Diffie-Hellman Multi-Challenge using a New Lossy Trapdoor Function Construction

I. Cherkaoui

Abstract—**Trapdoor functions contributed since their announcement in the evolvement cryptography as we know it, especially the lossy mode, by helping reduce the residual leakage for an optimal rate, but to make it more resilient cryptographically: generic constructions were made based on graph isomorphism, or other NP-hard problems defended by the zero-knowledge proof, such were used in Indistinguishability under Chosen-Plaintext Attack (IND-CPA), Computationnal Diffie-Hellman (CDH), or Decisional Diffie-Hellman (DDH).**

Once schemes like Indistinguishability under Chosen-Ciphertext Attack (IND-CCA) were adopted it became clear it cannot simulate a decryption using Lossy Trapdoor Functions (LTF); the problem with existing trapdoor functions in general is partial information leakage, lack of randomness and multiple messages insecurity.

In the light of the following issues came the idea to present through this paper a simple but important fix, in the note of randomness a new Variate of the Engel expansion (VEE) is chosen, providing a pseudo-random bit sequence as an output, the reason being to recover the seed of the algorithm for an attacker, it is considered a hard number theory problem, and surely after the new construction in this paper, another NP-complete problem emerging from tensors the scheme is more secure. As for the strenghtening evidence of how it can be trusted, it seems more robust to supply a proof of its ergodicity as being done in this article, instead of semantic security analysis, to prove the efficiency of the new construction resolving the issues surrounding multi-challenge using a lossy trapdoor function.

Index Terms—**Engel expansion, ergodicity, chaos, LTF, PRNG, IND-CCA, DDH.**

I. Introduction

FIRST and foremost, it is essential to tackle the definition of the Engel expansion [1].

Let x be a positive real number such that:

$$x = \frac{1}{a_1} + \frac{1}{a_1 a_2} + \frac{1}{a_1 a_2 a_3} + ...$$

The unique non-decreasing sequence of positive integers a_1, a_2, a_3, a_4, ... is called the Engel expansion.

The Engel expansion of x can be obtained through executing the flowing algorithm:

- let $u_1 = x$,
- $a_k = \left[\dfrac{1}{u_k}\right] + 1$ and $u_{k+1} = u_k a_k - 1$
- If $u_k = 0$ the algorithm stops.

Let $\overline{a_i}$ be the number of digits of a_i and T_E the Variate Engel Expansion (VEE) defined by the following expression:

$$x = \frac{1}{a_1 a_1 10^{-\overline{a_1}}} + \frac{1}{a_1 a_2 a_2 10^{-\overline{a_2}}} + \frac{1}{a_1 a_2 a_3 a_3 10^{-\overline{a_3}}} + ...$$

with the same initial conditions and starting domain required for the Engel expansion.

A. Brief introduction to chaos-based cryptogrtaphy

Chaos-based cryptography is interesting due to the broadband power spectrum of chaotic signals, high rates of information transmission, and efficiency at sufficiently low signal-to-noise ratio, chaos is a behaviour of a nonlinear system, looking random, with no stochastic reason [2]. To encrypt using this method keys are generated with chaotic maps or in this case the ergodic nature of the chaotic trajectory, emerging from a seed intializing the system at first.

B. Random number generators

The main one used primarily is the pseudo-random number generator (PRNG) which is periodic and deterministic and the other is the true random number generator (TRNG). When dealing with cryptography, a PRNG is called cryptographically strong if an intruder intercepts information generated by the PRNG, but still doesn't have the possibility to reconstruct the remaining data of the output.

C. Ergodic theory

Ergodic theory is the study of the asymptotic average behavior of systems evolving in time. The collection of all states of the system form a space X, and the evolution is represented by a transformation $T : X \to X$, where Tx is the state of the system at time $t = 1$, when the system (at time $t = 0$) was initially in state x.

D. One way function

1) Negligible function: A function $r : \mathbb{N} \to \mathbb{N}$ is negligible if $\forall p : \mathbb{N} \to \mathbb{N}$ polynomial, $\exists k_0$ integer such that: $r(k) \leq \dfrac{1}{p(k)}$ for $k \geq k_0$.

2) One way function definition: A function f is called a one way function if:

1) f is polynomial time computable.
2) Any probabilstic algorithm for inverting $f(x)$ given a random $y = f(x)$ (x at random) has negligible chance of finding a preimage of y.

E. Trapdoor function

A trapdoor function is given an input m is easy to compute the result, but the reversible process is a NP-Hard problem except if we know a special piece of information being the secret.

Manuscript received December 26, 2020; revised May 23, 2021. This work was supported by the National Center of Scientific and Technical Research under Grant 22UM5R2018.

I. Cherkaoui is a PhD candidate of University Mohammed V, Rabat, Morocco, BP 1014 e-mail: (ilias.cherkaoui17@gmail.com).

F. Losiness

When you switch to lossy mode, you no longer have to deal with polynomial time machines as the proofs become statistical arguments. Thus, a cipher made by an injective key is decrypted, while the one made by a lossy key is statistically independent of the original message, making the both keys indistinguishable from each other.

