ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 2 - 2026

Optimization practice of continuous fraction representation in high-precision numerical computation

Zhiheng Zhang[1,*]

[1] Department of Basic Courses, Zhengzhou Vocational College of Finance and Taxation, Zhengzhou, Henan, 450048, China

SUMMARY: *This study analyzes the application of the concatenated fractional representation in high-precision numerical computation, and concentrates on its role in cryptanalysis for deciphering, such as deciphering the Okamoto regime, deciphering the Throwfan Tou public key regime, and deciphering the RSA regime with a short decryption index. On this basis, an attack algorithm based on the Legendre's theorem of continuous fractional approximation is proposed. The experimental platform is built for simulation and analysis, and it is found that the attack result of this RSA attack algorithm is consistent with the set 512bit key, which realizes the successful attack on the key of RSA algorithm. Moreover, the concatenated score RSA attack algorithm has good time computation efficiency and small communication cost, and its total time consumed for preprocessing, authentication, and server for 1GB file is within 51%, 64%, and 51% of the comparison methods, respectively, and the average value of communication cost is within 88% of the comparison methods. The results show that the proposed concatenated fractional attack algorithm is effective for RSA, which makes the complexity of the RSA attack greatly reduced and improves the execution efficiency of RSA deciphering.*

KEYWORDS: *continuous fraction representation; RSA attack; Wiener algorithm; cryptanalysis*

1 Introduction

Many practical problems, such as the flow field often have surge, vortex and separation phenomena, and meteorology, oceanography, oil exploration, electromagnetism, hydrodynamics, weather forecasting, aerospace, etc., their numerical solutions are prone to large gradients, large deformation and various types of interruptions, it is difficult to avoid non-physical oscillation phenomena, which need to be solved with the help of high-precision numerical computation methods [1-5]. Therefore, how to design stable, effective, high-precision, high-resolution numerical methods is increasingly being emphasized by researchers and scholars, and a variety of high-precision numerical computation methods have emerged in large numbers.

Zou et al [6] designed a high-precision numerical calculation method for the solar radiation pressure force of pleated solar sails by means of the fold analysis method and the micro-element stress restoring force calculation method, which can cope with the analysis of solar sails with complex boundary conditions. Han et al [7] implanted a form of energy equation into Open FOAM with the help of volume-based method to form a high-precision

*13703937813@163.com
https://doi.org/10.65102/is2026654
Published: 30 April, 2026

computational solver, which is used to reduce the grid size of heat transfer in oil-water displacement process, reduce the computational cost, and improve the computational accuracy. Van Houcke et al [8] used a deterministic graphical Monte Carlo algorithm in order to solve the high-precision numerical solution of the Fermi polarizable subproblem and its large-order behavior of the graphical hierarchy making the computational accuracy unprecedented. Chakraborty et al [9] proposed a highly accurate numerical computation of principal points of univariate distributions by calculating the principal points and error quantization for integer n and introducing Newton's method to compute all the principal points for integer n. Han et al [10] incorporated a high-precision numerical method with low computational complexity into the Gray-Scott model, utilizing the Runge Kutta method and the Fourier Transform for spatio-temporal discretization and Richter extrapolation for error reduction. Mora et al [11] constructed a new model for representing rational numbers using fractional place value representation and periodic encoding behavior, the model is able to guarantee that there is no loss of accuracy in the representation of numbers and achieve more complex and high precision computations. Xue and Bai [12] pointed out that in fractional-order calculus, high-precision numerical solution requires increasing the order O(h) level of the algorithm, and its numerical computation error decreases with decreasing the value of h and increasing the order. LEITOLD et al. [13] proposed a toolbox called “MATLAB” to realize high-precision numerical computation in a multi-progress computing environment, using floating-point operations for numerical representation beyond the standard double-precision format.

With the in-depth development of aerospace, financial analysis, cryptography, scientific computing, quantum computing and other fields, the high-precision numerical computation puts forward the demand for higher accuracy, efficiency, stability and real-time performance [14-16]. And the connected fraction is a mathematical concept used to accurately represent the numerical value of a real number. It consists of an integer part and an infinite sequence of fractional parts, each of which is an integer divided by a positive integer [17]. The concatenated fraction representation is a special form of fractions that has important applications in number theory, approximation theory, and other areas of mathematics, providing a new paradigm for high-precision numerical computation [18-20]. Duverney and Shiokawa [21] confirmed the validity of an irrational exponential formula for semiconventional connected fractions that satisfies certain conditions and provided an application case for the exact computation of semiconventional connected fraction irrationals. Hingu et al. [22] combined connected fraction and polynomial approximation methods for optimizing a neural activation function in an artificial intelligence/machine learning workload, and the results showed that the optimized function can maintain high accuracy while reducing power consumption and computation time.

The study firstly realizes to introduce the basic knowledge of the concatenated fraction, and based on its application in high-precision numerical computation, discusses its deciphering application to the Okamoto system, the public key system of the Throwing Fantom system, and the RSA system of the short decryption exponent, and so on. Then for the problem of RSA encryption algorithm attack, an attack algorithm based on continuous fraction approximation Legendre's theorem is proposed, which is optimized on the basis of Wiener's algorithm, and adopts real quadratic irrational number approximation to weaken the restriction condition of Wiener's algorithm on small decryption exponent of RSA encryption algorithm. Use PC, card reader and oscilloscope to build an experimental platform, set 512bit key, and utilize the even fraction RSA attack algorithm to simulate the experiment. Then two comparison methods are selected to compare the changes of computation time and communication cost of each algorithm with the growth of file size, to explore the

computational efficiency and communication complexity of the even-fractional RSA attack algorithm. The proposed RSA attack algorithm can be used to recover the decryption key to obtain the plaintext information, which not only optimizes the original scheme efficiently, but also provides a basic cryptanalysis tool for analyzing the security of RSA cryptosystem.

