IET Information Security

Research Article

Deterministic lattice reduction on knapsacks with collision-free properties

ISSN 1751-8709
Received on 4th March 2017
Revised 18th November 2017
Accepted on 8th December 2017
E-First on 23rd April 2018
doi: 10.1049/iet-ifs.2017.0107
www.ietdl.org

Yuan Ping[1,2], Baocang Wang[3] ✉, Shengli Tian[1], Yuehua Yang[1], Genyuan Du[1]

[1]School of Information Engineering, Xuchang University, Xuchang 461000, People's Republic of China
[2]Information Technology Research Base of Civil Aviation Administration of China, Civil Aviation University of China, Tianjin 300300, People's Republic of China
[3]State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, People's Republic of China
✉ *E-mail: bcwang79@aliyun.com*

Abstract: The knapsack problem is an important problem in computer science and had been used to design public key cryptosystems. Low-density subset sum algorithms are powerful tools to reduce the security of trapdoor knapsacks to the shortest vector problem (SVP) over lattices. Several knapsack ciphers Chor–Rivest, Okamoto–Tanaka–Uchiyama, and Kate–Goldberg were proposed to defend low-density attacks by utilising low-weight knapsack problems. Some evidence was also found on the vulnerabilities of the above three knapsack ciphers to lattice attacks. However, previous lattice-based cryptanalytic results have been established via a probabilistic approach. The authors investigate some collision-free properties and derive from the properties a deterministic reduction from the knapsack problems in the Chor–Rivest, Okamoto–Tanaka–Uchiyama, and Kate–Goldberg knapsack ciphers to SVP without imposing any restriction and assumption. To the best of the authors' knowledge, the proposed reduction is the first deterministic reduction from public key cryptographic knapsacks to SVP.

1 Introduction

1.1 Background

The knapsack problem or more precisely the subset sum problem is an important problem in computer science. Some generic exponential-time algorithms were developed for the problem [1–3]. In fact, it seems very unlikely to develop an efficient algorithm due to the nondeterministic polynomial time (NP)-completeness nature of the decisional knapsack problem [4]. So the knapsack problem was ever considered as an important tool for developing practical and secure public key cryptosystems, especially during the 1980s.

Since the first proposal of Merkle–Hellman trapdoor knapsack [5], many variants were proposed in the literature [6, 7]. However, most of these variants were claimed to be vulnerable to the low-density attacks [8–13] due to their low densities. Chor and Rivest proposed a knapsack public key encryption scheme achieving a high knapsack density [14, 15]. However, the Chor–Rivest cryptosystem was broken by key-recovery attacks [16]. Some more secure parameters [17–19] were suggested to avoid Vaudenay's attacks [16]. Okamoto, Tanaka and Uchiyama proposed another knapsack cryptosystem [20], which is secure against Vaudenay's key-recovery attacks [16] and can obtain an arbitrarily high knapsack density. However, quantum algorithms [21] are required during the key generation and decryption phases. Kate and Goldberg [22] replaced the underlying algebraic structure in [20] with the group used in the Damgard–Jurik cryptosystem [23] to exclude the use of quantum algorithms. The Chor–Rivest, Okamoto–Tanaka–Uchiyama, and Kate–Goldberg cryptosystems allow to encrypt low-weight plaintexts, thus they were called low-weight knapsack public key cryptosystems [24–27]. The security of low-weight trapdoor knapsacks against low-density attacks was examined in [24–27].

1.2 Related work

The cryptanalytic attacks dedicated to the underlying knapsack problems can be classified into two categories. The first category consists of algorithms that find the exact solution but requires exponential computational complexity [1–3]. The second category includes the ones that perform in polynomial time but only provides the solution to some special cases with some probabilities. These algorithms include the low-density subset sum algorithms [8–13] and their instantiations [24–27] in low-weight knapsack cryptosystems.

1.2.1 Low-density subset sum algorithms: Brickell showed [8] that if a knapsack problem $\sum_{i=0}^{n-1} a_i x_i = s$ has a density $d = n/\log_2 \max\{a_i | i = 0, \dots, n-1\} < 1/\log_2 n$, one can apply the lattice reduction algorithms to solve the knapsack problem. Lagarias and Odlyzko [9, 10] proved that the knapsack problems with density below 0.645 can be solved via a single access to the shortest vector problem (SVP) oracle. The critical density bound was further improved in [11–13]. It was shown in [11–13] that if the density is below 0.9408, then a single access to an SVP oracle will derive the solution to the knapsack problems with an overwhelming probability. The density bound 0.9408 is optimal, and hence cannot be improved further [13].

1.2.2 Low-weight attacks: Oomura and Tanaka [24] observed the low-weightness of low-weight knapsack cryptosystems [14, 15, 20, 22], and claimed that low-weight knapsack cryptosystems are still vulnerable to the Lagarias–Odlyzko low-density attacks [9, 10]. In [26], it was observed via numerical examples that the success probability of the low-density subset sum algorithms [11–13] can be further enlarged by increasing the number of accesses to SVP oracles. To measure the asymptotical behaviour of low-density attacks on the low-weight cryptosystems, Nguyen and Stern introduced the notion of pseudo-density and showed that a single call to an SVP oracle almost always reveals the solution to the underlying knapsack problems if the pseudo-density is low [25]. Kunihiro [27] defined a new definition of density D, which unifies the usual density definition and pseudo-density definition in [25], and showed that the knapsack problem with $D < 0.8677$ can be solved with a single call to an SVP oracle.

1.3 Motivation

Our research is motivated by the following facts.

Table 1 Notations

Symbol	Explanation
$\mathbb{R}$	field of real numbers
$\mathbb{Z}$	ring of integers
$\mathbb{N}$	$= \{0 \le a \in \mathbb{Z}\}$, the set of non-negative integers
$\mathbb{Z}_N$	$= \{0, 1, \ldots, N-1\}$, the ring of residue classes
$\boldsymbol{x}$	n-dimensional row vector
$\hat{\boldsymbol{x}}$	$(n+2)$-dimensional row vector
$\boldsymbol{x}[i]$	ith (starting from the 0th) entry of $\boldsymbol{x}$
$\boldsymbol{0}, \hat{\boldsymbol{0}}$	n and $(n+2)$-dimensional zero vector
$\max \boldsymbol{x}$	maximum value of components in $\boldsymbol{x}$
$\min \boldsymbol{x}$	minimum value of components in $\boldsymbol{x}$
$\lfloor x \rfloor$	largest integer not greater than x
$\boldsymbol{x} \cdot \boldsymbol{y}$	$= \sum_{i=0}^{n-1} \boldsymbol{x}[i]\boldsymbol{y}[i]$, the scalar product of $\boldsymbol{x}$ and $\boldsymbol{y}$
$\mathscr{M}$	plaintext space, $\left\{\boldsymbol{m} \in \{0, 1\}^n : \sum_{i=0}^{n-1} \boldsymbol{m}[i] = k\right\}$

1.3.1 Deterministic reduction versus probabilistic reduction: Previous lattice-based cryptanalytic results were established via probabilistic arguments. The known low-density attacks [8–13] and low-weight attacks [24–27] show that the solution to the knapsack problems can be determined only with some certain probabilities. Previous arguments are established by observing the asymptotical behaviours of the reduction methods on solving cryptographic knapsack problems [8–13, 25, 27] or through some concrete numerical values [24–26]. Therefore deterministic reductions from cryptographic knapsack problems to SVP are desired.

