A Lever Function to a New Codomain with Adequate Indeterminacy [*]

Shenghui Su [1, 2], Maozhi Xu [3], Shuwang Lü [4]

[1] College of Computers, Beijing University of Technology, Beijing 100124, P.R.China
[2] College of Information Engi., Yangzhou University, Yangzhou 225009, P.R.China
[3] School of Mathematics, Peking University, Beijing 100871, P.R.China
[4] Graduate School, Chinese Academy of Sciences, Beijing 100039, P.R.China

Abstract: The key transforms of the REESSE1+ cryptosystem is $C_i \equiv (A_i W^{\ell(i)})^{\delta}$ (% M) with $\ell(i) \in \Omega = \{5, 7, \ldots, 2n + 3\}$ for $i = 1, \ldots, n$, where $\ell(i)$ is called a lever function. In this paper, the authors give a new codomain $\Omega_{\pm} \subset \{\pm 5, \ldots, \pm(n + 4)\}$ and subjected to $x + y \neq 0\ \forall\ x, y \in \Omega_{\pm}$, where "$\pm x$" means the coexistence of "$+x$" and "$-x$", which indicates that $\Omega_{\pm}$ is indeterminate. Then, discuss the necessity and sufficiency of $\ell(.)$ to $\Omega_{\pm}$ for resisting continued fraction attack (CFA), prove indeterminacy and other properties of $\ell(.)$ to $\Omega_{\pm}$, illustrate the ineffectualness of CFA by using two examples which show that some conditions are only necessary but not sufficient for the counteraction of powers of W and W^{-1} even though $\Omega_{\pm} = \{5, \ldots, n + 4\}$ is selected and known, analyze the time complexities of CFA and root finding attack with guess, and expound a relation between a lever function and a random oracle. Our research manifests that $\ell(.)$ to $\Omega_{\pm}$ makes it generally impossible to extract a private key from a flat public key $C_i \equiv A_i W^{\ell(i)}$ (% M) for $i = 1, \ldots, n$ in polynomial time.

Keywords: Public key cryptosystem, Coprime sequence, Lever function, Continued fraction attack, Random oracle

1 Introduction

Theories of computational complexity such as the class P, the class NP, one-way functions, and trapdoor functions provide public key cryptosystems with foundation stones [1][2][3]. For instance, the RSA cryptosystem is founded on the integer factorization problem (IFP) [4], and the ElGamal cryptosystem is founded on the discrete logarithm problem (DLP) [5]. It appeals to people whether polynomial time algorithms for solving IFP and DLP on electronic computers exist or not since IFP and DLP are not proved NP-complete.

To $m = pq$ with p and q prime, if m is given, the values of p and q are determined. To $y \equiv g^x$ (% p) with g a generator of $(\mathbb{Z}_p^*, \cdot)$, if y is given, the value of x is also determined. Nevertheless there exists such a class of computational problems, which looks very ordinary, but leads indeterminacy into the analysis of a cryptosystem — a permutation problem for example.

In the REESSE1+ public key cryptosystem [6], the key transform is $C_i \equiv (A_i W^{\ell(i)})^{\delta}$ (%M) with $\ell(i) \in \Omega = \{5, 7, \ldots, 2n + 3\}$. The analysis in [6] shows that a REESSE1+ private key $(\{A_i\}, \{\ell(i)\}, W, \delta)$ is secure without doubt due to the existence of δ.

It is very interesting whether a flat REESSE1+ private key $(\{A_i\}, \{\ell(i)\}, W, \delta = 1)$ can be inferred from a related public key $\{C_i \mid C_i \equiv A_i W^{\ell(i)}$ (%M) with $\ell(i) \in \Omega_{\pm} \subset \{\pm 5, \ldots, \pm(n + 4)\}$ and subjected to $x + y \neq 0\ \forall\ x, y \in \Omega_{\pm}\}$or not, where "$\pm x$" means the coexistence of "$+x$" and "$-x$", which indicates that $\Omega_{\pm}$ is indeterminate.

In this paper, we will investigate the indeterminacy and other properties of the lever function $\ell(.)$ to a new codomain $\Omega_{\pm}$.

Throughout the paper, unless otherwise specified, $n \geq 80$ is the bit-lengthof a plaintext block or the item-length of a sequence, the sign % means "modulo", $\bar{M}$ does "$M - 1$" with M prime, lg$x$ denotes a logarithm of x to the base 2, $\neg x$ does the opposite of a bit x, Ᵽ does the maximal prime allowed in coprime sequences, $|x|$ does the absolute value of an integer x, $¦S¦$ does the size of a set S, and gcd(a, b) represents the greatest common divisor of two integers a and b. Without ambiguity, "% M" is usually omitted in expressions.

2 Flat REESSE1+ Encryption Scheme

To probe the indeterminacy of the lever function $\ell(.)$ to $\Omega_{\pm}$, let the parameter $\delta = 1$ in the key transform of REESSE1+.

We first observe the flat REESSE1+ with $\delta = 1$.

[*] This work is supported by MOST with Project 2007CB311100 and 2009AA01Z441.

2.1 Two Definitions

Definition 1: If $A_1, \ldots, A_n$ are n pairwise distinct positive integers such that $\forall\, A_i, A_j$ $(i \ne j)$, either $\gcd(A_i, A_j) = 1$ or $\gcd(A_i, A_j) = F \ne 1$ with $(A_i / F) \nmid A_k$ and $(A_j / F) \nmid A_k$ $\forall\, k \ne i, j \in [1, n]$, these integers are called a coprime sequence, denoted by $\{A_1, \ldots, A_n\}$, and shortly $\{A_i\}$.

Notice that the elements of a coprime sequence are not necessarily pairwise coprime, but a sequence whose elements are pairwise coprime must be a coprime sequence.

Property 1: Let $\{A_1, \ldots, A_n\}$ be a coprime sequence. If randomly select $m \in [1, n]$ elements from the sequence, and construct a subsequence (or a subset) $\{A x_1, \ldots, A x_m\}$, then the subset product $G = \prod_{i=1}^{m} A x_i$ $= A x_1 \ldots A x_m$ is uniquely determined, namely the mapping from $\{A x_1, \ldots, A x_m\}$ to G is one-to-one.

Refer to [6] for its proof.

Definition 2: The secret parameter $\ell(i)$ in the key transform of a public key cryptosystem over the prime field $\mathbb{GF}(M)$ is called a lever function, if it has the following features:

- $\ell(.)$ is an injection from the domain $\{1, \ldots, n\}$ to the codomain $\Omega \subset \{5, \ldots, \bar{M}\}$;
- the mapping between i and $\ell(i)$ is established randomly without an analytical expression;
- an attacker has to be faced with all the arrangements of n elements in Ω when extracting a related private key from a public key;
- the owner of a private key only needs to consider the accumulative sum of n elements in Ω when recovering a related plaintext from a ciphertext.

Obviously, there are the large amount of calculation on $\ell(.)$ at "a public terminal", and the small amount of calculation on $\ell(.)$ at "a private terminal".

Notice that ① in modular arithmetic, $-x$ represents $M - x$; ② the number of elements in Ω is not less than n; ③ considering the speed of decryption, the absolute values of all the elements should be comparatively small; ④ the lower limit 5 will make seeking the root W from $W^{\ell(i)} \equiv A_i^{-1} C_i$ (% M) face an unsolvable Galois group when $A_i \le 1201$ is guessed [7].

2.2 Key Generation Algorithm

We substitute $\Omega = \{5, 7, \ldots, 2n + 3\}$ with $\Omega_{\pm}$ in the flat REESSE1+.

Let $¦\Omega_{\pm}¦ = n$, $\Omega_{\pm} \subset \{\pm 5, \ldots, \pm(n + 4)\}$, and be subjected to $x + y \ne 0$ $\forall\, x, y \in \Omega_{\pm}$, where "$\pm x$" means the coexistence of "$+x$" and "$-x$". It indicates $\Omega_{\pm}$ is one of 2^n potential sets.

Let $|\Omega_{\pm}|$ be a set of absolute values of all the elements in $\Omega_{\pm}$.

Let $\Lambda = \{2, \ldots,$ Ᵽ$\}$, where Ᵽ $= 863, 937, 991$, or 1201 when $n = 80, 96, 112$, or 128.

This algorithm is employed by a certificate authority or the owner of a key pair.

S1: Randomly produce pairwise coprime $A_1, \ldots, A_n \in \Lambda$.

S2: Find a prime $M > \prod_{i=1}^{n} A_i$ making $q^2 \mid \bar{M}$ $\forall$ prime $q \in |\Omega_{\pm}|$.

S3: Stochastically pick the integer $W \in (1, \bar{M})$.

S4: Randomly produce pairwise distinct $\ell(1), \ldots, \ell(n) \in \Omega_{\pm}$.