2 Preparatory knowledge

2.1 Basic Concepts of Continuous Fractions

The simplest connected fractions have the following spread:

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\cdots}}} \tag{1}$$

In general, $a_0,a_1,a_2,a_3,\cdots,a_n,\cdots$ denote mutually independent variables. Depending on the specific application, the domain of definition of these variables can be any set of numbers, so it can be assumed that these $a_0,a_1,a_2,a_3,\cdots,a_n,\cdots$ are real numbers, complex numbers or functions, etc. In the applications that follow, assume that $a_i\ (i>0)$ is always positive and that a_0 is any real number, and refer to these numbers as the partial quotient of the concatenated fraction. There are either only finitely many partial quotients or infinitely many partial quotients; when there are only finitely many partial quotients, the corresponding connected fraction is called a finite connected fraction, e.g., (1), otherwise, it becomes an infinite connected fraction, e.g.,:

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\cdots+a_n}}} \tag{2}$$

For simplicity of notation, denote the finite continuous fraction as:

$$[a_0;a_1,a_2,\cdots,a_n] \tag{3}$$

The infinite concatenated score is denoted as:

$$[a_0;a_1,a_2,\cdots] \tag{4}$$

Thus, by calling $r_k=[a_k,a_{k+1},a_{k+2},\cdots,a_n]$ the remainder of a finitely connected fraction and $r_k=[a_k,a_{k+1},a_{k+2},\cdots]$ the remainder of an infinitely connected fraction, it is clear that the remainder of an infinitely connected fraction is an infinitely connected fraction and the remainder of a finitely connected fraction is a finitely connected fraction, and that there is a relation (5) for finitely connected fractions, and similarly, there is a relation (6) for infinitely connected fractions:

$$[a_0;a_1,a_2,\cdots,a_n]=[a_0;a_1,a_2,\cdots,a_{k-1},r_k],\left(0\le k\le n\right) \tag{5}$$

$$[a_0;a_1,a_2,\cdots]=[a_0;a_1,a_2,\cdots,a_{k-1},r_k]\left(k\ge 0\right) \tag{6}$$

For infinitely connected fractions, r_k on the right-hand side of the equation is undefined for a definite value, so it has only a formal meaning. Also, call $s_k=[a_1,a_2,a_3,\cdots,a_k]$ the k -order approximation factor for the connected fractions.

2.2 Convergence factors for continuous fractions

For each finite connected fraction $[a_0;a_1,a_2,\cdots,a_n]$, which is the result of a finite number of rational operations performed on the partial quotient, and is also a rational function of the partial quotient, it can be written as $\frac{P(a_0,a_1,a_2,\cdots,a_n)}{Q(a_0,a_1,a_2,\cdots,a_n)}$, where $P(a_0,a_1,a_2,\cdots,a_n)$, $Q(a_0,a_1,a_2,\cdots,a_n)$ are the values of the quotient about $a_0,a_1,a_2,\cdots,a_n$ polynomials with integer coefficients.

Therefore, denote the approximation factor $s_k=[a_1,a_2,a_3,\cdots,a_k]$ of a connected fraction θ as $\frac{p_k}{q_k}$ and call it the k -order convergence factor of the connected fraction α. Obviously, there are infinite convergence factors for infinite connected fractions and $k+1$ convergence factors for finite connected fractions (of order $0,1,2,\cdots,k$) and $\theta=\frac{p_k}{q_k}$, and the following conclusions are drawn about the convergence factors of connected fractions.

Theorem 1: For any $k(k\ge 0)$, there are:

$$p_k=a_kp_{k-1}+p_{k-2};\ q_k=a_kq_{k-1}+q_{k-2} \tag{7}$$

where $p_{-1}=1$, $p_0=a_0$, $q_{-1}=0$, and $q_0=1$.

Theorem 2: For any $k(k\ge 0)$, there are:

$$q_kp_{k-1}-p_kq_{k-1}=(-1)^k \tag{8}$$

Corollary: for any $k(k\ge 1)$, there is:

$$\frac{p_{k-1}}{q_{k-1}}-\frac{p_k}{q_k}=\frac{(-1)^k}{q_kq_{k-1}} \tag{9}$$

Theorem 3: For any $k(k\ge 1)$, there is:

$$q_kp_{k-2}-p_kq_{k-2}=(-1)^{k-1}a_k \tag{10}$$

Corollary: for any $k(k\ge 2)$, there is:

$$\frac{p_{k-2}}{q_{k-2}} - \frac{p_k}{q_k} = \frac{(-1)^{k-1} a_k}{q_k q_{k-2}} \tag{11}$$

Theorem 4: The convergence factors of even orders form an increasing series, the convergence factors of odd orders form a decreasing series, and the value of the convergence factor of each even order is less than the value of the convergence factor of any odd order.

Theorem 5: For any $k(1 \le k \le n)$, there are:

$$[a_0; a_1, a_2, \cdots, a_n] = \frac{p_{k-1} r_k + p_{k-2}}{q_{k-1} r_k + q_{k-2}} \tag{12}$$

Theorem 6: For any $k(k \ge 1)$, there is:

$$\frac{q_k}{q_{k-1}} = [a_k; a_{k-1}, \cdots, a_1] \tag{13}$$

2.3 Optimal Approximation of Continuous Fractions

Definition 1: Let θ be a real number and $\frac{a}{b}$ a rational fraction, if for any $\frac{c}{d}(0 < d \le b, \frac{c}{d} \ne \frac{a}{b})$, one can derive $\left|\theta - \frac{c}{d}\right| > \left|\theta - \frac{a}{b}\right|$, then we call $\frac{a}{b}$ the best approximation of θ.

Theorem 6: Every best approximation of θ is either a convergence factor of θ or an intermediate partition of θ.

Definition 2: Let θ be a real number and $\frac{a}{b}$ a rational manifold, if for any $\frac{c}{d}(0 < d \le b, \frac{c}{d} \ne \frac{a}{b})$, one can derive $|d\theta - c| > |b\theta - a|$, then we call $\frac{a}{b}$ the second-order best approximation of θ.

Theorem 7: Every second-order best approximation is a convergence factor.

Theorem 8: Every irreducible partition $\frac{a}{b}$ that satisfies inequality $\left|\theta - \frac{a}{b}\right| < \frac{1}{2b^2}$ is $\frac{a}{b}$ a convergence factor of θ.

PROOF: By Theorem 7, it is sufficient to show that $\frac{a}{b}$ is a second-order best approximation of θ.

Let $|d\theta - c| \le |b\theta - a| \le \frac{1}{2b}(d > 0, \frac{c}{d} \ne \frac{a}{b})$, then $\left|\theta - \frac{c}{d}\right| < \frac{1}{2bd}$, and hence with the following Inequality:

$$\left|\frac{c}{d} - \frac{a}{b}\right| \le \left|\theta - \frac{c}{d}\right| + \left|\theta - \frac{a}{b}\right| < \frac{1}{2bd} + \frac{1}{2b^2} = \frac{b+d}{2b^2 d} \tag{14}$$

Also by $\frac{c}{d} \neq \frac{a}{b}$, $\left|\frac{c}{d}-\frac{a}{b}\right| \geq \frac{1}{bd}$, so there is $\frac{1}{bd} < \frac{b+d}{2b^2d}$, and thus, $d > b$. This shows that $\frac{a}{b}$ is indeed a second-order best approximation, so the theorem is proved.

