Mathematical and Computational Applications

Article

An Efficient Golden Ratio Method for Secure Cryptographic Applications

Anthony Overmars and Sitalakshmi Venkatraman *

School of Engineering, Construction & Design, Melbourne Polytechnic, Preston, VIC 3072, Australia; AnthonyOvermars@melbournepolytechnic.edu.au

* Correspondence: SitaVenkat@melbournepolytechnic.edu.au; Tel.: +61-3-9269-1171

Received: 17 September 2018; Accepted: 9 October 2018; Published: 10 October 2018

Abstract: With the increase in the use of electronic transactions in everyday life, secure communications and data storage to withstand any kind of attack is warranted. The golden ratio, being the most irrational among irrational numbers, can be used in elliptic curve cryptosystems, power analysis security, and other applications. However, in such applications, cryptographic operations should take place very quickly before the keys are extracted or decoded by the attackers. This paper proposes an efficient method of golden ratio computation in cryptography to resist information security breaches. We compare our new golden ratio method with the well-known Fibonacci sequence method. The experimental results show that our proposed method is more efficient than the Fibonacci sequence method. Our golden ratio method with infinite precision provides reliable counter measure strategy to address the escalating security attacks.

Keywords: golden ratio; Fibonacci sequence; Diophantine equation; cryptography; secret key; information security; efficient computation

1. Introduction

With technological advancements, electronic communications have evolved to be in various forms and media. Since the early theories of digital communication and secrecy [1,2], there have been rapid advancements in information communication technologies [3]. However, security threats have also increased rapidly, affecting businesses and individuals worldwide [4,5]. Hence, secured communication with appropriate cryptographic techniques plays a key role in this networked society. Cryptography, the art and science of secret writing, is being used by many security systems to securely communicate information over the Internet [6,7]. It uses patterns and algorithms to encrypt all forms of communication messages, including text, images, and signals. Encryption is a process of applying cryptography to encode a message or information in such a way that it becomes unreadable to unauthorized users. In encryption, the original message or plaintext for communication is encoded using an encryption algorithm (cipher) to generate a ciphertext that can only be read if decrypted [8,9]. The encryption algorithm generates a pseudo-random encryption key or secret key, which is used to decrypt the ciphertext for the authorized access of the message. Organizations use cryptography for secure data transmission and storage. Typically, a cryptosystem consists of a set of cryptographic techniques for key generation, encryption, and decryption of the information to preserve its confidentiality, privacy and integrity [10,11].

Many cryptographic techniques are adopted by various businesses and governments to communicate sensitive information to their stakeholders over the Internet. However, cyber-attacks are still on the rise. Hence, many advanced encryption algorithms have emerged to help uphold the security of communication. The size and randomness of the secret key plays a role in addressing security attacks. The golden ratio, defined as the ratio of the hypotenuse of an isosceles triangle to its base, has interesting properties. A golden rectangle with a longer side a and shorter side b, when placed adjacent to a square with sides of length a, will produce a similar golden rectangle with longer side $a + b$ and shorter side a. While researchers have been deriving connections between the golden ratio, resulting in many applications in physics, including Lorentz transformation recently [12], the motivation of our work lies in its application to cryptography. Calculating a precise golden ratio with a higher decimal place of accuracy is of interest in generating more secure keys [13,14]. There is a need for an innovative and efficient method to look beyond the popular Fibonacci method. The aim of this paper is to propose a golden ratio method which is more efficient than the Fibonacci method to develop a faster cryptosystem. By enhancing the cryptographic techniques, this work plays an important role in arriving at a security solution that forms an improved counter measure for cyber-attacks, which are on the rise.

We organize the remainder of the paper as follows. Section 2 gives a literature review of related work. In Section 3, we provide a background theory about the golden ratio and its various properties. We derive the key mathematical relationships of the golden ratio with right-angled triangles and a Fibonacci sequence. These relationships aid in proposing a new faster method for golden ratio computation in Section 4. The experimental results of our proposed method as compared to the commonly used Fibonacci method are summarized in Section 5. Finally, conclusions and future work are given in Section 6.

2. Literature Review

The most popular commercial application of the golden ratio is in RSA cryptography, where primes of about 150 digits are required [2,14–16]. Even though there are many prime number generation algorithms, data breaches and security attacks are still escalating, since attackers are using advanced technologies to decipher these algorithms. In another security context, an interesting example is power analysis, where the attacker uses the patterns of power consumption of a cryptographic hardware device for gaining secret information [17,18]. In other words, devices such as a smart card, integrated circuit chips, microprocessors, or other hardware can be non-invasively attacked by extracting cryptographic keys and other secret information from the device. While simple power analysis (SPA) involves visual interpretation of power signals over a period of time, differential power analysis (DPA) is a more advanced power analysis, where the intermediate values between any two cryptographic operations are statistically analyzed. The attackers study and perform pattern analysis of power signals whenever operations using secret keys are performed that vary the power consumption of such devices.