A lossy function means the size of their image is smaller than the one of their domain.

Let us assume having an input message x of n bits and r exists such that $|ImF| < 2^r$ in lossy mode, with the image consisting of the residual leakage (leaks bits from the input), if given less than $n - r$ bits of x, then f cannot be inverted.

G. Plan

This paper is divided into several sections as follows:

- Related works: where the aim is to mention previous works in similar domains which gather the essence of our contribution.
- LTF construction: where the construction of the trapdoor function starts its building blocks towards the one-way function as a first step.
- Preliminary: which is a section englobing multiple pre-requesites necessary to understand how the issue at hand is approached.
- Effectiveness proof: is a section in which we use the prerequisites we already mentioned before, to prove some properties such as ergodicity.
- Using the VEE as LTF for the DDH: This is the final attained objective where the Diffie-Hellman assumption and trapdoor function are gathered via the first one-way function to solve the problem of Multi-Challenges in IND-CCA.
- Conclusion: It is the final section summing up the focus of our contribution in this paper and possible perspectives.

II. Related work

One-way trapdoor functions are one of the most fundamental cryptographic primitives, especially lossy trapdoor functions LTFs attracting a lot of attention since the contribution of the pioneers [6], unleashed a wave of similar works on LTFs. [7] thought of a new technique to shrink the public key of matrix construction of [6]. [8] and [9] showed LTFs imply correlated-product TDFs and adaptive TDFs.

After being introduced by [6], Lossy trapdoor functions have become more popular in the recent years, due to the multiple varieties they can offer and how it can benefit other concepts like extending it to the identity-based setting, and trying other constructions more efficient hence the design suggested in this paper.

A previous paper [14] did investiga a novel computational problem "the Composite Residuosity Class Problem, and its applications to public-key cryptography" in which he suggested a new trapdoor mechanism, he also came up in the same work with a trapdoor permutation and two homomorphic probabilistic encryptions.

Another paper can be mentionned here as well [16] showing techniques used for generic constructions of fully-secure IBE(Identity-Based Encryption) and selectively-secure HIBE (Hierarchical IBE).

Another technical novelty was back when the paper [7] proposed a compact encoding technique for generating compressed representations for some sequences of group elements using public parameters, which also focuses on shkrinking the discrete-log lossy trapdoor functions key size.

III. LTF construction

Random proceses cause electronic noise, varrying a signal from its digital position in time, this "jitter" would later serve us in generating random numbers.

The idea is to assemble with a XOR operation multiple outputs coming from inverter ring oscillators. Instead of Brownian noise, so ϕ_i is the i-th term of the VEE (Variate Engel Expansion).

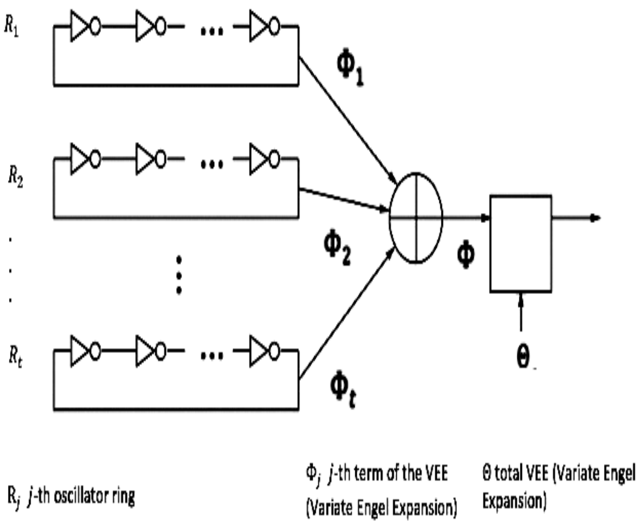
R_1
R_2
R_t
Φ_1
Φ_2
Φ_t
Φ
θ
R_j j-th oscillator ring
Φ_j j-th term of the VEE (Variate Engel Expansion)
Θ total VEE (Variate Engel Expansion)

Fig. 1. Circuit diagram ring design of the LTF

The events $\phi_1, \phi_2, ...\phi_r$ fill the oscillation period of the signal ϕ which is subdivided into r equal time intervals "urns" less than the jitter boundaries of one ring output, providing a random bit when sampling it as the time lapse is shortened between events as in figure 1.

Now in each of those rings the output value is made following the process we choose to detail afterwards. Once we choose the seed x and number N of iterations, we may follow both strategies below:

1) Divide $[0, 1[$ using the Variate Engel Expansion (VEE) to get an ideal true random number generator allowing the harvest of random integers.
2) Divide $[0, 1[$ using a partition P_n of 2^n intervals, to get a non-ideal true random number generator with 2^n random integers.

Given X an irrational number on which we count on applying the expansion, the procedure is like the following described algorithm:

During the initialisation, the counter C and key K are set to null giving a clear assumption that the generator is not seeded at first as shown in algorithm 1.

Then the internal entity of the PRNG generates at random a number of blocks.

