Cryptanalysis of the Merkle-Hellman Knapsack Cryptosystem Using Continued Fraction: Two Attack Scenarios

Rana Abdul Latif [1], Rifaat Z. Khalaf [1] and Aqeel Ismael Hasan[2]
[1]*Department of Mathematics, College of Science, University of Diyala, 32001 Baqubah, Iraq*
[2]*Department of Computer Science, Al-Miqdad College, University of Diyala, 32001 Baqubah, Iraq*
scimathms242502@uodiyala.edu.iq, drrifaat55@gmail.com, aqeel.muq@ uodiyala.edu.iq

Keywords: Merkle-Hellman Knapsack, Continued Fractions, Public-Key, Cryptography.

Abstract: This paper presents a mathematical cryptanalysis of the Merkle-Hellman knapsack cryptosystem: using continued fractions as the sole analytical tool. We explore two distinct attack scenarios: (1) partial knowledge of the private key, and (2) access to the public key only. In both cases, we demonstrate how continued fractions can be used to approximate the transformation ratio r⁄q, enabling recovery of the secret parameters and the original super increasing sequence. Our results show that this approach is effective under certain conditions. The aim of this section is to evaluate the effectiveness of our method in two different cases of attacker knowledge. In the first case, the attacker knows the public key and only one element of the private key (the increasing sequence). In the second case, the attacker knows only the public key. These two cases will be presented in detail in the experiments section to measure the efficiency of the proposed method under different levels of the attacker knowledge. Furthermore, our method was compared with other well-known attacks on the Merkle-Hellman cryptosystem, and the results demonstrated the proposed approach achieves high efficiently for analyzing this type of encryption scheme.

1 INTRODUCTION

The Merkle-Hellman knapsack cryptosystem was one of the first public key encryption schemes designed to enable secure communication without prior key exchange [1]. It was based on the hardness of the super increasing knapsack problem, which was believed to be computationally infeasible. The system transforms a numerical string into a public-key using a large modulo multiplier, making recovery of the private key seemingly impossible without knowledge of the transformation. Despite its innovative design, the Merkl- Hellman system was quickly shown to be vulnerable. Analytical attacks exploited the numerical structure of the public key, particularly through continued fractions, which approximate ratios between multipliers and the modulus [2]. Famously demonstrated a polynomial-time algorithm that successfully increasing sequence is created and then converted into a public-key using secret coefficients. In the encryption phase, the plaintext message is converted into a binary vector, which is multiplied by the elements of the public-key to produce the ciphertext. Finally, in the decryption phase, the private key and secret transformation factors are used to reverse the process, allowing the original message to be retrieved efficiently due to the properties of the super-increasing sequence [3].

1.1 The Merkle-Hellman

Although the Merkle-Hellman system [4] was a groundbreaking innovation in the early days of public-key cryptography, it was eventually broken. In, demonstrated a polynomial - time attack using lattice reduction and continued fractions, exposing the weaknesses of the system [3]. Since then, the algorithm has been considered insecure and is no longer used in practice. However, its historical importance lies in paving the way for later cryptographic systems and inspiring research into lattice - based cryptography, which is now a leading candidate for pos -quantum security. Recent studies confirm this perspective, showing that while Merkle-Hellman remains academically significant, it is not secure for practical us proposed a method to strengthen knapsack-based cryptosystems against the Lenstra-Lenstra-Lovász (LLL) algorithm using continued fractions, highlighting theoretical improvements but confirming the original system

remains vulnerable [3]. Improving upon Shamir's original method by reducing computational complexity [1]. Another study by Anantharaman and Ding explored experimental hybrid encryption schemes combining Merkle-Hellman with optical techniques, though these remain academic prototypes without strong security guarantees [3].

1.2 Continued Fractions

Continued fractions are a fundamental concept in number theory and cryptography because they provide optimal rational approximations of real number [5]. A continued fraction expansion of a real number x that is the most common type of continued fraction is that of continued fraction s for real numbers this is the case where Q(R) = Q with usual Euclidean metric is expressed as:

$$\boldsymbol{x} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}$$

Where $a_0, a_1, a_2, a_3, \ldots$ are integers. Each truncation of this infinite expansion yields a rational approximation known as a convergent [6]. These convergent are particularly useful because each step produces a better approximation of the original number, and they are guaranteed to be the best possible approximations with respect to their denominators [7].

