Broadcast Attacks against Lattice-Based Cryptosystems*

Thomas Plantard and Willy Susilo

Centre for Computer and Information Security Research
School of Computer Science and Software Engineering
University of Wollongong, Australia
{thomaspl,wsusilo}@uow.edu.au

Abstract. In 1988, Håstad proposed the classical broadcast attack against public key cryptosystems. The scenario of a broadcast attack is as follows. A single message is encrypted by the sender directed for several recipients who have different public keys. By observing the ciphertexts only, an attacker can derive the plaintext without requiring any knowledge of any recipient's secret key. Håstad's attack was demonstrated on the RSA algorithm, where low exponents are used. In this paper, we consider the broadcast attack in the lattice-based cryptography, which interestingly has never been studied in the literature. We present a general method to rewrite lattice problems that have the same solution in one unique easier problem. Our method is obtained by intersecting lattices to gather the required knowledge. These problems are used in lattice based cryptography and to model attack on knapsack cryptosystems. In this work, we are able to present some attacks against both lattice and knapsack cryptosystems. Our attacks are heuristics. Nonetheless, these attacks are practical and extremely efficient. Interestingly, the merit of our attacks is not achieved by exploring the weakness of the trapdoor as usually studied in the literature, but we merely concentrate on the problem itself. As a result, our attacks have many security implications on most of the lattice-based or knapsack cryptosystems.

Keywords: Broadcast attack, lattice-based cryptosystem, knapsack cryptosystem, intersecting lattice.

1 Introduction

In 1988, Håstad [1] proposed the first broadcast attack against public key cryptosystems. The attack enables an attacker to recover the plaintext sent by a sender to multiple recipients, without requiring any knowledge of the recipient's secret key. Håstad's attack was originally proposed against the RSA public key cryptosystem that incorporates low exponents. To prevent this classical attack, several researchers have studied the necessity to have a strong security notion in the single user setting in contrast to the multi user setting [2,3]. For instance,

* This work is supported by ARC Discovery Grant DP0663306.

M. Abdalla et al. (Eds.): ACNS 2009, LNCS 5536, pp. 456–472, 2009.

it is well known that to avoid such an attack, paddings (in the random oracle model) will need to be incorporated to achieve the IND-CCA security notion [2,3]. Nevertheless, this type of attacks has never been discussed in the lattice-based scenario.

Our Contribution. In this paper, we revisit the classical broadcast attack and consider it in the lattice-based scenario. Interestingly, this is the first work that considers this type of attack in lattice-based scenario. Our approach is as follows. We present a general method to rewrite lattice problems that have the same solution in one unique easier problem. Our method is obtained by intersecting lattices to gather the required knowledge. These problems are used in lattice based cryptography and to model attack on knapsack cryptosystems. We are able to present some attacks against both lattice and knapsack cryptosystems. Our attacks are heuristics. Nonetheless, these attacks are practical and extremely efficient, as demonstrated in our experiment. We also discuss some countermeasures against such attacks in the context of lattice-based cryptography.

1.1 Related Works

Knapsack Cryptosystems

In 1978 [4], Merkle and Hellman proposed the first public key cryptosystem based on a NP-hard problem, namely the knapsack problem. This is the first practical public key cryptosystem as a positive answer to the proposed seminal notion of public key cryptography by Diffie and Hellman [5]. The knapsack problem is as follows.

Problem 1 (Knapsack). Let $a_1, \ldots, a_n \in \mathbb{N}$ n positive integers and $s \in \mathbb{N}$ a positive integer. The *Knapsack Problem* is to find, if there exists, $\alpha_i \in \{0, 1\}$, $i = 1, \cdots n$, (n Boolean) such that

$$\sum_{i=1}^{n} \alpha_i a_i = s.$$

The problem to find whether there exists such α_i is called the Knapsack Decision Problem.

Theorem 1 (Karp [6]). *The Knapsack Decision Problem is NP-Complete.*

The cryptosystem proposed in [4], and most of other knapsack cryptosystems, can been illustrated as follows.

- **Setup:** Create n integers $a_1, \ldots, a_n$ with a trapdoor function to solve the Knapsack Problem on a_i. Provide $a_1, \ldots, a_n$ as public.
- **Encrypt:** To encrypt a message $m \in [0, 1]^n$, compute

$$s = \sum_{i=1}^{n} m_i a_i.$$

  Publish s as the encrypted message of m.

- **Decrypt:** Use the trapdoor to solve the knapsack problem on $a_1, \ldots, a_n$ and s and extract m.

Merkle-Hellman's first proposition was attacked severely and broken using two different methods: the first attack on the trapdoor itself was proposed by Shamir [7,8] and the second attack on the knapsack problem using lattice theory was proposed by Adleman [9]. In 1985 [10], Lagarias and Odlyzko proposed a general attack against knapsack cryptosystems. Their attack do not incorporate the weakness on the trapdoor itself, rather than only using the fact that the knapsack problems produced are generally weaker that a random one. This weakness appears in a lower density of the knapsack problem. The density of a knapsack problem is defined as

$$d = \frac{n}{max_{i=1}^{n} \log_2 a_i}.$$

Density represents a trade-off between the need to be able to decrypt (and hence, to have a unique solution) using a low density and an acceptable security level using a bigger density. A lot of improvements have be made in order to attack lower density knapsack [11,12,13,14]. For instance, in [12], the authors successfully cryptanalyzed knapsack cryptosystems with density less than 0.9408. These low density attacks use lattice reduction tools. However, some improvements of knapsack cryptosystems were also proposed (e.g. [15,16]) with a bigger density, generally close to 1. We refer the reader to [17] for these two faces of knapsack cryptology. Nonetheless, as mentioned in [18], the knapsack cryptosystem proposed by Okamoto, Tanaka and Uchiyama in 2000 [16] seems to be the only remaining secure knapsack cryptosystem.