2.4 Legendre's Theorem

In addition to the best approximation, another useful conclusion about continuous fractions is the following Legendre's Theorem.

Theorem (Legendre): if there exists a rational number $\frac{n}{m}$ satisfying:

$$\left|\xi-\frac{n}{m}\right| < \frac{1}{2m^2} \tag{15}$$

Then there must exist j such that $\frac{\alpha_j}{\beta_j} = \frac{n}{m}$.

Using the extended Euclidean algorithm one can efficiently compute the concatenated scores of ξ and the two sequences $\{\alpha_j\}$ and $\{\beta_j\}$.

3 Application and optimization of practice in the representation of continuous fractions

3.1 Application to high-precision numerical calculations

The core applications of the concatenated fraction representation in high-precision numerical computation focus on key cracking in cryptanalysis and high-precision parameter extraction in signal processing, and it is a key tool for solving specific engineering problems. In cryptanalysis and cracking, when attacking cryptosystems based on large number decomposition such as RSA or discrete logarithm problems, the concatenated fraction is one of the classic tools for cryptographic attacks as it can approximate and restore the private key from the intercepted partial information. Based on this, this section discusses the application of the concatenated fraction representation in cryptanalysis.

3.1.1 Deciphering the Okamoto system

Public key for the Okamoto system: $n = p^2q, u = a + bpq$.

Key: (p,q,a,b), where p,q are two large prime numbers $p < q$, $0 < a < \sqrt{pq}/2$, $a \in Z_{pq}^*$, $0 < b < p$.

Let the public fraction $\alpha = u/n$ and the secret fraction $\alpha' = b/p, (b,p) = 1$. is not difficult to verify:

$$\left|\alpha-\alpha'\right| = a/(p^2q) < 1/(2p^2) \tag{16}$$

This shows that the asymptotic condition holds. The predicate $B(i)$ can be replaced by

"$q_i = 1$ or $q_i \nmid n$" due to the fact that a nontrivial factor of n is obtained when $q_i = p$. Notice that $q_i \nmid n$ if and only if:

$$n - q_i \cdot \lfloor n / q_i \rfloor \neq 0 \tag{17}$$

So the time $D = O_B(M(|n|))$ to discriminate $B(i)$ and thus the computation time is $O_B(|n| M(|n|))$.

3.1.2 Deciphering the Dupontu public key system

Public key: $m = p^2 q, n = up^2 + v$.

Key: (p, q, u, v), where $p > (1/4)q^{3/2}, (q, up^2 + v) = 1, v < (1/2)p^{1/2}q^{1/4}$.

If $(m, n) = (u, q) = 1$ does not hold, the regime is easily decipherable, so only the scenario $(m, n) = (u, q) = 1$ must be considered. Let the overt fraction $\alpha = n/m$ and the secret fraction $\alpha' = u/q$, then it is not difficult to verify that the asymptotic condition is satisfied. The discriminating predicate $B(i)$ can be replaced by "$q_i = 1$ or $q_i \nmid m$".

3.1.3 The RSA regime for breaking short decryption indices

The RSA system is the most successful public key cryptography system today and has been used in many information security systems. When using the RSA system to establish security mechanisms for information systems, it is common to encounter the problem of confidentiality of communication between users with unbalanced computing power like Smart card and computer, terminal and host, and the nature of the connecting scores gives the method of attacking the RSA system with a short decryption index.

It is well known that the public key of the RSA system consists of $n = pq$ and e, where p, q are two different large prime numbers, and e is the encryption exponent that satisfies $(e, \varphi(n)) = 1$, and usually the bit lengths of p and q are the same or similar. The p, q is kept secret and the decryption index d is determined by $ed \equiv 1 (\mathrm{mod} \varphi(n))$. The RSA system with short decryption index is designed as follows: choose some shorter $d, (d, \varphi(n)) = 1$, the encryption index e is determined by $ed \equiv 1 (\mathrm{mod} \varphi(n))$, and usually e is taken in the range of $0 \sim \varphi(n) - 1$.

From the relationship between the encryption index and the decryption index, we know that there exists an integer k such that $ed = k(p-1)(q-1) + 1$, which establishes that $(k, d) = 1$ and $e/n = (k/d)(1 - \delta)$, where $\delta = (p + q - 1 - 1/k)/n$, that is, $|e/n - k/d| = (k/d)\delta$. Let $\alpha = e/n$ be the open fraction and $\alpha' = k/d$ be the secret fraction, then the asymptotic condition holds if and only if $(k/d)\delta < (2/3) \cdot (1/d^2)$, i.e., if and only if $kd < (2/3) \cdot (1/\delta)$, then $kd < (2/3) \cdot (1//\delta)$ holds if $e < \varphi(n)$, then $k < d$, and thus the asymptotic condition holds when $d < \sqrt{(2/3)(1/\delta)} (\approx O(n^{1/4}))$.

Notice the following set of equations:

$$\begin{cases} (p+q)/2 = (1/2)[-(ed-1)/k + (n+1)] \\ (p-q)/2 = \pm\sqrt{[(p+q)/2]^2 - n^2} \end{cases} \tag{18}$$

It can be seen that p and q are known immediately when $p_i = k, q_i = d$, so the discriminating predicate $B(i)$ can be replaced by the following subroutine:

(1) $x_i := (1/2)\left[-\lfloor (eq_i - 1)/p_i \rfloor + (n+1)\right]$.

$y_i := \left\lfloor \sqrt{x_i^2 - n^2} \right\rfloor, z_i := x + y$.

(2) If $z = 1, n$ or $z \nmid n$, then $B(i)$ is regarded as true, otherwise it is false.

Since division and squaring are of the same order of magnitude as multiplication, the computation time of the previous subroutine:

$$D = O_B(M(|n|)) \tag{19}$$

The computation time to find the short decryption index d is thus $O_B(|n| M(|n|))$.

A more compact form of the RSA regime is one in which the encryption and decryption exponents e and d satisfy a relation:

$$ed \equiv 1 (\text{mod } LCM[p-1, q-1]) \tag{20}$$

That is, there exists an integer K such that $ed = K \cdot \text{LCM}[p-1, q-1] + 1$. Let $G = (p-1, q-1)$, then:

$$ed = (K/G)(p-1)(q-1) + 1 \tag{21}$$

Then let $k = K/(K,G), g = G/(K,G)$, then $k/g = K/G$ and $(k,g) = 1$, and:

$$(k,d) \leqslant (K,d) = 1 \tag{22}$$

This yields $(k, dg) = 1$. It is easy to see that $e/n = (k/(dg))(1-\delta)$, where:

$$\delta = (p + q - 1 - g/k)/n \tag{23}$$

Let the overt fraction $\alpha = e/n$ and the secret fraction $\alpha' = k/(dg)$, then the asymptotic condition holds, if and only if:

$$k\delta/(dg) < (2/3) \cdot (1/(dg))^2 \tag{24}$$

That is, $kdg < (2/3) \cdot (1/\delta)$.

