Information Sciences 451–452 (2018) 210–222

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Improved broadcast attacks against subset sum problems via lattice oracle

Yang Yu[a,1], Dianyan Xiao[b,1,*]

[a] Department of Computer Science and Technology, Tsinghua University, Beijing, China
[b] Institute for Advanced Study, Tsinghua University, Beijing, China

ARTICLE INFO

Article history:
Received 19 June 2017
Revised 5 February 2018
Accepted 3 April 2018
Available online 4 April 2018

Keywords:
Subset sum problem
Lattice-based cryptography
Broadcast attack

ABSTRACT

Subset sum problem is a classical NP-hard problem viewed as a candidate to design quantum-resistant cryptography. Cryptographic constructions based on extended modular subset sum problems are proposed subsequently in recent years. In this paper, we propose an improved broadcast attack against subset sum problems via lattice oracle. We reduce multi-dimensional (modular) subset sum problems to BDD oracle and present an explicit relationship among parameters. To the best of our knowledge, it is the first analysis on the trade-off between the efficiency of broadcast attacks and the number of obtained ciphertexts on subset sum problems. We implement our broadcast attack using LLL and BKZ algorithm and show experimentally that our method is quite practical. Furthermore, our algorithm is applicable to those low-weight subset sum problems which some cryptographic schemes are based on. We claim that our attack is efficient for both binary encoding and powerline encoding under certain parameter settings.

1. Introduction

Subset sum problem is a classical NP-hard problem and has been considered as an alternative to factoring and discrete logarithm problem to design public key cryptosystems. The *subset sum* problem, also known as *knapsack* problem, is defined as: given a set of positive integers $\{a_1, \cdots, a_n\}$ and a target sum s, find a subset of a_i's that exactly sum up to s. If we write $\mathbf{a} = (a_1, \cdots, a_n)$, the subset sum problem asks to find $\mathbf{x} = (x_1, \cdots, x_n) \in \{0, 1\}^n$ such that

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = s.$$

The appealing of subset sum problem to cryptographers depends on its two outstanding features. On one hand, computing the subset sum function can be done within a few addition operations, which is quite efficient. On the other, there is no known polynomial time quantum algorithm that can break subset sum problem, which is distinguished from factoring and discrete logarithm [34].

Merkle and Hellman proposed the first instantiated public key cryptosystem based on subset sum problem in 1978 [22]. Since then, an army of public key encryption schemes based on subset sum problem have been proposed. The pity is that most of these proposals have been broken subsequently. They are mainly subject to two classes of attacks. One class heavily

[*] Corresponding author.
E-mail addresses: y-y13@mails.tsinghua.edu.cn (Y. Yu), xiaody12@mails.tsinghua.edu.cn (D. Xiao).
[1] These authors contributed equally and should be considered as co-first authors.

https://doi.org/10.1016/j.ins.2018.04.021
0020-0255/© 2018 Elsevier Inc. All rights reserved.

relies on the specific structure of the proposed trapdoor, such as Shamir's polynomial attack on Merkle–Hellman system [33] and Brickell's attack on multi-iterated Merkle–Hellman scheme [7]. The other class deals with generic knapsacks with large weight via lattice algorithms, which is also known as *low-density attack* [1,6,12,17,18].

In order to avoid low-density attack, some schemes selected *low-weight* knapsacks in their encryption [11,26] where the Hamming weight of the plaintext is fixed. It can be generalized to *powerline encoding* where the plaintext is a vector belonging to $\mathbb{N}^n$ with fixed coordinate sum.

Besides, there are still some cryptographic constructions based on subset sum problems remaining secure today including the universal one-way hash functions, pseudorandom generators and bit-commitment schemes [16]. Moreover, a provably secure scheme based on modular subset sum problem was proposed by Ajtai and Dwork [4]. Since then, lattice-based cryptosystems with the worst-case hardness were developed in succession [20,28,31,32]. In some sense, their underlying problems can be viewed as extended subset sum problems.

Broadcast attack is a classical technique, proposed by Håstad in 1988, to analyze public key cryptosystems. It is applied in the scenario where a sender encrypts a single message by different public keys of multiple recipients. This attack enables an attacker to recover the message from the ciphertexts without any knowledge of these recipients' secret keys. Usually, the efficiency of broadcast attack is related to the number of ciphertexts which are referred to as *challenges*.

1.1. Related work

The hardness of a single subset sum problem can be reduced to either a CVP problem of the orthogonal lattice with a constructed target vector [25], or an SVP oracle of the embedded lattice for density < 0.9408 [12]. Plantard and Susilo constructed a broadcast attack against knapsack problems exploiting lattice intersections to enlarge the parameter of uSVP [29]. A broadcast attack via SVP oracle was proposed in [27] later. However, both works do not present relations between the power of oracle and the number of required challenges. Lattice algorithms for single low-weight subset sum problems were discussed in [25]. We will explore further on those low-weight knapsack problems with multiple challenges.

1.2. Our contribution

In this paper, we construct a broadcast attack on subset sum problems via BDD (or uSVP) oracle. By an improved analysis of the orthogonal lattice, we give an explicit relationship between the parameter γ in $\mathrm{BDD}_{1/\gamma}$ oracle and the number of required challenges, which are two crucial factors impacting on the efficiency of broadcast attacks. Our work will lead to a better understanding of subset sum problems, and can be used to quantify the security of relevant cryptosystems more precisely.

Moreover, we implemented our attack using LLL and BKZ algorithm and show experimentally that our method is practical because it suffices to recover the solution from only a small number of challenges. We also apply our attack to low-weight subset sum problems used in Okamoto–Tanaka–Uchiyama scheme [26], and claim that our attack is efficient for certain parameters.

We note that our result on modular subset sum problem will help to explore secure parameter setting for modular knapsack based cryptography theoretically, especially for those vectorial modular subset sum problems such as SIS (Small Integer Solution) problem [2,15].

1.3. Roadmap

We start in Section 2 with some notations and basic facts. In Section 3, we report on our reduction from multi-dimensional subset sum problem to BDD and apply our method to low-weight subset sum problem in Section 4. We discuss modular subset sum problem in Section 5 and conclude in Section 6.

2. Preliminary

We denote by $\|\cdot\|$ the Euclidean norm and $\langle\cdot,\ \cdot\rangle$ the inner product in $\mathbb{R}^n$. Let $\mathbf{1}_n$ be the vector in $\mathbb{R}^n$ with entries all 1's. For a finite set E, we denote by $U(E)$ the uniform distribution over E. Let $[B] = \mathbb{N} \cap [0, B]$ for $B > 0$. We write vectors of $\mathbb{R}^n$ in the form of columns.

Definition 1 (Lattice)**.** Given m linearly independent vectors $\mathbf{b}_1, \cdots, \mathbf{b}_m \in \mathbb{R}^n$, the lattice generated by the $\mathbf{b}_i$'s is $\mathcal{L} = \left\{\sum_{i=1}^m x_i\mathbf{b}_i \mid x_i \in \mathbb{Z}\right\}$.

We refer to $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_m)$ as a *basis* of the lattice $\mathcal{L}$. We say that the *rank* of the lattice is m and the *dimension* is n. If $n = m,$ the lattice is called a *full-rank lattice*.

Definition 2 (Determinant)**.** Given a lattice $\mathcal{L}$ and its basis $\mathbf{B}$, the determinant of $\mathcal{L}$ is defined as $\det\mathcal{L} = \sqrt{\det(\mathbf{B}^T\mathbf{B})}$, which equals the volume of the fundamental parallelepiped $\mathcal{P}(\mathbf{B}) = \left\{\sum_{i=1}^n c_i\mathbf{b}_i \mid c_i \in [0, 1)\right\}$, denoted by $\mathrm{vol}(\mathcal{L})$.

We denote by $\mathcal{B}_n(r)$ and $\mathcal{S}_{n-1}(r)$ the n-dimensional ball and sphere of radius r centered at the origin respectively.

Definition 3 (Successive Minima)**.** Let $\mathcal{L}$ be a lattice of rank n. For $i \in [n]\backslash\{0\}$, we define the ith successive minimum as the radius of the smallest sphere containing at least i linearly independent lattice vectors, *i.e.*

$$\lambda_i(\mathcal{L}) = \inf\{r \mid \dim(span(\mathcal{L} \cap \mathcal{B}_n(r))) \geq i\}.$$

Definition 4 (Dual Lattice)**.** For a lattice $\mathcal{L}$, we define its dual lattice $\mathcal{L}^* = \{\mathbf{y} \in span(\mathcal{L}) \mid \forall \mathbf{x} \in \mathcal{L}, \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}\}$.

