A Practical Elliptic Curve Public Key Encryption Scheme Provably Secure Against Adaptive Chosen-message Attack

Huafei Zhu

InfoComm Security Department, Institute for InfoComm Research.
21 Heng Mui Keng Terrace, Singapore 119613.
huafei@i2r.a-star.edu.sg

Abstract. We study elliptic curve cryptosystems by first investigating the schemes defined over Z_p and show that the scheme is provably secure against adaptive chosen cipher-text attack under the decisional Diffie-Hellman assumption. Then we derive a practical elliptic curve cryptosystem by making use of some nice elliptic curve where the decisional Diffie-Hellman assumption is reserved.

Keywords: Decisional Diffie-Hellman assumption, elliptic curve, standard intractability paradigm

1 Introduction

Elliptic curve cryptosystems were first studied by Miller [9] and Koblitz [7]. The most attractive feature that makes elliptic curve interesting both from the point views of the practice and the theoretical research is the relatively short operand length relative to RSA and systems based on the discrete logarithm in finite fields. Cryptosystems which explore the discrete logarithm problem over elliptic curve can be built with an operand length of 150-200 bits ([10], [8]). Thus, smaller parameters can be used in elliptic curve cyrptosystem than with discrete logarithm systems but with equivalent levels of security. IEEE and other standard bodies such as ANSI and ISO are in the process of standardizing elliptic curve cryptosystems. It is thus very attractive to provide efficient public key algorithms which allow for efficient implementations of elliptic curve cryptosystems.

A public key encryption scheme is secure definitely related to the ability of adversaries and underlying assumptions. To define the ability of adversaries, three basic models are considered:

-Semantic secure: a public key encryption scheme is said semantic secure, which is first mentioned by Goldwasser and Micali [6], if an adversary should not be able to obtain any partial information about a message given its cipher-text.

-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 [11], 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.

-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 [12], 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.

Our goal is to provide a practical public key encryption scheme that is provably secure against adaptive chosen cipher-text attack in the standard intractability paradigm. We study elliptic curve cryptosystem by first investigate the schemes defined over Z_p and showing that the scheme is provably secure against adaptive chosen cipher-text attack under the decisional Diffie-Hellman assumption in the above setting, then deriving a practical elliptic curve cryptosystem by making use of some nice elliptic curve where the decisional Diffie-Hellman assumption is reserved.

2 Primitives

We make use of standard reduction technique. We therefore sketch the related notions below:

COMPUTATIONAL INDISTINGUISHABILITY: Two families of distributions δ_1 and δ_2 are said to be computationally indistinguishable if no probabilistic polynomial time Turing machine distinguisher can decide which distribution it is sampling from with a probability of success non-negligibly better than random guessing.

According to the definition of computationally indistinguishable, it is not hard for one to show the following facts.

-Fact 1: If δ_1 and δ_2 are computationally indistinguishable and δ_2 and δ_3 are computationally indistinguishable, then δ_1 and δ_3 are computationally indistinguishable.

-Fact 2: If δ_1 and δ_2 are computationally indistinguishable, then $\delta_1 \times \delta$ and $\delta_2 \times \delta$ are computationally indistinguishable for any independent distribution δ, where $\delta_1 \times \cdots \times \delta_k$, the productive distribution, is defined to be a distribution on k-tuples where the ith component is sampled according to the distribution δ_i.

The underlying primitive of our scheme is the hardness assumption of the decisional Diffie-Hellman problem as well as the existence of collision-free hash functions. We review the famous quadruple decisional Diffie-Hellman Problem by considering 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, where G is a large cyclic group of prime order q.

-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 whilst $u_1 = g_1^r$ and $u_2 = g_2^r$ for an r uniformly distributed in Z_q.

An algorithm that solves the quadruple Decisional Diffie-Hellman problem 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. To prove the security of our scheme, we make use of the following Lemma.