3.2 Optimization of RSA attack algorithm

For the application of the concatenated fractional representation in deciphering the short decryption index RSA regime, an improved concatenated fractional RSA attack algorithm based on Wiener's algorithm is proposed in this section.

3.2.1 Wiener's algorithm

Wiener's algorithm presents the first attack on a private key d, stating that N can be decomposed in polynomial time using the method of concatenated fractions when $d < \frac{1}{3} N^{\frac{1}{4}}$.

The method is described in detail below.

Theorem (Wiener): Let $N = pq$ be an RSA module and $q < p < 2q$, let $d < \frac{1}{3}N^{\frac{1}{4}}$, and given N and the public key index e, which satisfies the RSA equations $ed \equiv 1 \mod \phi(N)$, the RSA equation can be decomposed in polynomial time $(\log N)$ within a polynomial time decomposition of the RSA module N.

Proof: from the RSA equation, there exists an integer k that satisfies:

$$ed = 1 + k\phi(N). \tag{25}$$

Both sides of the equation are obtained by dividing $d\phi(N)$ identically:

$$\frac{e}{\phi(N)} - \frac{k}{d} = \frac{1}{d\phi(N)} \tag{26}$$

That is, $\frac{k}{d}$ is a good approximation of $\frac{e}{\phi(N)}$. $\phi(N)$ is unknown, however, $\phi(N) = (p-1)(q-1) = N + 1 - (p+q)$ and $|N - \phi(N)| < 3N^{\frac{1}{2}}$. Therefore, we want $\frac{k}{d}$ to be a good approximation of the known fraction $\frac{e}{N}$. Then:

$$\begin{aligned} \left|\frac{e}{N} - \frac{k}{d}\right| &= \left|\frac{ed - kN}{dN}\right| = \left|\frac{(ed - k\phi(N)) + k(\phi(N) - N)}{dN}\right| \\ &= \left|\frac{1 - k(N - \phi(N))}{dN}\right| \le \left|\frac{3kN^{\frac{1}{2}}}{dN}\right| = \frac{3k}{dN^{\frac{1}{2}}} \end{aligned} \tag{27}$$

Also since $k\phi(N) < ed, e < \phi(N)$, we get $k < d < \frac{1}{3}N^{\frac{1}{4}}$. Therefore:

$$\left|\frac{e}{N} - \frac{k}{d}\right| \le \frac{3k}{dN^{\frac{1}{2}}} < \frac{1}{dN^{\frac{1}{4}}} < \frac{1}{3d^2} \tag{28}$$

By Legendre's theorem, $\frac{k}{d}$ must be the best asymptotic fraction of the fraction $\frac{e}{N}$. The best asymptotic fraction of $\frac{e}{N}$ can be computed by the extended Euclidean algorithm. The complexity of the extended Euclidean algorithm is $O(\log^3 N)$, and the minimum number of times it needs to be computed $\log N$, so the time complexity of recovering the private key d is $O(\log^4 N)$.

Assuming that d and k are known, $\phi(N)$ can be obtained by the equation $ed = 1 + k\phi(N)$ and then solved:

$$\begin{cases}\phi(N)=N+1-(p+q)\\ N=pq\end{cases} \tag{29}$$

Obtain a decomposition of N.

If d is known and k is unknown, then N can also be decomposed in polynomial time.

Theorem 9: Let $N=pq$ be an RSA module, and assume that e,d satisfy the RSA equation $ed\equiv 1 \mod\phi(N)$, then the RSA module N can be decomposed in probabilistic polynomial time $(\log N)$.

3.2.2 Algorithms for chained-count RSA attacks

Let p,q be prime numbers and $n=pq$ be an RSA module, given n and the encryption index e. There exists a positive integer k that satisfies the RSA equation $ed=k\phi+1$, where $\phi=\phi(n)$ is the Euler function, given by:

$$\begin{aligned}\phi&=(p-1)(q-1)=pq+1-(p+q)\\ &=n+1-(p+q)<n+1-2\sqrt{pq}=n+1-2\sqrt{n}=(\sqrt{n}-1)^2\end{aligned} \tag{30}$$

Let $\phi_1=(\sqrt{n}-1)^2$, get $\phi<\phi_1$, by $ed=k\phi+1<k\phi_1+1$, i.e., $ed-k\phi_1<1$, and dividing both sides by the same amount of $d\phi_1$, get $\frac{e}{\phi_1}-\frac{k}{d}<\frac{1}{d\phi_1}$, and approximating Legendre's theorem by the concatenated fractional approximation, such that $\left|\frac{e}{\phi_1}-\frac{k}{d}\right|<\frac{1}{2d^2}$, we get $\begin{cases}\frac{e}{\phi_1}-\frac{k}{d}<\frac{1}{d\phi_1}<\frac{1}{2d^2},\\ \frac{e}{\phi_1}-\frac{k}{d}>-\frac{1}{2d^2},\end{cases}\begin{cases}d<\frac{\phi_1}{2},\\ k<\frac{ed}{\phi_1}+\frac{1}{2d}=\frac{1+\frac{\phi_1}{2d}}{\Delta\phi},\end{cases}$, where $\Delta\phi=\phi_1-\phi=(\sqrt{p}-\sqrt{q})^2$, satisfies this inequality, and $\frac{k}{d}$ must be a convergent of a simple continuous fractional expansion of $\frac{e}{\phi_1}$.

Also from $k=\frac{ed-1}{\phi}<\frac{ed}{\phi_1}+\frac{1}{2d}$, we get $d^2-\frac{\phi_1}{e\Delta\phi}d-\frac{\phi\phi_1}{2e\Delta\phi}<0$, such that $m=\frac{\phi_1}{2e\Delta\phi}$, the above equation becomes $d^2-2md-m\phi<0$, so that the function $f(d)=d^2-2md-m\phi$, $f(0)=-m\phi<0$, and the 2nd root of the quadratic equation $f(d)=0$ is $d_1=m-\sqrt{m^2+m\phi}<0$, $d_2=m+\sqrt{m^2+m\phi}$, and the condition for satisfying the inequality $f(d)=d^2-2md-m\phi<0$ is $0<d<d_2=\frac{\phi_1}{2e\Delta\phi}\left(1+\sqrt{1+\frac{2e\ phi\Delta\phi}{\phi_1}}\right)$.

