Advances in Cryptology – Proceedings of CRYPTO '97
(August 17–21, 1997, Santa Barbara, California, USA)
B. Kaliski (Ed.), vol. 1294 of Lecture Notes in Computer Science, pages 198–212

Merkle-Hellman Revisited: A Cryptanalysis of the Qu-Vanstone Cryptosystem Based on Group Factorizations

Phong Nguyen and Jacques Stern

École Normale Supérieure
Laboratoire d'Informatique
45, rue d'Ulm
F – 75230 Paris Cedex 05
{Phong.Nguyen,Jacques.Stern}@ens.fr
http://www.dmi.ens.fr/~{pnguyen,stern}/

Abstract. Cryptosystems based on the knapsack problem were among the first public key systems to be invented and for a while were considered quite promising. Basically all knapsack cryptosystems that have been proposed so far have been broken, mainly by means of lattice reduction techniques. However, a few knapsack-like cryptosystems have withstood cryptanalysis, among which the Chor-Rivest scheme [2] even if this is debatable (see [16]), and the Qu-Vanstone scheme proposed at the Dagstuhl'93 workshop [13] and published in [14]. The Qu-Vanstone scheme is a public key scheme based on group factorizations in the additive group of integers modulo n that generalizes Merkle-Hellman cryptosystems. In this paper, we present a novel use of lattice reduction, which is of independent interest, exploiting in a systematic manner the notion of an orthogonal lattice. Using the new technique, we successfully attack the Qu-Vanstone cryptosystem. Namely, we show how to recover the private key from the public key. The attack is based on a careful study of the so-called Merkle-Hellman transformation.

1 Introduction

The knapsack problem is as follows : given a set $\{a_1, a_2, \ldots, a_n\}$ of positive integers and a sum $s = \sum_{i=1}^{n} x_i a_i$, where each $x_i \in \{0, 1\}$, recover the x_i. It is well known that this problem is NP-complete, and accordingly it is considered to be quite hard in the worst case. However some knapsacks are very easy to solve : if the set $S = \{a_1, a_2, \ldots, a_n\}$ of positive integers is a *superincreasing sequence*, *e.g.*

$$\forall i \geq 2 \ \ a_i > \sum_{j=1}^{i-1} a_j,$$

then the corresponding knapsack can easily be solved in linear time. Most of the public key schemes based on knapsacks are of the following form :

The Public Key: a set of positive integers $\{a_1, a_2, \ldots, a_n\}$.
The Private Key: a method to transform the presumed hard public knapsack into an easy knapsack.
The Message Space: all $0-1$ vectors of length n.
Encryption: a message $M = (x_1, x_2, \ldots, x_n)$ is enciphered into $C = \sum_{i=1}^{n} x_i a_i$.

In 1978, Merkle and Hellman [10] devised a method to convert superincreasing sequences into what they believed were hard knapsacks. If $S = \{a_1, a_2, \ldots, a_n\}$ is a superincreasing sequence and $a = \sum_{i=1}^{n} a_i$, select two coprime integers m and w such that $m > a$. The *Merkle-Hellman transformation* associated with the pair (m, w) is the function f that maps any $x \in \{0, 1, \ldots, m-1\}$ to the least positive residue of wx modulo m. This function is a permutation, and its reciprocal f^{-1} maps any $y \in \{0, 1, \ldots, m-1\}$ to the least positive residue of $w^{-1}y$ modulo m, where w^{-1} is an inverse of w modulo m. Merkle and Hellman applied such a transformation f to form a new knapsack $\bar{S} = \{b_1, b_2, \ldots, b_n\}$ where $b_i = f(a_i)$. To decrypt a ciphertext $c = \sum_{i=1}^{n} x_i b_i$, one computes $f^{-1}(c)$. Since

$$f^{-1}(c) \equiv \sum_{i=1}^{n} x_i b_i w^{-1} \equiv x_i a_i \pmod{m},$$

with $\sum_{i=1}^{n} x_i a_i \leq a < m$, we have $f^{-1}(c) = \sum_{i=1}^{n} x_i a_i$. By solving the easy knapsack $S = \{a_1, a_2, \ldots, a_n\}$, one recovers the x_i. Applying a sequence of Merkle-Hellman transformations is not equivalent to a single application, and hence, should enhance the security of the system. Unfortunately, these systems were both shown to be insecure (see [17, 1]). Despite the failure of Merkle-Hellman cryptosystems, researchers continued to search for knapsack-like cryptosystems because such systems are very easy to implement and can attain very high encryption/decryption rates. But most of the proposed knapsack-like cryptosystems have been broken (for a survey, see [12]), either by specific attacks or by the so-called low-density attacks.

The *density* of a knapsack $S = \{a_1, a_2, \ldots, a_n\}$ is defined to be $d = \frac{n}{N}$ where $N = \max_{1 \leq i \leq n} \log_2 a_i$. When the density is small (namely, less than 0.94...), one can prove the knapsack problem can be solved using lattice reduction with high probability (see [4]). Such attacks are called low-density attacks. The attack has recently been improved by [16], but is still uneffective against high-density knapsacks. The few knapsack cryptosystems that have so far withstood all attacks use knapsacks of high density. In [13], Qu and Vanstone showed that Merkle-Hellman knapsack cryptosystems could be viewed as special cases of knapsack-like cryptosystems arising from subset factorizations in finite groups. They proposed a generalization of these knapsack cryptosystems by constructing a supposedly hard factorization of finite group, using Merkle-Hellman-like transformations and superincreasing sequences. This hard factorization problem can be restated as a knapsack problem of density higher than 3. We will attack the Qu-Vanstone system by showing how to recover the hidden easy factorization (the private key) from the presumed hard factorization (the public key), in a reasonable time.

2 The orthogonal lattice

We will use the word *lattice* for any integer lattice, that is any additive subgroup of $\mathbf{Z}^n$. Background on lattices can be found in [5, 3]. We denote vectors by bold-face lowercase letters. Let Λ be a lattice in $\mathbf{Z}^n$.

Let $\mathbf{b}_1, \ldots, \mathbf{b}_d$ be vectors of Λ. These d vectors form a *basis* of Λ if they are linearly independent over $\mathbf{Z}$, and if any element of Λ can be expressed as a linear combination of the $\mathbf{b}_i$'s with integral coefficients. There exists at least one basis of Λ. The bases of Λ all have the same cardinality, called the *dimension* of Λ. We say that Λ is a *sublattice* of a lattice Ω in $\mathbf{Z}^n$ if Ω contains Λ and if both have the same dimension. All bases of Λ span the same $\mathbf{Q}$-vector subspace of $\mathbf{Q}^n$, which we denote by E_Λ. The dimension of E_Λ over $\mathbf{Q}$ is equal to the dimension of Λ. Define the lattice $\overline{\Lambda} = E_\Lambda \cap \mathbf{Z}^n$. Λ is a sublattice of $\overline{\Lambda}$. We say that Λ is a *complete lattice* if $\Lambda = \overline{\Lambda}$. In particular, $\overline{\Lambda}$ is a complete lattice.