Lattice-based cryptosystems

In 1997, Ajtai and Dwork [19] proposed the first lattice cryptosystem where its security is based on a variant of the Shortest Vector Problem (SVP). This cryptosystem received wide attention due to a surprising security proof based on worst-case assumptions. Nonetheless, this cryptosystem is merely a theoretical proposition and it cannot be used in practice. Furthermore, Nguyen and Stern presented a heuristic attack against this cryptosystem [20]. Until then, this initial proposition has been improved [21,22,23] and inspiring for other cryptosystems based on SVP [24,25,26]. The main drawback in these cryptosystems is a huge extension factor between the initial message and its encrypted version.

In 1996, Goldreich, Goldwasser and Halevi (GGH) [27] proposed an efficient way to use lattice theory to build a cryptosystem inspired by McEliece cryptosystem [28] and based on the Closest Vector Problem (CVP). Their practical proposition of a cryptosystem was attacked and broken severely by Nguyen in 1999 [29]. However, the general idea is still viable. Until then, the other propositions were made using the same principle [30,31,32].

In the following, we briefly review the GGH cryptosystem. A GGH cryptosystem comprises of the following algorithms.

- **Setup:** Compute a "good basis" A and a "bad basis" B of a lattice $\mathcal{L}$,

$$\mathcal{L}(A) = \mathcal{L}(B).$$

  Provide B as public and keep A secret.
- **Encrypt:** To encrypt a vector-message m: use the bad basis to create a random vector r of $\mathcal{L}$. Publish the encrypted message which is the addition of the vector message with the random vector:

$$c = m + r.$$

- **Decrypt:** Use the good basis to find the closest vector in the lattice of the encrypted message c. The closest vector of the encrypted message c is the random vector r[1]. Subtract the random vector of the encrypted message to obtain the vector message m.

Remark 1. In their initial paper [27], Goldreich, Goldwasser and Halevi also proposed another cryptosystem where the message is transformed into a lattice point prior to adding to it a random vector noise.

The important points for the security and efficiency of those cryptosystems are defined as follows.

i) It is easy to compute a "bad basis" from a "good basis", but it is difficult to compute a "good basis" from a "bad basis".
ii) It is easy to create a random vector of a lattice even with a "bad basis".
iii) It is easy to find the closest vector with a "good basis" but difficult to do so with a "bad basis".

After the first Nguyen's attack [29], utilization of the initial GGH proposition requires lattice with big dimension (> 500), to ensure its security. Nonetheless, the computation of the closest vector even with a "good basis" becomes very expensive. In 2000, Fischlin and Seifert [30] proposed a very intuitive way to build lattice with good basis which are able to solve the closest vector problem. They used a tensor product of lattice to obtain a divide and conquer approach to solve CVP. In 2001, Micciancio [31] proposed some major improvements of the speed and the security of GGH. In this scheme, the public key uses a Hermite Normal Form (HNF) for the bad basis. The HNF basis is better to answer the inclusion question and it also seems to be more difficult to transform to a "good basis" compared to another basis. In 2003, Paeng, Jung and Ha [32] proposed to use some lattices build on polynomial ring. However, in 2007, Han, Kim, and Yeom [33] used lattice reduction to cryptanalysis this scheme. Their attack can successfully recover the secret key even in a huge dimension (> 1000) and make the PJH scheme unusable. However, there exists a secure (and yet 'unbroken') cryptosystem using polynomial representation, namely the NTRU cryptosystem, for N^{th} degree truncated polynomial ring units. NTRU was originally proposed in 1998 by Hoffstein, Pipher and Silverman [34]. Even if this cryptosystem was not modelled initially as a GGH-type cryptosystem, it can actually be represented as one. This has been useful specially for analysing its security [35].

[1] Under the supposition that the norm of m is sufficiently small.

Organization of the Paper

The rest of this paper is organized as follows. In the next section, we recall some basic concepts of lattice theory. Section 3 presents the main theorem which is how to intersect lattices to simplify lattice problems. Some practical attacks inspired by this main theorem are proposed in Section 4. Section 5 presents some test results. We conclude the paper in Section 6 by presenting some solutions against these new broadcast attacks.

2 Lattice Theory

In this section, we will review some concepts of the lattice theory useful for the comprehension of this paper. For a more complex account, we refer the readers to [36].

The lattice theory, also known as the geometry of numbers, has been introduced by Minkowski in 1896 [37]. A complete discussion on the basic of lattice theory can be found from [38,39,40].

Definition 1 (Lattice). *A lattice $\mathcal{L}$ is a discrete sub-group of $\mathbb{R}^n$, or equivalently the set of all the integral combinations of $d \leq n$ linearly independent vectors over $\mathbb{R}$.*

$$\mathcal{L} = \mathbb{Z}\, b_1 + \cdots + \mathbb{Z}\, b_d, \quad b_i \in \mathbb{R}^n.$$

$B = (b_1, ..., b_d)$ is called a basis of $\mathcal{L}$ and d, the dimension of $\mathcal{L}$, noted $dim(\mathcal{L})$.
We will refer $\mathcal{L}(B)$ as a lattice of basis B.
We will represent a lattice basis by a matrix $B \in \mathbb{R}^{d,n}$ where each rows $B[i]$ of B correspond to a vector b_i of the basis.

Theorem 2 (Determinant). *Let $\mathcal{L}$ a lattice. There exists a real value, denoted as $\det \mathcal{L}$, such that for any basis B, we have*

$$\det \mathcal{L} = \sqrt{\det (BB^T)}.$$

$\det \mathcal{L}$ is called the determinant of $\mathcal{L}$.

For a given lattice $\mathcal{L}$, there exists an infinity of basis. However, the Hermite Normal Form basis (Definition 2) is unique [41].

Definition 2 (HNF). *Let $\mathcal{L}$ a integer lattice of dimension d and $H \in \mathbb{Z}^{d,n}$ a basis of $\mathcal{L}$. H is a Hermite Normal Form basis of $\mathcal{L}$ if and only if*

$$\forall 1 \leq i, j \leq d \quad H_{i,j} \begin{cases} = 0 & \text{if } i > j \\ \geq 0 & \text{if } i \leq j \\ < H_{j,j} & \text{if } i < j \end{cases}$$

The HNF basis can be computed from a given basis in a polynomial time [42]. For efficient solutions, we refer the readers to [43].