Theorem 1 [8]: For K ≥ 1 the k^{th} convergent can Written with numerator and denominator satisfying the following recurrence relation:

$$p_k = a_k\, p_{k-1} + p_{k-2}\, p_{-1} = 1, p_0 = a_0 q_k = a_k q_{k-1} + q_{k-2}, q_{-1} = 0\; q_0 = 1.$$

Theorem 2 [9] the continued fraction expansion of a real number is finite if and only if the number is rational. This result establishes a direct link between rationality and the termination of the expansion, while irrational numbers always produce infinite continued fractions.

Theorem 3 [9]: Every odd convergent is greater than any even convergent**.**

Theorem 4 [10]: For every fraction in the Fraction Tree, there corresponds a unique natural number.

Theorem 5 [10]: Known as the fundamental recurrence relation, states that for all i ≥ 0:

$$p_i q_{i-1} - p_{i-1} q_k = (-1)^i \text{ for all i} \geq 0.$$

This identity guarantees that successive convergent alternate around the true value of the number being approximated, and that they are the closest possible rational approximations given their denominators. In cryptography, these theorems are not merely theoretical but have practical implications. Continued fractions have been used in attacks on cryptosystems such as RSA and the Merkle-Hellman knapsack system [3]. Their ability to approximate hidden parameters makes them powerful in cryptanalysis. As a notable example, Shamir based his attack on the Merkle-Hellman system relied on continued fraction to recover the private key [2]. Shamir's attack on Merkle-Hellman relied on continued fractions to reconstruct private keys. More recently [6] and [11] proposed strengthening knapsack-based cryptosystems against LLL attacks using continued fractions, while [1] and [5] presented an efficient attack on Merkle-Hellman that improved upon Shamir's method [2]. [5] and [6] explored hybrid encryption schemes combining Merkle-Hellman with optical techniques, and combined continued fractions with Coppersmith's method to enhance RSA cryptanalysis [6]. These studies confirm that continued fractions remain highly relevant in modern cryptographic research.

1.3 Application to Cryptanalysis

The application of continued fractions to cryptanalysis is one of the most powerful techniques for breaking certain public-key cryptosystems, particularly those based on the knapsack problem such as the Merkle-Hellman scheme [3]. The main idea is that if an attacker can estimate the ratio r/q, where $r$and q are secret parameters used in transforming the private super-increasing sequence into the public key, then candidate values for these parameters can be derived using the convergents of the continued fraction expansion of r/q.

Once these candidates are obtained, the attacker computes the modular inverse $r^{-1} mod\, q$and attempts to reconstruct the original private sequence using:

$$w_i = (r^{-1} \cdot A_i) mod\, q.$$

where A_i are elements of the public key. If the resulting sequence $\{w_i\}$is super-increasing, the attack is successful because the private key has been recovered.

This method exploits the fact that continued fractions provide the best rational approximations of real numbers, enabling the attacker to narrow down possible values of $r$and q with high accuracy. The technique was first formalized in Shamir's polynomial-time attack on the Merkle-Hellman cryptosystem, where continued fractions were used to

approximate hidden parameters and reduce the problem to a super-increasing knapsack.

Modern research has further refined this approach. Some studies have proposed improvements in resistance against attacks combining continued fractions with lattice reduction methods [5], while others have developed more efficient attacks that reduce computational complexity compared to Shamir's original method [1] and [5]. In addition, hybrid techniques combining continued fractions with Coppersmith's method have been applied to RSA cryptanalysis, showing that this approach is not limited to knapsack systems but extends to broader areas of public-key cryptography [7].

Thus, the use of continued fractions in cryptanalysis highlights both the vulnerabilities of early cryptosystems and the continuing importance of number-theoretic methods in modern cryptographic research.