We now recall two most basic computational problems involving lattices, SVP and CVP. Both SVP and CVP are NP-hard problems [3,35].

Definition 5 (SVP)**.** Given a lattice $\mathcal{L}$, the shortest vector problem(SVP) is to find $\mathbf{v} \in \mathcal{L}$ such that $\|\mathbf{v}\| = \lambda_1(\mathcal{L})$.

Definition 6 (CVP)**.** Given a lattice $\mathcal{L}$ and target vector $\mathbf{t}$, the closest vector problem(CVP) is to find $\mathbf{v} \in \mathcal{L}$ such that $\|\mathbf{v} - \mathbf{t}\| \leq \|\mathbf{u} - \mathbf{t}\|$ for arbitrary $\mathbf{u} \in \mathcal{L}$.

We usually use $\text{dist}(\mathbf{t}, \mathcal{L})$ to represent the closest distance from $\mathbf{t}$ to $\mathcal{L}$. That is $\text{dist}(\mathbf{t}, \mathcal{L}) = \inf\{\|\mathbf{v} - \mathbf{t}\| \mid \mathbf{v} \in \mathcal{L}\}$.

There are lattice attacks known as low-density attacks on generic subset sum problems. In the whole paper, we denote by log the logarithm function with base 2 and d the density of the subset sum problem, *i.e.* $d = \frac{n}{\log B}$.

Lemma 2.1. *Let B be a positive integer, and $a_1, a_2, \cdots, a_n$ be uniformly random integers in $[1, B]$. Let $e = (e_1, e_2, \cdots, e_n) \in \{0, 1\}^n$ be arbitrary, and $s = \sum_{i=1}^n a_i e_i$. If the density $d < 0.9408\ldots$, then the subset sum problem defined by $(a_1, a_2, \cdots, a_n; s)$ can be solved in polynomial time with a single call to an SVP oracle. Furthermore, the subset sum problem of $(a_1, a_2, \cdots, a_n; s)$ can be solved with a single call to a CVP oracle independently of the density.*

Proof. By Theorem 3.1 in [12] and Lemma 2 in [25], we complete the proof directly. □

Definition 7 (BDD $_{1/\gamma}$). Given a lattice $\mathcal{L}$ and target vector $\mathbf{t}$, where $\lambda_1(\mathcal{L}) \geq \gamma \cdot \text{dist}(\mathbf{t}, \mathcal{L})$, the $1/\gamma$-bounded distance decoding($\text{BDD}_{1/\gamma}$) is to find a vector $\mathbf{v} \in \mathcal{L}$ such that $\|\mathbf{v} - \mathbf{t}\| = \text{dist}(\mathbf{t}, \mathcal{L})$.

Definition 8 (uSVP $_\gamma$). Given a lattice $\mathcal{L}$ such that $\lambda_2(\mathcal{L}) > \gamma\lambda_1(\mathcal{L})$, the γ-unique SVP (uSVP_γ) is to find the shortest non-zero vector in $\mathcal{L}$.

We have the following reductions between $\text{BDD}_{1/\gamma}$ and uSVP [5,19]:

$$\text{uSVP}_\gamma \leq \text{BDD}_{1/\gamma} \leq \text{uSVP}_{\gamma(1+\varepsilon)/\sqrt{2}},$$

where $\varepsilon = \Omega(1/n)$. As γ increases, the $\text{BDD}_{1/\gamma}$ (or uSVP_γ) instance becomes easier, which implies a lower requirement for the algorithm to solve it.

The most popular tool to estimate the number of lattice points in a set is the so-called Gaussian Heuristic [10,14].

Gaussian Heuristic . Given a lattice $\mathcal{L}$ and a "nice" set S, the number of points in $S \cap \mathcal{L}$ is $\approx \text{vol}(S)/\text{vol}(\mathcal{L})$.

We denote by $N_{\mathcal{B}}(n, r)$ the number of integer points in $\mathcal{B}_n(r)$. From Gaussian Heuristic, we have that $N_{\mathcal{B}}(n, r)$ is proportional to r^n for large radius r and the hidden constant coefficient is $\frac{\pi^{n/2}}{\Gamma(n/2+1)}$.

3. Broadcast attack against subset sum problem

In this section, we are to expound our broadcast attack against subset sum problem by reducing multi-dimensional subset sum problem to BDD and show the efficiency experimentally.

Given k challenges, all we need is to recover the solution $\mathbf{e} = (e_1, e_2, \cdots, e_n) \in \{0, 1\}^n$,

$$\begin{cases} a_{1,1}e_1 + a_{1,2}e_2 + \cdots + a_{1,n}e_n = & s_1 \\ a_{2,1}e_1 + a_{2,2}e_2 + \cdots + a_{2,n}e_n = & s_2 \\ & \cdots \\ a_{k,1}e_1 + a_{k,2}e_2 + \cdots + a_{k,n}e_n = & s_k \end{cases}$$

where $a_{i,j}$'s are uniformly chosen in $[B]$ for $i \in [k]\backslash\{0\}$, $j \in [n]\backslash\{0\}$.

Let $\mathbf{A} = (a_{i,j})$ be the coefficient matrix, which is a uniformly random matrix of $[B]^{k\times n}$, and $\mathbf{s} = (s_1, s_2, \cdots, s_n) \in \mathbb{Z}^n$. We are interested in the case where $2^{\log^2 n} \leq B \leq 2^{2n}$ since the subset sum problem is easy to solve when B is extremely large (see Lemma 2.1) or small [9].

3.1. Improved reduction from multi-dimensional subset sum problems to lattice problems

It stands to reason that the larger k is, the easier to recover $\mathbf{e}$ is. Especially when $k \approx n$, one can figure out $\mathbf{e}$ simply by solving these linear equations. Without loss of generality, we make an assumption that $k \leq n/3$, which is the fault tolerance of consensus protocol in distributed systems [8].

Now we define the orthogonal lattice and target vector that will be used later. We denote by $\mathbf{A}^\perp$ the lattice

$$\mathbf{A}^\perp = \{\mathbf{x} \in \mathbb{Z}^n \mid \mathbf{A}\mathbf{x} = \mathbf{0}\}$$

and $\mathbf{y} \in \mathbb{Z}^n$ an arbitrary solution to $\mathbf{A}\mathbf{x} = \mathbf{s}$. We set the target point $\mathbf{t}$ as

$$\mathbf{t} = -\mathbf{y} + \frac{1}{2}\mathbf{1}_n.$$

By running $\mathrm{BDD}_{1/\gamma}$ oracle with input ($\mathbf{A}^\perp$, $\mathbf{t}$), we can recover $\mathbf{e}$ with overwhelming probability. The following result is our main conclusion.

Theorem 3.1 (Main Theorem)**.** *Let $\mathbf{A}$ be uniformly distributed over $[B]^{k\times n}$ for $\log^2 n \le \log B \le 2n$. There exists an algorithm to find a solution to $\mathbf{A}\mathbf{x} = \mathbf{s}$ for $\mathbf{x} \in \{0, 1\}^n$ with overwhelming probability via a single call to $BDD_{1/2}$ oracle when $k \ge 3d$, where $d = n/\log B$ is the density.*

In particular, when $\frac{1}{2}d\log n + 1 \le k \le \frac{n}{3}$, one can find a solution to $\mathbf{A}\mathbf{x} = \mathbf{s}$ for $\mathbf{x} \in \{0, 1\}^n$ with overwhelming probability via a single call to $BDD_{1/\gamma}$ oracle with

$$1 \le \log\gamma \le \frac{n}{n-k}\left(\frac{k-1}{d} - \frac{1}{2}\log n\right) + 1.$$

With the reduction from $\mathrm{BDD}_{1/\gamma}$ to $\mathrm{uSVP}_{\gamma/\sqrt{2}}$, we can obtain the following corollary directly.

Corollary 3.2. *There exists an algorithm to find a solution to $\mathbf{A}\mathbf{x} = \mathbf{s}$ for $\mathbf{x} \in \{0, 1\}^n$ with overwhelming probability via a polynomial number of calls to $uSVP_\gamma$ oracle with*

$$\frac{1}{2} < \log\gamma \le \frac{n}{n-k}\left(\frac{k-1}{d} - \frac{1}{2}\log n\right) + \frac{1}{2}$$

where $d = \frac{n}{\log B}$ is the density and $\mathbf{A}$ is uniformly distributed over $[B]^{k\times n}$ for $\log^2 n \le \log B \le 2n$ and $\frac{1}{2}d\log n + 1 \le k \le \frac{n}{3}$.