Remark 2. As it was remarked by [31], the HNF basis is a "good basis" for solving the problem of inclusion of a vector in a lattice [41] or more generally finding a basis of a lattice from a set of non-independent vectors generating this lattice [36].

Intersecting lattice is the main tool used in this paper. Lattices intersection can easily be done using dual lattices (Definition 3).

Definition 3 (Dual). *Let $\mathcal{L}$ a lattice and B a basis of $\mathcal{L}$. Then, $\mathcal{L}^*$ is noted as the dual lattice of $\mathcal{L}$ and $(BB^T)^{-1}B$ is a basis of $\mathcal{L}^*$*[2].

Property 1 (Intersection). Let $\mathcal{L}_1, \mathcal{L}_2$ two lattices. Then,

$$\mathcal{L}_1 \cap \mathcal{L}_2 = (\mathcal{L}_1^* \cup \mathcal{L}_2^*)^* .$$

As $\mathcal{L}_1 \subseteq \mathcal{L} = \mathcal{L}_1 \cap \mathcal{L}_2$, $\mathcal{L}_1$ is called a sublattice of $\mathcal{L}$.

Remark 3 (Union). The lattice union of two lattices is generated by the set of vectors composed by the union of the two sets of vector of each basis. As remark before (Remark 2), using HNF for example, we can build from this set of non-independent vector, a basis.

The lattice theory problem is based on distance minimization. The natural norm used in lattice theory is the euclidean norm.

Definition 4 (Euclidean norm). *Let w a vector of $\mathbb{R}^n$. The euclidean norm is the function $\|.\|$ defined by*

$$\begin{aligned} \|w\| &= \sqrt{< w, w >} \\ &= \sqrt{ww^T} \\ &= \sqrt{\textstyle\sum_{i=1}^{n} w_i^2} \end{aligned}$$

Using a norm, we can define some other invariants crucial in lattice theory.

Definition 5 (Successive Minima). *Let $\mathcal{L}$ a lattice and $i \in \mathbb{N}$ an integer. The i^{th} Successive Minima, noted $\lambda_i(\mathcal{L})$ is the smallest real number such there exist i non-zero linear independent vector $v_1, \ldots, v_i \in \mathcal{L}$ with*

$$\|v_1\|, \ldots, \|v_i\| \leq \lambda_i(\mathcal{L}).$$

The problem to find such a vector v_1 is called the Shortest Vector Problem (SVP).

Theorem 3 (Ajtai [44]). *SVP is NP-Hard under randomized reductions.*

Another important invariant is the Hermite invariant which is defined as follows.

[2] This definition of the duality is extremely practical and doesn't represent the full interest of this notion. However, we will only focus on notion needed for the understanding of this paper.

Definition 6 (Hermite Invariant). *Let $\mathcal{L}$ a lattice. The Hermite invariant, denoted as $\gamma(\mathcal{L})$, is the real number such that*

$$\gamma(\mathcal{L}) = \left(\frac{\lambda_1(\mathcal{L})}{\det(\mathcal{L})^{1/dim(\mathcal{L})}}\right)^2.$$

There exist two extremely useful properties around this invariant.

Theorem 4 (Minkowski [37]). *For any lattice $\mathcal{L}$ of dimension d,*

$$\gamma(\mathcal{L}) \leq 1 + \frac{d}{4}.$$

The second theorem provides a general property which concerns random lattices.

Theorem 5 (Ajtai [45]). *Let $\mathcal{L}$ a random lattice of dimension d. Then,*

$$\frac{\lambda_i(\mathcal{L})}{\det(\mathcal{L})^{1/d}} \simeq \sqrt{\frac{d}{2\pi e}}.$$

Corollary 1. *Let $\mathcal{L}$ a random lattice of dimension d. Then,*

$$\gamma(\mathcal{L}) \simeq \frac{d}{2\pi e}.$$

Random lattice is a complex notion [46,47,45]. Goldstein and Mayer's characterization of random lattices [47] allows to create random lattices for experiment for example [48]. We will use the same method in our practical section (Section 5) to evaluate our method in the case of random lattices.

Remark 4. Hermite invariant is a way to evaluate the weakness of a lattice. If the value is smaller than the average $\frac{d}{2\pi e}$ on a lattice, then it will be "easier" to solve SVP or other related problem on it.

Another useful invariant is the lattice gap defined in [49] for practical reason.

Definition 7 (Lattice Gap). *Let $\mathcal{L}$ a lattice. The gap, noted $\alpha(\mathcal{L})$, is the real number such that*

$$\alpha(\mathcal{L}) = \frac{\lambda_2(\mathcal{L})}{\lambda_1(\mathcal{L})}.$$

Remark 5 (Unicity). To assure unicity of the solution and hence, removing the decryption failure, lattice-based cryptosystems generally use gap of at least $\alpha(\mathcal{L}) > 2$. Moreover, generally the gap of lattice used in cryptosystems are polynomial in its dimension.

Remark 6. As Hermite invariant is used to evaluate the resistance of a lattice, the bigger the gap of a lattice, the easier it will be practically to solve SVP or other problem on it. For a recent analysis of practical attacks against lattice with a big gap, please refer to [50].

As SVP is NP-hard, a relaxation factor has been introduced in the initial SVP to be able to propose and evaluate the quality of the polynomial algorithms.

Problem 2 (γ-SVP). Let $\mathcal{L}$ a lattice and $\gamma \geq 1$ a real positive number. Then, the γ-*SVP* is to find a vector $u \in \mathcal{L}$ such that

$$0 < \|u\| \leq \gamma \lambda_1.$$

In 1982 [51], Lenstra, Lenstra and Lovasz proposed a powerful algorithm which have a time complexity polynomial in the dimension d . It is known as the LLL algorithm and this algorithm returns a solution for $\gamma-$SVP for $\gamma = 2^{\frac{d-1}{2}}$ where $d = dim(\mathcal{L})$[3]. This property leads to break cryptosystems using lattice with gap bigger than $2^{\frac{d-1}{2}}$. However, in practice, LLL seems to be much more efficient [48]. In addition, a lot of improvements have been proposed on LLL to obtain a better approximation factor and/or a better time complexity. For the recent result on LLL, we refer the readers to [52,53].