S5: Compute $C_i \leftarrow A_i W^{\ell(i)}$ % M for $i = 1, \ldots, n$.

At last, regard $(\{C_i\}, M)$ as a public key, and $(\{A_i\}, \{\ell(i)\}, W, M)$ as a private key.

2.3 Encryption Algorithm

Assume that $(\{C_i\}, M)$ is a public key, and $b_1 \ldots b_n$ is an n-bit plaintext block or symmetric key.

S1: Set $\bar{G} \leftarrow 1$, $i \leftarrow 1$.

S2: If $b_i = 1$, let $\bar{G} \leftarrow \bar{G} C_i$ % M.

S3: Let $i \leftarrow i + 1$.

S4: If $i \le n$, goto S2; else end.

So, the ciphertext $\bar{G} \equiv \prod_{i=1}^{n} C_i^{b_i}$ (% M) is obtained.

Definition 3: Given $\bar{G}$, $\{C_i\}$, and M, seeking $b_1 \ldots b_n$ from $\bar{G} \equiv \prod_{i=1}^{n} C_i^{b_i}$ (% M) is called a subset product problem, shortly SPP [6][8].

Notice that when $\lceil \lg M \rceil < 1024$, let g be a generator, $\bar{G} \equiv g^u$ (% M), $C_1 \equiv g^{v_1}$ (% M), $\ldots$, $C_n \equiv g^{v_n}$ (% M), and then the subset product problem $\bar{G} \equiv \prod_{i=1}^{n} C_i^{b_i}$ (% M) is degenerated to a subset sum problem $u \equiv b_1 v_1 + \ldots + b_n v_n$ (% $\bar{M}$) of density less than 1, which indicates $\bar{G}$ is not robust.

Therefore, compared with REESSE1+, the flat REESSE1+ has only theoretical sense, and has no practical value.

2.4 Decryption Algorithm

Assume that ($\{A_i\}$, $\{\ell(i)\}$, W, M) is a related private key, and $\bar{G}$ is a ciphertext.

```
S1: Set $X_0 \leftarrow \bar{G}$, $X_1 \leftarrow X_0$, $h \leftarrow 0$.
S2: Set $b_1 \ldots b_n \leftarrow 0$, $G \leftarrow X_h$, $h \leftarrow \neg h$, $i \leftarrow 1$.
S3: If $A_i \mid G$, let $b_i \leftarrow 1$, $G \leftarrow G / A_i$.
S4: Let $i \leftarrow i + 1$.
    If $i \le n$ and $G \ne 1$, goto S3.
S5: If $G \ne 1$, do $X_h \leftarrow X_h W^{(-1)^h} \% M$, goto S2;
    else end.
```

So, the original plaintext block or symmetric key $b_1 \ldots b_n$ is recovered.

Notice that only if $\bar{G}$ is a true ciphertext, can this algorithm always terminate normally.

3 Necessity of the Lever Function $\ell(.)$

We will discuss the necessity and sufficiency of the lever function $\ell(.)$ to $\Omega_{\pm}$ for resisting continued fraction attack.

The necessity of the lever function $\ell(.)$ means that if a flat REESSE1+ private key is secure, $\ell(.)$ as a one-to-one function must exist in the key transform. The equivalent contrapositive assertion is that if $\ell(.)$ as a one-to-one function does not exist (namely the value of every $\ell(i)$ equals a fixed integer $\underline{k}$ in the key transform), the flat REESSE1+ private key will be insecure.

Theorem 1: If α is an irrational number, r, $s > 0$ are two integers, and r / s is a rational in the lowest terms such that $|\alpha - r / s| < 1 / (2s^2)$, then r / s is a convergent of the simple continued fraction expansion of α.

Refer to [9] for the proof.

Notice that theorem 1 also holds when α is a rational number [9].

For a public key cryptosystem, if a private key is insecure, a plaintext must be insecure. Hence, the security of a private key is most foundational [10].

Property 2: Let $\underline{k} \in [1, \overline{M}]$ be any integer. If the key transform of the flat REESSE1+ cryptosystem is $C_i \equiv A_i W^{\underline{k}}$ (% M) for $i = 1, \ldots, n$, a flat REESSE1+ private key ($\{A_1, \ldots, A_n\}$, $W^{\underline{k}}$) is insecure.

Proof.

Assume that $\ell(1) = \ldots = \ell(n) = \underline{k}$, where $\underline{k}$ is a fixed integer. Then the key transform becomes as

$$C_i \equiv A_i W^{\underline{k}} \ (\% \ M),$$

and especially when $\underline{k} = 1$, $C_i \equiv A_i W$ (% M) for $i = 1, \ldots, n$.

Since $(\mathbb{Z}_M^*, \cdot)$ is an Abelian group [7], of course, there is

$$C_i^{-1} \equiv (A_i W^{\underline{k}})^{-1} \ (\% \ M).$$

$\forall x \in [1, n - 1]$, let

$$G_z \equiv C_x C_n^{-1}.$$

Substituting $A_x W^{\underline{k}}$ and $A_n W^{\underline{k}}$ respectively for C_x and C_n in G_z yields

$$G_z \equiv A_x W^{\underline{k}} (A_n W^{\underline{k}})^{-1} \ (\% \ M)$$
$$A_n G_z \equiv A_x \ (\% \ M)$$
$$A_n G_z - LM = A_x,$$

where L is a positive integer.

The either side of the equation is divided by $A_n M$ gives

$$G_z / M - L / A_n = A_x / (A_n M). \tag{1}$$

Due to $M > \prod_{i=1}^{n} A_i$ and $A_i \ge 2$, there is

$$G_z / M - L / A_n < A_x / (A_n \textstyle\prod_{i=1}^{n} A_i)$$
$$= A_x / (A_n^{\,2} \textstyle\prod_{i=1}^{n-1} A_i) \le 1 / (2^{n-2} A_n^{\,2}),$$

that is,

$$G_z / M - L / A_n < 1 / (2^{n-2} A_n^{\,2}). \tag{2}$$

Evidently, as $n > 2$, there is

$$G_z / M - L / A_n < 1 / (2 A_n^{\,2}). \tag{2$'$}$$

In terms of theorem 1, L / A_n is a convergent of the continued fraction of G_z / M.

Thus, L / A_n, namely A_n may be determined by (2′) in polynomial time since the length of the continued fraction will not exceed $\lceil \lg M \rceil$, and further $W^{\underline{k}} \equiv C_n A_n^{-1}$ (% M) may be computed, which indicates the original coprime sequence $\{A_1, \ldots, A_n\}$ with $A_i \le \grave{\mathbf{P}}$ can almost be recovered. □

Because W in every C_i has the same exponent, and the powers of W and W^{-1} in any $C_x C_n^{-1}$ % M always counteract each other, when $\ell(i)$ is a fixed integer $\underline{k}$, there does not exist the indeterministic reasoning problem.

It should be noted that when a convergent of the continued fraction of G_z / M satisfies (2′), the some subsequent convergents also possibly satisfies (2′), and if so, it will bring about the nonuniqueness of value of A_n. Therefore, we say that $\{A_1, …, A_n\}$ with $A_i \le$ **Ᵽ** can almost be recovered.

The above analysis manifests that when every $\ell(i)$ is a fixed integer $\underline{k}$, a related private key can be deduced from a public key, and further a related plaintext can be inferred from a ciphertext. Thus, the one-to-one lever function $\ell(.)$ is necessary to the security of a flat REESSE1+ private key.

4 Sufficiency of the Lever Function $\ell(.)$

The sufficiency of the lever function $\ell(.)$ for resisting continued fraction attack means that when $\ell(1), …, \ell(n) \in \Omega_\pm$ are pairwise distinct, the continued fraction attack is utterly ineffectual.

This section will show that the continued fraction attack do not necessarily threaten $C_i \equiv A_i W^{\ell(i)}$ (% M) even though when $\Omega_\pm = \{5, …, n + 4\}$ is selected and known to adversaries adventitiously, and is utterly ineffectual when it is only known that $\Omega_\pm \subset \{\pm 5, …, \pm(n + 4)\}$ and subjected to $x + y \ne 0 \ \forall\ x, y \in \Omega_\pm$ is indeterminate.

4.1 Continued Fraction Attack Is Faced with Indeterminacy and Insufficiency

According to Section 2.2, if the lever function $\ell(.)$ exists, we have

$$C_i \equiv A_i W^{\ell(i)} \ (\%\ M),$$

where $A_i \in \Lambda = \{2, …,$ **Ᵽ**$\}$ and $\ell(i) \in \Omega_\pm \subset \{\pm 5, …, \pm(n + 4)\}$ for $i = 1, …, n$.

4.1.1 Indeterminacy of $\ell(.)$

The lever function $\ell(.)$ brings adversaries at least two difficulties:

- No method by which one can directly judge whether the power of W in $C_{x_1} … C_{x_m}$ is counteracted by the power of W^{-1} in $(C_{y_1} … C_{y_h})^{-1}$ or not;
- No criterion by which the presupposition of an indeterministic reasoning can be verified in polynomial time.

