

Chapter 13 – Asymmetric Encryption

March 24, 2022

Terms of Use

- This work is published with a CC BY-ND 4.0 license (CC BY ND)
 - CC = Creative Commons (CC)
 - BY = Attribution (BY)
 - ND = No Derivatives (ND)

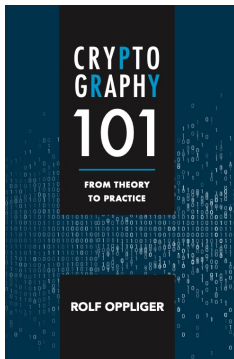
whoami



rolf-oppliger.ch
rolf-oppliger.com

- Swiss National Cyber Security Centre
NCSC (scientific employee)
- eSECURITY Technologies Rolf Oppliger
(founder and owner)
- University of Zurich (adjunct professor)
- Artech House (author and series editor for
information security and privacy)

Reference Book



© Artech House, 2021
ISBN 978-1-63081-846-3

<https://books.esecurity.ch/crypto101.html>

Challenge Me



13. Asymmetric Encryption

- A set of small navigation icons typically found in Beamer presentations, including symbols for back, forward, search, and other slide controls.

13. Asymmetric Encryption

13.1 Introduction

13.2 Probabilistic Encryption

13.3 Asymmetric Encryption Systems

13.4 Identity-Based Encryption

13.5 Fully Homomorphic Encryption

13.6 Final Remarks

13.1 Introduction

- An asymmetric encryption system can be implemented with a trapdoor (one-way) function
 - The (one-way) function can be computed with the public key $pk \rightarrow \text{encryption}$
 - The inverse function can be computed with the private (secret) key $sk \rightarrow \text{decryption}$
- The asymmetric encryption system consists of three efficiently computable algorithms, i.e., Generate, Encrypt, and Decrypt
- Encrypt and Decrypt must be inverse to each other

13.1 Introduction



13.1 Introduction

- If m is larger than one block, then a sequence of blocks must be generated and each block must be encrypted and decrypted individually (using a mode of operation)

13.1 Introduction

- Similar to a symmetric encryption system, one may wonder whether an asymmetric encryption system is secure
- Information-theoretic or unconditional security does not exist here
- The Encrypt algorithm works with a public key, and hence an adversary who is given a ciphertext can always mount a brute-force attack to find the appropriate plaintext message
- Such an attack may be computationally expensive but feasible
- The best one can achieve is (some possibly strong notion of) computational or conditional security

13.1 Introduction

- ◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ ▶ ↺ 🔍 ↻

13.1 Introduction

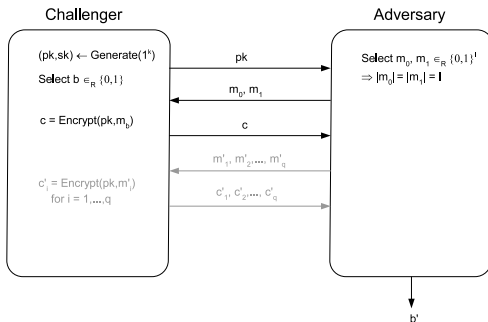
- The simplest and most straightforward notion of security is **one-way security**
- An asymmetric encryption system is **one-way secure**, if it is computationally infeasible for the adversary (one has in mind) to determine a plaintext message from a given ciphertext and public key
- This notion of security is not sufficient
- It does not exclude the case that the ciphertext may leak some partial information about the plaintext message

13.1 Introduction

- Stronger notions of security
 - Semantic security
 - Indistinguishability of ciphertext (IND)
 - Nonmalleability (NM)
- IND and NM can be considered under a CPA (CPA2) or CCA (CCA2)
- This can be formalized in IND-CPA and IND-CCA games
- In either case, the encryption must be probabilistic

