The Dilemma and Prospects of Academic Misconduct in Digital Forensics–A Case Study to Wan's Improved Scheme

Chenglian Liu[1][0000−0002−9086−9740] and Sonia Chien-I Chen[2][0000−0002−6296−4943]

[1] Software Engineering Institute of Guangzhou, Guangzhou 510990, China
liuzl@mail.seig.edu.cn
[2] Qingdao University, Qingdao 266061, China
drsoniachen@qdu.edu.cn

Abstract. In 2019, Wan, Liao, Yan and Tsai proposed an article "Discrete Sliding Mode Control for Chaos Synchronization and Its Application to an Improved ElGamal Cryptosystem". However, Wan et al. just renamed the variable names without modified the core algorithm. Their paper passed review phase and then published. For this case, it is difficult to detect this situation by computer/digital forensics techniques. In this paper the authors would like to point out this dilemmas.

Keywords: ElGamal algorithm · Protocol · Academic misconduct · Plagiarism

1 Erratum

The publisher regrets that error in the drawing of two parameters in Figure 6 of original article [15].

1) On the Master side, the r_m should be corrected to x_s.
2) On the Slave side, the x_s should be corrected to r_m.

It does not make sense, if Master holds r_m or Slave holds x_s, it should occur insecure. On the other hand; it also conflicts with original ElGamal algorithm conception. Please see Figure 1. Therefore, we would rather believe that the original authors Wan et al. just made a mistake in drawing.

2 Our Comments

Wan, Liao, Yan and Tsai [15] proposed an article "Discrete Sliding Mode Control for Chaos Synchronization and Its Application to an Improved ElGamal Cryptosystem" in 2019. They improved well-known public key cryptosystem, namely ElGamal [4] encryption algorithm. In this paper the authors would like to point out some suspicious points. According to "NCKU Regulations for the

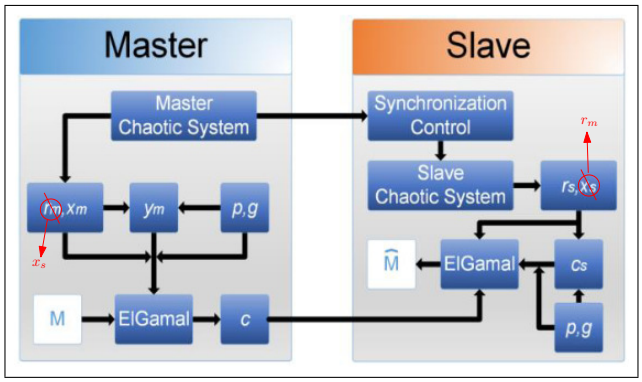

Fig. 1. Drew the wrong two parameters.

Review of Student Academic Ethics Violation Cases" [7], **Article 2:** An academic ethics violation defined herein refers to an academic work produced by an NCKU under or graduate student, including a thesis, discussion, creative work, or performance in fulfilment of a degree demand, or a paper published during their times of study, involving any of the following violations:

1) Fabrication: Creating absent operation documents, exploration accoutrements, or exploration results.
2) Falsification: Falsifying Operation documents, exploration accoutrements, or exploration results.
3) Plagiarism: Use of another existent's operation documents, exploration accoutrements, or exploration results of without proper criterion. indecorous criterion, if set up to be grave, should be treated as plagiarism.
4) Ghost authorship, or textbook written by another in your name.
5) Double or indistinguishable publication without acknowledgement.
6) Substantial citation of one's own preliminarily published work without proper citations.
7) Publishing a restatement as an original publication without acknowledgement.
8) Other acts in violation of academic ethics.

Wan et al. did not involve above seven rules directly, they cleverly avoided the rules, and how they successfully managed to do it? The authors will describe in this section.