The most common methods of encryption use Fibonacci numbers generated to convert the plaintext into ciphertext. Stakhov introduces the concept of the golden matrix and its application in cryptography [13]. However, subsequent studies proved that this method in cryptosystems was insecure against certain plaintext attacks [14,16]. In another set of research work, we found that cryptosystems using golden ratio methods were gaining importance by modifying the golden cryptosystem using a k-Fibonacci number [19,20]. While some new proposals of cryptosystem based on k-Fibonacci numbers are shown to be more secure than the original golden cryptography against a plaintext attack, there are still many cyber-attacks taking place [19,21,22].

We argue that a method based on the golden ratio can be used to achieve secure cryptography based on the work by De Castro with respect to realizing it as one-way function [23]. This can be further strengthened by other research work which has provided similar mathematical representations [24]. According to Levin [25], one-way functions are the most important problems in computer theory, and his work provides a unified approach to define this problem including its computational complexity. It is well known that the golden ratio is the most irrational of the irrational numbers. The irrational property of the golden ratio is consistent with Levin's one-way functions, and hence is the most difficult to resolve when used through a one-way function. By introducing an efficient method to calculate the golden ratio, the cycle time would be hastened so that intruders will not have sufficient time to probe or penetrate between two operations with the secret key. Hence, in this work, we explore the mathematical properties of the golden ratio to arrive at a much faster and efficient method for its computation. We compare our method in terms of its efficiency and precision with the popular Fibonacci method.

3. Theory and New Derivations of the Golden Ratio and its Properties

In this section, we define and summarize the theory behind the golden ratio and derive certain key relationships it has with right-angled triangles and the Fibonacci sequence. The relationships we establish here would be used in proposing our new method of golden ratio computation in the next section.

3.1. Definition of the Golden Ratio

The first mathematical definition of the golden ratio traces back to the famous Greek mathematician Euclid who, in the third century B.C., introduced it to solve a geometrical problem called the problem of division of a line segment in an extreme and mean ratio [26]. The essence of the problem is the following:

A line segment AB must be divided with a point C into two parts so that the ratio between the longer part CB and the shorter one AC is equal to the ratio between the whole line segment AB and the longer part CB, i.e.,

$$\frac{AB}{CB} = \frac{CB}{AC}$$

Let us consider a rectangle with dimensions as shown in Figure 1. Then, we can express the golden ratio based on its definition as follows:

$$\varphi = \frac{1}{\varphi - 1} \tag{1}$$

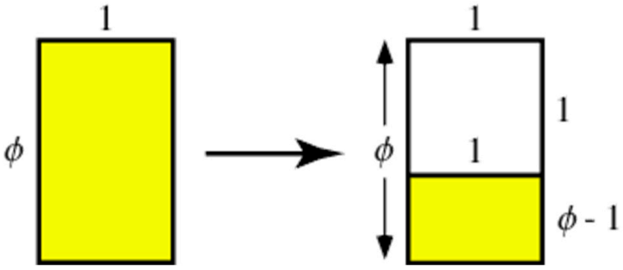

Figure 1. Pictorial representation of the golden ratio.

We determine the value of the golden ratio by undergoing various mathematical transformations as given below.

Performing a multiplication operation on both sides of Equation (1) with $(\varphi - 1)$, we get:

$$\varphi(\varphi - 1) = \frac{\varphi - 1}{\varphi - 1} = 1$$

$$\varphi^2 - \varphi - 1 = 0$$

Completing the square, we get:

$$(\varphi - 1)^2 = \varphi^2 - \varphi + \frac{1}{4} \Rightarrow -\frac{5}{4} \Rightarrow -1$$

$$(\varphi-\frac{1}{2})^2-\frac{5}{4}=0$$

$$(\varphi-\frac{1}{2})^2-\left(\frac{\sqrt{5}}{2}\right)^2=0$$

$$(\varphi-\frac{1}{2}-\frac{\sqrt{5}}{2})(\varphi-\frac{1}{2}+\frac{\sqrt{5}}{2})=0$$

$$(\varphi-\frac{1+\sqrt{5}}{2})(\varphi-\frac{1-\sqrt{5}}{2})=0$$

$$\varphi=\frac{1+\sqrt{5}}{2},\frac{1-\sqrt{5}}{2} \tag{2}$$

In order to arrive at a fast method to calculate the golden ratio, we consider the various properties of the golden ratio in the next sections. We derive mathematical relationships between these properties to propose a new efficient method for golden ratio computations. Such an efficient method is desired since the order of computational complexity plays a major role in cryptosystems [27,28]. The method and results of this paper advance previous work on the methods used for estimating the golden ratio and silver ratio [29,30].

