$ there are extended sets $S'_m = \{1, 3, 7, 8\}$ and $\{1, 5, 7, 8\}$ with $\beta > 0$ (namely, $\beta = 6$). The set $S'_m = \{1, 3, 5, 7, 8\}$ provides $\beta = 0$ and therefore the absence of the conversion.

Surprisingly, for odd m's the result is more encouraging: for all m and p in Table 2 which provide $\beta > 0$ for S_m, there were also extended sets S'_m with non-zero β. We summed them in Table 3. In the row $S'_m \setminus S_m$, there is a subset extending S_m up to S'_m. It is interesting

that *any* number of entries added from $S'_m \setminus S_m$ to S_m gives the same $rank(M_{\equiv})$ and β. It is also interesting that the set S'_m in all the checked cases with the odd m contains all the entries which are equal to 1 modulo p_2 (taking $p_1 = p$) except from 1 and $(0,1)_{\mathbb{Z}_m}$ which are already in S_m. Namely, $S'_m \setminus S_m = \{(2,1)_{\mathbb{Z}_m}, ..., (p-1,1)_{\mathbb{Z}_m}\}$.

Table 3. Extensions for some sets S_m allowing the share conversion.

p	3	3	3	5	5	7	7
m	$3 \cdot 5 = 15$	$3 \cdot 7 = 21$	$3 \cdot 11 = 33$	$3 \cdot 5 = 15$	$5 \cdot 7 = 35$	$3 \cdot 7 = 21$	$5 \cdot 7 = 35$
$S'_m \setminus S_m$	$\{11\}$	$\{8\}$	$\{23\}$	$\{4,7,13\}$	$\{8,22,29\}$	$\{4,10,13,16,19\}$	$\{6,11,16,26,31\}$
$rank(M_{\equiv})$	607	1201	2989	627	3511	1257	3547
β	12	30	90	2	30	2	12

Author Contributions: The authors contributed equally to this work. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by ISF grant 152/17 and by the Ariel Cyber Innovation Center in conjunction with the Israel National Cyber directorate in the Prime Minister's Office.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: We thank Yuval Ishai and Klim Efremenko for helpful discussions.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study, in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

PIR Private Information Retrieval
CC Communication complexity

Appendix A. The Correction Notice to Paskin-Cherniavsky and Schmerler

Here, we correct some computational mistakes made in [32]. The main mistake is the appearance of the matrix A^2, which correction implies also some changes in the following proof of the result. Thought, those mistakes do not affect the main result of [32] (namely, the existence of the conversion for $m = p_1 p_2$, $p = p_1$).

The major computation mistake appears in Subsection 4.5.1 of [32], therefore the following correction notice reproduces the corrected article starting from Subsection 4.5.1 up to the end the Section 4. In this section, we slightly change the enumeration of matrices to make them consistent with the present work, where we start with the matrix A in (9), which is denoted as $A^{(6)}$ in [32]. Here we correct the mistake made in the previous-step matrix $A^{(4)}$ and show how it affects the following proof. Therefore, we change the upper indexes in the following way: we write $A^{(-1),\cdot}$ instead $A^{(4),\cdot}$; $A^{(0),\cdot}$ instead $A^{(5),\cdot}$; $A^{\cdot}$ instead $A^{(6),\cdot}$; $A^{(1),\cdot}$ instead $A^{(7),\cdot}$, etc. In addition, as we changed some notation in matrices, we note that we use here the notation T_2 for the matrix previously denoted T_0 (to be consistent with the present work), and also we use $R_1^{\cdot}$ instead $\tilde{R}_1^{\cdot}$, and $R_2^{\cdot}$ instead $R_1^{\cdot}$. Similarly, we use $L_1^{\cdot}$ instead $\tilde{L}_1^{\cdot}$, and $L_2^{\cdot}$ instead $L_1^{\cdot}$.

Appendix A.1. The Matrix $A^{(-1),2}$

The mistake in the construction of A^1 and A^2 only affects the last block-rows of these matrices (i.e., for $i = p_2 - 1$). Therefore, we will consider in detail how these block-rows are built. According to the Section 4.5 in [32], the Type-2 vectors are in the form:

$$\mathbf{r}^2_{b,c} = \mathbf{e}_{b,c} - \mathbf{e}_{b,c+(1,0)_{\mathbb{Z}_m}} - \sum_{k=0}^{(0,-1)_{\mathbb{Z}_m}} (\mathbf{e}_{b+k,c} - \mathbf{e}_{b+k,c+1}). \tag{A1}$$

When $i = p_2 - 1$, each term under the summation in (A1) is similar to (17):

$$\mathbf{e}_{b+k,c} - \mathbf{e}_{b+k,c+1} = -\sum_{\ell=0}^{p_2-2} B_1[\ell, b+k] - \sum_{\ell=0}^{p_2-1+j} B_2[0, \ell, b+k] + \sum_{\ell=0}^{j-1} B_2[(p_2-1), \ell, b+k]. \tag{A2}$$

The first two terms of (A1) differ for distinct j: if $j < p_1 - 1$ they are

$$\mathbf{e}_{b,c} - \mathbf{e}_{b,c+(1,0)_{\mathbb{Z}_m}} = \mathbf{e}_{b,p_2-1+j(1,0)_{\mathbb{Z}_m}} - \mathbf{e}_{b,p_2-1+(j+1)(1,0)_{\mathbb{Z}_m}} = B_2[p_2-1, j, b]. \tag{A3}$$