2 ATTACK SCENARIO I: PARTIAL KNOLEDGE OF THE PRIVATE KEY

2.1 Attack Assumptions

Sequence W and the full public-key B. The most fundamental assumption is that the attacker has ssaccess to the complete public- key B=$\{A_1, A_2, A_3, \ldots, A_n\}$ since this key is openly distributed and used for encryption. In addition, it is assumed that the attacker may know one or more elements of the private sequence W=$\{w_1, w_2, \ldots, w_n\}$. This partial knowledge can arise from side-channel leaks, implementation flaws, or deliberate exposure of small parts of the private key. With these assumptions, the attacker's strategy is to exploit the mathematical relationship between the public-key and the private sequence. The public-key is generated by transforming the private super- increasing sequence using a secret multiplier (r) and modulus (q). It is assumed that gcd(r,q)=1 If the attacker knows even a single element of the private sequence, they can attempt to approximate the ratio r/q using continued fractions. This approximation allows them to generate candidate values for r and q, and then compute the modular inverse $r^{-1}\ mod\ q$.

By applying this inverse to the public-key elements, the attacker can attempt to reconstruct the private sequence:

$$w_i = (r^{-1} \cdot A_i) mod\ q. \quad (1)$$

If the reconstructed sequence is super - increasing, the attack is considered successful, since the attacker has effectively recovered the private key. The assumption that the attacker knows at least part of the private sequence significantly reduces the complexity of the attack. It provides a foothold for applying number-theoretic techniques such as continued fractions and lattice reduction. Modern research has shown that even limited knowledge of the private sequence can be enough to compromise the system. For instance and [5], [6] demonstrated that efficient attacks can be mounted with partial information, while explored methods to strengthen knapsack-based systems against such vulnerabilities [8]. These findings highlight that the security of the Merkle-Hellman system is critically undermined when attackers are assumed to have partial knowledge of the private sequence, reinforcing why the cryptosystem is no longer considered secure in practice.

2.2 Attack Method

The attack steps can be summarized as follows:

1) Step 1: Compute the ratio $b_i/w_i \approx$ r /q, where b_i are public-key elements and w_i are known private sequence elements.
2) Step 2: Generate continued fractions. Expand the ratio into a continued fraction to obtain convergent that approximate r/q.
3) Step 3: Extract candidate convergent. Select candidate values in the form r'/q' from the convergents.
4) Step 4: Test each candidate for every candidate pair (r, q′), verify the following conditions:
   - Gcd (r' ,q') = 1 to ensure coprimality.
   - q′ >$\sum w$, meaning the modulus is larger than the sum of the private sequence.
   - Check whether ($w_i = r'^{-1} \cdot A_i$) $mod\ q'$ reconstructs a super-increasing sequence.
5) Step 5: Confirm success. If the reconstructed sequence is super - increasing, the attack is successful and the private key is recovered.

3 ATTACK SCENARIO II: PUBLIC KEY ONLY

3.1 Attack Assumptions

The attacker has access only to the public- key B, with no knowledge of W.

3.2 Attack Method

The attack procedure can be summarized into clear steps as follows:

1) Step 1: Select pairs of public key elements. Choose pairs (b_i , b_j) from the public- key and compute the ratiob_i/b_j.These ratios provide approximations of the hidden parameters.
2) Step 2: Generate continued fractions. Expand each ratio into a continued fraction. This produces convergent that serve as candidate values for the secret multiplier r and modulus q.
3) Step 3: Extract convergent from the continued fraction expansion, identify convergent in the form r′/q′. Each convergent represents a possible candidate pair for the secret parameters.
4) Step 4: Test candidate pairs for each candidate (r′, q′), perform the following checks:
   - Compute modular inverse. Calculate r ′mod q′.
   - Recover private sequence. Apply the relation $w_{i'} = (r^{-1}. A_i)$mod q′ to reconstruct a candidate private sequence.
   - Check super - increasing property. Verify whether the recovered sequence w' is super - increasing. If it is, the candidate pair is valid.
5) Step 5: Confirm success If a candidate pair produces a super - increasing sequence, the attack is successful, meaning the attacker has effectively recovered the private key.

4 EXPERMENTAL EXAMPLES

Present two complete examples demonstrating its effectiveness under both scenarios: partial private To validate the proposed attack methodology using continued fractions, we key knowledge and public key-only access.

