A new public key encryption scheme provably secure against adaptive chosen cipher-text attack

Huafei ZHU

June 10, 2002

Department of Information and Electronics Engineering, Zhejiang University,
Hangzhou, 310027, PR. CHINA
Email: zhuhf@isee.zju.edu.cn

Abstract We present a new public key cryptosystem based on the notion called square decisional Diffie-Hellman problem. The scheme is provably secure against adaptive chosen cipher-text attack under the hardness assumption of the square decisional Diffie-Hellman problem. Compared with Cramer and Shoup's notable public key scheme, our scheme enjoys several nice features: (1)Both schemes are provably secure against adaptive chosen cipher-text attack under the intractability paradigm (the security of Cramer-Shoup's scheme is based on the standard decisional Diffie-Hellman problem while ours based on the square decisional Diffie-Hellman problem; (2)The computational and communication complexity of our scheme is equivalent to the Cramer and Shoup's scheme however, the test function of Cramer-shoup's scheme is linear while our scheme is non-linear, therefore our reduction is more efficient.

1 Introduction

The construction of secure encryption scheme is one of the most exciting research areas in modern cryptography. A public key encryption scheme is

secure definitely related to the ability of an adversary. There are three basic models related to the definitions of security: 1) Semantic secure: a public key encryption scheme is said semantic secure, which is first mentioned by Goldwasser and Micali [GM], if an adversary should not be able to obtain any partial information about a message given its cipher-text. 2) Secure against chosen cipher-text attack: a public key encryption scheme is said secure against chosen cipher-text attack (or lunch time attack or midnight attack), developed by Naor and Yung [NY], if an adversary, who has access to the decryption oracle before a target cipher-text is given, is not able to extract any information of message. 3) Secure against adaptive chosen cipher-text attack: a public key encryption scheme is called secure against adaptive chosen cipher-text, which is developed by Rackoff and Simon [RS], if an adversary, who has access the decryption oracle even after the target cipher-text is given and the adversary can query the decryption oracle any cipher-text but the target cipher-text, is unable to extract any information about the message. Rackoff and Simon's the strongest definition of security allows the crypto-system to be deployed in the widest range of applications. Due to the excellent works of Bellare et. al [BDPR], the notion of security against adaptive chosen cipher-text attack is equivalent to the notion of non-malleable property under adaptive chosen cipher-text attack introduced by Dolev, Dwork and Naor [DDN].

To study the security of a newly developed identification, one could employ two standard models - random oracle model and standard intractability model, we therefore sketch the two models a bit more details below:

Random oracle paradigm: The random oracle paradigm, an ideally random and imaginary oracle, is assumed when one proving the security of cryptographic algorithms[BR]. A random oracle H generates an answer randomly to the query posted to H at first, if the same query is asked later, H will answer the same value as was provided to the first query. The main advantage using of random oracle paradigm is that it can much more easily provide concrete security analysis, which avoids complexity theory and asymptotic theory. In practice, a random oracle is replaced by a random-like hash function such as SHA. We remark that all known cryptographic algorithms provably secure in the random oracle paradigm are very efficient and hence meeting for the practical requirements. However one must be caution that the schemes provably secure in the random oracle model do NOT implies that the schemes are also secure in the real world.

Standard intractability paradigm: There is alternative approach, called standard intractabilitiy model, to study the security of cryptographic

schemes. In this circumstance, the related cryptographic primitives are based on standard assumptions (the intractability assumption of factoring problem, discrete logarithm problem, as well as its of variants, such as the computational Diffie-Hellmen, the decisional Diffie-Hellman problem, for examples). It is therefore much hard for one to analyze whether the presented schemes are secure in this model compared to the random oracle model. Definitely this kind of security is encouraged both from the point views of the theoretical research and the practice.

