MTAT.07.006 Research Seminar in Cryptography
IND-CCA2 secure cryptosystems

Dan Bogdanov

October 31, 2005

Abstract

Standard security assumptions (IND-CPA, IND-CCA) are explained. A number of cryptosystems satisfying a more secure assumption (IND-CCA2) are explored.

1 Introduction

This paper gives an overview of some of the IND-CCA2 secure cryptosystems. The first such cryptosystem was presented by Naor and Yung [1]. A more practical scheme was proposed by Cramer and Shoup [2] who later also published a general method for constructing such encryption schemes [4].

In 2002 Elkind and Sahai presented a new generalization for generating IND-CCA2 secure public key encryption schemes they call the *oblivious decryptors* model. They claimed that they have unified models both from Naor and Yung [1] and Cramer and Shoup [2], [4].

One of the latest works in this area is from Boyen, Mei and Waters [7]. They construct a compact identity-based cryptosystem that is provably IND-CCA2 secure.

2 Definitions

2.1 Indistinguishability

2.1.1 General notion

Indistinguishability is a property of encryption schemes. Indistinguishability means, that our adversary is unable to distinguish pairs of ciphertexts which are based on messages they encrypt. Let's say that we have an encryption function E and two messages m_0 and m_1 which can be constructed by the adversary. The adversary sends m_0 and m_1 to E. They are encrypted, one of them is chosen randomly and returned to the adversary.

The encryption scheme is indistinguishable, if the adversary can't guess, which m was returned with a probability higher than $\frac{1}{2}$. If the probability is considerably higher than $\frac{1}{2}$, we call this an advantage in distinguishing the ciphertext. The advantage is a property of the adversary. If the advantage is considerably larger than zero, the scheme is no longer considered secure in terms of indistinguishability.

There are different kinds of security notions derived from indistinguishability. They are described in the following sections.

2.1.2 IND-CPA

IND-CPA means *Indistinguishability under chosen plaintext attack*. This is equivalent to the property of semantic security, and many cryptographic proofs use these definitions interchangeably. For an asymmetic key encryption scheme, IND-CPA is defined by using a game between an adversary and a challenger. The adversary is modeled by a probabilistic polynomial time Turing machine.

In the following game $E(PK, m)$ represents the encryption of a message m using the key PK.

1. The challenger generates a key pair PK, SK based on the security parameter k (which can be the key size in bits), and publishes PK to the adversary. The challenger retains SK.
2. The adversary may perform any number of encryptions or other operations.
3. Eventually, the adversary submits two distinct chosen plaintexts m_0 and m_1 to the challenger.

4. The challenger selects a bit $b \in \{0,1\}$ uniformly at random, and sends the challenge ciphertext $C = E(PK, m_b)$ back to the adversary.

5. The adversary is free to perform any number of additional computations or encryptions. Finally, it outputs a guess for the value of b.

A cryptosystem is indistinguishable under chosen plaintext attack if no adversary can win the above game with probability greater than $\frac{1}{2} + \epsilon$, where ϵ is a negligible function in the security parameter k ($\epsilon \leq poly(k)$ where $poly()$ is a polynomial function). In this case, the adversary is said to have a negligible "advantage" over random guessing.

2.1.3 IND-CCA and IND-CCA2

Indistinguishability under *non-adaptive* and *adaptive Chosen Ciphertext Attack* (IND-CCA, IND-CCA2) uses a definition similar to that of IND-CPA. However, in addition to the public key, the adversary is given access to a decryption oracle which decrypts arbitrary ciphertexts at the adversary's request, returning the plaintext. In the non-adaptive definition, the adversary is allowed to query this oracle only up until it receives the challenge ciphertext. In the adaptive definition, the adversary may continue to query the decryption oracle even after it has received a challenge ciphertext, with the caveat that it may not pass the challenge ciphertext for decryption.

1. The challenger generates a key pair PK, SK based on some security parameter k (e.g., a key size in bits), and publishes PK to the adversary. The challenger retains SK.

2. The adversary may perform any number of encryptions, calls to the decryption oracle based on arbitrary ciphertexts, or other operations.

3. Eventually, the adversary submits two distinct chosen plaintexts m_0, m_1 to the challenger.

4. The challenger selects a bit $b \in \{0,1\}$ uniformly at random, and sends the "challenge" ciphertext $C = E(PK, m_b)$ back to the adversary.

