Beauty of Cryptography: the Cryptographic Sequences and the Golden Ratio*

Shenghui Su [1, 3], Jianhua Zheng [2, 4], and Shuwang Lv [2, 5]

[1] College of Computers, Nanjing Univ. of Aeronautics & Astronautics, Nanjing 211106, PRC
[2] Lab. of Information Security, Chinese Academy of Sciences, Beijing 100039, PRC
[3] School of Computers, National University of Defense Technology, Changsha 410073, PRC
[4] Lab. of Digital ID, Peking Knowledge Security Engineering Center, Beijing 100083, PRC
[5] Lab. of Computational Complexity, BFID Corporation, Fuzhou 350207, PRC

Abstract: In this paper, the authors construct a new type of cryptographic sequence which is named an extra-super increasing sequence, and give the definitions of the minimal super increasing sequence $\{\underline{a}_1, \underline{a}_2, \cdots, \underline{a}_n\}$ and minimal extra-super increasing sequence $\{\underline{z}_1, \underline{z}_2, \cdots, \underline{z}_n\}$. Prove that the minimal extra-super increasing sequence is the odd-positioned subsequence of the Fibonacci sequence, namely $\{\underline{z}_1, \underline{z}_2, \ldots, \underline{z}_n, \ldots\} = \{F_1, F_3, \ldots, F_{2n-1}, \ldots\}$, which indicates that the approach to the golden ratio ϕ through the difference $(\underline{z}_{n+1} / \underline{z}_n - 1)$ is more smooth and expeditious than through the ratio (F_{n+1} / F_n). Further prove that the limit of the term ratio difference between the two cryptographic sequences equals the golden ratio conjugate Φ, namely $lim_{n\to\infty}(\underline{z}_n / \underline{z}_{n-1} - \underline{a}_n / \underline{a}_{n-1}) = \Phi$, which reveals the beauty of cryptography.

Keywords: Minimal extra-super increasing sequence, Fibonacci sequence, Golden ratio, Golden ratio conjugate, Term ratio difference

1 Introduction

In the world of numbers, there exist some interesting and unobservable phenomena.

A super increasing sequence and analogous sequences are ones about cryptography [1]. The Fibonacci sequence is a fabulous progression [2], and the golden ration is an important irrational number [3]. In this paper, the authors discuss the triangular relations among these three things, and propose and prove the two new theorems, which designate a stabler and faster approach to the golden ration, and display the beauty of cryptography on the golden ration conjugate.

Throughout the paper, unless otherwise specified, the sign ∞ denotes the infinity, ϕ signifies the golden ratio, Φ signifies the golden ratio conjugate, $\surd x$ represents the square root of a positive real number x, and $\sum$ means an accumulative sum.

2 Definitions of the Minimal Super Increasing Sequence and Minimal Extra-super Increasing Sequence

In cryptography, we always consider finite sequences. An infinite sequence may be truncated to a fitly finite sequence.

2.1 Four Definitions Relevant to Cryptographic Sequences

The concept of a super increasing sequence was firstly proposed in 1978 by R. C. Merkle and M. E. Hellman [1], and used for the design of the MH knapsack cryptosystems [4].

* This work is supported by MOST with Project 2009AA01Z441. Corresponding email: idology98@gmail.com. 5 Sep 2021.

Definition 1: For n positive integers $a_1, a_2, \ldots,$ and a_n (n goes infinite), if a_i ($2 \le i \le n$) satisfies

$$a_i > \sum_{j=1}^{i-1} a_j, \tag{1}$$

then this integer progression is called a super increasing sequence, denoted by $\{a_1, a_2, \ldots, a_n\}$, and shortly $\{a_i\}$, which is a known concept.

For example, $\{a_1, a_2, \ldots, a_8\} = \{2, 3, 7, 13, 29, 57, 113, 226\}$ is a super increasing sequence.

In what follows, we construct a new type of super increasing sequence.