2.1 Review Traditional ElGamal encryption algorithm

The ElGamal cryptosystem slides two parts: One is encryption/decryption algorithm, and the other one is digital signature, those are different algorithms. In this subsection, we introduce encryption/decryption algorithm. There are two parties Master and Slave, if Master wants to encrypt message m to Slave. He

does follow steps.
Key Generation Phase:

Step 1. Slave choose a large prime p, and a primitive root $g \in \mathbb{Z}_l^*$.
Step 2. Slave randomly selects an integer x to his secret key where it satisfies $1 < x < p-1$, and $\gcd(x, p-1) = 1$, then compute

$$y \equiv g^x \bmod p. \tag{1}$$

Step 3. Slave publishes public parameters $\{y,\ g,\ p\}$, and keeps secret key x.

Encryption Phase:
Master received the parameters $\{y,\ g,\ p\}$ by Slave. He does follow steps.

Step 1. Master randomly selects an integer r to his secret key where it satisfies $1 < r < p-1$, and $\gcd(r, p-1) = 1$, then compute

$$C_1 \equiv g^r \bmod p. \tag{2}$$

Step 2. Master digitized message m such that $1 < m < p-1$.
Step 3. Master encrypted m to C_2 where

$$C_2 \equiv m \cdot y^r \bmod p. \tag{3}$$

Step 4. Master sends $\{C_1,\ C_2\}$ to Slave.

Decryption Phase:
Slave received $\{C_1,\ C_2\}$, he also do follow steps.

Step 1. Slave recovered message m such that

$$m \equiv (C_1^x)^{-1} \cdot C_2 \bmod p. \tag{4}$$

Proof.

$$\begin{aligned} m' &\stackrel{?}{\equiv} (C_1^x)^{-1} \cdot C_2 \bmod p \\ &\equiv [(g^r)^x]^{-1} \cdot C_2 \bmod p \\ &\equiv y^{-r} \cdot C_2 \bmod p \\ &\equiv y^{-r} \cdot m \cdot y^r \bmod p \\ &\equiv m \bmod p \end{aligned} \tag{5}$$

The protocol see in Figure 2.

2.2 Review Improved ElGamal encryption algorithm

Wan, Liao, Yan and Tsai exchanged Master and Slave player roles in original paper Figure 6. But it does not affect what we discussion here. There are two parties Master and Slave, if Slave wants to encrypt message m to Master. He does follow steps.
Key Generation Phase:

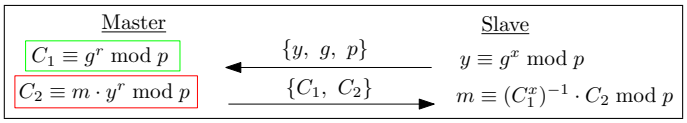

Fig. 2. Traditional ElGamal Protocol.

Step 1. Master choose a large prime p, and a primitive root $g \in \mathbb{Z}_{\mathrm{l}}^*$.
Step 2. Master randomly selects an integer x_m to his secret key where it satisfies $1 < x_m < p-1$, and $\gcd(x_m, p-1) = 1$, then compute

$$y_m \equiv g^{x_m} \bmod p. \tag{6}$$

Step 3. Master publishes public parameters $\{y_m,\ g,\ p\}$, and keeps secret key x_m.

Encryption Phase:
Slave received the parameters $\{y_m,\ g,\ p\}$ by Master. He does follow steps.

Step 1. Slave randomly selects an integer r_s to his secret key where it satisfies $1 < r_s < p-1$, and $\gcd(r_s, p-1) = 1$, then compute

$$C_s \equiv g^{r_s} \bmod p. \tag{7}$$

Step 2. Slave digitized message m such that $1 < m < p-1$.
Step 3. Slave encrypted m to C where

$$C \equiv m \cdot y_m^{r_m} \bmod p. \tag{8}$$

Step 4. Slave sends $\{C_s,\ C\}$ to Master.

Decryption Phase:
Master received $\{C_1,\ C_2\}$, he also do follow steps.