The indeterministic reasoning based on continued fractions means that ones first presuppose that the exponents on the parameter W and the inverse W^{-1} counteract each other in a product, and then judge whether the presupposition holds or not by the consequence.

According to Section 3, first select $m \in [1, n - 1]$ elements and $h \in [1, n - m]$ other elements from $\{C_1, …, C_n\}$. Let

$$G_x \equiv C_{x_1} … C_{x_m} \ (\%\ M),$$
$$G_y \equiv C_{y_1} … C_{y_h} \ (\%\ M),$$

where $C_{x_i} \ne C_{y_j}$ for $i \in [1, m]$ and $j \in [1, h]$.

Let

$$G_z \equiv G_x G_y^{-1} \ (\%\ M).$$

Since $\{\ell(1), …, \ell(n)\}$ is any arrangement of n elements in $\Omega_\pm$, it is impossible to predicate that G_z does not contain the factor W or W^{-1}. For a further deduction, we have to *presuppose* that the power of W in G_x is exactly counteracted by the power of W^{-1} in G_y^{-1}, and then,

$$G_z \equiv (A_{x_1} … A_{x_m})(A_{y_1} … A_{y_h})^{-1} \ (\%\ M)$$
$$G_z (A_{y_1} … A_{y_h}) \equiv A_{x_1} … A_{x_m} \ (\%\ M)$$
$$G_z (A_{y_1} … A_{y_h}) - L M = A_{x_1} … A_{x_m}$$
$$G_z / M - L / (A_{y_1} … A_{y_h}) = (A_{x_1} … A_{x_m}) / (M A_{y_1} … A_{y_h}),$$

where L is a positive integer.

Denoting the product $A_{y_1} … A_{y_h}$ by $\bar{A}_y$ yields

$$G_z / M - L / \bar{A}_y = (A_{x_1} … A_{x_m}) / (M \bar{A}_y). \tag{3}$$

Due to $M > \prod_{i=1}^{n} A_i$ and $A_i \ge 2$, we have

$$G_z / M - L / \bar{A}_y < 1 / (2^{n-m-h} \bar{A}_y^{\,2}). \tag{4}$$

Obviously, when $n > m + h$, (4) may have a variant, namely

$$G_z / M - L / \bar{A}_y < 1 / (2 \bar{A}_y^{\,2}). \tag{4′}$$

Notice that when $n = m + h$, if $M > 2(\prod_{i=1}^{n} A_i)$, (4′) still holds.

Especially, when $n > 3$, $h = 1$, and $m = 2$, there exists

$$G_z / M - L / A_{y_1} < 1 / (2^{n-3} {A_{y_1}}^2) < 1 / (2 {A_{y_1}}^2). \tag{4″}$$

Obviously, as a discriminant, (4) is stricter than (4′) and (4″). (4″) is consistent with theorem 1.

Property 3*:* Let $h + m \le n$. If $\ell(x_1) + \ldots + \ell(x_m) = \ell(y_1) + \ldots + \ell(y_h)$, the subset product $\bar{A}_y = A_{y_1} \ldots A_{y_h}$ in (4′) will be found in polynomial time.

Proof.

$\ell(x_1) + \ldots + \ell(x_m) = \ell(y_1) + \ldots + \ell(y_h)$ means that the exponent on W in $C_{x_1} \ldots C_{x_m}$ is counteracted by the exponent on W^{-1} in $(C_{y_1} \ldots C_{y_h})^{-1}$, and thus (4′) holds.

In terms of theorem 1, $L / \bar{A}_y$ is inevitably a convergent of the continued fraction of G_z / M, and thus $\bar{A}_y = A_{y_1} \ldots A_{y_h}$ can be found in polynomial time. □

Notice that (4′) is insufficient for $\ell(x_1) + \ldots + \ell(x_m) = \ell(y_1) + \ldots + \ell(y_h)$ (see Property 7), and $\bar{A}_y$ is faced with nonuniqueness because there may possibly exist several convergents of the continued fraction of G_z / M which all satisfy (4′).

Property 4* (Indeterminacy of $\boldsymbol{\ell}$(.)):* Let $h + m \le n$. $\forall x_1, \ldots, x_m, y_1, \ldots, y_h \in [1, n]$, when $\ell(x_1) + \ldots + \ell(x_m) \ne \ell(y_1) + \ldots + \ell(y_h)$,

① there always exist

$$C_{x_1} \equiv A'_{x_1} W'^{\ell(x_1)}, \ldots, C_{x_m} \equiv A'_{x_m} W'^{\ell(x_m)},$$
$$C_{y_1} \equiv A'_{y_1} W'^{\ell(y_1)}, \ldots, C_{y_h} \equiv A'_{y_h} W'^{\ell(y_h)} \ (\% \ M),$$

such that $\ell'(x_1) + \ldots + \ell'(x_m) \equiv \ell'(y_1) + \ldots + \ell'(y_h)$ ($\%$ $\bar{\boldsymbol{M}}$) with $A'_{y_1} \ldots A'_{y_h} \le \boldsymbol{Ƥ}^h$;

② probability that $C_{x_1}, \ldots, C_{x_m}, C_{y_1}, \ldots, C_{y_h}$ make (4) with $A'_{y_1} \ldots A'_{y_h} \le \boldsymbol{Ƥ}^h$ hold is roughly $1 / 2^{n-m-h-1}$.

Proof.

Because $A'_{y_1} \ldots A'_{y_h}$ need be observed, the constraint $A'_{y_1} \ldots A'_{y_h} \le \boldsymbol{Ƥ}^h$ is demanded while because $A'_{x_1}, \ldots, A'_{x_m}$ need not be observed, the constraints $A'_{x_1} \le \boldsymbol{Ƥ}, \ldots, A'_{x_m} \le \boldsymbol{Ƥ}$ are not demanded.

① Let $\bar{O}_\mathrm{d}$ be an oracle on a discrete logarithm.

Suppose that $W' \in [1, \bar{\boldsymbol{M}}]$ is a generator of $(\mathbb{Z}_M^*, \cdot)$.

Let $\mu = \ell'(y_1) + \ldots + \ell'(y_h)$. In terms of group theories, $\forall A'_{y_1}, \ldots, A'_{y_h} \in [2, \boldsymbol{Ƥ}]$ which need not be pairwise coprime, the equation

$$C_{y_1} \ldots C_{y_h} \equiv A'_{y_1} \ldots A'_{y_h} W'^{\mu} \ (\% \ M)$$

in μ has a solution. μ may be obtained through $\bar{O}_\mathrm{d}$.

$\forall \ \ell'(y_1), \ldots, \ell'(y_{h-1}) \in [1, \bar{\boldsymbol{M}}]$, let $\ell'(y_h) \equiv \mu - (\ell'(y_1) + \ldots + \ell'(y_{h-1}))$ ($\%$ $\bar{\boldsymbol{M}}$).

Similarly, $\forall \ \ell'(x_1), \ldots, \ell'(x_{m-1}) \in [1, \bar{\boldsymbol{M}}]$, let $\ell'(x_m) \equiv \mu - (\ell'(x_1) + \ldots + \ell'(x_{m-1}))$ ($\%$ $\bar{\boldsymbol{M}}$).

Further, from $C_{x_1} \equiv A'_{x_1} W'^{\ell(x_1)}, \ldots, C_{x_m} \equiv A'_{x_m} W'^{\ell(x_m)}$ ($\%$ M), we can obtain a tuple $(A'_{x_1}, \ldots, A'_{x_m})$, where $A'_{x_1}, \ldots, A'_{x_m} \in (1, M)$, and $\ell'(x_1) + \ldots + \ell'(x_m) \equiv \ell'(y_1) + \ldots + \ell'(y_h)$ ($\%$ $\bar{\boldsymbol{M}}$).

Thus, Property 4.1 is proven.

② Let $G_z \equiv C_{x_1} \ldots C_{x_m} (C_{y_1} \ldots C_{y_h})^{-1}$ ($\%$ M). Then in terms of Property 4.1, there is

$$C_{x_1} \ldots C_{x_m} (C_{y_1} \ldots C_{y_h})^{-1} \equiv A'_{x_1} \ldots A'_{x_m} W'^{\ell(x_1) + \ldots + \ell(x_m)} (A'_{y_1} \ldots A'_{y_h} W'^{\ell(y_1) + \ldots + \ell(y_h)})^{-1}$$

with $\ell'(x_1) + \ldots + \ell'(x_m) \equiv \ell'(y_1) + \ldots + \ell'(y_h)$ ($\%$ $\bar{\boldsymbol{M}}$).