3.2. The Golden Ratio and Right-Angled Triangles

We establish the first property of the golden ratio, where it can be expressed as the ratio of the sides of a right-angled triangle (Figure 2), as follows:

$$\varphi=\frac{a+c}{b}=\frac{1+\sqrt{5}}{2} \tag{3}$$

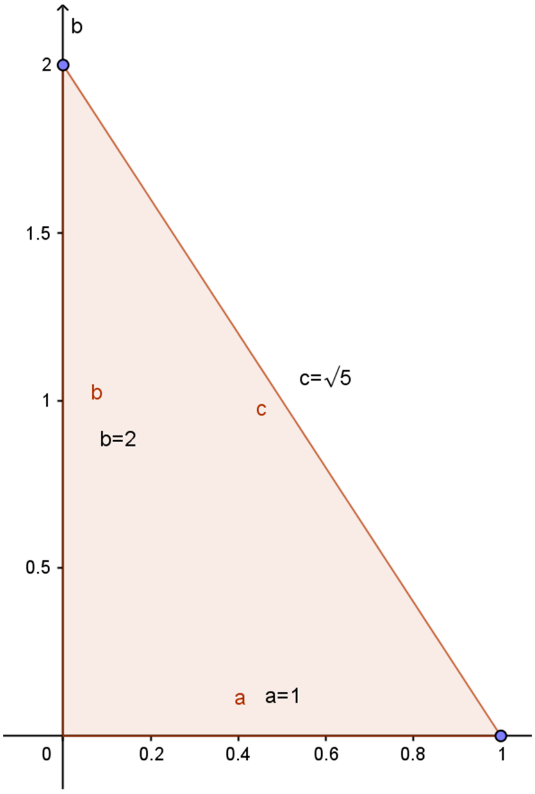

Figure 2. Right-angled triangle representation of the golden ratio.

The sides of a right-angled triangle can be expressed in terms of a, as shown below:

$$b = 2a,\ c = \sqrt{a^2 + b^2} = \sqrt{a^2 + 4a^2} = \sqrt{5a^2} = a\sqrt{5}$$

$$\varphi = \frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2} \tag{4}$$

Consider the following four propositions as shown in Figure 3:

(1) $c^2 = a^2 + (2a-1)^2 = 5a^2 - 4a + 1$
(2) $c^2 = a^2 + (2a+1)^2 = 5a^2 + 4a + 1$
(3) $c^2 = (a+1)^2 + (2a)^2 = 5a^2 + 2a + 1$
(4) $c^2 = (a-1)^2 + (2a)^2 = 5a^2 - 2a + 1$

We observe that proposition (2) given above increases more rapidly than that of the other three propositions because of the $+4a$ term.

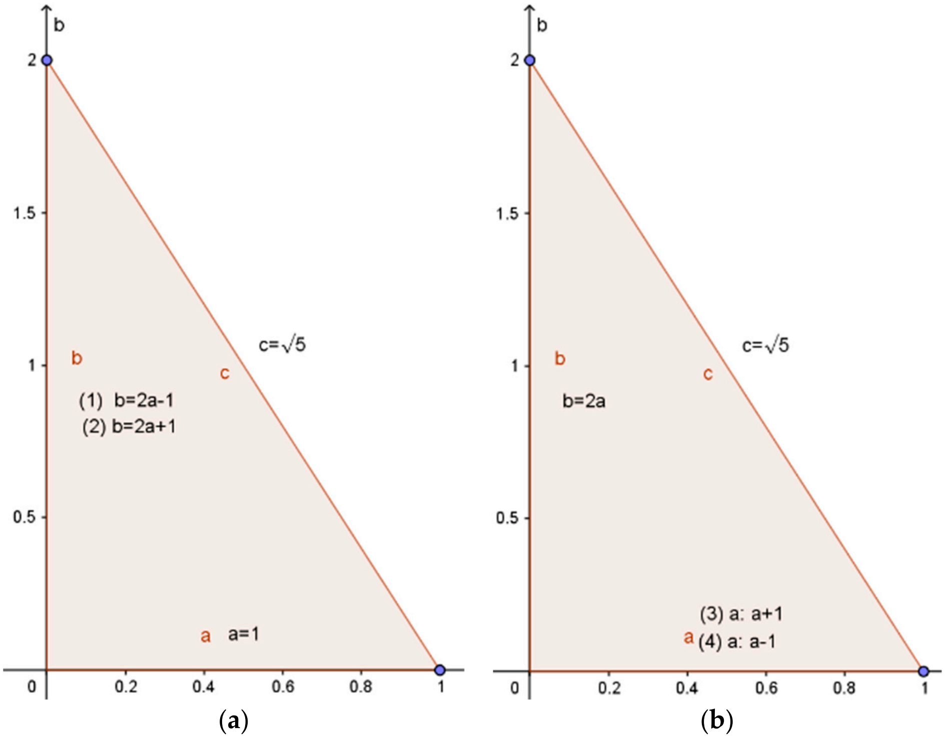

Figure 3. The triangle forms of the golden ratio: (**a**) $b = 2a - 1$; (**b**) $b = 2a$.