5. The adversary is free to perform any number of additional computations or encryptions.

   (a) In the non-adaptive case (IND-CCA), the adversary may not make further calls to the decryption oracle.

   (b) In the adaptive case (IND-CCA2), the adversary may make further calls to the decryption oracle, but may not submit the challenge ciphertext C.

6. Finally, the adversary outputs a guess for the value of b.

A scheme is IND-CCA/IND-CCA2 secure if no adversary has a non-negligible advantage in winning the given game.

2.2 Zero-knowledge

A *zero-knowledge proof* is an interactive method for one party (*Prover*) to prove to another (*Verifier*) that a (usually mathematical) statement is true, without revealing anything other than the truthfulness of the statement. It is also possible to construct *non-interactive* zero-knowledge proofs.

A zero-knowledge proof must satisfy three properties. First two are common to interactive proof systems, but the third is unique to zero-knowledge proofs. These properties are:

1. *Completeness*: if the statement is true, the honest verifier (that is, one following the protocol properly) will be convinced of this fact by an honest prover.

2. *Soundness*: if the statement is false, no cheating prover can convince the honest verifier that it is true, except with some small probability.

3. *Zero-knowledgeness*: if the statement is true, no cheating verifier learns anything other than this fact. This is formalized by showing that every cheating verifier has some simulator that, given only the statement to be proven (and no access to the prover), can produce a transcript that "looks like" an interaction between the honest prover and the cheating verifier.

3 The Naor-Yung cryptosystem

The first provably IND-CCA2 secure cryptosystem was proposed in 1990 by Naor and Yung [1]. They used a non-interactive zero-knowledge proof of language membership to show the consistency of the ciphertext.

The particular article is not discussed more thoroughly in this survey because there are newer and more important results. Still, their work has been an inspiration for other researchers, as can be seen from citations in this specific area.

4 The Cramer-Shoup cryptosystem

4.1 Overview

The Cramer-Shoup cryptosystem [2] is claimed to be both practical and provably secure against adaptive chosen ciphertext attacks under standard intractability assumption. The security proof is based on the hardness of the Diffie-Hellman decision problem in the used group.

4.2 The Scheme

We assume that we have a group G of prime order q where q is large. The encrypted messages are elements of G. An universal family one-way family of hash functions that map long bit strings to elements of $\mathbb{Z}_q$ is also required. Key generation, encryption and decryption are done as follows:

Key Generation: We choose two random elements $g_1, g_2 \in G$ and $x_1, x_2, y_1, y_2, z \in \mathbb{Z}_q$. Then we calculate $c = g_1^{x_1} g_2^{x_2}, d = g_1^{y_1} g_2^{y_2}, h = g_1^z$. Next, we choose a hash function H from our family of universal one-way hash functions. The public key is (g_1, g_2, c, d, h, H) and the secret key is (x_1, x_2, y_1, y_2, z).

Encryption: To encrypt a message $m \in G$ we choose a random $r \in \mathbb{Z}_q$ and compute $u_1 = g_1^r, u_2 = g_2^r, e = h^r m, \alpha = H(u_1, u_2, e), v = c^r d^{r\alpha}$. The ciphertext for m is (u_1, u_2, e, v).

Decryption: Given a ciphertext (u_1, u_2, e, v) we first compute $\alpha = H(u_1, u_2, e)$ and check if $u_1^{x_1+y_1\alpha} u_2^{x_2+y_2\alpha} = v$. If the condition does not hold, we reject the ciphertext as invalid. Otherwise we compute $m = e/u_1^z$ which is the decrypted message.

4.3 Scheme verification

To verify the scheme we have to check if we actually get our encrypted m back after decrypting. From key generation we know that $c = g_1^{x_1} g_2^{x_2}$ and from the encryption algorithm we know that $u_1 = g_1^r, u_2 = g_2^r$. From this we get $u_1^{x_1} u_2^{x_2} = g_1^{rx_1} g_2^{rx_2} = c^r$. Also, $u_1^{y_1} u_2^{y_2} = d^r$ and $u_1^z = h^r$.

The decryption algorithm tests, if $u_1^{x_1+y_1\alpha} u_2^{x_2+y_2\alpha} = v$. From encryption we have $v = c^r d^{r\alpha}$. This gives us the left side of the test equation and so the test will go through. If it does, we can get the m by simply reversing the $e = h^r m$ computation from encryption.