Suppose $\frac{\phi_1}{2e\Delta\phi}\left(1+\sqrt{1+\frac{2e\phi\Delta\phi}{\phi_1}}\right)<\frac{\phi_1}{2}\Rightarrow e\Delta\phi>2\left(1+\frac{\phi}{\phi_1}\right)$, by $1>\frac{\phi}{\phi_1}$, so it is only necessary to satisfy $e\Delta\phi>4$, which is the general RSA that satisfies this inequality. Remember that $t=\frac{p}{q}>1$, from $\begin{cases}p=tq\\pq=n\end{cases}\Rightarrow\begin{cases}p=\sqrt{t}\sqrt{n}\\q=\frac{\sqrt{n}}{\sqrt{t}}\end{cases}$, $\sqrt{\Delta\phi}=\sqrt{p}-\sqrt{q}=\left(\sqrt[4]{t}-\frac{1}{\sqrt[4]{t}}\right)\sqrt[4]{n}$, and so the equivalence condition for the algorithm of this paper to hold is obtained:

$$d<\frac{\phi_1}{2e\Delta\phi}\left(1+\sqrt{1+\frac{2e\phi\Delta\phi}{\phi_1}}\right)\approx\sqrt{\frac{\phi\phi_1}{2e\Delta\phi}}\approx\frac{n^{\frac{3}{4}}}{\sqrt{2e}\left(\sqrt[4]{t}-\frac{1}{\sqrt[4]{t}}\right)} \tag{31}$$

Satisfying this equivalent inequality, $\frac{k}{d}$ must be a convergent of a simple continuous fractional expansion of $\frac{e}{\phi_1}$, and k,d verifies as above.

Since $\phi<\phi_1<n$, $\frac{e}{n}-\frac{k}{d}<\frac{e}{\phi_1}-\frac{k}{d}$, if the condition of Wiener's algorithm is satisfied, i.e., $\left|\frac{e}{n}-\frac{k}{d}\right|<\frac{1}{2d^2}$, which leads to $-\frac{1}{2d^2}<\frac{e}{n}-\frac{k}{d}<\frac{e}{\phi_1}-\frac{k}{d}$, and $\frac{e}{\phi_1}-\frac{k}{d}<\frac{1}{d\phi_1}<\frac{1}{2d^2}\Rightarrow d<\frac{\phi_1}{2}$, which is easy to prove $\frac{n^{0.25}}{3}<\frac{\phi_1}{2}$. It is proved that as long as the conditions of Wiener's algorithm are satisfied, the conditions of this algorithm are also satisfied. The range of decoding indices d conditional on the establishment of this algorithm is much larger than the range of decoding indices required for the establishment of Wiener's algorithm.

4 Experimental results and analysis

The main work in this chapter is to validate the results of the previously proposed RSA attack algorithm based on approximating Legendre's theorem by concatenated fractions, and the validation method adopted is mainly comparative validation, and the main target of the attack is the original RSA algorithm smart card.

4.1 Construction of the experimental platform

Main equipment for the experiment: oscilloscope, card reader, computer and low-pass filter.

Attack Software: Inspector V4.4

The main application of this experiment is the continuous fractional RSA attack algorithm, in the whole attack operation process, Inspector software can directly provide tracking analysis results and intuitive graphical representation.

4.1.1 Data acquisition platform

In the Inspector attack system, a large number of hardware is used to complete the control of

the whole attack process, and the PC, card reader and filter are used in this experiment.

(1) PC: As the only interface for human-computer interaction, the main function is to send data and commands to other devices (card reader and oscilloscope), and receive feedback information, process, store and display the returned data. Usually by sending commands to complete the pre-setup of the smart card, including setting the key, write plaintext cipher card and collect signals.

(2) Card Reader: This module is the executor of PC commands, the main work for the direct operation of the smart card, which receives the sent plaintext/ciphertext and the key to encrypt and decrypt the information and return the ciphertext/plaintext. Usually the operation of the card reader on the smart card is also the key point of energy consumption, oscilloscope is through some external means to measure the smart card work energy consumption.

(3) Oscilloscope: This module is also the executor of PC commands, its main work is signal acquisition, when the PC sends the command to start acquisition, the oscilloscope starts to work, and through analog-to-digital conversion, the analog signals will be collected from the card reader part.

4.1.2 Data analysis platform

The Inspector software used for the experiments implements real-time signal processing of test objects, triggers, oscilloscopes and connected components during the data acquisition phase. It contains a data module capable of cryptanalyzing all algorithms and provides open source, enabling users to develop targeted modules or protocols according to their needs. The whole software realizes the acquisition, processing and analysis of signals.

(1) Data acquisition

Its main work is to guide the hardware to work, so that the external hardware can be customized according to the user to achieve automated configuration. In the specific work of smart card, it realizes the automatic generation of messages or the formation of messages according to the instruction (for example, the formation of a large number of plaintexts in the attack, etc.), encrypts and decrypts the smart card, and records the generated data. This data acquisition module basically realizes real-time signal acquisition.

(2) Data Processing

The data processing module includes functions such as filtering, spectrum analysis, statistics, alignment and correlation calculation, etc. The RSA attack requires the attacker to control the acquisition of traces and sample points.Inspector provides a spectrum filter, and the user can set the filter characteristics and harmonic filter according to requirements. The signal is processed using its harmonic, statistical and frequency analysis features. It is worth mentioning that the alignment function it provides is a key technique to ensure the success of the attack.

(3) Data Analysis

This part of the data analysis mainly focuses on the analysis of the key, Inspector provides a human-settable cryptanalysis module, this module through the human-settable algorithm (even points RSA attack algorithm) to carry out targeted attacks, relying on the data analysis of this part of the analysis mainly focuses on the analysis of the key. The key information is extracted by analyzing the energy consumption traces and sampling points, which is the core part of the whole attack system.

4.2 RSA Attack Experiments

To attack the RSA smart card using the continuous fractional RSA attack algorithm, insert the smart card with the RSA algorithm already written into the card reader, set the secret steel and sampling parameters, and get ready for the attack.

Set the 512bit key as:

3D 49 9E 3F 05 64 DG 57 2H C6 65 4C B2 1F 01 ET A9 C5 B8 E9 F6 13 5E 34 9V 55 F4 08 57 8F 44 2B A2 C7 24 FG 4N 78 06 56 8C 71 03 5D 57 BF 78 3B F6 71 B1 9E 04 5D 80 93 CE D2 E3 A4 3C E9 7F

4.2.1 Sampling Settings

After the key is set successfully, the sampling parameters are set. In this experiment, a 50Hz low-pass filter is used, the sampling rate is 250M samples/second, and the sampling time is set to 50ms. the RSA smart card is sampled and the energy consumption trajectory is shown in Fig. 1, which shows that the energy consumption of the RSA algorithm of the smart card is in the range of -500~1400mVolt.