For $i = p_2 - 1$, $j = p_1 - 1$, the first two terms in (A1) are

$$\mathbf{e}_{b,c} - \mathbf{e}_{b,c+(1,0)_{\mathbb{Z}_m}} = \mathbf{e}_{b,p_2-1+(p_1-1)(1,0)_{\mathbb{Z}_m}} - \mathbf{e}_{b,p_2-1+p_1(1,0)_{\mathbb{Z}_m}} = -\sum_{\ell=0}^{p_1-2} B_2[p_2-1, \ell, b]. \tag{A4}$$

Equations (A3) and (A4) give us the matrix R^1_2 in the last block of the last block-row of $A^{(-1),2}$. Equation (A2) gives the last block-row in $A^{(-1),L,2}$, and the blocks $-R^3_2$ and R^2_2 in the last block-row of $A^{(-1),R,2}$. Upper block-rows in $A^{(-1),2}$ remain as in [32].

$$A^{(-1),2} = \left(A^{(-1),L,2} | A^{(-1),R,2}\right)$$

Here, the "right side" $A^{(-1),R,2}$ is a $p_2 \times p_2$ block matrix. Its content is as follows.

$$A^{(-1),R,2} = \left(\begin{array}{c|ccccccc} & 0 & 1 & 2 & \cdots & p_2-2 & p_2-1 \\ \hline 0 & R^1_2+R^2_2 & -R^2_2 & & & & \\ 1 & & R^1_2+R^2_2 & -R^2_2 & & & \\ \vdots & & & & \ddots & & \\ p_2-2 & & & & & R^1_2+R^2_2 & -R^2_2 \\ p_2-1 & -R^3_2 & & & & & R^1_2+R^2_2 \end{array}\right)$$

The left-side matrix $A^{(-1),L,2}$ is a block matrix of size $p_2 \times 1$ (where indeed the number of rows in each of its p_2 blocks is consistent with that of $A^{(-1),R,2}$). It has the following structure (There was a missing "-" in the description of $A^{(-1),L,2}[p_2 - 1]$ in [32]).

$$A^{(-1),L,2} = \left(\begin{array}{c|c} 0 & L^{(-1),0}_2 \\ 1 & L^{(-1),1}_2 \\ \vdots & \vdots \\ p_2-2 & L^{(-1),p_2-2}_2 \\ p_2-1 & -\sum_{i=0}^{p_2-2} L^{(-1),i}_2 \end{array}\right)$$

We refer to this partition into $p_2 \times (p_2+1)$ blocks of $A^{(-1),2}$ as the "Level-1" partition of $A^{(-1),2}$. We continue next by describing the "Level-0" detail of $R^1_2, R^2_2, R^3_2, L^{(-1),i}_2$ in $A^{(-1),R,2}, A^{(-1),L,2}$. The matrix $L^{(-1),i}_2$ for $i \in \{0, \ldots, p_2-2\}$ is a $p_1 \times (p_2-1)$ block matrix of the following form:

$$L_2^{(-1),i} = \begin{array}{c|cccccc} & 0 & 1 & \cdots & i & \cdots & p_2-2 \\ \hline 0 & & & & T_2 & & \\ 1 & & & & T_2 & & \\ \vdots & & & & \vdots & & \\ p_1-2 & & & & T_2 & & \\ p_1-1 & & & & T_2 & & \end{array}$$

for a $m \times m$ circulant matrix T_2 specified in (4). Note that by the structure of $A^{(-1),L,2}$, the last matrix $L_2^{(-1),p_2-1}$ is a block matrix of size $p_1 \times (p_2-1)$, where each block equals $-T_2$. The matrix R_2^1 is a $p_1 \times (p_1-1)$ matrix specified in (5). The matrix R_2^2 is a $p_1 \times (p_1-1)$ matrix given in (6). Finally, the matrix R_2^3 is a $p_1 \times (p_1-1)$ block matrix (7).

Note that $(p_2 \mod p_1-1)$ is always smaller than p_1-1 since p_2 is prime (and thus is not a multiple of p_1).

Appendix A.2. The Matrix $A^{(-1),3}$

We choose $(B,C) = (0,0)$. Then, by Equation (12) and a simple calculation, the line is of the form (Note that another $T_{0,0}$ element is required to take care of the $\mathbf{e}_{0,0} - \mathbf{e}_{0,(0,1)_{\mathbb{Z}_m}}$ part, so it is subtracted, and is thus missing from the first sum):

$$\sum_{b=1}^{(0,1)_{\mathbb{Z}_m}-1} T_{b,0} + \sum_{j=0}^{p_1-2} R_{0,1+j\cdot(1,0)_{\mathbb{Z}_m}}$$

Appendix A.3. The Matrix $A^{(-1),1}$

We consider in detail now only the last block-row of $A^{(-1),1}$. According to the Section 4.5 in [32], the Type-1 vectors are in the form:

$$\mathbf{r}_c^1 = \sum_{b \in \mathbb{Z}_m} (\mathbf{e}_{b,c} - \mathbf{e}_{b,c+1}). \tag{A5}$$

When $i = p_2 - 1$, each term under the summation in (A5) is:

$$\mathbf{e}_{b,c} - \mathbf{e}_{b,c+1} = \mathbf{e}_{b,p_2-1+j(1,0)_{\mathbb{Z}_m}} - \mathbf{e}_{b,p_2+j(1,0)_{\mathbb{Z}_m}} = -\sum_{\ell=0}^{p_2-2} B_1[\ell,b] - \sum_{\ell=0}^{p_2-1+j} B_2[0,\ell,b] + \sum_{\ell=0}^{j-1} B_2[(p_2-1),\ell,b]. \tag{A6}$$

The first term in (A6) gives the block filled by (-1)'s in the left part of the matrix $A^{(-1),1}$, the second term gives R_1^3 in the first block of the right block-row, and the third term gives R_1^2 in the last block of the last block-row of $A^{(-1),1}$. Upper block-rows in $A^{(-1),1}$ remain as in [32].