Definition 2: For n positive integers $z_1, z_2, \ldots,$ and z_n (n goes infinite), if z_i ($2 \le i \le n$) satisfies

$$z_i > \sum_{j=1}^{i-1} (i-j)z_j, \tag{2}$$

then this integer progression is called an extra-super increasing sequence, denoted by $\{z_1, z_2, \ldots, z_n\}$, and shortly $\{z_i\}$.

For example, $\{z_1, z_2, \ldots, z_8\} = \{1, 3, 8, 21, 54, 139, 367, 960\}$ is an extra-super increasing sequence.

Definition 3: For n positive integers $\underline{a}_1, \underline{a}_2, \ldots,$ and $\underline{a}_n$ (n goes infinite), if the first term $\underline{a}_1 = 1$, and $\underline{a}_i$ ($2 \le i \le n$) satisfies

$$\underline{a}_i = 1 + \sum_{j=1}^{i-1} \underline{a}_j, \tag{3}$$

then this integer progression is called the minimal super increasing sequence, denoted by $\{\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_n\}$, and shortly $\{\underline{a}_i\}$, which is a special case of super increasing sequences.

For example, $\{\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_8\} = \{1, 2, 4, 8, 16, 32, 64, 128\}$ is the 8th minimal super increasing sequence.

Definition 4: For n positive integers $\underline{z}_1, \underline{z}_2, \ldots,$ and $\underline{z}_n$ (n goes infinite), if the first term $\underline{z}_1 = 1$, and $\underline{z}_i$ ($2 \le i \le n$) satisfies

$$\underline{z}_i = 1 + \sum_{j=1}^{i-1} (i-j)\underline{z}_j, \tag{4}$$

then this integer progression is called the minimal extra-super increasing sequence, denoted by $\{\underline{z}_1, \underline{z}_2, \ldots, \underline{z}_n\}$, and shortly $\{\underline{z}_i\}$, which is a special case of extra-super increasing sequences.

For example, $\{\underline{z}_1, \underline{z}_2, \ldots, \underline{z}_8\} = \{1, 2, 5, 13, 34, 89, 233, 610\}$ is the 8th minimal extra-super increasing sequence.

Owing to

$$\begin{aligned}\underline{z}_i &= 1 + \sum_{j=1}^{i-1} (i-j)\underline{z}_j = 1 + (i-1)\underline{z}_1 + (i-2)\underline{z}_2 + \ldots + 2\cdot\underline{z}_{i-2} + 1\cdot\underline{z}_{i-1} \\ &= (1 + ((i-1)-1)\underline{z}_1 + ((i-1)-2)\underline{z}_2 + \ldots + 1\cdot\underline{z}_{i-2}) + (\underline{z}_1 + \underline{z}_2 + \ldots + \underline{z}_{i-1}),\end{aligned}$$

Formula (4) may be expressed as

$$\underline{z}_i = \underline{z}_{i-1} + \sum_{j=1}^{i-1} \underline{z}_j, \tag{4$'$}$$

which will be employed in the following text.

2.2 Cryptographic Meanings of Extra-super Increasing Sequences

An extra-super increasing sequence bears a useful property.

Property 1: Assume that $\{z_1, z_2, \ldots, z_n\}$ is an extra-super increasing sequence. Then, for the term z_i ($1 < i \le n$) and any positive integer k, there exists

$$(k+1)z_i > \sum_{j=1}^{i-1}(k+i-j)z_j. \tag{5}$$

Proof:

According to Definition 2, there is $z_i > \sum_{j=1}^{i-1} (i-j)z_j$, and its development is

$$z_i > (i-1)z_1 + (i-2)z_2 + \ldots + 1\cdot z_{i-1}. \tag{2$'$}$$

Naturally,

$$z_i > z_1 + z_2 + \ldots + z_{i-1}.$$

Further, there is

$$kz_i > kz_1 + kz_2 + \ldots + kz_{i-1}, \tag{5$'$}$$

where k (> 0) is an arbitrary integer.

Adding (5′) to (2′) obtains

$$kz_i + z_i > (kz_1 + (i-1)z_1) + (kz_2 + (i-2)z_2) + \ldots + (kz_{i-1} + 1\cdot z_{i-1}),$$

namely

$$(k+1)z_i > \textstyle\sum_{j=1}^{i-1}(k+i-j)z_j.$$

Hence, Property 1 holds. □

Property 1 makes extra-super increasing sequences (including the minimal extra-super increasing sequence) possess cryptographic meanings.