13.1 Introduction

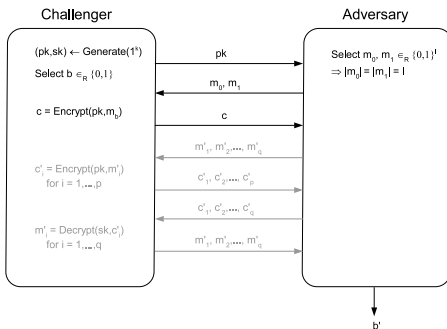
- The adversary wins the IND-CPA game if $\Pr[b' = b] = \frac{1}{2} + \epsilon$ for some nonnegligible ϵ



13. Asymmetric Encryption

13.1 Introduction

- The adversary wins the IND-CCA game if $\Pr[b' = b] = \frac{1}{2} + \epsilon$ for some nonnegligible ϵ



13.1 Introduction

-
- ```

graph TD
 A["INT-CTXT ∧ IND-CPA"] --> B["IND-CCA"]
 B <--> C["NM-CCA"]
 C --> D["NM-CPA"]
 D --> E["IND-CPA"]
 E --> F["INT-PTXT ∧ IND-CPA"]
 A --> F

```

# 13. Asymmetric Encryption

## 13.2 Probabilistic Encryption

- In the early 1980s, Shafi Goldwasser and Silvio Micali introduced the notion of semantic security and proposed **probabilistic encryption**
- It is based on the assumed intractability of the **quadratic residuosity problem (QRP)** in  $\mathbb{Z}_n^*$

### Definition A.31 (QRP)

If  $n \in \mathbb{N}$  is a composite integer and  $x \in \mathbb{Z}_n^*$ , then it is to decide whether  $x$  is a quadratic residue modulo  $n$ , i.e.,  $x \in QR_n$ , or not, i.e.,  $x \in QNR_n$ .

## 13.2 Probabilistic Encryption

- $$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{if } x \equiv 0 \pmod{p} \\ 1 & \text{if } x \in QR_p \\ -1 & \text{if } x \in QNR_p \end{cases}$$

- A set of small navigation icons typically found in Beamer presentations, including symbols for back, forward, search, and other slide controls.

# 13. Asymmetric Encryption

## 13.2 Probabilistic Encryption

- The Legendre symbol of  $x$  modulo  $p$  can be efficiently computed with Euler's criterion

$$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \pmod{p}$$

- It is one iff  $x$  is a quadratic residue modulo  $p$

$$x \in QR_p \Leftrightarrow \left(\frac{x}{p}\right) = 1$$

# 13. Asymmetric Encryption

## 13.2 Probabilistic Encryption

- If  $n$  is a composite number, then

$$x \in QR_n \Rightarrow \left(\frac{x}{n}\right) = 1$$

but

$$x \in QR_n \not\Leftrightarrow \left(\frac{x}{n}\right) = 1$$

- If  $x$  is a quadratic residue modulo  $n$ , then the Jacobi symbol of  $x$  modulo  $n$  must be 1
- The converse need not be true

## 13.2 Probabilistic Encryption

- $$x \in QNR_n \Leftrightarrow \left(\frac{x}{n}\right) = -1$$

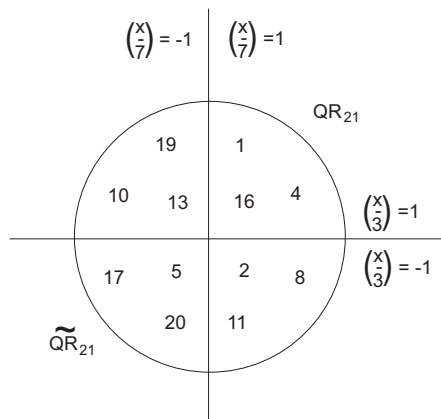
- A set of small navigation icons typically found in Beamer presentations, including symbols for back, forward, search, and other slide controls.