The matrix $A^{(-1),1}$ then is of the form $A^{(-1),1} = (A^{(-1),L,1}|A^{(-1),R,1})$. To describe the left and right parts, we apply a certain transformation to $A^{(-1),L,2}$ and $A^{(-1),R,2}$, respectively. As before, we view each as a block matrix comprised of blocks of size $m \times m$ ($A^{(-1),L,2}$ has $m \times (p_2-1)$ blocks, and $A^{(-1),R,2}$ has $m \times p_2(p_1-1)$ blocks. That is, the resulting $A^{(-1),L,1}$ equals:

$$A^{(-1),L,1} = \begin{array}{c|c} 0 & L_1^{(-1),0} \\ 1 & L_1^{(-1),1} \\ \vdots & \cdots \\ p_2-2 & L_1^{(-1),p_2-2} \\ p_2-1 & -\sum_{i=0}^{p_2-2} L_1^{(-1),i} \end{array}$$

where $L_1^{(-1),i}$ equals:

$$L_1^{(-1),i} = \begin{array}{c|cccccc} & 0 & 1 & \cdots & i & \cdots & p_2-2 \\ \hline 0 & & & & (1,\cdots,1) & & \\ 1 & & & & (1,\cdots,1) & & \\ \vdots & & & & \vdots & & \\ p_1-2 & & & & (1,\cdots,1) & & \\ p_1-1 & & & & (1,\cdots,1) & & \end{array}$$

The resulting matrix $A^{(-1),R,1}$ equals (The last block-row is changed to correct the mistake made in [32]):

$$A^{(-1),R,1} = \begin{array}{c|cccccc} & 0 & 1 & 2 & \cdots & p_2-2 & p_2-1 \\ \hline 0 & R_1^2 & -R_1^2 & & & & \\ 1 & & R_1^2 & -R_1^2 & & & \\ \vdots & & & & \ddots & & \\ p_2-2 & & & & & R_1^2 & -R_1^2 \\ p_2-1 & -R_1^3 & & & & & R_1^2 \end{array}$$

where the resulting R_1^2 is defined in (2), and R_1^3 in (3). (The matrix R_1^3 is corrected in comparison with [32]).

Appendix A.4. Another Elimination Sequence

From now on, assume that $p = p_1$ and that $p_2 > 2$. We leave the full analysis of other cases for future work. We are now able to apply Lemma 2. We perform this step for I_2 corresponding to the L-part blocks of $A^{(-1)}$ and proceed in several steps. We perform the row operations starting at a grosser resolution and then proceed to a finer resolution.

Appendix A.4.1. Step 1: Working at the Resolution of Level-1 Blocks

View $A^{(-1),2}$ as a block matrix of Level-1 as described above. Let $V^{(-1),2}$ denote the corresponding block matrix. Replace the last row of $V^{(-1),2}$, $V^{(-1),2}[p_1-1,\cdot]$ by $\sum_{i=0}^{p_2-1} V^{(-1),2}[i,\cdot]$. We thus obtain a new matrix $A^{(0),2}$ of the following form. $A^{(0),2} = \left(A^{(0),L,2}|A^{(0),R,2}\right)$ has the same block structure as $A^{(-1),2}$ on all levels, so we do not repeat that, but rather only review its content.

The resulting right side $A^{(0),R,2}$ is as follows. (The matrix $A^{(0),R,2}$ corresponds to $A^{(5),R,2}$ in [32] and has the different form in the last block-row because of the corrected mistake)

$$A^{(0),R,2} = \begin{array}{c|ccccccc} & 0 & 1 & 2 & \cdots & p_2-2 & p_2-1 \\ \hline 0 & R_2^1+R_2^2 & -R_2^2 & & & & \\ 1 & & R_2^1+R_2^2 & -R_2^2 & & & \\ \vdots & & & & \ddots & & \\ p_2-2 & & & & & R_2^1+R_2^2 & -R_2^2 \\ p_2-1 & R_2^1+R_2^2-R_2^3 & R_2^1 & R_2^1 & \cdots & R_2^1 & R_2^1 \end{array}$$

The resulting left-side matrix $A^{(0),L,2}$ is (The matrix $A^{(0),L,2}$ corresponds to $A^{(5),L,2}$ in [32]):

$$A^{(0),L,2} = \begin{array}{c|c} 0 & L_2^{(-1),0} \\ 1 & L_2^{(-1),1} \\ \vdots & \vdots \\ p_2-2 & L_2^{(-1),p_2-2} \\ p_2-1 & 0 \end{array}$$