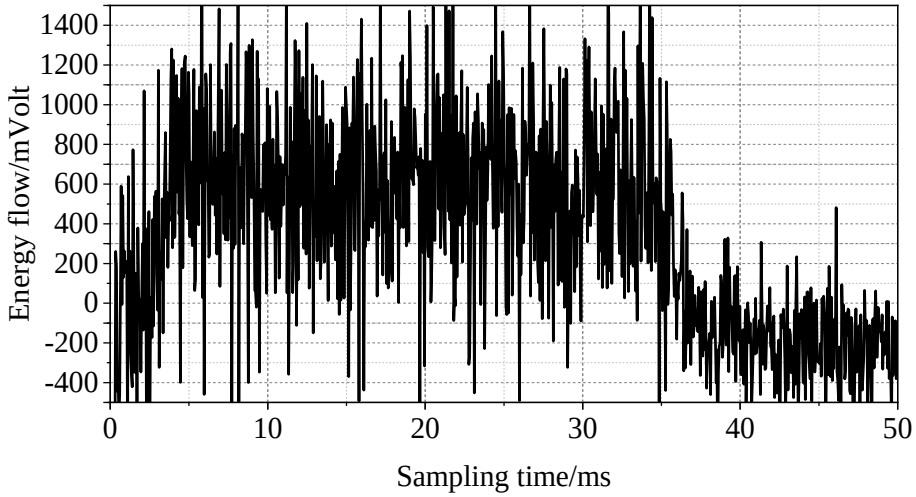

Figure 1: The energy consumption trajectory of the smart card RSA algorithm

4.2.2 Attack process

The main data analysis carried out in this research is also known as the attack of RSA algorithm.

Step 1: Selection of the attack area, an example of RSA trajectory map area selection is shown in Figure 2. Using the continuous fraction RSA attack algorithm, the analysis module is run and the modulus is entered and the analysis is performed using the previous settings.

Step 2: At the end of the run, the following information will be displayed in the status window:

Best correlation:

0,sub key:249(0xBC),value:0.4563,at position:2245

1,sub key:250(0xB7),value:0.4627,at position:228

2,sub key:251(0xBF),value:0.4851,at position:2340

3,sub key:252(0xB5),value:0.4338,at position:2365

Partial prime estimate:BF

This means that the first bit of information of the prime number has been cracked. The high risk energy leakage region is shown in Fig. 3.Observe the location of the energy leakage in the trajectory diagram, as it is possible to generate energy leakage of all bits in a very narrow region, so the sample point region with high energy leakage is selected for attack in the following attack.

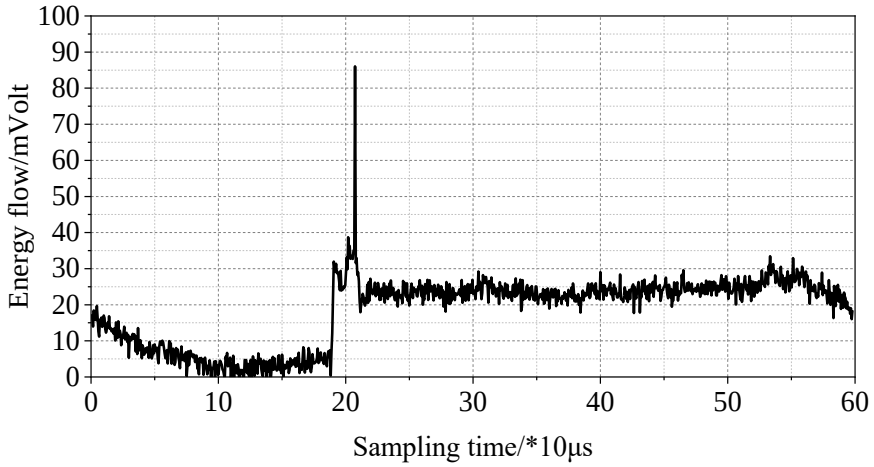

Figure 2: Examples of RSA trajectory map area selection

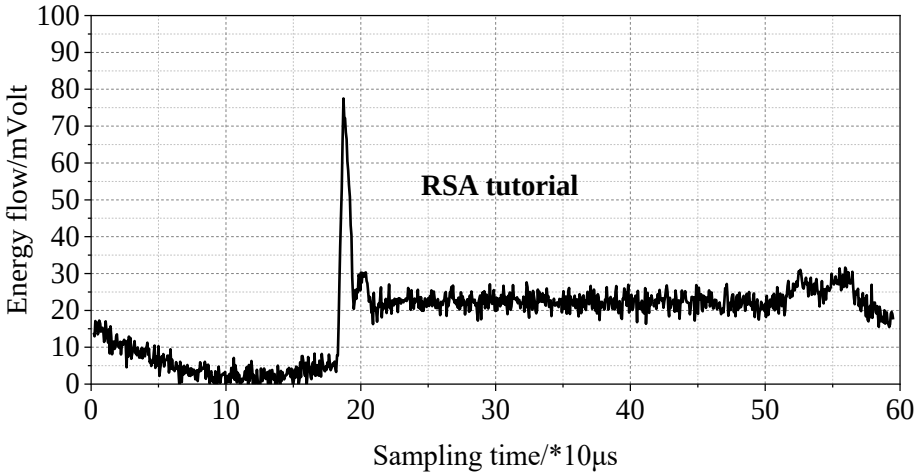

Figure 3: High risk energy leakage area

Step 3: From the above attack, the information of the second bit of the prime number is obtained.

Step 4: Based on the above steps, the attack of the next bit bits is carried out sequentially, and when the third bit of the attack result is obtained, there is a correction of the former bit by the latter bit.

Step 5: The calculation of the remaining bits of information is carried out sequentially, and the information in the last three bits is calculated by forced fusion, and the result of the attack is obtained:

3D 49 9E 3F 05 64 DG 57 2H C6 65 4C B2 1F 01 ET A9 C5 B8 E9 F6 13 5E 34 9V 55 F4 08 57 8F 44 2B A2 C7 24 FG 4N 78 06 56 8C 71 03 5D 57 BF 78 3B F6 71 B1 9E 04 5D 80 93 CE D2 E3 A4 3C E9 7F

Up to this point gives the attack out of the key, from the comparison can be seen, this paper even points RSA attack algorithm of the smart card key, the results of its attack and the actual results match, successfully complete the attack on the key of the RSA algorithm.