## 13.2 Probabilistic Encryption

- $$|QR_n| = |\widetilde{QR_n}| = (p-1)(q-1)/4$$

- This means that half of the elements in  $J_n$  are quadratic residues and the other half are pseudosquares modulo  $n$
- For a given element of  $J_n$  it is computationally infeasible to decide whether it is a quadratic residue (square) or a pseudosquare modulo  $n$  — unless one knows the factorization of  $n$

## 13.2 Probabilistic Encryption



- $p = 3$
- $q = 7$
- $n = 3 \cdot 7 = 21$
- $\phi(n) = 2 \cdot 6 = 12$
- $\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$
- $QNR_{21} = \{2, 8, 10, 11, 13, 19\}$
- $J_{21} = \{1, 4, 5, 16, 17, 20\}$
- $QR_{21} = \{1, 4, 16\}$
- $\widetilde{QR_{21}} = \{5, 17, 20\}$



## 13.2 Probabilistic Encryption

System parameters: —

| Generate                                                                                        | Encrypt                                                                                                                                               | Decrypt                                                                                                         |
|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| $((1^l))$                                                                                       | $((n, y), m)$                                                                                                                                         | $((p, q), c)$                                                                                                   |
| $p, q \xleftarrow{r} \mathbb{P}_{l/2}$<br>$n = p \cdot q$<br>$y \xleftarrow{r} \overline{QR_n}$ | for $i = 1, \dots, w$<br>$x_i \xleftarrow{r} \mathbb{Z}_n^*$<br>if $m_i = 1$<br>then $c_i \equiv x_i^2 \pmod{n}$<br>else $c_i \equiv yx_i^2 \pmod{n}$ | for $i = 1, \dots, w$<br>$e_i = \left(\frac{c_i}{p}\right)$<br>if $e_i = 1$<br>then $m_i = 1$<br>else $m_i = 0$ |
| $((n, y), (p, q))$                                                                              | $c = c_1, \dots, c_w$                                                                                                                                 | $m = m_1, \dots, m_w$                                                                                           |
|                                                                                                 | (c)                                                                                                                                                   | (m)                                                                                                             |

# 13. Asymmetric Encryption

## 13.2 Probabilistic Encryption

- In its original form, probabilistic encryption has a huge message expansion (i.e., every bit is encrypted with an element of  $\mathbb{Z}_n^*$ )
- This can be improved considerably
- Probabilistic encryption is still not used in the field, because it competes with RSA-OAEP and many other efficient asymmetric encryption systems
- The bottom line is that probabilistic encryption is theoretically (and historically) interesting but practically irrelevant

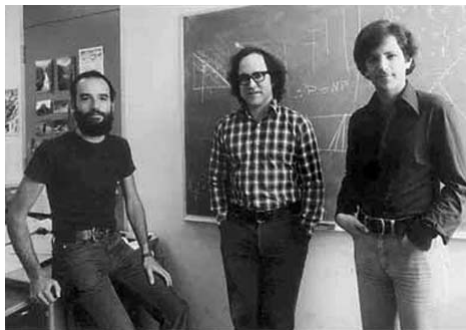
### 13.3 Asymmetric Encryption Systems

- After the discovery of the Diffie-Hellman key exchange in the mid-1970s, a few public key cryptosystems were invented and proposed
  - RSA (1977)
  - Rabin (1979)
  - Elgamal (1984)
  - ...
- These systems can be used for asymmetric encryption

# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — RSA

- RSA was invented by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977



# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — RSA

- A U.S. patent application was filed on December 14, 1977
- A corresponding article was published in the February 1978 issue of the *Communications of the ACM*
- The company RSA Security was founded in 1982
- On September 20, 1983, the U.S. patent 4,405,829 entitled “Cryptographic Communications System and Method” was assigned to MIT (expired in 2000)
- Rivest, Shamir, and Adleman were granted the prestigious ACM A.M. Turing Award in 2002

# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — RSA

- As its name suggests, the RSA public key cryptosystem is based on the RSA family of trapdoor permutations
- Contrary to other public key cryptosystems, it yields both an asymmetric encryption system and a DSS
- A major advantage of RSA is that the same algorithms
  - Generate
  - Encrypt
  - Decryptare used in either case