Let us now express the sides of the triangle as $\lim\limits_{a\to\infty}$, and we get:

$$a = a,\ b = \lim_{a\to\infty} 2a + 1 = 2a,$$
$$c = \lim_{a\to\infty} \sqrt{5a^2 + 4a + 1} = a\sqrt{5}$$

From previous work [31,32], it can be shown that the sides (a, b, c) can be expressed as three Diophantine equations (an equation that allows only integer solutions) in terms of (m, n) :

$$P(a, b, c) = P(m, n)$$

where

$$a = 2n^2 + 2n(2m-1) \tag{5}$$

$$b = 2n(2m-1) + (2m-1)^2 \tag{6}$$

$$c = 2n^2 + 2n(2m-1) + (2m-1)^2 \tag{7}$$

It is worth noting the special condition that we had specified in proposition (2): $b = 2a + 1$. By substituting this in the above Equations (5) and (6), and by bringing a and b in terms of m and n, we get:

$$2n(2m-1) + (2m-1)^2 = 2\left[2n^2 + 2n(2m-1)\right] + 1$$

This gives us the special condition, a Diophantine equation, given below:

$$4n^2 + 2n(2m-1) - (2m-1)^2 + 1 = 0 \tag{8}$$

Solving this Diophantine Equation (8) given above, we get $m = 7, n = 4$.

By substituting $P(m,\ n) = P(7,\ 4)$ into Equations (5)–(7), we derive $\Rightarrow P(a, b, c) = (136,\ 273,\ 305)$.

Next, substituting $P(a,\ b,\ c) = (136,\ 273,\ 305)$ into Equation (3), we get:

$$\varphi = \frac{a+c}{b} = \frac{136+305}{273} = \frac{441}{273} = \frac{21}{13} \approx 1.61$$

It is noted that the numbers in the quotients above, namely 13 and 21, are both sequential Fibonacci numbers. It is well known that the golden ratio can be expressed as the ratio of two sequential Fibonacci sequence numbers. A brief explanation and simple proof are given in the next section.

3.3. The Golden Ratio and Fibonacci Sequence

We establish the second property of the golden ratio by expressing it as a ratio of the terms in the Fibonacci sequence. The Fibonacci sequence is an infinite series of integers, where each term is the sum of the two previous terms [20,33]. It is defined by the following mathematical function:

$$F(i) = F(i-1) + F(i-2) \text{ with } F(0) = 0 \text{ and } F(1) = 1$$

i	0	1	2	3	4	5	6	7	8	9	10	11
F_i	0	1	1	2	3	5	8	13	21	34	55	89

As i takes large values when we go farther and farther to the right of the Fibonacci sequence, the ratio of a term to the one before it will be approximately equal to the golden ratio.

The golden ratio as defined earlier is given by:

$$\varphi = \frac{1}{\varphi - 1} = \frac{1+\sqrt{5}}{2} = 1.618$$

$$\varphi = \lim_{i \to \infty} \frac{F_{i+1}}{F_i} \Rightarrow \frac{F_{11}}{F_{10}} = \frac{89}{55} \approx 1.618 \tag{9}$$

The golden ratio as a ratio of the Fibonacci number sequence can be pictorially visualized as the golden rectangle, as shown in Figure 4. We start with a square and, by placing another square of the same size adjacent to it, we can form a new rectangle. As we continue to place adjacent squares, the longer side of the rectangle formed will always be a successive Fibonacci number. The larger rectangle formed becomes a golden rectangle, as shown in Figure 4.

In this section, we have shown that for higher terms in the Fibonacci sequence, i.e., when we go farther and farther to the right of the Fibonacci sequence, the ratio of a term (n) to the one before it ($n-1$) approximates to the golden ratio. Since the Fibonacci sequence is an infinite series of numbers, the time/space complexity grows with larger terms and varies according to various implementations already reported in literature [34]. Some implementations have the space/time complexity to have exponential dependence on n. Certain others, using the constant-time arithmetic, have the space/time complexity to be O(n). These analytical proofs assume infinite precision. However, from the software-based computational aspects, there are limitations on the precision due to hardware or software constraints and this has a major impact on the space/time complexity. Hence, our purpose in this paper is not to provide an analytical proof in general. Rather, the purpose of our paper is to propose the golden ratio using Diophantine equations for its use in cryptographic software solutions. In this context, we compare its space/time complexity to the commonly used Fibonacci sequence method experimentally up to a certain computing precision that is feasible and applicable for secure cryptography. We make use of a few more properties of the golden ratio as described below before we provide our proposed method to compute the golden ratio in Section 4 and the experimental comparison results of our experiments in Section 5.

