Secure Adaptive RSA Crypto-Systems Are Useless Without Erasures

Deshak Bhatnagar

Abstract- The main aim or objective of this research is to prove that the Secure Adaptive RSA Crypto-Systems in Threshold Cryptography require the erasures as explained by the Research Paper Adaptive Security for Threshold Crypto-Systems. Also, the other primary aim is to draw comparison between two Research Papers i.e. Adaptive Security for Threshold Crypto-Systems and Adaptively Secure Threshold Crypto-Systems Without Erasures which also have a common link between them.

Index Terms- RSA, Threshold, Secure (keywords)

I. INTRODUCTION

RSA stands for Rivest-Shamir-Adleman Algorithm. It is a type of Threshold Crypto-System & used for secure data transmission. A Threshold Crypto-System is the one which intends to protect information by encrypting it and allocating among cluster of computers. The Adaptive Secure Threshold Crypto-Systems are revelation for Algorithms like RSA as they make them fault tolerant & secure by introducing the concept of erasures. The Erasures are used to refresh the sharing of the keys after each signature generation in Adaptive Secure RSA Systems, the generated signatures guarantee that the contents of a message have not been altered in transit. The RSA System has two keys one public & one private key which are used for encryption & decryption respectively.

So, it becomes important that the keys are refreshed each time in order for secure data transmission which led to use of erasures. This research is completely based on drawing the comparisons between the two papers & justifying the need of Erasures for the Secure Adaptive RSA Systems through it.

II. RELATED WORK

The work dates back to 1999 when Ran Canetti, Rosario Gennaro, Stainslaw Jarecki, Hugo Krawezyk, and Tal Rabin that Adaptive Security of Threshold Crypto-Systems is possible. It showed the RSA Algorithm in an adaptively secured way that made it more secure and reliable by assigning partial keys after each signature generation & using Erasures to refresh the sharing of the keys after each signature generation.

Further on no more developments came into it for years, until in early 2020 a group of Researchers named Stainslaw Jarecki, and Anna Lysyanskaya which includes one of the researchers Jarecki who co-wrote the 1999 paper. This new paper is called Adaptively Secure Threshold Crypto-Systems Without Erasures. It says the erasures are not required which are used to refresh the sharing of the keys after each signature generation.

III. METHODOLOGY

This Research is based on the fact of Justifying & Supporting the use of Erasures in RSA for secure transmission & protection of data from unwanted sources. The approach which will be used is simple & does not involve any kind of large mathematical calculations. If any kind of mathematical calculation is performed or found, then it is done only to show the working of RSA System for public and private key generation along with Encryption & Decryption of Plain-Text Message. The Methodology which was used is simple & is called as Comparative Research, it is based & mainly focused on studying two or more different things and then comparing them.

A. 1999 PAPER

The work dates back to 1999 when Ran Canetti, Rosario Gennaro, Stainslaw Jarecki, Hugo Krawezyk, and Tal Rabin that Adaptive Security for Threshold Crypto-Systems is possible. It showed the RSA Algorithm in an adaptively secured way that made it more secure and reliable by assigning partial keys after each signature generation & using Erasures to refresh the sharing of the keys after each signature generation. This process can be simply elaborated with the fact that it was used to solve a problem which was adamant during the complete secret data transfer.

If the Public Key (which is used for encryption) remains same for all then the data can be easily stolen as the private key (which is used for decryption) is also similar due to the fact that partial keys of all players cannot be known thus if any of the player is broken during the simulation or the transfer then it can affect the complete system and further result in bigger consequences like data theft, loss of data & more can even lead to loss of encryption & decryption keys. So, the use of Erasures was an answer to this problem as they refresh the keys after each signature generation which indeed solves this problem. This is achieved in a straightforward manner but with a slight issue that the it adds performance penalty to the whole system.

B. 2020 PAPER

Further on no more developments came into the topic for years, until in early 2020 a group of Researchers named Stainslaw Jarecki, and Anna Lysyanskaya which includes one of the researchers Jarecki who co-wrote the 1999 paper. This new paper is called as Adaptively Secure Threshold Crypto-Systems Without Erasures. And it quotes that the Erasures (which are used to refresh the sharing of the keys after each signature generation) are not required for Secure Adaptive Threshold RSA Crypto-Systems.

It further says that the same results which were obtained using Erasures in 1999 Paper can be achieved using a set of calculations as stated in ELGamal Protocol, which says that: The decryption of a Cipher-Text C or input C uses a signature, accounts to produce the C^n value. The secret key n is shared additively, n= x1+…+xn, that every participant generates C^xi & claims in zero knowledge that log (C^xi) = log (M^xi) where M, M^xi is a message and P partial signature on it. If the participant fails in any situation then the additive share is redeveloped from back-ups. The major difference this protocol puts on the table is that it works without the share-refreshment after each signature generation.

