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 th at aprime 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 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 $(\alpha^b)^a = \alpha^{ab} \mod p$ 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.)

- Assume that

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.

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