Introduction to Cryptology

9.1 - The Public-key Revolution

Federico Pintore
Mathematical Institute, University of Oxford (UK)

UNIVERSITY OF OXFORD

Michaelmas term 2020

Private keys

Assuming that communicating parties are able to share a secret key, symmetric-key schemes ensure secrecy and integrity.

Private keys

Assuming that communicating parties are able to share a secret key, symmetric-key schemes ensure secrecy and integrity.

How communicating parties share a secret key?

Private keys

Assuming that communicating parties are able to share a secret key, symmetric-key schemes ensure secrecy and integrity.

How communicating parties share a secret key?

They should have access to a secure channel.

Private keys

Assuming that communicating parties are able to share a secret key, symmetric-key schemes ensure secrecy and integrity.

How communicating parties share a secret key?

They should have access to a secure channel.

- A secure channel is usually slow and costly!

Private keys

Assuming that communicating parties are able to share a secret key, symmetric-key schemes ensure secrecy and integrity.

How communicating parties share a secret key?

They should have access to a secure channel.

- A secure channel is usually slow and costly!
- It does not work well for open systems.

Private keys

Assuming that communicating parties are able to share a secret key, symmetric-key schemes ensure secrecy and integrity.

How communicating parties share a secret key?

They should have access to a secure channel.

- A secure channel is usually slow and costly!
- It does not work well for open systems.
- There is the need to securely store a big number of keys.

Key-Distribution Centers (KDCs)

A KDC is a trusted third party; each user share a key with the KDC by means of a secure channel.

When Alice and Bob want to communicate, the KDC provides a key to them.

Key-Distribution Centers (KDCs)

A KDC is a trusted third party; each user share a key with the KDC by means of a secure channel.

When Alice and Bob want to communicate, the KDC provides a key to them.

- Each user has to store only one long-term secret key.

Key-Distribution Centers (KDCs)

A KDC is a trusted third party; each user share a key with the KDC by means of a secure channel.

When Alice and Bob want to communicate, the KDC provides a key to them.

- Each user has to store only one long-term secret key.
- Still requires the use of a private channel.
- Each user must trust the KDC.
- The KDC is a single point of failure, and a high-value target.

New Directions in Cryptography

In 1976, Diffie and Hellman published a paper, titled

New Directions in Cryptography

that has revolutionised Cryptography.

- They posed the first step towards Public-key Cryptography, but they did not give any candidate construction.
- They proposed an interactive protocol to share a secret key via communication over a public channel.

New Directions in Cryptography

In 1976, Diffie and Hellman published a paper, titled

New Directions in Cryptography

that has revolutionised Cryptography.

- They posed the first step towards Public-key Cryptography, but they did not give any candidate construction.
- They proposed an interactive protocol to share a secret key via communication over a public channel.

In 1977, R. Rivest, A. Shamir and L. Adleman introduced the RSA problem, and designed the first public-key encryption and digital signature scheme based on its hardness.

Key-exchange protocol

It is a probabilistic protocol Π to generate a shared, secret key.

Key-exchange protocol

It is a probabilistic protocol Π to generate a shared, secret key.

- Alice and Bob start by holding a security parameter n.
- They run Π using independent random bits.
- At the end of the protocol, they output k_A and k_B, respectively.

Key-exchange protocol

It is a probabilistic protocol Π to generate a shared, secret key.

- Alice and Bob start by holding a security parameter n.
- They run Π using independent random bits.
- At the end of the protocol, they output k_A and k_B, respectively.

Correctness: with overwhelming probability $k_A = k_B$.

Key-exchange - Security definition

The key-exchange Experiment $\mathrm{KE}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)$

Key-exchange - Security definition

The key-exchange Experiment $\mathrm{KE}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)$

Challenger Ch		Adversary $\mathcal{A}$
Execute Π		
		Access to the transcript
$b \leftarrow \{0,1\}$		
If $b = 0$, $\hat{k} := k$ else $\hat{k} \leftarrow \{0,1\}^{\lvert k \rvert}$	$\xrightarrow{\hat{k}}$	
		Output their guess b'

$\mathcal{A}$ wins the game, i.e. $\mathrm{KE}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n) = 1$, if $b' = b$.

Key-exchange - Security definition

Definition

The key-exchange protocol Π *is secure if, for every PPT* $\mathcal{A}$*, the following holds:*

$$\mathrm{Adv}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n) = \Pr(\mathrm{KE}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n) = 1) \leq 1/2 + \mathrm{negl}(n)\,.$$

Public-Key Cryptography

In the public-key setting, a party generates a pair of keys: a public key and a private key.