1.3.2 Assumptions on the underlying cryptographic knapsack problems: Previous low-density and low-weight attacks were formalised under some assumptions, e.g. the distribution of the entries of the knapsack problem, the density, the weight of the solution, etc.. However, we should note that the knapsack problems used in the knapsack cryptosystems [14, 15, 20, 22] must have some special cryptographic properties, which were overlooked in the previous attacks. An in-depth investigation into the cryptographic properties may be helpful to establish stronger cryptanalytic results by imposing minimum assumptions on the involved knapsack problems.

1.4 Our contributions

We observe some cryptographic collision-free properties in low-weight trapdoor knapsacks [14, 15, 17–20, 22], and give a deterministic reduction from the knapsack problems in low-weight trapdoor knapsacks to SVP. Compared with previous cryptanalytic results, our reduction provides the following advantages.

1.4.1 Deterministic reduction: We provide the first deterministic reduction from cryptographic knapsack problems to SVP, which will make us better understand the security of low-weight knapsack ciphers in both theoretical and practical perspectives.

1.4.2 Minimum assumptions: The proposed reduction is completed without imposing any assumption on the involved knapsack problems, and without considering any restriction on the knapsack density and the weight of the solution. So our reduction applies to all parameters of low-weight knapsack ciphers.

1.4.3 More norms: Our reduction is more general than previous ones in the sense that our results apply to an arbitrary l_p norm with $1 < p \le \infty$, while previous results were developed mainly under the Euclidean norm l_2.

1.5 Organisation

The rest of the paper is organised as follows. Section 2 formalises some notions, provides some preliminaries about lattice theory, and reviews the low-weight knapsack cryptosystems Chor–Rivest [14, 15], Okamoto–Tanaka–Uchiyama [20], and Kate–Goldberg [22]. In Section 3, we provide the lattice reduction from the knapsack problems in the Chor–Rivest, Okamoto–Tanaka–Uchiyama, and Kate–Goldberg cryptosystems to SVP, and prove the correctness of the reduction. Section 4 presents some concluding remarks.

2 Notations and preliminaries

2.1 Notations

The notations in Table 1 will be used in this paper.

2.2 Norms

An important norm is the l_p norm with $1 \le p \le \infty$ defined as $\| \boldsymbol{x} \|_p = \left(\sum_{i=0}^{n-1} |\boldsymbol{x}[i]|^p\right)^{1/p}$ for $\boldsymbol{x} \in \mathbb{R}^n$. The l_p norms are linked via the following lemma.

Lemma 1: For $\boldsymbol{x} \in \mathbb{Z}^n$ and $1 < p \le \infty$, $\| \boldsymbol{x} \|_p \ge (\| \boldsymbol{x} \|_1)^{1/p}$ with equality if and only if $\boldsymbol{x} \in \{0, 1, -1\}^n$.

Proof: Just observe that for any integer z, $|z|^p \ge |z|$ and $|z|^p = |z|$ if and only if $z = 0, 1, -1$. □

2.3 Knapsack problem

We first define the following knapsack problems. The following Definitions 2 and 4 describe two collision-free properties derived from the knapsack problems in the Chor–Rivest, Okamoto–Tanaka–Uchiyama, and Kate–Goldberg cryptosystems. The two properties play an important role for us to build a deterministic reduction.

Definition 1: (Knapsack problem) The subset sum or knapsack problem is to determine, given an n-dimensional positive integral vector $\boldsymbol{a}$ and an integer c, $\boldsymbol{a}$ vector $\boldsymbol{x} \in \{0, 1\}^n$ such that $\boldsymbol{a} \cdot \boldsymbol{x} = c$. A knapsack problem instance is denoted as $\mathrm{KP}(\boldsymbol{a}, c)$.

Definition 2: (Collision-free knapsack problem) Given an integer k: $0 < k \le n$, if a knapsack problem instance $\mathrm{KP}(\boldsymbol{a}, c)$ has at most one binary solution $\boldsymbol{x}$ with weight exactly $\| \boldsymbol{x} \|_1 = k$, we call $\mathrm{KP}(\boldsymbol{a}, c)$ a k-collision-free knapsack problem.

After we review the Chor–Rivest, Okamoto–Tanaka–Uchiyama, and Kate–Goldberg cryptosystems, we will show through the unique-decipherability property that the knapsacks in the cryptosystems are k-collision-free.

Definition 3: (General or compact knapsack problem) The compact or general knapsack problem is to find, given an n-dimensional vector $\boldsymbol{a}$ and an integer c, $\boldsymbol{a}$ vector $\boldsymbol{x} \in \mathbb{N}^n$ such that $\boldsymbol{a} \cdot \boldsymbol{x} = c$. A compact knapsack problem instance is denoted as $\mathrm{CKP}(\boldsymbol{a}, c)$.

The compact knapsack problem can be viewed as a natural generalisation of the knapsack problem. We also provide the following collision-free compact knapsack problem.

Definition 4: ($\lfloor k/2 \rfloor$ -Collision-free compact knapsack problem) given an integer k: $0 < k \le n$, if a compact knapsack problem $\mathrm{CKP}(\boldsymbol{a}, c)$ has at most one non-negative integral solution $\boldsymbol{x}$ in the set $\mathscr{N}(\lfloor k/2 \rfloor, n) = \{\boldsymbol{x} \in \mathbb{N}^n : \| \boldsymbol{x} \|_1 = \lfloor k/2 \rfloor\}$, we call $\mathrm{CKP}(\boldsymbol{a}, c)$ a $\lfloor k/2 \rfloor$ -collision-free compact knapsack problem.

We will also illustrate by observing the parameter specifications that give the public key $\boldsymbol{a}$ and k of the Chor–Rivest, Okamoto–Tanaka–Uchiyama, and Kate–Goldberg cryptosystems, and an integer c, the compact knapsack problem $\mathrm{CKP}(\boldsymbol{a}, c)$ is $\lfloor k/2 \rfloor$ -collision-free.

2.4 Lattice

A lattice is a discrete additive subgroup of $\mathbb{R}^n$, which consists of all integral linear combinations of a set of linearly independent vectors $\boldsymbol{V} = \{\boldsymbol{v}_0, \ldots, \boldsymbol{v}_{d-1}\}$, i.e.

$$\mathscr{L}(\boldsymbol{V}) = \left\{ \sum_{i=0}^{d-1} z_i \boldsymbol{v}_i | z_i \in \mathbb{Z} \right\}.$$

The set of ordered vectors $\{\boldsymbol{v}_i\}$ is called a lattice basis.

An important problem in lattice theory is SVP, which asks for the shortest non-zero vector in a lattice $\mathscr{L}$. SVP is proven to be NP-hard under randomised reductions [28], so it seems impossible to develop a polynomial-time algorithm for SVP. Known practical lattice reduction algorithms [29–31] solve SVP only with sub-exponential factors. However, interestingly, experimental results showed that lattice reduction algorithms behave much more nicely especially in low-dimensional (<300) lattices than it was expected from the worst-case proved bounds. For example, Nguyen broke the Goldreich–Goldwasser–Halevi (GGH) challenges up to dimension 350 [32], and Lee and Hahn conquered the dimension 400 challenge of GGH [33]. Lattice reduction algorithms were also proven a powerful cryptanalytic tool in knapsack cryptography. For example, Schnorr and Horner [34] utilised lattice reduction algorithms to break a 103-dimensional Chor–Rivest [14, 15] instance and a 151-dimensional Damgard's knapsack hash function [35].

