MULTIPLE MODULAR UNIQUE FACTORIZATION DOMAIN SUBSET PRODUCT WITH ERRORS

TREY LI

ABSTRACT. We propose the multiple modular subset product with errors problem over unique factorization domains and give search-to-decision reduction as well as average-case-solution to worst-case-solution reduction for it.

1. INTRODUCTION

In [Li22a] we proposed a family of new computational problems. One of them is the modular unique factorization domain subset product with errors problem (MUSPE). It was defined as a single-instance problem, and we had only studied its *global-case hardness*, which is a notion stronger than worst-case hardness but incomparable with average-case hardness. If we zoom in each unique factorization domain (UFD), then global-case hardness is about worst-case hardness in the UFDs.

In this paper we consider the multiple-instance version of the problem and study its average-case hardness in certain UFDs. We call it the multiple modular unique factorization domain subset product with errors problem (M-MUSPE).

We give a search-to-decision reduction for M-MUSPE over unique factorization domains that are also cyclic groups. We give a worst-case-solution to average-case-solution reduction for M-MUSPE over unique factorization domains that are also cyclic groups and with integral solutions $x \in \mathbb{Z}^n$ (i.e. not restricted to be in $\{0,1\}^n$).

2. PROBLEM

First recall that (worst-case single-instance) MUSPE [Li22a] is given $n+1$ elements $a_1,\ldots,a_n,X$ of a unique factorization domain (UFD) R, an ideal I of R, as well as a set $L \subset R$ of prime elements of R that are coprime to all a_i, find a binary vector $(x_1,\ldots,x_n) \in \{0,1\}^n$ and a square-free ring element e factored over L such that

$$\prod_{i=1}^{n} a_i^{x_i} \cdot e \equiv X \pmod{I}.$$

A concrete example is the *modular subset product with errors problem* (MSPE) [Li22a], which is given $n+2$ integers $a_1,\ldots,a_n,X,N$ and a set L of primes such that no elements of L divide any a_i for $i \in [n]$, find a binary vector $x=(x_1,\ldots,x_n) \in \{0,1\}^n$ and a square-free integer e factored over L such that

$$\prod_{i=1}^{n} a_i^{x_i} \cdot e \equiv X \pmod{N}.$$

Now we define the average-case multiple-instance problem.

This is the 4th paper of the series. Previously: [Li22a; Li22b; Li22c].

Date: October 4, 2022.

Email: treyquantum@gmail.com

Setup

Let R be a UFD and I be an ideal of R such that the quotient ring R/I is a cyclic group.[1]

Let $L = \{\ell_1, \ldots, \ell_w\}$ be a set of (random) prime elements of R, where w is super-polynomial in n.[2]

Let D_ℓ be a (not low entropy) distribution over L.

Let D_e be the distribution that samples t elements $u_1, \ldots, u_t \leftarrow D_\ell$, a uniform vector $v \leftarrow \{-1,1\}^t$, and outputs the integer $e := \prod_{i=1}^t u_i^{v_i}$.[3]

An M-MUSPE oracle O_x with respect to some $x \in \{0,1\}^n$ is an oracle that outputs random MUSPE instances of the form $(a_1, \ldots, a_n, X)$, where $a_1, \ldots, a_n \leftarrow R/I$, $e \leftarrow D_e$, and $X = \prod_{i=1}^n a_i^{x_i} \cdot e \pmod{I}$.[4]

Problem

Search M-MUSPE (or M-MUSPE) is given access to O_x, find x.

Decision M-MUSPE is given access to either an M-MUSPE oracle O_x for some $x \in \{0,1\}^n$, or a random oracle O_{ran} which outputs random instances $(a_1, \ldots, a_n, X) \leftarrow (R/I)^{n+1}$, decide which oracle is given.

3. UNIQUE SOLUTION

This section is about quotient order $R/I := \mathcal{O}_K/I = \langle g \rangle$ that is a cyclic group of even order d and that the second power residue symbol of the generator g is $(g/I)_2 = -1$. The reason for requiring R to be an order $\mathcal{O}_K$ is because we want the second power residue symbol to be defined; and requiring $(g/I)_2 = -1$ and even order d is for a convenient probability argument[5].

A typical example is $R/I = (\mathbb{Z}/q\mathbb{Z})^\times = \mathbb{Z}_q^\times$ with q a rational prime.

PROPOSITION 1. The solution $x \in \{0,1\}^n$ to an M-MUSPE over a quotient order $\mathcal{O}_K/I = \langle g \rangle$ which is a cyclic group of even order d is unique with overwhelming (in n) probability if $(g/I)_2 = -1$.