GenerateRandom function check first if C is not null, as the generator is not seeded in algorithm 2, then the loop

```
Algorithm 1: Initialisation
Input: Initialise
    Allocate a real number value to $x$ and
    an integer one to $N$ /* $N$ being the
      $N$-th term of the VEE of $x$          */
Output: Generator state
    $(K, C) \leftarrow (0, 0)$
    $(X, N) \leftarrow (x, n)$ /* $x \in \mathbb{R}$  and  $n \in \mathbb{N}$
                                                          */
```

```
Algorithm 2: GenerateRandom
Input: GenerateRandom
/* The VEE($j$) of the iteration $j$ is
   loaded and given the couple $(x, n)$
   */
    G: Generator state has the VEE
    k: block number
Output: Pseudorandom string
while $C \neq 0$ do
    $r \leftarrow \epsilon$ /* empty string               */
    Append block
    for i=1,...,k do
        $r \leftarrow VEE(i)$
        $C \leftarrow C + 1$
    return $r$
```

starts with ϵ in r and appends blocks that are computed into r building the output value by the VEE.
Now we know if we take a rational $x_0 \in]0, 1]$, and u_n is a serie of its Engel expansion starting from rank N, then Engel's algorithm offers an expansion of x_0 as a limited continued fraction [13].

$$x_0 = \frac{1}{u_0 - \frac{u_0}{u_1 + 1 - \frac{u_1}{u_2 + 1 - \dots}} \dots - \frac{u_{N-2}}{u_{N-1} + 1 - \frac{u_{N-1}}{u_N}}}$$

While a mapping of continued fractions is given by:

$$x_{n+1} = T(x_n) = \frac{1}{x_n} - \lceil \frac{1}{x_n} \rceil$$

Gauss found this probability distribution:

$$p(x) = \frac{1}{(1 + x) \ln 2}$$

The amplification sensitivity measured by the kolmogorov entropy [12] is as follows:

$$h = \int_0^1 \ln |\frac{dT}{dx}| p(x) dx$$

Which results in the following for the mapping T:

$$h = \int_0^1 \frac{-2 \ln(x)}{(1 + x) \ln 2} dx = \frac{\pi^2}{6 \ln 2}$$

Knowing h is non-zero the mapping is considered chaotic so we can deduce Engel Continued Fractions (ECF) is therefore at least sensitive dependent on initial conditions.
The algorithm we chose following the function F is similar to the r-adic Rényi transformation in shifting [11]: $S(x) = rx(mod 1)$ which is already chaotic for $0 \leq x \leq 1$ and $r > 1$.

Due to the relation between regular continued fractions and ECF we can deduce that the VEE of x has the approximation [10] :

$$\tilde{x} : x \longrightarrow \frac{p}{q}$$

with $p, q \in \mathbb{Q}$.
For $n \geq 1$ and $1 \leq k \leq a_{n+1} - 1$ the mediants are defined by:

$$\tilde{f} : \frac{p}{q} \longrightarrow \frac{kp_n(x) + p_{n-1}(x)}{kq_n(x) + q_{n-1}(x)} 10^{\overline{a_n}}$$

which is the finite-precision approximating function, with $\frac{p_n(x)}{q_n(x)}$ the convergents of x in regular continued fractions (RCF).
Let $|f(x) - \tilde{f}(x)| = \epsilon(x)$, then if for all x: $\epsilon(x) << 1$ we can conclude that $\tilde{f}$ shadows f [2] for the pseudo-chaotic approximation $\tilde{f} o \tilde{x}$.
Hence, the use of the ergodic property for this map, to create a nonlinear PRNG which is the main concern and core of our intended LTF, aiming towards a low-complexity implementation and strong statistical test results.

IV. Preliminary

A. Prerequisites

Let (Ω_1, F_1, P_1) and (Ω_2, F_2, P_2) be probability spaces and T a transformation:

1) T is measurable if $\forall E \in F_2 \Rightarrow T^{-1}E \in F_1$
2) A measurable transformation T is non-singular if $\forall E \in F_2 : P_2(E) = 0 \Rightarrow P_1(T^{-1}E) = 0$
3) A measurable non-singular transformation T is ergodic if $T^{-1}E = E$ for $E \in F \Rightarrow P(E) = 0$ or $P(E) = 1$

B. Theorem:[3]

Let E a Lebesgue measurable subset of $[0, 1]$ with $P(E) > 0$ and Lebesgue measure is $\lambda(B_n) = \prod_{j=1}^{n} \frac{1}{k_j'}$ $\forall n \in \mathbb{N}^*$, J a collection of subintervals of $[0, 1]$:

1) Every open subinterval of $[0, 1]$ is almost a denumerable union of disjoint elements of J (P almost surely)
2) $\forall B \in J, P(EB) \geq cP(E)$ with constant
$c > 0 \Rightarrow P(E) = 1$