4.3 Comparative Performance Analysis

In this subsection, based on the implementation of the RSA attack experiments, several sets of experiments are designed to test the performance of this paper's concatenated score RSA

attack algorithm. In order to compare with existing schemes, Wiener algorithm and OP-RSA algorithm (which utilizes the principle of best approximation of finite simple concatenated fractions to decipher the public key cryptography RSA) are selected as the comparison methods in this paper.The 3 algorithms are carried out in the same experimental environment, and all the codes are written in C++, and MIRACL cryptographic library is used in the implementation process.

4.3.1 Calculation time

The experiment first specifies the size of the file as 1GB and tests the time required for the three RSA attack algorithms to be computed at the user's end when the size of the file varies with the size of the file chunks. Fig. 4 and Fig. 5 depict the preprocessing time for the file and the time used to verify the proof, respectively. In this paper, the preprocessing time and verification proof time for files in the connected fraction RSA attack algorithm are on average 50.06% and 20.34% of Wiener's algorithm, respectively, and the preprocessing time and verification proof time for files in the connected fraction RSA attack algorithm are on average 63.56% and 32.46% of OP-RSA's algorithm. Fig. 6 shows the comparison of the time spent by the three algorithms at the server side (response time of the challenge). The server-side computational time consumed consists of two main blocks: the time to read the blocks and the time for key generation. Considering the time consumed for reading the file blocks, the total server-side computation consumption time of the even-count RSA attack algorithm is only 46.15% and 50.48% of the corresponding time for the Wiener and OP-RSA algorithms, on average.

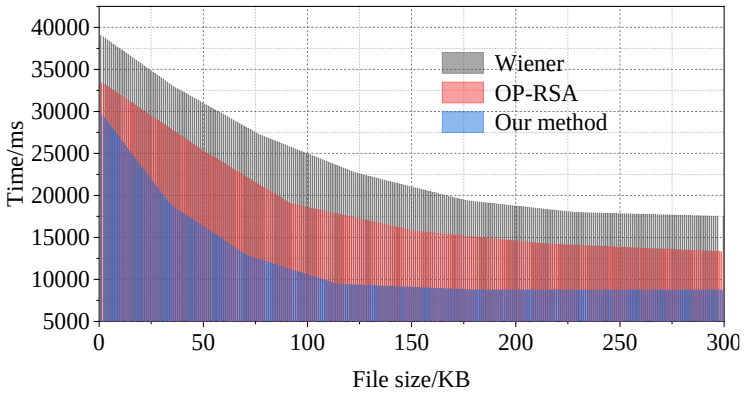

Figure 4: Comparison of pretreatment time

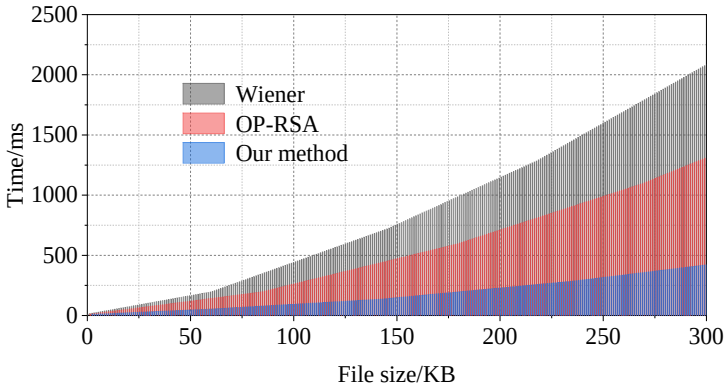

Figure 5: The comparison of the proof and the validation time

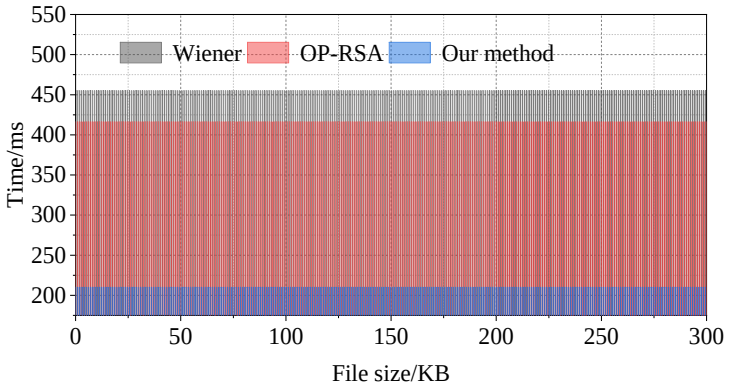

Figure 6: The time comparison of the server generation key

4.3.2 Communication costs

Then, the experiment also tests to compare the communication cost of the two schemes. A file of size 1GB is still selected for the experiment and the effect of different chunk sizes on the communication cost is observed. In order to remove the effect of file size on the communication cost and better highlight the essential differences between the schemes, only the communication cost caused by key generation is considered here. The comparison of the communication cost when the file size is 1 GB is shown in Fig. 7. The communication cost of the three algorithms is almost linearly related to the size of the file chunks, and with the increase of the file chunk size, the size of the communication cost also increases. When at a relatively small chunk (e.g., 20KB), both schemes converge to an optimal value, i.e., the communication cost is minimized. Combined with the results of the experiments, it can be concluded that the combined performance of the schemes is optimal when the size of the chunks is between 15KB and 30KB for a file with a size of 1GB. When the file size is 1GB, the average value of communication cost of this paper's even fraction RSA attack algorithm is 75.42% and 87.45% of that of Wiener's algorithm and OP-RSA algorithm, which possesses a smaller communication cost.

