Communications in Mathematics and Applications
Vol. 8, No. 2, pp. 183–189, 2017
ISSN 0975-8607 (online); 0976-5905 (print)
Published by RGN Publications

http://www.rgnpublications.com

Special Issue on
Numerical Analysis and Applications
Editor: Prof. Dr. Abdalah Rababah

Cryptanalysis of A New Method of Cryptography using Laplace Transform Hyperbolic Functions

Research Article

M. Tuncay Gençoğlu

Vocational School of Technical Sciences, Firat University, 23119 Elazig, Turkey
***Corresponding author:** mt.gencoglu@firat.edu.tr

Abstract. Although Laplace Transform is a good application field in the design of cryptosystems, many encryption algorithm proposals become unsatisfactory for secure communication since cryptanalysis studies are not sufficient. One of the important factors resulting in poor proposals is the fact that security analysis of the proposed encryption algorithms is performed with only statistical tests and experimental results. In this study, a general attack scenario was given in order to conduct security analyses of Laplace Transform based cryptosystems. The application of proposed general attack scenario was shown on recently proposed Laplace Transform based encryption scheme.

Keywords. Laplace transform; Cryptography; Cryptanalysis; A general attack scenario

MSC. 92D25

Received: February 6, 2017 **Revised:** April 29, 2017 **Accepted:** May 30, 2017

1. Introduction

Several encryption algorithms were designed by using the dynamics which were presented by Laplace Transform system for cryptographic applications [1–5]. However, security analyses

of the proposed algorithms in several designs were shown by using experimental results and statistical tests [6–10]. The resistance of algorithm to brute force attack was correlated to the number of parameters which are only used in key production. Eventually, the weakness of these Laplace Transform based cryptosystem designs is shown by using simple.

The fundamental difficulty of designing a cryptosystem is to express with a mathematical model for structures used in encryption architecture then to prove that these structures are cryptographically secure. Indeed, approaching problem with a cryptanalyst point of view while designing encryption scheme will disappear several possible problems which may exist in further stages. Same situation is valid for Laplace Transform based cryptology, as well. A Laplace Transform based text encryption algorithm was proposed in [3]. Security analyses of the proposed algorithm were done only by using statistical tests and experimental results. In this study, cryptanalysis of the proposed algorithm was performed. Firstly, a general attack scenario was given for cryptanalysis; secondly, how to obtain plaintext from ciphertext was shown using this scenario without knowing key parameter. In the last section, obtained results were discussed and some general proposals were presented.

2. Description of the Encryption Algorithm

Fundamental of the proposed encryption algorithm depends on encryption of the letters with substitution method produced with the help of a Laplace transform. Encryption process is carried out by using of Taylor series. Since the proposed algorithm is a symmetrical encryption algorithm, in the beginning a secret key in between sender and receiver is determined. The encryption algorithm steps are as follows:

Step 1: Before starting encryption process, sender and receiver agree on a key.

Step 2: Laplace Transform which will be used in the algorithm is determined. Hyperbolic functions were used in the proposed encryption algorithm. Standard expansion of Hyperbolic functions were given in eq. (2.1). Plaintext is determined by using eq. (2.2).

$$\sinh rt = rt + \frac{r^3t^3}{3!} + \frac{r^5t^5}{5!} + \frac{r^7t^7}{7!} + \cdots + \frac{r^{2i+1}t^{2i+1}}{(2i+1)!} + \cdots = \sum_{i=0}^{\infty} \frac{(rt)^{2i+1}}{(2i+1)!}, \tag{2.1}$$

where $r \in N$ is a constant,

$$t^2 \sinh 2t = 2t^3 + \frac{2^3t^5}{3!} + \frac{2^5t^7}{5!} + \frac{2^7t^9}{7!} + \cdots + \frac{2^{2i+1}t^{2i+3}}{(2i+1)!} + \cdots = \sum_{i=0}^{\infty} \frac{2^{2i+1}t^{2i+3}}{(2i+1)!}. \tag{2.2}$$

It allocated 0 to A and 1 to B then Z was 25.

Step 3: Given plaintext “SECURENET” was equivalent to

18 4 2 20 17 4 13 4 19.

Recognizing coefficients that $G_0 = 18$, $G_1 = 4$, $G_2 = 2$, $G_3 = 20$, $G_4 = 17$, $G_5 = 4$, $G_6 = 13$, $G_7 = 4$, $G_8 = 19$, $G_n = 18$ for $n \geq 9$.