## 13.3 Asymmetric Encryption Systems — RSA

System parameters: —





## 13.3 Asymmetric Encryption Systems — RSA

- The Generate algorithm first selects  $p = 11$  and  $q = 23$ , and computes  $n = 11 \cdot 23 = 253$  and  $\phi(253) = 10 \cdot 22 = 220$ , before it selects  $e = 3$  and computes  $d = 147$   
[ $3 \cdot 147 = 441 \equiv 1 \pmod{220}$ ]
- $(253, 3)$  is the public key, whereas 147 is the private key
- To encrypt  $m = 26$ , the Encrypt algorithm computes  $c = 26^3 \bmod 253 = 119$
- This value is transmitted to the recipient
- To decrypt  $c = 119$ , the Decrypt algorithm computes  $m = 119^{147} \bmod 253 = 26$

# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — RSA

- Since its invention in 1977, the security of the RSA public key cryptosystem has been subject to a lot of public scrutiny
- Many people have challenged and analyzed the security of RSA
- No devastating vulnerability or weakness has been found so far
- More than four decades of cryptanalytical research have provided insight into its security properties and guidelines for proper implementation and use

# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — RSA

- The RSA asymmetric encryption system is based on the RSA family of trapdoor permutations
- This means that its security is based on the RSAP that is (believed to be) computationally intractable
- If  $n$  is sufficiently large and  $m$  is widespread between 0 and  $n - 1$ , then the adversary must find the correct  $m$  by a brute-force attack
- Such an attack has an exponential running-time and is prohibitively expensive in terms of computational resources

## 13.3 Asymmetric Encryption Systems — RSA

- The RSAP polytime reduces to the IFP, i.e.,  $\text{RSAP} \leq_P \text{IFP}$
- This means that one can invert the RSA function if one can solve the IFP
- The converse is not known to be true, meaning that it is not known whether an algorithm to solve the IFP can be constructed from an algorithm to solve the RSAP

# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — RSA

- The following problems are computationally equivalent
  - Factorize  $n$
  - Compute  $\phi(n)$  from  $n$
  - Determine  $d$  from  $(n, e)$
- This suggests that the prime factors of  $n$  (i.e.,  $p$  and  $q$ ),  $\phi(n)$ , and  $d$  are all trapdoors

# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — RSA

- The LSB yields a hard-core predicate for the RSA function
- More generally, the RSA function has the bit security property (i.e., all bits are equally well protected)
- The bit security proof of the RSA encryption system is a double-edged sword, because the security reduction also provides a possibility to attack a leaky implementation
- If an implementation of the RSA Decrypt algorithm leaks some bit(s) of a plaintext message, then this leakage can be (mis)used to solve the RSAP and decrypt a ciphertext without knowing the private key (e.g., Bleichenbacher attack)

# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — RSA

- The encryption function of the RSA asymmetric encryption system is deterministic
- This means that it can neither be semantically secure nor provide IND-CPA
- Specific attacks (in addition to side-channel attacks)
  - Common modulus attacks ( $\rightarrow$  never reuse  $n$ )
  - Low exponent attacks ( $\rightarrow$  use  $e = 2^{16} + 1 = 65,537$  or larger)
  - Attacks that exploit the multiplicative structure (or homomorphic property) of the RSA function

# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — RSA

- If  $m_1$  and  $m_2$  are encrypted with  $(n, e)$ , then  $c_1 = m_1^e \bmod n$  and  $c_2 = m_2^e \bmod n$
- The product  $m = (m_1 m_2) \bmod n$  can be encrypted as

$$c = (c_1 c_2) \bmod n$$

- This follows from  $c_1 c_2 = (m_1^e m_2^e) = (m_1 m_2)^e \bmod n$
- So  $c$  can be computed without knowing  $m_1$ ,  $m_2$ , or  $m$
- This homomorphic property is a dual-edged sword



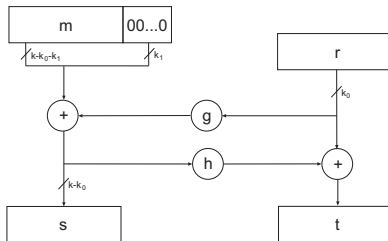
# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — RSA

