Chapter 7
A Review of Modern Cryptography: From the World War II Era to the Big-Data Era

Bojun Lu

Abstract This chapter briefly surveys the rapid development of *Modern Cryptography* from World War II (WW-II) to the prevailing Big-Data Era. Cryptography is the art and science of secret communication, which concerns about C.I.A., i.e., *Confidentiality*, *Integrity*, and *Authentication* of information, so as to guarantee the safety during information transmission. Meanwhile *Authentication* is the key step in information security, where an excellent example is online payment systems, which belongs to the field of Financial Technology (Fin-Tech) and is booming on multiple markets in recent years. The concept "Quantum" is popular in the recent decade, and the possibilities of inventing Quantum Cryptosystems are also raised in the literature, which is a promising direction in Modern Cryptosystem. We also select two classical cryptosystems, i.e., the Merkle–Hellman knapsack cryptosystem, and the subset sum problem (SSP)-based cryptosystem to present the mechanisms in encryption and decryption processes. Apart from being a brief survey, this chapter is also intended as an entry point to guide readers to this interesting and important field.

Keywords Big-Data • Cryptography • Cryptosystem • Information Security • Optimization • Financial Technology (Fin-Tech) • Quantitative Finance

7.1 Introduction

Cryptography is the art and science of secret communication (Singh 1999). In the recent decade, several brilliant research works in the field of *Modern Cryptography*, have successfully attracted the attention of *Turing Award*, which represents the highest honor to reward the achievements in the computing community, and is also stipulated that "The contributions should be of lasting and major technical importance to the computer field." For example, in 2015, winners are

B. Lu (✉)
Quantitative Researcher, Portfolio Management Department, Foresea Life Insurance Co., Ltd., Shenzhen, PRC
e-mail: bjlu.eva@foxmail.com

T.-M. Choi et al. (eds.), *Optimization and Control for Systems in the Big-Data Era*,
International Series in Operations Research & Management Science 252,
DOI 10.1007/978-3-319-53518-0_7

Martin E. Hellman and Whitfield Diffie, who described and predicted the new directions of cryptography in their celebrated paper (Diffie and Hellman 1976) published in 1976, and the citation from Turing Award is shown as follows:

"*For fundamental contributions to* ***modern cryptography****. Diffie and Hellman's groundbreaking 1976 paper, 'New Directions in Cryptography' (Diffie and Hellman 1976) introduced the ideas of public-key cryptography and digital signatures, which are the foundation for most regularly-used security protocols on the internet today.*"

In 2002, winners are Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman (please refer to Rivest et al. (1978) for their paper published in 1978), and the citation from Turing Award is: "*For their ingenious contribution for making* ***public-key cryptography*** *useful in practice*." In 2000, winner is Andrew Chi-Chih Yao with citation from Turing Award as: "*In recognition of his fundamental contributions to the theory of computation, including the complexity-based theory of pseudorandom number generation,* ***cryptography****, and communication complexity.*"

There is no doubt about the importance of cryptography in its nature, and if we try to explain the importance of cryptography in more detail, we would like to emphasize that cryptography concerns about C.I.A., i.e., *Confidentiality*, *Integrity*, and *Authentication* of information, so as to guarantee the safety during information transmission. Please notice that the C.I.A. we defined in this review paper does not refer to the *Central Intelligence Agency* (CIA) of the United States, although the CIA of the United States does also have close relationship with highly confidential information.

If we try to seek the starting point of *Modern Cryptography Era*, we could trace back to the dates of World War II (WW-II), and several important and interesting questions could also be proposed, for instance,

1. *What* invention/technique invented/proposed by *whom* demonstrates that *Vintage Cryptography Era* begins to migrate to *Modern Cryptography Era*?
2. What event could be counted as the blasting fuse that boosts this migration?

To answer the first question, please let us use the electromechanical rotor based cipher system *Enigma Machine* invented by Arthur Scherbius at the end of World War I (WW-I), around 1918 [please refer to Jennifer (2006)], to be the representative invention/technique that represents the beginning of *Modern Cryptography Era*. Actually, before WW-II, mechanical and electromechanical cryptographic cipher machines were already in wide use, although almost all were *impractical manual systems*. Later, during WW-II, great advances on practical and theoretical cryptography were developed all in secrecy. Moreover, before and during WW-II, several models were developed based on Enigma Machine, and these models were specially adopted by military and government services of some countries, such as Germany, Japan, Russia, France, and Italy. during WW-II. In recent years, some of the WW-II cryptography related information has begun to be declassified, which partly owes to (1) the official 50-year (British) secrecy period has come to an end, (2) relevant US archives have been opened gradually, and (3) assorted memoirs and articles have been published, etc. Besides Enigma Machine, *Purple Machine* also deserves our attention, which was invented and improved by the Japanese during WW-II with

Fig. 7.1 Enigma in use 1943

Fig. 7.2 Electronic implementation of an Enigma machine

inspiration from the mechanism of Enigma Machine used by Nazis; and which was used to transform the top level military secrets of Japanese Navy in the *Pearl Harbor War* (Figs. 7.1 and 7.2).

To answer the second question, one possible answer that we conjecture is that WW-II plays an important role as the blasting fuse that boosts the practical and theoretical development of modern cryptography. Meanwhile, because techniques become more mature, especially because the first computer has been invented around WW-II compared with scientific techniques in WW-I. All these enable cryptography to be used more widely in modern wars, for instance, in WW-II.

When we discuss cryptography, there are two angles of views, just like a coin has two sides, i.e., encryption technology and decryption technology. A good example is that by WW-II, there were unbreakable codes and then by the end, there was technology to break them. For example, Japan's Purple Machine was broken by US Army cryptographers (cryptologists) William F. Friedman, Frank Rowlett, and their subordinates in 1940, which enables America to hold a vantage position in the Pearl Harbor War during WW-II. It's worth to note that William F. Friedman is identified as the "Dean of American Cryptology" by the U.S. National Cryptologic Museum, and also the godfather of cryptology of the USA.