We perform a similar transformation on $A^{(-1),1}$, resulting in:

$$A^{(0),1} = (A^{(0),L,1}|A^{(0),R,1})$$

where $A^{(0),R,1}$ equals (The matrix $A^{(0),R,1}$ corresponds to $A^{(5),R,1}$ in [32] and is in different from it because of the corrected mistake):

$$A^{(0),R,1} = \begin{array}{c|cccccc} & 0 & 1 & 2 & \cdots & p_2-2 & p_2-1 \\ \hline 0 & R_1^2 & -R_1^2 & & & & \\ 1 & & R_1^2 & -R_1^2 & & & \\ \vdots & & & & \ddots & & \\ p_2-2 & & & & & R_1^2 & -R_1^2 \\ p_2-1 & R_1^2-R_1^3 & & & & & \end{array}$$

and $A^{(0),L,1}$ equals (The matrix $A^{(0),L,1}$ corresponds to $A^{(5),L,1}$ in [32]):

$$A^{(0),L,1} = \begin{array}{c|c} 0 & L_1^{(-1),0} \\ 1 & L_1^{(-1),1} \\ \vdots & \vdots \\ p_2-2 & L_1^{(-1),p_2-2} \\ p_2-1 & 0 \end{array}$$

Appendix A.4.2. Step 2: Working at the Resolution of Level-0 Blocks

Here, we view the matrix $A^{(0)}$ as a block matrix over Level-0 blocks. That is, denote by (i,j) the row block corresponding to the j^{th} Level-0 block inside the i^{th} Level-1 block of A. We transform $A^{(0)}$ into a matrix A as follows.

For each $i \in \{0,\ldots,p_2-2\}, j \in \{1,\ldots,p_1-1\}$, replace each row in $V^{(0),2}[(i,j),\cdot]$ with $V^{(0),2}[(i,j),\cdot] - V^{(0),2}[(i,0),\cdot]$. The resulting matrix A^2 is of the form $A^2 = (A^{L,2}|A^{R,2})$. (The matrix A^2 corresponds to $A^{(6),2}$ in [32].)

The right side $A^{R,2}$ is as follows. (The matrix $A^{R,2}$ corresponds to $A^{(6),R,2}$ in [32] and is in different from it because of the corrected mistake.)

$$A^{R,2} = \begin{array}{c|cccccc} & 0 & 1 & 2 & \cdots & p_2-2 & p_2-1 \\ \hline 0 & R_2^4+R_2^2 & -R_2^2 & & & & \\ 1 & & R_2^4+R_2^2 & -R_2^2 & & & \\ \vdots & & & & \ddots & & \\ p_2-2 & & & & & R_2^4+R_2^2 & -R_2^2 \\ p_2-1 & R_2^1+R_2^2-R_2^3 & R_2^1 & \cdots & & R_2^1 & R_2^1 \end{array},$$

where R_2^4 is given in (8). The resulting left-side matrix $A^{L,2}$ is (The matrix $A^{L,2}$ corresponds to $A^{(6),L,2}$ in [32].):

$$A^{L,2} = \begin{array}{c|c} 0 & L_2^0 \\ 1 & L_2^1 \\ \vdots & \vdots \\ p_2-2 & L_2^{p_2-2} \\ p_2-1 & 0 \end{array},$$

where L_2^i is given in (11).

Finally, we apply a similar transformation to $A^{(0),1}$ resulting in $A^{L,1}$ that equals (The matrix $A^{L,1}$ corresponds to $A^{(6),L,1}$ in [32]):

$$A^{L,1} = \begin{array}{|c|c|}\hline 0 & L_1^0 \\ \hline 1 & L_1^1 \\ \hline \vdots & \vdots \\ \hline p_2-2 & L_1^{p_2-2} \\ \hline p_2-1 & 0 \\ \hline \end{array},$$

where L_1^i is given in (10). The resulting right-hand side is $A^{R,1} = A^{(0),R,1}$ (there is no change, since the first block-row in $V^{(0),R,1}$ is zero).

Appendix A.4.3. Step 3: Working within Level-0 Blocks

Here, we move to working with individual rows and complete the task of leaving a basis of the original rows of $A^{(-1),L}$ as the set of non-zero rows of the matrix $A^{(1),L}$ obtained by a series of row operations. To this end, our goal is to understand the set of remaining rows in A^L. In the $A^{L,2}$ part, each Level-0 block-column (with blocks of size $m \times m$) has only $G \stackrel{def}{=} Rows(T_2) \cup \{(1,\ldots,1)\}$ (here, one appears m times) as non-zero rows, and in each row, there are non-zero entries in only one of the blocks. Thus, it suffices to find a basis for the set G of vectors.

Lemma A1. *Assume $p = p_1$. Then, the index set $I = \{k | 0 \le k \le (p_1-1)p_2\}$ satisfies that $Rows(T_2[I,[m]])$ is a basis for G. In particular, for each $i \in \mathbb{Z}_p$, we have $\sum_{j=0}^{p_1-1} T_2[i + j \cdot p_2, [m]] = x \cdot (1,\ldots,1)$. Here, x is computed as follows: first calculate y as p_2^{-1} modulo p_1 (that is, in $\mathbb{Z}_{p_1}$). Then, we "lift" y back into $\mathbb{Z}$ ($1 \le y \le p_1 - 1$) and then set x to be y modulo p—that is, x is an element of $\mathbb{Z}_p$ (note that all non-zero coefficients in the linear combination that results in $(1,\ldots,1)$ indeed belong to I).*

Another observation that will be useful to us identifies the dual of T_2.