A second category of lattice problems are based on different values that the successive minima.

Definition 8 (Minimum Distance). *Let $\mathcal{L}$ a lattice and u a vector. The Minimum Distance of u to $\mathcal{L}$, denoted as $dist(u, \mathcal{L})$ is the smallest real number such that there exists a vector $v \in \mathcal{L}$ with $\|u - v\| = dist(u, \mathcal{L})$. The problem to find such a vector v is known as the Closest Vector Problem (CVP).*

Theorem 6 (Emde Boas, [54]). *CVP is NP-Hard.*

As for SVP, CVP has a relaxed version as defined as follows.

Problem 3 (γ-CVP). Let $\mathcal{L}$ a lattice, w a vector and $\gamma \geq 1$ a real positive number. The γ-*CVP* is to find a vector $u \in \mathcal{L}, \|w - u\| \leq \gamma dist(u, \mathcal{L})$.

In 1986, Babai [55] proposed two polynomial methods to solve $\gamma-$CVP: the *nearest plane* and the *round-off* methods. Those algorithms solve γ-CVP within $\gamma = 2^{\frac{d}{2}}$ and $\gamma = 1+2d\left(\frac{9}{2}\right)^{\frac{d}{2}}$, respectively. Babai's algorithms use an LLL-reduced basis. Consequently all the variants of LLL, including BKZ utilization [56] proposed by Schnorr, are naturally the improvement of Babai's methods.

Moreover, there exists an heuristic way introduced by Kannan [57] to directly solve γ-CVP using algorithm made to solve γ-SVP: the *embedding method* . Instead of solving γ-CVP, we solve γ-SVP in a different lattice. Finding the closest vector of v in $\mathcal{L}(B)$ can be done by solving the shortest vector of $\mathcal{L}(B')$ with $B' = \begin{pmatrix} B & 0 \\ v & 1 \end{pmatrix}$. This method has been successfully used by Nguyen [29] for constructing his first attack against GGH cryptosystem and it seems practically the best way to attack a CVP-based cryptosystem.

[3] With $\delta = 0.75$ for LLL utilization parameter.

3 Intersecting Lattices

Each attack proposed in this paper is inspired by a new general simplification method of lattice problems.

Theorem 7. *Let $\mathcal{L}_1, \mathcal{L}_2$ two lattices and v a vector such that v is a shortest vector of both $\mathcal{L}_1$ and $\mathcal{L}_2$. Then, v is a shortest vector of the lattice $\mathcal{L}_1 \cap \mathcal{L}_2$,*

$$\gamma(\mathcal{L}_1 \cap \mathcal{L}_2) \leq \gamma(\mathcal{L}_1), \gamma(\mathcal{L}_2)$$
$$\textit{and}$$
$$\alpha(\mathcal{L}_1 \cap \mathcal{L}_2) \geq \alpha(\mathcal{L}_1), \alpha(\mathcal{L}_2).$$

Proof.

We prove that v is the shortest vector of $\mathcal{L}_1 \cap \mathcal{L}_2$.

As $v \in \mathcal{L}_1, \mathcal{L}_2$, we have $v \in \mathcal{L}_1 \cap \mathcal{L}_2$. Suppose that there exists a non-zero vector $v' \in \mathcal{L}_1 \cap \mathcal{L}_2$ such that $0 < \|v'\| < \|v\|$. As $v' \in \mathcal{L}_1 \cap \mathcal{L}_2$, we have $v' \in \mathcal{L}_1$ with $0 < \|v'\| < \|v\|$, which is impossible as v is the shortest non-zero vector of $\mathcal{L}_1$. We have proved that for any non-zero vector $v' \in \mathcal{L}_1 \cap \mathcal{L}_2, \|v\| \leq \|v'\|$: v is the shortest vector of $\mathcal{L}_1 \cap \mathcal{L}_2$.

We prove that $\gamma(\mathcal{L}_1 \cap \mathcal{L}_2) \leq \gamma(\mathcal{L}_1)$.

Let's compare $\gamma(\mathcal{L}_1 \cap \mathcal{L}_2)$ with $\gamma(\mathcal{L}_1)$. We have proved that $\lambda_1(\mathcal{L}_1 \cap \mathcal{L}_2) = \|v\| = \lambda_1(\mathcal{L}_1)$. As $\mathcal{L}_1 \cap \mathcal{L}_2 \subseteq \mathcal{L}_1$, we have $\dim(\mathcal{L}_1 \cap \mathcal{L}_2) \leq \dim(\mathcal{L}_1)$ and $\det(\mathcal{L}_1 \cap \mathcal{L}_2) \geq \det(\mathcal{L}_1)$. We obtain

$$\gamma(\mathcal{L}_1 \cap \mathcal{L}_2) = \left(\frac{\lambda_1(\mathcal{L}_1 \cap \mathcal{L}_2)}{\det(\mathcal{L}_1 \cap \mathcal{L}_2)^{1/dim(\mathcal{L}_1 \cap \mathcal{L}_2)}}\right)^2 \leq \left(\frac{\lambda_1(\mathcal{L}_1)}{\det(\mathcal{L}_1)^{1/dim(\mathcal{L}_1)}}\right)^2 = \gamma(\mathcal{L}_1).$$

The same proof can be performed with $\mathcal{L}_2$, and consequently, we obtain $\gamma(\mathcal{L}_1 \cap \mathcal{L}_2) \leq \gamma(\mathcal{L}_1), \gamma(\mathcal{L}_2)$.

We prove that $\alpha(\mathcal{L}_1 \cap \mathcal{L}_2) \geq \alpha(\mathcal{L}_1)$.