C. Theorem:

We define $B_n = B_n(k_1, k_2, ...) = \{x \in (0, 1]/a_1(x) = k, a_2(x) = k_2, ...a_n(x) = k_n\} \forall k_1, ...k_n \in \mathbb{N}^*$ for $a_i, i = 1, ..., n$ being the coefficients of the Variate Engel Expansion sequence.
The set is B_n is bounded and its bounds are:
$M_n = sup \, B_n(k_1, k_2, ..., k_n) = \frac{10^{\overline{k_1}}}{k_1} + \frac{10^{\overline{k_2}}}{(k_1 + 1)k_2} + ... + \frac{10^{\overline{k_n}}}{(k_1 + 1)(k_2 + 1)...(k_n + 1)k_n'}$
$m_n = inf \, B_n(k_1, k_2, ..., k_n) = \frac{10^{\overline{k_1}}}{k_1} + \frac{10^{\overline{k_2}}}{(k_1 + 1)k_2} + ... + \frac{10^{\overline{k_n}}}{(k_1 + 1)(k_2 + 1)...(k_{n-1} + 1)k_n} + \frac{10^{\overline{k_{n-1}}}}{(k_1 + 1)(k_2 + 1)...k_{n-1}'}$

Proof: If $a_n(x) = k_n$ then $r_{n-1}(x) = \frac{1}{k_n} - \frac{1}{k_{n+1}} r_n(x), n \in \mathbb{N}^*$ where $r_n(x) = \frac{1}{a_{n+1}(x)} + \frac{1}{a_{n+1}(x)+1}\frac{1}{a_{n+2}(x)} + ..$ with $a_{n+1} \in \mathbb{N}^* \quad \forall m \geq 1$ and $x \in B_{k_1 k_2 .. k_n}$
Therefore if $x \in B_{k_1 k_2 .. k_n}$ then:

$$x = \frac{10^{\overline{k_1}}}{k_1} + \frac{10^{\overline{k_2}}}{(k_1+1)k_2} + .. + 10^{\overline{k_n}} \frac{1}{(k_1+1)(k_2+1)..(k_{n-1}+1)k_n} + 10^{\overline{k_{n+1}}} \frac{1}{(k_1+1)(k_2+1)..(k_n+1)a_{n+1}(x)} + 10^{\overline{k_{n+2}}} \frac{1}{(k_1+1)..(k_n+1)(a_{n+1}(x)+1)a_{n+2}(x)} + .. = \frac{10^{\overline{k_1}}}{k_1} + \frac{10^{\overline{k_2}}}{(k_1+1)k_2} + .. + \frac{10^{\overline{k_n}}}{(k_1+1)(k_2+1)..(k_{n-1}+1)k_n} + \frac{10^{\overline{k_{n+2}}}}{(k_1+1)(k_2+1)..(k_n+1)} . \left(\frac{1}{a_{n+1}(x)} + \frac{1}{(a_{n+1}(x)+1)a_{n+2}(x)} + ..\right) = \frac{10^{\overline{k_1}}}{k_1} + \frac{10^{\overline{k_2}}}{(k_1+1)k_2} + .. + \frac{10^{\overline{k_n}}}{(k_1+1)(k_2+1)..(k_{n-1}+1)k_n} + \frac{10^{\overline{k_n}}}{(k_1+1)(k_2+1)..(k_n+1)} r_n(x)$$

Now we are facing two situations:

1) First scenario $n = 2k+1, k = 0, 1, 2, ..$

If $r_n(x) = 0$, then:

$$m_n = inf\, B_n(k_1, k_2, ..., k_n) = \frac{10^{\overline{k_1}}}{k_1} + \frac{10^{\overline{k_2}}}{(k_1+1)k_2} + .. \frac{10^{\overline{k_n}}}{(k_1+1)(k_2+1)..(k_{n-1}+1)k_n}$$

and if $r_n(x) = 1$, then

$$M_n = sup\, B_n(k_1, k_2, ..., k_n) = \frac{10^{\overline{k_1}}}{k_1} + \frac{10^{\overline{k_2}}}{(k_1+1)k_2} + .. \frac{10^{\overline{k_n}}}{(k_1+1)(k_2+1)..(k_{n-1}+1)k_n} + \frac{10^{\overline{k_n}}}{(k_1+1)..(k_n+1)}$$

2) Second scenario $n = 2k, k = 0, 1, 2, ..$

If $r_n(x) = 0$, then:

$$m_n = inf\, B_n(k_1, k_2, ..., k_n) = \frac{10^{\overline{k_1}}}{k_1} + \frac{10^{\overline{k_2}}}{(k_1+1)k_2} + .. \frac{10^{\overline{k_n}}}{(k_1+1)..(k_{n-1}+1)k_n} + \frac{10^{\overline{k_{n-1}}}}{(k_1+1)..(k_{n-1}+1)}$$

while if $r_n(x) = 1$, then:

$$M_n = sup\, B_n(k_1, k_2, ..., k_n) = \frac{10^{\overline{k_1}}}{k_1} + \frac{10^{\overline{k_2}}}{(k_1+1)k_2} + .. + \frac{10^{\overline{k_n}}}{(k_1+1)..(k_{n-1}+1)k_n}$$

V. Effectiveness Proof

Ergodicity is the chaotic property equivalent to the cryptographic confusion of Shannon in information theory, where the output has the same distribution for all inputs, making the keystream sequence unpredictable, and kept secret with absence of redundancy.