They can be used to achieve:

- secrecy, by means of a public-key encryption scheme;
- integrity and authenticity, by means of a digital signature scheme.

Public-Key Cryptography

- Key distribution over public, but authenticated channels.
- The need to store many secret keys is reduced.
- Suitable for open systems.

Public-Key Encryption

A public-key encryption scheme $(\text{KeyGen}, \text{Enc}, \text{Dec})$ consists of three algorithms:

- $(\text{PK}, \text{SK}) \leftarrow \text{KeyGen}(n)$: randomised algorithm which, on input n, returns a pair of keys (PK, SK) - the public key PK and the corresponding secret key SK.
- $c \leftarrow \text{Enc}(\text{PK}, m)$: a (possibly randomised) algorithm that takes a public key PK, a message m and returns a ciphertext c.
- $m \leftarrow \text{Dec}(\text{SK}, c)$: a deterministic algorithm that, on input a secret key SK and a ciphertext c, returns a message $m \in \mathcal{M} \cup \perp$.

Correctness: for every $m \in \mathcal{M}$ it holds

$$\Pr(\text{Dec}(\text{SK}, \text{Enc}(\text{PK}, m)) = m | (\text{SK}, \text{PK}) \leftarrow \text{KeyGen}(n)) = 1$$

Public-key Encryption - Definition of Security

The eavesdropping indistinguishability Experiment $\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},E}(n)$

Public-key Encryption - Definition of Security

The eavesdropping indistinguishability Experiment $\text{PubK}^{\text{eav}}_{\mathcal{A},E}(n)$

Challenger Ch | Adversary $\mathcal{A}$

$(\text{PK}, \text{SK}) \leftarrow \text{KeyGen}(n)$

$\xrightarrow{\text{PK}}$

$\xleftarrow{m_0, m_1, |m_0| = |m_1|}$

$b \leftarrow \{0, 1\}$

$\xrightarrow{c = \text{Enc}(\text{PK}, m_b)}$

Output their guess b'

Public-key Encryption - Definition of Security

The eavesdropping indistinguishability Experiment $\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},E}(n)$

Challenger Ch		Adversary $\mathcal{A}$
$(\mathrm{PK}, \mathrm{SK}) \leftarrow \mathrm{KeyGen}(n)$		
	$\xrightarrow{\mathrm{PK}}$	
	$\xleftarrow{m_0, m_1, \lvert m_0\rvert = \lvert m_1\rvert}$	
$b \leftarrow \{0, 1\}$		
	$\xrightarrow{c = \mathrm{Enc}(\mathrm{PK}, m_b)}$	
		Output their guess b'

$\mathcal{A}$ wins the game, i.e. $\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},E}(n) = 1$, if $b' = b$.

Public-key Encryption - Definition of Security

Definition

An encryption scheme E has indistinguishable encryptions in the presence of an eavesdropper if, for every PPT adversary $\mathcal{A}$, the following holds:

$$\mathrm{Adv}^{\mathrm{eav}}_{\mathcal{A},E}(n) = \Pr(\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},E}(n) = 1) \leq 1/2 + \mathrm{negl}(n)\,.$$

CPA-security

$\mathcal{A}$ knows PK, hence they have access to an encryption oracle.

Consequently, if E has indistinguishable encryptions in the presence of an eavesdropper, then it is CPA-secure.

CPA-security

$\mathcal{A}$ knows PK, hence they have access to an encryption oracle.

Consequently, if E has indistinguishable encryptions in the presence of an eavesdropper, then it is CPA-secure.

This is in contrast to the symmetric-key setting.

CPA-security

$\mathcal{A}$ knows PK, hence they have access to an encryption oracle.

Consequently, if E has indistinguishable encryptions in the presence of an eavesdropper, then it is CPA-secure.

This is in contrast to the symmetric-key setting.

Also in the public-key setting, a deterministic encryption scheme cannot be CPA-secure.

Public-key Encryption - CCA-security

CCA Indistinguishability Experiment $\mathrm{PubK}^{\mathrm{cca}}_{\mathcal{A},E}(n)$

Public-key Encryption - CCA-security

CCA Indistinguishability Experiment $\mathrm{PubK}^{\mathrm{cca}}_{\mathcal{A},E}(n)$