Lemma: Two distributions defined below are indistinguishable under the sole assumption of the standard quadruple Decisional Diffie-Hellman problem:

-The distribution R^{2k} of any random tuple $(g_1, \cdots, g_k, u_1, \cdots, u_k) \in G^{2k}$, where $g_1, \cdots, g_k$, and $u_1, \cdots, u_k$ are uniformly distributed in G^{2k};

-The distribution D^{2k} of tuples $(g_1, \cdots, g_k, u_1, \cdots, u_k) \in G^{2k}$, where $g_1, \cdots, g_k$ are uniformly distributed in G^k while $u_1 = g_1^r, \cdots, u_k = g_k^r$ for an r uniformly distributed in Z_q.

Proof: By mathematics induction. Let G be a large cyclic group of prime order q defined above. The Six-tuple Decisional Diffie-Hellman Problem (6-DDH for short), is to study the intractability of the following two distributions. More precisely:

-The distribution R^6 of random six-tuple $(g_1, g_2, g_3, u_1, u_2, u_3) \in G^6$, where g_1, g_2, g_3, u_1, u_2 and u_3 are uniformly distributed in G^6.

-The distribution D^6 of six-tuple $(g_1, g_2, g_3, u_1, u_2, u_3) \in G^6$, where g_1, g_2 and g_3 are uniformly distributed in G^3 while $u_1 = g_1^r, u_2 = g_2^r$ and $u_3 = g_3^r$ for an r uniformly distributed in Z_q.

Let us consider a machine M that can get a non-negligible advantage ϵ between D^4 and R^4. We define a 6-DDH distinguisher M', which runs as follows: Given any six-tuple $(g_1, g_2, g_3, u_1, u_2, u_3)$, which comes from either R^6 or D^6, M' runs M on the quadruple $(g_1g_2, g_3, u_1u_2, u_3)$ and simply forwards the answer. As explained by the equations presented below, that if $(g_1, g_2, g_3, u_1, u_2, u_3)$ follows the distribution D^6, then $(g_1g_2, g_3, u_1u_2, u_3)$ follows the distribution D^4. It is also the same between R^6 and R^4. As a consequence, our new machine gets the same advantage ϵ in distinguishing D^6 and R^6 with the help of M in distinguishing D^4 and R^4, performing just one more multiplication in G, where G is assumed to be a cyclic group of order q, and g is assumed to be a generator of this group. We denote the output of M(respectively M')as follows: If the the input comes from D^4(D^6 respectively), it outputs 1 and 0 if the input tuple comes from R^4(R^6 respectively).

$Pr[M(g_1g_2, g_3, u_1u_2, u_3) = 1|(g_1, g_2, g_3, u_1, u_2, u_3) \in R^6]$
$=Pr[M(g^{x_1+x_2}, g^{x_3}, g^{x_4+x_5}, g^{x_6}) = 1|x_1, x_2, x_3, x_4, x_5, x_6 \in Z_q]$
$=Pr[M(g^x, g^y, g^z, g^r) = 1|x, y, z, r \in Z_q]$
$=Pr[M(g_1, g_2, u_1, u_2) = 1|(g_1, g_2, u_1, u_2) \in R^4]$

And

$Pr[M(g_1g_2, g_3, u_1u_2, u_3) = 1|(g_1, g_2, g_3, u_1, u_2, u_3) \in D^6]$
$=Pr[M(g^{x_1+x_2}, g^{x_3}, g^{r(x_1+x_2)}, g^{rx_3}) = 1|x_1, x_2, x_3, r \in Z_q]$
$=Pr[M(g^x, g^y, g^{rx}, g^{ry}) = 1|x, y, r \in Z_q]$
$=Pr[M(g_1, g_2, u_1, u_2) = 1|(g_1, g_2, u_1, u_2) \in D^4]$