Let $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x}.\mathbf{y}$ be the usual euclidian inner product, and $\|.\|$ be its corresponding norm. Let $F = (E_\Lambda)^\perp$ be the orthogonal vector subspace with respect to this inner product. We define the *orthogonal lattice* to be $\Lambda^\perp = F \cap \mathbf{Z}^n$. Thus, $\Lambda^\perp$ is a complete lattice in $\mathbf{Z}^n$, with dimension $n - d$ if d is the dimension of Λ. This implies that $(\Lambda^\perp)^\perp$ is equal to $\overline{\Lambda}$. Let $\mathcal{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_d)$ be a basis of Λ. Decompose each $\mathbf{b}_j$ over the canonical basis of $\mathbf{Z}^n$ as :

$$\mathbf{b}_j = \begin{pmatrix} b_{1,j} \\ b_{2,j} \\ \vdots \\ b_{n,j} \end{pmatrix}$$

Define the $n \times d$ integral matrix $B = (b_{i,j})_{1 \le i \le n, 1 \le j \le d}$. The lattice Λ is spanned by the columns of B : we say that Λ is *spanned* by B. Let $Q = {}^tBB$ be the $d \times d$ symmetric Gram matrix. The determinant of Q is a positive integer independent of $\mathcal{B}$. The *determinant* of Λ is defined as $\det(\Lambda) = \sqrt{\det(B)}$.

Theorem 1. *Let Λ be a complete lattice in $\mathbf{Z}^n$. Then $\det(\Lambda^\perp) = \det(\Lambda)$.*

Proof. We have $\Lambda = E_\Lambda \cap \mathbf{Z}^n$ and $\Lambda^\perp = E_\Lambda^\perp \cap \mathbf{Z}^n$. We know from [9] that :

$$\det(\mathbf{Z}^n) = \frac{\det(E_\Lambda \cap \mathbf{Z}^n)}{\det((E_\Lambda)^\perp \cap (\mathbf{Z}^n)^*)},$$

where $(\mathbf{Z}^n)^*$ denotes the polar lattice of $\mathbf{Z}^n$. But $\det(\mathbf{Z}^n) = 1$ and $(\mathbf{Z}^n)^* = \mathbf{Z}^n$, therefore $\det(\Lambda^\perp) = \det(\Lambda)$.

Corollary 2. *Let Λ be a lattice in $\mathbf{Z}^n$. Then $\det((\Lambda^\perp)^\perp) = \det(\Lambda^\perp) = \det(\overline{\Lambda})$.*

In 1982, Lenstra, Lenstra and Lovász introduced the famous LLL-algorithm [8], a polynomial time algorithm that computes a so-called LLL-reduced basis of any given lattice. For definitions and proofs regarding LLL-reduced bases, we refer to [8, 3]. In this paper, we only need the following properties of LLL-reduced bases :

Theorem 3. *Let* $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ *be an LLL-reduced basis of a lattice* Λ *in* $\mathbf{Z}^n$*. Then :*

1. $\det(\Lambda) \leq \prod_{i=1}^{d} \|\mathbf{b}_i\| \leq 2^{d(d-1)/4} \det(\Lambda)$.
2. *For any linearly independent vectors* $\mathbf{x}_1, \ldots, \mathbf{x}_t \in \Lambda$*, and* $1 \leq j \leq t$ *:*

$$\|\mathbf{b}_j\| \leq 2^{(d-1)/2} \max(\|\mathbf{x}_1\|, \ldots, \|\mathbf{x}_t\|).$$

We now describe a basic algorithm to compute an LLL-reduced basis of an orthogonal lattice. Let $\mathcal{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_d)$ be a basis of Λ, and $B = (b_{i,j})$ be its corresponding $n \times d$ matrix. Let c be a positive integer constant. Define Ω to be the lattice in $\mathbf{Z}^{n+d}$ spanned by the following $(n+d) \times n$ matrix :

$$B^{\perp} = \begin{pmatrix} c \times b_{1,1} & c \times b_{2,1} & \ldots & c \times b_{n,1} \\ c \times b_{1,2} & c \times b_{2,2} & \ldots & c \times b_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ c \times b_{1,d} & c \times b_{2,d} & \ldots & c \times b_{n,d} \\ 1 & 0 & \ldots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \ldots & 1 \end{pmatrix}$$

A similar matrix is used in [7]. The matrix $B^{\perp}$ is divided in two blocks : the upper $d \times n$ block is $c\,{}^tB$ and the lower $n \times n$ block is the identity matrix. Let $p_{\uparrow}$ and $p_{\downarrow}$ be the two projections that map any vector of $\mathbf{Z}^{n+d}$ to respectively the vector of $\mathbf{Z}^d$ made of its first d coordinates, and the vector of $\mathbf{Z}^n$ of its last n coordinates, all with respect to the canonical basis. Let $\mathbf{x}$ be a vector of Ω and denote $\mathbf{y} = p_{\downarrow}(\mathbf{x})$. Then

$$p_{\uparrow}(\mathbf{x}) = c \begin{pmatrix} \mathbf{y}.\mathbf{b}_1 \\ \vdots \\ \mathbf{y}.\mathbf{b}_d \end{pmatrix}.$$

Hence, $\mathbf{y} \in \Lambda^{\perp}$ if and only if $p_{\uparrow}(\mathbf{x}) = 0$. Furthermore, if $\|\mathbf{x}\| \leq c$, then $p_{\uparrow}(\mathbf{x}) = 0$.

Theorem 4. *Let* $(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)$ *be an LLL-reduced basis of* Ω*. If*

$$c > 2^{(n-1)/2+(n-d)(n-d-1)/4} \det(\overline{\Lambda}),$$

then $(p_{\downarrow}(\mathbf{x}_1), p_{\downarrow}(\mathbf{x}_2), \ldots, p_{\downarrow}(\mathbf{x}_{n-d}))$ *is an LLL-reduced basis of* $\Lambda^{\perp}$*.*

Using Hadamard's inequality, we derive the following algorithm :

Algorithm 5. *Given a basis* $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_d)$ *of a lattice* Λ *in* $\mathbf{Z}^n$*, this algorithm computes an LLL-reduced basis of* $\Lambda^{\perp}$*.*

1. *Select* $c = \lceil 2^{(n-1)/2+(n-d)(n-d-1)/4} \prod_{j=1}^{d} \|\mathbf{b}_j\| \rceil$.

2. *Compute the* $(n+d)\times n$ *integral matrix* $B^{\perp}$ *from* c *and the* $n \times d$ *matrix* $B = (b_{i,j})$ *corresponding to* $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_d$.
3. *Compute an LLL-reduced basis* $(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)$ *of the lattice spanned by* $B^{\perp}$.
4. *Output* $(p_{\downarrow}(\mathbf{x}_1), p_{\downarrow}(\mathbf{x}_2), \ldots, p_{\downarrow}(\mathbf{x}_{n-d}))$.

One can prove that this is a deterministic polynomial time algorithm with respect to the space dimension n, the lattice dimension d and any upper bound of the bit-length of the $\|\mathbf{b}_j\|$'s. In practice, one does not need to select such a large constant c because the theoretical bounds of the LLL algorithm (theorem 3) are quite pessimistic. We will use this algorithm throughout the attack.

3 The cryptanalysis of the Qu-Vanstone scheme

3.1 High level description of the Qu-Vanstone scheme

Since the Qu-Vanstone scheme is quite complicated, we give a simplified exposure. Additional information can be found in appendix and in [13, 14].