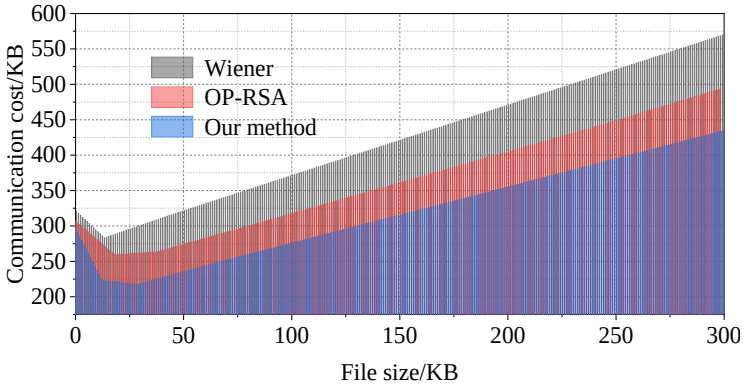

Figure 7: The comparison of the volume of the file in 1GB

5 Conclusion

In high-precision numerical computation, the application of the concatenated fractional representation is reflected in the college approximation of irrational numbers and compressed numerical storage. In this paper, we focus on its application in cryptanalytic decipherment and

explain its role in deciphering the Okamoto regime, the Throwback public key regime and the RSA regime with short decryption index. Based on this, the application of concatenated fractions to decipher RSA regimes with short decryption indices is optimized, and an improved concatenated fractions RSA attack algorithm based on Wiener's algorithm is proposed, which weakens the Wiener's constraints on the small decryption indices d and enlarges the range of choices for d. The experimental platform is built to simulate and analyze, and the comparison method is chosen to explore the performance of the RSA attack algorithm, the results are as follows: the key attacked by the RSA attack algorithm is in line with the set key, and the feasibility and validity of completing the successful attack on the key of the RSA algorithm are examined. Compared with the selected comparison method, when the file size is 1GB, the preprocessing time, authentication time, and total server time consumption of the even score RSA attack algorithm are less, accounting for less than 51%, 64%, and 51% of the computation time of the comparison method, respectively, and its communication cost is also significantly lower than that of the comparison method, accounting for less than 88% of the comparison method, which indicates that the even score RSA attack algorithm is superior to the comparison method in terms of both computational efficiency and communication complexity are better than the comparison scheme.

In the information age, the rapid development of data transmission and processing technology has changed all aspects of social daily life. The application of continuous fractional representation in high-precision numerical computation is conducive to the optimization of data transmission and processing, and its optimized practice in cryptography can promote the security of communication in the open and complex network environment.

References

[1] Zhu, L., Zhang, C., Zhang, Z., & Zhou, X. (2020). High-precision calculation of gas saturation in organic shale pores using an intelligent fusion algorithm and a multi-mineral model. Advances in Geo-Energy Research, 4(2), 135-151.

[2] Bêche, B. (2025, May). Despite the Heisenberg's uncertainty principle, why does it seem possible to calculate eigenvalues and eigenmodes with high precision in electromagnetism or integrated photonics confined in highly symmetrical guiding nanostructures with no cut-off frequency or thickness?. In Journée des sciences et technologies quantiques.

[3] Mougeot, X. (2019). Towards high-precision calculation of electron capture decays. Applied Radiation and Isotopes, 154, 108884.

[4] Tianbao, M., Huilan, R., Jian, L., & Jianguo, N. (2016). Large scale high precision computation for explosion and impact problems. Chinese Journal of Theoretical and Applied Mechanics, 48(3), 599-608.

[5] Cao, H., & Wen, L. (2022). High-precision numerical research on flow and structure noise of underwater vehicle. Applied Sciences, 12(24), 12723.

[6] Zou, J., Li, D., & Wang, J. (2022). High-precision numerical calculation method of solar radiation pressure force for wrinkled solar sails. Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering, 236(12), 2463-2471.

[7] Han, P. P., Chen, K., Liu, D. X., You, Y. X., & Wang, J. (2021). A high precision

computing method for heat transfer in the process of oil-water displacement. Journal of Hydrodynamics, 33(5), 958-969.

[8] Van Houcke, K., Werner, F., & Rossi, R. (2020). High-precision numerical solution of the Fermi polaron problem and large-order behavior of its diagrammatic series. Physical Review B, 101(4), 045134.

[9] Chakraborty, S., Roychowdhury, M. K., & Sifuentes, J. (2021). High precision numerical computation of principal points for univariate distributions. Sankhya B, 83(Suppl 2), 558-584.

[10] Han, C., Wang, Y. L., & Li, Z. Y. (2022). A high-precision numerical approach to solving space fractional Gray-Scott model. Applied Mathematics Letters, 125, 107759.

[11] Mora, H., Signes-Pont, M. T., López, F. P., Mora-Pascual, J., & Chamizo, J. G. (2024). Advancements in number representation for high-precision computing. The Journal of Supercomputing, 80(7), 9742-9761.

[12] Xue, D., & Bai, L. (2024). High-Precision Numerical Algorithms and Implementation in Fractional Calculus. In Fractional Calculus: High-Precision Algorithms and Numerical Implementations (pp. 101-138). Singapore: Springer Nature Singapore.

[13] LEITOLD, L., ALRWASHDEH, M., & KOLLAR, Z. (2025). High-Performance Multi-Precision Tool for Floating-Point Computations. RADIOENGINEERING, 34(4), 583.

[14] Laporta, S. (2017). High-precision calculation of the 4-loop contribution to the electron g-2 in QED. Physics Letters B, 772, 232-238.

[15] Park, I., & Cho, S. (2019). The influence of number line estimation precision and numeracy on risky financial decision making. International Journal of Psychology, 54(4), 530-538.

[16] Flores-Vergara, A., García-Guerrero, E. E., Inzunza-González, E., López-Bonilla, O. R., Rodríguez-Orozco, E., Cárdenas-Valdez, J. R., & Tlelo-Cuautle, E. (2019). Implementing a chaotic cryptosystem in a 64-bit embedded system by using multiple-precision arithmetic. Nonlinear Dynamics, 96(1), 497-516.

[17] Bjorklund, C., & Litman, M. (2024). Error approximation for backwards and simple continued fractions. Research in Number Theory, 10(1), 2.

[18] Pratsiovytyi, M., Goncharenko, Y., Lysenko, I., & Ratushnyak, S. (2023). Finite A 2-Continued Fractions in the Problems of Rational Approximations of Real Numbers. Ukrainian Mathematical Journal, 75(6), 972-983.

[19] Pratsiovytyi, M., & Chuikov, A. (2019). Continuous distributions whose functions preserve tails of an A-continued fraction representation of numbers. Random Operators and Stochastic Equations, 27(3), 199-206.

[20] Han, S., Masuda, A., Singh, S., & Thiel, J. (2020). Subgroups of $SL_2(\mathbb{Z})$ characterized by certain continued fraction representations. Proceedings of the American

Mathematical Society, 148(9), 3775-3786.

[21] Duverney, D., & Shiokawa, I. (2024). Irrationality exponents of semi-regular continued fractions. Tokyo Journal of Mathematics, 47(1), 89-109.

[22] Hingu, C., Fu, X., Saliyu, T., Hu, R., & Mishan, R. (2024). Power-Optimized Field-Programmable Gate Array Implementation of Neural Activation Functions Using Continued Fractions for AI/ML Workloads. Electronics, 13(24), 5026.