In the Big-Data Era now, cryptography continues to play an important role both in practical and theoretical aspects. Before listing the applications and emphasizing the importance of cryptography systems in Big-Data Era, we first briefly go through the evolvement of the concept of "big data." In 2001, Doug Laney, from META Group which is now re-named Gartner, defined big data in 3 dimensions, i.e., *Volume*, *Velocity*, and *Variety* with abbreviation "3Vs" [please see Gartner (2011)], which has been expanded to the following 5 dimensions in 2016 by Martin Hilbert (please refer to Hillbert (2015) and Wikipedia (https://en.wikipedia.org/wiki/Big_data) for more information):

- Volume: big data doesn't sample, but it observes and tracks what happens;
- Velocity: big data is often available in real time;
- Variety: big data draws from text, images, audio, video; plus it completes the missing pieces through data fusion;
- Machine Learning: big data often doesn't ask why and simply detects patterns;
- Digital footprint: big data is often a cost-free by-product of digital interaction.

Actually, based on our understanding, Big-Data Era precisely captures the trend of *information explosion*, since people interact so actively and share information so frequently through the internet, thus a huge amount of data is generated as "by-product." At the ACM Turing Centenary Celebration in 2012, Cerf et al. (2012) discussed the topic on "information, data, security in a networked future" to emphasize the importance of security of information and data in the modern real world. Then referring to our definition of C.I.A., in which the 3-dimensions depiction of information is provided, and as information is exploding, thus the importance of C.I.A. of information is manifested. Consequently, techniques and theories in cryptography, developed to protect information becomes even more vital nowadays. Real-world applications of cryptography can be evidenced in many industrial fields, such as modern financial systems, telecommunications, the newly emerging field called "Financial Technology (Fin-Tech)," etc.

In this paragraph, we would like to mention that the online payment systems is a good example to illustrate the crucial role that cryptography plays in modern finance with "big data." An online payment system called *WeChat Pay*, invented and run by Tencent Holdings, and another online payment system called *Alipay*, invented and run by Alibaba Group, are now the two biggest and most popular online payment platforms in Mainland China. Also as evidenced in the report from Credit Suisse, the online payment market grows rapidly, and the total value of online transactions in China grows from an insignificant size in 2008 to around RMB 4 trillion (US$660 billion) in 2012 (see Watling 2014). We also would like to mention that on February 18, 2016, the online payment platform called *Apply pay* developed by Apply Inc., lands in the market of Mainland China to show its interests in China's booming market. Meanwhile, Tencent Holdings and Alibaba Group also both have announced their plans to expand their mobile payment service to regions/countries outside Mainland China. To show that cryptography plays a crucial role in online payment systems, please notice that *Authentication*, i.e., the **A.** in C.I.A. is a crucial step during the completion of online payment, and to guarantee

Fig. 7.3 WeChat Pay v.s. Alipay

Fig. 7.4 Apply Pay

authentication of each party involved, digital signature or other private-key plus public-key crypto-techniques must be applied. For instances, the MD5 invented and designed by Ronald Rivest [see Rivest (1992) and Wang and Yu (2005)], and the SHA-1 (Secure Hash Algorithm 1) designed by National Institute of Standards and Technology (NIST) and National Security Agency (NSA) (see Wikipedia https://en.wikipedia.org/wiki/SHA-1) are two classical crypto-techniques that have been adopted in digital signatures for many years. Crypto-currencies known as Bitcoin with block-chain technique embedded is also an interesting case in modern finance which adopts modern cryptography as one of the key parts in its realization. Besides these Fin-Tech cases, actually we would like to say that modern cryptography is everywhere in our daily life now (Figs. 7.3 and 7.4).

When we talk about *Fin-Tech* which is a field booming in the recent years, other than online payment systems, we would also like to mention Fin-Tech companies that focus on quantitatively managing capitals for their customers, with Betterment (www.betterment.com) and Wealthfront (www.wealthfront.com) be the benchmarking enterprises (see http://fintechinnovators.com/). As we know in practice, Black–Litterman model (see Black and Litterman 1992) is a classical model adopted in the basket of quantitative strategies of these enterprises; and in academia, theoretically, Black–Litterman model is an extension of Markowitz's mean-variance model (see Markowitz 1952) which could blend information collected from real market to mend the weights on each asset and thus to improve the performance of portfolios. We would like very much to draw your attention to the brilliant research works that Professor Duan Li and his collaborators have done in the field of portfolio selection theory, and for details please refer to their papers (Zhu et al. 2014; Gao et al. 2015), etc.

The concept "Quantum" is popular in the recent decade, and the possibilities of inventing Quantum Cryptosystems are also raised in the literature, which is a promising direction in the field of Modern Cryptosystem (please see Okamoto et al. (2000) and the literature therein).

The remainder of this book chapter is organized as follows. Section 7.2.1 briefly describes the Merkle–Hellman knapsack cryptosystem, and Shamir's attack in 1984, where a hands-on numerical example is given for illustration. Section 7.2.2 presents the hardest subset sum problem based cryptosystem, and shows a decryption method which adopts the lattice theory and the distinguished LLL algorithm (see Lenstra et al. 1982). By the end, Sect. 7.3 includes the conclusion and further discussion.

7.2 Two Classical Cryptosystems

In Sects. 7.2.1 and 7.2.2, Merkle–Hellman knapsack cryptosystem and hardest subset sum problem (SSP)-based cryptosystem will be introduced which have both been well studied in the literature. (Note that in the literature, the SSP-based cryptosystem is also sometimes called the knapsack cryptosystem.) The Merkle–Hellman knapsack cryptosystem is one of the classical public-key knapsack cryptosystems, and is invented by Merkle and Hellman in 1978 (see Merkle and Hellman 1978) which has been broken by Shamir in 1984 (see Shamir 1984). Meanwhile, since the subset sum problem belongs to NP-class in its nature theoretically (see Garey and Johnson 1979), and it has been proven that the subset sum problem with a density approximately equals 1 is hardest (see Lagarias and Odlyzko 1985), it could be adopted to construct a trapdoor cryptosystem. Whereas in order to break the trapdoor cryptosystem, a *hard* subset sum problem must be solved.

7.2.1 The Merkle–Hellman Knapsack Cryptosystem

In 1978, Merkle and Hellman published their seminal paper (Merkle and Hellman 1978) which discovered a public-key cryptosystem. Although compared with an RSA cryptosystem (see Rivest et al. 1978) which is two-way system and can be adopted for *Authentication* in cryptographic signing, Merkle–Hellman cryptosystem is one-way, i.e., the public key is used only for encryption and the private key is used only for decryption. But Merkle–Hellman cryptosystem is the first so-called *knapsack cryptosystem*. In their paper, Merkle and Hellman proposed a *singly iterated cryptosystem* together with a *multiply iterated cryptosystem*. Later in 1984, Shamir (1984) found a polynomial time algorithm to break the singly iterated cryptosystem.