Further, there is

$$A'_{x_1} \ldots A'_{x_m} \equiv C_{x_1} \ldots C_{x_m} (C_{y_1} \ldots C_{y_h})^{-1} A'_{y_1} \ldots A'_{y_h} \ (\% \ M).$$

The above equation manifests that the values of W' and $(\ell'(y_1) + \ldots + \ell'(y_h)$ or $\ell'(x_1) + \ldots + \ell'(x_m))$ do not influence the value of the product $A'_{x_1} \ldots A'_{x_m}$.

If $A'_{y_1} \ldots A'_{y_h} \in [2^h, \boldsymbol{Ƥ}^h]$ changes, the product $A'_{x_1} \ldots A'_{x_m}$ also changes, where $A'_{y_1} \ldots A'_{y_h}$ is a composite integer. Therefore, $\forall \ x_1, \ldots, x_m, y_1, \ldots, y_h \in [1, n]$, the number of potential values of $A'_{x_1} \ldots A'_{x_m}$ is roughly $(\boldsymbol{Ƥ}^h - 2^h + 1)$.

Let $M = q \boldsymbol{Ƥ}^m (A'_{y_1} \ldots A'_{y_h}) 2^{n-m-h}$, where q is a rational number.

According to (3),

$$\begin{aligned} G_z / M - L / (A'_{y_1} \ldots A'_{y_h}) &= (A'_{x_1} \ldots A'_{x_m}) / (M A'_{y_1} \ldots A'_{y_h}) \\ &= (A'_{x_1} \ldots A'_{x_m}) / (q \boldsymbol{Ƥ}^m 2^{n-m-h} (A'_{y_1} \ldots A'_{y_h})^2). \end{aligned}$$

When $A'_{x_1} \ldots A'_{x_m} \le q \boldsymbol{Ƥ}^m$, there is

$$\begin{aligned} G_z / M - L / (A'_{y_1} \ldots A'_{y_h}) &\le q \boldsymbol{Ƥ}^m / (q \boldsymbol{Ƥ}^m 2^{n-m-h} (A'_{y_1} \ldots A'_{y_h})^2) \\ &= 1 / (2^{n-m-h} (A'_{y_1} \ldots A'_{y_h})^2), \end{aligned}$$

which satisfies (4).

Assume that the value of $A'_{x_1} \ldots A'_{x_m}$ distributes uniformly on the interval $(1, M)$. If $A'_{y_1} \ldots A'_{y_h}$ is a certain concrete value, the probability that $A'x_1 \ldots A'x_m$ makes (4) hold at a specific value of $A'y_1 \ldots A'y_h$ is

$$q Ƥ^m / M = q Ƥ^m / (q Ƥ^m (A'y_1 \ldots A'y_h) 2^{n-m-h})$$
$$= 1 / ((A'y_1 \ldots A'y_h) 2^{n-m-h}).$$

In fact, it is possible that $A'y_1 \ldots A'y_h$ take every value in the interval $[2^h, Ƥ^h]$ when $Cx_1, \ldots, Cx_m, Cy_1, \ldots, Cy_h$ are fixed. Thus, the probability that $A'x_1 \ldots A'x_m$ makes (4) hold is

$$\begin{aligned} P_{\forall x_1, \ldots, x_m, y_1, \ldots, y_h \in [1, n]} &= (1/(2^{n-m-h}))(1/2^h + 1/(2^h+1) + \ldots + 1/Ƥ^h) \\ &> (1/2^{n-m-h})(2(Ƥ^h - 2^h + 1)/(Ƥ^h + 2^h)) \\ &= (Ƥ^h - 2^h + 1)/(2^{n-m-h-1}(Ƥ^h + 2^h)) \\ &\approx 1/2^{n-m-h-1}. \end{aligned}$$

Obviously, the larger $m + h$ is, the larger the probability is, and the smaller n is, the larger the probability is also. □

***Property 5**:* Let $h + m \le n$. $\forall\, x_1, \ldots, x_m, y_1, \ldots, y_h \in [1, n]$, when $\ell(x_1) + \ldots + \ell(x_m) = \ell(y_1) + \ldots + \ell(y_h)$, the probability that another $\bar{A}_y$ makes (4) with $\bar{A}_y \le Ƥ^h$ hold is roughly $1/2^{n-m-h-1}$.

Proof.

Let

$$G_x \equiv Cx_1 \ldots Cx_m \equiv (Ax_1 \ldots Ax_m)\, W^{\ell(x_1) + \ldots + \ell(x_m)}\ (\%\ M),$$
$$G_y \equiv Cy_1 \ldots Cy_h \equiv (Ay_1 \ldots Ay_h)\, W^{\ell(y_1) + \ldots + \ell(y_h)}\ (\%\ M).$$

Due to $\ell(x_1) + \ldots + \ell(x_m) = \ell(y_1) + \ldots + \ell(y_h)$, there is

$$G_z \equiv G_x G_y^{-1} \equiv (Ax_1 \ldots Ax_m)(Ay_1 \ldots Ay_h)^{-1} \equiv (Ax_1 \ldots Ax_m) \bar{A}_y^{-1}\ (\%\ M).$$

According to the derivation of (4″), $\bar{A}_y$ will occur in a convergent of the continued fraction of G_z / M.

Let $p_1 / q_1, \ldots, p_x / q_x = L / \bar{A}_y, p_{x+1} / q_{x+1}, \ldots, p_t / q_t$ be the convergent sequence of the continued fraction of G_z / M, where $t \le \lceil \lg M \rceil$.

Because of $G_z / M - L / \bar{A}_y < 1/(2^{n-m-h} \bar{A}_y^2)$, it will lead

$$|G_z / M - p_{x+1} / q_{x+1}| < 1/(2^{n-m-h} q_{x+1}^2) \text{ with } q_{x+1} \le Ƥ^h,$$
$$\ldots\ldots, \text{ or}$$
$$|G_z / M - p_t / q_t| < 1/(2^{n-m-h} q_t^2) \text{ with } q_t \le Ƥ^h$$

to probably hold, and in terms of Property 4.2, the probability is roughly $1/2^{n-m-h-1}$.

Notice that in this case, there is $\ell'(x_1) + \ldots + \ell'(x_m) \equiv \ell'(y_1) + \ldots + \ell'(y_h)$ (% $\bar{M}$) with $A'y_1 \ldots A'y_h \le Ƥ^h$, where $\ell'(x_1), \ldots, \ell'(x_m), \ell'(y_1), \ldots, \ell'(y_h)$ satisfy

$$Cx_1 \equiv A'x_1 W'^{\ell(x_1)}, \ldots, Cx_m \equiv A'x_m W'^{\ell(x_m)}, Cy_1 \equiv A'y_1 W'^{\ell(y_1)}, \ldots, Cy_h \equiv A'y_h W'^{\ell(y_h)}\ (\%\ M).$$

End. □

Property 5 illuminates that the nonuniqueness of $\bar{A}_y$, namely there may exist the disturbance of $\bar{A}_y$. The smaller $m + h$ is, the less the disturbance is.

4.1.2 Some Conditions Are Only Necessary But Not Sufficient

***Property 6**:* (4) is necessary but not sufficient for $\ell(x_1) + \ldots + \ell(x_m) = \ell(y_1) + \ldots + \ell(y_h)$ with $x_1, \ldots, x_m, y_1, \ldots, y_h \in [1, n]$, namely for the powers of W and W^{-1} in G_z to counteract each other.

Proof. Necessity:

Suppose that $\ell(x_1) + \ldots + \ell(x_m) = \ell(y_1) + \ldots + \ell(y_h)$.

Let $\{C_1, \ldots, C_n\}$ be a public key sequence, and M be a modulus, where $C_i \equiv A_i W^{\ell(i)}$ (% M).

Let $G_x \equiv Cx_1 \ldots Cx_m$ (% M), $G_y \equiv Cy_1 \ldots Cy_h$ (% M), and $G_z \equiv G_x G_y^{-1}$ (% M).

Further, $G_z \equiv (Ax_1 \ldots Ax_m)(Ay_1 \ldots Ay_h)^{-1}$ (% M).

Denote the product $Ay_1 \ldots Ay_h$ by $\bar{A}_y$. Similar to Section 4.1.1, we have

$$G_z / M - L / \bar{A}_y < 1/(2^{n-m-h} \bar{A}_y^2),$$

Namely (4) holds.

Insufficiency:

Suppose that (4) holds.

The contrapositive of the proposition that if (4) holds, $\ell(x_1) + \ldots + \ell(x_m) = \ell(y_1) + \ldots + \ell(y_h)$ holds is that if $\ell(x_1) + \ldots + \ell(x_m) \ne \ell(y_1) + \ldots + \ell(y_h)$, (4) does not hold.

Hence, we need to prove that when $\ell(x_1) + \ldots + \ell(x_m) \ne \ell(y_1) + \ldots + \ell(y_h)$, (4) still holds.