- The homomorphic property can be eliminated with padding
- The **optimal asymmetric encryption padding (OAEP)** is a padding scheme that uses random values to turn the encryption algorithm into a probabilistic one
- OAEP was adopted in PKCS #1 (since version 2.0) and specified in RFC 2437 (version 2.1 in RFC 3447)
- RSA-OAEP is semantically secure and provides IND-CPA in the random oracle model

## 13.3 Asymmetric Encryption Systems — RSA

$$\text{OAEP}(m) = (s, t) = \underbrace{m \oplus g(r)}_s \parallel \underbrace{r \oplus h(m \oplus g(r))}_t$$



# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — RSA

- The recipient computes

$$r = t \oplus h(s) = r \oplus h(m \oplus g(r)) \oplus h(m \oplus g(r))$$

and

$$m = s \oplus g(r) = m \oplus g(r) \oplus g(r)$$

to retrieve the plaintext message  $m$

- This string still comprises the  $k_1$  zero bits that are appended to  $m$

# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — RSA

- Important facts (to keep in mind)
  - The modulus  $n$  should be  $\geq 2,048$  bits
  - The prime factors  $p$  and  $q$  should be equally long (but not too close to  $\sqrt{n}$ )
  - Due to its deterministic encryption function, RSA is at most one-way secure (i.e., it cannot provide IND-CPA and is not semantically secure)
  - As such, basic (textbook) RSA is in line with the state of the art in asymmetric encryption
  - RSA-OAEP should be used whenever possible

### 13.3 Asymmetric Encryption Systems — Rabin

- The RSAP is not computationally equivalent to the IFP
- This means that it may be possible to break RSA without solving the IFP (this may be worrisome)
- Since the beginning of public key cryptography, people have been looking for cryptosystems that are computationally equivalent to a hard problem, such as the IFP
- Michael Rabin was the first researcher who proposed such a system in 1979
- It is based on the Square family of trapdoor permutations and yields an asymmetric encryption system and a DSS

### 13.3 Asymmetric Encryption Systems — Rabin

System parameters: —

| Generate                                                   | Encrypt           | Decrypt                                                                 |
|------------------------------------------------------------|-------------------|-------------------------------------------------------------------------|
| $(1^l)$                                                    | $(n, m)$          | $((p, q), c)$                                                           |
| $p, q \xleftarrow{r} \mathbb{P}'_{l/2}$<br>$n = p \cdot q$ | $c = m^2 \bmod n$ | $m_1, m_2, m_3, m_4 = c^{1/2} \bmod n$<br>Determine correct value $m_i$ |
| $(n, (p, q))$                                              | $(c)$             | $(m_i)$                                                                 |

$\mathbb{P}'_{l/2}$  refers to the set of all  $l/2$ -bit primes that are equivalent to 3 modulo 4 (so  $n$  is an  $l$ -bit Blum integer)

# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — Rabin

- Toy example
  - The Generate algorithm selects  $p = 11$  and  $q = 23$  (both primes are equivalent to 3 modulo 4), and computes  $n = 11 \cdot 23 = 253$
  - 253 is the public key, whereas  $(11, 23)$  is the private key
  - To encrypt  $m = 158$ , the Encrypt algorithm computes  $c = 158^2 \bmod 253 = 170$
  - This value is transmitted to the recipient
  - To decrypt  $c = 170$ , the Decrypt algorithm first computes the square roots 26, 227, 95, and 158, and then decides that 158 is the correct value (e.g., using redundancy)

# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — Rabin

- Under the intractability assumption of the IFP, the Rabin asymmetric encryption system is one-way secure

### Theorem (Security of Rabin)

*Breaking the one-way security of the Rabin asymmetric encryption system is computationally equivalent to solving the IFP*

- If one uses redundancy to defeat the ambiguity in decryption, then the proof does no longer apply
- Consequently, one has to choose between practicability or (provable) one-way security



# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — Elgamal

- Public key cryptography started in the 1970s with the publication of the Diffie-Hellman key exchange
- In 1984, Taher Elgamal found a way to turn the Diffie-Hellman key exchange into a public key cryptosystem
- It yields an asymmetric encryption system and a DSS
- It can be defined in any cyclic group  $G$  in which the DLP is assumed to be intractable, such as
  - $\mathbb{Z}_p^*$
  - $q$ -order subgroup of  $\mathbb{Z}_p^*$  (generated by  $g$ )
  - group of points on an elliptic curve over a finite field

# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — Elgamal

**Table 13.4**  
Elgamal Asymmetric Encryption System

System parameters:  $G, g$

| Generate                        | Encrypt                         | Decrypt           |
|---------------------------------|---------------------------------|-------------------|
| $(-)$                           | $(m, y)$                        | $((c_1, c_2), x)$ |
| $x \xleftarrow{r} \mathbb{Z}_q$ | $r \xleftarrow{r} \mathbb{Z}_q$ | $K = c_1^x$       |
| $y = g^x$                       | $K = y^r$                       | $m = c_2 / K$     |
| $(x, y)$                        | $c_1 = g^r$                     | $(m)$             |
|                                 | $c_2 = Km$                      |                   |
|                                 | $(c_1, c_2)$                    |                   |

# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — Elgamal

- Toy example
  - For  $G = \mathbb{Z}_{17}^*$  and  $g = 7$  ( $q = 16$ ), the Generate algorithm may select  $x = 6$  and compute  $y = 7^6 \bmod 17 = 9$
  - 9 is the public key, whereas 6 is the private key
  - To encrypt  $m = 7$ , the Encrypt algorithm may select  $r = 3$ , compute  $K = 9^3 \bmod 17 = 15$ , and conclude with  $c_1 = 7^3 \bmod 17 = 3$  and  $c_2 = (15 \cdot 7) \bmod 17 = 3$
  - The ciphertext (3,3) is transmitted to the recipient
  - The Decrypt algorithm first computes  $K = 3^6 \bmod 17 = 15$ , and then solves  $15m \equiv 3 \pmod{17}$  for  $m$
  - The result is  $m = 7$  (because  $15 \cdot 7 = 105 \bmod 17 = 3$ )

# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — Elgamal

- Under the intractability assumption of the (computational) DHP, the Elgamal asymmetric encryption system is one-way secure
- Because its encryption algorithm is probabilistic, the Elgamal asymmetric encryption system can provide IND-CPA and is semantically secure under the DDHP intractability assumption

### Theorem (Security of Elgamal)

*If the DDHP is hard, then the Elgamal asymmetric encryption system provides IND-CPA and is semantically secure*

### 13.3 Asymmetric Encryption Systems — Elgamal

- The Elgamal asymmetric encryption system provides IND-CPA and is semantically secure
- But it is multiplicatively homomorphic, and hence highly malleable
- If one is given a ciphertext of some (unknown) plaintext message  $m$ , then one can easily construct a ciphertext for  $2m$
- Consequently, the Elgamal asymmetric encryption system cannot provide IND-CCA or NM-CCA
- The Cramer-Shoup variant (1998) can be used instead

# 13. Asymmetric Encryption

## 13.3 Asymmetric Encryption Systems — Elgamal

**Table 13.5**  
Cramer-Shoup Asymmetric Encryption System

System parameters:  $G, g_1, g_2$

| Generate                                                                                                                                                                                  | Encrypt                                                                                                                                                                                | Decrypt                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| $(-)$ <hr/> $x_1, x_2, y_1, y_2, z \xleftarrow{r} \mathbb{Z}_q^5$<br>$c = g_1^{x_1} g_2^{x_2}$<br>$d = g_1^{y_1} g_2^{y_2}$<br>$e = g_1^z$ <hr/> $(x_1, x_2, y_1, y_2, z)$<br>$(c, d, e)$ | $(m, (c, d, e))$ <hr/> $r \xleftarrow{r} \mathbb{Z}_q$<br>$u_1 = g_1^r$<br>$u_2 = g_2^r$<br>$v = e^r m$<br>$\alpha = h(u_1, u_2, v)$<br>$w = c^r d^{r\alpha}$ <hr/> $(u_1, u_2, v, w)$ | $((u_1, u_2, v, w), (x_1, x_2, y_1, y_2, z))$ <hr/> $\alpha = h(u_1, u_2, v)$<br>If $w = u_1^{x_1 + \alpha y_1} u_2^{x_2 + \alpha y_2}$<br>then return $m = w / u_1^z$<br>else return "reject" <hr/> $(m \text{ or "reject"})$ |