In Sect. 7.2.1.1, we present a description of the basic singly iterated knapsack cryptosystem proposed by Merkle and Hellman. In Sect. 7.2.1.2, Shamir's attack on the singly iterated knapsack cryptosystem is studied in detail.

7.2.1.1 Singly Iterated Merkle–Hellman Knapsack Cryptosystem

Suppose that the sender Bob wants to send a secret message to the receiver Anna, the message is represented as a binary vector $x = (x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ in the binary system. The question is: How could Bob send this message to Anna in a secure way? In Merkle–Hellman cryptosystem, a strategy is designed so that Bob can send this message to Anna against the potential eavesdropper. This strategy is described as follows:

1. Anna chooses a positive superincreasing integer sequence $a = (a_1, a_2, \ldots, a_n)^T$. Superincreasing is in the sense that

$$a_i > \sum_{j=1}^{i-1} a_j, \quad i = 2, 3, \ldots, n.$$

2. Anna chooses two relatively prime integers m and w, such that

$$m > \sum_{j=1}^{n} a_j, \quad \text{and} \quad \gcd(m, w) = 1.$$

3. Sequence $c = (c_1, c_2, \ldots, c_n)^T$ is calculated as follows:

$$c_i = a_i w \mod m.$$

4. The *public key* is sequence $c = (c_1, c_2, \ldots, c_n)^T$.
5. The *private key* consists of an integer pair (w, m).

Now, if Bob wants to send message x to Anna, he sends the number d instead of sending x directly, where $d = c^T x$. Anna receives d, and conducts the following calculation:

1. Calculates b, where $b = dw^{-1} \mod m$, and w^{-1} is the *modular multiplicative inverse* of w modulo m.
2. Solves the equation $a^T x = b$, where $x \in \{0,1\}^n$. Then the solution x is the message Bob sent. Actually, since a is superincreasing, the equation $a^T x = b$ can be solved in linear time.

While Anna could get the message easily, the eavesdropper needs to solve the equation $c^T x = d$ in order to get the message, which is much harder.

One thing should be noticed is that, actually, $a_i = c_i w^{-1} \mod m, i = 1, 2, \ldots, n$.

7.2.1.2 Analysis of Shamir's Attack on Singly Iterated Knapsack Cryptosystem

Basic Deductions

The public key $c = (c_1, \ldots, c_n)^T$ is known for everyone, what Shamir wanted to do is to find a positive and relatively prime integer pair $(\tilde{w}, \tilde{m})$, such that $a = c\tilde{w} \mod \tilde{m}$ is super-increasing. Actually (w^{-1}, m) is such a qualified pair, where w^{-1} is the *modular multiplicative inverse* of w modulo m and (w, m) is the private key. Notice that there may be qualified integer pairs other than (w^{-1}, m).

Let $\tilde{w} = w^{-1}$ and $\tilde{m} = m$, we do the following analysis. The super-increasing sequence a chosen by Anna is

$$a_i = c_i w^{-1} \mod m, \quad i = 1, 2, \ldots, n.$$

Divide both sides by m, an equivalent equation is obtained as follows:

$$\begin{aligned} \frac{a_i}{m} &= c_i \frac{w^{-1}}{m} \mod 1 \\ &= c_i \frac{w^{-1}}{m} - \left\lfloor c_i \frac{w^{-1}}{m} \right\rfloor, \quad i = 1, 2, \ldots, n. \end{aligned} \tag{7.1}$$

Since $a_i = c_i w^{-1} \mod m$, $i = 1, 2, \ldots, n$, there must exist positive integer q_i's such that

$$a_i = c_i w^{-1} - q_i m, \quad i = 1, 2, \ldots, n.$$

Divide both sides by m, we get the following equation,

$$\frac{a_i}{m} = c_i \frac{w^{-1}}{m} - q_i, \quad i = 1, 2, \ldots, n. \tag{7.2}$$

Relate Eqs. (7.1) and (7.2), we see that

$$q_i = \left\lfloor c_i \frac{w^{-1}}{m} \right\rfloor, \quad i = 1, 2, \ldots, n.$$

Moreover, $\frac{q_i}{c_i}$ is the closest minimum of the c_i-curve to the left of $\frac{w^{-1}}{m}$ (Fig. 7.5).

Observe the c_i-curve, or from Eq. (7.2), we see that the distance between $\frac{w^{-1}}{m}$ and $\frac{q_i}{c_i}$ is

$$\frac{w^{-1}}{m} - \frac{q_i}{c_i} = \frac{a_i}{m c_i}, \quad i = 1, 2, \ldots, n. \tag{7.3}$$

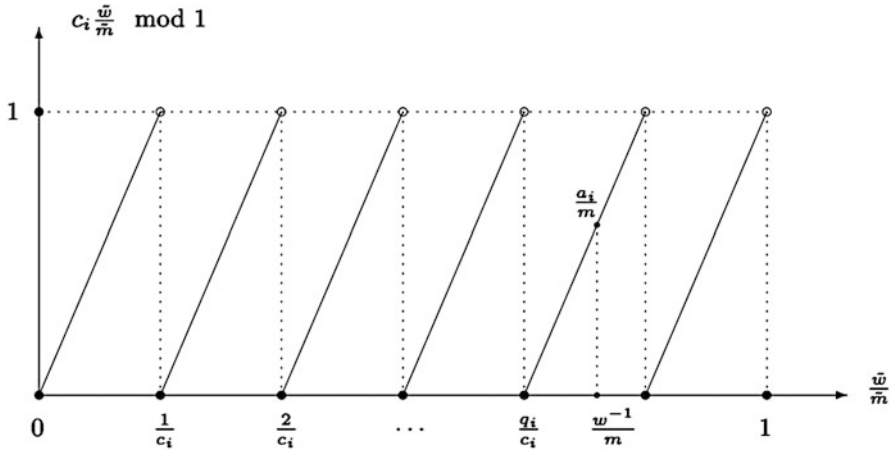

Fig. 7.5 c_i-curve: the relationship between $c_i \frac{\tilde{w}}{\tilde{m}} \mod 1$ and $\frac{\tilde{w}}{\tilde{m}}$

Then based on Eq. (7.3), we have

$$\frac{q_1}{c_1} - \frac{q_i}{c_i} = \frac{a_i}{mc_i} - \frac{a_1}{mc_1}, \quad i = 2, 3, \ldots, n, \tag{7.4}$$

and

$$q_1 c_i - q_i c_1 = \frac{a_i c_1}{m} - \frac{a_1 c_i}{m}, \quad i = 2, 3, \ldots, n. \tag{7.5}$$

How Many c_i-Curves Do We Need

According to Shamir's assumption, a_i is chosen to be a $dn - n + i - 1$ bit number, $i = 1, 2, \ldots, n$ and m is chosen to be a dn bit number. Here we just simply treat d as a parameter, and in Shamir's attack, $1 < d < 2$. (Actually d has much to do with the *density of a subset sum problem*, which will not be studied here. We just point out the relationship between them, which is: The lower of d the higher of the density of the subset sum problem, vice versa.)

