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 $D_\ell$ be a (not low entropy) distribution over $L$.

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

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 $a_1, \ldots, a_n \sim R/I$, $e \sim D_e$, 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 $(a_1, \ldots, a_n, X) \sim (R/I)^{n+1}$, decide which oracle is given.

### 3. UNIQUE SOLUTION

This section is about quotient order $R/I := OK/I = \langle g \rangle$ 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 $OK$ 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 $OK/I = \langle g \rangle$ 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

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

$$\iff \prod_{j=1}^{n} \left(\frac{a_i}{I}\right)_2 \cdot \left(\frac{e}{I}\right)_2 \equiv \left(\frac{X}{I}\right)_2,$$

$$\iff \prod_{j=1}^{n} \left(\frac{a_i}{I}\right)_2 \equiv \left(\frac{eX}{I}\right)_2.$$
This gives a linear equation
\[ \sum_{i=1}^{n} \alpha_i x_i = \beta \pmod{2}, \]
where \( \alpha_i \) and \( \beta \) are 1 if \((a_i/I)_2\) and \((eX/I)_2\) are \(-1\), respectively; \( \alpha_i \) and \( \beta \) 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 \( \alpha_i = g^{r_i} \pmod{I} \) for a uniform \( r_i \leftarrow \mathbb{Z}_d \). Also \( g \) is a quadratic non-residue modulo \( I \). Hence \( \alpha_i \) 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
\[ p = \prod_{i=k-n+1}^{k} \left( 1 - \frac{1}{2^i} \right) \geq \prod_{i=n+1}^{2n} \left( 1 - \frac{1}{2^i} \right) \geq \left( 1 - \frac{1}{2^n} \right)^n, \]
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 \( p \). \( \square \)

4. Search-to-decision reduction

**Theorem 1.** Search M-MUSPE \( \leq \) Decision M-MUSPE.

**Proof.** Assume a distinguisher \( D \) 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
\[ b_k = a_k \cdot r; \quad \text{and} \quad b_i = a_i \text{ for } i \in [n], i \neq k. \]
Let
\[ Y \equiv X \cdot r \pmod{I}. \]
Call the distinguisher $D$ with $$(b_1, \ldots, b_n, Y)$$ and record the output of $D$.

Repeat the above process for poly$(n)$ times with poly$(n)$ MUSPE instances; and output $x_k = 1$ if $D$ 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 $b^k$ is uniform. Therefore $(b_1, \ldots, b_n)$ is a legal base vector for both $O_x$ and $O_{ran}$.

Again, note that
$$Y \equiv \prod_{i=1}^n a_i^{x_i} \cdot r^e \equiv \prod_{i=1}^n b_i^{x_i} \cdot r^{1-x_k} \cdot e \pmod{I}.$$ 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 $D$ 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. \hfill \Box

5. **AVERAGE-TO-WORST SOLUTION REDUCTION**

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

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

**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 $x \in \mathbb{Z}^n_d$ such that
$$\prod_{i=1}^n a_i^{x_i} \cdot e \equiv X \pmod{I},$$ choose a random vector $y \leftarrow \mathbb{Z}^n_d$, 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

\[ x \equiv z - y \pmod{d}. \]

\section{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 \((a_1, \ldots, a_n, \beta)\), where \( a_1, \ldots, a_n \leftarrow D_1, \epsilon \leftarrow D_2 \), and \( \beta = \sum_{i=1}^n a_i x_i + \epsilon \pmod{N} \). We define the \textit{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) \cite{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) \cite{BMT78, BFKL94, BKW03, Pie12}, which is given oracle access to instances of the form \((a_1, \ldots, a_n, \epsilon)\) with respect to the same vector \((x_1, \ldots, x_n) \in \mathbb{Z}_2^n \), where \( a_1, \ldots, a_n, \epsilon \leftarrow \mathbb{Z}_2 \) and \( \beta = \sum_{i=1}^n a_i x_i + \epsilon \pmod{2} \), 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 \( O_K/I = \langle g \rangle \) that is a cyclic group of even order \( d \); (2) the second power residue symbol of the generator \( g \) is \( \langle g/I \rangle_2 = -1 \); and (3) both the bases \( a_i \) and the errors \( \epsilon \) are sampled uniformly from \( O_K/I \). 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 \((/p)_2\) is always well-defined for any prime ideal \( p \in O_K \).

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

\[
\prod_{i=1}^n \left( \frac{a_i}{T} \right)^{x_i} \cdot \left( \frac{e}{T} \right) = \left( \frac{X}{T} \right). \]

This gives a linear equation

\[
\sum_{i=1}^n a_i x_i + \epsilon = \beta \pmod{2},
\]

where \( a_i, \epsilon \), and \( \beta \) are 1 if \((a_i/I)_2, (e/I)_2 \) and \((X/I)_2 \) are \(-1\), respectively; or \( a_i, \epsilon \), and \( \beta \) are 0 if \((a_i/I)_2, (e/I)_2 \) and \((X/I)_2 \) are \(1\), respectively.

\footnote{Here we use the typical definition of LPN with uniform coefficient and noise distributions.}

\footnote{Let \( p \in O_K \) be a prime ideal and let \( \ell \in \mathbb{Z}_{>2} \) be an integer coprime to \( p \). I.e., \( \ell \not\in p \); in particular, \( \ell \) can be a rational prime. We say that the \( \ell \)-\textit{th} power residue symbol \((a/p)_\ell\) is well-defined if \( N(p) \equiv 1 \pmod{\ell} \) so that by the analogue of Fermat’s theorem \( a^{N(p) - 1} \equiv 1 \pmod{p} \) for any \( a \in O_K - p \), the number \( a^{\frac{N(p) - 1}{\ell - 1}} \) is “well-defined”, namely \( a^{\frac{N(p) - 1}{\ell - 1}} \equiv \zeta^k \pmod{p} \) for a unique \( \ell \)-\textit{th} root of unity \( \zeta^k \), where \( \zeta \) is a primitive \( \ell \)-\textit{th} root of unity and \( k \in \mathbb{Z}_{>0} \), also \( N(p) := |O_K/p| \) is the norm of the ideal \( p \).}
By similar arguments as in the proof of Proposition 1, \(a_i\) and \(\epsilon\) 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


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