Let's compare $\alpha(\mathcal{L}_1 \cap \mathcal{L}_2)$ with $\alpha(\mathcal{L}_1)$. We have proved that $\lambda_1(\mathcal{L}_1 \cap \mathcal{L}_2) = \|v\| = \lambda_1(\mathcal{L}_1)$. Suppose that we have two independent vectors $v_1, v_2 \in \mathcal{L}_1 \cap \mathcal{L}_2$ such that $max(\|v_1\|, \|v_2\|) = \lambda_2(\mathcal{L}_1 \cap \mathcal{L}_2)$. Then, since v_1, v_2 are also two independent vectors of $\mathcal{L}_1$, we obtain $\lambda_2(\mathcal{L}_1) \leq max(\|v_1\|, \|v_2\|)$. We have $\lambda_2(\mathcal{L}_1) \leq max(\|v_1\|, \|v_2\|) = \lambda_2(\mathcal{L}_1 \cap \mathcal{L}_2)$. Finally, we obtain

$$\alpha(\mathcal{L}_1 \cap \mathcal{L}_2) = \left(\frac{\lambda_2(\mathcal{L}_1 \cap \mathcal{L}_2)}{\lambda_1(\mathcal{L}_1 \cap \mathcal{L}_2)}\right) \geq \left(\frac{\lambda_2(\mathcal{L}_1)}{\lambda_1(\mathcal{L}_1)}\right) = \alpha(\mathcal{L}_1).$$

The same proof can be performed with $\mathcal{L}_2$, and consequently, we obtain $\alpha(\mathcal{L}_1 \cap \mathcal{L}_2) \geq \alpha(\mathcal{L}_1), \alpha(\mathcal{L}_2)$. □

Theorem 7 is crucial as it demonstrates that to solve the shortest vector problem on the intersection of lattices will be at least easier that in the initial lattice. We

will see in Section 5 that practical problems become a lot easier. Nevertheless, the practical efficiency can not be shown in a general theorem as Theorem 7. This is simply because if $\mathcal{L}_1 = \mathcal{L}_2$, we obtain $\mathcal{L}_1 \cap \mathcal{L}_2 = \mathcal{L}_1 = \mathcal{L}_2$,

$$\gamma(\mathcal{L}_1 \cap \mathcal{L}_2) = \gamma(\mathcal{L}_1) = \gamma(\mathcal{L}_2)$$
and
$$\alpha(\mathcal{L}_1 \cap \mathcal{L}_2) = \alpha(\mathcal{L}_1) = \alpha(\mathcal{L}_2).$$

Remark 7. For cryptosystems based on CVP, we will use the embedding method to model as a SVP before applying Theorem 7.

4 Practical Broadcast Attacks

In this section, we adapt the general method (Theorem 7) to different lattice or knapsack cryptosystems. For convenience, we will always firstly recall the 'challenge' in the cryptosystem involved followed by our proposed attack. All of our attacks are heuristic.

4.1 A Broadcast Attack on GGH Type A

Problem 4 (GGH$_A$ Challenge). Let $B \in \mathbb{Z}^{n,n}$ a basis and $c \in \mathbb{Z}^n$ a vector such that there exist two vectors $r, m \in \mathbb{Z}^n$ with $c = rB + m$. Then, the GGH$_A$ challenge (B, c) is to find m.

Algorithm 1. Broadcast Attack on GGH$_A$ Challenges

Input : (B_i, c_i) k GGH$_A$ challenges.
Output: $m \in \mathbb{Z}^n$.
begin
  Compute $B'_i = \begin{pmatrix} B_i & 0 \\ c_i & 1 \end{pmatrix}$.
  Compute $\mathcal{L} = \bigcap_{i=1}^{k} \mathcal{L}(B'_i)$.
  Find $\begin{pmatrix} m & 1 \end{pmatrix}$ shortest vector of $\mathcal{L}$.
end

Example 1. The initial proposition in [27] is obviously concerned by this attack. However, we will refer to Micciancio cryptosystems [31] as a non-broken cryptosystem that will also be susceptible against this attack.

4.2 A Broadcast Attack on GGH Type B

Problem 5 (GGH$_B$ Challenge). Let $B \in \mathbb{Z}^{n,n}$ a basis and $c \in \mathbb{Z}^n$ a vector such that there exist two vectors $m, r \in \mathbb{Z}^n$ with $c = mB + r$. Then, the GGH$_B$ challenge (B, c) is to find m.

The idea here is a bit different. As we have $mB_1+r_1 = c_1$ and $mB_2+r_2 = c_2$, we construct a third challenge $mB_3+r_3 = c_3$ with $B_3 = B_1+B_2$ and $c_3 = c_1+c_2$. Practically, the fact that $\|r\|$ grows will be less important than the growth of B.

Algorithm 2. Broadcast Attack on GGH_B Challenges

Input : (B_i, c_i) k GGH_B challenges.
Output: $m \in \mathbb{Z}^n$.
begin
  Compute $B = \sum_{i=1}^{k} B_i$.
  Compute $c = \sum_{i=1}^{k} c_i$.
  Find the closest vector v of c in $\mathcal{L}(B)$.
  Compute $m = vB^{-1}$.
end

Algorithm 2 do not use Theorem 7 and cannot be proved to have a simpler problem as the $\lambda_1(\mathcal{L}(B_1 + B_2))$ can be bigger than $\lambda_1(\mathcal{L}(B_1))$. However, we will see than practically $\lambda_1(\mathcal{L}(B_1 + B_2))$ will be bigger. Practically, we will also use the embedding method for the third step of Algorithm 2.

Example 2. Cryptosystems concerned with this attack include [30] and the more recent work of [32].

4.3 A First Broadcast Attack on Knapsack Cryptosystems

Problem 6 (Knapsack Challenge). Let $a \in \mathbb{N}^n$ a positive integer vector and $s \in \mathbb{N}$ an integer such that there exists $m \in [0,1]^n$ a boolean vector such $ma^T = s$. Then, the Knapsack challenge (a, s) is to find m.