Let n be a positive integer of the form $n = d_1 d_2 d_3 d_4 d_5$, where $2^{s-1} \leq d_\ell < 2^s$ (for $\ell = 1, 2, 3, 4$), $d_5 \leq 16$, and s is some fixed even positive integer. Let $G = \mathbf{Z}_n$ be the additive group of integers modulo n. Qu and Vanstone found a way to build an efficient subset factorization in G. Namely, with help of 4 superincreasing sequences and 4 Merkle-Hellman transformations, they construct s blocks $C_i = \{c[i,j] \;:\; 0 \leq j \leq 15\}$ of 16 integers of G where $1 \leq i \leq s$ such that : for any $g \in G$ of form $g = \sum_{i=1}^{s} c[i, j_i] \pmod{n}$, one can quickly recover the j_i's from g and a trapdoor. This construction is intricate, a detailed description can be found in the appendix.

Qu and Vanstone further use k additional Merkle-Hellman-like transformations and s permutations to hide the subset factorization. The process consists of k iterations, starting with $m^{(0)} = n$ and $c^{(0)}[i,j] = c[i,j]$, $1 \leq i \leq s$, $0 \leq j \leq 15$. Consider the eth iteration $(1 \leq e \leq k)$:

- select s positive integers $a_1^{(e-1)}, \ldots, a_s^{(e-1)}$ such that $0 \leq a_i^{(e-1)} < m^{(e-1)}$, and define $\bar{c}^{(e)}[i,j] = c^{(e-1)}[i,j] + a_i^{(e-1)} \pmod{m^{(e-1)}}$.
- select $m^{(e)}$ strictly greater than $\sum_{i=1}^{s} \max_{0 \leq j \leq 15} \bar{c}^{(e)}[i,j]$. Choosing $w^{(e)}$ coprime to $m^{(e)}$, define $c^{(e)}[i,j] = w^{(e)} \bar{c}^{(e)}[i,j] \pmod{m^{(e)}}$.

These Merkle-Hellman-like transformations differ from the original Merkle-Hellman transformations by the use of a modular addition which is performed before the modular multiplication. Now that the $c^{(k)}[i,j]$'s are defined, select s permutations $\pi_1, \ldots, \pi_s$ acting on $\{0, 1, \ldots, 15\}$. Let

$$d[i,j] = c^{(k)}[i, \pi_i^{-1}(j)] - c^{(k)}[i, \pi_i^{-1}(0)] \pmod{m^{(k)}}.$$

Notice that $d[i,0] = 0$. Let $C = \sum_{i=1}^{s} c^{(k)}[i, \pi_i^{-1}(0)] \pmod{m^{(k)}}$.

The public key consists of the s blocks $D_i = \{d[i,j] \;:\; 0 \leq j \leq 15\}$, that is $15s$ non-zero positive integers. The private key is : C, π_i's, $w^{(e)}$'s, $m^{(e)}$'s, $\sum_{i=1}^{s} a_i^{(e)}$'s and the trapdoor corresponding to the subset factorization.

The message space is $\mathbf{Z}_{16^s}$, and the numbers in each D_i are roughly around $s^k n$. Qu and Vanstone suggested $s \geq 32$ and $k \geq 3$. In the smallest case, the message space is $\mathbf{Z}_{128}$, and the maximum element in the public key is less than 2^{151}. The keys are quite large but encryption/decryption rates are high.

To encode a message m, write m in its base 16 expansion as $m = p_1 + 16p_2 + \cdots + 16^{s-1}p_s$, where $0 \leq p_i \leq 15$. Then the ciphertext associated with m is

$$c = d[1, p_1] + d[2, p_2] + \cdots + d[s, p_s].$$

To decrypt c, compute $c^{(k)} = c + C \pmod{m^{(k)}}$. Then invert Merkle-Hellman-like transformations by applying the following process with $e = k, k-1, \ldots, 1$:

$$\begin{aligned} \overline{c}^{(e)} &= (w^{(e)})^{-1} c^{(e)} \pmod{m^{(e)}}, \\ c^{(e-1)} &= \overline{c}^{(e)} - \textstyle\sum_{i=1}^{s} a_i^{(e-1)} \pmod{m^{(e-1)}}. \end{aligned}$$

At this point, $c^{(0)} = \sum_{i=1}^{s} c[i, j_i] \pmod{n}$ where each $j_i = \pi_i^{-1}(p_i)$ is still unknown. From the subset factorization trapdoor, the j_i's can be recovered. This technical step is described in the appendix. From the j_i's, one computes $p_i = \pi_i(j_i)$ and the message $m = p_1 + 16p_2 + \cdots + 16^{s-1}p_s$.

This public key system has features similar to the original knapsack scheme. The security rests on the Merkle-Hellman-like transformations that hide the 4 superincreasing sequences and the coset structure. The knapsack based on the blocks D_i has density higher than 3, so it looks immune to the usual low-density attacks. Qu and Vanstone discuss several attacks on this system in their paper [13]. We now describe our attack which mainly consists of two steps : we first attack Merkle-Hellman-like transformations by reducing several orthogonal lattices, then we compute successive orthogonal lattices to reveal the secret key. The first step is quite general but the second step is based on the particular structure of the hidden subset factorization. We advise to read the further description of the Qu-Vanstone scheme given in appendix in order to fully understand the second step.

3.2 Peeling off Merkle-Hellman transformations

Let N be an integer and $\mathbf{c}^{(0)}, \mathbf{c}^{(1)}, \ldots, \mathbf{c}^{(k)}$ be vectors of $\mathbf{Z}^N$ such that :

$$\|\mathbf{c}^{(e)}\| \leq \sqrt{N} m^{(e)},\ 0 \leq e \leq k \tag{1}$$

$$\mathbf{c}^{(e)} \equiv w^{(e)} \mathbf{c}^{(e-1)} \pmod{m^{(e)}},\ 1 \leq e \leq k \tag{2}$$

Note that in equation (2), we mean component-wise operations and that we only assume congruences, not necessarily equalitities. Under these hypotheses (1) and (2), we will see that $\mathbf{c}^{(0)}$ and $\mathbf{c}^{(k)}$ almost share the same orthogonal lattice.

Heuristic 6. *Let Λ be the lattice spanned by $\mathbf{c}^{(k)}$. Let $(\mathbf{e}_1, \ldots, \mathbf{e}_{N-1})$ be an LLL-reduced basis of $\Lambda^\perp$. If we denote by Γ the lattice spanned by $(\mathbf{e}_1, \ldots, \mathbf{e}_{N-k-1})$, then $\mathbf{c}^{(0)} \in \Gamma^\perp$.*

This heuristic confines $\mathbf{c}^{(0)}$ in a low-dimensional lattice that we can determine just by knowing $\mathbf{c}^{(k)}$. When $m^{(0)} \ll m^{(1)} \ll \cdots \ll m^{(k)}$, this heuristic works well in practice. Namely, if we define

$$m = \min \left\{ \frac{m^{(1)}}{m^{(0)}}, \frac{m^{(2)}}{m^{(1)}}, \ldots, \frac{m^{(k)}}{m^{(k-1)}} \right\},$$

experiments show that the heuristic is verified as soon as $m \geq 8$ and $N \geq 50$. We are unable to prove this heuristic, but we can offer some explanations.