Let us consider a machine M that can get a non-negligible advantage ϵ between D^6 and R^6. We define a 4-DDH distinguisher M', which runs as follows: on a given quadruple (g_1, g_2, u_1, u_2), M' runs M on the six-tuple $(g_1, g_2, g_1^s g_2^t, u_1, u_2, u_1^s u_2^t)$, for randomly chosen s and t in Z_q, and simply forwards the answer. Once again, the advantage of our new distinguisher M' is exactly the same as the advantage of M, with very few more computations: we assume again g to be a generator of G, and we insist on the fact that Z_q is a field.
$Pr[M'(g_1, g_2, u_1, u_2) = 1|(g_1, g_2, u_1, u_2) \in D^4]$
$=Pr[M(g^{x_1}, g^{x_2}, g^{sx_1+tx_2}, g^{rx_1}, g^{rx_2}, g^{srx_1+trx_2}) = 1|x_1, x_2, r, s, t \in Z_q]$
$=Pr[M(g^{x_1}, g^{x_2}, g^{x_3}, g^{rx_1}, g^{rx_2}, g^{rx_3}) = 1|x_1, x_2, x_3, r \in Z_q]$
$=Pr[M(g_1, g_2, g_3, u_1, u_2, u_3) = 1|(g_1, g_2, g_3, u_1, u_2, u_3) \in D^6]$

And
$Pr[M'(g_1, g_2, u_1, u_2) = 1|(g_1, g_2, u_1, u_2) \in R^4]$
$=Pr[M(g^{x_1}, g^{x_2}, g^{sx_1+tx_2}, g^{y_1}, g^{y_2}, g^{sy_1+ty_2}) = 1|x_1, x_2, s, t, y_1, y_2 \in Z_q]$
$= Pr[M(g^{x_1}, g^{x_2}, g^{x_3}, g^{y_1}, g^{y_2}, g^{y_3}) = 1|(x_1, x_2, x_3, y_1, y_2, y_3) \in {Z_q}^6]$
$=Pr[M(g_1, g_2, g_3, u_1, u_2, u_3) = 1|(g_1, g_2, g_3, u_1, u_2, u_3) \in R^6]$

Based on the above arguments, we obtain the useful result: The Decisional Diffie-Hellman Problems, 4-DDH and 6-DDH, are equivalent. We now obtain reductions that are optimal since an advantage against one of these problems can be reached against the other one. Therefore, under the sole classical Decisional Diffie-Hellman assumption, for any k, the following distributions are indistinguishable:

- The distribution R^{2k} of any random tuple $(g_1, \cdots, g_k, u_1, \cdots, u_k) \in G^{2k}$, where $g_1, \cdots, g_k$, and $u_1, \cdots, u_k$ are uniformly distributed in G^{2k};
- The distribution D^{2k} of tuples $(g_1, \cdots, g_k, u_1, \cdots, u_k) \in G^{2k}$, where $g_1, \cdots, g_k$ are uniformly distributed in G^k while $u_1 = g_1^r, \cdots, u_k = g_k^r$ for an r uniformly distributed in Z_q.

3 A practical public key cryptosystem

Our encryption scheme is described as follows:

-Key generation: Let G be a sub-group of prime order q. Let H be a collision free hash function; We choose $g_1 \in G\backslash\{1\}$ and $w, x, y, z \in Z_q$ at random and compute $g_2 = g_1^w$, $c = g_1^x$, $d = g_1^y$ and $h = g_1^z$. The private keys are (w, x, y, z). The public keys are (g_1, g_2, c, d, h, H).

-Encryption: To encrypt a message $m \in G$, it computes $u_1 = g_1^r$, $u_2 = g_2^r$, $e = mh^r$, $\alpha = H(u_1, u_2, e)$ and $v = c^r d^{r\alpha}$. The cipher-text is (u_1, u_2, e, v).

-Decryption: Given a putative cipher (u_1, u_2, e, v), it computes $\alpha = H(u_1, u_2, e)$, and tests whether $u_2 = u_1^w$ and $u_1^{x+y\alpha} = v$ hold. If the both conditions hold, then the decryption algorithm outputs $m = e/u_1^z$, Otherwise it outputs reject.