Proof. Take the second power residue symbol for an MUSPE equation

$$\prod_{i=1}^n a_i^{x_i} \cdot e \equiv X \pmod{I}$$

we have an equation

$$\begin{aligned} &\prod_{i=1}^n \left(\frac{a_i}{I}\right)_2^{x_i} \cdot \left(\frac{e}{I}\right)_2 = \left(\frac{X}{I}\right)_2, \\ \iff &\prod_{j=1}^n \left(\frac{a_i}{I}\right)_2^{x_i} = \left(\frac{e}{I}\right)_2 \cdot \left(\frac{X}{I}\right)_2, \\ \iff &\prod_{j=1}^n \left(\frac{a_i}{I}\right)_2^{x_i} = \left(\frac{eX}{I}\right)_2. \end{aligned}$$

[1] A variant is to consider different random ideals I for different MUSPE instances.

[2] A typical choice for w is 2^n.

[3] A typical choice for t is 1.

[4] Here we assume the existence of an efficient algorithm for uniform sampling from R/I.

[5] We could see from the proof that an odd d does not make a big difference and that the uniqueness of solutions is plausible in that case.

This gives a linear equation

$$\sum_{i=1}^{n} \alpha_i x_i = \beta \pmod 2,$$

where α_i and β are 1 if $(a_i/I)_2$ and $(eX/I)_2$ are -1, respectively; α_i and β are 0 if $(a_i/I)_2$ and $(eX/I)_2$ are 1, respectively.

For $k > n$ MUSPE equations we have a system of k linear equations of this kind. Write the system as a matrix equation we have

$$Ax \equiv b \pmod 2,$$

where $A \in \mathbb{Z}_2^{k\times n}$ and $b \in \mathbb{Z}_2^k$.

Note that $a_i = g^{r_i} \pmod I$ for a uniform $r_i \leftarrow \mathbb{Z}_d$. Also g is a quadratic non-residue modulo I. Hence a_i is a quadratic residue if an only if r_i is even, of which the probability is 1/2. Therefore A is uniform over $\mathbb{Z}_2$.

Now notice that the probability [Lan93; Ber80; BS06] that a uniform matrix in $\mathbb{F}_2^{k\times n}$ with $k > n$ is of full $\mathbb{F}_2$-rank n is

$$p = \prod_{i=k-n+1}^{k} \left(1 - \frac{1}{2^i}\right).$$

Hence A is of full $\mathbb{F}_2$-rank n with probability p.

In particular, if $k \geq 2n$ then A is of full $\mathbb{F}_2$-rank n with probability

$$p = \prod_{i=k-n+1}^{k} \left(1 - \frac{1}{2^i}\right) \geq \prod_{i=n+1}^{2n} \left(1 - \frac{1}{2^i}\right) > \left(1 - \frac{1}{2^n}\right)^n,$$

which is overwhelming in n.

If A is really of full $\mathbb{F}_2$-rank n then $Ax \equiv b \pmod 2$ has a unique solution and thus M-MUSPE has a unique solution. Therefore M-MUSPE has a unique solution with overwhelming probability p. □

4. Search-to-decision reduction

Theorem 1. Search M-MUSPE ≤ Decision M-MUSPE.

Proof. Assume a distinguisher $\mathcal{D}$ for Decision M-MUSPE. We learn each entry of $x \in \{0,1\}^n$ from multiple fresh MUSPE instances from O_x.

To learn the k-th entry x_k, we do the following. Each time sample an MUSPE instance

$$(a_1, \ldots, a_n, X),$$

where

$$X \equiv \prod_{i=1}^{n} a_i^{x_i} \cdot e \pmod I.$$

Sample a random element

$$r \leftarrow R/I.$$

Let

$$b_k = a_k \cdot r; \text{ and } b_i = a_i \text{ for } i \in [n], i \neq k.$$

Let

$$Y \equiv X \cdot r \pmod I.$$

Call the distinguisher $\mathcal{D}$ with

$$(b_1,\ldots,b_n,Y)$$

and record the output of $\mathcal{D}$.

Repeat the above process for *poly*(n) times with *poly*(n) MUSPE instances; and output $x_k = 1$ if $\mathcal{D}$ outputs 1 more than *poly*(n)/2 times, or output $x_k = 0$ otherwise.

Now we show how it works. Note that both a_k and r are uniform over R/I. Thus $b_k = a_k \cdot r$ is uniform. Therefore $(b_1,\ldots,b_n)$ is a legal base vector for both O_x and O_{ran}.