Lemma 7. *Let* $\mathbf{x}$ *be a vector of* $\mathbf{Z}^N$ *such that* $\mathbf{x} \perp \mathbf{c}^{(k)}$ *and* $||\mathbf{x}|| < m/\sqrt{N}$. *Then* $\mathbf{x}$ *is orthogonal to* $\mathbf{c}^{(k-1)}, \mathbf{c}^{(k-2)}, \ldots, \mathbf{c}^{(0)}$.

Proof. We have $\mathbf{x}.\mathbf{c}^{(k-1)} \equiv 0 \pmod{m^{(k)}}$ since $\mathbf{c}^{(k)} \equiv w^{(k)}\mathbf{c}^{(k-1)} \pmod{m^{(k)}}$ and $\mathbf{x}.\mathbf{c}^{(k)} = 0$. If we assume that $\mathbf{x}$ is not orthogonal to $\mathbf{c}^{(k-1)}$, then $|\mathbf{x}.\mathbf{c}^{(k-1)}| \geq m^{(k)}$. Therefore, by Cauchy-Schwarz and inequality (1) :

$$m^{(k)} \leq \|\mathbf{x}\|.\|\mathbf{c}^{(k-1)}\| \leq \|\mathbf{x}\| m^{(k-1)}\sqrt{N}.$$

This contradicts the fact that $\|\mathbf{x}\| \leq m/\sqrt{N}$. Thus $\mathbf{x} \perp \mathbf{c}^{(k-1)}$. Iterating this process, we find that $\mathbf{x}$ is orthogonal to $\mathbf{c}^{(k-2)}, \ldots, \mathbf{c}^{(0)}$.

This means that if $\mathbf{x} \in \Lambda^{\perp}$ is short enough, then $\mathbf{x}$ is orthogonal to $\mathbf{c}^{(0)}$. Now we will see that there exist $N-k-1$ independent vectors of $\Lambda^{\perp}$ that are short, and hopefully short enough.

Lemma 8. *Let* Ω *be the lattice spanned by*

$$\left(\mathbf{c}^{(0)}, \lfloor \frac{w^{(1)}\mathbf{c}^{(0)}}{m^{(1)}} \rfloor, \lfloor \frac{w^{(2)}\mathbf{c}^{(1)}}{m^{(2)}} \rfloor, \ldots, \lfloor \frac{w^{(k)}\mathbf{c}^{(k-1)}}{m^{(k)}} \rfloor \right).$$

Then $\left(\mathbf{c}^{(0)}, \mathbf{c}^{(1)}, \ldots, \mathbf{c}^{(k)}\right)$ *is a sublattice of* Ω, *and*

$$\det(\Omega) \leq ||\mathbf{c}^{(0)}|| N^{k/2} < m^{(0)} N^{(k+1)/2}.$$

Proof. We have $\mathbf{c}^{(e)} = w^{(e)}\mathbf{c}^{(e-1)} - m^{(e)} \lfloor \frac{w^{(e)}\mathbf{c}^{(e-1)}}{m^{(e)}} \rfloor$ for $1 \leq e \leq k$. Therefore $(\mathbf{c}^{(0)}, \mathbf{c}^{(1)}, \ldots, \mathbf{c}^{(k)})$ is a sublattice of Ω. Furthermore :

$$\begin{aligned}\det(\Omega) &= \|\mathbf{c}^{(0)} \wedge \lfloor \frac{w^{(1)}\mathbf{c}^{(0)}}{m^{(1)}} \rfloor \wedge \cdots \wedge \lfloor \frac{w^{(k)}\mathbf{c}^{(k-1)}}{m^{(k)}} \rfloor \| \\ &= \|\mathbf{c}^{(0)} \wedge (\frac{w^{(1)}\mathbf{c}^{(0)}}{m^{(1)}} - \lfloor \frac{w^{(1)}\mathbf{c}^{(0)}}{m^{(1)}} \rfloor) \wedge \cdots \wedge (\frac{w^{(k)}\mathbf{c}^{(k-1)}}{m^{(k)}} - \lfloor \frac{w^{(k)}\mathbf{c}^{(k-1)}}{m^{(k)}} \rfloor)\|.\end{aligned}$$

Since $\| \frac{w^{(e)}\mathbf{c}^{(e-1)}}{m^{(e)}} - \lfloor \frac{w^{(e)}\mathbf{c}^{(e-1)}}{m^{(e)}} \rfloor \| \leq \sqrt{N}$, this proves that :

$$\det(\Omega) \leq ||\mathbf{c}^{(0)}|| N^{k/2} < m^{(0)} N^{(k+1)/2}.$$

Since $\det(\Omega^{\perp}) = \det(\overline{\Omega})$, we can thus hope that there exists a basis of $\Omega^{\perp}$ whose vectors have norm less than $m' = (m^{(0)}N^{(k+1)/2})^{1/(N-k-1)}$. But these $N-k-1$ vectors also belong to $\Lambda^{\perp}$, so the first $N-k-1$ vectors of any LLL-reduced basis of $\Lambda^{\perp}$ are likely to have norm less than m'. Since m' is very small (smaller than $m/\sqrt{N}$ most of the time), it is not surprising that by lemma 7 $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_{N-k-1}$ are orthogonal to $\mathbf{c}^{(0)}$, which implies that $\mathbf{c}^{(0)} \in \Gamma^{\perp}$.

Although the Qu-Vanstone scheme uses Merkle-Hellman-like transformations instead of Merkle-Hellman transformations, there are particular vectors related to the scheme that satisfy conditions (1) and (2).

Let $N = 15s$. We index the coordinates of any vector of $\mathbf{Z}^N$ by $\gamma(i,j) = 15(i-1)+j-1$, where $1 \leq i \leq s$, $1 \leq j \leq 15$. From the public key, we construct the vector $\mathbf{c}^{(k)}$ whose $\gamma(i,j)$ entry is $d[i,j]$. For $e = k-1, k-2, \ldots, 0$, let $\mathbf{c}^{(e)}$ be the (unknown) vector whose $\gamma(i,j)$ entry is $\bar{c}^{(e)}[i, \pi_i^{-1}(j)] - \bar{c}^{(e)}[i, \pi_i^{-1}(0)]$.

Lemma 9. *The vectors $\mathbf{c}^{(0)}, \mathbf{c}^{(1)}, \ldots, \mathbf{c}^{(k)}$ satisfy conditions (1) and (2).*

Proof. Since the coordinates of each $\mathbf{c}^{(e)}$ are less than $m^{(e)}$ in absolute value, we have (1). Write the Merkle-Hellman-like equations defining $d[i,j]$'s starting with $c^{(k)}[i,j]$'s, ending with $c^{(0)}[i,j]$'s. Collecting additions and multiplications that use the same modulus, $a_i^{(e)}$'s disappear by subtraction, proving (2).