Our works In this report, we present a practical public key cryptosystem based on the notion called square decisional Diffie-Hellman problem (SDDH for short). The scheme is provably secure against adaptive chosen cipher-text attack under the hardness assumption of the square decisional Diffie-Hellman problem. Compared with Cramer and Shoup's notable public key scheme, our scheme enjoys several nice features: (1)Both schemes are provably secure against adaptive chosen cipher-text attack under the intractability paradigm (the security of Cramer-Shoup's scheme is based on the standard decisional Diffie-Hellman problem while ours based on the square decisional Diffie-Hellman problem; (2)The computational and communication complexity of our scheme is equivalent to the Cramer and Shoup's scheme however, the test function of Cramer-shoup's scheme is linear while our scheme is non-linear, therefore the reduction of our scheme is more efficient.

2 New primitives

The Diffie-Hellman problem [DH] is a golden mine for cryptographic purposes and is more and more studied. Furthermore, it is by now a classical problem on which the security of many protocols relies, and namely the semantic security of public key encryption schemes, with all the El Gamal's variants [CS] and [NR] for examples. The public key cryptosystem presented in this report, heavily relies on the hardness assumption of the Square Decisional Diffie-Hellman assumption(SDDH, for short), a NON-trivial notion study first in this report. Therefore we discuss this notion a bit more details below:

2.1 Square computational Diffie-Hellman problem

Let p be a large prime number such that the discrete logarithm problem defined in Z_p^* is hard. Let $G \subseteq Z_p^*$, be a large cyclic group of prime order

q and g be a generator of G, where $p = 2q + 1$. We are interested in the following two useful assumptions which are computational equivalent.

- Computational Diffie-Hellman problem (Assumption 1): Given an oracle A_1, on input g^x, g^y, outputs g^{xy};
- Square computational Diffie-Hellman problem (Assumption 2): Given an oracle A_2, on input g^x, outputs g^{x^2};

We are able to argue that the above two assumptions are equivalent.

Assumption 1 $\Rightarrow$ Assumption 2: Given an oracle A_1, on input g^x, g^y, outputs g^{xy}, we want to show that there exist an oracle A_2, on input g^x, outputs g^{x^2}. Given $u := g^r$, we choose $t_1, t_2 \in Z_q$ at random, and compute $u_1 = u^{t_1} = g^{rt_1}$, and $u_2 = u^{t_2} = g^{rt_2}$. Therefore we are able to compute $v = A_1(u_1, u_2) = g^{r^2 t_1 t_2}$ with non-negligible probability. It follows that g^{r^2} can be computed from v, t_1, t_2 immediately.

Assumption 2 $\Rightarrow$ Assumption 1: Given an oracle A_2, on input g^x, outputs g^{x^2}, we want to show that there exists an oracle A_1, on input g^x, g^y, outputs g^{xy}. Given g^x, we choose $s_1, s_2, t_1, t_2 \in Z_q$ at random and compute $v_1 := A_2(g^{xs_1}) = g^{(xs_1)^2}$, $v_2 := A_2((g^y)^{s_2}) = g^{(ys_2)^2}$. Finally, we compute $v_3 := A_2(g^{xs_1t_1 + ys_2t_2}) = g^{(xs_1t_1 + ys_2t_2)^2}$. Since s_1, s_2, t_1, t_2 are known already, it follows that g^{xy} can be computed from $v_1, v_2, v_3, s_1, s_2, t_1, t_2$ immediately.

2.2 Square decisional Diffie-Hellman assumption

We remark that the security of the Cramer-Shoup's scheme [CS] is based on the quadruple decisional Diffie-Hellman assumption stated below.

Let G be a large cyclic group of prime order q defined above. We consider the following two distributions:

- The distribution R^4 of random quadruple $(g_1, g_2, u_1, u_2) \in G^4$, where g_1, g_2, u_1 and u_2 are uniformly distributed in G^4.
- The distribution D^4 of quadruples $(g_1, g_2, u_1, u_2) \in G^4$, where g_1 and g_2 are uniformly distributed in G^2 while $u_1 = g_1^r$ and $u_2 = g_2^r$ for an r uniformly distributed in Z_q.