Again, note that

$$Y \equiv \prod_{i=1}^{n} a_i^{x_i} \cdot r \cdot e \equiv \prod_{i=1}^{n} b_i^{x_i} \cdot r^{1-x_k} \cdot e \pmod{I}.$$

Hence Y is an MUSPE product with respect to $(b_1,\ldots,b_n)$ if $x_k = 1$; and it is a random element if $x_k = 0$ because r is uniform. It follows that $(b_1,\ldots,b_n,Y)$ is an MUSPE instance from O_x if $x_k = 1$; and it is a random instance from O_{ran} if $x_k = 0$. Note that the advantage of learning x_k is the same as the advantage of $\mathcal{D}$ distinguishing D_1 and D_2, which is noticeable by assumption. Hence with polynomially many trials we are able to amplify the success probability to approximately 1. □

5. Average-to-worst solution reduction

The following reduction is for M-MUSPE with integral solutions $x \in \mathbb{Z}_d^n$.

Theorem 2. M-MUSPE with average-case-solution $x \leftarrow \mathbb{Z}_d^n$ is at least as hard as the problem with worst-case-solution $x \in \mathbb{Z}_d^n$.

Proof. For each instance

$$(a_1,\ldots,a_n,X)$$

from the MUSPE distribution D_x with respect to an arbitrary (i.e. worst-case) solution $x \in \mathbb{Z}_d^n$ such that

$$\prod_{i=1}^{n} a_i^{x_i} \cdot e \equiv X \pmod{I},$$

choose a random vector $y \leftarrow \mathbb{Z}_d^n$, compute

$$\prod_{i=1}^{n} a_i^{y_i} \equiv Y \pmod{I}$$

and

$$Z \equiv XY \pmod{I}.$$

Call the M-MUSPE solver with the instances of the form

$$(a_1,\ldots,a_n,Z).$$

Note that

$$\prod_{i=1}^{n} a_i^{x_i+y_i} \cdot e \equiv Z \pmod{I};$$

where y_i are uniform, hence $x_i + y_i \pmod{d}$ are uniform. Hence the M-MUSPE solver will return

$$z \equiv x + y \pmod{d}$$

and we have that

$$x \equiv z - y \pmod{d}.$$

□

6. SUBSET SUM WITH ERRORS

We show relation with other problems.

Let $N \in \mathbb{N}$ and D_1, D_2 be two distributions over $\mathbb{Z}_N$. Let O_x with respect to some $x \in \{0,1\}^n$ be an oracle that outputs instances of the form $(\alpha_1, \ldots, \alpha_n, \beta)$, where $\alpha_1, \ldots, \alpha_n \leftarrow D_1$, $\epsilon \leftarrow D_2$, and $\beta = \sum_{i=1}^n \alpha_i x_i + \epsilon \pmod{N}$. We define the *multiple modular subset sum with errors problem* (M-MSSE) to be given access to O_x, find x.

A special case is the learning with errors problem (LWE) [Reg09], which is M-MSSE with uniform coefficient distribution D_1 and Gaussian error distribution D_2.

Another special case is the learning parity with noise problem (LPN) [BMT78; BFKL94; BKW03; Pie12], which[6] is given oracle access to instances of the form $(\alpha_1, \ldots, \alpha_n, \beta)$ with respect to the same vector $(x_1, \ldots, x_n) \in \mathbb{Z}_2^n$, where $\alpha_1, \ldots, \alpha_n, \epsilon \leftarrow \mathbb{Z}_2$ and $\beta = \sum_{i=1}^n \alpha_i x_i + \epsilon \pmod{2}$, find the vector $(x_1, \ldots, x_n)$. We see that LPN is the special case of M-MSSE with $N = 2$ and uniform D_1 and D_2.

We show that M-MSSE is at least as hard as the M-MUSPE variant that satisfy the following conditions: (1) it is over a quotient order $\mathcal{O}_K/I = \langle g \rangle$ that is a cyclic group of even order d; (2) the second power residue symbol of the generator g is $(g/I)_2 = -1$; and (3) both the bases a_i and the errors e are sampled uniformly from $\mathcal{O}_K/I$. In other words, this is the M-MUSPE in Section 3 with uniform error distribution.

In particular, we will work with LPN since the second power residue symbol $(\cdot/\mathfrak{p})_2$ is always well-defined for any prime ideal $\mathfrak{p} \subset \mathcal{O}_K$.[7]

In fact, the reduction is implied by the proof of Proposition 1. Specifically, take the second power residue symbols for an MUSPE equation

$$\prod_{i=1}^n a_i^{x_i} \cdot e \equiv X \pmod{I}$$

we have an equation

$$\prod_{i=1}^n \left(\frac{a_i}{I}\right)_2^{x_i} \cdot \left(\frac{e}{I}\right)_2 = \left(\frac{X}{I}\right)_2.$$

This gives a linear equation

$$\sum_{i=1}^n \alpha_i x_i + \epsilon = \beta \pmod{2},$$

where α_i, ϵ and β are 1 if $(a_i/I)_2$, $(e/I)_2$ and $(X/I)_2$ are -1, respectively; or α_i, ϵ and β are 0 if $(a_i/I)_2$, $(e/I)_2$ and $(X/I)_2$ are 1, respectively.