The attack proposed here is an adaptation of Algorithm 1 to the knapsack challenge as it has been already modelled by [10] in a lattice problem. Other modellings can been also adapted with the same technique.

Algorithm 3. Broadcast Attack on Knapsack Challenge

Input : (a_i, s_i) k knapsack challenges.
Output: $m \in [0,1]^n$.
begin
  Compute $B_i = \begin{pmatrix} Id & a_i^T & 0 \\ 0 & s & 1 \end{pmatrix}$.
  Compute $\mathcal{L} = \bigcap_{i=1}^{k} \mathcal{L}(B_i)$.
  Find $\begin{pmatrix} m & 0 & 1 \end{pmatrix}$ shortest vector of $\mathcal{L}$.
end

Example 3. The examples of practical schemes that are susceptible against our attack are as follows. We refer to the survey of Odlysko [17] for knapsack cryptosystems that are susceptible against this attack. However, we also refer to [16]

for one of the 'rare' non-broken knapsack cryptosystems that are also susceptible against this attack. The recent proposition of [58] is also concerned.

Remark 8. We remark that the dimension of $\mathcal{L}$ decreases further when k increases. Practically, we have $\dim(\mathcal{L}) = n - k$ with a high probability[4]. It is because each $\mathcal{L}(B_i)$ have a dimension smaller than n, $\dim(\mathcal{L}(B_i)) = n - 1$. This decrease will obviously stop at a dimension of 1 with a lattice of a basis only composed by $\begin{pmatrix} m & 0 & 1 \end{pmatrix}$.

4.4 A Second Broadcast Attack on Knapsack Cryptosystems

Inspired by the previous remark (Remark 8), we notice that if we have n equations $ma_i^T = s_i$, we can concatenate these equations to obtain $mA = s$ with $A \in \mathbb{Z}^{n,n}$ and $s \in \mathbb{Z}^n$. Moreover, these equations can be solved with high probability.

Algorithm 4. Broadcast Attack on Knapsack Challenges without Lattice Reduction

Input : (a_i, s_i) n knapsack challenges.
Output: $m \in [0, 1]^n$.
begin
  Compute $A = \begin{pmatrix} a_1^T & \dots & a_n^T \end{pmatrix}$.
  Compute $s = \begin{pmatrix} s_1 & \dots & s_n \end{pmatrix}$.
  Compute $m = sA^{-1}$.
end

The main advantage of our second attack is to avoid the use of any lattice reduction. The impact of this gain will enable us to use the attack in a huge dimension where the use of LLL will be computationally expensive. However, its drawback is the number of challenge required. The first attack will require practically less challenges to reveal the plaintext.

This method is also heuristic as A can be singular [5] and A^{-1} does not exist. However, probability of such a situation is extremely low and will be less probable with more knapsack challenges.

5 Practical Result

In this section, we present result of the previously presented techniques to attack different lattice-based cryptosystems. To perform these attacks, we use the embedding method with a lattice reduction done with LLL[6]. Cryptosystems and attacks were implemented under the MAGMA library [59]. Tests were made 20 times, for each 10 dimensions between 10 and 300. For each test, a random

[4] Under the probability that $\forall 1 \leq i_1, i_2 \leq k, 1 \leq j \leq n, a_{i_1}[j] \neq a_{i_2}[j]$.
[5] $det(A) = 0$.
[6] With $\delta = 0.9999$ for LLL utilization parameter.

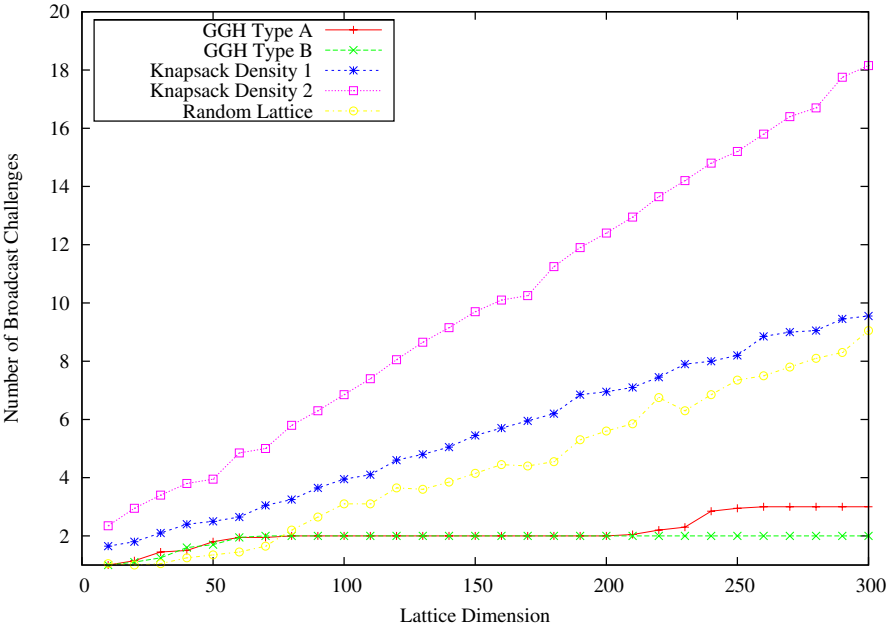

Fig. 1. Number of needed broadcast challenges to extract message from different cryptosystems

message is encrypted with a different random public basis repetitively until the attack is successful. Cryptosystems are implemented as close as possible to the initial paper. The list of different cryptosystems analyzed is as follows:

1. The initial GGH cryptosystem (Type A) attacked with Algorithm 1.
2. The second GGH cryptosystem (Type B) attacked with Algorithm 2.
3. A knapsack problem of density 1.0. This problem does not correspond to a real cryptosystem but to any knapsack cryptosystem which use such a problem. This attack is more general that the previous ones.
4. A knapsack problem of density 2.0. This problem is an extreme case. As we do not know if some trapdoor functions can be created for such a problem, for instance due to the reason of unicity. However, it gives us a security bound as problems with lower density will be easier to attack.
5. A random lattice CVP problem. This problem is the one which gives us a reference. For this one, we have created random lattice and a vector with $dist \sim \frac{\lambda_1}{2}$ to assure that at least the existence of a decryption algorithm. To create a random lattice, we use the same technique proposed in [48,50] using the results on random lattice from [47]. This problem corresponds to the general situation to a lattice-based cryptosystem which have the possibility to decrypt even if some trapdoors may not exist. This problem corresponds to a security upper bound for CVP based cryptosystems.