Writing these numbers as a coefficients of $t^2 \sinh 2t$, and assuming $f(t) = Gt^2 \sinh 2t$, we get

$$\begin{aligned} f(t) &= \left[G_0 \cdot 2t + G_1 \frac{2^3 t^3}{3!} + G_2 \frac{2^5 t^5}{5!} + G_3 \frac{2^7 t^7}{7!} + G_4 \frac{2^9 t^9}{9}! + G_5 \frac{2^{11} t^{11}}{11!} + G_6 \frac{2^{13} t^{13}}{13!} \right. \\ &\quad \left. + G_7 \frac{2^{15} t^{15}}{15!} + G_8 \frac{2^{17} t^{17}}{17!} \right] \\ &= \sum_{i=0}^{\infty} \frac{2^{2i+1} t^{2i+3}}{(2i+1)!} G_i \qquad (2.3) \\ &= 18 \frac{2t^3}{1!} + 4 \frac{2^3 t^5}{3!} + 2 \frac{2^5 t^7}{5!} + 20 \frac{2^7 t^9}{7!} + 17 \frac{2^9 t^{11}}{9!} + 4 \frac{2^{11} t^{13}}{11!} + 13 \frac{2^{13} t^{15}}{13!} + 4 \frac{2^{15} t^{17}}{15!} + 19 \frac{2^{17} t^{19}}{17!}. \end{aligned}$$

Step 4: Taking Laplace transform on both sides He have

$$\begin{aligned} L\{f(t)\} &= L\{Gt^2 \sinh 2t\} \\ &= \frac{216}{s^4} + \frac{640}{s^6} + \frac{2688}{s^8} + \frac{184320}{s^{10}} + \frac{957440}{s^{12}} + \frac{1277952}{s^{14}} + \frac{22364160}{s^{16}} \\ &\quad + \frac{35651584}{s^{18}} + \frac{851705856}{s^{20}}. \qquad (2.4) \end{aligned}$$

Adjusting the resultant values

216 640 2688 184320 957440 1277952 35651584 851705856 to mod 26,

216 = 8 mod 26, 640 = 16 mod 26, 2688 = 10 mod 26, 184320 = 6 mod 26,

657440 = 16 mod 26, 1277952 = 0 mod 26, 22364160 = 0 mod 26,

35651585 = 20 mod 26, 851705856 = 14 mod 26.

Step 5: Sender sends the values (These are quotients in the mode operation.)

8 24 103 7089 36824 49152 860160 1371214 32757917 as a key.

$G'_0 = 8$, $G'_1 = 16$, $G'_2 = 10$, $G'_3 = 6$, $G'_4 = 16$, $G'_5 = 0$, $G'_6 = 0$, $G'_7 = 20$, $G'_8 = 14$, $G'_n = 0$ for $n \geq 9$.

The given plain text was converted to ciphertext

8 16 10 6 16 0 0 20 14.

The message “SECURENET” was converted to “IQKGQAAUO”.

3. A General Attack Scenario for Laplace Transform based Encryption Schemes

Below, a general attack scenario which a cryptanalyst can use while analyzing any Laplace transform based encryption schemes was briefly summarized.

Case 1: The structures used in encryption scheme must be expressed with a mathematical model. It must be investigated if the model can be expressed with simpler equations or cannot and, if exist, algebraic dependencies must be revealed.

Case 2: Encryption system must be shown to be resistant to known attacks. According to Taylor series expansion (Laplace Transform) and modular arithmetic of principle; it should be assumed that the attacker knows everything except secret key in encryption scheme and what kind of things can be obtained with specifically chosen plaintext/cipher text pairs about encryption scheme should be investigated.

Case 3: Since the security of encryption algorithm is dependent on chosen key space, the specifications which can be done on key space must be investigated. Key design algorithm must be expressed mathematically; the existence of poor keys caused by design must be investigated.

Case 4: Topological properties of Laplace Transform systems used in encryption architecture should be investigated in detail. It must not be forgotten that the required confusion and diffusion properties which cryptographic systems need to be secure are provided by Laplace Transform used in encryption scheme.

Case 5: The problems which can occur because of divide rules when Laplace Transform systems and mode are carried out on digital computers must be investigated. Although very strong structures are used, special attacks to the design must be investigated by taking into account that the tiniest opening can affect entire system.