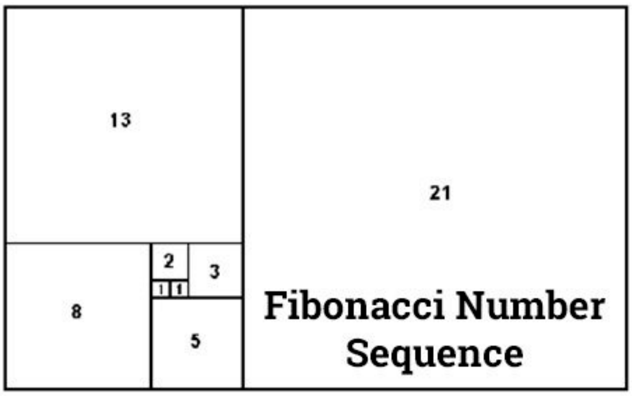

Figure 4. Representation of the golden ratio as the Fibonacci sequence.

3.4. The Golden Ratio as a Ratio in Terms of (m, n) : $\varphi(m, n)$

Having established the basic forms of the golden ratio, we are now in a position to explore some more advanced properties, which lay the foundation of our proposed new method for computing the Golden Ratio. In Section 3.2, we solved the special condition Equation (8):

$$4n^2 + 2n(2m-1) - (2m-1)^2 + 1 = 0$$

Let us now express a general equation for φ in terms of $m, n : \varphi(m, n)$ from Equation (3):

$$\varphi = \frac{a+c}{b}$$

Equations (5)–(7) become as follows:

$$a = 2n^2 + 2n(2m-1),\ b = 2n(2m-1) + (2m-1)^2$$
$$c = 2n^2 + 2n(2m-1) + (2m-1)^2$$

Substituting these into Equation (3), we get

$$\begin{aligned} \varphi = \tfrac{a+c}{b} &= \tfrac{4n^2+4n(2m-1)+(2m-1)^2}{2n(2m-1)+(2m-1)^2} \\ &= \tfrac{4n^2+2n(2m-1)+2n(2m-1)+(2m-1)^2}{2n(2m-1)+(2m-1)^2} \\ &= \tfrac{4n^2+2n(2m-1)}{2n(2m-1)+(2m-1)^2} + 1 \\ &= \tfrac{(2n)(2n)+2n(2m-1)}{2n(2m-1)+(2m-1)^2} + 1 \\ &= \tfrac{2n(2n+2m-1)}{(2m-1)(2n+2m-1)} + 1 \\ \varphi &= \tfrac{2n}{2m-1} + 1 \end{aligned}$$

From Equation (1):

$$\varphi = \frac{1}{\varphi - 1} \Rightarrow \frac{1}{\varphi} = \varphi - 1 = \frac{2n}{2m-1}$$

$$\varphi = \frac{2m-1}{2n} \tag{10}$$

We note the following:

$$\lim_{m \to \infty} 2m - 1 = 2m$$

$$\varphi = \frac{m}{n} \tag{11}$$

It should be noted that, for the special condition in Equation (8), there are multiple solutions.

3.5. The Golden Ratio and the Infinite Series for (m:n)

We establish another advanced property of the golden ratio by deriving the infinite series for m, n so that any resolution for $\varphi(m,n)$ can now be arrived at. We had previously solved the special condition Equation (8) given below:

$$4n^2 + 2n(2m-1) - (2m-1)^2 + 1 = 0$$

Next, we derive the general expression for n in terms of m:

$$\begin{array}{c} 4n^2 + 2n(2m-1) - (2m-1)^2 + 1 = 0 \\ n^2 + \frac{n(2m-1)}{2} = \frac{(2m-1)^2-1}{4} \\ \Rightarrow n^2 + \frac{n(2m-1)}{2} + \frac{(2m-1)^2}{16} = \frac{(2m-1)^2}{16} + \frac{(2m-1)^2-1}{4} \\ \left(n + \frac{2m-1}{4}\right)^2 = \frac{(2m-1)^2}{16} + \frac{(2m-1)^2-1}{4} \Rightarrow \\ n + \frac{2m-1}{4} = \sqrt{\frac{(2m-1)^2}{16} + \frac{(2m-1)^2-1}{4}} \Rightarrow \\ n = \sqrt{\frac{(2m-1)^2}{16} + \frac{(2m-1)^2-1}{4}} - \frac{2m-1}{4} \Rightarrow \end{array}$$

$$n = \frac{\sqrt{20m^2 - 20m + 1} - 2m + 1}{4} \tag{12}$$

The above set of mathematical derivations lead us towards the proposal of our new efficient golden ratio method with infinite precision.

4. Proposed Method for Golden Ratio Computations

We propose a new method to solve the Diophantine Equation (8)—$4n^2 + 2n(2m-1) - (2m-1)^2 + 1 = 0$—by finding solutions to Equation (12) for values of m which provide integer values of n. The results of these solutions are shown in Table 1. The first two values of i_1 and i_2 determine the series.