Based on the assumption on the sizes of a_i and m, we choose a_i and m in the following way:

1. a_1 is a random integer number between 1 and 2^{dn-n}, with a uniform probability distribution.
2. a_i is a random integer number between $\sum_{j=1}^{i-1} a_j$ and $2^{dn-n+i-1}$, with a uniform probability distribution. Notice that there always has $\sum_{j=1}^{i-1} a_j < 2^{dn-n+i-1}$.
3. m is a random integer number between $\sum_{j=1}^{n} a_j$ and 2^{dn}, with a uniform probability distribution.

From Eq. (7.3), we have

$$\begin{aligned}\frac{w^{-1}}{m}-\frac{q_i}{c_i}&=\frac{a_i}{mc_i}\\&<\frac{2^{dn-n+i-1}}{mc_i}\\&\approx\frac{2^{dn-n+i-1}}{2^{dn}c_i}\qquad(\because m\approx 2^{dn})\\&=\frac{2^{-n+i-1}}{c_i}.\end{aligned}$$

Hence,

$$\frac{q_i}{c_i}\in\left(\frac{w^{-1}}{m}-\frac{2^{-n+i-1}}{c_i},\frac{w^{-1}}{m}\right),\quad i=1,2,\ldots,n.$$

For an arbitrary $\frac{\tilde{w}}{\tilde{m}}$, there must be a minimum of c_i-curve, such that the minimum belongs to the interval of,

$$\left(\frac{\tilde{w}}{\tilde{m}}-\frac{1}{c_i},\frac{\tilde{w}}{\tilde{m}}\right).$$

Roughly, suppose that the minimum follows a uniform probability distribution in the above interval, then the probability that the minimum belongs to interval

$$\left(\frac{\tilde{w}}{\tilde{m}}-\frac{2^{-n+i-1}}{c_i},\frac{\tilde{w}}{\tilde{m}}\right),$$

is

$$\frac{2^{-n+i-1}}{c_i}/\frac{1}{c_i}=2^{-n+i-1}.$$

For an arbitrary c_1-curve's minimum $\frac{p}{c_1}$, choose $\frac{\tilde{w}}{\tilde{m}}$ and let it be in the following interval

$$\left(\frac{p}{c_1},\frac{p}{c_1}+\frac{2^{-n}}{c_1}\right).$$

Suppose other $c_2,\ldots,c_l$-curves are chosen, then for the $\frac{\tilde{w}}{\tilde{m}}$, the probability that there exists one c_i-curve's minimum which belongs to the following interval

$$\left(\frac{\tilde{w}}{\tilde{m}}-\frac{2^{-n+i-1}}{c_i},\frac{\tilde{w}}{\tilde{m}}\right),$$

at the same time for $i = 2, \ldots, l$ is

$$2^{-n+1} \cdot 2^{-n+2} \cdot \cdots \cdot 2^{-n+l-1} = 2^{l^2/2-nl-l/2+n}.$$

Let p run from 0 to $c_1 - 1$, then the expected number of $\frac{p}{c_1}$'s which satisfies the above condition is

$$\begin{aligned} c_1 \cdot 2^{l^2/2-nl-l/2+n} &= \alpha_1 \cdot m \cdot 2^{l^2/2-nl-l/2+n} \\ &\approx \alpha_1 \cdot 2^{dn+l^2/2-nl-l/2+n}, \end{aligned}$$

where $0 < \alpha_1 < 1$. When $2^{dn+l^2/2-nl-l/2+n} < 1$, we have $\alpha_1 \cdot 2^{dn+l^2/2-nl-l/2+n} < 1$. Simple mathematical deduction yields

$$2^{dn+l^2/2-nl-l/2+n} < 1,$$

which is equivalent to

$$l \in \left(n + \frac{1}{2} - \sqrt{n(n-1-2d) + \frac{1}{4}},\ n + \frac{1}{2} + \sqrt{n(n-1-2d) + \frac{1}{4}} \right).$$

Since $l \leq n$ and $n + \frac{1}{2} + \sqrt{n(n-1-2d) + \frac{1}{4}} > n$, we have

$$l \in \left(n + \frac{1}{2} - \sqrt{n(n-1-2d) + \frac{1}{4}},\ n \right].$$

It can be checked that $n + \frac{1}{2} - \sqrt{n(n-1-2d) + \frac{1}{4}}$ is a convex and decreasing function with respect to n. When $n = 10$ and $d = 2$, $n + \frac{1}{2} - \sqrt{n(n-1-2d) + \frac{1}{4}} = 3.4113$. In this sense, 4 or 5 c_i-curves are enough for the analysis.

An Illustrative Example

Next we illustrate Shamir's attack based on the following concrete example.

Example 1 We generate a super-increasing sequence $a = (a_1, \ldots, a_n)$, $n = 10$,

$$a = (42, 64, 115, 263, 545, 1083, 2122, 4278, 8555, 17100)$$

where $a_i < 2^{dn-n+i-1}$, $i = 1, 2, \ldots, n$.

$m = 29193006$ is chosen such that $\sum_{i=1}^{n} a_i < m < 2^{dn}$.
$w = 11198095$ is randomly chosen such that $\gcd(w, m) = 1$.

c is calculated as follows,

$$\begin{aligned} c &= aw \mod m \\ &= (3231894, 16045936, 3288661, 25798385, 1623521, \\ &\quad 12439395, 28443712, 28920570, 17450039, 10498146). \end{aligned}$$

We have $w^{-1} = 1152457$, and

$$c/m = (0.1107, 0.5497, 0.1127, 0.8837, 0.0556, 0.4261, 0.9743, 0.9907, 0.5977, 0.3596).$$

□

7.2.2 *Hardest Subset Sum Problem (SSP)-Based Cryptosystem*

A subset sum problem is defined as follows:

$$ax^T = a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{7.6}$$

with $a = (a_1, a_2, \ldots, a_n) \in \mathbb{R}_+^n$, $b \in \mathbb{R}_+^n$ be known, and $x = (x_1, x_2, \ldots, x_n) \in \{0, 1\}^n$ be unknown.