The purpose of those tests is not to give some security parameter bounds (as more powerfull SVP solver can be used than LLL, BKZ for example) but to show how

evolves the difficulty of those problems with more and more challenges. Figure 1 summarizes our results.

6 Conclusion and Countermeasures

In this paper, we proposed an efficient way to simplify lattice problems which have the same solution. This technique leads to some heuristic and efficient attacks on the existing lattice or knapsack cryptosystems. However, some lattice-based cryptosystems naturally resist to those attacks. Ajtai-Dwork cryptosystem [19] and its different improvements, such as [21,22,23] or [24,25,26], are not concerned by our attacks. This is clearly due to the huge extension factor which allows those cryptosystems to put a strong part of random and hence, there is no common vector. For the same reason, the proposition of knapsack-based probabilistic encryption of [60] will be naturally resistant as well. In the same direction, we remark that after some tests, NTRU lattices should be extremely weak against intersecting lattices. However, the fact that half of its message is random leads to a complete protection against broadcast attacks. Those remarks inspired an obvious countermeasure. Concerned cryptosystems have just to add to their messages a random part (e.g. a hash of the public key itself) that is sufficiently big to prevent two messages to be equal under a reasonable probability. This is inline with the direction suggested in the traditional cryptography (e.g. [2,3]) to ensure the security in the IND-CCA sense. The cost of such counter measure is an expansion factor which have repercussion in both space and time complexity. If the solution was known before, the utility of such counter measure was never shown to be necessary. This is the result of this work. Nonetheless, if the solution is 'simple', some further techniques should be incorporated as for cryptosystems which resist to LLL attacks with two messages, after intersection even of only two messages, the new problem will be easier compared to the original problem.

Intersecting lattice has shown to be interesting to perform cryptanalysis. However, we believe that those kind of techniques can also lead to constructive utilization as original from other techniques used generally in cryptography.

References

1. Håstad, J.: Solving simultaneous modular equations of low degree. SIAM J. Comput. 17, 336–341 (1988)
2. Bellare, M., Boldyreva, A., Micali, S.: Public-key encryption in a multi-user setting: Security proofs and improvements. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 259–274. Springer, Heidelberg (2000)
3. Baudron, O., Pointcheval, D., Stern, J.: Extended notions of security for multicast public key cryptosystems. In: Welzl, E., Montanari, U., Rolim, J.D.P. (eds.) ICALP 2000. LNCS, vol. 1853, pp. 499–511. Springer, Heidelberg (2000)
4. Merkle, R.C., Hellman, M.E.: Hiding information and signatures in trapdoor knapsacks. IEEE Transactions on Information Theory IT-24, 525–530 (1978)

5. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Transactions on Information Theory IT-22, 644–654 (1976)
6. Karp, K.M.: Reducibility among combinatorial problems. Complexity of Computer Computations (1972)
7. Shamir, A.: A polynomial time algorithm for breaking the basic merkle-hellman cryptosystem. In: CRYPTO, pp. 279–288 (1982)
8. Shamir, A.: A polynomial-time algorithm for breaking the basic merkle-hellman cryptosystem. IEEE Transactions on Information Theory 30, 699–704 (1984)
9. Adleman, L.M.: On breaking generalized knapsack public key cryptosystems (abstract). In: STOC, pp. 402–412 (1983)
10. Lagarias, J.C., Odlyzko, A.M.: Solving low-density subset sum problems. Journal of the ACM 32, 229–246 (1985)
11. Coster, M.J., LaMacchia, B.A., Odlyzko, A.M.: An improved low-density subset sum algorithm. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 54–67. Springer, Heidelberg (1991)
12. Coster, M.J., Joux, A., LaMacchia, B.A., Odlyzko, A.M., Schnorr, C.P., Stern, J.: Improved low-density subset sum algorithms. Computational Complexity 2, 111–128 (1992)
13. Schnorr, C.-P., Hörner, H.H.: Attacking the chor-rivest cryptosystem by improved lattice reduction. In: Guillou, L.C., Quisquater, J.-J. (eds.) EUROCRYPT 1995. LNCS, vol. 921, pp. 1–12. Springer, Heidelberg (1995)
14. Omura, K., Tanaka, K.: Density attack to the knapsack cryptosystems with enumerative source encoding. IEICE Trans. Fundam. Electron Commun. Comput. Sci. 87, 1564–1569 (2004)
15. Chor, B., Rivest, R.L.: A knapsack-type public key cryptosystem based on arithmetic in finite fields. IEEE Transactions on Information Theory 34, 901–909 (1988)
16. Okamoto, T., Tanaka, K., Uchiyama, S.: Quantum public-key cryptosystems. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 147–165. Springer, Heidelberg (2000)
17. Odlyzko, A.M.: The rise and fall of knapsack cryptosystems. Cryptology and Computational Number Theory 42, 75–88 (1990)
18. Nguyen, P.Q., Stern, J.: Adapting density attacks to low-weight knapsacks. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 41–58. Springer, Heidelberg (2005)
19. Ajtai, M., Dwork, C.: A public-key cryptosystem with worst-case/average-case equivalence. In: Twenty-Ninth Annual ACM Symposium on the Theory of Computing (STOC 1997), pp. 284–293 (1997)
20. Nguyen, P.Q., Stern, J.: Cryptanalysis of the ajtai-dwork cryptosystem. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 223–242. Springer, Heidelberg (1998)
21. Goldreich, O., Goldwasser, S., Halevi, S.: Eliminating decryption errors in the ajtai-dwork cryptosystem. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 105–111. Springer, Heidelberg (1997)
22. Cai, J.-Y., Cusick, T.W.: A lattice-based public-key cryptosystem. In: Tavares, S., Meijer, H. (eds.) SAC 1998. LNCS, vol. 1556, pp. 219–233. Springer, Heidelberg (1999)
23. Kawachi, A., Tanaka, K., Xagawa, K.: Multi-bit cryptosystems based on lattice problems. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 315–329. Springer, Heidelberg (2007)
24. Regev, O.: Improved inapproximability of lattice and coding problems with preprocessing. In: IEEE Conference on Computational Complexity, pp. 363–370 (2003)

25. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: STOC, pp. 84–93 (2005)
26. Ajtai, M.: Representing hard lattices with o(n log n) bits. In: STOC, pp. 94–103 (2005)
27. Goldreich, O., Goldwasser, S., Halevi, S.: Public-key cryptosystems from lattice reductions problems. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 112–131. Springer, Heidelberg (1997)
28. McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. Deep Space Network Progress Report 44, 114–116 (1978)
29. Nguyen, P.Q.: Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from crypto 1997. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 288–304. Springer, Heidelberg (1999)
30. Fischlin, R., Seifert, J.P.: Tensor-based trapdoors for cvp and their application to public key cryptography. In: IMA Int. Conf., 244–257 (1999)
31. Micciancio, D.: Improving lattice based cryptosystems using the Hermite normal form. In: Silverman, J.H. (ed.) CaLC 2001. LNCS, vol. 2146, pp. 126–145. Springer, Heidelberg (2001)
32. Paeng, S.H., Jung, B.E., Ha, K.C.: A lattice based public key cryptosystem using polynomial representations. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 292–308. Springer, Heidelberg (2003)
33. Han, D., Kim, M.-H., Yeom, Y.: Cryptanalysis of the paeng-jung-ha cryptosystem from pkc 2003. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 107–117. Springer, Heidelberg (2007)
34. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: Buhler, J.P. (ed.) ANTS 1998. LNCS, vol. 1423, pp. 267–288. Springer, Heidelberg (1998)
35. Coppersmith, D., Shamir, A.: Lattice attacks on ntru. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 52–61. Springer, Heidelberg (1997)
36. Micciancio, D., Goldwasser, S.: Complexity of Lattice Problems, A Cryptographic Perspective. Kluwer Academic Publishers, Dordrecht (2002)
37. Minkowski, H.: Geometrie der Zahlen. B. G. Teubner, Leipzig (1896)
38. Cassels, J.W.S.: An Introduction to The Geometry of Numbers. Springer, Heidelberg (1959)
39. Lovász, L.: An Algorithmic Theory of Numbers, Graphs and Convexity. In: CBMS-NSF Regional Conference Series in Applied Mathematics, vol. 50. SIAM Publications, Philadelphia (1986)
40. Conway, J.H., Sloane, N.J.A.: Sphere Packings, Lattices and Groups. Springer, Heidelberg (1988)
41. Cohen, H.: A course in computational algebraic number theory. Graduate Texts in Mathematics, vol. 138. Springer, Heidelberg (1993)
42. Kannan, R., Bachem, A.: Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix. SIAM Journal of Computing 8, 499–507 (1979)
43. Micciancio, D., Warinschi, B.: A linear space algorithm for computing the Hermite normal form. In: International Symposium on Symbolic Algebraic Computation (ISSAC 2001), pp. 231–236 (2001)
44. Ajtai, M.: The shortest vector problem in l_2 is NP-hard for randomized reductions (extended abstract). In: Thirtieth Annual ACM Symposium on the Theory of Computing (STOC 1998), pp. 10–19 (1998)
45. Ajtai, M.: Generating random lattices according to the invariant distribution (2006)

46. Ajtai, M.: Random lattices and a conjectured 0 - 1 law about their polynomial time computable properties. In: FOCS, pp. 733–742 (2002)
47. Goldstein, D., Mayer, A.: On the equidistribution of Hecke points. Forum Mathematicum 15, 165–189 (2003)
48. Nguyen, P.Q., Stehlé, D.: LLL on the average. In: Hess, F., Pauli, S., Pohst, M. (eds.) ANTS 2006. LNCS, vol. 4076, pp. 238–256. Springer, Heidelberg (2006)
49. Nguyen, P.Q., Stern, J.: The two faces of lattices in cryptology. In: Silverman, J.H. (ed.) CaLC 2001. LNCS, vol. 2146, pp. 146–180. Springer, Heidelberg (2001)
50. Gama, N., Nguyen, P.Q.: Predicting lattice reduction. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 31–51. Springer, Heidelberg (2008)
51. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische Annalen 261, 513–534 (1982)
52. Nguyen, P.Q., Stehlé, D.: Floating-point LLL revisited. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 215–233. Springer, Heidelberg (2005)
53. Schnorr, C.P.: Fast LLL-type lattice reduction. Information and Computation 204, 1–25 (2006)
54. Boas, P.V.E.: Another NP-complete problem and the complexity of computing short vectors in lattices. Technical Report 81-04, Mathematics Department, University of Amsterdam (1981)
55. Babai, L.: On Lovász' lattice reduction and the nearest lattice point problem. Combinatorica 6, 1–13 (1986)
56. Schnorr, C.P.: Block reduced lattice bases and successive minima. Combinatorics, Probability & Computing 3, 507–522 (1994)
57. Kannan, R.: Minkowski's convex body theorem and integer programming. Math. Oper. Res. 12, 415–440 (1987)
58. Murakami, Y., Nasako, T.: Knapsack public-key cryptosystem using chinese remainder theorem. IACR ePrint Archive (2007)
59. Bosma, W., Cannon, J., Playoust, C.: The magma algebra system. i. the user language. J. Symobolic Computation 24, 235–265 (1997)
60. Wang, B., Wu, Q., Hu, Y.: A knapsack-based probabilistic encryption scheme. Inf. Sci. 177, 3981–3994 (2007)