## 13.4 Identity-Based Encryption

- In an asymmetric encryption system, every user has a public key pair, and the keys look arbitrary and random
- One thus faces the problem that one cannot easily attribute a public key to a particular entity (e.g., user) and that one has to work with public key certificates
- A public key certificate is a data structure that is issued by a trusted certification authority (CA)
- If there are multiple CAs in place, then one usually talks about public key infrastructures (PKIs)
- The implementation of a PKI has turned out to be more difficult than originally anticipated

## 13.4 Identity-Based Encryption

- In the early 1980s, Shamir came up with an alternative idea
- If one chooses a public key to uniquely identify its holder, then one no longer has to care about public key certification
- Shamir coined the term **identity-based cryptography** to refer to this idea
  - The advantages are related to the avoidance of public key certificates and respective key directory services.
  - The most important disadvantages are related to the necessity of having a unique naming scheme and the fact that a trusted authority is needed to generate the public key pairs and distribute them to the entities




# 13. Asymmetric Encryption

## 13.4 Identity-Based Encryption

- In his original publication, Shamir introduced the notion of identity-based cryptography and proposed a DSS
- In 2001, Dan Boneh and Matthew K. Franklin proposed an **identity-based encryption (IBE)** system based on bilinear maps (pairings) on elliptic curves
- In the same year, Clifford Cocks proposed an IBE system based on the QRP (less practical)
- In summary, IBE is a nice idea in theory, but it has not been adopted in practice

## 13.5 Fully Homomorphic Encryption

- 

## 13.5 Fully Homomorphic Encryption

- Homomorphic encryption is about encrypting data in a way that allows computations to be done only on the ciphertexts (i.e., without decryption)
- More specifically, if  $\odot$  is a computation on  $m_1$  and  $m_2$  and  $E$  is a homomorphic encryption function, then there is another computation  $\otimes$  (that can also be the same) for which  $E(m_1 \odot m_2) = E(m_1) \otimes E(m_2)$  holds
- This means that one can compute  $E(m_1 \odot m_2)$  even if one only knows  $E(m_1)$  and  $E(m_2)$

## 13.5 Fully Homomorphic Encryption

- Many asymmetric encryption systems in use today are partially homomorphic
- For example, RSA and Elgamal are both multiplicatively homomorphic
- Similarly, the Paillier system is additively homomorphic
- For three decades, it was not clear whether **fully homomorphic encryption (FHE)**, in which both addition and multiplication are supported, is feasible at all

## 13.5 Fully Homomorphic Encryption

- In 2009, Craig Gentry solved the problem and proposed a FHE system using lattice-based cryptography
- Gentry's proposal is a major theoretical breakthrough, but it is impractical for real-world applications
- Since then, many researchers are working on FHE systems that are more practical
- FHE is sometimes claimed to be the holy grail for secure cloud computing

## 13.6 Final Remarks

- ◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ ↺ 🔍 ↻

# 13. Asymmetric Encryption

## 13.6 Final Remarks

- There are many other asymmetric encryption systems that have been developed and proposed in the literature
- Some of these systems have been broken and become obsolete
- For example, the **NP**-complete subset sum problem has served as a basis for many public key cryptosystems
- All knapsack-based public key cryptosystems (including the Chor-Rivest knapsack cryptosystem) have been broken
- It is thus necessary but not sufficient that a public key cryptosystem is based on a mathematically hard problem

# 13. Asymmetric Encryption

## 13.6 Final Remarks

- There are a few systems that have turned out to be resistant against all types of attacks
- In 1978, Robert McEliece proposed an asymmetric encryption system back that has remained secure
- The respective McEliece asymmetric encryption system was the first to use randomization in the encryption process
- Due to its relative inefficiency and use of large keys, the system has never gained widespread use
- This is about to change, because Classic McEliece is a finalist in the NIST PQC competition



# Questions and Answers