COMPARISONS: The scheme can be viewed as a variation of Cramer-Shoup's encryption scheme with reduced key sizes. More details:

-The key generation algorithm in our scheme is more efficient than that in the basic Cramer and Shoup's encryption scheme. The public keys are g_1, $g_2 = g_1^w$, $c = g_1^x$, $d = g_1^y$ and $h = g_1^z$ and the secret keys are (w, x, y, z) in our scheme. The public keys are g_1, g_2, $c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$ and $h = g_1^z$ and the secret keys are (x_1, x_2, y_1, y_2, z) in Cramer-Shoup's encryption scheme.

-The computational costs of the decryption algorithm of our scheme is equivalent to that in the basic Cramer-Shoup's encryption however our decryption algorithm is more efficient to reject any invalid cipher-text. This property may be useful in practice.

PROOF OF SECURITY: The above scheme is denoted G_0 and the transformed games are denoted G_i, for $i = 1, 2$.

Defining game G_1 as follows:

-Key generation: Let G be a sub-group of prime order q. We choose x_1, x_2, y_1, y_2, z_1, $z_2 \in Z_q$ at random and computes $c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$ and $h = g_1^{z_1} g_2^{z_2}$. The private keys are $(x_1, x_2, y_1, y_2, z_1, z_2)$ and the public keys are (g_1, g_2, c, d, h, H), where H is a collision free hash function.

-Encryption oracle: Suppose (g_1, g_2, u_1, u_2) is a random Diffie-Hellman quadruple, we then compute $e = m u_1^{z_1} u_2^{z_2}$, $\alpha = H(u_1, u_2, e)$ and $v = u_1^{x_1+y_1\alpha} u_2^{x_2+y_2\alpha}$. The cipher-text is (u_1, u_2, e, v).

-Decryption: Given a putative cipher-text (u_1, u_2, e, v), it computes $\alpha = H(u_1, u_2, e)$, and tests whether $u_1^{x_1+y_1\alpha} u_2^{x_2+y_2\alpha} = v$, if this condition does not hold, the decryption algorithm outputs reject; otherwise, it outputs $m = e/u_1^{z_1} u_2^{z_2}$.

Claim 1: The two games G_0 and G_1 are equivalent up to the point where any invalid cipher-text can be rejected except for a negligible amount.

Proof: We say a cipher-text (u_1, u_2, e, v) valid if $\log_{g_1} u_1 = \log_{g_2} u_2$. Since the decryption algorithm in game G_0 knows the trapdoor information $w = \log_g h$, we can assume that (g_1, g_2, u_1, u_2) is always from the Diffie-Hellman quadruple. As the decryption algorithm in the game G_1 is able to reject any invalid cipher-text except for negligible amount (the same argument as Lemma 1 presented in [CS]), it follows that the two games are equivalent up to the point where an invalid cipher-text is not rejected (however, the probability that this happens is negligible).

Claim 2: The adversary's advantage in game G_0 and in game G_1 are same.

Proof: By Claim 1, the adversary's mount is restricted to adaptive choose valid cipher-text attack in game G_1 and in game G_2. The distribution of valid cipher-texts in game G_1 is denoted by δ_1 and the distribution of valid cipher-texts in game G_2 is denoted by δ_2. Therefore the distribution δ_1 is statistical indistinguishable to the distribution δ_2. It follows the adversary's advantage in game G_0 differs from game G_1 by a negligible amount.

Defining game G_2 as follows:

Now, we replace (g_1, g_2, u_1, u_2) in game G_1 by arbitrary (g_1, g_2, u'_1, u'_2), which is either a Diffie-Hellman quadruple or a random quadruple.

-Key generation: Let G be a sub-group of prime order q. We chosen x_1, x_2, y_1, y_2, z_1, $z_2 \in Z_q$ at random and computes $c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$ and $h = g_1^{z_1} g_2^{z_2}$. The private keys are $(x_1, x_2, y_1, y_2, z_1, z_2)$ and the public keys are (g_1, g_2, c, d, h, H), where H is a collision free hash function.