An algorithm that solves the quadruple Decisional Diffie-Hellman problem (4-DDH for short) is a statistical test that can efficiently distinguish

these two distributions. Decisional Diffie-Hellman assumption means that there is no such a polynomial statistical test. This assumption is believed to be true for many cyclic groups, such as the prime sub-group of the multiplicative group of finite fields.

While the security of our new public key cryptosystem is based on the square decisional Diffie-Hellman assumption.

- The distribution R^2 of random quadruple (g, g^x, g^y), where $x, y \in Z_q$ are uniformly distributed.
- The distribution D^2 of quadruples (g, g^x, g^{x^2}), where x uniformly distributed in Z_q.

SDDH $\hookrightarrow$ DDH: Suppose we are given a distinguisher D_1 which is able to distinguish the standard decisional Diffie-Hellman triple and the random triple with non-negligible advantage, then we are able to show that there exists a distinguisher D_2 that is able to distinguish the square decisional Diffie-Hellman pair with non-negligible advantage. Given u_1, u_2 which is either g^x, g^y or g^x, g^{x^2}, we choose two strings s, t at random, and compute $u \leftarrow u_1^s$,$v \leftarrow u_1^t$,$w \leftarrow u_2^{st}$, finally, the triple (u, v, w) is given to the distinguisher D_1 as an random input, it follows that D_1 is able to distinguish a Diffie-Hellman triple or random triple with non-negligible advantage. We define the output of D_2 is the copy of the output of D_1. Therefore, we complete the proof.

We are NOT able to show that DDH $\hookrightarrow$ SDDH. Recall that the computational Diffie-Hellman problem (CDH assumption) equivalents the square computational Diffie-Hellman problem (SCDH assumption), therefore we have the conjecture below:

Conjecture Given a distinguisher D_2 that is able to distinguish the square decisional Diffie-Hellman pair with non-negligible advantage, then there exists D_1 which is able to tell a Diffie-Hellman triple from a random triple with non-negligible advantage.

3 A new public key cryptosystem

A public key cryptosystem consists three basic components: a key generation algorithm G, a probability encryption algorithm and a determined decryption algorithm. We state the basic components more details below:

- **Key generation** Let G be a sub-group of prime order q. Let H be a collision free hash function from G^3 to G. Randomly chosen $x, y, z, z' \in Z_q$ and computes $c = g^x$, $d = g^y$ and $h = g^z$ and $h' = g^{z'}$. The private keys are (x, y, z, z'); The public keys are (g, c, d, h, h', H);

- **Encryption** To encrypt a message $m \in G$, it chooses $r \in z_q$ at random and computes $u = g^r$, $v = (uh)^r$, $e = mh'^r$, $\alpha = H(u, u, e)$ and $w = c^{r\alpha}d^{r^2}$. The cipher-text is (u, v, e, w).

- **Decryption** Given a putative cipher-text (u, v, e, w), it computes $\alpha = H(u, v, e)$, and tests whether the condition $u^{\alpha x - yz}v^y = w$ holds, if this condition does not hold, the decryption algorithm outputs $reject$; Otherwise, it outputs $m = e/u^{z'}$.

The proof of security We consider the following game: first the encryption's key generation algorithm is run, with a security parameter as input. Next the adversary chooses two messages m_0 and m_1 and sends them to the encryption oracle. The encryption oracle chooses a bit b at random and encrypts the message m_b. The correspondent cipher-text, called the target cipher-text is given to the adversary. Finally, the adversary is given the access to the decryption oracle. We say that a public key encryption scheme is secure against adaptive chosen cipher-text the target cipher-text, if the adversary's advantage to guess the bit b is negligible.

Main result The public key scheme described above is secure against adaptive chosen cipher-text attack under the assumptions that H is a collision free hash function as well as the square decisional Diffie-Hellman problem is hard.

Proof:

Now we want to show the fact that if the public key scheme is NOT secure against adaptive chosen message attack, then there exist an efficient distinguisher that can tell the difference from a SDDH pair and a random pair with non-negligible advantage.