In terms of Property 4.2, when $\ell(x_1) + \ldots + \ell(x_m) \ne \ell(y_1) + \ldots + \ell(y_h)$, the (4) holds with the probability $1/2^{n-m-h-1}$, which reminds us that when $\{C_1, \ldots, C_n\}$ is generated, some subsequences in the forms $\{Cx_1, \ldots, Cx_m\}$ and $\{Cy_1, \ldots, Cy_h\}$ which are verified to satisfy (4) with $\ell(x_1) + \ldots + \ell(x_m) \ne \ell(y_1) + \ldots + \ell(y_h)$ can always be found beforehand through adjusting the values of W and some elements in $\{A_1,$

$A_2, \ldots, A_i\}$ or $\{\ell(1), \ell(2), \ldots, \ell(n)\}$.

Hence, the (4) is not sufficient for $\ell(x_1) + \ldots + \ell(x_m) = \ell(y_1) + \ldots + \ell(y_h)$. □

Property 7: (4′) is necessary but not sufficient for $\ell(x_1) + \ldots + \ell(x_m) = \ell(y_1) + \ldots + \ell(y_h)$ with $x_1, \ldots, x_m, y_1, \ldots, y_h \in [1, n]$, for the powers of W and W^{-1} in G_z to counteract each other.

Proof.

Because (4′) is derived from (4), and Property 6 holds, naturally Property 7 holds. □

Property 8: Let $m = 2$ and $h = 1$. $\forall\, x_1, x_2, y_1 \in [1, n]$, when $\ell(x_1) + \ell(x_2) \neq \ell(y_1)$,

① there always exist

$$C_{x_1} \equiv A'_{x_1} W'^{\ell'(x_1)},\ C_{x_1} \equiv A'_{x_2} W'^{\ell'(x_2)},\ C_{y_1} \equiv A'_{y_1} W'^{\ell'(y_1)}\ (\%\ M),$$

such that $\ell'(x_1) + \ell'(x_2) \equiv \ell'(y_1)$ ($\%\ \bar{M}$) with $A'_{y_1} \leq Ƥ$;

② $C_{x_1}, C_{x_2}, C_{y_1}$ make (4″) with $A'_{y_1} \leq Ƥ$ hold in all probability.

Proof.

① It is similar to the proving process of Property 4.1.

② Let

$$G_z \equiv C_{x_1} C_{x_2} C_{y_1}^{-1} \equiv A'_{x_1} A'_{x_2} W'^{\ell'(x_1)+\ell'(x_2)} (A'_{y_1} W'^{\ell'(y_1)})^{-1}\ (\%\ M)$$

with $\ell'(x_1) + \ell'(x_2) \equiv \ell'(y_1)$ ($\%\ \bar{M}$).

Further, there is $A'_{x_1} A'_{x_2} \equiv C_{x_1} C_{x_2} C_{y_1}^{-1} A'_{y_1}$ ($\% M$).

It is easily seen from the above equations that the values of W' and $\ell'(y_1)$ do not influence the value of $(A'_{x_1} A'_{x_2})$.

If $A'_{y_1} \in [2, Ƥ]$ changes, $A'_{x_1} A'_{x_2}$ also changes. Thus, $\forall\, x_1, x_2, y_1 \in [1, n]$, the number of potential values of $A'_{x_1} A'_{x_2}$ is $Ƥ - 1$.

Let $M = 2qƤ^2 A'_{y_1}$, where q is a rational number.

According to (3),

$$\begin{aligned} G_z / M - L / A'_{y_1} &= A'_{x_1} A'_{x_2} / (M A'_{y_1}) \\ &= A'_{x_1} A'_{x_2} / (2qƤ^2 A'^{2}_{y_1}). \end{aligned}$$

When $A'_{x_1} A'_{x_2} \leq qƤ^2$, there is

$$\begin{aligned} G_z / M - L / A'_{y_1} &\leq qƤ^2 / (2qƤ^2 A'^{2}_{y_1}) \\ &= 1 / (2A'^{2}_{y_1}), \end{aligned}$$

which satisfies (4″).

Assume that the value of $A'_{x_1} A'_{x_2}$ distributes uniformly on $(1, M)$. Then, the probability that $A'_{x_1} A'_{x_2}$ makes (4″) hold is

$$\begin{aligned} P_{\forall x_1, x_2, y_1 \in [1, n]} &= (qƤ^2 / (2qƤ^2))(1/2 + \ldots + 1/Ƥ) \\ &\geq (1/2)(2(Ƥ - 1)/(Ƥ + 2)) \\ &= 1 - 3/(Ƥ + 2). \end{aligned}$$

Apparently, $P_{\forall x_1, x_2, y_1 \in [1, n]}$ is very large, and especially when $Ƥ$ is pretty large, it is close to 1. □

According to Property 8.2, for a certain C_{y_1} and $\forall\, C_{x_1}, C_{x_2} \in \{C_1, \ldots, C_n\}$, attack by (4″) will produce roughly $n^2/2$ possible values of A_{y_1}, including the repeated, while attack by (4) may filter out most of the disturbing data of A_{y_1}. Because every $A_{y_1} \leq Ƥ < n^2/2$ in REESSE1, the number of potential values of A_{y_1} is at most $Ƥ$ in terms of the pigeonhole principle, which indicates the running time of discriminating the original coprime sequence from the values of $A_1, \ldots$, the values of A_n is $O(Ƥ^n)$.

Property 9: (4″) is necessary but not sufficient for $\ell(x_1) + \ell(x_2) = \ell(y_1)$ with $x_1, x_2, y_1 \in [1, n]$, namely for the powers of W and W^{-1} in G_z to counteract each other.

Proof.

Because (4″) is derived from (4), and Property 6 holds, naturally Property 9 holds. □

It should be noted that Property 2, 3, …, 9 do not depend on the selection of codomain of the lever function $\ell(.)$, namely regardless of selecting the old Ω or the new $\Omega_{\pm}$, Property 2, 3, …, 9 still hold.

4.2 Discussion of the Two Discrepant Cases

The cases of $h = 1$ and $h \neq 1$ should be treated distinguishingly.

4.2.1 Case of *h* = 1

The $h = 1$ means that $\bar{A}_y = A_{y_1}$. If $\bar{A}_y$ is determined, a certain A_{y_1} might be exposed directly. A single A_{y_1} may be either prime or composite, and thus “whether A_{y_1} is prime” may not be regarded as the criterion of the powers of W and W^{-1} counteracting each other.

If take $m = 2$ and $h = 1$, in terms of Property 4.2, the probability $P_{\forall x_1, x_2, y_1 \in [1, n]}$ that $A'_{x_1} A'_{x_2}$ makes (4) hold is roughly $1/2^{n-4}$, and the number of rationals formed as G_z / M which lead (4) to hold is roughly $n^3 / 2^{n-4}$ when the interval $[1, n]$ is traversed by x_1, x_2, y_1 separately. Notice that $P_{\forall x_1, x_2, y_1 \in [1, n]}$ is with respect to (4), but not with respect to (4′) or (4″).

Notice that due to $\Omega_\pm \subset \{\pm 5, \ldots, \pm(n + 4)\}$, the value of $\ell(x_1) + \ell(x_2)$ — $(-5) + 6 = 1$ for example does not necessarily occur in $\Omega_\pm$.

In what follows, we validate Property 6 and 8 with two examples when $m = 2$, $h = 1$. Especially we simply select $\Omega_\pm = \{5, \ldots, n + 4\}$ for explaining the ineffectuality of continued fraction attack.

Example 1:

It will illustrate the ineffectuality of continued fraction attack by (4).

Assume that the bit-length of a plaintext block is $n = 6$.

Let $\{A_i\} = \{11, 10, 3, 7, 17, 13\}$ and $\Omega_\pm = \{5, 6, 7, 8, 9, 10\}$.

Let $M = 510931 > 11 \times 10 \times 3 \times 7 \times 17 \times 13$.

Stochastically pick $W = 17797$, and

$$\ell(1) = 9,\ \ell(2) = 6,\ \ell(3) = 10,\ \ell(4) = 5,\ \ell(5) = 7,\ \ell(6) = 8.$$

From $C_i \equiv A_i W^{\ell(i)}$ (% M), we obtain

$\{C_i\} = \{113101, 79182, 175066, 433093, 501150, 389033\}$.

Stochastically pick $x_1 = 2$, $x_2 = 6$, and $y_1 = 5$.

Notice that there is $\ell(5) \neq \ell(2) + \ell(6)$.

Compute

$$G_z \equiv C_2 C_6 C_5^{-1} \equiv 79182 \times 389033 \times 434038 \equiv 342114 \text{ (\% 510931)}.$$

Presuppose that the power of W in $C_2 C_6$ is just counteracted by the power of W^{-1} in C_5^{-1}, and then

$$342114 \equiv A_2 A_6 A_5^{-1} \text{ (\% 510931)}.$$

According to (3),

$$342114 / 510931 - L / A_5 = A_2 A_6 / (510931 A_5).$$

It follows that the continued fraction expansion of $342114 / 510931$ equals

$$1 / (1 + 1 / (2 + 1 / (37 + 1 / (1 + 1 / (2 + \ldots + 1 / 4))))),$$

where the denominators $1 = a_1$, $2 = a_2$, $37 = a_3$, … .