From the description of the scheme, we know that $m \approx s \geq 32$, therefore heuristic 6 is likely to be satisfied. Hence, applying algorithm 5 twice, we can construct $k+1$ vectors $\mathbf{e}_1, \ldots, \mathbf{e}_{k+1}$ of $\mathbf{Z}^N$ such that there exist $\lambda_1, \ldots, \lambda_{k+1} \in \mathbf{Z}$ satisfying

$$\mathbf{c}^{(0)} = \lambda_1 \mathbf{e}_1 + \lambda_2 \mathbf{e}_2 + \cdots + \lambda_{k+1} \mathbf{e}_{k_1}.$$

In the second step of the attack, we determine these unknown integers λ_j. The knowledge of $\mathbf{c}^{(0)}$ then reveals the trapdoor and the rest of the secret key : this is sketched in the appendix because it is based on the structure of the subset factorization. We emphasize that the difficult part of the attack is to determine $\mathbf{c}^{(0)}$, not to obtain the secret key from $\mathbf{c}^{(0)}$ which is rather easy.

3.3 Breaking the kernel of the system

We say that $C_i = \{c[i,j] \ : \ 0 \leq j \leq 15\}$ is a *weak block* if $f(i)$ is of form $(4, i')$. For the definition of f, we refer to the description of the scheme in appendix. Clearly, half of the s blocks C_i are weak blocks. We call these blocks weak due to the following :

Lemma 10. *Let $C_i = \{c[i,j] \ : \ 0 \leq j \leq 15\}$ be a weak block.*

1. *For $j \in \{0, 4, 8, 12\}$, we have*

$$c[i,j+1] + c[i,j+2] \equiv c[i,j] + c[i,j+3] \pmod{d_1 d_2 d_3 d_4}.$$

2. *There exist distinct $j_1(i)$, $j_2(i)$ and $j_3(i)$ computable from π_i such that*

$$\hat{c}[i, j_1(i)] + \hat{c}[i, j_2(i)] - \hat{c}[i, j_3(i)] \equiv 0 \pmod{d_1 d_2 d_3 d_4},$$

where $\hat{c}[i,j]$ denotes the $\gamma(i,j)$ entry of $\mathbf{c}^{(0)}$.

Proof. From the definition of the $c[i,j]'s$, if $\lfloor j/4 \rfloor = \lfloor j'/4 \rfloor$ then

$$c[i,j] - c[i,j'] \equiv a^{v+2u}[f(i),w] - a^{v+2u}[f(i),w'] \pmod{n},$$

where $j = w + 4v + 8u$ and $j' = w' + 4v + 8u$. Since $f(i)$ is of form $(4,i')$, we obtain 1 by definition of $a^t[4,i',w]$. To prove 2, write $\pi_i^{-1}(0)$ as $j+\ell$ where $j = \lfloor \pi_i^{-1}(0)/4 \rfloor$. Apply 1 to find distinct j_1^*, j_2^*, j_3^* such that

$$c[i,j_1^*] + c[i,j_2^*] \equiv c[i,j_3^*] + c[i,j+\ell] \pmod{d_1 d_2 d_3 d_4}.$$

Conclude with $j_1(i) = \pi_i(j_1^*)$, $j_2 = \pi_i(j_2^*)$ and $j_3 = \pi_i(j_3^*)$.

To simplify the exposition of the attack, we now assume that f and the π_i's are known to the attacker. We will show how to adapt the attack to the general case at the end of the section. We define a transformation ϕ that maps any $\mathbf{x}$ of $\mathbf{Z}^N$ to

$$\phi(x) = \begin{pmatrix} x[i_1, j_1(i_1)] + x[i_1, j_2(i_1)] - x[i_1, j_3(i_1)] \\ x[i_2, j_1(i_2)] + x[i_2, j_2(i_2)] - x[i_2, j_3(i_2)] \\ \vdots \\ x[i_{s/2}, j_1(i_{s/2})] + x[i_{s/2}, j_2(i_{s/2})] - x[i_{s/2}, j_3(i_{s/2})] \end{pmatrix},$$

where $C_{i_1}, C_{i_2}, \ldots, C_{i_{s/2}}$ denote the $s/2$ weak blocks, and $x[i,j]$ denotes the $\gamma(i,j)$ entry of $\mathbf{x}$. One sees that ϕ is linear, which implies that

$$\phi(\mathbf{c}^{(0)}) = \lambda_1 \phi(\mathbf{e}_1) + \cdots + \lambda_{k+1} \phi(\mathbf{e}_{k+1}).$$

By lemma 10, the vector $\frac{\phi(\mathbf{c}^{(0)})}{d_1 d_2 d_3 d_4}$ has integral entries, so it must belong to $\overline{\Omega}$ where Ω denotes the lattice spanned by $\phi(\mathbf{e}_1), \phi(\mathbf{e}_2), \ldots, \phi(\mathbf{e}_{k+1})$, which we can determine. But this vector is unusually short : indeed, each coordinate of $\frac{\phi(\mathbf{c}^{(0)})}{d_1 d_2 d_3 d_4}$ is less than $3(d_5 - 1) \leq 45$ in absolute value, which makes a norm less than $45\sqrt{s/2}$ (note that this is a very pessimistic bound). Therefore it must have small coordinates with respect to any LLL-reduced basis because an LLL-reduced basis is almost orthogonal :

Lemma 11. *Let $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_d)$ be an LLL-reduced basis of a lattice Λ. If $\mathbf{x} = \sum_{j=1}^{d} x_j \mathbf{b}_j$ where $x_j \in \mathbf{R}$ then, for $1 \leq j \leq d$,*

$$|x_j|.\|\mathbf{b}_j\| \leq \|\mathbf{x}\| \sqrt{2^{j-1} \frac{(9/2)^{d-j} + 6}{7}}.$$

(this statement can be found in an unpublished draft [11] by P. Montgomery)

Proof. Denote by $(\mathbf{b}_1^*, \ldots, \mathbf{b}_d^*)$ the corresponding orthogonal Gram-Schmidt $\mathbf{Q}$-basis. Decompose $\mathbf{x}$ as $\mathbf{x} = \sum_{j=1}^{d} x_j^* \mathbf{b}_j^*$. By orthogonality, one finds that

$$x_j = x_j^* - \sum_{i=j+1}^{d} x_i \frac{\mathbf{b}_i.\mathbf{b}_j^*}{\|\mathbf{b}_j\|^2}.$$

It follows by induction on $d-j$ that :

$$|x_j| \leq |x_j^*| + \frac{1}{3}\sum_{i=j+1}^{d}(3/2)^{i-j}|x_i^*|.$$

Since $(\mathbf{b}_1,\ldots,\mathbf{b}_d)$ is an LLL-reduced basis, if $j \leq i$ then $\|\mathbf{b}_j\| \leq 2^{(i-1)/2}\|\mathbf{b}_i^*\|$. From this and Cauchy-Schwarz, we obtain

$$|x_j|^2\|\mathbf{b}_j\|^2 \leq 2^{j-1}(\sum_{i=j}^{d}|x_i^*|^2\|\mathbf{b}_i^*\|^2)(1+\frac{1}{3^2}((9/2)+\cdots+(9/2)^{d-j}),$$

and the result follows.

Hence, we compute an LLL-reduced basis $(\mathbf{b}_1,\ldots,\mathbf{b}_d)$ of $\overline{\Omega} = (\Omega^\perp)^\perp$ by applying algorithm 5 twice. The unknown vector $\frac{\phi(\mathbf{c}^{(0)})}{d_1d_2d_3d_4}$ has integral coordinates x_j with respect to $(\mathbf{b}_1,\ldots,\mathbf{b}_d)$. We make an exhaustive search on the x_j's within the bounds given by lemma 11. Since we are in low dimension ($d \leq k+1$), these bounds are very small, making exhaustive search possible.