Lemma A2. *Assume $p = p_1$. Then, the set of vectors:*

$$S = \{\sum_{j=0}^{p_1-1} \mathbf{e}_{j \cdot p_2} - \mathbf{e}_{i+(j+1)\cdot p_2} | i \in \mathbb{Z}_{p_2} \setminus \{0\}\}$$

is a basis of $Ker(T_2)$, where $Ker(T_2) \stackrel{def}{=} \{v | v \cdot T_2\}$ denotes the left kernel of the matrix T_2.

The observations are rather simple to prove by basic techniques; see [32]. Note that the general theory of cyclotomic matrices is not useful here, as it holds over infinite or large (larger than matrix size) fields, so we proceed by ad-hoc analysis of the (particularly simple) matrices at hand.

We handle the $A^{(1),2}$ part first (The matrix $A^{(1),2}$ corresponds to $A^{(7),2}$ in [32]). We conclude from Lemma A1 that for every block specified by (i,j) where $i \neq p_2 - 1$, in $V^{L,2}[(i,j),\cdot]$, the rows indexed by $b \in I$ (as in Lemma A1) span all rows in that block. Furthermore, for the purpose of Lemma 2, we b-zero the rest of the rows, by a sequence of row operations as specified by $Ker(T_2)$ in Lemma A2, starting from row $(p_1-1)p_2+1$ and moving forward up to $m-1$. That is, for b -zeroing row $(p_1-1)p_2+k$ (where $k > 0$) in $V^{L,2}[(i,j),\cdot]$ as above, we store the combination:

$$\sum_{h=0}^{p_1-1} \left(V^1[(i,j,k+h\cdot p_2),\cdot] - V^1[(i,j,k+(h+1)\cdot p_2),\cdot] \right)$$

in row (i,j,k) of $A^{(1),2}$.

Overall, the resulting $A^{(1),2}$ is as follows: $A^{(1),R,2}$ is identical to $A^{R,2}$, except for replacing R_2^4 with R_2^5. That is, in the last block row R_2^5, all cells are R_{-1}^2, and there are p_1 such cells.

Here, R_{-1}^2 is of the form:

$$R_{-1}^2 = \begin{array}{c|cccccc} & 0 & 1 & 2 & \cdots & p_2-2 & p_2-1 \\ \hline 1 & 1 & -1 & & & & \\ 2 & 1 & & -1 & & & \\ \vdots & & & & \ddots & & \\ p_2-2 & 1 & & & & -1 & \\ p_2-1 & 1 & & & & & -1 \end{array}$$

$$R_2^5 = \begin{array}{c|ccccccccc} & 0 & \cdots & p_2-1 & \cdots & 2p_2-1 & \cdots & m-p_2 & \cdots & m-1 \\ \hline 0 & & & & & & & & & \\ & & & & & & & & & \\ \vdots & & & & & \text{I} & & & & \\ & & & & & & & & & \\ & & & & & & & & & \\ m-p_2 & & & & & & & & & \\ m-p_2+1 & R_{-1}^2 & & R_{-1}^2 & & \cdots & & R_{-1}^2 & & \\ \vdots & & & & & & & & & \\ m-1 & & & & & & & & & \end{array}$$

Next, we handle the $A^{(1),1}$ part (Here, $A^{(1),1}$ corresponds to $A^{(7),1}$ in [32]). Here, we b-zero the remaining rows in $A^{L,1}$ by adding the right combination of rows in $A^{L,2}$. The combination is determined by the "in particular" part of Lemma A2. The resulting matrix $A^{(1),L,2}$ is identical to $A^{L,2}$, except for T_2 in each L_2^i being replaced by T_2'. Here, T_2' has the form:

$$\begin{array}{c|ccccccccccc} & 0 & 1 & \cdots & (1,0)_{\mathbb{Z}_m}-p_2-1 & \cdots & (1,0)_{\mathbb{Z}_m}-1 & (1,0)_{\mathbb{Z}_m} & \cdots & m-p_2 & \cdots & m-1 \\ \hline 0 & 1 & 1 & & \cdots & & 1 & & & & & \\ \vdots & & 1 & & \cdots & & & 1 & & & & \\ & & & & & \vdots & & & & & & \\ m-p_2 & 1 & 1 & \cdots & 1 & & & & & 1 & \cdots & 1 \\ m-p_2+1 & & & & & & & & & & & \\ \vdots & & & & & & & & & & & \\ m-1 & & & & & & & & & & & \end{array}$$

Here, $A^{(1),L,1}$ becomes zero, which was our goal. Note that as opposed to previous transformations, the transformation performed on $A^{L,1}$ does not "mirror" the transformation performed on $A^{L,2}$ and in fact involves rows from both $A^{L,2}$ and $A^{L,1}$. $A^{(1),R,1}$ is identical to $A^{R,1}$, except that in each Level-1 block (i,i) for $i \in \{0,\ldots,p_2-2\}$, the first row of R_1^2 (the content of this block) is replaced by (We correct here the typo in [32], by adding the exponent (-1) to x):

$$-\sum_{i=0}^{p_1-1} x^{-1}\mathbf{e}_{i\cdot p_2}.$$

It remains to b-zero the L-part of A^3. For simplicity, we focus on $V^{L,3}[0,0]$ (which is the only non-zero block in $V^{L,2}$) and then use the resulting linear dependence to produce the new row $V^3[0,\cdot]$.