-Encryption oracle: Given (g_1, g_2, u'_1, u'_2), it computes $e' = m{u'}_1^{z_1} {u'}_2^{z_2}$, $\alpha' = H(u'_1, u'_2, e')$ and $v' = {u'}_1^{x_1+y_1\alpha'} {u'}_2^{x_2+y_2\alpha'}$. The cipher-text is (u'_1, u'_2, e', v').

-Decryption: Given a putative cipher-text (u'_1, u'_2, e', v'), it computes $\alpha' = H(u'_1, u'_2, e')$, and tests whether ${u'}_1^{x_1+y_1\alpha'} {u'}_2^{x_2+y_2\alpha'} = v'$, if this condition does not hold, the decryption algorithm outputs reject; otherwise, it outputs $m = e'/{u'}_1^{z_1} {u'}_2^{z_2}$.

Claim 3: Under the decisional Diffie-Hellman assumption, as well as the collision free assumption of hash function The adversary's advantage in game G_1 differs form its advantage in game G_2 by a negligible amount.

Proof: G_1 is Cramer-Shoup's encryption scheme while G_2 is the simulator of Cramer-Shoup's encryption scheme. Therefore under the decisional Diffie-Hellman assumption, as well as the collision free assumption of hash functions, the adversary's advantage in game G_1 differs form its advantage in game G_2 by a negligible amount.

Claim 4: The scheme G_0, is secure against adaptive chosen cipher-text attack under the Decisional Diffie-Hellman assumption, as well as the collision free assumption of hash functions.

Proof: Suppose there is an adversary which is able to break the scheme G_0 with non-negligible probability. By Claim 1 and Claim 2, one knows that the adversary's advantage in game G_1 differs form its advantage in game G_0 by negligible amount. Therefore the adversary is able to break game G_1 with non-negligible probability. By Claim 3, the adversary's advantage in game G_2 differs form its advantage in game G_1 by negligible amount, therefore, the adversary is able to break game G_2 with non-negligible probability. Equivalently, two distributions $(g_1, g_2, h, {g_1}^r, {g_2}^r, h^r)$ and $(g_1, g_2, h, {u_1}', {u_2}', {u_1}^{z_1} {u_2}^{z_2})$ are distinguishable. By lemma, this contradicts the decisional Diffie-Hellman assumption.

4 Practical elliptic curve public key cryptosystem

CHOICE OF ELLIPTIC CURVES: To transform a public key cryptosystem defined over Z_p to elliptic curve setting, one should be caution enough to choose the good elliptic curves so that the decisional Diffie-Hellman assumption is believed true. A set of elliptic curve are those recommended but not mandated by NIST in June 1999 for U.S. Federal Government use (these curves are also recommended in the FIPS 186-2 standard [5]). These recommended elliptic curves are defined over the prime field or binary field. These elliptic curves have been carefully studied so that they meet fast implementations as well as integrability with other cryptographic primitives.

- The prime fields F_p for $p{=}2^{192}-2^{64}-1$, $p{=}2^{224}-2^{96}+1$, $p{=}2^{256}-2^{224}+2^{192}+2^{96}-1$, $p={=}2^{384}-2^{128}-2^{96}+2^{32}-1$ and $p{=}\ 2^{521}-1$;
- The binary fields $F_{2^{163}}$, $F_{2^{233}}$, $F_{2^{283}}$, $F_{2^{409}}$ and $F_{2^{571}}$.

We restrict our attention to the prime field F_p, specially for $p{=}2^{192}-2^{64}-1$ since it is easy for one to consider the rest cases. In the setting we choose a, b the coefficients of the elliptic curve $y^2 = x^3 + ax + b$ satisfying $rb^2 = ja^3 \bmod p$ at random. Notice that IEEE P1363 recommend the selection $a = -3$ for efficiency considering. Let (xG, yG) be the x and y coordinates of the base point G and n denote the (prime) order of G and h denote the cofactor. We make use of the elliptic curve defined over F_p where $p = 2^{192} - 2^{64} - 1$). The system parameters listed below.