In order to ensure the chaotic behaviour of the PRNG, ergodicity is a must, knowing with this property at hand trajectories have an invariant distribution unattached to the initial state, and visiting all intervals of all sizes. Thus, what follows in the paper is the ergodicity establishment of the function T_E defined in the beginning.

A. Theorem

The built up transformation based on the Variate Engel expansion T_E is ergodic relatively to the Lebesgue measure λ.

Proof: Let's define a function $\psi_n = \psi_n(k_1, k_2, ..., k_n), \psi_n\, [0, 1] \rightarrow B_n$,

$\psi_n(v) = \sum_{j=1}^{n} \frac{10^{\overline{k_j}} \lambda(B_{j-1})}{k_j} + 10^{\overline{k_n}}.v.\lambda(B_n) = \sum_{j=1}^{n} \frac{10^{\overline{k_j}}}{k_1 k_2 .. k_{j-1}} \left(1 + \frac{10^{\overline{k_{j-1}}}}{k_j}\right) + 10^{\overline{k_n}}.v. \prod_{j=1}^{n} \frac{1}{k_j}$

if $x \in B_n$ then:

$$\begin{aligned} x &= \sum_{j=1}^{\infty} \frac{10^{\overline{k_j}}}{a_1 a_2 .. a_{j-1} a_j} \\ &= \sum_{j=1}^{n} \frac{10^{\overline{k_j}} \lambda(B_{j-1})}{k_j} + \lambda(B_n). \sum_{j=n+1}^{\infty} \frac{10^{\overline{k_j}}}{a_{n+1} a_2 .. a_{j-1} a_j} \\ &= \psi_n(T_E^n(x)) \end{aligned}$$

then $\psi_n = T_E^n : B_n \rightarrow I$
and $M_n = \psi_n(1)$, $m_n = \psi_n(0)$, $\forall n = 2, 4..$
with $\psi_n(0) = \frac{10^{\overline{k_1}}}{k_1} + \frac{10^{\overline{k_2}}}{k_1 k_2} + .. + \frac{10^{\overline{k_n}}}{k_1 .. k_n}$
and $\psi_n(1) = \sum_{j=1}^{n} \frac{10^{\overline{k_j}} \lambda(B_{j-1})}{k_j} + 10^{\overline{k_n}} \lambda(B_n)$
(If n is odd we invert)
So for any interval $]a, b[\subseteq I$ we have:

$$\begin{aligned} \lambda(T_E^n]a, b] \cap B_n) &= \lambda(\psi_n[a, b] \cap B_n) \\ &= |\psi_n(b) - \psi_n(a)| \\ &= (b-a)\lambda(B_n) \\ &= \lambda]a, b].\lambda(B_n) \end{aligned}$$

thus

$$\lambda(T_E^{-n} E \cap B_n) = \lambda(E)\lambda(B_n) \qquad (*)$$

No matter the set inside the boolean ring R of all finite disjoint unions of intervals $]a, b] \subset I$ the equation is still valid for all borel set E in I.
Let now E be a Borel set in I such that:
$T_E^{-1} E = E$ then: $T^{-n} E = E, \forall n \geq 1$
and (*) $\Rightarrow \lambda(E \cap B_n) = \lambda(E)\lambda(B_n)$
or $\lambda(E \cap B_n) = K\lambda(B_n)$ with $K = \lambda(E) > 0$
If C is the collection of all cylinders B_n, $n > 1$, and $a_{j+1} > a_j$, $a_j > 1 \forall j \geq 1$, then any open subinterval of $(0, 1]$ would be denumerable at most as a disjoint union of elements of C, therefore:
$\lambda(E \cap B) = K\lambda(B), \forall B = B_n$ a set of a countable disjoint union. Hence:
From [**Theorem 4.2, property 1)**] we have $\lambda(E) = 1$ and by [**Prerequisite 4.1 assertion 3)**]
$\Rightarrow T_E^{-1} E = E \Rightarrow P(E) = 1 \Rightarrow T_E$ is ergodic.

B. Product's sequence correlation

Using the wavelet scalogram as in the figure 2 it is shown there is no consistent correlation in the product resulting from the expansion of the specific sequence being chosen, where the horizontal axis represents the time, the vertical axis represents the scale, with which normally correlation is found by measuring energy, where the wavelet transform is defined like the following:

$$Wf(u,s) := \langle\, f, \psi_{u,s} \rangle = \int_{-\infty}^{+\infty} f(t)\psi^*_{u,s}(t)dt$$

where

$$\psi_{u,s} := \frac{1}{\sqrt{s}}\psi(\frac{t-u}{s})$$

$u \in \mathbb{R}$, $s > 0$.
Hence the scalogram of f, S is:

$$S(s) := \|Wf(u,s)\| = (\int_{-\infty}^{+\infty} |Wf(u,s)|^2 du)^{\frac{1}{2}}$$