Table 1. Recursive solutions to the Diophantine equations.

i	1	2	3	4	5	6
m	7	117	2,091	37,513	673,135	12,078,909
n	4	72	1,292	23,184	416,020	746,5176

Now, using Equation (10), we get:

$$\begin{array}{l} \varphi(6) = \frac{2m_6-1}{2n_6} = \frac{2(12{,}078{,}909)-1}{2(7{,}465{,}176)} = 1.618033988749894 \mid 08 \\ Actual\ \varphi = 1.618033988749894848204\ldots \end{array}$$

From Table 1, the following infinite series for m, n can now be derived.

$$m_i = 18m_{i-1} - m_{i-2} - 8 \tag{13}$$

$$n_i = 18n_{i-1} - n_{i-2} \tag{14}$$

From the above Equations (13) and (14), given that the 5th and 6th values are known, we determine the 7th value, $i = 7$ as follows:

$$\begin{gathered} m_7 = 18(12,078,909) - 673,135 - 8 = 216,747,219 \\ n_7 = 18(7,465,176) - 416,020 = 133,957,148 \\ \varphi(7) = \frac{2m_7-1}{2n_7} = \frac{2(216,747,219)-1}{2(133,957,148)} \\ = 1.61803398874989485 \mid 4,435. \end{gathered}$$

From the above, we can easily see that there is an improvement of two places between the values of $\varphi(6)$ and $\varphi(7)$. The accuracy of $\varphi(8)$ is 19 places, as derived below:

$$\begin{gathered} m_8 = 18(216,747,219) - 12,078,909 - 8 = 3,889,371,025 \\ n_8 = 18(133,957,148) - 7,465,176 = 2,403,763,488 \\ \varphi(8) = \frac{2m_8-1}{2n_8} = \frac{2(3,889,371,025)-1}{2(2,403,763,488)} \\ = 1.6180339887498948482 \mid 2 \end{gathered}$$

5. Results

We demonstrate the efficiency of our proposed method for determining the golden ratio by performing experiments to compare our proposed method with the commonly used Fibonacci sequence method.

We consider Equation (9): $\varphi = \lim\limits_{n\to\infty} \frac{F_{i+1}}{F_i}$ and Equation (10): $\varphi = \frac{2m-1}{2n}$. We can make the following observations:

$$F_{i+1} = 2m - 1 \text{ and } F_i = 2n$$

Consider $m_8 = 3,889,371,025,\ n_8 = 2,403,763,488$

$$\begin{gathered} F_{48} = 2n_8 = 2(2,403,763,488) = 4,807,526,976 \\ F_{49} = 2m_8 - 1 = 2(3,889,371,025) - 1 = 7,778,742,049 \end{gathered}$$

Hence, to calculate φ to 19 decimal places requires 49 Fibonacci loops, which are essentially additions and one division.

Solving the Diophantine Equation (12) is tedious. However, once the first two values of the each of the sequences m_i and n_i are known, the series Equations (13) and (14) very quickly determine the desired values for m_i and n_i. Doubling these and one subtraction elegantly places values in the Fibonacci sequence. We revise Table 1 to include the number of computations performed in our proposed method to calculate the golden ratio using Diophantine equations as compared to Fibonacci sequence method. These comparisons are summarized in Table 2.

Table 2. Comparison of the proposed method vs. Fibonacci sequence method.

i	1	2	3	4	5	6	7	8
m	7	117	2,091	37,513	673,135	12,078,909	216,747,219	3,889,371,025
n	4	72	1,292	23,184	416,020	7,465,176	133,957,148	2,403,763,488
$2m-1$	13	233	4,181	75,025	1,346,269	24,157,817	433,494,437	7,778,742,049
F_i	7	13	19	25	31	37	43	49
$2n$	8	144	2,584	46,368	832,040	14,930,352	267,914,296	4,807,526,976
F_{i-1}	6	12	18	24	30	36	42	48

From Table 2, it can be observed that once our initial m_i and n_i are known, each succeeding value for each sequence requires a multiplication (×18) and a subtraction of the previous sequence value, and for m_i, a minor subtraction of a constant (8). This essentially results in four operations versus six additions in the Fibonacci sequence to obtain the same value. Equations (9)–(11) require a division. Now, we reconsider the following equations:

$$\varphi = \lim_{i\to\infty}\frac{F_{i+1}}{F_i}\ (9) \quad \varphi = \frac{2m-1}{2n}\ (10) \quad \varphi = \frac{m}{n}\ (11)$$

Let us now consider eight iterations of our new method, which is essentially 32 operations. We compare our proposed method and Fibonacci sequence method of computations for the golden ratio by considering 32 operations in each method.