$$V^{L,3}[0,0] = x^{-1}\sum_{i=0}^{p_1-1} V^{L,2}[(0,0,i\cdot p_2),0] - V^{L,2}[(0,0,(-1,0)_{\mathbb{Z}_m}+1),0]$$

This results in:

$$A^{(1),R,3} = -x^{-1}\sum_{i=0}^{p_1-1}\mathbf{e}_{(0,0,i\cdot p_2)} + \mathbf{e}_{(0,0,(-1,0)_{\mathbb{Z}_m})} + \sum_{b=1}^{(0,1)_{\mathbb{Z}_m}-1} T_{b,0}[R] + \sum_{j=0}^{p_1-2} R_{0,1+j\cdot(1,0)_{\mathbb{Z}_m}}[R] \tag{A7}$$

Appendix A.4.4. A Reduced Matrix We Will Analyze Directly

Taking I_1 to be the set of rows in $A^{(1)}$ that correspond to non-zero rows in $A^{(1),L,1}$ and I_2 corresponding to L, we obtain the following matrix $A^{(2)}$. (The matrix $A^{(2)}$ here corresponds to $A^{(8)}$ in [32].) On Level-1, it has a block structure similar to that of $A^{(1),R}$ (where the number of rows changes in some of the matrices). More concretely, $A^{(2),2}$ has the form (The correction of the mistake in [32] leads to the changed first block in the last block-row in $A^{(2),2}$):

$A^{(2),2} =$

	0	1	2	$\cdots$	p_2-2	p_2-1
0	$R_2^{5,-}+R_2^{2,-}$	$-R_2^{2,-}$				
1		$R_2^{5,-}+R_2^{2,-}$	$-R_2^{2,-}$			
$\vdots$				$\ddots$		
p_2-2					$R_2^{5,-}+R_2^{2,-}$	$-R_2^{2,-}$
p_2-1	$R_2^1+R_2^2-R_2^3$	R_2^1	$\cdots$		R_2^1	R_2^1

Here, $R_2^{5,-}$ is identical to R_2^5 except that the top $m-p_2+1$ rows in it are removed. That is, it is identical to R_2^4, except that the $(0,0)^{\text{th}}$ Level-0 block in R_2^4 replaces I by C, which are equal.

$m-p_2+1$	R_{-1}^2	R_{-1}^2	$\cdots$	R_{-1}^2
$\vdots$				
$m-1$				

.

Similarly, $R_2^{2,-}$ is obtained from R_2^2 in the same manner. In this case, only zero rows are removed. $A^{(2),1}$ is precisely $A^{(1),R,1}$ (no rows were eliminated from there, as all corresponding rows on the left side became zero). Similarly, $A^{(2),3} = A^{(1),R,3}$.

Appendix A.5. Completing the Proof—Analysis of $A^{(2)}$

We are now ready to make our conclusion, assuming $p = p_1$ and $p_1, p_2 > 2$. We stress that further analysis of the matrix is needed for identifying all p's for which a share conversion exists. In fact, some of the detailed calculations of the resulting matrix structure are not needed for our conclusion, and we could instead identify only the properties that we need of various sub-matrices. However, some of the details may be useful for future analysis, so we made all the calculations.

Our last step is to reduce the matrix $A^{(2)}$ "modulo" the set G: for every row r in $A^{(2)}$ and every Level-0 block in this row, we reduce the contents of that row "modulo" $span(Rows(T_2))$. That is, we complement the basis of $Rows(T_2)$ specified in Lemma A1 into a basis of $\mathbb{Z}_p^m$, where $\mathbf{e}_0$ is one of the added vectors and define a linear mapping L taking elements of $Rows(T_2[I,\cdot])$ to zero and other elements of the basis onto themselves (it is inconsequential what the other base elements are). Indeed, observe that $\mathbf{e}_0$ is not in $span(Rows(T_2))$, as it is not in $Ker(Ker(span(Rows(T_2))))$, as implied by Lemma A2. To verify this, observe for instance that:

$$\left\langle \sum_{i=0}^{p_1-1} (\mathbf{e}_{i\cdot p_2} - \mathbf{e}_{1+i\cdot p_2}), \mathbf{e}_0 \right\rangle = 1 \neq 0.$$

We apply a linear mapping L taking $x \in span(Rows(T_2))$ to $\mathbf{0}$ and other base elements to themselves. Recall that Level-0 blocks indeed have m columns each. We make the following observations. We let $A^{(3)}$ denote the resulting matrix. (Here, $A^{(3)}$ corresponds to $A^{(9)}$ in [32].)

Observation A1. *The rows of $A^{(3),1}$ are zero.*

Observation A2. *$A^{(3),3}$ maps to $\sum_{b=1}^{(0,1)_{\mathbb{Z}_m}-1} T_{b,0}[R] + \sum_{j=0}^{p_1-2} R_{0,1+j\cdot(1,0)_{\mathbb{Z}_m}}[R]$.*

Observation A1 follows easily from the form of the matrix $A^{(2)}$ and Lemmas A1 and A2, which implies that span$(Rows(T_2))$ is exactly the kernel of S from Lemma A2 (this is the reason we need Lemma A2: it is easier to verify that a given vector is not in $Ker(span(S))$, rather than verifying it is not in $span(T_2)$).