Let $b_1b_2\ldots b_8 = 11011001$ be a plaintext block, and $L_i = \sum_{j=i}^{8} b_j$ ($1 \le i \le 8$).

Again let $\{z_1, z_2, \ldots, z_8\} = \{1, 2, 5, 13, 34, 89, 233, 610\}$ be an extra-super increasing sequence (also the 8th minimal extra-super increasing sequence).

Then the anomalous subset sum

$$\begin{aligned} S &= \textstyle\sum_{i=1}^{8} b_i L_i z_i \\ &= 1\cdot5\cdot1 + 1\cdot4\cdot2 + 0\cdot3\cdot5 + 1\cdot3\cdot13 + 1\cdot2\cdot34 + 0\cdot1\cdot89 + 0\cdot1\cdot233 + 1\cdot1\cdot610 \\ &= 730 \end{aligned}$$

is a ciphertext.

If $\{z_1, z_2, \cdots, z_8\} = \{1, 2, 5, 13, 34, 89, 233, 610\}$ is known, and $L = 0$ set, the plaintext $b_1b_2\ldots b_8$ can be recovered as follows:

Due to $S = 730 \ge (L+1)$ (z_8 (= 610)), there are $b_8 = 1$, $L = 0 + 1 = 1$, and $S = 730 - 610 = 120$.

Due to $S = 120 < (L+1)$ (z_7 (= 233)), there are $b_7 = 0$, $L = 1 + 0 = 1$, and $S = 120 - 0 = 120$.

Due to $S = 120 < (L+1)$ (z_6 (= 89)), there are $b_6 = 0$, $L = 1 + 0 = 1$, and $S = 120 - 0 = 120$.

Due to $S = 120 \ge (L+1)$ (z_5 (= 34)), there are $b_5 = 1$, $L = 1 + 1 = 2$, and $S = 120 - 2\cdot34 = 52$.

Due to $S = 52 \ge (L+1)$ (z_4 (= 13)), there are $b_4 = 1$, $L = 2 + 1 = 3$, and $S = 52 - 3\cdot13 = 13$.

Due to $S = 13 < (L+1)$ (z_3 (= 5)), there are $b_3 = 0$, $L = 3 + 0 = 3$, and $S = 13 - 0 = 13$.

Due to $S = 13 \ge (L+1)$ (z_2 (= 2)), there are $b_2 = 1$, $L = 3 + 1 = 4$, and $S = 13 - 4\cdot2 = 5$.

Due to $S = 5 \ge (L+1)$ (z_1 (= 1)), there are $b_1 = 1$, $L = 4 + 1 = 5$, and $S = 5 - 5\cdot1 = 0$.

In this way, the ciphertext $b_1b_2\ldots b_8 = 11011001$ is recovered.

During the above process, $\{z_1, z_2, \ldots, z_8\}$ is equivalent to a private key. In practicable asymmetrical cryptosystem, a private key should be converted into a related public key.

Understandably, super increasing sequences and extra-super increasing sequences are referred as the cryptographic sequences.

3 The Fibonacci Sequence and the Golden Ratio

The Fibonacci sequence is a famous one, and the golden ratio is a famous irrational number. There exists a relation between them.

3.1 The Fibonacci Sequence and Its Three Properties

The Fibonacci sequence may be defined recursively.

Definition 5: Let $\{F_0, F_1, \ldots, F_n, \ldots\}$ be a sequence, where

① $F_n = F_{n-1} + F_{n-2}$ (recursion formula)

② $F_0 = 0$, $F_1 = 1$ (initial conditions),

and then $\{F_0, F_1, \ldots, F_n, \ldots\}$ is called the Fibonacci sequence [5][6].

Under the circumstances of having no divergence, $F_0 = 0$ is ignored.

Generally, we have the Fibonacci sequence

$$\{F_1, F_2, \ldots, F_{17}, \ldots\} = \{1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, \ldots\}.$$

The Fibonacci sequence has many properties, of which three are concerned.