Known low-density and low-weight attacks on knapsack ciphers aim at reducing the knapsack problems to SVP. One may doubt that it seems meaningless to reduce an intractability problem to another one. However, the state-of-the-art in lattice reduction algorithms demonstrates that the known practical lattice reduction algorithms can serve as an SVP oracle in low-dimensional lattices. Therefore, when we reduce the knapsack problem to SVP, we can say that the knapsack cryptosystem is insecure for low-dimensional parameters. We do not claim totally breaking the corresponding cryptosystems due to the gaps of lattice reduction algorithms for solving SVP and SVP oracles. To avoid the attacks, the dimension of a knapsack cryptosystem must be chosen sufficiently large, say, >500 [22]. However, this will seriously compromise the practicability of trapdoor knapsacks and hence render them less attractive.

2.5 Chor–Rivest cryptosystem

Our reduction does not rely on the decryption algorithms, so we omitted the description of them. The construction of the Chor–Rivest cryptosystem is based on the following Bose–Chowla theorem [14, 15], which states a collision-free property.

Theorem 1: (Bose–Chowla theorem) Given a prime n and $2 \leq k \in \mathbb{Z}$, there must exist an n-dimensional vector $\boldsymbol{u}$ with $0 \leq \boldsymbol{u}[i] \leq n^k - 1$ for all $i = 0, \ldots, n-1$ such that $\boldsymbol{u} \cdot \boldsymbol{x} \neq \boldsymbol{u} \cdot \boldsymbol{y}$ for any n-dimensional vector pair $(\boldsymbol{x}, \boldsymbol{y})$ with $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{N}^n$, $\boldsymbol{x} \neq \boldsymbol{y}$, and $\| \boldsymbol{x} \|_1$, $\| \boldsymbol{y} \|_1 \leq k$.

2.5.1 Key generation: Given the system parameters: a prime n and $2 \leq k \in \mathbb{Z}$, construct an n-dimensional vector $\boldsymbol{u}$ satisfying the Bose–Chowla theorem. Randomly choose a permutation π and apply it on $\boldsymbol{u}$ to give a new vector $\boldsymbol{u}^* = \pi(\boldsymbol{u})$. Add some noise d with $0 \leq d \leq n^k - 2$ to the entries of $\boldsymbol{u}^*$ to derive the public vector $\boldsymbol{a}$ with $\boldsymbol{a}[i] = \boldsymbol{u}^*[i] + d$ for all $i = 0, \ldots, n-1$. The public key of the Chor–Rivest cryptosystem consists of $\boldsymbol{a}$, n, and k, and the secret key contains π^{-1}, d, and two elements g and t in the finite field $\mathrm{GF}(n^k)$ used in the construction of $\boldsymbol{u}$.

2.5.2 Encryption: The ciphertext for $\boldsymbol{m} \in \mathscr{M}$ is $c = \boldsymbol{a} \cdot \boldsymbol{m} (\bmod n^k - 1)$.

2.5.3 Remark: The Chor–Rivest cryptosystem uses a modular knapsack problem. However, we can view the encryption function as a standard knapsack problem because there must exist a unique integer $0 \leq l \leq k - 1$ such that $c + l(n^k - 1) = \boldsymbol{a} \cdot \boldsymbol{m}$. By doing so, we only increase the computational complexity by a factor of k. So in order to uniformly describe low-weight knapsack cryptosystems [14, 15, 17–20, 22], we view the underlying encryption function as $c = \boldsymbol{a} \cdot \boldsymbol{m}$.

2.6 Okamoto–Tanaka–Uchiyama cryptosystem

2.6.1 Key generation: Randomly generate n pair-wise co-prime integers $p_0, \ldots, p_{n-1}$ and a prime P such that $1 < p_0, \ldots, p_{n-1} < P^{1/k}$ with $2 \leq k \in \mathbb{Z}$. Then randomly choose a generator g of the multiplicative group $\mathrm{GF}(P)^* = \{1, \ldots, P-1\} = \langle g \rangle$ and uses Shor's quantum algorithm [21] to solve the discrete logarithm of every p_i to the base g and gets n integers $u_0, \ldots, u_{n-1} \in \{1, 2, \ldots, P-1\}$, that is, $p_i = g^{u_i} (\bmod P)$. The knapsack vector $\boldsymbol{a}$ is computed by $\boldsymbol{a}[i] = (u_i + d) (\bmod P - 1)$ for $i = 0, \ldots, n-1$, where $d \in \mathrm{GF}(P)$ is a randomly-chosen integer. The public key is $(n, k, \boldsymbol{a})$. The secret key is $(g, d, P, p_0, \ldots, p_{n-1})$.

2.6.2 Encryption: The ciphertext for $\boldsymbol{m} \in \mathscr{M}$ is $c = \boldsymbol{a} \cdot \boldsymbol{m}$.

2.7 Kate–Goldberg cryptosystem

2.7.1 Key generation: The system parameters consist of three positive integers n, k, r such that $2 \leq k < n/2$ and $k < r$. Randomly generate two distinct primes P and Q and compute their product $N = PQ$. Note that $\{\alpha N + 1 \in \mathbb{Z}_{N^{r+1}} : 0 \leq \alpha \leq N^r - 1\}$ forms a cyclic group with order being N^r [23]. Randomly choose a generator g of the cyclic group $\langle g \rangle$, and n pairwise co-prime integers $p_0, \ldots, p_{n-1} \in \langle g \rangle$ such that $1 < p_0, \ldots, p_{n-1} < N^{(r+1)/k}$. We use the logarithm function L [23] to compute n integers $u_0, \ldots, u_{n-1} \in \{1, 2, \ldots, N^r\}$ such that $p_i = g^{u_i} (\bmod N^{r+1})$. Finally, randomly choose an integer $d \in \mathbb{Z}_{N^r}$ and compute the knapsack vector $\boldsymbol{a}$ with $\boldsymbol{a}[i] = (u_i + d) (\bmod N^r)$ for $i = 0, \ldots, n-1$. The public key is $(n, k, \boldsymbol{a})$. The secret key is $(P, Q, N, r, g, d, p_0, \ldots, p_{n-1})$.

2.7.2 Encryption: The ciphertext for $\boldsymbol{m} \in \mathscr{M}$ is $c = \boldsymbol{a} \cdot \boldsymbol{m}$.

3 Reduction

In this section, we provide a deterministic reduction from the knapsack problems in the Chor–Rivest, Okamoto–Tanaka–Uchiyama, and Kate–Goldberg cryptosystems to SVP over a lattice. In this section, the vector $\boldsymbol{a}$ denotes the public key of the three cryptosystems, k is the weight of a plaintext $\boldsymbol{m}$, and c stands for a ciphertext, namely, $\boldsymbol{a} \cdot \boldsymbol{m} = c$ and $| | \boldsymbol{m} | |_1 = k$.