Step 1. Master recovered message m such that

$$m \equiv (C_s^{x_s})^{-1} \cdot C \bmod p. \tag{9}$$

Proof.

$$\begin{aligned} m' &\stackrel{?}{\equiv} (C_s^{x_s})^{-1} \cdot C \bmod p \\ &\equiv ((g^{r_s})^{x_s})^{-1} \cdot m \cdot y_m^{r_m} \bmod p \\ &\equiv ((g^{x_m})^{r_m})^{-1} \cdot m \cdot y_m^{r_m} \quad \bmod p \\ &\equiv y_m^{-r_m} \cdot m \cdot y_m^{r_m} \bmod p \\ &\equiv m \bmod p \end{aligned} \tag{10}$$

The protocol see in Figure 3.

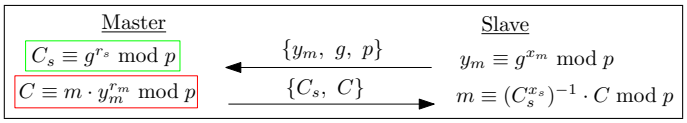

Fig. 3. Improved ElGamal Protocol.

2.3 Compared Traditional and Improved ElGamal algorithm

In this subsection, the authors analyzed and compared two protocol, we obtained some information. The original authors Wan, Liao, Yan and Tsai [15] only changed the variable names as follows:

1) Rename x to x_x, and set $x_s = x_m$.
2) Rename r to r_s, and set $r_s = r_m$.
3) Rename y to y_m.
4) Rename C_1 to c_s.
5) Rename C_2 to C.

If you just renamed the some variable names without modified or changed the protocol or algorithm in itself, it is not considered an improvement scheme. Unfortunately, the original authors Wan, Liao, Yan and Tsai [15], they did that. Please see Figure 4.

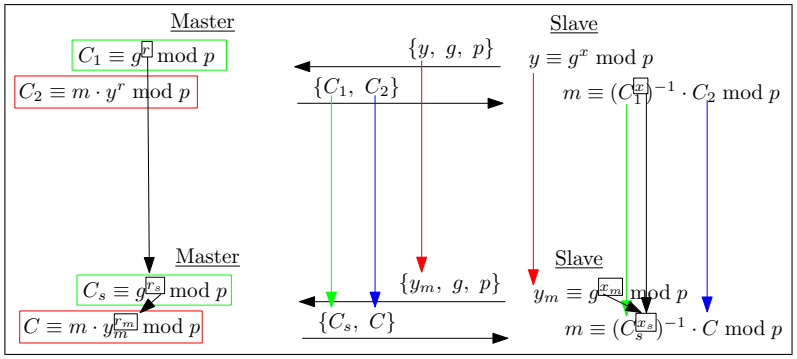

Fig. 4. Compared Traditional and Improved ElGamal Protocol.

3 Discussing Open Questions

About plagiarism and academic misconduct, the University of Cambridge [13] provides clearly definitions, there are include sevens types: 1)Plagiarism, 2)Self-plagiarism, 3)Contract cheating, 4)Collusion, 5)Impersonating someone or being impersonated, 6)Fabrication, falsification or misrepresentation, and 7)Failure to

meet legal, ethical and professional obligations. As indicated by the aforementioned observations. In this section the author would like discuss three parts, the first is on article itself, second is publisher, and third is about forensics.
Article side:

1) Just only rename the variable names without modified the core algorithm, does it belong improvement contribution work?
2) The original authors Wan, Liao, Yan and Tsai claimed they improved the ElGamal algorithm. In the same time, they also provided good testing results in original paper Table 1 to Table 3, and Figure 10. However, we know that this is contradictory because there is essentially no difference between the traditional ElGamal and Improved ElGamal algorithms. Does someone fake experimental data?
3) Is this behavior considered academic misconduct [3]?

Publisher Side: The editor fulfilled the responsibility of technical review, we do not think that software such as iThenticate, Cross Check, Tunitin or other related system can detect problems to Wan et al.'s article. The reviewer is a manual operation stage, which is a role that is difficult to replace by a machine. Unfortunately, the reviewers did not play the role of peer review here.

1) Why reviewers and editors did not found this problem [1, 9, 10]?
2) Are original authors considered academic misconduct [14, 2, 6, 12, 16]?