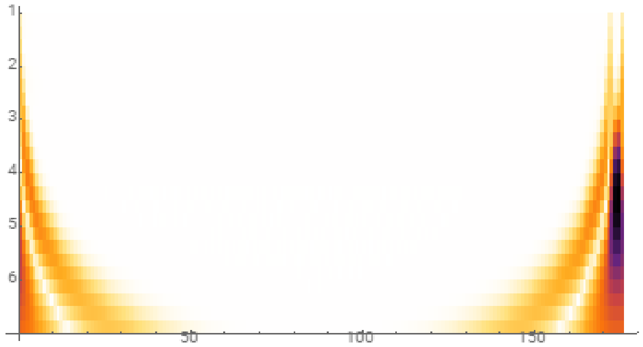

Fig. 2. Wavelet scalogram for an egyptian product

Using the innerscalogram which is the normalized scalogram [4], the observer can deduce the scale index obtained by dividing the minimal value of the last one by its maximum, will lead obviously here close to 1 for this highly non periodic expansion [5].
As for the wavelot plot of our egyptian product, it can be noticed on figure 3 that when cross-correlating the wavelot transform with this signal there is no spots at the first rows that may show matches, so it may happen at high number rows randomly due to the specification of the VEE algorithm, thus proving the point.

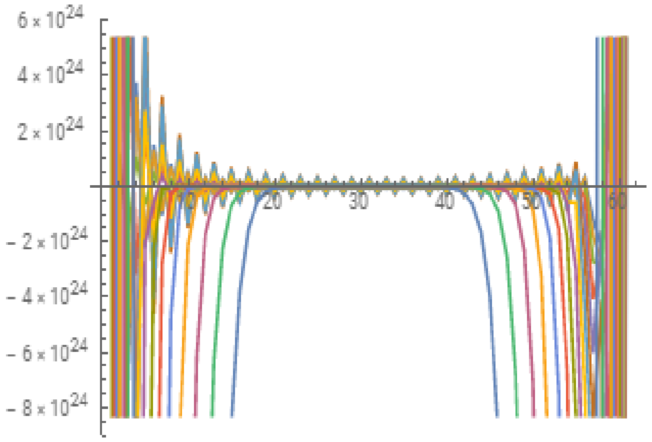

Fig. 3. Wavelet plot for an egyptian product

VI. Using the VEE as LTF for the DDH

In this section, the Variant Engel Expansion is being put use as a Lossy Trapdoor Function for the Decisional Diffie-Hellman problem in order to establish a well put together encryption.

A. Multi-Challenge solution in IND-CCA

When dealing with one sender or user in IND-CCA, the trapdoor is used in one challenge making easy to perform hashes or encryption via a one-way function; the issue at hands occurs when dealing with multiple users forcing the encryption modules to handle Multi-Challenges.
Selective Openings do target this topic :

$$\begin{tikzcd}
Alice \arrow[r, Rightarrow, "\mathcal{C}_1^*, ..., \mathcal{C}_n^*"] \arrow[d] & Oscar \arrow[d, "\mathcal{I}"] \arrow[dl, dashed, dash] \\
\cdot \arrow[r, "(c_i^*) \quad \forall i \in \mathcal{I}"'] & \cdot
\end{tikzcd}$$

As you can see, there is no indistinguishability with this adaptive corrutpion of multiple senders, giving away open (c_i^*) $\forall i \in \mathcal{I}$ while sending the ciphertexts $\mathcal{C}_1^*, ..., \mathcal{C}_n^*$, which makes the attacker well aware of important informationnal parts on the public key p_k and ciphers (c_i^*), since the randomness uses openings in committment.
Now let's consider in what follows this keyed function:

$$x \longrightarrow f_{k_i}(x)$$

with k_1: the key corresponding to the invertible mode
and k_2: the key corresponding to the lossy mode
where $k_1 \approx k_2$ and the VEE will be used as the trapdoor function f.
In the case of invertibility, an invertible key is being called upon while when needing lossiness the construction of the function guarantees that the image set is much smaller than the preimage set $(f_{k_2}(x) \ll X)$.
So getting back to the issue, knowing the attacker gets the LTF key and image p_k, c^* from the sender, then although switching LTF to lossy mode would deny the eavesdropper from reaching information on the messages, if the sender is operating under IND-CCA the decryption oracle is unable to function in lossy mode, due to its limitation to work either under a cipher using fully invertible mode or lossy, and cannot alternate between the two.
To prevent this from happening while keeping the encryption functional, tags like t^* are being introduced [14] that switch the function $f_{k,t}$ to lossy mode only for one special tag.
Let f be an n-degree polynomial function such that :

$$f(t) = \sum f_i t^i$$

with f_i being the output pf the VEE.
and the only tags non-null are $t_1^*, ..., t_n^*$.
then $k = (p_k, C_0 = E_{p_k}(f_0), ..., C_n = E_{p_k}(f_n))$
and $f_{k,t}(x) = (\prod c_i^{t^i})^* = E_{p_k}(f(t)X)$. Now due to the number of challenges to encode n lossy tags the space complexity is linear, and the Selective Openings chosen-ciphertext attack (SO-CCA) model would secure the public key echange (PKE) but will make the public key p_k larger,

so the sender will have to consider each t_i^* sampled by the trapdoor function is corresponding to a ciphertext challenge, because there are many superpolynomial lossy tags.