- $p{=}62771017||35386680||76383578||94232076||66416083||90870039||03249612||79$;
- $seedE{=}0x||3045ae6f||c8422f64||ed579528||d38120ea||e12196d5$;
- $r{=}0x||3099d2bb||bfcb2538||542dcd5f||b078b6ef||5f3d6fe2||c745de65$;
- $a{=}-3$;
- $b{=}0x||64210519||e59c80e7||0fa7e9ab||72243049||feb8deec||c146b9b1$;
- $xG{=}0x||188da80e||b03090f6||7cbf20eb||43a18800||f4ff0afd||82ff1012$;
- $yG{=}0x||07192b95||ffc8da78||631011ed||6b24cdd5||73f977a1||1e794811$;
- $n{=}6277101735386680763835789423176059013767194773182842284081$;
- $h{=}1$.

Since the elliptic curve we chosen with large prime order, the decisional Diffie-Hellman assumption is held in this setting. We describe the corresponding EC system parameters below:

- Key generation algorithm: Let g_1 be a rational point of the EC described above. We choose w, α, β, γ at random and compute $g_2 = wg_1$, $c{=}\ \alpha g_1$, $d{=}\ \beta g_1$ and $h{=}\gamma g_1$. H is a collision free hash function. The public key are those (g_1, g_2, h, c, d, H) together with the description of EC.
- To encrypt a message m, one computes $u_1 = rg_1$, $u_2 =, rg_2$, $e = m \oplus rh$, $\lambda = H(u_1, u_2, e)$ and $v = rc + \lambda rd$. The cipher-text is (u_1, u_2, e, v).
- Given a putative cipher (u_1, u_2, e, v), it computes $\lambda = H(u_1, u_2, e)$, and tests whether the conditions $u_2{=}\ wu_1$ and $(x + \lambda y)u_1 = v$ hold. If the both conditions hold, then the decryption algorithm outputs $m{=}e \oplus \gamma u_1$, Otherwise it outputs reject.

Again, since the elliptic curve we choose with large prime order, the decisional Diffie-Hellman assumption is held in this setting. Consequently, we have the statement: the EC cryptosystem described above is provably secure against adaptive chosen cipher-text attack under the Decisional Diffie-Hellman assumption, as well as the collision free assumption of hash function.

References

1. M. Bellare, A. Desai, D. Pointcheval and P. Rogaway. Relations among notions of security for public-key encryption schemes. Extended abstract in Advances in Cryptology- Crypto'98 Proceedings, Lecture Notes in Computer Science Vol. 1462, Springer-Verlag, 1998.
2. J. Borst, B. Preneel, J. Vandewalle, An adaptive chosen ciphertext attack on a variation of the Cramer-Shoup public-key encryption scheme, Electronics Letters, Vol. 36, No. 1, 2000.
3. 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.
4. 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.
5. FIPS 186-2 standard. http://cs-www.ncsl.nist.gov/cryptval/dss.htm
6. S. Goldwasser, S. Micali. Probabilistic encryption. Journal of computer system and science. Vol.28, 270-299, 1984.
7. N. Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, 48:203–209, 1987.
8. J. Koeller,A. Menezes, M. Qu, and S. Vanstone. Elliptic Curve Systems. Draft8, IEEE P1363 Standard for RSA, Diffie-Hellman and Related Public key Cryptography, May 1996. working document.
9. V. Miller. Uses of elliptic curves in cryptography. In Lecture Notes in Computer Science 218: Advances in Cryptology-CRYPTO'85, pages 417-426, Springer-verlag, Berlin.
10. A.J. Menezes. Elliptic Curve Public Key Cryptosystems. Kluwer Academic Publishers, 1993.
11. M. Naor, M. Yung. Public key cryptosystem secure against chosen ciphertext attacks.22nd Annual ACM Symposium on the theory of computing, 1990, 427-437.
12. C. Rackoff, D. Simon. Non-interactive zero-knowledge proof of knowledge and chosen cipher-text attacks. Cryptology-Crypto'91. 433-444, Springer-Verlag, 1992.