Property 2: There are

$$F_{n+1} / F_n \approx \phi, \text{ and } lim_{n\to\infty}(F_{n+1} / F_n) = \phi,$$

where n is comparative large, and ϕ is the golden ratio [5].

Property 3: Summing consecutive odd-positioned Fibonacci numbers, beginning with F_1, will yield a number which is the next Fibonacci number following the last term in the sum [5]. Namely there is

$$F_1 + F_3 + \ldots + F_{2n-1} = F_{2n},$$

where n is equal to or bigger than 1.

For example, there is $F_1 + F_3 + F_5 + F_7 = 1 + 2 + 5 + 13 = 21 = F_8$.

Property 4: For the Fibonacci sequence $\{F_1, \ldots, F_n, \ldots\}$, there is

$$F_n = (\surd 5)^{-1}(\phi^n - (-\phi^{-1})^n),$$

where F_n is called n-th Fibonacci number [5].

The proofs of Property 2, 3, and 4 can be found in Reference [5].

3.2 The Golden Ratio and Golden Ratio Conjugate

The golden ratio exists in art, nature, and science.

Definition 6: The golden ratio is such a ratio of two quantities that it satisfies that the ratio of the sum of the two quantities to the larger is equal to the ratio of the larger to the smaller [7][8].

Let $\phi = a / b$ be a ratio with $a > b > 0$. Then, a and b are said to be in the golden ratio if

$$(a + b) / a = a / b = \phi,$$

namely

$$1 + 1 / \phi = \phi, \tag{6}$$

and further

$$\phi^2 = \phi + 1. \tag{6′}$$

Formula (6) indicates that ϕ is an irrational constant number, and equals approximately to 1.618033988749 [3]. Other names frequently used for the golden ratio are the golden section, golden mean, divine proportion, etc [9].

Again let $\Phi = b / a$ be a ratio with $a > b > 0$. Then, we can derive from Formula (6) the equation

$$1 + \Phi = 1 / \Phi. \tag{7}$$

Commonly, Φ is called the golden ratio conjugate [10]. Furthermore, we have

$$\Phi = \phi - 1, \tag{7′}$$

which can easily be inferred from Formula (6) and (7).

Besides, ϕ may be represented as a continued fraction [11]

$$\phi = [1; 1, 1, 1, \cdots], \tag{8}$$

and also represented as an infinite series [12]

$$\phi = 13 / 8 + \textstyle\sum_{n=0}^{\infty}((-1)^{n+1}(2n + 1)!) / (4^{2n+3}n!(n + 2)!). \tag{9}$$

Evidently, an approximation of ϕ can be fetched from Formula (8) or (9).

4 Relations among Cryptographic Sequences, Fibonacci Sequence, and Golden Ratio

The Fibonacci sequence is a bridge between the cryptographic sequences and the golden ratio.

4.1 Term Ratio of the Minimal Extra-super Increasing Sequence

A term ratio is the ratio of two successive items in the minimal super increasing sequence or the minimal extra-super increasing sequence.

The term ratio μ_i is defined as $\mu_i = a_{i+1} / a_i$ (for $i = 1, 2, \ldots, n, \ldots$).

Property 5: Let $\{a_1, a_2, \ldots, a_n, \ldots\}$ be the minimal super increasing sequence, and then there exists

$$a_{i+1} / a_i = 2 \text{ (for } i = 1, 2, \ldots, n, \ldots),$$

that is to say, the term ratio a_{i+1} / a_i (for $i = 1, 2, \ldots, n, \ldots$) is a constant number.

Proof:

According to Definition 3, there is $a_i = 1 + \sum_{j=1}^{i-1} a_j$ (for $i = 1, 2, \ldots, n, \ldots$), and its development is

$$a_i = 1 + (a_1 + a_2 + \ldots + a_{i-1}).$$

Adding a_i to either of the above expression obtains

$$a_i + a_i = 1 + (a_1 + a_2 + \ldots + a_{i-1} + a_i),$$

namely

$$2a_i = a_{i+1}, \Rightarrow a_{i+1} / a_i = 2.$$

Hence, the term ratio $a_{i+1} / a_i = 2$ (for $i = 1, 2, \ldots, n, \ldots$) is a constant number. □

Similarly, the term ratio ν_i is defined as $\nu_i = z_{i+1} / z_i$ (for $i = 1, 2, \ldots, n, \ldots$).