Before we prove our main result Theorem 3.1, it is necessary to explore the random lattice $\mathbf{A}^\perp$. Over the randomness of $\mathbf{A}$, the probability of an arbitrary $\mathbf{z} \in \mathbb{Z}^n$ belonging to $\mathbf{A}^\perp$ is quite crucial in the reduction later. Since the rows of $\mathbf{A}$ are independent and identically distributed, we have

$$\Pr[\mathbf{x} \in \mathbf{A}^\perp] = \prod_i \Pr[\mathbf{x} \in \mathbf{a}_i^\perp] = (\Pr[\mathbf{x} \in \mathbf{a}^\perp])^k.$$

Recall the single subset sum problem:

$$a_1e_1 + a_2e_2 + \cdots + a_ne_n = s$$

where $a_i \sim U([B])$ for integer $\log^2 n \le \log B < 2n$, $e_i \in \{0, 1\}$. Let $\mathbf{a} = (a_1, a_2, \cdots, a_n)$ and $\mathbf{e} = (e_1, e_2, \cdots, e_n)$.

In the analysis of [12], the probability $\Pr[\mathbf{z} \in \mathbf{a}^\perp]$ for arbitrary $\mathbf{z} \in \mathbb{Z}^n$ has already been bounded as follows.

Lemma 3.3 ([12])**.** *Given arbitrary $\mathbf{z} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ and $\mathbf{a} \sim U([B])^n$, the probability that $\mathbf{z} \in \mathbf{a}^\perp$ is*

$$\Pr[\mathbf{z} \in \mathbf{a}^\perp] \le \frac{1}{B}.$$

We claim that this bound $\frac{1}{B}$ can be optimized.

Lemma 3.4. *Given $\mathbf{z} = (z_1, \cdots, z_n) \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ and $\mathbf{a} \sim U([B])^n$ where $n^2\|\mathbf{z}\| \le B$, we have that*

$$\Pr[\mathbf{z} \in \mathbf{a}^\perp] \le \frac{ce^{\frac{1}{n}}}{B\|\mathbf{z}\|_\infty} \le \frac{c\sqrt{n}e^{\frac{1}{n}}}{B\|\mathbf{z}\|},$$

where $c = \gcd(z_1, \cdots, z_n)$ and $\|\mathbf{z}\|_\infty = \max_i\{|z_i|\}$ for $i \in [n]\backslash\{0\}$.

Proof. Let $z_i' = z_i/c$ for any $i \in [n]\backslash\{0\}$, and $\mathbf{z}' = (z_1', \cdots, z_n')$, then we get that $\Pr[\mathbf{z} \in \mathbf{a}^\perp] = \Pr[\mathbf{z}' \in \mathbf{a}^\perp]$. W.l.o.g., we let $z_1' = \|\mathbf{z}\|_\infty/c$, and obtain

$$\begin{aligned}\Pr\left[\mathbf{z}' \in \mathbf{a}^\perp\right] &= \Pr\left[a_1z_1' + \sum_{i=2}^n a_iz_i' = 0\right] \\ &= \sum_{j=0}^B \Pr[a_1 = j]\Pr\left[\sum_{i=2}^n a_iz_i' = -z_1'j\right] \\ &\le \frac{1}{B+1}\Pr\left[\sum_{i=2}^n a_iz_i' = 0 \bmod z_1'\right].\end{aligned}$$

It suffices to prove that

$$\Pr\left[\sum_{i=2}^{n} a_i z_i' = 0 \bmod z_1'\right] \le \frac{1}{z_1'} e^{\frac{1}{n}}.$$

Now we prove the above inequality. Let $\alpha(x) = \exp(2\pi x\sqrt{-1}/z_1')$, then

$$\frac{1}{z_1'}\sum_{\lambda=0}^{z_1'-1} \alpha(\lambda x) = \begin{cases} 1 & x = 0 \bmod z_1' \\ 0 & x \neq 0 \bmod z_1' \end{cases}. \tag{1}$$

Let $\mathbf{z}'' = (z_2', \cdots, z_n')$ and $N_{\mathbf{z}''}(z_1')$ be the number of vectors $\mathbf{x} \in [B]^{n-1}$ such that $\langle \mathbf{z}'', \mathbf{x}\rangle = 0 \bmod z_1'$. Accordingly, we may obtain that

$$N_{\mathbf{z}''}(z_1') = \frac{1}{z_1'} \sum_{\mathbf{x}\in[B]^{n-1}} \sum_{\lambda=0}^{z_1'-1} \alpha(\lambda\langle \mathbf{z}'', \mathbf{x}\rangle) \tag{2}$$

Assuming that $B = r_1 z_1' + r_2$ with $r_2 \in [0, z_1')$, then we have that for arbitrary $\mathbf{x}' \in \mathbb{Z}_{z_1'}^{n-1}$, the number of vectors $\mathbf{x} \in [B]^{n-1}$ satisfying $\mathbf{x} \equiv \mathbf{x}' \bmod z_1'$ is at most $(r_1+1)^{n-1}$. Therefore, we have

$$\begin{aligned} N_{\mathbf{z}''}(z_1') &\le \frac{(r_1+1)^{n-1}}{z_1'} \sum_{\lambda=0}^{z_1'-1} \sum_{\mathbf{x}'\in\mathbb{Z}_{z_1'}^{n-1}} \alpha(\lambda\langle \mathbf{z}'', \mathbf{x}'\rangle) \\ &= \frac{(r_1+1)^{n-1}}{z_1'} \sum_{\lambda=0}^{z_1'-1} \prod_{j=1}^{n-1} \left(\sum_{x_j'=0}^{z_1'-1} \alpha(\lambda x_j' z_{j+1}') \right). \end{aligned}$$

From Eq. (1), the term $\prod_{j=1}^{n-1} \left(\sum_{x_j'=0}^{z_1'-1} \alpha(\lambda x_j' z_{j+1}') big\right)$ does not equal 0 if and only if $\lambda z_{j+1}' = 0 \bmod z_1'$ for $1 \le j \le n-1$. Due to the fact that $\gcd(z_1', \cdots, z_n') = 1$, it can be verified that $\prod_{j=1}^{n-1} \left(\sum_{x_j'=0}^{z_1'-1} \alpha(\lambda x_j' z_{j+1}')\right)$ does not equal 0 if and only if $\lambda = 0$. Consequently, we get that

$$N_{\mathbf{z}''}(z_1') \le \frac{(r_1+1)^{n-1}(z_1')^{n-1}}{z_1'}.$$

Therefore, we have that

$$\Pr\left[\sum_{i=2}^{n} a_i z_i' = 0 \bmod z_1'\right] = \frac{N_{\mathbf{z}''}(z_1')}{B^{n-1}} \le \frac{1}{z_1'}\left(1 + \frac{z_1'}{B}\right)^{n-1} \le \frac{e^{\frac{1}{n}}}{z_1'}$$

Due to the fact that $\|\mathbf{z}\|_\infty \ge \frac{\|\mathbf{z}\|}{\sqrt{n}}$, we now complete the proof. □

Thanks to the independence among the rows of **A**, we immediately obtain the following result.

Lemma 3.5. *Given* $\mathbf{z} = (z_1, \cdots, z_n) \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ *and* $\mathbf{A} \sim U([B])^{k\times n}$ *where* $k \le n$ *and* $n^2\|\mathbf{z}\| \le B$, *we have that*

$$\Pr[\mathbf{z} \in \mathbf{A}^\perp] \le \left(\frac{ce^{\frac{1}{n}}}{B\|\mathbf{z}\|_\infty}\right)^k \le 3\left(\frac{c\sqrt{n}}{B\|\mathbf{z}\|}\right)^k.$$

where $\|\mathbf{z}\|_\infty = \max_i\{|z_i|\}$ *and* $c = \gcd(z_1, \cdots, z_n)$ *for* $i \in [n]\backslash\{0\}$.

Before proving Theorem 3.1, we need to review a classical problem in number theory. Let $r_n(t)$ denote the number of representations of non-negative integer t as a sum of n squares, counting permutations and sign changes. Actually $r_n(t)$ equals the number of integer points on $\mathcal{S}_{n-1}(\sqrt{t})$. The general formula of $r_n(t)$ for even n was stated by Ramanujan [30], and proved by Mordell [23]. We will give an upper bound of $r_n(t)$.