Heuristically let

$$L / A_5 = 1 / (1 + 1 / 2) = 2 / 3,$$

which indicates it is probable that $A_5 = 3$. Further,

$$342114 / 510931 - 2 / 3 = 0.002922769 < 1 / (2^3 \times 3^2) = 0.013888889,$$

which satisfies (4). Then $A_5 = 3$ is deduced, which is in direct contradiction to factual $A_5 = 17$, so it is impossible that (4) may serve as a sufficient condition.

Meantime, in Example 1, we observe $a_2 = 2$ and $a_3 = 37$, and the increase from a_2 to a_3 should be sharp. However, even though the case is this, the continued fraction attack by (4) fails.

Example 2:

It will illustrate the ineffectuality of a continued fraction attack by a discriminant relevant to (4″).

The following Algorithm 1 which is evolved from the analysis task in [11] describes a continued fraction attack on a flat REESSE1+ private key. The attack rests on the *Discriminant* ($q_s \Delta < q_{s+1}$) with ($q_s < \max A$). In terms of [11], the *Discriminant* is derived from (4″), seemingly stricter than (4″), and intended to uniquely determine A_{y_1}.

```
Algorithm 1:
Let $p_1, \ldots, p_n$ be the first $n$ primes in the natural set $\mathbb{N}$.
S1: Set $\Delta \leftarrow (M / (2\prod_{i=n-2}^{u} p_i))^{1/2}$, $\max A \leftarrow M / \prod_{i=1}^{n-1} p_i$,
      where $u$ meets $\prod_{i=1}^{u} p_i < M \le \prod_{i=1}^{u+1} p_i$.
S2: For ($x_1 \leftarrow 1, x_1 \le n, x_1 + +$)
      For ($x_2 \leftarrow 1, x_2 \le n, x_2 + +$)
      For ($y_1 \leftarrow 1, y_1 \le n, y_1 + +$) {
         Let $G_z \leftarrow C_{x_1} C_{x_2} C_{y_1}^{-1}$ % $M$.
         Get convergent sequence $\{r_0/q_0, r_1/q_1, \ldots, r_t/q_t\}$ of continued fraction of $G_z / M$.
         Get denominator sequence $\{q_1, q_2, \ldots, q_t\}$ from the convergent sequence.
         For ($s \leftarrow 1, s \le t, s + +$)
         If ($q_s \Delta < q_{s+1}$) and ($q_s < \max A$), then {
            Let $A_{y_1} \leftarrow q_s$.
```

```
        Output $(A_{y_1}, x_1, x_2, y_1)$.
    }
}
```

Notice that s++ denotes $s \leftarrow s + 1$, and the others are similar.

However, this algorithm is ineffectual. Please see the following example.

Assume that the bit-length of a plaintext block is $n = 10$.

Let $\{A_i\} = \{437, 221, 77, 43, 37, 29, 41, 31, 15, 2\}$ and $\Omega_\pm = \{5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$.

Let $M = 13082761331670077 > \prod_{i=1}^{n} A_i = 13082761331670030$.

Randomly select $W = 944516391$, and

$\ell(1) = 11$, $\ell(2) = 14$, $\ell(3) = 13$, $\ell(4) = 8$, $\ell(5) = 10$, $\ell(6) = 5$, $\ell(7) = 9$, $\ell(8) = 7$, $\ell(9) = 12$, $\ell(10) = 6$.

By $C_i \equiv A_i W^{\ell(i)}$ (% M), get $\{C_i\} = \{3534250731208421, 12235924019299910, 8726060645493642, 10110020851673707, 2328792308267710, 8425476748983036, 6187583147203887, 10200412235916586, 9359330740489342, 5977236088006743\}$.

On input of the public key $\{C_i\}$ and M, the program by Algorithm 1 will take $\varDelta = 506$, max$A$ = 58642670, and output A_{y_1} and the triples of which the number is greater than 100. See Table 1.

A_{y_1}	Triple (x_1, x_2, y_1)
$A_1 = 187125$	(1, 1, 1)
$A_1 = 121089$	(2, 1, 1), (1, 2, 1)
$A_1 = 77$	(5, 3, 1), (3, 5, 1)
$A_1 = 23$	(8, 6, 1), (6, 8, 1), (10, 10, 1)
$A_1 = 437$	(10, 6, 1), (6, 10, 1)
$A_2 = 1251$	(1, 1, 2)
$A_2 = 187125$	(2, 1, 2), (1, 2, 2)
$A_2 = 121089$	(2, 2, 2)
$A_2 = 17$	(8, 4, 2), (6, 5, 2), (5, 6, 2), (10, 7, 2), (4, 8, 2), (7, 10, 2)
$A_2 = 221$	(10, 4, 2), (7, 6, 2), (6, 7, 2), (8, 8, 2), (4, 10, 2)
$A_2 = 77$	(9, 8, 2), (8, 9, 2)
$A_2 = 4204$	(10, 10, 2)
$A_3 = 187125$	(3, 1, 3), (1, 3, 3)
$A_3 = 12$	(7, 1, 3), (1, 7, 3)
$A_3 = 121089$	(3, 2, 3), (2, 3, 3)
$A_3 = 77$	(6, 4, 3), (4, 6, 3), (10, 8, 3), (8, 10, 3)
$A_3 = 11$	(10, 4, 3), (7, 6, 3), (6, 7, 3), (8, 8, 3), (4, 10, 3)
$A_3 = 2113$	(8, 7, 3), (7, 8, 3)
$A_3 = 769$	(9, 8, 3), (8, 9, 3)
$A_4 = 187125$	(4, 1, 4), (1, 4, 4)
$A_4 = 121089$	(4, 2, 4), (2, 4, 4)
$A_4 = 76$	(10, 6, 4), (6, 10, 4)
$A_4 = 56$	(10, 9, 4), (9, 10, 4)
$A_5 = 187125$	(5, 1, 5), (1, 5, 5)
$A_5 = 630269$	(6, 1, 5), (1, 6, 5)
$A_5 = 121089$	(5, 2, 5), (2, 5, 5)
$A_5 = 41$	(8, 2, 5), (2, 8, 5)
$A_5 = 97$	(4, 3, 5), (3, 4, 5)
$A_5 = 37$	(6, 6, 5), (10, 6, 5), (6, 10, 5)
$A_6 = 187125$	(6, 1, 6), (1, 6, 6)
$A_6 = 121089$	(6, 2, 6), (2, 6, 6)
$A_7 = 187125$	(7, 1, 7), (1, 7, 7)
$A_7 = 121089$	(7, 2, 7), (2, 7, 7)
$A_7 = 3$	(9, 3, 7), (3, 9, 7)
$A_8 = 187125$	(8, 1, 8), (1, 8, 8)
$A_8 = 34945619$	(6, 2, 8), (2, 6, 8)

$A_8 = 121089$	(8, 2, 8), (2, 8, 8)
$A_9 = 187125$	(9, 1, 9), (1, 9, 9)
$A_9 = 121089$	(9, 2, 9), (2, 9, 9)
$A_9 = 5$	(6, 4, 9), (4, 6, 9), (10, 8, 9), (8, 10, 9)
$A_9 = 15$	(8, 6, 9), (6, 8, 9), (10, 10, 9)
$A_{10} = 259970$	(4, 1, 10), (1, 4, 10)
$A_{10} = 187125$	(10, 1, 10), (1, 10, 10)
$A_{10} = 121089$	(10, 2, 10), (2, 10, 10)
$A_{10} = 7629$	(8, 3, 10), (3, 8, 10)

Table 1: A_{y_1} and the Triple (x_1, x_2, y_1)

On Table 1, we observe that
A_{y_1} from 5 tuples is $A_2 = 221$ or $A_3 = 11$,
A_{y_1} from 4 tuples is $A_3 = 77$ or $A_9 = 5$,
A_{y_1} from 3 tuples is $A_1 = 23$, $A_5 = 37$, or $A_9 = 15$,
A_{y_1} from 2 tuples is $A_1 = 77$, $A_2 = 77$, $A_3 = 12$, $A_4 = 56$, $A_5 = 41$, or $A_7 = 3$ etc,
A_{y_1} from 1 tuples is $A_1 = 187125$, $A_2 = 1251$, $A_2 = 121089$, or $A_2 = 4204$.

Among these A_{y_1}'s, there exist at least 2^5 compatible selections from which we can obtain some elements of the coprime sequence $\{A_i\}$.