4.1 Case I: Partial Knowledge of the Private Key Setup

Super -increasing sequence (private key):

W=[2,5,11,23].

- Modulus: q = 67;
- Multiplier: r = 13;
- Public key: B = [26,65,9,31];
- Assumption: The attacker knows only one element of the private key.

4.2 Attack Method (Step by Step):

The attack method consists of a sequence of computational steps that exploit partial knowledge of the private sequence to reconstruct the secret key. The complete procedure is summarized as follows:

1) Step 1: Use partial knowledge. The attacker begins with the known element of the private sequence (for example, w_1 =2). This provides a starting point to approximate the hidden parameters.
2) Step 2: Compute ratios. The attacker computes ratios between public- key elements and the known private element, such as b_i w_1. These ratios approximate the fraction rq.
3) Step 3: Generate continued fractions Each ratio is expanded into a continued fraction. This produces convergent that serve as candidate values for r and q.
4) Step 4: Extract candidate convergent. From the continued fraction expansion, the attacker selects convergent in the form $r'q'$. These are possible values for the multiplier and modulus.
5) Step 5: Test candidate pairs For each candidate pair (r',q'), the attacker performs the following checks:
   - Compute the modular invers(r'^{-1}mod q') .
   - Recover the private sequence using the relation:

$$w_{r'} = \left(r'^{-1} \cdot A_i\right) mod\ q' \qquad (2)$$

   - Verify whether the recovered sequence w' is super - increasing.
6) Step 6: Confirm success. If the reconstructed sequence is super-increasing, the attack is successful. The attacker has effectively recovered the private key despite knowing only one element initially.

4.3 Attack Execution

Here is the detailed breakdown of the attack procedure in Case I: Partial Knowledge of the Private Key using the given setup:

1) Estimate the ratio r/q: The attacker starts by using the known private element w_1=2 and the corresponding public element $b_1 = 26$.

$$b_1/w_1 = 26/2 = 13 \Rightarrow r/q \approx 13/67.$$

Table 1: Comparison with other attack.

Attack Type	Methodology	Requirements	Complexity	Effectiveness
Shamir	Polynomial al algebra	Full public key	Moderate	Limited
LLL(Lattice)	Lattice reduction	Partial/ full Key	High	Strong
Continued fractions	Arithmetic ratios	Partial or public Key	Low	Conditional

This gives an approximation of the hidden parameters r and q.

2) Generate the continued fraction expansion: The fraction 13/67 is expanded into a continued fraction:

$$13 / 67 = [0;5,6,2].$$

Table 1 compares the proposed attack with other well-known attacks on the Merkle–Hellman cryptosystem in terms of methodology, requirements, computational complexity, and effectiveness.

Each convergent provides candidate values for r and q.

3) Verify candidate conditions: For the candidate pair (r = 13,q = 67), the attacker checks:
   - gcd (13, 67) =1, confirming coprimality.
   - Compute the modular inverse:

$$r^{-1} \, mod \, 67 = 31.$$

This ensures that the inverse exists and can be used to reconstruct the private sequence.

4) Recover the private key sequence: Using the relation:

$$w_i = (r^{-1} \cdot A_i) \text{mod } q.$$

the attacker reconstructs the sequence:

$$W' = [2,5,11,23].$$

5) Confirm success: The recovered sequence w' matches the original super-increasing sequence. This confirms that the attack has succeeded, even though the attacker initially knew only one element of the private key.

4.4 Case II: Public-Key Only Attack

Setup:

- Public key B [51, 119, 124, 20, 74]
- Assumption No knowledge of the private-key is available.
- Attack steps:
  1) Estimate $r/q \; using \; public - key \; ratio$: $b_1/b_5 = 17/131 \approx 1.545$.
  2) Generate Continued fraction for: $17/131 \approx 1.545$ convergent: $17/131 \approx [0,7,1,2,2,2]$.
  3) Test candidate r =17, q = 131.
- gcd (17,61) = 1,$r^{-1} \, mod \, 131 = 5.$
4) Recover private key: ($b_i \cdot 45$) $mod \; 131 \rightarrow w' = [3,7,15,32,66]$.

This approximation was obtained after trying all possible approximations.