Forensics Techniques Side: The technologies of text comparison, image text extraction, and image recognition are advanced [11, 8, 5]. However, the cryptographics algorithms are different from ordinary text content. Some mathematical symbols may be extracted, but the algorithm and semantic meaning, whether it is digital forensics or computer forensics, still requires manual interpretation. In particular, cryptographic algorithms are different from ordinary program codes. This job requires people who are engaged in cryptography research (Cryptographer) to perform it, so it has threshold requirements and qualifications.

4 Conclusions

As everyone knows, no matter how powerful a machine is, it cannot replace humans. In this case, there contains mathematical symbols, logical inferences and protocols. Machines cannot recognize as accurately as humans. The reviewer may not necessarily be specialized in this content or field. Thus, we resulted this case in this article. Finally, the authors proved what we claimed.

References

1. Bohannon, J.: Who's afraid of peer review? Science **342**(6154), 60–65 (2013)
2. Bos, J.: Plagiarism, pp. 55–80. Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-48415-6_4

3. Cheng, Y.C., Hung, F.C., Hsu, H.M.: The relationship between academic dishonesty, ethical attitude and ethical climate: The evidence from taiwan. Sustainability **13**(21) (2021). https://doi.org/10.3390/su132111615
4. ElGamal, T.: A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory **31**(4), 469–472 (1985)
5. Jutten, C.: Scientific integrity: A duty for researchers [from the editor]. IEEE Signal Processing Magazine **39**(6), 3–84 (2022). https://doi.org/10.1109/MSP.2022.3198298
6. Krishan, K., Kanchan, T., Baryah, N., Mukhra, R.: Plagiarism in student research: Responsibility of the supervisors and suggestions to ensure plagiarism free research. Science and Engineering Ethics **23**(4), 1243–1246 (Aug 2017). https://doi.org/10.1007/s11948-016-9822-x
7. National Cheng Kung University, Taiwan: NCKU regulations for the review of student academic ethics violation cases. Website (May 2020), https://www.cc.ncku.edu.tw/rule/files/20030000/a17acad_e.pdf
8. Oettinger, W.: Learn Computer Forensics: Your one-stop guide to searching, analyzing, acquiring, and securing digital evidence. Packt Publishing Ltd (2022)
9. Predatory Reports: MDPI peer review problem. Website (October 2023), https://predatoryreports.org/news/f/mdpi-peer-review-problem
10. Retraction Watch: Article that assessed MDPI journals as "predatory"' retracted and replaced. Website (October 2023), https://retractionwatch.com/2023/05/08/article-that-assessed-mdpi-journals-as-predatory-retracted-and-replaced/
11. Rocha, A.: The information forensics and security technical committee: Then, now, and in the future [in the spotlight]. IEEE Signal Processing Magazine **37**(3), 175–176 (2020). https://doi.org/10.1109/MSP.2020.2974447
12. Roostaee, M., Sadreddini, M.H., Fakhrahmad, S.M.: An effective approach to candidate retrieval for cross-language plagiarism detection: A fusion of conceptual and keyword-based schemes. Information Processing Management **57**(2), 102150 (2020). https://doi.org/10.1016/j.ipm.2019.102150
13. University of Cambridge: Plagiarism and academic misconduct. Website (Juy 2023), https://www.plagiarism.admin.cam.ac.uk/definition
14. Uzun, A.M., Kilis, S.: Investigating antecedents of plagiarism using extended theory of planned behavior. Computers Education **144**, 103700 (2020). https://doi.org/10.1016/j.compedu.2019.103700
15. Wan, P.Y., Liao, T.L., Yan, J.J., Tsai, H.H.: Discrete sliding mode control for chaos synchronization and its application to an improved el-gamal cryptosystem. Symmetry **11**(7) (2019). https://doi.org/10.3390/sym11070843
16. Xiong, J., Yang, J., Yan, L., Awais, M., Khan, A.A., Alizadehsani, R., Acharya, U.R.: Efficient reinforcement learning-based method for plagiarism detection boosted by a population-based algorithm for pretraining weights. Expert Systems with Applications p. 122088 (2023). https://doi.org/10.1016/j.eswa.2023.122088