5 Using Universal Hash Proofs to Construct IND-CCA2 secure cryptosystems

5.1 Overview

In 2001 Cramer and Shoup published a general approach to constructing IND-CCA2 secure cryptosystems [4]. They introduce the notion of a *universal hash proof system* which is a kind of non-interactive zero-knowledge proof system for a language. They show that when given an efficient universal hash proof system for a language with certain natural cryptographic indistinguishability properties, one can construct an efficient public-key encryption schemes secure against adaptive chosen ciphertext attack in the standard model (IND-CCA2 secure systems).

Based on that theory they construct two more IND-CCA2 secure systems and show that their original system is a case in their general theory. The other cryptosystems are based on Paillier's Decision Composite Residuosity assumption and Quadratic Residuosity assumption respectively.

6 The Oblivious Decryptors Model

6.1 Introduction

This model was presented by Elkind and Sahai [5]. They present a methodology for constructing IND-CCA2 secure encryption schemes. They also show how to present all known efficient (provably secure) CCA secure publickey encryption schemes as special cases of this model.

6.2 Main cryptographic notions

6.2.1 Simulation-Sound Non-Interactive Zero-Knowledge Proofs

The notion of *Simulation-Sound (Non-Malleable) Non-Interactive Zero-Knowledge* (NIZK) was proposed by Sahai [3]. It is a kind of non-interactive zero-knowledge proof, with an additional requirement – whatever one can prove after seeing a NIZK proof, one could have also proved without seeing it, except for the ability to duplicate the proof. This is a stronger notion than a standard NIZK proof.

6.2.2 Oblivious Decryptors Model

Essentially, an *oblivious decryptors* encryption scheme is an ordinary encryption scheme augmented with a pair of "alternative" decryption oracles, which always produce the correct result on wellformed ciphertexts – but whose behavior on invalid ciphertexts is unconstrained.

The security guarantees of this scheme come in the form of indistinguishability conditions related to these oracles. Namely, we require that:

- An efficient adversary that only has access to the first oracle cannot distinguish a wellformed ciphertext from an invalid ciphertext, which is produced by an invalid ciphertext sampling algorithm (which is a part of the scheme).

- An efficient adversary that only has access to the second oracle has no significant advantage in distinguishing an invalid "encryption" of one message from an invalid "encryption" of another message.

6.3 Method for constructing encryption schemes

Elkind and Sahai propose the following method for constructing IND-CCA2 secure encryption schemes.

First, construct an encryption scheme which satisfies the "bare" oblivious decryptors model: This can be done quite easily, with simple proofs of security. Then, by adding a Simulation-Sound NIZK proof, the scheme becomes provably IND-CCA2 secure.

6.4 Unifications and other important results

In their article [5] Elkind and Sahai show the following:

1. *Smooth Hash Proof Systems* as described by Cramer and Shoup [4] are a case in the oblivious decryptors model.

2. The IND-CCA2 secure encryption scheme proposed by Sahai [3] is also a case of the oblivious decryptors model.

3. Any proof system, whether noninteractive or not, which is based on Universal Projective Hashing [4] must necessarily be limited to problems which admit Statistical Zero-Knowledge Proofs. This implies that if any NP-complete language admits a proof based on Universal Projective Hashing, then the polynomial-time hierarchy must collapse.

7 A Compact IND-CCA2 Secure Identity-Based Encryption Scheme

7.1 Introduction

in their article from 2005 [7], Boyen, Mei and Waters build a compact encryption system based on the Waters identity-based encryption system (IBE) [6]. An identity-based cryptosystem is a key authentication system in which the public key of a user is some unique information about the identity of the user (eg. a user's email address). The

proposed cryptosystem is efficient and has short ciphertexts. This is due to integration with the underlying IBE.

7.2 The Scheme

Let G and $\hat{G}$ be two cyclic groups of prime order p, between which there exists an efficiently computable bilinear map into G_T. Specifically, let $e : G \times \hat{G} \rightarrow G_T$ denote the bilinear map, and let $g \in G$ and $h \in \hat{G}$ be the corresponding generators. The size p of the groups is determined by the security parameter. It is also assumed, that a collision resistant (but not necessarily one-way) function family H_i is available.

The cryptosystem is described by the following three algorithms.

Key Generation: A users public/private key pair generation algorithm proceeds as follows. First, a secret $\alpha \in \mathbb{Z}_p$ is chosen at random, from which the values $h_0 = h^\alpha$ and $Z = e(g, h_0)$ are calculated.