Assume that one wants to check whether $\mathbf{x} = \sum_{j=1}^{d} x_j\mathbf{b}_j$ is the expected $\frac{\phi(\mathbf{c}^{(0)})}{d_1d_2d_3d_4}$. Decompose each $\mathbf{b}_j$ as a linear combination of $\phi(\mathbf{e}_\ell)$'s with rational coefficients. Derive an integral linear dependence relation of form

$$\mu\mathbf{x} = \mu_1\phi(\mathbf{e}_1)+\cdots+\mu_{k+1}\phi(\mathbf{e}_{k+1}),$$

where $\mu > 0$ and $gcd(\mu,\mu_1,\ldots,\mu_{k+1}) = 1$. Since

$$d_1d_2d_3d_4\frac{\phi(\mathbf{c}^{(0)})}{d_1d_2d_3d_4} = \lambda_1\phi(\mathbf{e}_1)+\cdots+\lambda_{k+1}\phi(\mathbf{e}_{k+1}),$$

it is likely that $d_1d_2d_3d_4 = \mu$ and $\lambda_j = \mu_j$ if $\mathbf{x}$ is the expected vector. Since $d_1d_2d_3d_4$ has bit-length $4s$, we can quickly check whether μ is consistent. Furthermore, we obtain $d_1d_2d_3d_4$ and the λ_j's, which gives $\mathbf{c}^{(0)}$. But we can easily check whether this is a consistent $\mathbf{c}^{(0)}$, because $\mathbf{c}^{(0)}$ reveals the trapdoor corresponding to the subset factorization (see the appendix). Hence, the exhaustive search is really feasible and provides the secret key.

Now if we do not know the permutations π_i's and the bijection f, we construct the linear transformation ϕ by choosing randomly 2 distinct integers i_1, i_2 between 1 and s : for each of these 2 integers, we select randomly 3 distinct j_1, j_2, j_3 between 1 and 15 such that $j_1 < j_2$. The probability that both i_1 and i_2 correspond to weak blocks is $1/4$. For each of these 2 integers, we have to test at most $15 \times \frac{14\times 13}{2} = 1365$ triplets (j_1, j_2, j_3) to find one that satisfies lemma 10. This means that we have to check at most $4 \times 1365^2 = 7452900$ choices of ϕ. But such a check can be done very quickly : if ϕ is correct, then $\overline{\Omega}$ has a very small vector (at least as short as $\frac{\phi(\mathbf{c}^{(0)})}{d_1d_2d_3d_4}$), and otherwise, there is no reason that such a situation happens. Since computing $\overline{\Omega}$ can be done in less than a second (involved lattices have very small dimension), we can check all choices of ϕ in a reasonable time (namely, less than one week with 10 workstations). Once a suitable ϕ has been found, we perform an exhaustive search on $\frac{\phi(\mathbf{c}^{(0)})}{d_1 d_2 d_3 d_4}$ as before. If one wants to improve success probabilities, one can increase the number of components of ϕ by adding new integers i, once a suitable ϕ with two components has been found. Each additional integer i costs at most 1365 tests and we can determine them successively, therefore we can easily determine the $s/2$ weak blocks, which reveals f. Then we apply the previous strategy in order to obtain the rest of the secret key.

3.4 Experiments

The attack has been successfully implemented using blockwise Korkine-Zolotarev lattice reductions [15] instead of LLL reductions to improve the reduced basis for heuristic 6. We used the package previously developped by A. Joux [6] in our lab. Timings are given for a 50Mhz Sparc 4, with parameters $s = 32$ and $k = 3$. It takes about 9 hours to obtain the $k+1$-dimensional lattice from the 32 blocks of 16 integers that form the public key. In our implementation, we assumed that the permutations π_i's and the bijection f were known, which gave the secret key almost immediately : both the computation of $\overline{\Omega}$ and the exhaustive search of $\frac{\phi(\mathbf{c}^{(0)})}{d_1 d_2 d_3 d_4}$ are performed in a few minutes. In practice, the vector $\frac{\phi(\mathbf{c}^{(0)})}{d_1 d_2 d_3 d_4}$ happens to be a very small linear combination of the LLL-reduced basis vectors (coefficients less than 10 in absolute value). In the case where we do not know the permutations π_i's and the bijection f, initial experiments confirm the above discussion.

4 Conclusion

We introduced the basic notion of an orthogonal lattice. This concept first leads to an efficient attack against both Merkle-Hellman and Merkle-Hellman-like transformations. This attack differs from Shamir's and Brickell's attacks against original Merkle-Hellman cryptosystems. It points out that one should be cautious with the cryptographic use of Merkle-Hellman transformations. The notion of an orthogonal lattice also enables us to exploit weaknesses in the subset factorization (the trapdoor). These two applications of lattice reduction form an attack against the Qu-Vanstone scheme that works for any choice of the parameters. The attack has been successfully implemented and reveals the secret key from the public key in a reasonable time.

Acknowledgements

We would like to thank Anne-Marie Bergé for the proof of theorem 1. We also thank Jean-Marc Couveignes for his help.

A Appendix

In this appendix, we describe the subset factorization used in the Qu-Vanstone scheme and we provide the missing proofs of sections 2 and 3.

A.1 Further description of the Qu-Vanstone scheme

Construction of the s blocks C_i Recall that n is a positive integer of the form $n = d_1d_2d_3d_4d_5$, where $2^{s-1} \leq d_\ell < 2^s$ (for $\ell = 1,2,3,4$), $d_5 \leq 16$, and s is some fixed even positive integer. In the additive group $G = \mathbf{Z}_n$, we distinguish the subgroups G_1, G_2, G_3 and G_4 where G_ℓ is generated by $d_1d_2 \ldots d_\ell$.

For each d_ℓ, $1 \leq \ell \leq 4$, select a superincreasing sequence $h[\ell,1], \ldots, h[\ell,s]$ such that $\sum_{i=1}^{s} h[\ell,i] < d_\ell$. Choose integers q_1, q_2, q_3 and q_4 such that q_ℓ and d_ℓ are coprime. Apply a Merkle-Hellman transformation to get $\bar{h}[\ell,i] = h[\ell,i]q_\ell \pmod{d_\ell}$ where $0 < \bar{h}[\ell,i] < d_\ell$.