Observation A2 follows by the structure of $A^{(2)}$ and definition of L.

Now, if $A^{(2),3}$ is spanned by the rest of the rows in $A^{(2)}$, then it must be the case that the same dependence exists in $A^{(3)}$. Thus, it suffices to prove that the latter does not hold. Assume for the sake of contradiction that:

$$v(A^{(3),1}; A^{(3),2}) = A^{(3),3}$$

for some vector v. In the following, we use V^0 for viewing v as a block vector with Level-0 blocks. Note that unusually for this type of matrix, the blocks in the first row have $p_2 - 1$ rows, and in other block row, the cells have m rows, as usual. Similarly, we use V^1 to impose Level-1 structure onto v.

By the structure of $R_2^{2,-}$, we conclude that $A^{(3),2}$ is of the form (we note that the corrected mistake in [32] does not affect the appearance of $A^{(3),2}$ as it does apply only to the blocks spanned by the basis of T_2. Hence the following consideration is exactly as in the original work of Paskin-Cherniavsky and Schmerler):

$A^{(3),2} =$

	0	1	2	$\cdots$	p_2-2	p_2-1
0	$R_2^{5,-}$					
1		$R_2^{5,-}$				
$\vdots$				$\ddots$		
p_2-2					$R_2^{5,-}$	
p_2-1	R_2^1	R_2^1	$\cdots$		R_2^1	R_2^1

Observe that in $A^{(3),3}$, non-zero values exist only in Level-1 blocks $i = 0, 1$. As there are p_2 such blocks and $p_2 > 2$, by our assumption, we conclude that the last row contributes zero to $v(A^{(3),1}; A^{(3),2})$, as in the last block, the output needs to be zero, and it equals $V[p_2]A^{(3),2}$, which is the same contribution for all (Level-1) blocks.

To agree with $A^{(3),3}$ at block i, we must then have $v \cdot R_2^{5,-} = \mathbf{e}_0$. Viewing $R_2^{5,-}$ as a block-matrix of Level-0, because of the zeroes at all blocks but Block 0, the contributions of all block-rows but the first one to $v \cdot R_2^{5,-}$ is:

$$-(2 + (p_1 - 2)) \cdot V^1[p_2] = -p_1 \cdot V^1[0] = 0.$$

In the above, the last equality is due to the fact that $p = p_1$. Thus, we must have $V^1[0] \cdot C = \mathbf{e}_0$. However, we observe that $Rows(C)$ is a subset of $Ker(\text{span}(S))$, where S is specified in Lemma A2 and thus cannot equal $\mathbf{e}_0$ (which is not in $Ker(\text{span}(S))$).

This concludes the proof of Theorem A1:

Theorem A1. *Assume $m = p_1 \cdot p_2$, $p = p_1$, and $p_1, p_2 > 2$. Then, there exists a row v in $M_{\not\equiv}$ such that $Rows(M_{\equiv})$ does not span v.*