Lemma 3.6. *Let* $r_n(t)$ *denote the number of integer solutions to* $\sum_{i=1}^n x_i^2 = t$ *for non-negative integer* t. *When* $n \ge 6$, *we have the following inequality for* $r_n(t)$

$$r_n(t) \le Ct^{\frac{n}{2}-1}.$$

where C *is a positive constant.*

Proof. When n is even, with the results in [30], we have $r_n(t) = \delta_n(t) + e_n(t)$, where $\delta_n(t)$ is the divisor function and $e_n(t)$ is the error. It was claimed that $\delta_n(t) = C' t^{\frac{n}{2}-1}$ for some positive constant C' and $e_n(t) = O\left(t^{\frac{n}{2}-1-\frac{1}{2}\left[\frac{n}{3}\right]+\epsilon}\right)$ for those $n \geq 6$. As a result, we obtain an upper bound of $r_n(t)$ for even n: $r_n(t) \leq (C'+1)t^{\frac{n}{2}-1}$.

Now we discuss the case where n is odd. We consider the solution to $x_1^2 + \sum_{i=2}^n x_i^2 = t$. Taking $x_1 = 0, \pm 1, \cdots, \pm \lfloor \sqrt{t} \rfloor$, we obtain that

$$r_n(t) \leq 2 \sum_{i=0}^{\lfloor \sqrt{t} \rfloor} r_{n-1}(t - i^2) \leq 2(C'+1)\sqrt{t} \cdot t^{\frac{n-1}{2}-1} = Ct^{\frac{n}{2}-1}.$$

where $C = 2(C'+1)$. □

Remark 1. By Gaussian Heuristic, we may evaluate $r_n(t)$ for $t > n^2$ by

$$V(\mathcal{B}_n(\sqrt{t})) - V(\mathcal{B}_n(\sqrt{t-1})) = \frac{n\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)} t^{\frac{n}{2}-1}\left(1 + o\left(\frac{1}{\sqrt{t}}\right)\right).$$

The estimation of $r_n(t)$ coincides with that by Gaussian Heuristic for large t. The item $\frac{n\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)} \leq 1$ for large dimension n. Especially when n is even, the bound $Ct^{\frac{n}{2}-1}$ is somewhat explicit, which offers convincing evidence for Gaussian Heuristic.

3.1.1. Proof of Main Theorem

Recall that $\mathbf{t} = -\mathbf{y} + \frac{1}{2}\mathbf{1}_n$ where $\mathbf{y} \in \mathbb{Z}^n$ is an arbitrary solution to $\mathbf{Ax} = \mathbf{s}$ and $\mathbf{e} \in \{0, 1\}^n$ is a small solution to $\mathbf{Ax} = \mathbf{s}$. Then we can derive that $\text{dist}(\mathbf{t}, \mathbf{A}^{\perp}) = \frac{\sqrt{n}}{2}$. Also we notice that $\mathbf{e} - \mathbf{y}$ is the unique closest vector of $\mathbf{A}^{\perp}$ to $\mathbf{t}$ if $k \geq d$, following Theorem 1 in [25].

We note that the lattice $\mathbf{A}^{\perp}$ is quite sparse. For random $\mathbf{A} \sim U([B]^{k \times n})$, it follows that

$$\Pr[\lambda_1(\mathbf{A}^{\perp}) \geq R] = 1 - \Pr[\lambda_1(\mathbf{A}^{\perp}) < R] \geq 1 - \sum_{0<\|\mathbf{z}\|<R} \Pr[\mathbf{z} \in \mathbf{A}^{\perp}].$$

Since the cardinality of $\{\mathbf{x} \in \mathbb{Z}^n \mid \|\mathbf{x}\| \leq \sqrt{n}\}$ is less than $e^{1.4189n}$ [21], by Lemma 3.3, we know that, when $k \geq 3d$,

$$\sum_{0<\|\mathbf{z}\|\leq\sqrt{n}} \Pr[\mathbf{z} \in \mathbf{A}^{\perp}] \leq \frac{1}{B^k} \cdot 2^{2.047n} \leq 2^{-0.9n}.$$

Thus, with $3d$ instances, the solution $\mathbf{e}$ can be recovered with overwhelming probability via a single call to $\text{BDD}_{1/2}$. However, $\text{BDD}_{1/2}$ is hard that cannot be solved in polynomial time so far.

Indeed for some parameters, the $\text{BDD}_{1/2}$ oracle can be replaced by $\text{BDD}_{1/\gamma}$ with a large γ. Now we are to discuss $\Pr[\lambda_1(\mathbf{A}^{\perp}) \geq R]$ for $R > \sqrt{n}$.

We denote by $S(t, c)$ the set

$$S(t, c) = \{\mathbf{z} = (z_1, \cdots, z_n) \in \mathbb{Z}^n \mid \|\mathbf{z}\| = t, \gcd(z_1, \cdots, z_n) = c\}. \tag{3}$$

With Lemma 3.5 and the observation that $S(t, c) = cS(t/c, 1)$, it can be derived that when $\sqrt{n} < R \leq B/n^2$,

$$\begin{aligned}
\sum_{0<\|\mathbf{z}\|<R} \Pr[\mathbf{z} \in \mathbf{A}^{\perp}] &\leq \frac{3}{B^k} \sum_{j=1}^{R^2-1} \sum_{c^2 | j} \sum_{\mathbf{z} \in S(\sqrt{j}, c)} \left(\frac{c}{\|\mathbf{z}\|_\infty}\right)^k \\
&= \frac{3}{B^k} \sum_{l=1}^{R^2-1} \sum_{0<lc^2<R^2} \sum_{\mathbf{z} \in S(\sqrt{l}, 1)} \frac{1}{\|\mathbf{z}\|_\infty^k}.
\end{aligned}$$

Due to the fact that the number of c's such that $0 < lc^2 < R^2$ is at most $R/\sqrt{l}$, and $\|\mathbf{z}\|_\infty \geq \|\mathbf{z}\|/\sqrt{n}$, we have

$$\begin{aligned}
&\sum_{0<\|\mathbf{z}\|<R} \Pr[\mathbf{z} \in \mathbf{A}^{\perp}] \\
&\leq \frac{3}{B^k} \sum_{l=1}^{R^2-1} \frac{R}{\sqrt{l}} \sum_{\mathbf{z} \in S(\sqrt{l}, 1)} \frac{1}{\|\mathbf{z}\|_\infty^k} \\
&\leq \frac{3R}{B^k} \left(\sum_{l=1}^{n} |S(\sqrt{l}, 1)| \cdot 1 + \sum_{l=n+1}^{R^2-1} |S(\sqrt{l}, 1)| \cdot \frac{1}{\sqrt{l}} \cdot \left(\sqrt{\frac{n}{l}}\right)^k \right).
\end{aligned}$$

We notice that $\sum_{l=1}^{n} |S(\sqrt{l}, 1)| \le 2^{2.047n}$ according to [21]. It is also noted that for $l \ge n$, $S(\sqrt{l}, 1)$ is the set of primitive integer solutions to $\sum_{i=1}^{n} x_i^2 = l$, which implies that $|S(\sqrt{l}, 1)| \le r_n(l) \le Cl^{\frac{n}{2}-1}$ by Lemma 3.6. Combining the fact that

$$\sum_{j=n+1}^{R^2-1} j^{\frac{n-k-3}{2}} \le \sum_{j=n+1}^{R^2-1} \int_j^{j+1} x^{\frac{n-k-3}{2}} dx \le \frac{2(R^{n-k-1} - n^{\frac{n-k-1}{2}})}{n-k-1},$$

it follows that if $R = \gamma \cdot \frac{\sqrt{n}}{2}$, then

$$\begin{aligned}\sum_{l=n+1}^{R^2-1} |S(\sqrt{l}, 1)| \cdot \frac{1}{\sqrt{l}} \cdot \left(\sqrt{\frac{n}{l}}\right)^k &\le C(\sqrt{n})^k \sum_{l=n+1}^{R^2-1} l^{\frac{n-k-1}{2}-1} \\ &\le \frac{2C(\sqrt{n})^{n-1}}{n-k-1}\left(\left(\frac{\gamma}{2}\right)^{n-k-1} - 1\right).\end{aligned}$$

Finally, when $\sqrt{n} < R = \gamma \cdot \frac{\sqrt{n}}{2} < \frac{B}{n^2}$, we obtain that

$$\sum_{0<\|\mathbf{z}\|<R} \Pr[\mathbf{z} \in \mathbf{A}^{\perp}] \le \frac{3\gamma\sqrt{n} \cdot 2^{2.047n}}{2B^k} + \frac{6C(\sqrt{n})^n\left(\gamma^{n-k} - 2^{n-k}\right)}{(n-k-1) \cdot 2^{n-k} \cdot B^k}.$$

When $\frac{1}{2}d\log n + 1 \le k \le \frac{n}{3}$ and $\log\gamma \le \frac{n}{n-k}\left(\frac{k-1}{d} - \frac{1}{2}\log n\right) + 1$, we have

$$\sum_{0<\|\mathbf{z}\|<R} \Pr[\mathbf{z} \in \mathbf{A}^{\perp}] \le \frac{3 \cdot 2^{3.047n}\sqrt{n}}{2^{0.5n\log n}} + \frac{6C}{(n-k-1)B}$$

which is negligible since $B \ge 2^{\log^2 n}$.