Select a permutation ξ_1 on $\{1,2,\ldots,s\}$. For $1 \leq i \leq s$, select two positive integers $x[1,i,0]$, $x[1,i,1] < d_2d_3d_4d_5$ and define two elements in distinct cosets of G_1 in G by :

$$\begin{aligned}
a[1,i,0] &= x[1,i,0]d_1, \\
a[1,i,1] &= \bar{h}[1,\xi_1(i)] + x[1,i,1]d_1 \pmod{n}.
\end{aligned}$$

Select a permutation ξ_2 on $\{1,2,\ldots,s\}$. For $1 \leq i \leq s$ and $u = 0,1$, select two positive integers $x^u[2,i,0], x^u[2,i,1] < d_3d_4d_5$ and define two elements in distinct cosets of G_2 in G_1 by :

$$\begin{aligned}
a^u[2,i,0] &= x^u[2,i,0]d_1d_2, \\
a^u[2,i,1] &= \bar{h}[2,\xi_2(i)]d_1 + x^u[2,i,1]d_1d_2 \pmod{n}.
\end{aligned}$$

Select a bijection g_1 from $\{1,2,\ldots,s/2\}$ to $\{s/2+1, s/2+2, \ldots, s\}$. For $t,l = 0,1,2,3$ and $i = 1,2,\ldots,s/2$, select a positive integer $x^t[3,i,l] < d_4d_5$. Define four elements in distinct cosets of G_3 in G_2 by :

$$\begin{aligned}
a^t[3,i,0] &= x^t[3,i,0]d_1d_2d_3, \\
a^t[3,i,1] &= \bar{h}[3,i]d_1d_2 + x^t[3,i,1]d_1d_2d_3 \pmod{n}, \\
a^t[3,i,2] &= \bar{h}[3,g_1(i)]d_1d_2 + x^t[3,i,2]d_1d_2d_3 \pmod{n}, \\
a^t[3,i,3] &= (\bar{h}[3,i] + \bar{h}[3,g_1(i)])d_1d_2 + x^t[3,i,3]d_1d_2d_3 \pmod{n}.
\end{aligned}$$

Select a bijection g_2 from $\{1,2,\ldots,s/2\}$ to $\{s/2+1, s/2+2, \ldots, s\}$. For $t,l = 0,1,2,3$ and $i = 1,2,\ldots,s/2$, select a positive integer $x^t[4,i,l] < d_5$. Define four elements in distinct cosets of G_4 in G_3 by :

$$\begin{aligned}
a^t[4,i,0] &= x^t[4,i,0]d_1d_2d_3d_4, \\
a^t[4,i,1] &= \bar{h}[4,i]d_1d_2d_3 + x^t[4,i,1]d_1d_2d_3d_4 \pmod{n}, \\
a^t[4,i,2] &= \bar{h}[4,g_2(i)]d_1d_2d_3 + x^t[4,i,2]d_1d_2d_3d_4 \pmod{n}, \\
a^t[4,i,3] &= (\bar{h}[4,i] + \bar{h}[4,g_2(i)])d_1d_2d_3 + x^t[4,i,3]d_1d_2d_3d_4 \pmod{n}.
\end{aligned}$$

Let f be a bijection from $\{1,2,\ldots,s\}$ to $\{3,4\}\times\{1,2,\ldots,s/2\}$. For $1\le i\le s$ and $0\le j\le 15$, define $c[i,j]=a[1,i,u]+a^u[2,i,v]+a^{v+2u}[f(i),w] \pmod n$, where j is uniquely decomposed as $j=w+4v+8u$ with $0\le u\le 1$, $0\le v\le 1$ and $0\le w\le 3$. Qu and Vanstone proved in [13] that the s blocks $C_i=\{c[i,j]\ :\ 0\le j\le 15\}$ form a direct sum in G. The trapdoor consists of the d_ℓ's, $h[\ell,i]$'s, $a[1,i,l]$'s, $a^u[2,i,l]$'s, $a^t[3,i,l]$'s, $a^t[4,i,l]$'s, the bijections f, g_1, g_2; the permutations ξ_1, ξ_2.

Factoring with the trapdoor We now describe how, given any $g\in G$ of form $g=\sum_{i=1}^s c[i,j_i] \pmod n$, one can quickly recover j_i's just by knowing g and the trapdoor.

Let $g_1=g=\sum_{i=1}^s c[i,j_i] \pmod n$. Recall that in G, we have :

$$c[i,j_i]=a[1,i,u]+a^u[2,i,v]+a^{v+2u}[f(i),w] \pmod n,\ \ j_i=w+4v+8u.$$

We recover the values of u, v, w for each j_i value by solving 4 sub-knapsack problems based on appropriate superincreasing sequence :

Step 1. Compute $S_1=q_1^{-1}g_1 \pmod{d_1}$, and solve the superincreasing knapsack $\sum_{i=1}^s u_i h[1,\xi_1(i)]=S_1$, $u_i\in\{0,1\}$. Compute $g_2=g_1-\sum_{i=1}^s a[1,i,u_i]$.

Step 2. Compute $S_2=q_2^{-1}\frac{g_2}{d_1} \pmod{d_2}$, and solve the superincreasing knapsack $\sum_{i=1}^s v_i h[2,\xi_2(i)]=S_2$, $v_i\in\{0,1\}$. Compute $g_3=g_2-\sum_{i=1}^s a^{u_i}[2,i,v_i]$.

Step 3. Compute $S_3=q_3^{-1}\frac{g_3}{d_1d_2} \pmod{d_3}$, and solve the superincreasing knapsack $\sum_{i=1}^s x_i h[3,i]=S_3$, $x_i\in\{0,1\}$. Compute

$$g_4=g_3-\sum_{f(i)=(3,1)}^{(3,s/2)} a^{v_i+2u_i}[f(i),x_i+2x_{g_1(i)}].$$

Step 4. Compute $S_4=q_4^{-1}\frac{g_4}{d_1d_2d_3} \pmod{d_4}$, and solve the superincreasing knapsack $\sum_{i=1}^s y_i h[4,i]=S_4$, where $y_i\in\{0,1\}$. For $i=1,2,\ldots,s/2$ define $w_i=x_i+2x_{g_1(i)}$ and $w_{i+s/2}=y_i+2y_{g_2(i)}$.

Finally, we recover $j_i=w_i+4v_i+8u_i$ for $i=1,2,\ldots,s$.

A.2 Proof of theorem 4

Assume $c>2^{(n-1)/2+(n-d)(n-d-1)/4}\det(\overline{\Lambda})$ and let $(\mathbf{x}_1,\mathbf{x}_2,\ldots,\mathbf{x}_n)$ be an LLL-reduced basis of Ω. Let $(\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_{n-d})$ be an LLL-reduced basis of $\Lambda^\perp$. Define $\mathbf{y}_1,\mathbf{y}_2,\ldots,\mathbf{y}_{n-d}$ in Ω by $p_\uparrow(\mathbf{y}_j)=0$ and $p_\downarrow(\mathbf{y}_j)=\mathbf{b}_j$. These $n-d$ vectors are linearly independent, therefore by theorem 3 (2), for $1\le j\le n-d$:

$$\begin{aligned}\|\mathbf{x}_j\| &\le 2^{(n-1)/2}\max(\|\mathbf{y}_1\|,\ldots,\|\mathbf{y}_{n-d}\|)\\ &\le 2^{(n-1)/2}\max(\|\mathbf{b}_1\|,\ldots,\|\mathbf{b}_{n-d}\|).\end{aligned}$$

But theorem 3 (1) ensures us that $\|\mathbf{b}_j\|\le 2^{(n-d)(n-d-1)/4}\det(\Lambda^\perp)$. Thus :

$$\|\mathbf{x}_j\|\le 2^{(n-1)/2}2^{(n-d)(n-d-1)/4}\det(\Lambda^\perp)<c.$$

This implies that $p_\uparrow(\mathbf{x}_j) = 0$ and $p_\downarrow(\mathbf{x}_j) \in \Lambda^\perp$ for $1 \leq j \leq n-d$. Therefore $p_\downarrow(\mathbf{x}_1), \ldots, p_\downarrow(\mathbf{x}_{n-d})$ are linearly independent and they form a $\mathbf{Q}$-basis of $E_\Lambda^\perp$.