B. DDH construction over LTF

The adopted approach her is where matrices are used instead of single bits, hence the encryption will be performed over a matrix M as the message, the E denotes the DDH encryption scheme and t is the lossy tag used alongside the trapdoor function (TDF).

$$t \to E(M) = \begin{bmatrix} E(M_{1,1}) & \dots & E(M_{1,n}) \\ \vdots & \ddots & \vdots \\ E(M_{n,1}) & \dots & E(M_{n,n}) \end{bmatrix}$$

then the function becomes $f_{k,t}(x) = E(M) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

So

$$f_{k,t}(x) = \begin{pmatrix} \prod_i E(M_{1,i})^{x_i} \\ \vdots \\ \prod_i E(M_{n,i})^{x_i} \end{pmatrix} = E(MX)$$

Notice $f_{k,t}$ is lossy $\iff$ M is non-invertible

$$\iff det(M) = 0$$

This $det(M)$ can be used to encode complex computations when being cubic, but this is not the aim in this section.

In Diffie-Hellman, the model relies on a number $g \in G$ considered as a group generator such that if M is a bit sequence of the message:

$$M \in \mathbb{Z}_p^{n\times n} \Rightarrow [M] = g^M$$

Giving

$$[M] \in G^n$$

Allowing any integer matrix M to be encoded as $[M]$, therefore any input of the TDF as bits $x \in \{0, 1\{$ can be encoded as $[Mx]$.

The slight twist here is to substitute the exponentiation g^M by $E(M)$ which is additively homomorphic and the pairing becomes the multiplication introduced earlier (Paillier) when dealing with matrices.

In order, to establish the earlier method for a multi-dimensionnal purpose tensors are considered and instead of matrix multiplication tensor product is adopted.

Let there be the field $\mathbb{G} = GF2$ and vector spaces

$$F \cong \mathbb{G}^{d_1}, M \cong \mathbb{G}^{d_2}, X \cong \mathbb{G}^{d_3}$$

Then $\mathbb{E}$ is a 3-tensors space :

$$\mathbb{E} = F \otimes M \otimes X$$

and let $F^\star = \mathrm{Hom}(F, \mathbb{G})$

Given the action of the group $G = GL(F) \times GL(M) \times GL(X)$ on $\mathbb{E}$ if $(e_1, \dots, e_{d_1})$ is the considered basis for U, the dual basis is $\left(e_1^\star, \dots, e_{d_1}^\star\right)$ for $U^\star$ where $e_i^\star e_j = \delta_{ij};.$

The $(\mathbb{E}; n)$-tensor is as follows:

$$E = \sum_{i=1}^{n} f_i \otimes m_i \otimes x_i$$

for vectors $f_1, \dots, f_n \in F$ being the decomposition of f the Variant Engel Expansion (VEE) one-way function $m_1, \dots, m_n \in M$ those of the message sequence and $x_1, \dots, x_n \in X$ an input sequence of bits.

Let E be a bilinear mapping, the difficulty the attacker would encounter arrises from the bilinear inversion problem which is NP-complete:

Given $E \in \mathbb{T}$ and $z \in X$, find x and y such that $E(x, y) = z$.

Let $d_1 = |F| = d_2 = |M|, d_3 = |X|$ and $\mathbb{E}$ the space of bilinear mappings

$$E : F^\star \times M^\star \to X$$
$$E(x, y) = E \cdot (x \otimes y)$$

So

$$(E(x, y))_k = \sum_{i,j} E_{i,j,k} x_i y_j \quad \text{for } k \in \{1, \dots, m\}$$

The public key is E and the private key is the decomposition $f_1, \dots, f_{d_3} \in F, v_1, \dots, v_{d_3} \in M, w_1, \dots, w_{d_3} \in X$.

The one-way function is the bilinear map

$$T : \mathbb{F}^{2d_1} \to \mathbb{F}^{d_3}, (x, y) \to T(x, y) = z$$

taking m and n two factors (a_i) of the VEE expansion such that $n < m$, leaving the problem NP-Hard, thus the robustness of the encryption scheme.

VII. Conclusion

Ergodic theory is a gathering of number theory, probability theory, group actions of homogenous spaces and other fields. An additional concept may arise and can be relied on, the one of asymptotic average weak independence much stronger which is *mixing*, deriving from the *Birkhoff's ergodic theorem.*

This notion presented the opportunity to entangle LTFs from another point of view, the seed of the system became the parameter of the key generation algorithm, while the VEE designed in this paper outputs the one-way trapdoor function, and the chaotic behaviour made the lossy mode accessible through the ergodic property.

Over the line of this work, this new construction combines both aspects of number theory problem and a chaos theory: the use of a lossy trapdoor function was aimed towards fixing revolving issues surrounding multi-party communications, while using the DDH for exchange, thus making a sound proof to what may become a IND-CCA resistant scheme, especially if studied in the future along distributed systems or adopted in certain communication protocols.

REFERENCES

[1] Erdös, P., Rényi, A., and Szüsz, P., (1958) 'On Engel's and Sylvester's series', Ann. Univ. Sci. Budapest, Eötvös Sect. Math. 1, 7-32.

[2] Kocarev, L., Lian, S., (2011) 'Chaos-Based Cryptography, Theory, Algorithms and Applications', *Studies in Computational Intelligence*, springer, Volume 354.