Therefore, when $\frac{1}{2}d\log n + 1 \le k \le \frac{n}{3}$, it holds that $\lambda_1(\mathbf{A}^{\perp}) \ge \gamma\frac{\sqrt{n}}{2}$ with overwhelming probability for

$$1 \le \log\gamma \le \frac{n}{n-k}\left(\frac{k-1}{d} - \frac{1}{2}\log n\right) + 1.$$

□

Remark 2. The inequality in Theorem 3.1 shows a trade-off between the power of BDD oracle and the size k of the multi-dimensional subset sum problem. As k increases, γ can reach a larger value, which means we can recover the solution by solving a weaker BDD instance.

According to the extended experiments in [13], the practical limits of γ are 0.25×1.021^n by LLL and 0.48×1.012^n by BKZ-20. Thus we can recover a solution in $\{0, 1\}^n$ to $\mathbf{Ax} = \mathbf{s}$ with less than $\frac{0.03n+0.5\log n}{0.03+1/d}$ challenges via LLL, or less than $\frac{0.017n+0.5\log n}{0.017+1/d}$ challenges via BKZ-20. We note that the lattice $\mathbf{A}^{\perp}$ is of rank $n-k$.

Overall, the relation of our reduction in Theorem 3.1 is much more accurate due to the improvement in Lemma 3.4 and should be considered when setting parameters for cryptographic constructions based on subset sum problems.

3.2. Broadcast attacks and analysis

In this section, we describe a broadcast attack based on Theorem 3.1. Given k challenges $\mathbf{Ax} = \mathbf{s}$ where $\mathbf{x} \in \{0, 1\}^n$, we compute a basis $\mathbf{B}$ of $\mathbf{A}^{\perp}$ following the method in [24] and a target vector $\mathbf{t} = -\mathbf{y} + \frac{1}{2}\mathbf{1}_n$ where $\mathbf{y}$ is an arbitrary solution to $\mathbf{Ax} = \mathbf{s}$. We will use lattice basis reduction algorithms (LLL and BKZ) to solve uSVP of the lattice $(\mathbf{B}|\mathbf{t})$. Similarly, one may apply some other algorithms to solve the BDD instance $(\mathbf{B}, \mathbf{t})$ directly.

3.2.1. Experimental method and performance

We next report on our experimental results on the broadcast attack. We ran experiments on subset sum instances of various density d and dimension n. For each instance, we measured the minimal k such that the solution can be recovered from k challenges. In our experiments, we added a new challenge if the existing challenges were not enough to recover the solution, which is more appropriate to the situation in real world.

To begin with, we introduce a faster method of computing a basis of orthogonal lattice when new challenge is added. Given a basis $\mathbf{B}$ of $\mathbf{A}^{\perp}$ and a new challenge $(\mathbf{a}, s)$, we can easily compute $\mathbf{U}$ as the basis of $(\mathbf{a}^T\mathbf{B})^{\perp}$. It is easy to verify that $\mathbf{BU}$ is a basis of the new lattice $\begin{pmatrix}\mathbf{A} \\ \mathbf{a}^T\end{pmatrix}^{\perp}$. We followed the method proposed in [24] but with a smaller scaling factor to obtain a basis of orthogonal lattice.

For each pair (d, n), we worked on 10 sets of random instances and evaluated the average of the minimal k such that the broadcast attack succeeded with k challenges. We applied LLL algorithm with Lovász parameter 0.9999 and BKZ algorithm with blocksize 20. Fig. 1 shows our practical broadcast attacks against subset sum problems for different parameters.

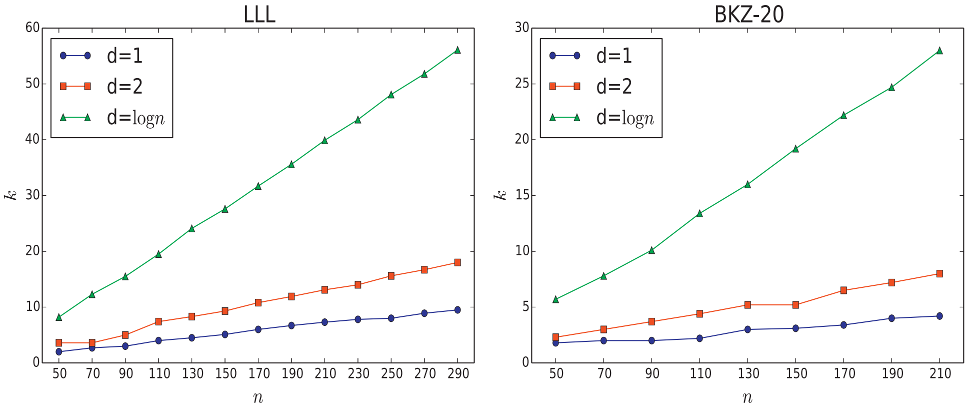

Fig. 1. Experimental results of our broadcast attack.

For the case of low density ($d = 1, 2$), it suffices to recover the solution from a small number of challenges using our attack. When d is a monotonically increasing function of n (say $d = \log n$), the number of required challenges seems large, but still within the range of fault tolerance in some consensus protocols [8]. Therefore, our attack is quite practical. Furthermore, the performance of our broadcast attack is heavily affected by the lattice basis reduction algorithm. Exploiting more advanced algorithms such as BKZ 2.0 [10], we may achieve higher dimensions with less challenges.

3.2.2. Comparison with other broadcast attacks

In this subsection, we compare our attack with two existing broadcast attacks proposed in [27,29] from the aspect of the lattice problems that the subset sum problem was reduced to.

Plantard-Susilo's broadcast attack. In [29], Plantard and Susilo proposed a broadcast attack against GGH and knapsack problem by intersecting the following lattices of dimension $n + 2$ and rank $n + 1$ for $i = 1, \cdots, k$

$$\mathcal{L}_i = \mathcal{L}\begin{pmatrix} \mathbf{I}_n & \mathbf{0}_n & \mathbf{a}_i \\ \frac{1}{2}\mathbf{1}_n^T & 1 & s_i \end{pmatrix}^T.$$

They observed that once these $\mathcal{L}_i$'s share a same nonzero shortest vector $(\mathbf{e}, 0)$, their intersection lattice $\mathcal{L}' = \bigcap \mathcal{L}_i$ would be of a much larger gap, *i.e.*

$$\frac{\lambda_2(\mathcal{L}')}{\lambda_1(\mathcal{L}')} \geq \max_i \left\{ \frac{\lambda_2(\mathcal{L}_i)}{\lambda_1(\mathcal{L}_i)} \right\}.$$

That is why they can recover $\mathbf{e}$ with a uSVP oracle to the lattice $\mathcal{L}'$.

Pan-Zhang's broadcast attack. The Pan-Zhang's attack [27] against multi-subset sum problem reduced the problem to an SVP instance

$$\mathcal{L}'' = \mathcal{L}\begin{pmatrix} \mathbf{I}_n & \mathbf{0}_n & N\mathbf{A}^T \\ \frac{1}{2}\mathbf{1}_n^T & 1 & N\mathbf{s}^T \end{pmatrix}^T,$$

where N is a large integer. It is noted that $\mathcal{L}''$ is of dimension $n + k + 1$ and rank $n + 1$. They proved that when $k \geq 0.9408d$, the multi-subset sum problem can be solved by a single call to SVP algorithm on $\mathcal{L}''$.

Recall that we reduce the subset sum problem to BDD instance $(\mathcal{L}(\mathbf{B}), \mathbf{t})$ where $\mathbf{B}$ is a basis of $\mathbf{A}^\perp$ and $\mathbf{t} = -\mathbf{y} + \frac{1}{2}\mathbf{1}_n$ for arbitrary $\mathbf{y} \in \mathbb{Z}^n$ such that $\mathbf{Ay} = \mathbf{s}$. In order to explicitly compare our attack with above attacks, we transform our BDD instance to a uSVP instance

$$\mathcal{L} = \mathcal{L}\begin{pmatrix} \mathbf{B} & \mathbf{t} \\ \mathbf{0}_{n-k}^T & 1 \end{pmatrix},$$

which is of dimension $n + 1$ and rank $n - k + 1$.