In conformity to Definition 4, it is easy to calculate

$\{z_1, z_2, \ldots, z_{17}\}$

$= \{1, 2, 5, 13, 34, 89, 233, 610, 1597, 4181, 10946, 28657, 75025, 196418, 514229, 1346269, 3524578\}$.

Now compute the term ratios $\nu_1, \nu_2, \ldots, \nu_{16}$.

As $i = 1$, $\nu_1 = z_2 / z_1 = 2 / 1 = 2$.

As $i = 2$, $\nu_2 = z_3 / z_2 = 5 / 2 = 2.5$.

As $i = 3$, $\nu_3 = z_4 / z_3 = 13 / 5 = 2.6$.

As $i = 4$, $\nu_4 = z_5 / z_4 = 34 / 13 \approx 2.615$.

As $i = 5$, $\nu_5 = z_6 / z_5 = 89 / 34 \approx 2.61764$.

As $i = 6$, $\nu_6 = z_7 / z_6 = 233 / 89 \approx 2.6179775$.

As $i = 7$, $\nu_7 = z_8 / z_7 = 610 / 233 \approx 2.618025751$.

As $i = 8$, $\nu_8 = z_9 / z_8 = 1597 / 610 \approx 2.61803278688$.

As $i = 9$, $\nu_9 = z_{10} / z_9 = 4181 / 1597 \approx 2.6180338134001$.

As $i = 10$, $\nu_{10} = z_{11} / z_{10} = 10946 / 4181 \approx 2.618033963166706$.

As $i = 11$, $\nu_{11} = z_{12} / z_{11} = 28657 / 10946 \approx 2.61803398501735793$.

As $i = 12$, $\nu_{12} = z_{13} / z_{12} = 75025 / 28657 \approx 2.6180339882053250514$.

As $i = 13$, $\nu_{13} = z_{14} / z_{13} = 196418 / 75025 \approx 2.61803398870443185604$.

As $i = 14$, $\nu_{14} = z_{15} / z_{14} = 514229 / 196418 \approx 2.61803398873830300685273$.

As $i = 15$, $\nu_{15} = z_{16} / z_{15} = 1346269 / 514229 \approx 2.6180339887482036213437981$.

As $i = 16$, $\nu_{16} = z_{17} / z_{16} = 3524578 / 1346269 \approx 2.6180339887496481015309718 93$.

In what follows, we estimate the term ratio difference $\nu_i - \mu_i$ ($i = 1, 2, \ldots, 16$).

As $i = 1$, $\nu_1 - \mu_1$ (or 1) = 0 (or 1).

As $i = 2$, $\nu_2 - \mu_2$ (or 1) = 0.5 (or 1.5).

As $i = 3$, $\nu_3 - \mu_3$ (or 1) = 0.6 (or 1.6).

As $i = 4$, $\nu_4 - \mu_4$ (or 1) = 0.615 (or 1.615).

As $i = 5$, $\nu_5 - \mu_5$ (or 1) = 0.61764 (or 1.61764).

As $i = 6$, $\nu_6 - \mu_6$ (or 1) = 0.6179775 (or 1.6179775).

As $i = 7$, $\nu_7 - \mu_7$ (or 1) = 0.618025751 (or 1.618025751).

As $i = 8$, $\nu_8 - \mu_8$ (or 1) = 0.61803278688 (or 1.61803278688).

As $i = 9$, $\nu_9 - \mu_9$ (or 1) = 0.6180338134001 (or 1.6180338134001).

As $i = 10$, $\nu_{10} - \mu_{10}$ (or 1) = 0.618033963166706 (or 1.618033963166706).

As $i = 11$, $\nu_{11} - \mu_{11}$ (or 1) = 0.61803398501735793 (or 1.61803398501735793).