3.1 Overview

Let the public n-dimensional positive integral knapsack vector be $\boldsymbol{a}$ in low-weight knapsack cryptosystems [14, 15, 17–20, 22], and $c = \boldsymbol{m} \cdot \boldsymbol{a}$ be a ciphertext of a plaintext $\boldsymbol{m} \in \mathscr{M}$. Our task is to determine the solution $\boldsymbol{m} \in \mathscr{M}$ to the knapsack problem $\mathrm{KP}(\boldsymbol{a}, c)$ by accessing SVP oracles.

We define an integer $\Delta > k$, and $n+1$ linearly independent vectors $\boldsymbol{b}_0, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-1}, \boldsymbol{b}_n$ as follows:

$$\boldsymbol{B} = \begin{pmatrix} \boldsymbol{b}_0 \\ \boldsymbol{b}_1 \\ \vdots \\ \boldsymbol{b}_{n-1} \\ \boldsymbol{b}_n \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 & \Delta \boldsymbol{a}[0] & \Delta \\ 0 & 1 & \cdots & 0 & \Delta \boldsymbol{a}[1] & \Delta \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \Delta \boldsymbol{a}[n-1] & \Delta \\ 0 & 0 & \cdots & 0 & -c\Delta & -k\Delta \end{pmatrix}.$$

The integral linear combinations of the $n+1$ vectors form a lattice

$$\mathscr{L} = \mathscr{L}(\boldsymbol{B}) = \left\{ \sum_{i=0}^{n} z_i \boldsymbol{b}_i : z_i \in \mathbb{Z} \right\}.$$

For any l_p norm with $1 \le p \le \infty$, SVP defined on the lattice $\mathscr{L}$ is to find a non-zero vector $\boldsymbol{v} \in \mathscr{L}$ such that $\| \boldsymbol{v} \|_p \le \| \boldsymbol{w} \|_p$ for any non-zero lattice vector $\boldsymbol{w} \in \mathscr{L}$.

Lemma 2: If we denote $\hat{\boldsymbol{m}} = (\boldsymbol{m}[0], \dots, \boldsymbol{m}[n-1], 0, 0)$, we must have $\pm \hat{\boldsymbol{m}} \in \mathscr{L}$.

Proof: Recalling $\boldsymbol{a} \cdot \boldsymbol{m} = c$ and $|\boldsymbol{m}|_1 = \sum_{i=0}^{n-1} \boldsymbol{m}[i] = k$, we immediately have

$$\pm \hat{\boldsymbol{m}} = \pm \left(\sum_{i=0}^{n-1} \boldsymbol{m}[i] \boldsymbol{b}_i + \boldsymbol{b}_n \right) \in \mathscr{L}.$$

□

Noting that $\| \hat{\boldsymbol{m}} \|_p = k^{1/p}$ is relatively small, we may expect that $\pm \hat{\boldsymbol{m}}$ are the shortest vectors in the lattice $\mathscr{L}$. To show that we can recover the plaintext $\boldsymbol{m} \in \mathscr{M}$ from an arbitrary shortest vector of $\mathscr{L}$, we need to illustrate that there are no non-zero vectors other than $\pm \hat{\boldsymbol{m}}$ in $\mathscr{L}$ enjoying an l_p norm (where $1 < p \le \infty$) not larger than $\| \hat{\boldsymbol{m}} \|_p = k^{1/p}$. So we consider the problem whether there exists a lattice vector $\hat{\boldsymbol{x}} \in \mathscr{L}$ or not such that $\hat{\boldsymbol{x}} \notin \left\{ \hat{\boldsymbol{0}}, \hat{\boldsymbol{m}}, -\hat{\boldsymbol{m}} \right\}$ and $\| \hat{\boldsymbol{x}} \|_p \le \| \hat{\boldsymbol{m}} \|_p$.

Our main result is the following theorem.

Theorem 2: Given the public key $(\boldsymbol{a}, n, k)$ of the Chor–Rivest, Okamoto–Tanaka–Uchiyama, and Kate–Goldberg cryptosystems and a ciphertext c, the shortest vectors in $\mathscr{L}$ are $\pm \hat{\boldsymbol{m}}$ under any l_p norm with l_p.

3.2 Cryptographic properties

To prove Theorem 2, we need to investigate some collision-free properties of the Chor–Rivest, Okamoto–Tanaka–Uchiyama, and Kate–Goldberg cryptosystems.

Lemma 3: Given the public key $(\boldsymbol{a}, n, k)$ of the Chor–Rivest, Okamoto–Tanaka–Uchiyama, and Kate–Goldberg cryptosystems and a ciphertext c, the knapsack problem $\mathrm{KP}(\boldsymbol{a}, c)$ is k-collision-free.

Proof: If c is a valid ciphertext, c can be uniquely decrypted into the corresponding plaintext $\boldsymbol{m} \in \mathscr{M}$. So $\mathrm{KP}(\boldsymbol{a}, c)$ has a unique solution in $\mathscr{M}$. If c is an invalid ciphertext, $\mathrm{KP}(\boldsymbol{a}, c)$ has no solutions in $\mathscr{M}$. □

In fact, Lemma 3 can be proven by observing the parameters of the Chor–Rivest, Okamoto–Tanaka–Uchiyama, and Kate–Goldberg cryptosystems. The parameter settings ensure the unique decipherability of ciphertexts. See the decryption algorithms of [14, 15, 20, 22] to justify the property of unique decipherability of ciphertexts.

Given the public key $(\boldsymbol{a}, n, k)$ of the Chor–Rivest, Okamoto–Tanaka–Uchiyama, and Kate–Goldberg cryptosystems and a ciphertext c, we also can construct a compact knapsack problem $\mathrm{CKP}(\boldsymbol{a}, c)$. We investigate the key generations of the three cryptosystems and find that the compact knapsack problem $\mathrm{CKP}(\boldsymbol{a}, c)$ also has a collision-free property.

Lemma 4: Given the public key $(\boldsymbol{a}, n, k)$ of the Chor–Rivest, Okamoto–Tanaka–Uchiyama, and Kate–Goldberg cryptosystems and an integer c, the compact knapsack problem $\mathrm{CKP}(\boldsymbol{a}, c)$ is $\lfloor k/2 \rfloor$-collision-free.

Proof: To derive contradictions, we assume that there exists $c \in \mathbb{N}$ such that there exist $\boldsymbol{x}, \boldsymbol{y} \in \mathscr{N}(\lfloor k/2 \rfloor, n)$ satisfying $\boldsymbol{x} \ne \boldsymbol{y}$ and $\boldsymbol{x} \cdot \boldsymbol{a} = \boldsymbol{y} \cdot \boldsymbol{a} = c$.