The concept *density* of a subset sum problem is defined as

$$density = \frac{n}{\max_{1 \le i \le n}(\log_2 a_i)}. \tag{7.7}$$

It has been revealed in the literature that subset sum problems in (7.6) with their density close to 1 constitute the hardest subclass of subset sum problems [see Lagarias and Odlyzko (1985), Coster et al. (1991) and Schnorr and Shevchenko (2012)]. Besides the *density* defined in (7.7), some other factors have also been proposed in the literature to describe the difficulty level of subset sum problems [see Jen et al. (2012b) and Jen et al. (2012a)].

Next we will review two decryption methods [see Lagarias and Odlyzko (1985), Coster et al. (1992), Schnorr and Euchner (1994)] which are designed based on the lattice theory and the distinguished LLL algorithm [see Lenstra et al. (1982), Nguyen and Vallée (2010)]. Lagarias and Odlyzko (1985) claimed that they could break "almost all" problems with a density < 0.645, and Coster et al. (1992) claimed that they could break "almost all" problems with a density < 0.941. It is worth mentioning that in Lu and Li's working paper (see Lu and Li 2016), and Lu's Ph.D. thesis (see Lu 2014), an algorithm that combines *disaggregation techniques* and *LLL algorithm* could break "almost all" problems with a density ≈ 1, compared with Lagarias and Odlyzko (1985) and Coster et al. (1992), for problems of the same dimension.

Here we spend a concise paragraph to elaborate the initial intuition of *disaggregation techniques* related work proposed in Lu's Ph.D. thesis (see Lu 2014) which aims to propose efficient algorithms equipped with *disaggregation techniques* together with *LLL algorithm*, for solving the following problem, i.e., a system of linear Diophantine equations:

$$Ax = b, \quad \text{with } x \text{ be unknown integer vectors and be bounded,} \tag{7.8}$$

which belongs to NP-class and where subset sum problems are special cases of Problem (7.8). The intuitions which stimulate us to conduct research work on *disaggregation techniques* are:

1. We are inspired by the time complexity of the cell enumeration method proposed by Prof. Duan Li and et al. in Li et al. (2011), which is bounded by $O((n \max\{u_1, \ldots, u_n\})^{n-m})$ and thus depends on the magnitude of $n - m$, where n is the number of unknown variables, m is the number of equations in the system $Ax = b$, and $(u_1, \ldots, u_n)$ are the upper bounds of the unknown variables. Obviously, reducing the magnitude of $n - m$ directly benefits us in the computing. Aiming to reduce the magnitude of $n - m$, we thus study possible solution schemes for disaggregation.
2. Glover and Woolsey formulated for the first time the inverse problem of aggregation, i.e., the *disaggregation problem*, in their paper (Glover and Woolsey 1972) in 1972. After presenting rich work on *aggregation* in Glover and Woolsey (1972), in their conclusion remarks, they strongly encouraged research on *disaggregation*: "The development of effective ways to do this (disaggregation) would be especially worthwhile." However, although Glover and Woolsey proposed this disaggregation problem, they actually didn't provide available and effective techniques to handle this problem, as evidenced by a sentence in their conclusion remarks in Glover and Woolsey (1972), "The theorems of this paper ..., but do not give an immediate clue about what multiples should be examined to effect the disaggregation." Though disaggregation problem is of importance, we discovered that the literature on proposing solutions to disaggregation problem is pretty limited. This fact encouraged us to study possible solution schemes for disaggregation.

For details of our research work on *disaggregation techniques*, please refer to Chap. 4 of Lu (2014).

Next we continue to spend our efforts to explain the two algorithms proposed by Lagarias and Odlyzko (1985) and Coster et al. (1992), respectively.

The $(n + 1) \times (n + 1)$ lattice proposed by Lagarias and Odlyzko (1985) is of the following form:

$$B_{LO} = \begin{pmatrix} I & \mathbf{0}^{n\times 1} \\ -a & b \end{pmatrix}. \tag{7.9}$$

We denote the column-wise LLL reduced matrix of B_{LO} by $\tilde{B}_{LO}$. The algorithm checks whether *any* column of $\tilde{B}_{LO}$ has the form of $\tilde{b}_{i,j} \in \{0, \lambda\}$, $i = 1, 2, \ldots, n$, for some fixed value λ and $\tilde{b}_{n+1,j} = 0$, where $1 \leq j \leq n+1$. If it fails, the algorithm repeats with b replaced by $\sum_{i=1}^{n} a_i - b$. If such a column appears, then we divide $\tilde{b}_{i,j} \in \{0, \lambda\}$, $i = 1, 2, \ldots, n$ by λ, and check whether the binary vector is a solution. We denote the method proposed in Lagarias and Odlyzko (1985) as **LO-Alg**. An analysis for **LO-Alg** method is presented in Frieze (1986) in 1986.

The $(n+1) \times (n+1)$ lattice proposed by Coster et al. (1992) is of the following form:

$$B_{CJOS} = \begin{pmatrix} I & \frac{1}{2} \times \mathbf{1}^{n \times 1} \\ aN & bN \end{pmatrix}, \tag{7.10}$$

with $N > \frac{1}{2}\sqrt{n}$. We denote the column-wise LLL reduced matrix of B_{CJOS} by $\tilde{B}_{CJOS}$. The algorithm checks whether *any* column of $\tilde{B}_{CJOS}$ has the form of $\tilde{b}_{i,j} \in \{-\frac{1}{2}, \frac{1}{2}\}$, $i = 1, 2, \ldots, n$, and $\tilde{b}_{n+1,j} = 0$, where $1 \leq j \leq n+1$. If yes, then we add back $\frac{1}{2}$ to $\tilde{b}_{i,j} \in \{-\frac{1}{2}, \frac{1}{2}\}$, $i = 1, 2, \ldots, n$, and check whether the binary vector is a solution. We denote the method proposed in Coster et al. (1992) as **CJOS-Alg**.