As $i = 12$, $\nu_{12} - \mu_{12}$ (or 1) = 0.6180339882053250514 (or 1.6180339882053250514).

As $i = 13$, $\nu_{13} - \mu_{13}$ (or 1) = 0.61803398867044318 5604 (or 1.61803398867044318 5604).

As $i = 14$, $\nu_{14} - \mu_{14}$ (or 1) = 0.6180339887383030068 5273 (or 1.6180339887383030068 5273).

As $i = 15$, $\nu_{15} - \mu_{15}$ (or 1) = 0.618033988748203621343 7981 (or 1.618033988748203621343 7981).

As $i = 16$, $\nu_{16} - \mu_{16}$ (or 1) = 0.618033988749648101530971893 (or 1.618033988749648101530971893).

From the above, we observe that $lim_{i\to\infty}(\nu_i - \mu_i)$ is approaching a certain number, and $lim_{i\to\infty}(\nu_i - 1)$ is also approaching a certain number.

4.2 The Minimal Extra-super Increasing Sequence Being a Regular Subsequence of the Fibonacci Sequence

Let $\{z_1, z_2, \ldots, z_9, \ldots\} = \{1, 2, 5, 13, 34, 89, 233, 610, 1597, \ldots\}$ is the minimal extra-super increasing sequence.

$\{F_1, F_2, \ldots, F_{17}, \ldots\} = \{1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, \ldots\}$ is the Fibonacci sequence.

It is not hard to watch $z_1 = F_1$, $z_2 = F_3$, $z_3 = F_5$, …, and $z_9 = F_{17}$.

Theorem 1: The minimal extra-super increasing sequence $\{z_1, z_2, \ldots, z_n, \ldots\}$ is the odd-positioned subsequence of the Fibonacci sequence $\{F_1, F_2, \ldots, F_n, \ldots\}$, namely $\{z_1, z_2, \ldots, z_n, \ldots\} = \{F_1, F_3, \ldots, F_{2n-1}, \ldots\}$.

Proof (by induction):

① When $n = 1$, it holds that $\{z_1\} = \{1\} = \{F_{2\cdot 1-1}\} = \{F_1\}$.

② When $n = 2$, it holds that $\{z_1, z_2\} = \{1, 2\} = \{F_{2\cdot 1-1}, F_{2\cdot 2-1}\} = \{F_1, F_3\}$.

③ When $n = 3$, it holds that $\{z_1, z_2, z_3\} = \{1, 2, 5\} = \{F_{2\cdot 1-1}, F_{2\cdot 2-1}, F_{2\cdot 3-1}\} = \{F_1, F_3, F_5\}$.

④ Assume that when $n = k$, it holds that $\{z_1, z_2, \ldots, z_k\} = \{F_1, F_3, \ldots, F_{2\cdot k-1}\}$.

⑤ In succession, we need to proof that when $n = k + 1$, it holds that

$$\{z_1, z_2, \ldots, z_k, z_{k+1}\} = \{F_1, F_3, \ldots, F_{2\cdot k-1}, F_{2\cdot k+1}\}.$$

In light of Formula (4′), there is

$$z_{k+1} = z_k + \textstyle\sum_{j=1}^{k} z_j = z_1 + z_2 + \ldots + z_k + z_k.$$

Again in light of the assumption at ④, there is

$$z_{k+1} = z_1 + z_2 + \ldots + z_k + z_k = F_1 + F_3 + \ldots + F_{2\cdot k-1} + F_{2\cdot k-1}.$$

By Property 3, there is

$$z_{k+1} = F_1 + F_3 + \ldots + F_{2\cdot k-1} + F_{2\cdot k-1} = F_{2\cdot k} + F_{2\cdot k-1}.$$

Again by Definition 5, there is

$$z_{k+1} = F_{2\cdot k} + F_{2\cdot k-1} = F_{2\cdot k+1}.$$

Namely

$$\{z_1, z_2, \ldots, z_k, z_{k+1}\} = \{F_1, F_3, \ldots, F_{2\cdot k-1}, F_{2\cdot k+1}\}.$$

Hence, $\{z_1, z_2, \ldots, z_n, \ldots\}$ is the odd-positioned subsequence of $\{F_1, F_2, \ldots, F_n, \ldots\}$. □

Section 4.1 and Theorem 1 manifest together that the ratio difference $(z_{n+1}/z_n - 1/1)$ or $(F_{2n+1}/F_{2n-1} - 1/1)$ is a more smooth and expeditious approach to ϕ than the ratio (F_{n+1}/F_n).