Next, the algorithm chooses a random $y_0 \in \mathbb{Z}_p$ and a random n-length vector $\vec{y} = (y_1, \ldots, y_n)$, whose elements are chosen at random from $\mathbb{Z}_p$. It then calculates $u\prime = g^{y\prime}$ and $u_i = g^{y_i}$ for $i = 1$ to n.

Finally, a random seed s for the collision resistant family is chosen. The published public key is

$$(s, Z = e(g,h)^\alpha, u' = g^{y'}, u_1 = g^{y_1}, \ldots, u_n = g^{y_n}) \in$$
$$\in \{s\} \times G_T \times G^{n+1},$$

and the private key is

$$h_0 = h^\alpha, y', y_1, \ldots, y_n) \in \hat{G} \times Z_p^{n+1}.$$

Encryption: A message $m \in G_T$ is encrypted as follows. First, a value $t \in \mathbb{Z}_p$ is randomly chosen. Next, the first two elements of the ciphertext are computed: $C_0 = m \cdot Z^t = m \cdot e(g,h)^{\alpha t}$ and $C_1 = g^t$. Next, a bit string $w \in \{0,1\}^n$ is derived as $w = H_s(C_0, C_1)$. Let $w_1 w_2 \ldots w_n$ denote the binary expansion of w, where each bit $w_i \in \{0,1\}$.

The final step is to compute $C_2 = (u', \prod_{i=1}^n u_i^{w_i})^t$. The complete ciphertext, $C = (C_0, C_1, C_2)$, consists of the three group elements

$$\left(m \cdot Z^t, g^t, (u' \prod_{i=1}^n u_i^{w_i})^t \right) \in G_T \times G^2.$$

Decryption: Let $C = (C_0, C_1, C_2)$ be a ciphertext and $w = H_s(C_0, C_1)$. In a well-formed ciphertext, the quadruple $(g, C_1, u', \prod_{i=1}^n u_i^{w_i}, C_2) \in G^4$ will be a Diffie-Hellman tuple, which can be efficiently tested by the private key holder as follows.

Given a ciphertext C the algorithm first computes $w = H_s(C_0, C_1)$, expressed in binary as $w_1 w_2 \ldots w_n$. Next, it raises C_1 to the power of $w' = y' + \sum_{i=1}^n y_i w_i mod p$, and compares the result $(C_1)^{w'}$ with C_2. If these two values are unequal, then $(g, C_1, u', \prod_{i=1}^n u_i^{w_i}, C_2)$ is not a Diffie-Hellman tuple, and the algorithm rejects the ciphertext.

Otherwise, the ciphertext is valid, and the algorithm decrypts the message as

$$C_0 / e(C_1, h_0) = m \in G_T.$$

8 In conclusion

An overview of IND-CCA2 secure cryptosystems is given. It is clear that we will see further advances in the coming years.

References

[1] M. Naor, M. Yung. "Public-key cryptosystems provably secure against chosen ciphertext attacks". Proceedings of the 22nd Annual Symposium on Theory of Computing, ACM, 1990.

[2] R. Cramer, V. Shoup. "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack". In Advances in Cryptology-CRYPTO 1998, volume 1462 of LNCS, 1998.

[3] A. Sahai. "Non–Malleable Non–Interactive Zero Knowledge and Adaptive Chosen–Ciphertext Security". Proceedings of the 40th Symposium on Foundations of Computer Science, IEEE, 1999.

[4] R. Cramer, V. Shoup. "Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public–key encryption". In Advances

in Cryptology-EUROCRYPT 2002, volume 2729 of LNCS, pages 4564, 2002.

[5] E. Elkind, A.Sahai. "A Unified Methodology For Constructing Public-Key Encryption Schemes Secure Against Adaptive Chosen-Ciphertext Attack". Cryptology ePrint Archive, Report 2002/042, 2002, http://eprint.iacr.org/

[6] B. Waters. "Efficient identity based encryption without random oracles". In Advances in CryptologyEUROCRYPT 2005, Lecture Notes in Computer Science. Springer Verlag, 2005.

[7] X. Boyen, Q. Mei, B. Waters. "Direct Chosen Ciphertext Security from Identity-Based Techniques". Cryptology ePrint Archive, Report 2005/288, 2005, http://eprint.iacr.org/