We claim that $\mathcal{L}$ is sparser than $\mathcal{L}'$ and $\mathcal{L}''$. Indeed, our lattice $\mathcal{L}$ is a sublattice of both $\mathcal{L}'$ and $\mathcal{L}''$. More precisely, it holds that $(\mathcal{L}, 0)^T \subseteq \mathcal{L}'$ and $(\mathcal{L}, \mathbf{0}_k^T)^T \subseteq \mathcal{L}''$. For any $(\mathbf{u}_1^T, u_2)^T \in \mathbb{Z}^n \times \mathbb{Z}$ and $i \in [k] \backslash \{0\}$, we have

$$\begin{bmatrix} \mathbf{B} & \mathbf{t} \\ \mathbf{0}_{n-k}^T & 1 \\ \mathbf{0}_{n-k}^T & 0 \end{bmatrix} \begin{bmatrix} \mathbf{u}_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} \mathbf{B}\mathbf{u}_1 - u_2\mathbf{y} + \frac{1}{2}u_2\mathbf{1}_n \\ u_2 \\ \mathbf{0} \end{bmatrix} = \begin{bmatrix} \mathbf{I}_n & \frac{1}{2}\mathbf{1}_n \\ \mathbf{0}_n^T & 1 \\ \mathbf{a}_i^T & s_i \end{bmatrix} \begin{bmatrix} \mathbf{B}\mathbf{u}_1 - u_2\mathbf{y} \\ u_2 \end{bmatrix} \in \mathcal{L}_i,$$

Table 1
Comparison with other attacks.

	Oracle	Lattice size	Required k
Plantard-Susilo	uSVP	$(n+2)\times(n+1)$	–
Pan-Zhang	SVP	$(n+k+1)\times(n+1)$	$k\geq 0.9408d$
Our work	BDD	$n\times(n-k)$	$k\geq 3d$
	uSVP	$(n+1)\times(n-k+1)$	

which implies that $\binom{\mathcal{L}}{\mathbf{0}}\subseteq\mathcal{L}'=\bigcap_i\mathcal{L}_i$. Meanwhile, it can be proved that $\binom{\mathcal{L}}{\mathbf{0}_k}\subseteq\mathcal{L}''$ because

$$\begin{bmatrix}\mathbf{B}\mathbf{u}_1+u_2\mathbf{t}\\ u_2\\ \mathbf{0}_k\end{bmatrix}=\begin{bmatrix}\mathbf{I}_n & \frac{1}{2}\mathbf{1}_n\\ \mathbf{0}_n^T & 1\\ N\mathbf{A}_i^T & N\mathbf{s}\end{bmatrix}\begin{bmatrix}\mathbf{B}\mathbf{u}_1-u_2\mathbf{y}\\ u_2\end{bmatrix}\in\mathcal{L}''.$$

These three attacks success only when $(\mathbf{e}^T-\frac{1}{2}\mathbf{1}_n^T,-1,\mathbf{0}^T)^T$ (the dimension of $\mathbf{0}$ depends on the dimension of lattice) is the shortest vector of $\mathcal{L},\mathcal{L}'$ and $\mathcal{L}''$. Together with the above comparison that $\mathcal{L}$ is a sublattice of both $\mathcal{L}'$ and $\mathcal{L}''$, the λ_2-gap of $\mathcal{L}$ is no less than $\mathcal{L}'$ and $\mathcal{L}''$, which means that solving uSVP on $\mathcal{L}$ is easier (at least not harder) than that on $\mathcal{L}'$ and $\mathcal{L}''$.

Pan-Zhang's attack can successfully recover the solution when $k>0.9408d$, while ours requires k to be larger. However, Pan-Zhang's attack relies on an SVP algorithm which is stronger than BDD or uSVP algorithm in general.

We list the difference of these three attacks in Table 1.

3.3. Defense mechanisms against broadcast attacks

Broadcast attacks apply to the scenario that a same plaintext is encrypted under several public keys. Notice that the efficiency of the broadcast attack is closely related to the number of samples. Theorem 3.1 shows that the more instances the attacker obtains, the easier it is to recover the plaintext. Thus restricting the number of recipients receiving the same plaintext (the parameter k) may be a feasible method to defense broadcast attack.

Also, the reusage of a plaintext would lead to insecurity, since the ciphertexts can leak the information about the plaintext in multiple encryptions. An effectual approach would be embedding some nonce into the message in encryption algorithm.

4. Applications to low-weight subset sum problems

In this section, we will discuss the case of low-weight subset sum problems particularly. Low-weight subset sum problems have been used as the foundations of some known cryptographic schemes including Chor–Rivest cryptosystem [11] and Okamoto–Tanaka–Uchiyama(OTU) cryptosystem [26]. Our attacks is applicable to average-case low-weight subset sum problems with certain parameters.

A low-weight subset sum problem is to find a “small” solution to

$$a_1x_2+a_2x_2+\cdots+a_nx_n=s,$$

where a_i's are uniformly selected from $[B]$ and $\sum_{i=1}^n x_i=m$. Usually, we set that $B\geq n^m$ and $m\leq\frac{n}{\log n}$. There are two kinds of encodings

- Binary encoding: $\mathbf{x}\in\{0,1\}^n$, $\sum_{i=1}^n x_i=m$;
- Powerline encoding: $\mathbf{x}\in\mathbb{N}^n$, $\sum_{i=1}^n x_i=m$.

Using our broadcast attack, we can recover the small solution $\mathbf{e}'$ of low-weight subset sum problems from k challenges,

$$\begin{cases}\mathbf{A}\mathbf{e}' & = & \mathbf{s}\\ \langle\mathbf{e}',\mathbf{1}_n\rangle & = & m\end{cases},$$

where $A\sim U([B]^{k\times n})$ for $B\geq n^m$ and $m\leq\frac{n}{\log n}$. We denote by $\mathbf{A}'$ the matrix $\binom{\mathbf{1}_n^T}{\mathbf{A}}$, by $\mathbf{s}'$ the matrix $\binom{m}{\mathbf{s}}$ and by $\mathbf{y}'$ a solution to $\mathbf{A}'\mathbf{x}=\mathbf{s}'$.

For the binary encoding, we set the target vector $\mathbf{t}'=\mathbf{y}'-\frac{1}{2}\mathbf{1}_n$ and reduce the low-weight subset sum problem to a BDD instance $(\mathbf{A}'^{\perp},\mathbf{t}')$ (or corresponding uSVP). For powerline encoding, we reduce it to BDD instance $(\mathbf{A}'^{\perp},\mathbf{y}')$ (or corresponding uSVP) directly.

We ran experiments using LLL algorithm with Lovász parameter 0.9999. The dimension n ranges from 40 to 300 by step 20. As explained in [25], two cases where $m=O\left(\frac{n}{\log n}\right)$ and $m=2^{\log^c n}$ for $c<1$ are worth studying. In our experiments, we set $m=\frac{n}{2\log n}$ and $m=2^{\log^{0.75}n}$ with $B=n^m$ respectively as a moderate choice, and considered these two cases for both

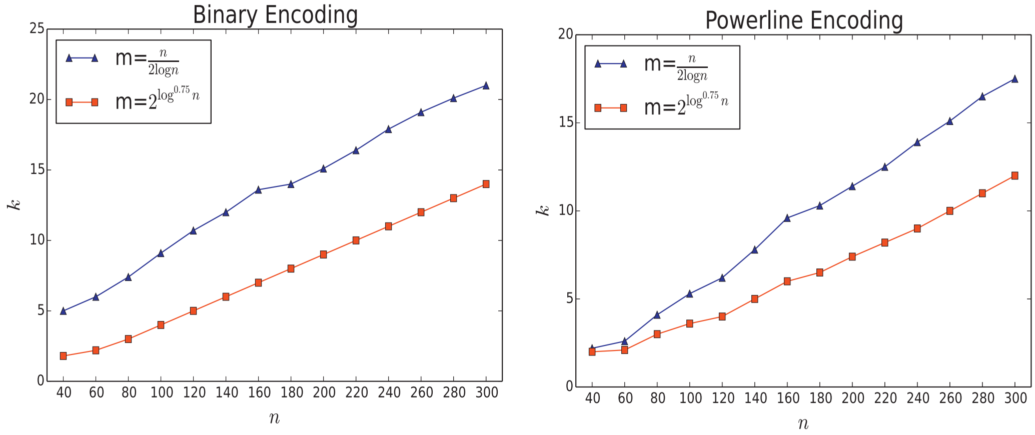

Fig. 2. Practical performance for low-weight subset sum problem.

binary and powerline encodings. For each pair (n, m), we tested 10 sets of random instances and evaluated the average of the minimal k such that our attack succeeded with k challenges.