References

1. Chor, B.; Kushilevitz, E.; Goldreich, O.; Sudan, M. Private Information Retrieval. *J. ACM* **1998**, *45*, 965–981. [CrossRef]
2. Angel, S.; Setty, S. Unobservable communication over fully untrusted infrastructure. In Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16), Savannah, GA, USA, 2–4 November 2016; pp. 551–569.
3. Mittal, P.; Olumofin, F.G.; Troncoso, C.; Borisov, N.; Goldberg, I. PIR-Tor: Scalable Anonymous Communication Using Private Information Retrieval. In Proceedings of the 20th USENIX Security Symposium, San Francisco, CA, USA, 8–12 August 2011; p. 31.
4. Gupta, T.; Crooks, N.; Mulhern, W.; Setty, S.; Alvisi, L.; Walfish, M. Scalable and private media consumption with Popcorn. In Proceedings of the 13th (USENIX) Symposium on Networked Systems Design and Implementation (NSDI 16), Santa Clara, CA, USA, 16–18 March 2016; pp. 91–107.
5. Henry, R.; Herzberg, A.; Kate, A. Blockchain access privacy: Challenges and directions. *IEEE Secur. Priv.* **2018**, *16*, 38–45. [CrossRef]
6. Gentry, C.; Halevi, S.; Magri, B.; Nielsen, J.B.; Yakoubov, S. Random-Index PIR and Applications. Technical Report, Cryptology ePrint Archive, Report 2020/1248. 2020. Available online: https://eprint.iacr.org (accessed on 19 December 2021).
7. Green, M.; Ladd, W.; Miers, I. A protocol for privately reporting ad impressions at scale. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 1591–1601.
8. Grissa, M.; Hamdaoui, B.; Yavuz, A.A. Unleashing the power of multi-server pir for enabling private access to spectrum databases. *IEEE Commun. Mag.* **2018**, *56*, 171–177. [CrossRef]
9. Tan, Z.; Wang, C.; Yan, C.; Zhou, M.; Jiang, C. Protecting privacy of location-based services in road networks. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 6435–6448. [CrossRef]
10. Günther, D.; Holz, M.; Judkewitz, B.; Möllering, H.; Pinkas, B.; Schneider, T. PEM: Privacy-preserving Epidemiological Modeling. *Cryptol. ePrint Arch.* **2020**. Available online: https://eprint.iacr.org/2020/1546 (accessed on 20 December 2021)
11. Efremenko, K. 3-Query Locally Decodable Codes of Subexponential Length. *SIAM J. Comput.* **2012**, *41*, 1694–1703. [CrossRef]
12. Yekhanin, S. Towards 3-query locally decodable codes of subexponential length. *J. ACM* **2008**, *55*, 1:1–1:16. [CrossRef]
13. Beimel, A.; Ishai, Y.; Kushilevitz, E.; Orlov, I. Share Conversion and Private Information Retrieval. In Proceedings of the 27th Conference on Computational Complexity, CCC 2012, Porto, Portugal, 26–29 June 2012; pp. 258–268. [CrossRef]
14. Dvir, Z.; Gopi, S. 2-Server PIR with Subpolynomial Communication. *J. ACM* **2016**, *63*, 39:1–39:15. [CrossRef]
15. Kushilevitz, E.; Ostrovsky, R. Replication is NOT Needed: SINGLE Database, Computationally-Private Information Retrieval. In Proceedings of the 38th Annual Symposium on Foundations of Computer Science, FOCS'97, Miami Beach, FL, USA, 19–22 October 1997; pp. 364–373. [CrossRef]
16. Mughees, M.H.; Chen, H.; Ren, L. OnionPIR: Response Efficient Single-Server PIR. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual, Korea, 15–19 November 2021; pp. 2292–2306.
17. Ali, A.; Lepoint, T.; Patel, S.; Raykova, M.; Schoppmann, P.; Seth, K.; Yeo, K. Communication–Computation Trade-offs in PIR. In Proceedings of the 30th USENIX Security Symposium (USENIX Security 21), Virtual, 11–13 August 2021; pp. 1811–1828.
18. Park, J.; Tibouchi, M. SHECS-PIR: Somewhat Homomorphic Encryption-Based Compact and Scalable Private Information Retrieval. In *European Symposium on Research in Computer Security*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 86–106.
19. Corrigan-Gibbs, H.; Kogan, D. Private information retrieval with sublinear online time. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 44–75.
20. Gilboa, N.; Ishai, Y. Distributed point functions and their applications. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 640–658.
21. Beimel, A.; Ishai, Y.; Kushilevitz, E.; Raymond, J. Breaking the O(n1/(2k-1)) Barrier for Information-Theoretic Private Information Retrieval. In Proceedings of the 43rd Symposium on Foundations of Computer Science (FOCS 2002), Vancouver, BC, Canada, 16–19 November 2002; pp. 261–270. [CrossRef]
22. Ben-Aroya, A.; Efremenko, K.; Ta-Shma, A. Local list decoding with a constant number of queries. In Proceedings of the 2010 IEEE 51st Annual Symposium on Foundations of Computer Science, Las Vegas, NV, USA, 23–26 October 2010; pp. 715–722.
23. Chee, Y.M.; Feng, T.; Ling, S.; Wang, H.; Zhang, L.F. Query-efficient locally decodable codes of subexponential length. *Comput. Complex.* **2013**, *22*, 159–189. [CrossRef]
24. Dvir, Z.; Gopalan, P.; Yekhanin, S. Matching Vector Codes. *SIAM J. Comput.* **2011**, *40*, 1154–1178. [CrossRef]
25. Efremenko, K. From irreducible representations to locally decodable codes. In Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing, New York, NY, USA, 20–22 May 2012; pp. 327–338.
26. Itoh, T.; Suzuki, Y. Improved constructions for query-efficient locally decodable codes of subexponential length. *IEICE Trans. Inf. Syst.* **2010**, *93*, 263–270. [CrossRef]
27. Cramer, R.; Damgård, I.; Ishai, Y. Share Conversion, Pseudorandom Secret-Sharing and Applications to Secure Computation. In Proceedings of the Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, 10–12 February 2005; Kilian, J., Ed.; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3378, pp. 342–362. [CrossRef]
28. Vapnik, V.N.; Chervonenkis, A.Y. On the uniform convergence of relative frequencies of events to their probabilities. *Theory Probab. Appl.* **1971**, *16*, 264–280. [CrossRef]

29. Ben-Or, M.; Goldwasser, S.; Wigderson, A. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation (Extended Abstract). In Proceedings of the 20th Annual ACM Symposium on Theory of Computing, Chicago, IL, USA, 2–4 May 1988; Simon, J., Ed.; ACM: New York, NY, USA, 1988; pp. 1–10. [CrossRef]
30. Grolmusz, V. Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs. *Combinatorica* **2000**, *20*, 71–86. [CrossRef]
31. Ito, M.; Saito, A.; Nishizeki, T. *Multiple Assignment Scheme for Sharing Secret*; Springer: Berlin/Heidelberg, Germany, 1993; Volume 6, pp. 15–20.
32. Paskin-Cherniavsky, A.; Schmerler, L. On Share Conversions for Private Information Retrieval. *Entropy* **2019**, *21*, 826. [CrossRef]
33. Beimel, A. Secret-Sharing Schemes: A Survey. In *Coding and Cryptology—Proceedings of the Third International Workshop, IWCC 2011, Qingdao, China, 30 May–3 June 2011*; Chee, Y.M., Guo, Z., Ling, S., Shao, F., Tang, Y., Wang, H., Xing, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6639, pp. 11–46. [CrossRef]