4.5 Results and Discussion

The experimental analysis confirms that the proposed continued-fraction attack is capable of recovering the original super-increasing sequence under both investigated scenarios. In the first scenario, where partial knowledge of the private sequence is available, the correct values of the hidden parameters were successfully identified, allowing complete reconstruction of the private key. In the second scenario, where only the public key is available, continued-fraction approximations generated suitable candidate parameters that also enabled successful recovery of the original sequence. In both cases, the reconstructed sequences satisfied the super-increasing property, confirming the correctness of the recovered private key. These results demonstrate that the proposed continued-fraction approach provides an effective and computationally inexpensive cryptanalytic technique for the Merkle–Hellman cryptosystem, particularly when small key parameters are used or partial information about the private sequence is available. Compared with more computationally demanding lattice-based attacks, the proposed method relies primarily on arithmetic operations and rational approximations, making it straightforward to implement while remaining effective under the considered attack scenarios.

5 CONCLUSIONS

This paper has demonstrated that continued fractions can be applied as a powerful cryptanalytic tool against the Merkle-Hellman Knapsack cryptosystem under realistic scenarios, including cases of partial knowledge of the private key. The attack method is fundamentally arithmetic in nature, relying on rational approximations, modular inverses, and the super-increasing property of sequences. It requires minimal computational resources compared to other cryptanalytic techniques, yet it remains highly

effective when key parameters are small or when even limited information about the private sequence is leaked. The analysis of attack cases shows that once an attacker can approximate the ratio r/q, continued fractions provide convergent that lead directly to candidate values for the secret parameters. With these candidates, the attacker can reconstruct the private sequence and verify its super-increasing property, thereby confirming the success of the attack. This highlights the inherent weakness of the Merkle-Hellman system: its reliance on predictable mathematical structures that can be exploited through number - theoretic methods.

ACKNOWLEDGMENTS

The author gratefully acknowledges the support of department of mathematics, college of science, university of Diyala.

REFERENCES

[1] J. Bi, L. Su, H. Peng, and L. Wang, “A simple and efficient attack on the Merkle-Hellman knapsack cryptosystem,” PLOS ONE, vol. 20, no. 5, p. e0322726, 2025.

[2] A. A. Khaleell, “Secure knapsack cryptosystem against LLL algorithm based on continued fraction,” 2024.

[3] H. Tahiri Alaoui, A. Azouaoui, and J. El Kafi, “Artificial neural networks cryptanalysis of Merkle-Hellman knapsack cryptosystem,” Lecture Notes in Networks and Systems, vol. 637, 2023.

[4] H. Grari, S. Lamzabi, A. Azouaoui, and K. Zine-dine, “Cryptanalysis of Merkle-Hellman cipher using ant colony optimization,” IAES Int. J. Artif. Intell. (IJ-AI), vol. 10, no. 2, pp. 490-500, Jun. 2021, [Online]. Available: https://doi.org/10.11591/ijai.v10.i2.pp490-500.

[5] G. Anantharaman and J. Ding, “Camera zoom-based paper-pencil cipher encryption scheme atop Merkle-Hellman knapsack cryptosystem,” 2025.

[6] M. Zheng, Y. Feng, A. Nitaj, and Y. Pan, “Improving RSA cryptanalysis: Combining continued fractions and Coppersmith’s techniques,” 2025.

[7] G. Romeo, “Continued fractions in the field of p-adic numbers,” Bulletin of the American Mathematical Society, vol. 61, no. 2, p. 343, 2024.

[8] T. Sauer, Continued Fraction, Version 1.0, University of Passau, Mar. 26, 2019.

[9] A. D. Kumar and R. Sivaraman, “On some properties of fabulous fraction tree,” Mathematics and Statistics, vol. 10, no. 3, pp. 477-485, 2022.

[10] C. Elsner and C. R. M. Havens, Continued Fraction: A Modern and Classical Journey into the World of Siegel’s Continued Fraction. Cham, Switzerland: Springer, 2025.

[11] R. Z. Khalaf, H. B. Habib, and T. A. Jawad, “Attacking the Knapsack Public-key Cryptosystem,” Webology, vol. 19, no. 1, pp. 5302-5309, 2022.