RSA and El-Gamal Cryptosystems

Yanan Xiao, *Student Member, IEEE* Maryam Al Mehrezi

Abstract—We present our analysis of RSA and ElGamal cryptosystem with great detail. We show that there are some attacks on RSA. The mathematical foundation of ElGamal cryptosystem, namely discrete logarithm problem is discussed. Basic structure of our implementation codes is also mentioned.

Keywords—RSA, El-Gamal, implementation, public key, cryptosystem

1 Introduction

PUBLIC key cryptosystem. The rest

2 Public Key Cryptosystem

2.1 More Details

Some problems with this template...I mean, the subsubsection part.

3 RSA Cryptosystem

This is just another testing case.

4 El-Gamal Cryptosystem

As stated in the Section 1, after the introduction of public key cryptosystems concept by Diffie and Hellman in [1], a lot of trials and errors have been made to find feasible cryptosystems. The security of RSA system discussed above has much to do with large integers factorization. The knapsack public key encryption scheme relies on the complexity of subset sum problem, which is NP-complete [2]. The first example of *provably secure* public key encryption scheme, i.e. the Rabin scheme, is based on the problem of finding square roots of a modulo a prime. In a more generic manner, the Rabin encryption scheme is derived from the problem of finding d^{th} roots in a finite field, which is intensively discussed in [3]. In this section, we discuss another cryptosystem that is still being widely used, i.e. ElGamal cryptosystem.

It is well recognized that the ElGamal cryptosystem could be regarded as Diffie-Hellman key agreement [4] in key transfer mode. Thus, the security of ElGamal cryptosystem has much to do with the intractability of discrete logarithm problem as well as the Diffie-Hellman problem. We analyze them one by one thereafter. We follow the definition style in [5].

4.1 Diffie-Hellman Problem

The Diffie-Hellman key exchange agreement and its derivatives, alongside with ElGamal public key encryption scheme are formed on the basis of Diffie-Hellman problem.

Definition The Diffie-Hellman problem (DHP): find $\alpha^{ab} \mod p$, provided that a prime p, a generator α of Z_p^*, and elements $\alpha^a \mod p$ and $\alpha^b \mod p$

Definition The *generalized Diffie-Hellman problem (GDHP)*: find α^{ab}, provided that a finite cyclic group G, a generator α of G, and group elements α^a and α^b are known.

The link between Diffie-Hellman problem and discrete logarithm problem (DLP) is established as follows. Under the assumption that it is easy to solve discrete logarithm problem in Z_p^*, one is able to compute a from α, p, $\alpha^a \mod p$ by way of solving a discrete logarithm equation. And then he can compute $\left(\alpha^b\right)^a = \alpha^{ab} \mod p$ with the knowledge of $\alpha^b \mod p$ at the same time.

The most recent findings still show that it remains unknown whether generalized discrete

• *Yanan Xiao and Maryam Al Mehrezi are with the Department of Electrical Engineering and Computer Science, Masdar Institute of Science and Technology, Masdar City, Abu Dhabi, UAE, 54224.*
E-mail: {yxiao,malmehrezi}@masdar.ac.ae

logarithm problem (GDLP) and GDHP are computationally equivalent. Nevertheless, we summarize some recent progress with regard to this open problem below. The Euler phi function is marked as ϕ. B-smooth is defined under the fact that all prime factors of an integer are $\leq B$. (B is a given positive integer.)

1) Assume that p is a prime and the factorization of $p-1$ is known. Under the circumstance that $\phi(p-1)$ is B-smooth, in which $B = O((\ln p)^c)$ for some constant c, the DHP and DLP in Z_p^* are computationally equivalent. Proof of this statement can be found in [6].
2) A more general case is that when G is an order n finite cyclic group where the factorization of n is known. In this case we can also conclude the GDHP and GDLP in G are computationally equivalent.
3) In this situation, group G is assumed to have the same property as above. When either $p-1$ or $p+1$ for p as a prime divisor of n is B-smooth (B has the same property as above, too), we then conclude that the GDHP and GDLP in G are computationally equivalent. Proof of this statement, and some stronger ones can be found in [7].

Diffie-Hellman key exchange scheme is based on the Diffie-Hellman problem discussed above. It was proposed by Whitfield Diffie and Martin Hellman in *New Directions in Cryptography* [1]. What's more important in their invited paper is that they carefully examined two kinds of then contemporary development in cryptography, and shed light on methods of utilizing theories of communication and computation as tools to solve future cryptography problems. The Diffie-Hellman key exchange scheme has been widely used in Secure Shell (SSH), Transport Layer Security (TLS), and Internet Protocol Security (IPSec) since its proposal. Moreover, it is a key exchange protocol and *not* used for encryption. On the other hand, the ElGamal cryptosystem that is discussed below can be employed in both encryption and digital signature.

Diffie-Hellman key exchange scheme serves as a fundamental technique which provides unauthenticated key exchange. Herein we analyze the basic Diffie-Hellman protocol and briefly introduce some related ones which provide various authentication assurances.