7.2.2.1 Review of the LLL Algorithm

In this part, we briefly introduce the mechanics behind LLL basis reduction algorithm and show how it works. We abbreviate LLL basis reduction algorithm to *LLL algorithm* and name the basis obtained by LLL algorithm as the *LLL-reduced basis*. Algebraically speaking, to obtain the LLL-reduced basis, a series of unimodular row operations need to be conducted on one ordered basis. Geometrically speaking, vectors in an LLL-reduced basis are relatively short and nearly orthogonal to one another. LLL algorithm has been proved to be very powerful as evidenced by its remarkable achievements in both theoretical advancement and successful applications, which is also an algorithm of polynomial time and arithmetic operation steps [see Sect. 4.3 of Bremner (2011)]. In theory, Lenstra (1983) proved that integer programming with a fixed dimension is polynomially solvable with the aid of the lattice basis reduction algorithm. In applications, many efficient algorithms have been developed in the last 30 years with LLL algorithm being their essential parts, including numerous cryptography-purpose algorithms for breaking knapsack public-key cryptosystems. By adopting LLL-based algorithms, e.g., the generalized LLL and the BKZ process (Lovász and Scarf 1992; Schnorr and Euchner 1994), efficient algorithms are designed in Brickell (1983), Lagarias and Odlyzko (1983), Lagarias and Odlyzko (1985), Coster et al. (1991), Coster et al. (1992), Schnorr and Euchner (1991) for breaking low density knapsack public-key cryptosystems. Among them, the algorithms in Lagarias and Odlyzko (1985) and Coster et al. (1992) represent two cornerstones of the development.

Definition 1 (Lattice) Given row vectors $b_1, b_2, \ldots, b_m \in \mathbb{R}^n$ with $m \leq n$. The set L defined as below

$$L = \mathbb{Z}b_1 + \mathbb{Z}b_2 + \cdots + \mathbb{Z}b_m = \left\{ \sum_{i=1}^{m} z_i b_i \mid z_i \in \mathbb{Z},\ i = 1, 2, \ldots, m \right\},$$

is called a lattice of dimension m. Moreover, $\{b_1, b_2, \ldots, b_m\}$ is called a basis for lattice L.

Theorem 1 *Given a lattice L, row vectors of B and row vectors of $\tilde{B}$ are two bases for L, if and only if there exists a unimodular matrix U, such that $B = U\tilde{B}$.*

Lemma 1 *If $\{b_1, b_2, \ldots, b_n\}$ is an α-reduced basis of the lattice $\Lambda \in \mathbb{R}^{\tilde{n}}$ with $\tilde{n} \geq n$, and $y_1, y_2, \ldots, y_t \in \Lambda$ are any t linearly independent lattice vectors, then for $1 \leq j \leq t$ we have*

$$||b_j||^2 \leq \beta^{n-1} \max\{||y_1||^2, ||y_2||^2, \ldots, ||y_t||^2\}.$$

The major steps of the LLL algorithm can be described as follows (Fig. 7.6).

- First, we conduct the Gram–Schmidt Orthogonalization (GSO) process on the input basis b_i, $i = 1, 2, \ldots, m$,

$$\begin{aligned}
&b_1^* = b_1,\\
&b_2^* = b_2 - \mu_{2,1} b_1^*, \quad \mu_{2,1} = \tfrac{b_2 \cdot b_1^*}{b_1^* \cdot b_1^*}\\
&\cdots\\
&b_i^* = b_i - \mu_{i,i-1} b_{i-1}^* - \mu_{i,i-2} b_{i-2}^* - \cdots - \mu_{i,1} b_1^*, \quad \mu_{i,j} = \tfrac{b_i \cdot b_j^*}{b_j^* \cdot b_j^*},\ 1 \leq j < i,\\
&\cdots\\
&b_m^* = b_m - \mu_{m,m-1} b_{m-1}^* - \mu_{m,m-2} b_{m-2}^* - \cdots - \mu_{m,1} b_1^*.
\end{aligned}$$

- Second, we conduct the following two main operations on basis vectors $b_1, \ldots, b_m$, which are called "Reduce" and "Exchange," respectively,
  - (Reduce) If $|\mu_{i,j}| > \frac{1}{2}$, then $b_i \leftarrow b_i - \lceil \mu_{i,j} \rfloor b_j$,
  - (Exchange) If $||b_i^* + \mu_{i,i-1} b_{i-1}^*||^2 < \alpha ||b_{i-1}^*||^2$, then exchange b_i and b_{i-1}, where $\frac{1}{4} < \alpha < 1$ is a parameter with the pre-given value.

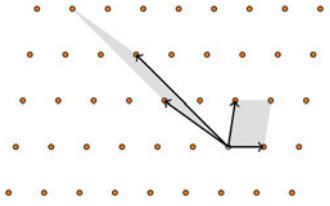

Fig. 7.6 Illustration of the LLL-reduced basis

As for the output, the LLL algorithm returns an α-reduced basis which satisfies the following conditions,

- $|\mu_{i,j}| \leq \frac{1}{2}$, $1 \leq j < i \leq m$,
- $||b_i^* + \mu_{i,i-1} b_{i-1}^*||^2 \geq \alpha ||b_{i-1}^*||^2$, $1 < i \leq m$.

The pseudocode for the LLL algorithm is presented in Algorithm 5 in Lu (2014). For a more detailed description of the LLL basis reduction algorithm, please refer to Chap. 4 of Bremner's book (Bremner 2011). As a remark, the book edited by Nguyen and Vallée (2010) is a more advanced introduction and survey for the theory and applications of the LLL basis reduction algorithm.

7.2.2.2 Illustrative Examples

Next we present a hands-on numerical example to illustrate how algorithms **LO-Alg** and **CJOS-Alg** work.

Example 2 Let's consider the following subset sum problem with $n = 3$,

$$3x_1 + 5x_2 + 7x_3 = 8,$$

where $x = (x_1, x_2, x_3) \in \{0, 1\}^3$, and density $= \frac{3}{\log_2 7} = 1.0686$.