The Chor–Rivest cryptosystem: Recalling the key generation algorithm of the Chor–Rivest cryptosystem, we have that

$$\begin{aligned} \boldsymbol{x} \cdot \boldsymbol{a} &= \sum_{i=0}^{n-1} (\boldsymbol{u}^*[i] + d) \boldsymbol{x}[i] = \boldsymbol{u}^* \cdot \boldsymbol{x} + d \lfloor k/2 \rfloor \\ &= \pi(\boldsymbol{u}) \cdot \boldsymbol{x} + d \lfloor k/2 \rfloor = \boldsymbol{u} \cdot \pi^{-1}(\boldsymbol{x}) + d \lfloor k/2 \rfloor. \end{aligned}$$

Similarly, we also have $\boldsymbol{y} \cdot \boldsymbol{a} = \boldsymbol{u} \cdot \pi^{-1}(\boldsymbol{y}) + d \lfloor k/2 \rfloor$. So we get $\boldsymbol{u} \cdot \pi^{-1}(\boldsymbol{x}) = \boldsymbol{u} \cdot \pi^{-1}(\boldsymbol{y})$. Recalling that the generated vector $\boldsymbol{u}$ satisfies the Bose–Chowla theorem and that $\| \pi^{-1}(\boldsymbol{x}) \|_1 = \| \pi^{-1}(\boldsymbol{y}) \|_1 = \lfloor k/2 \rfloor \le k$, we immediately have that $\pi^{-1}(\boldsymbol{x}) = \pi^{-1}(\boldsymbol{y})$, so $\boldsymbol{x} = \boldsymbol{y}$, which contradicts $\boldsymbol{x} \ne \boldsymbol{y}$.

The Okamoto–Tanaka–Uchiyama cryptosystem: From the key generation algorithm of the Okamoto–Tanaka–Uchiyama cryptosystem, we know

$$\begin{aligned} \sum_{i=0}^{n-1} \boldsymbol{x}[i] u_i + d \lfloor k/2 \rfloor &= \boldsymbol{x} \cdot \boldsymbol{a} = \boldsymbol{y} \cdot \boldsymbol{a} \\ &= \sum_{i=0}^{n-1} \boldsymbol{y}[i] u_i + d \lfloor k/2 \rfloor (\bmod P - 1), \end{aligned}$$

from which we get

$$\sum_{i=0}^{n-1} \boldsymbol{x}[i] u_i = \sum_{i=0}^{n-1} \boldsymbol{y}[i] u_i (\bmod P - 1).$$

Thus,

$$g^{\sum_{i=0}^{n-1} \boldsymbol{x}[i] u_i} = g^{\sum_{i=0}^{n-1} \boldsymbol{y}[i] u_i} (\bmod P).$$

So we have $\prod_{i=0}^{n-1} p_i^{\boldsymbol{x}[i]} = \prod_{i=0}^{n-1} p_i^{\boldsymbol{y}[i]} (\bmod P)$. Noting the settings of the size p_i, we claim that $\prod_{i=0}^{n-1} p_i^{\boldsymbol{x}[i]} = \prod_{i=0}^{n-1} p_i^{\boldsymbol{y}[i]}$. Noting that $p_0, \dots, p_{n-1}$ are pairwise relatively prime, we immediately get $\boldsymbol{x}[i] = \boldsymbol{y}[i]$ for all $i = 0, \dots, n-1$, which also contradicts $\boldsymbol{x} \ne \boldsymbol{y}$.

The Kate–Goldberg cryptosystem: from $\boldsymbol{a}[i] = (u_i + d)(\bmod N^r)$ and $\boldsymbol{x} \cdot \boldsymbol{a} = \boldsymbol{y} \cdot \boldsymbol{a}$, we can easily derive $\sum_{i=0}^{n-1} \boldsymbol{x}[i] u_i = \sum_{i=0}^{n-1} \boldsymbol{y}[i] u_i$ $(\bmod N^r)$, so we have

$$\prod_{i=0}^{n-1} p_i^{\boldsymbol{x}[i]} = g^{\sum_{i=0}^{n-1} \boldsymbol{x}[i] u_i} = g^{\sum_{i=0}^{n-1} \boldsymbol{y}[i] u_i} = \prod_{i=0}^{n-1} p_i^{\boldsymbol{y}[i]} \left(\bmod N^{r+1} \right).$$

From the sizes of p_i, we have $\prod_{i=0}^{n-1} p_i^{\boldsymbol{x}[i]} = \prod_{i=0}^{n-1} p_i^{\boldsymbol{y}[i]}$. Similar to the case of the Okamoto–Tanaka–Uchiyama cryptosystem, we know $\boldsymbol{x} = \boldsymbol{y}$, which contradicts $\boldsymbol{x} \ne \boldsymbol{y}$. □

3.3 Proof

To show the lattice $\mathscr{L} = \mathscr{L}(\boldsymbol{B})$ only has two non-zero shortest vectors $\pm \hat{\boldsymbol{m}} \in \mathscr{L}$, we define a sub-lattice

$$\mathscr{L}^* = \mathscr{L}(\boldsymbol{b}_0, \dots, \boldsymbol{b}_{n-1}) = \left\{ \sum_{i=0}^{n-1} z_i \boldsymbol{b}_i : z_i \in \mathbb{Z} \right\},$$

and the subset

$$\mathscr{C} = \mathscr{L} - \mathscr{L}^* = \left\{ \sum_{i=0}^{n} z_i \boldsymbol{b}_i : z_i \in \mathbb{Z}, z_n \ne 0 \right\}.$$

Similarly, we can define SVP over $\mathscr{L}^*$ and $\mathscr{C}$. If we show that the shortest vectors in $\mathscr{C}$ are exactly and that all the non-zero vectors in $\mathscr{L}^*$ achieve an l_p norm larger than $\| \hat{\boldsymbol{m}} \|_p = k^{1/p}$ with $1 < p \le \infty$, we prove that the shortest vectors in $\mathscr{L} = \mathscr{L}^* \cup \mathscr{C}$ are exactly $\pm \hat{\boldsymbol{m}}$. So we prove Theorem 2.

We first prove the following lemma.

Lemma 5: For any $1 \le p \le \infty$ and $\hat{\boldsymbol{x}} \in \mathscr{L}$ with $\| \hat{\boldsymbol{x}} \|_p \ \le \| \hat{\boldsymbol{m}} \|_p$, the last two entries of $\hat{\boldsymbol{x}}$ must be 0, $\hat{\boldsymbol{x}}[n] = \hat{\boldsymbol{x}}[n+1] = 0$.

Proof: . Otherwise, either $\hat{\boldsymbol{x}}[n]$ or $\hat{\boldsymbol{x}}[n+1]$ must be a non-zero integral multiple of $\Delta > k$. So we can derive a contradiction, $\| \hat{\boldsymbol{x}} \|_p \ \ge \Delta^{1/p} > k^{1/p} = \| \hat{\boldsymbol{m}} \|_p$. □

In the following lemma, we show that $\mathscr{C}$ only contains two shortest vectors $\pm \hat{\boldsymbol{m}}$.

Lemma 6: The set $\mathscr{C}$ only has two shortest vectors $\pm \hat{\boldsymbol{m}}$ under any norm l_p *with* $1 < p \le \infty$.