C. COMPARISON

Now coming onto the fact that both the papers are equally right in their place & also take different approaches towards the secure data transmission. The following is the data which were able accumulate from the two:

1. The 1999 Paper focuses more on Threshold RSA System as whole, while the 2020 Paper fails to do that.
2. The 1999 Paper points out the major issue of players being broken during the simulation or gets corrupted and thus Erasures were introduced to counter this fact, while the 2020 Paper project the use of another approach for achieving the Secure Adaptive Threshold RSA System but fails to give a solution to the problem of players getting corrupted & inconsistency in the view.
3. The 1999 Paper was able to layout the fact clearly that the use of Erasures adds a performance penalty to the protocol, while the 2020 Paper does not mention any kind of adversaries to the protocol which is area of concern as it is yet still unknown whether it is capable of safe data transmission or not.

From the above discussions we were able to conclude that the 1999 paper has stronger case than the 2020 Paper and to prove this fact we used Comparative Research. The Research further says that the use of Erasures is Justified & Supported by the fact that the Erasures are necessary is proven by the fact that if the Public Key (which is used for encryption) remains same for all then the data can be easily stolen as the private key (which is used for decryption) is also similar due to the fact that partial keys of all players cannot be known thus if any of the player is broken then it can affect the complete system and further result in bigger consequences.

So, the use of Erasures was an answer to this problem as they refresh the keys after each signature generation. While the 2020 Paper researcher were also not able to resolve this issue and according to them if any of the player in the system becomes corrupt or goes AWOL then it can hamper the complete system and may result in data loss.

IV. CONCLUSION

The proposed work/research aims at ensuring secure data transmission & data protection along with the secrecy of data which is currently is a need of the hour. This Research is based on the Methodology of Comparative Research which means it works by studying two or more groups/things & then comparing them and at last drawing conclusion & argument out of it. Further this Research in whole or total was able to justify

and support the use of the Erasures in RSA Systems for the fact that they are necessary to defend data from being easily stolen due to the fact that partial keys of all players in RSA cannot be known thus if any of the player is broken then it can affect the complete system and further result in bigger consequences, while this can be averted by refreshing the sharing of keys after each signature generation i.e. what Erasures do. Further no contradiction was found to the fact that Erasures are the only solution available as option for this problem currently. Thus, the use of Erasures is justified along with the fact that Secure Adaptive RSA Crypto-Systems need to have the Erasures otherwise they are Useless Without them.

REFERENCES

[1] Jarecki, S., & Lysyanskaya, A. Adaptively secure threshold cryptosystems without erasures. Eurocrypt.

[2] Canetti, R., Gennaro, R., Jarecki, S., Krawczyk, H., & Rabin, T. (1999, August). Adaptive security for threshold cryptosystems. In Annual International Cryptology Conference (pp. 98-116). Springer, Berlin, Heidelberg.

[3] Desmedt, Y., & Frankel, Y. (1989, August). Threshold cryptosystems. In Conference on the Theory and Application of Cryptology (pp. 307-315). Springer, New York, NY.

[4] Milanov, E. (2009). The RSA algorithm. RSA Laboratories, 1-11.

[5] Jonsson, J., & Kaliski, B. (2003). Public-key cryptography standards (PKCS)# 1: RSA cryptography specifications version 2.1 (pp. 1-68). RFC 3447, February.

[6] Desmedt, Y. G. (1994). Threshold cryptography. European Transactions on Telecommunications, 5(4), 449-458.

[7] Katz, J., & Lindell, Y. (2014). Introduction to modern cryptography. CRC press.

[8] Forouzan, B. A. (2007). Cryptography & network security. McGraw-Hill, Inc.

[9] Jarecki, S., & Lysyanskaya, A. (2000, May). Adaptively secure threshold cryptography: Introducing concurrency, removing erasures. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 221-242). Springer, Berlin, Heidelberg.

[10] Goshwe, N. Y. (2013). Data encryption and decryption using RSA algorithm in a network environment. International Journal of Computer Science and Network Security (IJCSNS), 13(7), 9.

[11] Kunihiro, N., Shinohara, N., & Izu, T. (2014). Recovering RSA secret keys from noisy key bits with erasures and errors. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 97(6), 1273-1284.

[12] Henecka, W., May, A., & Meurer, A. (2010, August). Correcting errors in RSA private keys. In Annual Cryptology Conference (pp. 351-369). Springer, Berlin, Heidelberg.

[13] YU, L. C., ZHANG, W., LIN, Q., XU, J. X., & ZHONG, B. (2011). The Application of RS Erasure Codes in the Cloud Storage. Microelectronics & Computer, 28(8), 234-236.

[14] Threshold Cryptography. Retrieved from https://wikipedia.org/wiki/Thresold_cryptosystems