4.3 Limit of Term Ratio Difference ($z_{n+1}/z_n - a_{n+1}/a_n$) Being Equal to Φ

By the medium of the Fibonacci sequence $\{F_1, F_2, \ldots, F_n, \ldots\}$, the term ratio difference $(z_{n+1}/z_n - a_{n+1}/a_n)$ between the two cryptographic sequences corresponds to the golden ratio conjugate Φ.

Theorem 2: Let $\{z_1, z_2, \ldots, z_n\}$ be the minimal extra-super increasing sequence, and $\{a_1, a_2, \ldots, a_n\}$ be the minimal super increasing sequence, and then $lim_{n\to\infty}(z_{n+1}/z_n - a_{n+1}/a_n) = \Phi$.

Proof.

By Theorem 1, there is $\{\underline{z}_1, \underline{z}_2, \ldots, \underline{z}_n, \ldots\} = \{F_1, F_3, \ldots, F_{2n-1}, \ldots\}$, and by Property 5, $\underline{a}_{n+1} / \underline{a}_n = 2$. Thus, there exists

$$\begin{aligned} lim_{n\to\infty}(\underline{z}_{n+1}/\underline{z}_n - \underline{a}_{n+1}/\underline{a}_n) &= lim_{n\to\infty}(F_{2n+1}/F_{2n-1} - \underline{a}_{n+1}/\underline{a}_n) \\ &= lim_{n\to\infty}(F_{2n+1}/F_{2n-1} - 2) \\ &= lim_{n\to\infty}(F_{2n+1}/F_{2n-1}) - 2. \end{aligned}$$

Again by Property 4,

$$\begin{aligned} & lim_{n\to\infty}(F_{2n+1}/F_{2n-1}) \\ &= lim_{n\to\infty}((\sqrt{5})^{-1}(\phi^{2n+1} - (-\phi^{-1})^{2n+1})) / ((\sqrt{5})^{-1}(\phi^{2n-1} - (-\phi^{-1})^{2n-1})) \\ &= lim_{n\to\infty}(\phi^{2n+1} - (-\phi^{-1})^{2n+1}) / (\phi^{2n-1} - (-\phi^{-1})^{2n-1}) \\ &= lim_{n\to\infty}(\phi^2(\phi^{2n-1} - (-\phi^{-1})^{2n+3})) / (\phi^{2n-1} - (-\phi^{-1})^{2n-1}) \\ &= \phi^2\, lim_{n\to\infty}(\phi^{2n-1} - (-\phi^{-1})^{2n+3}) / (\phi^{2n-1} - (-\phi^{-1})^{2n-1}) \\ &= \phi^2\, lim_{n\to\infty}(\phi^{2n-1}(1 + (\phi^{-1})^{4n+2})) / (\phi^{2n-1}(1 + (\phi^{-1})^{4n-2})) \\ &= \phi^2\, lim_{n\to\infty}(1 + (\phi^{-1})^{4n+2}) / (1 + (\phi^{-1})^{4n-2}) \\ &= \phi^2\, lim_{n\to\infty}(1 + 0) / (1 + 0) \\ &= \phi^2. \end{aligned}$$

In terms of Formula (6′), there is $\phi^2 = \phi + 1$.

Further, there is

$$lim_{n\to\infty}(F_{2n+1}/F_{2n-1}) = \phi + 1.$$

Again In terms of Formula (7′), there is

$$lim_{n\to\infty}(F_{2n+1}/F_{2n-1}) - 2 = \phi + 1 - 2 = \phi - 1 = \Phi.$$

Hence, the limit $lim_{n\to\infty}(\underline{z}_{n+1}/\underline{z}_n - \underline{a}_{n+1}/\underline{a}_n) = \Phi$ holds. □

Theorem 2 shows the relation between the cryptographic sequences and the golden ratio.