$$\varphi = \frac{F_{32}}{F_{31}} = \frac{2{,}178{,}309}{1{,}346{,}269} = 1.6180339887496$$
$$\varphi = \frac{m_8}{n_8} = \frac{3{,}889{,}371{,}025}{2{,}403{,}763{,}488} = 1.618034$$

If we allow three addition calculations, we get:

$$\varphi = \frac{F_{35}}{F_{34}} = \frac{9{,}227{,}465}{5{,}702{,}887}$$
$$= 1.6180339887499 \text{ (13 decimal places)}$$
$$\varphi = \frac{2m_8-1}{2n_8} = \frac{2(3{,}889{,}371{,}025)-1}{2(2{,}403{,}763{,}488)} = \frac{7{,}778{,}742{,}049}{4{,}807{,}526{,}976}$$
$$= 1.6180339887498948482 \text{ (18 decimal places)}$$

This would require 49 cycles in the Fibonacci sequence method to obtain the same accuracy.

Overall, it is observed that 35 calculations of our new proposed method provide the golden ratio with an accuracy to 19 decimal places, while 35 calculations of the Fibonacci sequence method provide the golden ratio with only 13 decimal places of accuracy. In other words, 49 calculations in the Fibonacci sequence method are required to arrive at the same level of accuracy as the proposed new method. We note that Equation (10) provides a much better result than Equation (11) with very little performance penalty.

Next, let us consider 48 operations + 3 addition calculations, totaling 51 operations altogether.

$$\varphi = \frac{F_{51}}{F_{50}} = \frac{20{,}365{,}011{,}074}{12{,}586{,}269{,}025}$$
$$= 1.61803398874989484820 \text{ (20 decimal places)}$$
$$\varphi = \frac{2m_{12}-1}{2n_{12}}$$
$$= \frac{2(403{,}257{,}766{,}524{,}697)-1}{2(249{,}227{,}005{,}939{,}632)} = \frac{806{,}515{,}533{,}049{,}393}{498{,}454{,}011{,}879{,}264}$$
$$= 1.61803398874989484820458683436 7 \text{ (29 decimal places)}$$
$$\varphi = 1.6180339887498948482045868343 65$$

These results clearly indicate the trend that with more iterations performed, our new method far outperforms that of Fibonacci sequence method in terms of precision for the same number of arithmetic operations. Hence, the computations of our proposed method for the golden ratio are much faster than the existing well-known methods using the Fibonacci sequence, meeting the need of faster cryptosystems with high precisions.

6. Conclusions and Future Work

In this paper, we presented an efficient method to compute the golden ratio, which has wide applications in secret key generations and in secure cryptographic applications. While simple to very complex cipher-based cryptography are available, these methods have failed to counter the rising security attacks due to the lack of speed in their computations. More recently a new cryptography called golden cryptography is studied, where golden ratio computations are used. Compared with previous methods where the well-known Fibonacci sequence method is used to compute the golden ratio, our proposed method adopts the advanced properties of applying the Diophantine equations in the computations. Firstly, we established these properties and the proposed method mathematically. Then, we experimentally computed the golden ratio using the proposed method with infinite precision. Finally, we evaluated our method by comparing the computational results with the well-known Fibonacci sequence method. We established the efficiency of our proposed golden ratio method in terms of both speed of calculation and precision.

This research has applications in faster cryptographic algorithms, and future work would study their impact in preventing security attacks. It would be of interest to explore how our faster method for golden ratio computations would facilitate cryptographic protection by establishing efficient secret keys for the timely combating of any possible information security penetration.

Author Contributions: A.O. devised the mathematical models and derivations and performed the comparison of results. S.V. contributed in directing the research application, benchmarking and the writing of the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
2. Rivest, R.L. Cryptography. In *Handbook of Theoretical Computer Science*; van Leeuwen, J., Ed.; Elsevier: New York, NY, USA, 1990.
3. Archer, D.W.; Bogdanov, D.; Pinkas, B.; Pullonen, P. Maturity and Performance of Programmable Secure Computation. *IEEE Secur. Priv.* **2016**, *14*, 48–56. [CrossRef]
4. Wall, D.S. Crime, Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3005872 (accessed on 17 September 2018).
5. Venkatraman, S. Autonomic Framework for IT Security Governance. *Int. J. Manag. Inf. Tech.* **2017**, *9*, 1–14. [CrossRef]
6. Menezes, A.J.; Oorschot, P.C.V.; Vanstone, S.A. *Handbook of Applied Cryptography*, 5th ed.; CRC Press: Boca Raton, FL, USA, 2001.
7. Buchmann, J. *Introduction to Cryptography*, 2nd ed.; Springer: Berlin, Germany, 2005.
8. Kelly, S.; Frankel, S. Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec. Available online: https://www.rfc-editor.org/info/rfc4868 (accessed on 17 September 2018).
9. Sudha, K.R.; Sekhar, A.C.; Reddy, P.V.G.D. Cryptography protection of digital signals using some recurrence relations. *Int. J. Comput. Sci. Netw. Secur.* **2007**, *7*, 203–207.
10. Koblitz, N. Elliptic curve cryptosystems. *Math. Comput.* **1987**, *48*, 203–209. [CrossRef]
11. Mohamed, M.H.; Abul-Kasim, I.H. Data Hiding by LSB Substitution using Gene Expression Programming. *Int. J. Comput. Appl.* **2012**, *45*, 13–20.
12. Jozsef, C. The Golden Ratio. *J. Mod. Phys.* **2016**, *7*, 1944–1948. [CrossRef]
13. Stakhov, A.P. The golden matrices and a new kind of cryptography. *Chaos Solitons Fractals* **2007**, *32*, 1138–1146. [CrossRef]
14. Rey, A.M.; Sanchez, G.R. On the Security of Golden Cryptography. *Int. J. Netw. Secur.* **2008**, *7*, 448–450.