For instance, randomly select compatible A_{y_1}'s: $A_3 = 11$, $A_9 = 5$, $A_1 = 23$, $A_5 = 41$, and $A_2 = 1251$, and work out $\ell(y_1)$'s: $\ell(3) = 14$, $\ell(9) = 13$, $\ell(1) = 12$, $\ell(5) = 11$, and $\ell(2) = 10$ according to the rule that the number of the tuples in the form (A_{y_1}, x_1, x_2, y_1) equals $(\ell(y_1) - 9)$ when $\ell(y_1) \geq 10$ [11].

Obviously, such A_1, A_2, A_3, A_5, A_9 are not original elements, which indicates the *Discriminant* that is derived from (4″), and seemingly stricter than (4″) is essentially insufficient even if select a concrete $\Omega_{\pm} = \{5, 6, \ldots, n + 4\}$.

4.2.2 Case of $h \neq 1$

The $h \neq 1$ means $\bar{A}_y = A_{y_1} \ldots A_{y_h}$. It is well known that any composite $\bar{A}_y \neq p^k$ (p is a prime) can be factorized into some prime multiplicative factors, and many coprime sequences of the same length can be obtained from a prime factor set.

For instance, let $h = 3$ and $\bar{A}_y = 210$ with the prime factor set $\{2, 3, 5, 7\}$. We can obtain the coprime sequences $\{5, 6, 7\}$, $\{6, 5, 7\}$, $\{3, 7, 10\}$, $\{10, 3, 7\}$, $\{2, 15, 7\}$, $\{3, 2, 35\}$, etc. Which is the original?

Property 4 makes it clear that due to the indeterminacy of $\ell(.)$, no matter whether the power of W and W^{-1} counteract each other or not, in some cases, one or several values of $\bar{A}_y$ which may be written as the product of h coprime integers, and satisfy (4) can be found out from the convergents of the continued fraction of G_z / M when the interval $[1, n]$ is traversed respectively by $x_1, \ldots, x_m, y_1, \ldots, y_h$. Thus, "whether $\bar{A}_y$ can be written as the product of h coprime integers" may not be regarded as a criterion for verifying that the powers of W and W^{-1} counteract each other.

Moreover, even if the k values $v_1, \ldots, v_k$ of the product $A_{y_1} A_{y_2} \ldots A_{y_h}$ are obtained, where y_1 is fixed, and $y_2, \ldots, y_h$ are varied, $\gcd(v_1, \ldots, v_k)$ can not be judged to be A_{y_1} in terms of the definition of a coprime sequence.

If take $m = 2$ and $h = 2$, in terms of Property 4.2 and $P_{\forall x_1, x_2, y_1, y_2 \in [1, n]}$, the number of rationals formed as G_z / M which leads (4) to hold is roughly $n^4 / 2^{n-5}$ when the interval $[1, n]$ is traversed by x_1, x_2, y_1, y_2 respectively. What is most pivotal is that the value of $\ell(x_1) + \ell(x_2)$ or $\ell(y_1) + \ell(y_2)$ $\forall x_1, x_2, y_1, y_2 \in [1, n]$ does not necessarily occur in a concrete $\Omega_{\pm}$.

4.3 Time Complexity of Continued Fraction Attack by (4), (4′), or (4″)

It can be seen from section 4.1.1 that continued fraction attacks are based the assumption that $\ell(x_1) + \ldots + \ell(x_m) = \ell(y_1) + \ldots + \ell(y_h)$.

For convenience sake, let $m = 2$ and $h = 1$.

If $\Omega_{\pm}$ is determined as $\{5, \ldots, n + 4\}$, the continued fraction attack by (4″) dominantly contains four steps.

Algorithm 2:

```
S1: Initialization.
S2: Respectively cycle $x_1, x_2, y_1$ from 1 to $n$:
    Compute $G_z \equiv C_{x_1} C_{x_2} C_{y_1}^{-1}$ (% $M$).
S3: Judge $A_{y_1}$ by (4″) or the Discriminant derived from (4″).
S4: Compute $\ell(y_1)$ according to $A_{y_1}$ and Table 2.
```

$\ell(y_1)$	10	11	……	$n + 4$
$\ell(x_1) + \ell(x_2)$	$5 + 5$	$5 + 6, 6 + 5$	……	$5+(n-1), \ldots, (n-1)+5$
number of equalities	1	2	……	$n - 5$

Table 2: Number of Equalities Formed as $\ell(x_1) + \ell(x_2) = \ell(y_1)$

However, in fact, a concrete $\Omega_\pm$ is one of 2^n potential sets, and undetermined. Under the circumstances, the value of $\ell(x_1)+\ell(x_2)$ — $(-5) + 6$ for example does not necessarily occur in $\Omega_\pm$, and Table 2 is invalid.

Therefore, an adversary who employ the continued fraction attack by (4), (4′), or (4″) to extract a flat REESSE1+ private key must determine the elements in $\Omega_\pm$ as the first step of Algorithm 2, namely the sign before each of numbers from 5 to $n + 4$, which will take the running time of $O(2^n)$.

4.4 Time Complexity of Root Finding Attack with Guess

Due to $C_i \equiv A_i W^{\ell(i)}$ (% M) with $A_i \in \Lambda = \{2, \ldots, \text{Ƥ}\}$ and $\ell(i) \in \Omega_\pm \subset \{\pm 5, \ldots, \pm(n + 4)\}$ for $i = 1, \ldots, n$, and elements in the sets Λ and $\Omega_\pm$ small, an adversary may attempt the following attack with guess.

Algorithm 3:

```
S1: Convert $C_i \equiv A_i W^{\ell(i)}$ (% $M$) into $W^{\ell(i)} \equiv C_i A_i^{-1}$ (% $M$).
S2: Let $\ell(i)$ traverse $\{5, \ldots, n + 4, -5, \ldots, -(n + 4)\}$, and $A_i$ traverse $\Lambda$ for every $C_i$:
    S2.1: Compute every $W$ by the root finding method in [12].
    S2.2: Place every possible triple $(W, A_i, \ell(i))$ into the set $\Theta_i$.
S3: Seek the intersection $\Theta = \Theta_1 \cap \ldots \cap \Theta_n$ on $W$.
S4: If $W$ unique in $\Theta$, and $(A_i, \ell(i))$ in every $\Theta_i$ unique, a key $(\{A_i\}, \{\ell(i)\}, W)$ is extracted, the best;
    else if $W$ nonunique in $\Theta$, or $(A_i, \ell(i))$ nonunique in some $\Theta_i$ while $W$ unique, the thing is intricate:
        the adversary need to judge whether every possible $\{A_1, \ldots, A_n\}$ is a coprime sequence, and
        the elements in every possible $\{\ell(1), \ldots, \ell(n)\}$ are pairwise distinct.
```

The time complexity of the above attack is dominantly involved in Step 2 and 4.

At S2, seeking W will take $O(\ell(i)^{1/2} \lg M) \approx O(n^{1/2} \lg M)$ operations in terms of [12], the size of every Θ_i is about $O(|\Lambda||\Omega_\pm|^2) \approx O(\text{Ƥ} n^2)$ due to $q^2 \mid \bar{M}\ \forall$ prime $q \in |\Omega_\pm|$, and integrally the running time is $O(n \text{Ƥ} n^2 n^{1/2} \lg M) = O(\text{Ƥ} n^{3.5} \lg M)$ which is of polynomial time in n.

At S4, a coprime sequence can be found in polynomial time under the best circumstance with tiny probability, but it will take $O(2^n)$ comparisons under the most circumstances.

Thus, the adversary cannot extract a flat REESSE1+ private key in polynomial time generally.

5 Relation between a Lever Function and a Random Oracle

5.1 What Is a Random Oracle

An oracle is a mathematical abstraction, a theoretical black box, or a subroutine of which the running time may not be considered [10][13]. In particular, in cryptography, an oracle may be treated as a subcomponent of an adversary, and lives its own life independent of the adversary. Usually, the adversary interacts with the oracle but cannot control its behavior.

A random oracle is an oracle which answers to every query with a completely random and unpredictable value chosen uniformly from its output domain, except that for any specific query, it outputs the same value every time it receives that query if it is supposed to simulate a deterministic function [13].

Random oracles are utilized in cryptographic proofs for relpacing any irrealizable function so far which can provide the mathematical properties required by the proof. A cryprosystem or a protocol that is proven secure using such a proof is described as being secure in the random oracle model, as opposed to being secure in the standard model where the integer factorization problem, the discrete logarithm problem etc are assumed to be hard. When a random oracle is used within a security proof, it is made available to all participants, including adversaries. In practice, random oracles producing a bit-string of infinite length which can be truncated to the length desired are typically used to model cryptographic hash functions in schemes where strong randomness assumptions of a hash function′ s output are needed.