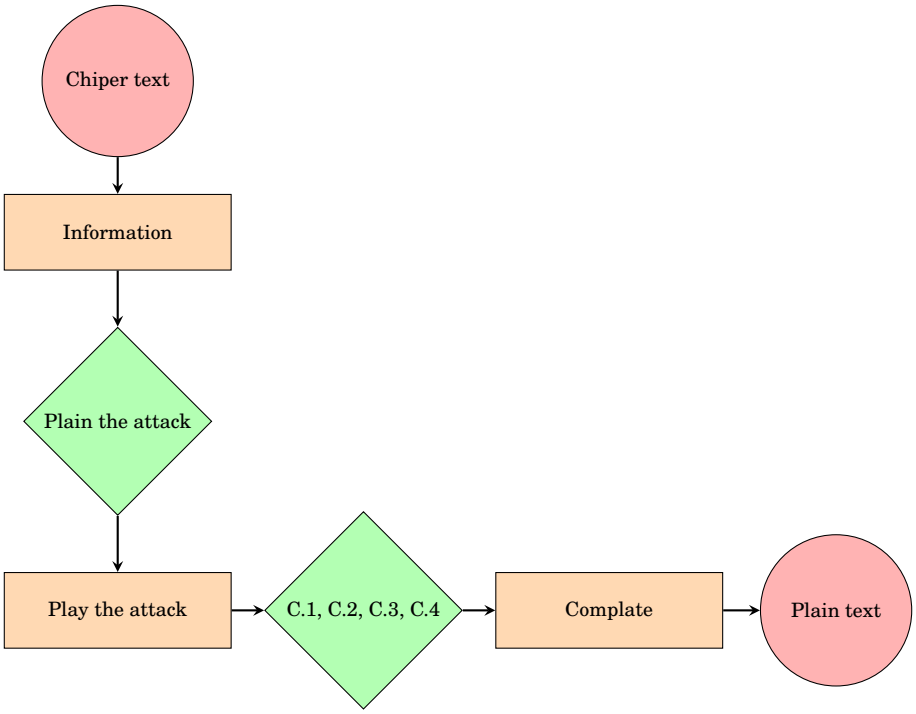

Figure 1. Flow Chart of Proposed Attack Scenario

4. Cryptanalysis

In this section, how a cryptanalysis is carried out by applying the attacks scenario given in previous section on to the proposed Laplace Transform based text encryption algorithm [3] step by step was demonstrated. Encryption architecture was expressed with a simple mathematical model as shown in eq. (4.1). In the proposed algorithm, it was stated that a relationship between numbers correspond to cipher text and modular arithmetic exists. It is not necessary to know the secret key since cipher is solved according to modular arithmetic principle. The existence of dependencies in between numbers correspond to cipher text and modular arithmetic is one of the drawbacks in algorithm.

$$L\left\{\sum_{i=0}^{\infty}\frac{2^{2i+1}t^{2i+3}}{(2i+1)!}G_i\right\}=\sum_{i=0}^{\infty}\frac{2^{2i+1}\cdot(2i+3)!}{(2i+1)!\cdot s^{2i+4}}G_i\,. \tag{4.1}$$

Encrypted text is converted to numbers with the method used by the author;

"IQKGQAAUO" → 8 16 10 6 16 0 0 20 14.

These numbers were obtained in eq. (4.1). Then, we get

$$\begin{aligned}&G_0\cdot\frac{2\cdot 3!}{1!\cdot s^4}+G_1\cdot\frac{2^3\cdot 5!}{3!\cdot s^6}+G_2\cdot\frac{2^5\cdot 7!}{5!\cdot s^8}+G_3\cdot\frac{2^7\cdot 9!}{7!\cdot s^{10}}+G_4\cdot\frac{2^9\cdot 11!}{9!\cdot s^{12}}+G_5\cdot\frac{2^{11}\cdot 13!}{11!\cdot s^{14}}\\&+G_6\cdot\frac{2^{13}\cdot 15!}{13!\ddot{s}^{16}}+G_7\cdot\frac{2^{15}\cdot 17!}{15!\cdot s^{18}}+G_8\cdot\frac{2^{17}\cdot 19!}{17!\cdot s^{20}}\,.\end{aligned} \tag{4.2}$$

Since $G_i\le 25$ and numbers have used equivalents in mod 26, we get

$$G_0\cdot 12=26\cdot K_0+8\Rightarrow G_0=\frac{26\cdot K_0+8}{12}\Rightarrow\begin{cases}K_0=2 \text{ for } G_{0,1}=5\\K_0=8 \text{ for } G_{0,2}=18,\end{cases}$$

$$G_1\cdot 160=26\cdot K_1+16\Rightarrow G_1=\frac{26\cdot K_1+16}{160}\Rightarrow\begin{cases}K_1=24 \text{ for } G_{1,1}=4\\K_1=104 \text{ for } G_{1,2}=17,\end{cases}$$