Challenger Ch		Adversary $\mathcal{A}$
$(\mathrm{PK}, \mathrm{SK}) \leftarrow \mathrm{KeyGen}(n)$		
	$\xrightarrow{\mathrm{PK}}$	
		Access to $\mathrm{Dec}(\mathrm{SK}, \cdot)$
	$\xleftarrow{m_0, m_1, \lvert m_0 \rvert = \lvert m_1 \rvert}$	
$b \leftarrow \{0, 1\}$		
	$\xrightarrow{c = \mathrm{Enc}(\mathrm{PK}, m_b)}$	
		Access to $\mathrm{Dec}(\mathrm{SK}, \cdot)^c$
		Output their guess b'

Public-key Encryption - CCA-security

CCA Indistinguishability Experiment $\mathrm{PubK}^{\mathrm{cca}}_{\mathcal{A},E}(n)$

Challenger Ch		Adversary $\mathcal{A}$
$(\mathrm{PK}, \mathrm{SK}) \leftarrow \mathrm{KeyGen}(n)$		
	$\xrightarrow{\mathrm{PK}}$	
		Access to $\mathrm{Dec}(\mathrm{SK}, \cdot)$
	$\xleftarrow{m_0, m_1, \lvert m_0 \rvert = \lvert m_1 \rvert}$	
$b \leftarrow \{0, 1\}$		
	$\xrightarrow{c = \mathrm{Enc}(\mathrm{PK}, m_b)}$	
		Access to $\mathrm{Dec}(\mathrm{SK}, \cdot)^c$
		Output their guess b'

$\mathcal{A}$ wins the game, i.e. $\mathrm{PubK}^{\mathrm{cca}}_{\mathcal{A},E}(n) = 1$, if $b' = b$.

Public-key Encryption - CCA-security

Definition

An encryption scheme is CCA-secure if, for every PPT adversary $\mathcal{A}$, the following holds:

$$\mathrm{Adv}^{\mathrm{cca}}_{\mathcal{A},E}(n) = \Pr(\mathrm{PubK}^{\mathrm{cca}}_{\mathcal{A},E}(n) = 1) \leq 1/2 + \mathrm{negl}(n)\,.$$

Dealing with arbitrary-length messages

In the indistinguishability of multiple encryptions experiment, $\mathcal{A}$ is given access to a left-or-right encryption oracle.

On input a pair of messages m_0, m_1 (with $|m_0| = |m_1|$), the oracle returns $c \leftarrow \text{Enc}(\text{PK}, m_b)$.

Dealing with arbitrary-length messages

In the indistinguishability of multiple encryptions experiment, $\mathcal{A}$ is given access to a left-or-right encryption oracle.

On input a pair of messages m_0, m_1 (with $|m_0| = |m_1|$), the oracle returns $c \leftarrow \mathrm{Enc}(\mathrm{PK}, m_b)$.

Theorem

If a public-key encryption scheme is CPA-secure, then it also has indistinguishable multiple encryptions.

Dealing with arbitrary-length messages

In the indistinguishability of multiple encryptions experiment, $\mathcal{A}$ is given access to a left-or-right encryption oracle.

On input a pair of messages m_0, m_1 (with $|m_0| = |m_1|$), the oracle returns $c \leftarrow \mathrm{Enc}(\mathrm{PK}, m_b)$.

Theorem

If a public-key encryption scheme is CPA-secure, then it also has indistinguishable multiple encryptions.

Any CPA-secure public-key encryption scheme for fixed-length messages (down to one bit!) can be used as a CPA-secure public key-encryption scheme for arbitrary-length messages.

Further Reading I

Mihir Bellare, Alexandra Boldyreva, and Silvio Micali.
Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements.
In Bart Preneel, editor, Advances in Cryptology — EUROCRYPT 2000, volume 1807 of Lecture Notes in Computer Science, pages 259–274. Springer Berlin Heidelberg, 2000.

Dan Boneh.
Simplified OAEP for the RSA and Rabin Functions.
In Joe Kilian, editor, Advances in Cryptology — CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pages 275–291. Springer Berlin Heidelberg, 2001.

Further Reading II

Ronald Cramer and Victor Shoup.
Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack.
SIAM Journal on Computing, 33(1):167–226, 2003.

Whitfield Diffie and Martin E Hellman.
New directions in cryptography.
Information Theory, IEEE Transactions on, 22(6):644–654, 1976.

Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir.
New attacks on Feistel Structures with Improved Memory Complexities.
In Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I, pages 433–454, 2015.

Further Reading III

Naofumi Homma, Atsushi Miyamoto, Takafumi Aoki, Akashi Satoh, and Adi Shamir.
Collision-Based Power Analysis of Modular Exponentiation Using Chosen-Message Pairs.
In Cryptographic Hardware and Embedded Systems - CHES 2008, 10th International Workshop, Washington, D.C., USA, August 10-13, 2008. Proceedings, pages 15–29, 2008.