As the first practical key exchange scheme proposed to tackle key distribution problem, which becomes with an urgent issue after the discovery of public key cryptosystem, Diffie-Hellman key exchange scheme (also called *exponential key exchange*) makes it possible that two parties of communication can establish a common secrete, which is strongly against eavesdropping theoretically, by way of a simple exponential calculation through an open channel. And this seemingly unrealistic approach is done without the prerequisite of, say Alice and Bob having met each other before or shared critical component of the scheme in advance. However, the primitive Diffie-Hellman technique has its defects. Even though this sort of protection performs well when eavesdroppers (passive adversaries) are cutting in the communication, it lacks key procedures to protect users from active adversaries who possess the ability to intercept, modify or inject messages. As reflected in Fig. 1, in real world communication scenarios, neither party (of one specific communication) can 100% tell that the source identity of the incoming message is the one it makes the request for. The identity of the other party may be the one that "happenly" know the resulting key, i.e. entity authentication or key authentication.

In order to deal with key authentication issue brought up by basic Diffie-Hellman key exchange scheme, a simple method is to set α^x and $\alpha^y \mod p$ constant public keys for the corresponding parties. In this way, these public keys can be distributed through signed certificates, and the problem of long-term shared key is "seemingly" fixed. When such certificates are available *a prior*, key exchange process evolves into a zero-pass key exchange scheme, which no cryptographic message is required to finish the exchange. Nevertheless, an obvious drawback is that as *a prior*, once being hacked, all messages encrypted with this key are under attack. One solution for this drawback is proposed as MTI/A0 key exchange protocol in [8].

SUMMARY: A and B communicates with each other through open channel. In this simplified case, they are sending the other one message.
RESULT: A common secrete known to both A and B is established.

1. *One-time Setup.* Select and publish an appropriate prime p and generator α of Z_p^*.

2. *Protocol messages.*

$$A \rightarrow B : \alpha^x \mod p \tag{1}$$

$$A \leftarrow B : \alpha^y \mod p \tag{2}$$

3. *Protocol actions.* Each time a shared key is required, the following actions would be carried out.

1) A selects some random secrete x, $1 \leq x \leq p-2$. Then sends B message (1).
2) B selects some random secrete y, $1 \leq y \leq p-2$. Then sends A message (2).
3) B computes $K = (\alpha^x)^y \mod p$ as the shared key after receiving α^x.
4) A computes $K = (\alpha^y)^x \mod p$ as the shared key after receiving α^y.

Fig. 1. **Protocol** Diffie-Hellman key exchange scheme (basic version)

4.2 Basic El-Gamal Encryption

Well, I really want to finish those stuff as soon as possible. In this way I have to abort something else.

4.3 Generalized El-Gamal Encryption

Life is so damn hard. Isn't it? Just another

4.4 El-Gamal in Digital Signature

4.5 Some Possible Attacks

5 Implementation

Implementation process will be discussed here. Let the hunt begin [4].

5.1 RSA

5.2 El-Gamal

6 Conclusion

Conclusion and Contributions.

Appendix A
Proof of the First Zonklar Equation

Appendix one text goes here.

Appendix B
Some related math stuff will be displayed here

Appendix two text goes here.

ACKNOWLEDGMENTS

The authors would like to thank Dr. Zeyar for his amazing lectures throughout the semester, as well as assigning us a challenging but rewarding project like this. In addition, we would show our gratitude to Masdar Institute for creating the world-class research environment.

REFERENCES

[1] W. Diffie and M. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, 1976.

[2] A. M. Odlyzko, "The rise and fall of knapsack cryptosystem," *Cryptology and Computational Number Theory*, vol. 42, pp. 75–88, 1990.

[3] E. Bach and J. Shallit, *Algorithmic Number Theory*. Cambridge, Massachusetts: MIT Press, 1996, vol. 1: Efficient Algorithms.

[4] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *Information Theory, IEEE Transactions on*, vol. 31, no. 4, pp. 469–472, 1985.

[5] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 2010.

[6] B. Boer, "Diffie-hellman is as strong as discrete log for certain primes," in *Advances in Cryptology CRYPTO 88*, ser. Lecture Notes in Computer Science, S. Goldwasser, Ed. Springer New York, 1990, vol. 403, pp. 530–539. [Online]. Available: http://dx.doi.org/10.1007/0-387-34799-2_38

[7] U. Maurer, "Towards the equivalence of breaking the diffie-hellman protocol and computing discrete logarithms," in *Advances in Cryptology CRYPTO 94*, ser. Lecture Notes in Computer Science, Y. Desmedt, Ed. Springer Berlin Heidelberg, 1994, vol. 839, pp. 271–281. [Online]. Available: http://dx.doi.org/10.1007/3-540-48658-5_26

[8] T. MATSUMOTO, Y. TAKASHIMA, and H. IMAI, "On seeking smart public key distribution systems," *The Transactions of the IECE of Japan*, vol. E69, no. 2, pp. 99–106, Feb. 1986.

Yanan Xiao is a first year master student at Masdar Institute. For his undergraduate, he spent three years in information security related area, mainly computer networks. Right now he is with Dr. Chi-Kin Chau to earn his MSc degree. His research interests are wireless networks, embedded systems and all kinds of algorithms. When he does not have much research workload, he usually takes some tea while reading books.

Maryam Al Mehrezi is a first year master student at Masdar Institute.

sizes