The B_{LO} matrix defined in (7.9) is as follows:

$$B_{LO} = \begin{pmatrix} I & \mathbf{0}^{n\times 1} \\ -a & b \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -3 & -5 & -7 & 8 \end{pmatrix}.$$

Conducting GSO process yields the following decomposition,

$$\begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \mu_{2,1} & 1 & 0 & 0 \\ \mu_{3,1} & \mu_{3,2} & 1 & 0 \\ \mu_{4,1} & \mu_{4,2} & \mu_{4,3} & 1 \end{pmatrix} \begin{pmatrix} d_1^* \\ d_2^* \\ d_3^* \\ d_4^* \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1.5 & 1 & 0 & 0 \\ 2.1 & 1.9310 & 1 & 0 \\ -2.4 & -2.2069 & 1.6467 & 1 \end{pmatrix} \begin{pmatrix} d_1^* \\ d_2^* \\ d_3^* \\ d_4^* \end{pmatrix},$$

where d_i^T with $i = 1, 2, 3, 4$ is the ith column of matrix B_{LO}.

Setting $\alpha = 3/4$ in LLL algorithm yields the column-wise LLL reduced matrix as follows:

$$\tilde{B}_{LO} = \begin{pmatrix} 1 & 0 & -2 & -1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix}.$$

where we could identify the following binary solution from the first column of matrix $\tilde{B}_{LO}$,

$$(x_1, x_2, x_3) = (1, 1, 0).$$

Remarks Recall that the **LO-Alg** algorithm identifies the binary solution in the following way,

"The algorithm checks whether any column of $\tilde{B}_{LO}$ has the form of $\tilde{b}_{i,j} \in \{0, \lambda\}$, $i = 1, 2, \ldots, n$, for some fixed value λ and $\tilde{b}_{n+1,j} = 0$, where $1 \leq j \leq n + 1$. If it fails, the algorithm repeats with b replaced by $\sum_{i=1}^{n} a_i - b$. If such a column appears, then we divide $\tilde{b}_{i,j} \in \{0, \lambda\}$, $i = 1, 2, \ldots, n$ by λ, and check whether the binary vector is a solution. " □

Example 3 Let's reconsider the problem in Example 2. The B_{CJOS} matrix defined in (7.10) is as follows:

$$B_{CJOS} = \begin{pmatrix} I & \frac{1}{2} \times \mathbf{1}^{n \times 1} \\ aN & bN \end{pmatrix}.$$

We substitute the values of a and b into B_{CJOS}, choose $N = 10^2$, and set $\alpha = 3/4$ in LLL algorithm, then calculate the column-wise LLL reduced matrix as follows:

$$\tilde{B}_{CJOS} = \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 0 & -N \end{pmatrix}.$$

where we could identify the following binary solution from the third column of matrix $\tilde{B}_{CJOS}$,

$$(x_1, x_2, x_3) = (1, 1, 0).$$

Note Although the first and second column of $\tilde{B}_{CJOS}$ also satisfy the following condition,

" $\tilde{b}_{i,j} \in \{-\frac{1}{2}, \frac{1}{2}\}$, $i = 1, 2, \ldots, n$, and $\tilde{b}_{n+1,j} = 0$."
But after checking we discover that when we add back $\frac{1}{2}$, $(0, 1, 0)$ and $(0, 0, 0)$ are not binary solutions to the original problem.

Remarks Recall that the **CJOS-Alg** algorithm identifies the binary solution in the following way,

"The algorithm checks whether any column of $\tilde{B}_{CJOS}$ has the form of $\tilde{b}_{i,j} \in \{-\frac{1}{2}, \frac{1}{2}\}$, $i = 1, 2, \ldots, n$, and $\tilde{b}_{n+1,j} = 0$, where $1 \leq j \leq n+1$. If yes, then we add back $\frac{1}{2}$ to $\tilde{b}_{i,j} \in \{-\frac{1}{2}, \frac{1}{2}\}$, $i = 1, 2, \ldots, n$, and check whether the binary vector is a solution." □

7.3 Conclusion and Further Discussion

In this book chapter, we first go through, in introduction part, the development of Modern Cryptography from the era of World War II, to the prevailing Big Data Era now. The invention of "computer" empowers human computing ability, and together with wars between developed countries around 1930s, boost the development of theory and techniques of *Modern* Cryptography. Nowadays, applications of cryptography can be found everywhere in our daily life and multiple channels of industrial businesses, such as applications in Financial Technology (Fin-Tech), and Electric Power Industry, etc. We also use the "Authentication" step in online payment systems as an illustrative case to demonstrate the importance of cryptosystems in the newly emerging field *Fin-Tech*.

Later in Sect. 7.2, we review the classical knapsack cryptosystem designed by Merkle and Hellman in their seminal paper published in 1978 (Merkle and Hellman 1978) and also study the decryption technique proposed by Shamir (1984) in 1984. It's worth mentioning that Hellman is one of the winners of *Turing Award* in 2015 for his brilliant work together with Diffie in 1976 (Diffie and Hellman 1976). Besides, we also review and present the lattice theory based decryption technique proposed (Lagarias and Odlyzko 1985; Coster et al. 1992) to break the hardest subset sum problem (SSP)-based cryptosystem.

Cryptography existing as a science and art of secrecy communication has developed from Vintage Cryptography Era and Caesar's code adopted in *Gallic Wars* being one typical representative, to Enigma and Purple machines used in modern war, i.e., WW-II, to the MD5 and the SHA-1 techniques used in modern internet communication nowadays. We conjecture that one promising future development direction of cryptography theory and technique could be the quantum cryptosystems, equipped with the rapid development of quantum theory and quantum computer, which involves some notions from quantum mechanics explaining how objects behave at the microscopic level, and in the presence of a massive amount of "big data."

Last but not least, we would like to emphasize that this book chapter only serves as a modest spur to induce more valuable discussions, and is a starting point for readers to delve deeper into this promising field. We would like to thank all readers for their patience to go through this book chapter, and we would be more than happy to know that readers also find and believe modern cryptography is an interesting field with huge importance in the prevailing Big-Data Era.

Acknowledgements We would like to express our gratitude to Prof. Duan Li for sharing his comments and suggestions on this paper. We also would like to thank Dr. Junxian HUANG, the CEO of BeeCloud CO., Ltd. for sharing his knowledge on online payment systems, and Dr. Don HUANG for sharing his knowledge on Black–Litterman model.