[6] Here we use the typical definition of LPN with uniform coefficient and noise distributions.

[7] Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal and let $\ell \in \mathbb{Z}_{\geq 2}$ be an integer coprime to $\mathfrak{p}$. I.e., $\ell \notin \mathfrak{p}$; in particular, ℓ can be a rational prime. We say that the ℓ-th power residue symbol $(a/\mathfrak{p})_\ell$ is well-defined if $N(\mathfrak{p}) \equiv 1 \pmod{\ell}$ so that by the analogue of Fermat's theorem $a^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}$ for any $a \in \mathcal{O}_K - \mathfrak{p}$, the number $a^{\frac{N(\mathfrak{p})-1}{\ell}}$ is "well-defined", namely $a^{\frac{N(\mathfrak{p})-1}{\ell}} \equiv \zeta^k \pmod{\mathfrak{p}}$ for a *unique* ℓ-th root of unity ζ^k, where ζ is a primitive ℓ-th root of unity and $k \in \mathbb{Z}_{\geq 0}$, also $N(\mathfrak{p}) := |\mathcal{O}_K/\mathfrak{p}|$ is the norm of the ideal $\mathfrak{p}$.

By similar arguments as in the proof of Proposition 1, α_i and ϵ are uniform over $\mathbb{Z}_2$. This means that we can always transform an M-MUSPE oracle into an LPN oracle by taking second power residue symbols for the MUSPE instances $(a_1, \ldots, a_n, X)$; and by similar arguments as in the proof of Proposition 1, the LPN problem has a unique solution with overwhelming probability. Hence if one solves the LPN, one solves the source M-MUSPE with overwhelming probability.

References

[Ber80] E.R. Berlekamp. "The technology of error-correcting codes". In: *Proceedings of the IEEE* 68.5 (1980), pp. 564–593. DOI: 10.1109/PROC.1980.11696.

[BFKL94] Avrim Blum, Merrick Furst, Michael Kearns, and Richard J. Lipton. "Cryptographic Primitives Based on Hard Learning Problems". In: *Advances in Cryptology — CRYPTO' 93*. Ed. by Douglas R. Stinson. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 278–291. ISBN: 978-3-540-48329-8.

[BKW03] Avrim Blum, Adam Kalai, and Hal Wasserman. "Noise-tolerant learning, the parity problem, and the statistical query model". In: *Journal of the ACM (JACM)* 50.4 (2003), pp. 506–519.

[BMT78] E. Berlekamp, R. McEliece, and H. van Tilborg. "On the inherent intractability of certain coding problems (Corresp.)" In: *IEEE Transactions on Information Theory* 24.3 (1978), pp. 384–386. DOI: 10.1109/TIT.1978.1055873.

[BS06] Ian F Blake and Chris Studholme. "Properties of random matrices and applications". In: *Unpublished report available at http://www. cs. toronto. edu/˜ cvs/coding* (2006).

[Lan93] Georg Landsberg. "Ueber eine Anzahlbestimmung und eine damit zusammenhängende Reihe." In: *Journal für die reine und angewandte Mathematik* 111 (1893), pp. 87–88. URL: http://eudml.org/doc/148874.

[Li22a] Trey Li. "Subset Product with Errors over Unique Factorization Domains and Ideal Class Groups of Dedekind Domains". 1st paper of the series. 2022, October 1.

[Li22b] Trey Li. "Jacobi Symbol Parity Checking Algorithm for Subset Product". 2nd paper of the series. 2022, October 2.

[Li22c] Trey Li. "Power Residue Symbol Order Detecting Algorithm for Subset Product over Algebraic Integers". 3rd paper of the series. 2022, October 3.

[Pie12] Krzysztof Pietrzak. "Cryptography from Learning Parity with Noise". In: *SOFSEM 2012: Theory and Practice of Computer Science*. Ed. by Mária Bieliková, Gerhard Friedrich, Georg Gottlob, Stefan Katzenbeisser, and György Turán. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 99–114. ISBN: 978-3-642-27660-6.

[Reg09] Oded Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *Journal of the ACM (JACM)* 56.6 (2009), p. 34.