Simulator Given a pair (u_1, u_2), which comes from either SDDH or a random pair. We build a simulator below:

Key generation oracle: The key generation oracle is the same as the real key generation algorithm;

Encryption oracle: For a random pair (u_1, u_2), and given two message m_0, m_1, the encryption oracle chooses a bit b at random and computes as follows: $u \leftarrow u_1$, $v \leftarrow u_2 u^z$, $e \leftarrow m_b {u_1}^{z'}$, $\alpha \leftarrow H(u, u, e)$ and $w \leftarrow u^{\alpha x - yz}v^y$. The output of the simulator is (u, v, e, w).

This completes the description of the simulator.

We remark that if the pair (u_1, u_2) comes from the SDDH, then the simulator is perfect; The rest works are to show that both the actual encryption algorithm and the encryption oracle can reject invalid cipher-text with overwhelm probability. Since our test function is non-linear, we can test whether a putative cipher-text is a valid cipher-text by single one step. More details, suppose the adversary submits a cipher-text (u, v, e, w) to the decryption oracle. The decryption oracle computes $u^{\alpha x - yz} v^y$ and tests whether it equals to w. We rewrite $u^{\alpha x - yz} v^y = g^{(\alpha x - yz)r} v^y$. Since g^x, g^y, g^{xy} is from the Diffie-Hellman triple, it follows that g^{yz} is a random variable uniformly distributed over Z_p, therefore the adversary's success probability of the first time accepted by the decryption oracle is $1/q$ which is negligible. Also notice that if (u_1, u_2) comes from the random pair, then b is a random value from the point view's of the adversary. We now describe SDDH distinguisher as follows: we choose a bit b at random. The distinguisher outputs 1 if the adversary's output bit b' is equal to b, and outputs 0 otherwise. This distinguisher can tell the SDDH pair from the random pair with non-negligible amount provided the adversary has non-negligible advantage breaking the public key cryptosystem in Rackoff-Simon's sense.

4 Conclusions

We have developed a new practical public key cryptosystem based on the notion called square decisional Diffie-Hellman problem. The scheme enjoys nice features compared with notable works of Cramer-Shoup's: (1)The security of Cramer-Shoup's scheme is based on standard decisional Diffie-Hellman problem while ours based on the square decisional Diffie-Hellman problem; (2)The computational and communication complexity of our scheme is equivalent to the Cramer and Shoup's scheme; (3)The test function of Cramer-shoup's scheme is linear while our scheme is non-linear, therefore our reduction is more efficient.

References

[**BDPR**] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway. Relations among notions of security for public-key encryption schemes. Ex-

tended abstract in Advances in Cryptology- Crypto'98 Proceedings, Lecture Notes in Computer Science Vol. 1462, Springer-Verlag, 1998.

[**CS**] R. Cramer and V. Shoup. A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack. In Crypto '98, LNCS 1462, pages 13-25, Springer-Verlag, Berlin, 1998.

[**DDN**] D. Dolev, C. Dwork, and M. Naor. Non-Malleable Cryptography, proceedings, the 23rd ACM SIGACT Symposium on Theory of Computing, pp. 542-552. May 1991.

[**DH**] Diffie, W., M. E. Hellman, M. E.: New Directions in Cryptography. In IEEE Transactions on Information Theory, IT-22(6):644-654, November 1976.

[**GM**] S. Goldwasser, S. Micali. Probabilistic encryption. Journal of computer system and science. Vol.28, 270-299, 1984.

[**NR**] M. Naor, Omer Reingold, Number-Theoretic constructions of efficient pseudo-random functions, Extended abstract in: Proc. 38th IEEE Symp. on Foundations of Computer Science, 1997, pp. 458-467.

[**NY**] M. Naor, M. Yung. Public key cryptosystem secure against chosen cipher-text attacks.22nd Annual ACM Symposium on the theory of computing, 1990, 427-437.

[**RS**] Rackoff, C., Simon, D.: Non-interactive Zero-knowledge Proof of Knowledge and Chosen Cipher-text Attacks. Cryptology-Crypto'91. 433-444, Springer-Verlag, 1992.