References

F. Black, R. Litterman, Global portfolio optimization. Financ. Anal. J. **48**(5), 28–43 (1992)

M.R. Bremner, *Lattice Basis Reduction: An Introduction to the LLL Algorithm and Its Applications* (CRC, Boca Raton, FL, 2011)

E.F. Brickell, Solving low density knapsacks, in *Advances in Cryptology, Proceedings of CRYPTO '83, Santa Barbara, CA, August 21–24, 1983*, ed. by D. Chaum (Plenum, New York, 1983), pp. 25–37

V. Cerf, J.E. Hopcroft, R.E. Kahn, R.L. Rivest, A. Shamir, Information, data, security in a networked future, in *ACM-TURING'12 ACM Turing Centenary Celebration, San Francisco, CA, June 15–16*, no. 14 (2012)

M.J. Coster, B.A. LaMacchia, A.M. Odlyzko, C.P. Schnorr, An improved low-density subset sum algorithm, in *Advances in Cryptology: Proceedings of Eurocrypt '91* (1991), pp. 54–67

M.J. Coster, A. Joux, B.A. LaMacchia, A.M. Odlyzko, C.P. Schnorr, J. Stern, Improved low-density subset sum algorithms. Comput. Complex. **2**, 111–128 (1992)

W. Diffie, M.E. Hellman, New directions in cryptography. IEEE Trans. Inf. Theory **IT-22**, 644–654 (1976)

A.M. Frieze, On the Lagarias-Odlyzko algorithm for the subset sum problem. SIAM J. Comput. **15**, 536–539 (1986)

J. Gao, D. Li, X. Cui, S. Wang, Time cardinality constrained mean-variance dynamic portfolio selection and market timing: a stochastic control approach. Automatica **54**, 91–99 (2015)

M.R. Garey, D.S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness* (W. H. Freeman, San Francisco, 1979)

Gartner, Gartner says solving 'big data' challenge involves more than just managing volumes of data. Gartner Special Report Examines How to Leverage Pattern-Based Strategy to Gain Value in Big Data (June 27, 2011)

F. Glover, R.E. Woolsey, Aggregating diophantine equations. Z. Oper. Res. **16**, 1–10 (1972)

M. Hillbert, Big data for development: a review of promises and challenges. Dev. Policy Rev. **34**, 1–41 (2015)

S.M. Jen, C.Y. Lu, T.L. Lai, J.F. Yang, Empirical exploration of lattice attacks for building secure knapsack cryptosystems, in *2012 International Conference on Anti-Counterfeiting, Security and Identification* (IEEE, New York, 2012a), pp. 1–5

S.M. Jen, T.L. Lai, C.Y. Lu, J.F. Yang, Knapsack cryptosystems and unreliable reliance on density, in *AINA*, ed. by L.T. Barolli, F. Enokido, Xhafa, M. Takizawa (IEEE, New York, 2012b), pp. 748–754

W. Jennifer, *Solving the Enigma: History of the Cryptanalytic Bombe* (Center for Cryptological History, National Security Agency, Fort George G. Meade, 2006)

J.C. Lagarias, A.M. Odlyzko, Solving low-density subset sum problems, in *24th Annual Symposium on Foundations of Computer Science, 7–9 November 1983, Tucson, AZ* (IEEE, New York, 1983), pp. 1–10

J.C. Lagarias, A.M. Odlyzko, Solving low-density subset sum problems. J. Assoc. Comput. Mach. **32**, 229–246 (1985)

H.W. Lenstra, Integer programming with a fixed number of variables. Math. Oper. Res. **8**, 538–548 (1983)

A.K. Lenstra, H.W. Lenstra Jr., L. Lovász, Factoring polynomials with rational coefficients. Math. Ann. **261**, 515–534 (1982)

D. Li, X. Sun, J. Gao, S. Gu, X. Zheng, Reachability determination in acyclic Petri nets by cell enumeration approach. Automatica **47**, 2094–2098 (2011)
L. Lovász, H.E. Scarf, The generalized basis reduction algorithm. Math. Oper. Res. **17**, 751–764 (1992)
B. Lu, Linear diophantine equations: integration of disaggregation with LLL algorithm. Ph.D. Thesis, The Chinese University of Hong Kong (2014)
B. Lu, D. Li, Tackling density one subset sum problems: integration of disaggregation technique with lattice attacks. Working paper (2016)
H. Markowitz, Portfolio selction. J. Financ. **7**(1), 77–91 (1952)
R.C. Merkle, M.E. Hellman, Hiding information and signatures in trapdoor knapsacks. IEEE Trans. Inf. Theory **IT-24**, 525–530 (1978)
P.Q. Nguyen, B. Vallée (eds.) *The LLL Algorithm: Survey and Applications*. Information Security and Cryptography. Springer, Berlin, Heidelberg (2010)
T. Okamoto, K. Tanaka, S. Uchiyama, Quantum public-key cryptosystems, in *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, CA, August 20–24, 2000, Proceedings*, ed. by M. Bellare. Lecture Notes in Computer Science, vol. 1880 (Springer, Berlin, 2000), pp. 147–165
R. Rivest, *The MD5 Message-Digest Algorithm* (MIT Laboratory for Computer Science and RSA Data Security, Cambridge, MA, 1992)
R.L. Rivest, A. Shamir, L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
C.P. Schnorr, M. Euchner, Lattice basis reduction: improved practical algorithms and solving subset sum problems, in *Fundamentals of Computation Theory, 8th International Symposium, FCT 91, Gosen, September 9–13, 1991, Proceedings*, ed. by L. Budach. Lecture Notes in Computer Science, vol. 529 (Springer, Berlin, 1991), pp. 68–85
C.P. Schnorr, M. Euchner, Lattice basis reduction: improved practical algorithms and solving subset sum problems. Math. Program. **66**, 181–191 (1994)
C.P. Schnorr, T. Shevchenko, Solving subset sum problems of density close to 1 by "randomized" BKZ-reduction. IACR Cryptol. ePrint Archive, 1–5 (2012)
A. Shamir, A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem. IEEE Trans. Inf. Theory **IT-30**, 699–704 (1984)
S. Singh, *The Code Book: The Science of Secrecy From Ancient Egypt to Quantum Cryptography* (Anchor, New York, 1999)
X. Wang, H. Yu, How to break MD5 and other hash functions, in *Advances in Cryptology - EUROCRYPT 2005*. Lecture Notes in Computer Science, vol. 3494 (Springer, Berlin, 2005), pp. 19–35
J. Watling, China's internet giants lead in online finance. The Financialist (Retrieved 15 February 2014), Credit Suisse
S. Zhu, M. Fan, D. Li, Portfolio management with robustness in both prediction and decision: a mixture model based learning approach. J. Econ. Dyn. Control **48**, 1–25 (2014)