Proof: Note $\pm \hat{\boldsymbol{m}} = \pm \left(\sum_{i=0}^{n-1} \boldsymbol{m}[i] \boldsymbol{b}_i + \boldsymbol{b}_n \right) \in \mathscr{C}$. So it suffices to show that for any shortest vector $\hat{\boldsymbol{x}} \in \mathscr{C}$, we must have $\hat{\boldsymbol{x}} = \hat{\boldsymbol{m}}$ or $-\hat{\boldsymbol{m}}$.
Let

$$\begin{aligned} \hat{\boldsymbol{x}} &= \sum_{i=0}^{n-1} \hat{\boldsymbol{x}}[i] \boldsymbol{b}_i + z \boldsymbol{b}_n \\ &= \left(\hat{\boldsymbol{x}}[0], \ldots, \hat{\boldsymbol{x}}[n-1], \Delta(\boldsymbol{a} \cdot \boldsymbol{x} - zc), \Delta\left(\sum_{i=0}^{n-1} \boldsymbol{x}[i] - zk \right) \right), \end{aligned}$$

where $z \ne 0$ and $\boldsymbol{x} = (\hat{\boldsymbol{x}}[0], \ldots, \hat{\boldsymbol{x}}[n-1])$. Lemma 5 implies that the last two entries of $\hat{\boldsymbol{x}}$ are 0, so we have $\boldsymbol{a} \cdot \boldsymbol{x} = zc$ and $\sum_{i=0}^{n-1} \boldsymbol{x}[i] = zk$. Note that the norm of the shortest vector $\hat{\boldsymbol{x}}$ must not exceed that of $\hat{\boldsymbol{m}}$. So for any norm l_p with $1 < p \le \infty$, we get

$$\begin{aligned} |zk|^{1/p} &= \left| \sum_{i=0}^{n-1} \hat{\boldsymbol{x}}[i] \right|^{1/p} \le \left(\sum_{i=0}^{n-1} |\hat{\boldsymbol{x}}[i]| \right)^{1/p} \le \left(\sum_{i=0}^{n-1} |\hat{\boldsymbol{x}}[i]|^p \right)^{1/p} \\ &= \| \hat{\boldsymbol{x}} \|_p \le \| \hat{\boldsymbol{m}} \|_p = k^{1/p}. \end{aligned}$$

From the above inequalities, we derive $|z| \le 1$. Recall $z \ne 0$, and we get $|z| = 1$ and $\| \hat{\boldsymbol{x}} \|_p = k^{1/p}$.
When $z > 0$, we have $\boldsymbol{a} \cdot \boldsymbol{x} = c$ and $\sum_{i=0}^{n-1} \hat{\boldsymbol{x}}[i] = \sum_{i=0}^{n-1} \boldsymbol{x}[i] = k$. Recall $\| \hat{\boldsymbol{x}} \|_p = k^{1/p}$ and Lemma 1, and we have

$$k^{1/p} = \| \hat{\boldsymbol{x}} \|_p \ge \left(\| \hat{\boldsymbol{x}} \|_1 \right)^{1/p} \ge \left(\sum_{i=0}^{n-1} \hat{\boldsymbol{x}}[i] \right)^{1/p} = k^{1/p}.$$

So the two symbols '$\ge$' must be '='. Therefore, $\| \hat{\boldsymbol{x}} \|_1 = \sum_{i=0}^{n-1} \hat{\boldsymbol{x}}[i]$, which implies $\hat{\boldsymbol{x}}[i] \ge 0$ for all $i = 0, \ldots, n-1$. Apply the necessary condition of Lemma 1 on the equation $\| \hat{\boldsymbol{x}} \|_p = \left(\| \hat{\boldsymbol{x}} \|_1 \right)^{1/p}$ and we get $\hat{\boldsymbol{x}}[i] \in \{0, 1, -1\}$ for all $i = 0, \ldots, n-1$. Combing the two facts, we have $\boldsymbol{x} \in \{0, 1\}^n$ must be a binary solution to the knapsack problem $\mathrm{KP}(\boldsymbol{a}, c)$ satisfying $\sum_{i=0}^{n-1} \boldsymbol{x}[i] = k$. From the k-collision-free property of $\mathrm{KP}(\boldsymbol{a}, c)$, we immediately get $\boldsymbol{x} = \boldsymbol{m}$, and hence $\hat{\boldsymbol{x}} = \hat{\boldsymbol{m}}$.
When $z < 0$, we replace each $\hat{\boldsymbol{x}}[i]$ for $i = 0, \ldots, n$ with $-\hat{\boldsymbol{x}}[i]$ and z with $-z$, and can argue that $-\boldsymbol{x} = \boldsymbol{m}$, namely, $\boldsymbol{x} = -\boldsymbol{m}$. So $\hat{\boldsymbol{x}} = -\hat{\boldsymbol{m}}$. □

Given the public key $(\boldsymbol{a}, n, k)$ of the Chor–Rivest, Okamoto–Tanaka–Uchiyama, and Kate–Goldberg cryptosystems and an integer c, we use the $\lfloor k/2 \rfloor$ -collision-free property of the compact knapsack problem $\mathrm{CKP}(\boldsymbol{a}, c)$ to prove the following result.

Lemma 7: For any $\hat{\boldsymbol{0}} \ne \hat{\boldsymbol{x}} \in \mathscr{L}^*$, we must have $\| \hat{\boldsymbol{x}} \|_p > \| \hat{\boldsymbol{m}} \|_p$ with $1 < p \le \infty$.

Proof: To derive contradictions, we assume that there exists a vector $\hat{\boldsymbol{0}} \ne \hat{\boldsymbol{x}} \in \mathscr{L}^*$ such that $1 \le \| \hat{\boldsymbol{x}} \|_p \le \| \hat{\boldsymbol{m}} \|_p$. Note that $\hat{\boldsymbol{x}} = \left(\hat{\boldsymbol{x}}[0], \ldots, \hat{\boldsymbol{x}}[n-1], \Delta(\boldsymbol{a} \cdot \boldsymbol{x}), \Delta\left(\sum_{i=0}^{n-1} \hat{\boldsymbol{x}}[i] \right) \right)$, where we define $\boldsymbol{x} = (\hat{\boldsymbol{x}}[0], \ldots, \hat{\boldsymbol{x}}[n-1])$. Lemma 5 implies that $\hat{\boldsymbol{x}}[n] = \Delta(\boldsymbol{a} \cdot \boldsymbol{x}) = 0$ and $\hat{\boldsymbol{x}}[n+1] = \Delta\left(\sum_{i=0}^{n-1} \hat{\boldsymbol{x}}[i] \right) = 0$, namely, $\boldsymbol{a} \cdot \boldsymbol{x} = 0$ and $\sum_{i=0}^{n-1} \hat{\boldsymbol{x}}[i] = 0$. From $\boldsymbol{a} \cdot \boldsymbol{x} = 0$, we obtain

$$\sum_{\hat{\boldsymbol{x}}[i] > 0} \hat{\boldsymbol{x}}[i] \boldsymbol{a}[i] = \sum_{\hat{\boldsymbol{x}}[i] < 0} (-\hat{\boldsymbol{x}}[i]) \boldsymbol{a}[i]. \tag{1}$$

From $\sum_{i=0}^{n-1} \hat{\boldsymbol{x}}[i] = 0$, we obtain

$$\sum_{\hat{\boldsymbol{x}}[i] > 0} \hat{\boldsymbol{x}}[i] = \sum_{\hat{\boldsymbol{x}}[i] < 0} (-\hat{\boldsymbol{x}}[i]). \tag{2}$$