5 Conclusion

The paper constructs a new type of cryptographic sequence which is named an extra-super increasing sequence, and gives the definitions of the minimal super increasing sequence $\{\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_n\}$ and minimal extra-super increasing sequence $\{\underline{z}_1, \underline{z}_2, \ldots, \underline{z}_n\}$.

The paper discusses the triangular relations among the cryptographic sequences, the Fibonacci sequence, and the golden ratio. Theorem 1 tells us $\{\underline{z}_1, \underline{z}_2, \ldots, \underline{z}_n, \ldots\} = \{F_1, F_3, \ldots, F_{2n-1}, \ldots\}$, which indicates that the approach to ϕ through the difference value $(\underline{z}_{n+1} / \underline{z}_n - 1)$ is more smooth and expeditious than through the ratio (F_{n+1} / F_n). Theorem 2 tells us $lim_{n\to\infty}(\underline{z}_{n+1}/\underline{z}_n - \underline{a}_{n+1}/\underline{a}_n) = \Phi$, which reveals the beauty of cryptography.

Our tasks have not been completed by now. At the next step, we will research extra-super increasing sequences thoroughly, and devise new asymmetrical cryptosystems based on extra-super increasing sequences.

Acknowledgment

The authors would like to thank the Academicians Jiren Cai, Zhongyi Zhou, Zhengyao Wei, Xicheng Lu, Qinmin Wang, Jinpeng Huai, Huaimin Wang, Yaxiang Yuan, Andrew C. Yao, Binxing Fang, and Xiangke Liao for their important advice and help.

The authors also would like to thank the Professors Jie Wang, Zhiying Wang, Ronald L. Rivest, Moti Yung, Dingzhu Du, Hanliang Xu, Yixian Yang, Yupu Hu, Ping Luo, Maozhi Xu, Wenbao Han, Zhiqiu Huang, Zhihui Wei, Lusheng Chen, Bogang Lin, Yiqi Dai, Lequan Min, Dingyi Pei, Mulan Liu, Huanguo Zhang, Qibin Zhai, Hong Zhu, Renji Tao, Quanyuan Wu, and Zhichang Qi for their important suggestions and corrections.

References

1. R. C. Merkle and M. E. Hellman. Hiding Information and Signatures in Trapdoor Knapsacks. IEEE Transactions on Information Theory, v24(5), 1978, pp. 525-530.
2. T. H. Garland. Fascinating Fibonaccis: Mystery and Magic in Numbers. PaloAlto, CA: Dale Seymour, 1987.
3. E. W. Weisstein. CRC Concise Encyclopedia of Mathematics (2nd Ed.). New York, NY: CRC Press, 2002.
4. A. J. Menezes, P. van Oorschot, and S. Vanstone. Handbook of Applied Cryptography. New York, NY: CRC Press, 1997.
5. A. S. Posamentier and I. Lehmann. The Fabulous Fibonacci Numbers. Amherst, NY: Prometheus Books, 2007.
6. R. A. Dunlap. The Golden Ratio and Fibonacci Numbers. Singapore, SG: World Scientific Publishing, 1997.
7. K. H. Rosen. Discrete Mathematics and Its Applications. New York, NY: McGraw-Hill, 2012.
8. M. Frings. The Golden Section in Architectural Theory. Nexus Network Journal, v4(1), 2002.
9. P. Hemenway. Divine Proportion: Phi in Art, Nature, and Science. New York, NY: Sterling Publishing, 2005.
10. E. W. Weisstein. CRC Concise Encyclopedia of Mathematics (2nd Ed.). New York, NY: CRC Press, 2002.
11. M. Livio. The Golden Ratio: The Story of Phi, the World's Most Astonishing Number. New York, NY: Broadway Books, 2002.
12. B. Roselle. Development of an Infinite Series Representation for Phi (the Golden Mean or Golden Ratio). New York, NY: CRC Press, 1999.