MTAT.07.006 Research Seminar in Cryptography

IND-CCA2 secure cryptosystems

Dan Bogdanov
University of Tartu
db@ut.ee

Overview

- Notion of indistinguishability
- The Cramer-Shoup cryptosystem
- Newer results

Indistinguishability assumptions

Indistinguishability under a ...

- Chosen Plaintext Attack - (*IND-CPA security*)
- Chosen Ciphertext Attack - (*IND-CCA security*)
- Adaptive Chosen Ciphertext Attack - (*IND-CCA2 security*)

Who is the bad guy?

We are protecting ourselves from the evil **A**, who

- is a probabilistic polynomial time Turing machine,
- has all the algorithms and
- has full access to communication media.

IND-CPA Definition - Startup

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.

IND-CPA Definition - The Challenge

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.

IND-CPA Definition - The Result

- The adversary **A** wins the game if it guesses the bit b.
- A cryptosystem is **indistinguishable under chosen plaintext attack** if no adversary can win the above game with probability p greater than $\frac{1}{2} + \epsilon$, where ϵ is a negligible function in the security parameter k.
- If $p > \frac{1}{2}$ then the difference $p - \frac{1}{2}$ is the **advantage** of the given adversary in distinguishing the ciphertext.

IND-CCA Definition - Startup

NEW: The adversary **A** gains access to a decryption oracle which decrypts arbitrary ciphertexts at the adversary's request, returning the plaintext.

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.

IND-CCA Definition - The Challenge

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. 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 before guessing.

    (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.

5. In the end it will guess the value of b.

IND-CCA Definition - The Result

- Again, the adversary **A** wins the game if it guesses the bit b.

- A cryptosystem is **indistinguishable under chosen ciphertext attack** if no adversary can win the above game with probability p greater than $\frac{1}{2} + \epsilon$, where ϵ is a negligible function in the security parameter k.

- If $p > \frac{1}{2}$ then the difference $p - \frac{1}{2}$ is the **advantage** of the given adversary in distinguishing the ciphertext.

The Cramer-Shoup cryptosystem

Published in:
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.

- Provably secure against adaptive chosen ciphertext attacks.

- The first practical such cryptosystem.

- The security proof is based on the hardness of the Diffie-Hellman decision problem in the used group.

The Cramer-Shoup Scheme - Assumptions

- 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 $\mathbf{Z}_q$ is also required.

The Cramer-Shoup Scheme - Key Generation

1. We choose two random elements
   $g_1, g_2 \in G$ and $x_1, x_2, y_1, y_2, z \in \mathbf{Z}_q$.

2. We calculate $c = g_1^{x_1} g_2^{x_2}, d = g_1^{y_1} g_2^{y_2}, h = g_1^z$.

3. We choose a hash function H from our family of universal one-way hash functions.

4. 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).

The Cramer-Shoup Scheme - Encryption

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

The Cramer-Shoup Scheme - Encryption

1. Given a ciphertext (u_1, u_2, e, v) we first compute $\alpha = H(u_1, u_2, e)$
2. Check if $u_1^{x_1+y_1\alpha} u_2^{x_2+y_2\alpha} = v$
   (a) If the condition does not hold, we reject the ciphertext as invalid.
   (b) Otherwise we decrypt the message $m = e/u_1^z$.

The Cramer-Shoup 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.

The Cramer-Shoup generalisation

In 2001 Cramer and Shoup published a general approach to constructing IND-CCA2 secure cryptosystems.

- They introduce *Universal Hash Proof Systems* (UHPS) which is a kind of non-interactive zero-knowledge proof system for a language.
- They show that when given an efficient UHPS for a language with certain natural cryptographic indistinguishability properties, one can construct an efficient IND-CCA2 secure public-key encryption scheme.
- They construct two more systems and show that their original system is a case in their general theory.

The Oblivious Decryptors method

Proposed in 2002 by Elkind and Sahai.

- A unifying methodology for constructing IND-CCA2 secure schemes. Generalises the Cramer-Shoup scheme and other schemes (at the time of writing the article).

- Main construction: An encryption scheme satisfying *Oblivious Decryptors* can be extended with *Simulation-Sound Non-Interactive Zero-Knowledge* proof to produce an IND-CCA2 secure encryption system.

An Identity-Based IND-CCA2 secure cryptosystem

Bleeding-edge: proposed by Boyen, Mei and Waters in 2005.

- An *Identity-Based Encryption* (IBE) scheme 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).
- Build a compact IND-CCA2 encryption system based on the Waters identity-based encryption system.
- A fresh approach as it doesn't fall under previous unified models.
- The proposed cryptosystem is efficient and has short ciphertexts. This is due to integration with the underlying IBE.

End of talk

Thanks for listening!