As shown in Fig. 2, we only require a small number of challenges to recover the solution, which shows the power of our broadcast attack for low-weight subset sum problem. Moreover, it seems that the number of required challenges increases with growing m, which provides a new evidence to support the rationality of replacing usual density ($d = \frac{n}{\log B}$) with pseudo-density for low-weight subset sum problem claimed in [25]. However, we note that the pseudo-density $d = \frac{r \log n}{\log B}$, where r is an upper bound of $\|\mathbf{e}'\|^2$, could not be viewed as the only criterion since in our experiments, these cases of different m's for binary decoding have equal pseudo-densities but diverse hardness.

5. Discussion on modular subset sum problems

In this section, we are to discuss the broadcast attack against modular subset sum problem, which is quite different from original subset sum problem. Given k challenges of modular subset sum problems

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n = & s_1 \bmod q \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n = & s_2 \bmod q \\ & \cdots \\ a_{k,1}x_1 + a_{k,2}x_2 + \cdots + a_{k,n}x_n = & s_k \bmod q \end{cases}$$

where $a_{i,j} \sim U(\mathbb{Z}_q)$ for $q > 0$ and $i \in [k] \backslash \{0\}, j \in [n] \backslash \{0\}$. Let $\mathbf{A}_q = (a_{i,j}) \in \mathbb{Z}_q^{k\times n}$ and $\mathbf{s} = (s_1, \cdots, s_k)$. The goal is to find a solution $\mathbf{e} \in \{0, 1\}^n$ to the equation $\mathbf{A}_q\mathbf{x} = \mathbf{s} \bmod q$. Similarly, we can define the lattice

$$\mathbf{A}_q^{\perp} = \{\mathbf{z} \in \mathbb{Z}^n \mid \mathbf{A}_q\mathbf{z} = \mathbf{0} \bmod q\}.$$

We will reduce the multi-dimensional modular subset sum problem $\mathbf{A}_q\mathbf{x} = \mathbf{s} \bmod q$ to BDD instance $(\mathbf{A}_q^{\perp}, \mathbf{y}_q - \frac{1}{2}\mathbf{1}_n)$ where $\mathbf{y}_q$ is arbitrary solution to $\mathbf{A}_q\mathbf{x} = \mathbf{s} \bmod q$. To this end, we are to take a further study on the lattice $\mathbf{A}_q^{\perp}$.

Lemma 5.1. *Given $\mathbf{z} = (z_1, \cdots, z_n) \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$, we have that*

$$\Pr[\mathbf{z} \in \mathbf{A}_q^{\perp}] = \left(\frac{c}{q}\right)^k,$$

where $\mathbf{A}_q \sim U(\mathbb{Z}_q^{k\times n})$ and $c = \gcd(q, z_1, \cdots, z_n)$.

Proof. We note that given $\mathbf{z} = (z_1, \cdots, z_n) \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ and $c = \gcd(q, z_1, \cdots, z_n)$, the following holds on the randomness of a_i,

$$\Pr_{a_i \sim U(\mathbb{Z}_q)}\left[\sum_{i=1}^{n} a_i z_i = 0 \bmod q\right] = \Pr_{a_i \sim U(\mathbb{Z}_q)}\left[\sum_{i=1}^{n} a_i \frac{z_i}{c} = 0 \bmod \frac{q}{c}\right].$$

Let $q' = q/c$ and $\mathbf{z}' = \mathbf{z}/c$. Using Eq. (2), we may obtain that

$$\Pr_{a_i \sim U(\mathbb{Z}_q)}\left[\sum_{i=1}^{n} a_i z_i' = 0 \bmod q'\right] = \frac{1}{q' \cdot q'^n}\left(\sum_{\mathbf{x}\in\mathbb{Z}_{q'}^n}\sum_{\lambda=0}^{q'-1} \alpha(\lambda\langle\mathbf{x}, \mathbf{z}'\rangle)\right) = \frac{1}{q'}.$$

Since the rows of $\mathbf{A}_q$ are independent, we complete the proof immediately. □

The following result shows a reduction from multi-dimensional modular subset sum problem to BDD.

Theorem 5.2. *There exists an algorithm to find a solution to* $\mathbf{A}_q\mathbf{x} = \mathbf{s} \bmod q$ *for* $\mathbf{x} \in \{0, 1\}^n$ *with probability* $1 - O(\frac{1}{n})$ *via a single call to* $BDD_{1/\gamma}$ *oracle for*

$$0 < \log\gamma \le \frac{k}{d} - \frac{1}{2}\log n + 1$$

where $k \ge \frac{1}{2} d \log n$, $\mathbf{A}_q$ *is uniformly distributed over* $\mathbb{Z}_q^{k\times n}$ *and* $d = \frac{n}{\log q}$ *is the density.*

Proof. Let $\mathbf{y}_q \in \mathbb{Z}^n$ be arbitrary solution to $\mathbf{A}_q\mathbf{x} = \mathbf{s}$ and $\mathbf{t}_q = \mathbf{y}_q - \frac{1}{2}\mathbf{1}_n$. We reduce the multi-dimensional modular subset sum problem to the BDD instance $(\mathbf{A}_q^{\perp}, \mathbf{t}_q)$. It is easy to verify that $\mathrm{dist}(\mathbf{A}_q^{\perp}, \mathbf{t}_q) = \frac{\sqrt{n}}{2}$. Then we will study the first minimum of lattice $\mathbf{A}_q^{\perp}$.

We define $\sigma_k(q, r) = \sum_{c|q, c\le r} c^k$, then for $R < q$ we have

$$\Pr[\lambda_1(\mathbf{A}_q^{\perp}) \le R] \le \sum_{\substack{c\le R\\ c|q}} \left(\frac{c}{q}\right)^k \sum_{l=1}^{\lfloor R^2/c^2 \rfloor} |S(c\sqrt{l}, c)| = \frac{1}{q^k}\sum_{j=1}^{R^2} |S(\sqrt{j}, 1)|\sigma_k\left(q, \frac{R}{\sqrt{j}}\right),$$

where $S(r, c)$ is defined as Eq. (3). There exists a trivial bound for $\sigma_k(q, r)$: $\sigma_k(q, r) \le \sum_{i=1}^{\lfloor r \rfloor} i^k \le r^{k+1}$. Thus, by Lemma 3.6, we can obtain that

$$\Pr[\lambda_1(\mathbf{A}_q^{\perp} \le R)] \le \frac{C}{q^k}\sum_{l=1}^{R^2} l^{\frac{n}{2}-1}\left(\frac{R}{\sqrt{l}}\right)^{k+1} \le \frac{CR^{k+1}}{q^k}\sum_{l=1}^{R^2} l^{\frac{n-k-1}{2}-1},$$

where C is given in Lemma 3.6. When $R \ge \frac{\sqrt{n}}{2}$, it follows that

$$\sum_{l=1}^{R^2} l^{\frac{n-k-1}{2}-1} \le \frac{2}{n-k-1}(R^2+1)^{\frac{n-k-1}{2}} \le \frac{18}{n-k-1}R^{n-k-1}.$$

Hence when $\log R \le \frac{k}{n}\log q \le \frac{k}{d}$, we derive that

$$\Pr[\lambda_1(\mathbf{A}_q^{\perp}) \le R] \le \frac{18CR^n}{(n-k-1)q^k} \le \frac{18C}{n-k-1}.$$

Therefore, when $0 \le \log\gamma \le \frac{k}{d} - \frac{1}{2}\log n + 1$, each call to $\mathrm{BDD}_{1/\gamma}$ oracle may succeed in solving the multi-dimensional modular subset sum problem with probability $\ge 1 - O(\frac{1}{n})$. □

Remark 3. The above result shows a reduction from ISIS (Inhomogeneous Small Integer Solution) to BDD. From another aspect, in a celebrated paper [2], the author gave a worst-case to average-case reduction from SIVP (Shortest Independent Vectors Problem) to SIS. Actually, this does not lead to a direct reduction from SIVP to BDD, because the dimension with respect to SIVP is k but that with respect to BDD is n under similar parameters, *i.e.* $n = \Omega(k\log q)$.

6. Conclusion and future work

We propose a reduction from multi-dimensional subset sum problem to BDD and a practical broadcast attack based on it. Moreover, we apply our method to low-weight subset sum problem and experimentally verify that our attack is quite efficient for suggested parameters.