To derive a contradiction with the collision-free property, we define $\boldsymbol{y} \in \mathbb{N}^n$ such that for $i = 0, \ldots, n-1$, $\boldsymbol{y}[i] = \hat{\boldsymbol{x}}[i]$ if $\hat{\boldsymbol{x}}[i] > 0$ and $\boldsymbol{y}[i] = 0$ otherwise, and $\boldsymbol{z} \in \mathbb{N}^n$ such that for $i = 0, \ldots, n-1$, $\boldsymbol{z}[i] = -\hat{\boldsymbol{x}}[i]$ if $\hat{\boldsymbol{x}}[i] < 0$ and $\boldsymbol{z}[i] = 0$ otherwise. It is obvious that $\boldsymbol{0} \ne \boldsymbol{y}$, $\boldsymbol{0} \ne \boldsymbol{z}$, and $\boldsymbol{y} \ne \boldsymbol{z}$. We also have $\| \hat{\boldsymbol{x}} \|_1 = \| \boldsymbol{x} \|_1 = \| \boldsymbol{y} \|_1 + \| \boldsymbol{z} \|_1$.
We rewrite (1) and (2) in terms of $\boldsymbol{y}$ and $\boldsymbol{z}$, and get $\boldsymbol{a} \cdot \boldsymbol{y} = \boldsymbol{a} \cdot \boldsymbol{z}$ and $\| \boldsymbol{y} \|_1 = \| \boldsymbol{z} \|_1 = \| \boldsymbol{x} \|_1 /2 = \| \hat{\boldsymbol{x}} \|_1 /2$. We apply Lemma 1 to $\| \hat{\boldsymbol{x}} \|_p \le \| \hat{\boldsymbol{m}} \|_p$ and obtain $\| \boldsymbol{x} \|_1 = \| \hat{\boldsymbol{x}} \|_1 \le \left(\| \hat{\boldsymbol{x}} \|_p \right)^p \le \left(\| \hat{\boldsymbol{m}} \|_p \right)^p = k$. So we conclude that $\| \boldsymbol{y} \|_1 = \| \boldsymbol{z} \|_1 = \| \hat{\boldsymbol{x}} \|_1 /2 \le k/2$.
We also define $\boldsymbol{y}^* \in \mathbb{Z}^n$ such that $\boldsymbol{y}^*[0] = \boldsymbol{y}[0] + \lfloor k/2 \rfloor - \| \boldsymbol{y} \|_1$ and for $i = 1, \ldots, n-1$, $\boldsymbol{y}^*[i] = \boldsymbol{y}[i]$, and $\boldsymbol{z}^* \in \mathbb{Z}^n$ such that $\boldsymbol{z}^*[0] = \boldsymbol{z}[0] + \lfloor k/2 \rfloor - \| \boldsymbol{z} \|_1$ and for $i = 1, \ldots, n-1$, $\boldsymbol{z}^*[i] = \boldsymbol{z}[i]$. From $\| \boldsymbol{y} \|_1 = \| \boldsymbol{z} \|_1 = \| \hat{\boldsymbol{x}} \|_1 /2 \le k/2$, we know $\lfloor k/2 \rfloor - \| \boldsymbol{y} \|_1 = \lfloor k/2 \rfloor - \| \boldsymbol{z} \|_1 \ge 0$. So $\boldsymbol{y}^*, \boldsymbol{z}^* \in \mathbb{N}^n$. We can easily verify the following three things. Firstly,

$$\| \boldsymbol{y}^* \|_1 = \| \boldsymbol{y} \|_1 + \lfloor k/2 \rfloor - \| \boldsymbol{y} \|_1 = \lfloor k/2 \rfloor = \| \boldsymbol{z}^* \|_1.$$

So $\boldsymbol{y}^*, \boldsymbol{z}^* \in \mathscr{N}(\lfloor k/2 \rfloor, n)$. Secondly, $\boldsymbol{y}^* \ne \boldsymbol{z}^*$. Thirdly,

$$\begin{aligned} \boldsymbol{y}^* \cdot \boldsymbol{a} &= \boldsymbol{y} \cdot \boldsymbol{a} + (\lfloor k/2 \rfloor - \| \boldsymbol{y} \|_1) \boldsymbol{a}[0] \\ &= \boldsymbol{z} \cdot \boldsymbol{a} + (\lfloor k/2 \rfloor - \| \boldsymbol{z} \|_1) \boldsymbol{a}[0] = \boldsymbol{z}^* \cdot \boldsymbol{a}. \end{aligned}$$

Thus if we set $s = \boldsymbol{y} \cdot \boldsymbol{a} + (\lfloor k/2 \rfloor - \| \boldsymbol{y} \|_1) \boldsymbol{a}[0]$, we know $\mathrm{CKP}(\boldsymbol{a}, s)$ is not $\lfloor k/2 \rfloor$-collision-free, which contradicts Lemma 4. □

From Lemmas 6 and 7, we can easily prove Theorem 2.

Proof: First, note $\mathscr{L} = \mathscr{L}^* \cup \mathscr{C}$. Lemma 7 illustrates that any non-zero vector in $\mathscr{L}^*$ must have a norm exactly greater than that of $\hat{\boldsymbol{m}}$ under any l_p norm with $1 < p \le \infty$. Lemma 6 says that there exist exactly two shortest vectors $\pm \hat{\boldsymbol{m}}$ in $\mathscr{C}$. So the lattice $\mathscr{L}$ only has two shortest vectors $\pm \hat{\boldsymbol{m}}$.□

4 Conclusion

In this study, we present a deterministic reduction from the cryptographic knapsacks to SVP. To best of our knowledge, this reduction is the first deterministic reduction known in the literature. Compared with previous results [8–13, 24–27], the proposed reduction reveals at the first time a deterministic connection between public key cryptographic knapsacks and SVP. The reduction is established without imposing any assumptions and restrictions on the involved knapsacks and applies to more l_p norms. Our observation illustrates that the Chor–Rivest, Okamoto–Tanaka–Uchiyama, and Kate–Goldberg cryptosystems are more vulnerable to lattice attacks.

5 Acknowledgments

The authors thank the anonymous reviewers' valuable comments, which simplify the reduction and essentially improve the quality of the paper. This work is supported by the National Key R&D Program of China under grant no. 2017YFB0802000, the National Natural Science Foundation of China under grant nos. 61572390 and U1736111, the Program for Science & Technology Innovation Talents in Universities of Henan Province under grant no. 18HASTIT022, the Plan for Scientific Innovation Talent of Henan Province (2018JQ0012), the Foundation of Henan Educational Committee under grant nos. 16A520025 and 18A520047, the Foundation for University Key Teacher of Henan Province under grant no. 2016GGJS-141, the Natural Science Foundation of Ningbo City under grant no. 201601HJ-B01382, and the Open Foundation of Key Laboratory of Cognitive Radio and Information Processing, Ministry of Education (Guilin University of Electronic Technology) under grant no. CRKL160202, the Open Project Foundation of Information Technology Research Base of Civil Aviation Administration of China under grant no. CAAC-ITRB-201702, and the Innovation Scientists and Technicians Troop Construction Projects of Henan Province.