$$G_2\cdot 1344=26\cdot K_2+10\Rightarrow G_2=\frac{26\cdot K_2+10}{1344}\Rightarrow\begin{cases}K_2=103 \text{ for } G_{2,1}=2\\K_2=775 \text{ for } G_{2,2}=15,\end{cases}$$

$$G_3\cdot 9216=26\cdot K_3+6\Rightarrow G_3=\frac{26\cdot K_3+6}{9216}\Rightarrow\begin{cases}K_3=2481 \text{ for } G_{3,1}=7\\K_3=7089 \text{ for } G_{3,2}=20,\end{cases}$$

$$G_4\cdot 56320=26\cdot K_4+16\Rightarrow G_4=\frac{26\cdot K_4+16}{56320}\Rightarrow\begin{cases}K_4=36824 \text{ for } G_4=17,\end{cases}$$

$$G_5\cdot 319488=26\cdot K_5+0\Rightarrow G_0=\frac{26\cdot K_5}{319488}\Rightarrow\begin{cases}K_5=49152 \text{ for } G_{5,1}=4\\G_{5,2}=17,\end{cases}$$

$$G_6\cdot 1720320=26\cdot K_6+0\Rightarrow G_6=\frac{26\cdot K_6}{1720320}\Rightarrow\begin{cases}K_6=860160 \text{ for } G_6=13,\end{cases}$$

$$G_7 \cdot 8912896 = 26 \cdot K_7 + 20 \Rightarrow G_7 = \frac{26 \cdot K_7 + 20}{8912896} \Rightarrow \begin{cases} K_7 = 1371214 \text{ for } G_{7,1} = 4 \\ G_{7,2} = 17, \end{cases}$$

$$G_8 \cdot 44826624 = 26 \cdot K_8 + 14 \Rightarrow G_8 = \frac{26 \cdot K_8 + 14}{44826624} \Rightarrow \begin{cases} K_8 = 32757917 \text{ for } G_8 = 19, \end{cases}$$

18 4 2 20 17 4 13 4 19 → “SECURENET”.

5. Conclusion

A symmetrical encryption algorithm was proposed by Hiwarekar [3]. In the proposed algorithm, by using modular arithmetic the secret key detected between sender and receiver and ciphertext solved. Namely; proposed encryption algorithm without knowing the key is broken only by seeing encrypted text. Therefore, claimed by author “For the breaking a key of 256 bit by Brute force attack when faster super computer are used” is disabled also the password is broken without a computer with simple divisibility and module theory.

Competing Interests

The authors declare that they have no competing interests.

Authors’ Contributions

All the authors contributed significantly in writing this article. The authors read and approved the final manuscript.

References

[1] D.S. Bodkhe and S.K. Panchal, Use of Sumudu transform in cryptography, *Bulletin of the Marathwada Mathematical Society* **16** (2) (2015), 1 – 6.

[2] A.P. Hiwarekar, A new method of cryptography using Laplace transform, *International Journal of Mathematical Archive* **3** (3) (2012), 1193 – 1197.

[3] A.P. Hiwarekar, A new method of cryptography using Laplace transform of Hyperbolic functions, *International Journal of Mathematical Archive* **4** (2) (2013), 208 – 213.

[4] G. Naga Lakshmi, B. Ravi Kumar and A. Chandra Sekhar, A cryptographic scheme of Laplace transforms, *International Journal of Mathematical Archive* **2** (12) (2011), 2515 – 2519.

[5] M.T. Gençoğlu, Use of integral transform in cryptology, *Science and Eng. J of Fırat Univ.* **28** (2) (2016), 217 – 220.

[6] C. Li and K.-T. Lo, Optimal quantitative cryptanalysis of permutation–only multimedia ciphers against plaintext attacks, *Signal Processing* **91** (2011), 949 – 954.

[7] X. Ge, F. Liu, B. Lu and C. Yang, Improvement of Rhouma’sattacks on Gaoalgorithm, *Physics Letters A* **374** (2010), 1362 – 1367.

[8] M. Safkhani, P. Lopez, J. Hernandez-Castroc and N. Bagheri, Cryptanalysis of the Cho et al. protocol: A hash-based RFID tag mutual authentication protocol, *Journal of Computational and Applied Mathematics* **259** (2014), 571 – 577.

[9] E.B. Kavun, E. Tischhauser and T. Yalçın, Large-scale high-resolution computational validation of novel complexity models in linear cryptanalysis Andrey-Bogdanov, *Journal of Computational and Applied Mathematics* **259** (2014), 592 – 598.

[10] M.T. Sakallı and B. Aslan, On the algebraic construction of cryptographically good 32×32 binary linear transformations, *Journal of Computational and Applied Mathematics* **259** (2014), 485 – 494.