Our results show some connections among lattice problems of worst-case hardness. It would be interesting to optimize the reduction parameter further. All discussions in this paper focus on generic subset sum problem, thus we leave it as future work to give a detailed cryptanalysis and determine the security parameter of concrete cryptosystems based on our attack. Furthermore, some results may be of independent interest and applicable to general subset sum problems where the solutions are not restricted to $\{0, 1\}^n$.

Acknowledgments

We thank our supervisor Professor Xiaoyun Wang for her guidance and helpful comments. This work was supported by China's 973 Program (grant number 2013CB834205) and National Natural Science Foundation of China (grant number 61502269).

References

[1] L.M. Adleman, On breaking generalized knapsack public key cryptosystems (abstract), in: Proceedings of the 15th Annual ACM Symposium on Theory of Computing, 25–27 April, 1983, Boston, Massachusetts, USA, 1983, pp. 402–412, doi:10.1145/800061.808771.

[2] M. Ajtai, Generating hard instances of lattice problems (extended abstract), in: Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22–24, 1996, 1996, pp. 99–108, doi:10.1145/237814.237838.

[3] M. Ajtai, The shortest vector problem in L_2 is *NP*-hard for randomized reductions (extended abstract), in: Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23–26, 1998, 1998, pp. 10–19, doi:10.1145/276698.276705.

[4] M. Ajtai, C. Dwork, A public-key cryptosystem with worst-case/average-case equivalence, in: Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing, El Paso, Texas, USA, May 4–6, 1997, 1997, pp. 284–293, doi:10.1145/258533.258604.

[5] S. Bai, D. Stehlé, W. Wen, Improved reduction from the bounded distance decoding problem to the unique shortest vector problem in lattices, in: 43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11–15, 2016, Rome, Italy, 2016, pp. 76:1–76:12, doi:10.4230/LIPIcs.ICALP.2016.76.

[6] E.F. Brickell, Solving low density knapsacks, in: Advances in Cryptology, Proceedings of CRYPTO '83, Santa Barbara, California, USA, August 21–24, 1983., 1983, pp. 25–37.

[7] E.F. Brickell, Breaking iterated knapsacks, in: Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19–22, 1984, Proceedings, 1984, pp. 342–358.

[8] M. Castro, B. Liskov, Practical Byzantine fault tolerance and proactive recovery, ACM Trans. Comput. Syst. 20 (4) (2002) 398–461, doi:10.1145/571637.571640.

[9] M. Chaimovich, G. Freiman, Z. Galil, Solving dense subset-sum problems by using analytical number theory, J. Complex. 5 (3) (1989) 271–282, doi:10.1016/0885-064X(89)90025-3.

[10] Y. Chen, P.Q. Nguyen, BKZ 2.0: better lattice security estimates, in: Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4–8, 2011. Proceedings, 2011, pp. 1–20, doi:10.1007/978-3-642-25385-0_1.

[11] B. Chor, R.L. Rivest, A knapsack-type public key cryptosystem based on arithmetic in finite fields, IEEE Trans. Inf. Theory 34 (5) (1988) 901–909, doi:10.1109/18.21214.

[12] M.J. Coster, A. Joux, B.A. LaMacchia, A.M. Odlyzko, C. Schnorr, J. Stern, Improved low-density subset sum algorithms, Comput. Complex. 2 (1992) 111–128, doi:10.1007/BF01201999.

[13] N. Gama, P. Nguyen, Predicting lattice reduction, in: Advances in Cryptology–EUROCRYPT 2008, 2008, pp. 31–51.

[14] N. Gama, P.Q. Nguyen, O. Regev, Lattice enumeration using extreme pruning, in: Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30, - June 3, 2010. Proceedings, 2010, pp. 257–278, doi:10.1007/978-3-642-13190-5_13.

[15] C. Gentry, C. Peikert, V. Vaikuntanathan, Trapdoors for hard lattices and new cryptographic constructions, in: Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17–20, 2008, 2008, pp. 197–206, doi:10.1145/1374376.1374407.

[16] R. Impagliazzo, M. Naor, Efficient cryptographic schemes provably as secure as subset sum, J. Cryptol. 9 (4) (1996) 199–216, doi:10.1007/BF00189260.

[17] A. Joux, J. Stern, Improving the critical density of the Lagarias-Odlyzko attack against subset sum problems, in: Fundamentals of Computation Theory, 8th International Symposium, FCT '91, Gosen, Germany, September 9–13, 1991, Proceedings, 1991, pp. 258–264, doi:10.1007/3-540-54458-5_70.

[18] J.C. Lagarias, A.M. Odlyzko, Solving low-density subset sum problems, in: 24th Annual Symposium on Foundations of Computer Science, Tucson, Arizona, USA, 7–9 November 1983, 1983, pp. 1–10, doi:10.1109/SFCS.1983.70.

[19] V. Lyubashevsky, D. Micciancio, On bounded distance decoding, unique shortest vectors, and the minimum distance problem, in: Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16–20, 2009. Proceedings, 2009, pp. 577–594, doi:10.1007/978-3-642-03356-8_34.

[20] V. Lyubashevsky, A. Palacio, G. Segev, Public-key cryptographic primitives provably as secure as subset sum, in: Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9–11, 2010. Proceedings, 2010, pp. 382–400, doi:10.1007/978-3-642-11799-2_23.

[21] J.E. Mazo, A.M. Odlyzko, Lattice points in high-dimensional spheres, Monatshefte für Mathematik 110 (1) (1990) 47–61.

[22] R.C. Merkle, M.E. Hellman, Hiding information and signatures in trapdoor knapsacks, IEEE Trans. Inf. Theory 24 (5) (1978) 525–530.

[23] L.J. Mordell, On the representation of numbers as the sum of 2r squares, Q. J. Pure Appl. Math. Oxford 48 (1917) 93–104.

[24] P.Q. Nguyen, J. Stern, Merkle-Hellman revisited: a cryptanalysis of the Qu-Vanstone cryptosystem based on group factorizations, in: Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17–21, 1997, Proceedings, 1997, pp. 198–212, doi:10.1007/BFb0052236.

[25] P.Q. Nguyen, J. Stern, Adapting density attacks to low-weight knapsacks, in: Advances in Cryptology - ASIACRYPT 2005, 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4–8, 2005, Proceedings, 2005, pp. 41–58, doi:10.1007/11593447_3.

[26] T. Okamoto, K. Tanaka, S. Uchiyama, Quantum public-key cryptosystems, in: Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20–24, 2000, Proceedings, 2000, pp. 147–165, doi:10.1007/3-540-44598-6_9.

[27] Y. Pan, F. Zhang, Solving low-density multiple subset sum problems with SVP oracle, J. Syst. Science . Complex. 29 (1) (2016) 228–242, doi:10.1007/s11424-015-3324-9.

[28] C. Peikert, Public-key cryptosystems from the worst-case shortest vector problem: extended abstract, in: Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31–June 2, 2009, 2009, pp. 333–342, doi:10.1145/1536414.1536461.

[29] T. Plantard, W. Susilo, Broadcast attacks against lattice-based cryptosystems, in: International Conference on Applied Cryptography and Network Security, Springer, 2009, pp. 456–472.

[30] S. Ramanujan, On certain arithmetical functions, Trans. Cambr. Philos. Soc 22 (9) (1916) 159–184.

[31] O. Regev, New lattice based cryptographic constructions, in: Proceedings of the 35th Annual ACM Symposium on Theory of Computing, June 9–11, 2003, San Diego, CA, USA, 2003, pp. 407–416, doi:10.1145/780542.780603.

[32] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, in: Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22–24, 2005, 2005, pp. 84–93, doi:10.1145/1060590.1060603.

[33] A. Shamir, A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem, IEEE Trans. Inf. Theory 30 (5) (1984) 699–704.

[34] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. 26 (5) (1997) 1484–1509.

[35] P. van Emde Boas, Another NP-complete partition problem and the complexity of computing short vectors in a lattice, Universiteit van Amsterdam. Mathematisch Instituut, 1981.

Yang Yu is a Ph.D. student of Tsinghua University, under the supervision of Professor Xiaoyun Wang. He obtained his bachelor degree from Department of Computer Science and Technology, Tsinghua University. His current research interests focus on lattice reduction algorithm, lattice-based cryptography and public key encryption.

Dianyan Xiao is currently a Ph.D. student of Institute for Advanced Study, Tsinghua University, under the supervision of Professor Xiaoyun Wang. She obtained her bachelor degree from School of Mathematics, Shandong University. Her research interests include (but not limited to) lattice-based cryptography, computational complexity and discrete logarithms.