6 References

[1] Schroeppel, R., Shamir, A.: 'A $T = \mathcal{O}(2^{n/2}), S = \mathcal{O}(2^{n/4})$ algorithm for certain NP-complete problems', *SIAM J. Computing*, 1981, **10**, (3), pp. 456–464

[2] Howgrave-Graham, N., Joux, A.: 'New generic algorithms for hard knapsacks'. Advances in Cryptology – EUROCRYPT 2010, French Riviera, May 30–June 3, 2010 (LNCS, **6110**), pp. 235–256

[3] Becker, A., Coron, J., Joux, A.: 'Improved generic algorithms for hard knapsacks', in Advances in Cryptology – EUROCRYPT 2011, Tallinn, Estonia, May 15–19, 2011 (LNCS, **6632**), pp. 364–385

[4] Garey, M.R., Johnson, D.S.: '*Computers and intractability, a guide to the theory of NP-completeness*' (W. H. Freeman, New York, USA, 1979, 1st edn.)

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

[6] Odlyzko, A.M.: 'The rise and fall of knapsack cryptosystems', in '*Cryptology and computational number theory*', Proc. Symposia in Applied Mathematics, vol. 42 (American Mathematical Society, Providence, 1990), pp. 75–88

[7] Lai, M.K.: 'Knapsack cryptosystems: the past and the future', available at http://www.ics.uci.edu/mingl/knapsack.html, accessed 2003

[8] Brickell, E.F.: 'Solving low density knapsacks', in Chaum, D. (ed.): '*Advances in cryptology*' (Springer, Boston, MA, 1984), pp. 25–37

[9] Lagarias, J.C., Odlyzko, A.M.: 'Solving low-density subset sum problems'. 24th Annual Symp. on Foundations of Computer Science (FOCS 1983), Tucson, Arizona, USA, 7–9 November 1983, pp. 229–246

[10] Lagarias, J. C., Odlyzko, A. M.: 'Solving low-density subset sum problems', *J. ACM*, 1985, **32**, pp. 229–246

[11] Coster, M.J., LaMacchia, B.A., Odlyzko, A.M., *et al.*: 'An improved low-density subset sum algorithm'. Advances in Cryptology – EUROCRYPT'91, April 8–11, 1991 (LNCS, **547**), pp. 54–67

[12] Joux, A., Stern, J.: 'Improving the critical density of the Lagarias-Odlyzko attack against subset sum problems'. Proc. 8th Int. Conf. of Fundamentals of Computation Theory – FCT 1991, Gosen, Germany, September 9–13, 1991 (LNCS, **529**), pp. 258–264

[13] Coster, M.J., Joux, A., LaMacchia, B.A., *et al.*: 'Improved low-density subset sum algorithms', *Comput. Complexity*, 1992, **2**, (2), pp. 111–128

[14] Chor, B., Rivest, R.L.: 'A knapsack-type public key cryptosystem based on arithmetic in finite fields (preliminary draft)'. Advances in Cryptology CRYPTO'84, Santa Barbara, California, USA, August 19–22, 1984 (LNCS, **196**), pp. 54–65

[15] Chor, B., Rivest, R.L..: 'A knapsack-type public key cryptosystem based on arithmetic in finite fields', *IEEE Trans. Inf. Theory*, 1988, **IT-34**, pp. 901–909

[16] Vaudenay, S.: 'Cryptanalysis of the Chor-Rivest cryptosystem', *J. Cryptol.*, 2001, **14**, pp. 87–100

[17] Encinas, L.H., Masqué, J. M., Dios, A.Q.: 'Maple implementation of the Chor-Rivest cryptosystem'. Proc. 6th Int. Conf. on Computational Science – ICCS 2006, Reading, UK, May 28–31, 2006 (LNCS, **3992**), pp. 438–445

[18] Encinas, L.H., Masqué, J.M., Dios, A.Q.: 'Safer parameters for the Chor-Rivest cryptosystem', *Comput. Math. Appl.*, 2008, **56**, (11), pp. 2883–2886

[19] Encinas, L.H., Masqué, J.M., Dios, A.Q.: 'Analysis of the efficiency of the Chor-Rivest cryptosystem implementation in a safe-parameter range', *Inf. Sci.*, 2009, **179**, (24), pp. 4219–4226

[20] Okamoto, T., Tanaka, K., Uchiyama, S.: 'Quantum public-key cryptosystems'. Advances in Cryptology – Crypto 2000, Santa Barbara, California, USA, August 20–24, 2000 (LNCS, **1880**), pp. 147–165

[21] Shor, P.W.: 'Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer', *SIAM J. Comput.*, 1997, **26**, **5**, pp. 1484–1509

[22] Kate, A., Goldberg, I.: 'Generalizing cryptosystems based on the subset sum problem', *Int. J. Inf. Secur.*, 2011, **10**, (3), pp. 189–199

[23] Damgard, I., Jurik, M.: 'A generalisation, a simplification and some applications of Paillier's probabilistic public-key system'. Proc. 4th Int. Conf. on Practice and Theory in Public-Key Cryptography – PKC '01, Cheju Island, Korea, February 13–15, 2001 (LNCS, **1992**), pp. 119–136

[24] Oomura, K., Tanaka, K.: 'Density attack to the knapsack cryptosystems with enumerative source encoding', *IEICE Trans. Fund.*, 2001, **E84-A**, (1), pp. 1564–1569

[25] Nguyen, P., Stern, J.: 'Adapting density attacks to low-weight knapsacks'. Advances in Cryptology – ASIACRYPT 2005, Chennai, India, December 4–8, 2005 (LNCS, **3788**), pp. 41–58

[26] Izu, T., Kogure, J., Koshiba, T., *et al.*: 'Low-density attack revisited', *Des. Codes Cryptogr.*, 2007, **43**, (1), pp. 47–59

[27] Kunihiro, N.: 'New definition of density on knapsack cryptosystems'. Progress in Cryptology – AFRICACRYPT 2008, June 11–14, 2008 (LNCS, **5023**), pp. 156–173

[28] Ajtai, M.: 'The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract)'. Proc. 13th Annual ACM Symp. on the Theory of Computing-STOC 1998, Dallas, Texas, USA, 24–26 May 1998, pp. 10–19

[29] Lenstra, A.K., Lenstra, H.W., Lovász, L.: 'Factoring polynomials with rational coefficients', *Math. Ann.*, 1982, **261**, (4), pp. 513–534

[30] Schnorr, C.P.: 'A hierarchy of polynomial time lattice basis reduction algorithms', *Theoret. Comput. Sci.*, 1987, **53**, (2–3), pp. 201–224

[31] Nguyen, P. Q., Stehle, D.: 'An LLL algorithm with quadratic complexity', *SIAM J. Comput.*, 2009, **39**, 3, pp. 874–903

[32] Nguyen, P.Q.: 'Cryptanalysis of the Goldreich–Goldwasser–Halevi cryptosystem from Crypto'97'. Advances in Cryptology – CRYPTO 1999, Santa Barbara, California, USA, August 15–19, 1999 (LNCS, **1666**), pp. 288–304

[33] Lee, M.S., Hahn, S.G.: 'Cryptanalysis of the GGH cryptosystem', *Math. Comput. Sci.*, 2010, **3**, (2), pp. 201–208

[34] Schnorr, C.P., Hörner, H.H.: 'Attacking the Chor–Rivest cryptosystem by improved lattice reduction'. Advances in Cryptology – Eurocrypt 1995, Saint-Malo, France, May 21–25, 1995 (LNCS, **921**), pp. 1–12

[35] Damgard, I.B.: 'A design principle for hash functions'. Advances in Cryptology – CRYPTO'89, Santa Barbara, California, USA, August 20–24, 1989 (LNCS, **435**), pp. 416–427