[3] Ganatsiou, Ch., (1997) 'On the stochastic behaviour of the digits in the modified Engel-type alternating series representations for real numbers', *IBSG Proceedings 5*, IProceedings of the Workshop on Global Analysis, Differential Geometry, Lie Algebra's, Aristotle University of Thessaloniki, July 1997, Balkan Society of Geometry, Geometry Balkan Press, Bucharest - Romania, 33-39.

[4] Akhshani, A., Akhavan, A., Mobaraki, A., Lim, S. C., Hassan, Z., (1994) 'Pseudo random number generator based on quantum chaotic map', *Commun Nonlinear Sci Numer Simulat*, 19, 101-111.

[5] Bolo, V. J., Benitez, R., (2013) 'The wavelet scalogram in the study of time series', *XXIII Congreso de Ecuaciones Diferenciales y Aplicaciones XIII Congreso de Matematica Aplicada*, pp. 1-8.

[6] Peikert, C., Waters, B., (2008) 'Lossy trapdoor functions and their applications', *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, STOC 2008, ACM, 2008, pp. 187–196.

[7] Boyen, X., Waters, B., (2010) 'Shrinking the keys of discrete-log-type lossy trapdoor functions', *Applied Cryptography and Network Security, 8th International Conference*, ACNS 2010, 2010, pp. 35–52.

[8] Rosen, A., Segev, G., (2009) 'Chosen-ciphertext security via correlated products', *Theory of Cryptography, 6th Theory of Cryptography Conference*, TCC 2009, in: LNCS, vol. 5444, Springer, 2009, pp. 419–436.

[9] Kiltz, E., Mohassel, P., O'Neill, A., (2010) 'Adaptive trapdoor functions and chosen-ciphertext security', *Advances in Cryptology – EUROCRYPT 2010*, LNCS, vol. 6110, Springer, 2010, pp. 673–692.

[10] Hu, H., Yu, Y., Zhao, Y., (2017) 'A note on approximation efficiency and partial quotients of Engel continued fractions', *International Journal of Number Theory Vol. 13, No. 9 (2017) 2433–2443*, World Scientific Publishing Company.

[11] Lasota, A. and Mackey, M. C., (1994) 'Chaos, Fractals, and Noise: Stochastic Aspects of Dynamics', *ISecond Edition, Applied Mathematical Sciences*, vol. 97.

[12] Barrow, J. D., (2000) 'Chaos in Numberland: The secret life of continued fractions', *plus.maths.org.*

[13] Euler, L., (1987) 'Introduction à l'analyse infinitésimale', *ACL-Editions*, 1987.

[14] Paillier, P., (1999) 'Public-key cryptosystems based on composite-degree residuosity classes', *Advances in Cryptology-EUROCRYPT'99, Lecture Notes in Computer Science*, vol. 1592, ed. J. Stern. Springer-Verlag, Berlin, 223–238.

[15] Alexeev, B., Forbes, M., and Tsimerman, J., (2011) 'Tensor rank: some lower and upper bounds', *Preprint arXiv:1102.0072v1*, 2011.

[16] Döttling, N., and Garg, S., (2017) 'Identity-based encryption from the Diffie-Hellman assumption', *Advances in Cryptology - CRYPTO*, pages 537–569, 2017.

[17] Hemenway, B., Ostrovsky, R., (2009) 'Lossy trapdoor functions from smooth homomorphic hash proof systems', *Electronic Colloquium on Computational Complexity*, (ECCC), 16:127.

[18] Bresson, E., Catalano, D., and Pointcheval, D., (2003) 'simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications.', *ASIACRYPT 2003, LNCS 2894*, p. 37–54. Springer, 2003.

[19] Hasegawa, S., Isobe, S., Shizuya, H., and Tashiro, K., (2009) 'On the pseudo-freeness and the CDH assumption', *International Journal of Information Security*, 8(5):347–355, 2009.

[20] Partala, J., (2011) 'Key agreement based on homomorphisms of algebraic structures', *Cryptology ePrint Archive* , report 2011/203, 2011.

[21] Kitagawa, F., and Matsuda, T., (2019) 'Cpa-to-cca transformation for KDM security', *Theory of Cryptography TCC*, pages 118–148, 2019.

[22] Chunming Xu, Yong Zhang, and Zhenglan Gu,(2020) 'A Novel Color Image Encryption Method Based on Sequence Cross Transformation and Chaotic Sequences', *Engineering Letters*, vol. 28, no.4, pp1088-1092, 2020.

[23] Kuang YueJuan, Li Yong, and Li Ping, (2020) 'A Searchable Ciphertext Retrieval Method Based on Counting Bloom Filter over Cloud Encrypted Data', *IAENG International Journal of Computer Science*, vol. 47, no.2, pp271-277, 2020.

[24] Xiangli Bu, Ning Wu, Fang Zhou, Muhammad Rehan Yahya, and Fen Ge, (2019) 'A Compact Implementation of SM4 Encryption and Decryption Circuit', *Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2019*, 22-24 October, 2019, San Francisco, USA, pp73-77.