15. Miller, V. Use of elliptic curves in cryptography. In Proceedings of the CRYPTO '85, Santa Barbara, CA, USA, 18–22 August 1985; pp. 417–426.
16. Tahghighi, M.; Turaev, S.; Jaafar, A.; Mahmod, R.; Said, M.M. On the Security of Golden Cryptosystems. *Int. J. Contemp. Math Sci.* **2012**, *7*, 327–335.
17. Kocher, P.; Jaffe, J.; Jun, B. Differential Power Analysis. In Proceedings of the CRYPTO '99, Santa Barbara, CA, USA, 15–19 August 1999.
18. Kamm, L.; Willemson, J. Secure floating point arithmetic and private satellite collision analysis. *Int. J. Inf. Secur.* **2015**, *14*, 531–548. [CrossRef]
19. Falcon, S.; Plaza, A. On the Fibonacci k-number. *Chaos Solitons Fractals* **2007**, *32*, 1615–1624. [CrossRef]
20. Johnson, R.C. Fibonacci Numbers and Matrices. Available online: http://maths.dur.ac.uk/~dma0rcj/PED/fib.pdf (accessed on 17 September 2018).
21. Falcon, S.; Plaza, A. The k-Fibonacci hyperbolic functions. *Chaos Solitons Fractals* **2008**, *38*, 409–420. [CrossRef]
22. Falcon, S.; Plaza, A. The k-Fibonacci sequence and the Pascal 2-triangle. *Chaos Solitons Fractals* **2007**, *33*, 38–49. [CrossRef]
23. De Castro, A. Quantum one-way permutation over the finite field of two elements. *Quantum Inf. Process.* **2017**, *16*, 149. [CrossRef]
24. Abiyev, A.A.; Abiyev, A. The simple recurrent formulas to find a sequences of numbers satisfying equation x2+(x+1)2=z2 and the properties of these integers. *Math. Comput. Appl.* **2003**, *8*, 173–180.
25. Levin, L.A. The tale of one-way functions. *Problems of Information Transm.* **2003**, *39*, 92–103. [CrossRef]
26. Euclid. *The Thirteen Books of Euclid's Elements. Translated with Introduction and Commentary by Sir Thomas L. Heath*, 2nd ed.; Dover Publications: New York, NY, USA, 1956.
27. Mohamed, M.H.; Mahdy, Y.B.; Shaban, W.A.E. Confidential Algorithm for Golden Cryptography Using Haar Wavelet. *Int. J. Comput. Sci. Inf. Secur.* **2014**, *12*, 1–9.
28. Kerik, L.; Laud, P.; Randmets, J. Optimizing MPC for robust and scalable integer and floating-point arithmetic. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 22–26 February 2016.
29. Overmars, A.; Venkatraman, S. A New Method of Golden Ratio Computation for Faster Cryptosystems. In Proceedings of the IEEE Conference on Cybersecurity and Cyberforensics, London, UK, 21–23 November 2017.
30. Overmars, A.; Venkatraman, S.; Parvin, S. Revisiting Square Roots with a Fast Estimator. *Lond. J. Res. Comput. Sci. Tech.* **2018**, *18*, 1–7.
31. Overmars, A.; Ntogramatzidis, L. A new parameterisation of Pythagorean triples in terms of odd and even series. *arXiv*, 2015; arXiv:1504.03163.
32. Overmars, A.; Venkatraman, S. Pythagorean-platonic lattice method for finding all co-prime right angle triangles. *Int. J. Comput. Inf. Eng.* **2017**, *4*, 1–4.
33. Falcon, S.; Plaza, A. *k*-Fibonacci sequence modulo *m*. *Chaos Solitons Fractals* **2009**, *41*, 497–504. [CrossRef]
34. Dasdan, A. Twelve simple algorithms to compute Fibonacci numbers. *arXiv* **2018**, arXiv:1803.07199.