In fact, it draws attention that certain artificial signature and encryption schemes are proven secure in the random oracle model, but are trivially insecure when any real function such as the hash function MD5 or SHA-1 is substituted for the random oracle [14][15]. Nevertheless, for any more natural protocol, a proof of security in the random oracle model gives very strong evidence that an attacker have to discover some unknown and undesirable property of the hash function used in the protocol.

A function or algorithm is randomized if its output depends not only on the input but also on some random ingredients, namely if its output is not uniquely determined by the input. Hence, to a function or algorithm, the randomness is almost equivalent to indeterminacy.

5.2 Design of a Random Oracle

Correspondingly, the indeterminacy of the $\ell(i)$ may be expounded in terms of a random oracle.

Suppose that $\bar{O}_d(y, g)$ is an oracle on solving $y \equiv g^x$ (% M) for x, and $\bar{O}_\ell$ is an oracle on solving $C_i \equiv A_i W^{\ell(i)}$ (% M) for $\ell(i)$, where M is prime, and i is from 1 to n.

Let $\underline{D}$ be a database which stores records ($\{C_1, \dots, C_n\}$, M, $\{\ell(1), \dots, \ell(n)\}$) computed already. If the arrangement order of some C_i's is changed, $\{C_1, \dots, C_n\}$ is regarded as a distinct sequence.

The structure of $\bar{O}_\ell$ is as Algorithm 4:

```
Input: $\{C_1, \dots, C_n\}$, $M$.
Output: $\{\ell(1), \dots, \ell(n)\}$.
S1: If find ($\{C_1, \dots, C_n\}$, $M$) in $\underline{D}$,
     return related $\{\ell(1), \dots, \ell(n)\}$, and end.
S2: Randomly produce a coprime sequence $A_1, \dots, A_n$
     with each $A_i \le Ᵽ$ and $\prod_{i=1}^{n} A_i < M$.
S3: Randomly pick a generator $W \in \mathbb{Z}_M^*$.
S4: Evaluate $\ell(i)$ by calling $\bar{O}_d(C_i A_i^{-1}, W)$ for $i = 1, \dots, n$.
S5: Store ($\{C_1, \dots, C_n\}$, $M$, $\{\ell(1), \dots, \ell(n)\}$) to $\underline{D}$.
S6: Return $\{\ell(1),\quad , \ell(n)\}$, and end.
```

Of course, $\{A_i\}$ and W as side results may be outputted.

Obviously, for the same input ($\{C_1, \dots, C_n\}$, M), the output is the same, and for a different input, a related output is random and unpredictable.

Since $C_i A_i^{-1}$ is pairwise distinct, and W is a generator, the result $\{\ell(1), \dots, \ell(n)\}$ will be pairwise distinct. In addition, according to Definition 2, every $\ell(i) \in [1, \overline{M}]$ may be outside of $\Omega_\pm$. Thus, $\{\ell(1), \dots, \ell(n)\}$ is a lever function although not the original.

The $\bar{O}_\ell$ is perhaps strange to some people because they have never met any analogous oracle in classical cryptosystems.

The above discussion soundly expounds once more why the indeterministic reasoning, namely the continued fraction attack by (4), (4′), or (4″) is ineffectual on $C_i \equiv A_i W^{\ell(i)}$ (% M).

6 Conclusion

Indeterminacy is ubiquitous. For example, for $x + y = z$, given $x = -122$ and $y = 611$, computing $z = 489$ is easy, and contrarily, given $z = 489$, seeking the original x and y is intractable since there exists indeterminacy in $x + y = z$. Indeterminacy in $C_i \equiv A_i W^{\ell(i)}$ (% M) is similar, and triggered by the lever function $\ell(.)$.

Discriminant (4) is stricter than (4″) although both (4) and (4″) are only necessary but not sufficient for $\ell(x_1) + \ell(x_2) = \ell(y_1)$. Property 4 and 8 show that attack by (4) is more effectual than attack by (4″). However, Section 4.3 shows that when $\Omega_\pm \subset \{\pm 5, \dots, \pm(n + 4)\}$ is indeterminate, the continued fraction attack by (4), (4′), (4″), or the *Discriminant* derived from (4″) will take $O(2^n)$ operations, and is computationally infeasible. Therefore, the lever function $\ell(.)$ from $\{1, \dots, n\}$ to a subset of $\{\pm 5, \dots, \pm(n + 4)\}$ is necessary and sufficient for resisting the continued fraction attack.

Meanwhile, Section 4.4 manifests that the root finding attack with guess cannot extract a private key in polynomial time generally, but it unveils some probabilistic risk.

Resorting to $C_i \equiv A_i W^{\ell(i)}$ (% M), we expound the indeterminacy of the lever function theoretically. In practice, to determinately assure the security of a private key and to decrease the length of modulus of the cryptosystem, the key transform should be strengthened to $C_i \equiv (A_i W^{\ell(i)})^{\delta}$ (% M) with $\delta \in [2, \bar{M}]$, $A_i \in \Lambda = \{2, \ldots, Ƥ\}$, and $\ell(i) \in \Omega_{\pm} \subset \{\pm 5, \ldots, \pm(n + 4)\}$ for $i = 1, \ldots, n$ [6][16].

Acknowledgment

The authors would like to thank the Academicians Jiren Cai, Zhongyi Zhou, Changxiang Shen, Zhengyao Wei, Andrew C. Yao, Binxing Fang, Xicheng Lu, and Guangnan Ni for their important guidance, suggestions, and help.

The authors also would like to thank the Professors Dingyi Pei, Dengguo Feng, Jie Wang, Ronald L. Rivest, Moti Yung, Adi Shamir, Dingzhu Du, Mulan Liu, Huanguo Zhang, Yixian Yang, Xuejia Lai, Xiaoyun Wang, Tao Xie, Yupu Hu, Jiwu Jing, Rongquan Feng, Ping Luo, Jianfeng Ma, Xiao Chen, Dongdai Lin, Zhenfu Cao, Lei Hu, Lusheng Chen, Wenbao Han, Bogang Lin, Qibin Zhai, Dake He, Hong Zhu, Zhiying Wang, and Quanyuan Wu for their important advice, suggestions, and corrections.

References

[1] D. Z. Du and K. Ko, *Theory of Computational Complexity*, New York: John Wiley & Sons, 2000, ch. 3-4.

[2] A. C. Yao, Theory and Applications of Trapdoor Functions, *Proc. the 23rd Annual Symposium on the Foundations of Computer Science*, IEEE, 1982, pp. 80-91.

[3] W. Diffie and M. E. Hellman, New Directions in Cryptography, *IEEE Transactions on Information Theory*, v. 22(6), 1976, pp. 644-654.

[4] R. L. Rivest, A. Shamir, and L. M. Adleman, A Method for Obtaining Digital Signatures and Public-key Cryptosystems, *Communications of the ACM*, v. 21(2), 1978, pp. 120-126.

[5] T. ElGamal, A Public-key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, *IEEE Transactions on Information Theory*, v. 31(4), 1985, pp. 469-472.

[6] S. Su and S. Lü, A Public Key Cryptosystem Based on Three New Provable Problems, *Theoretical Computer Science*, v. 426-427, 2012, pp. 91-117.

[7] T. W. Hungerford, *Algebra*, New York: Springer-Verlag, 1998, ch. 1-3.

[8] S. Su, S. Lü, and X. Fan, Asymptotic Granularity Reduction and Its Application, *Theoretical Computer Science*, v. 412(39), 2011, pp. 5374-5386.

[9] K. H. Rosen, *Elementary Number Theory and Its Applications* (5th ed.), Boston: Addison-Wesley, 2005, ch. 12.

[10] A. J. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, London, UK: CRC Press, 1997, ch. 2, 3, 8.

[11] S. Liu, F. Zhang etc, Cryptanalysis of REESSE1 Public Encryption Cryptosystem, *Information Security* (in Chinese), v. 5(7), 2005, pp. 121-124.

[12] N. A. Moldovyan, Digital Signature Scheme Based on a New Hard Problem, *Computer Science Journal of Moldova*, v. 16(2), 2008, pp. 163-182.

[13] M. Bellare and P. Rogaway, Random Oracles are Practical: A Paradigm for Designing Efficient Protocols, *Proc. the 1st ACM Conference on Computer and Communications Security*, New York: ACM Press, 1993, pp. 62-73.

[14] R. Canetti, O. Goldreich, and S. Halevi, The Random Oracle Methodology Revisited, *Proc. the 30th Annual ACM Symposium on Theory of Computing*, New York: ACM Press, 1998, pp. 209-218.

[15] N. Koblitz and A. Menezes, Another Look at "Provable Security" II, *Progress in Cryptology - INDOCRYPT 2006*, Berlin: Springer, 2006, pp. 148-175.

[16] S. Su and S. Lü, REESSE1-E Public-key Signature Scheme Based on Variable Combination, *Acta Electronica Sinica* (in Chinese), v. 38(7), 2010, pp. 234-238.