Now, let $\mathbf{y} \in \Lambda^\perp$. There exist $\lambda_1, \lambda_2, \ldots, \lambda_{n-d} \in \mathbf{Q}$ such that :

$$\mathbf{y} = \lambda_1 p_\downarrow(\mathbf{x}_1) + \lambda_2 p_\downarrow(\mathbf{x}_2) + \cdots + \lambda_{n-d} p_\downarrow(\mathbf{x}_{n-d}).$$

Defining $\mathbf{x} \in \Omega$ by $p_\uparrow(\mathbf{x}) = 0$ and $p_\downarrow(\mathbf{x}) = \mathbf{y}$, we have :

$$\mathbf{x} = \lambda_1 \mathbf{x}_1 + \lambda_2 \mathbf{x}_2 + \cdots + \lambda_{n-d} \mathbf{x}_{n-d}.$$

But there also exist $\mu_1, \mu_2, \cdots, \mu_n \in \mathbf{Z}$ such that $\mathbf{x} = \mu_1 \mathbf{x}_1 + \mu_2 \mathbf{x}_2 + \cdots + \mu_n \mathbf{x}_n$. Therefore :

$$(\mu_1 - \lambda_1)\mathbf{x}_1 + \cdots + (\mu_{n-d} - \lambda_{n-d})\mathbf{x}_{n-d} + \mu_{n-d+1}\mathbf{x}_{n-d+1} + \cdots + \mu_n \mathbf{x}_n = 0.$$

Since $\mathbf{x}_1, \ldots, \mathbf{x}_n$ are linearly independent, we deduce that $\lambda_j = \mu_j \in \mathbf{Z}$. Hence $(p_\downarrow(\mathbf{x}_1), \ldots, p_\downarrow(\mathbf{x}_{n-d}))$ is a $\mathbf{Z}$-basis of the lattice $\Lambda^\perp$.

Furthermore, for $1 \leq i \leq n-d$ and $1 \leq j \leq n-d$, $\|p_\downarrow(\mathbf{x}_j)\| = \|\mathbf{x}_j\|$ and $p_\downarrow(\mathbf{x}_i).p_\downarrow(\mathbf{x}_j) = \mathbf{x}_i.\mathbf{x}_j$. Since $(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ is an LLL-reduced basis, this proves that $(p_\downarrow(\mathbf{x}_1), \ldots, p_\downarrow(\mathbf{x}_{n-d}))$ is an LLL-reduced basis too.

A.3 Recovering the secret key from $\mathbf{c}^{(0)}$

Notice that $\hat{c}[i,j] \equiv c[i, \pi_i^{-1}(j)] - c[i, \pi_i^{-1}(0)] \pmod{n}$. Since we know $d_1 d_2 d_3 d_4$, we recover $n = d_1 d_2 d_3 d_4 d_5$ from the size of each $\hat{c}[i,j]$. But the form of each $c[i, \pi_i^{-1}(j)]$ is very particular :

$$c[i,j] = a[1,i,u] + a^u[2,i,v] + a^{v+2u}[f(i), w] \pmod{n}.$$

By enumerating all possible cases, one notices that the knowledge of $c[i, \pi_i^{-1}(j)] - c[i, \pi_i^{-1}(0)] \pmod{n}$ reveals d_1, $d_1 d_2$, $d_1 d_2 d_3$ by particular gcd's, hence the π_i's by looking at the order in each block of 15 integers. By subtractions, we then obtain the $\bar{h}[1,i]$'s, $\bar{h}[2,i]$'s, $\bar{h}[3,i]$'s and the $\bar{h}[4,i]$'s. Since we now know the d_ℓ's, we derive the q_ℓ's and the $h[\ell,i]$'s. This reveals the $a[1,i,l]$'s, $a^u[2,i,l]$'s, $a^t[3,i,l]$'s, $a^t[4,i,l]$'s, the bijections g_1, g_2 and the permutations ξ_1, ξ_2 (looking at the order of superincreasing sequences). We now know the complete trapdoor. The coordinates λ_j's are actually closely related to the $w^{(e)}$'s and the $m^{(e)}$'s : one can derive equivalent $w^{(e)}$'s and $m^{(e)}$'s so that $\mathbf{c}^{(k)}$ is obtained by Merkle-Hellman-like transformations from $\mathbf{c}^{(0)}$. Since we now know the $c[i,j]$'s from the trapdoor, we also find out equivalent $\sum_{i=1}^{s} a_i^{(e)}$'s. Hence, we recovered the complete secret key.

References

1. E. Brickell. Are most low density polynomial knapsacks solvable in polynomial time ? In *Proc. 14th Southeastern Conference on Combinatorics, Graph Theory, and Computing*, 1983.
2. B. Chor and R.L. Rivest. A knapsack-type public key cryptosystem based on arithmetic in finite fields. *IEEE Trans. Inform. Theory*, 34, 1988.

3. H. Cohen. *A course in computational algebraic number theory.* Springer-Verlag, Berlin, 1993.
4. M.J. Coster, A. Joux, B.A. LaMacchia, A.M. Odlyzko, C.-P. Schnorr, and J. Stern. Improved low-density subset sum algorithms. *Comput. Complexity*, 2:111–128, 1992.
5. P. M. Gruber and C. G. Lekkerkerker. *Geometry of numbers.* North-Holland, Amsterdam, 1969.
6. A. Joux. *La réduction des réseaux en cryptographie.* PhD thesis, École Polytechnique, 1993.
7. A. Joux and J. Stern. Lattice reduction: a toolbox for the cryptanalyst. (to appear in J. of Cryptology).
8. A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.
9. J. Martinet. *Les réseaux parfaits des espaces euclidiens (perfect lattices in euclidean spaces).* Editions Masson, 1996.
10. R. Merkle and M. Hellman. Hiding information and signatures in trapdoor knapsacks. *IEEE Trans. Inform. Theory*, IT-24:525–530, September 1978.
11. P. L. Montgomery. Square roots of products of algebraic numbers. Draft of June, 1995.
12. A. M. Odlyzko. The rise and fall of knapsack cryptosystems. In *Cryptology and Computational Number Theory*, volume 42 of *Proceedings of Symposia in Applied Mathematics*, pages 75–88. A.M.S., 1990.
13. M. Qu and S. A. Vanstone. New public-key cryptosystem based on the subset factorizations in $\mathbf{Z}_n$. (to appear).
14. M. Qu and S. A. Vanstone. The knapsack problem in cryptography. In *Finite Fields: Theory, Applications, and Algorithms*, volume 168 of *Contemporary Mathematics*, pages 291–308. A.M.S., 1994.
15. C.-P. Schnorr. A hierarchy of polynomial lattice basis reduction algorithms. *Theoretical Computer Science*, 53:201–224, 1987.
16. C.P. Schnorr and H.H. Hörner. Attacking the Chor-Rivest cryptosystem by improved lattice reduction. In *Advances in Cryptology : Proceedings of Eurocrypt' 95*, volume 921 of *LNCS*, pages 1–12. Springer-Verlag, 1995.
17. A. Shamir. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem. In *Proceedings of the 23rd Annual Symposium on the Foundations of Computer Science (IEEE)*, pages 145–152, 1982.