Homework 13
COMP543 Fall 2020 - Modern Cryptography

Erhan Tezcan 0070881

01.01.2021

1. Quesitons

Q1: Perform research on the subgroup decision problem and relate to the topics that you have just read.

A1: The answer is given below:

Definition 1.1 (Subgroup Decision Problem)**.** *Let $x \in G$ be an element of group G of order $\phi(G) = N = pq$. G_p and G_q are prime order subgroups of order p and q respectively. How can we prove that $x^q \in G_p$?*

Q2: What is the advantage of the Rabin Encryption Scheme over the RSA Encryption Scheme? What is the advantage of the RSA Encryption Scheme over the Rabin Encryption Scheme?

A2:

- The hardness of Rabin is equivalent to hardness of factoring, whereas the hardness of RSA is not implied by the hardness of factoring.
- Using large exponents in RSA makes it slightly slower compared to Rabin.
- The plain RSA and plain Rabin are both insecure against CCA, however RSA reveals the message on that attack whereas Rabin reveals the private key.
- Rabin permutation is over a subset of $\mathbb{Z}_N^*$, while RSA is a permutation over the whole $\mathbb{Z}_N^*$.

Q3: Provide examples of homomorphic encryption schemes. Research on the definitions of semi-homomorphic, fully-homomorphic, somewhat-homomorphic encryption schemes. (Do not try to understand the details of how they work. Just understand what they are capable of.)

A3: Homomorphic encryption schemes allow computations over the encrypted data without access to the secret key. The result of the computations remain encrypted too! The name comes from thinking about the encryption and decryption functions as homomorphisms among message spaces and ciphertext spaces. The homomorphism levels are (from weakest to strongest):

(1) **Partially Homomorphic Encryption** supports evaluation of circuits consisting of only one type of operation (e.g. addition or multiplication).
(2) **Somewhat Homomorphic Encryption** supports evaluation of two types of operations on a subset of circuits.
(3) **Leveled Fully Homomorphic Encryption** supports evaluation of arbitrary circuits of bounded depth.
(4) **Fully Homomorphic Encryption** supports evaluation of arbitrary circuits of unbounded depth.

Some examples are:

- **Pallier Encryption** is homomorphic with $pk = N, \mathbb{M} = \mathbb{Z}_N, \mathbb{C} = \mathbb{Z}^*_{N^2}$.

$$Enc(m_1) \cdot Enc(m_2) = (g^{m_1} r_1^n)(g^{m_2} r_2^n) \bmod n^2 = g^{m_1+m_2}(r_1 r_2)^n \bmod n^2 = Enc(m_1+m_2)$$

- **RSA Encryption** is actually homomorphic when you dont do padding (Unpadded RSA).

$$Enc(m_1) \cdot Enc(m_2) = m_1^e m_2^e \bmod n = (m_1 m_2)^e \bmod n = Enc(m_1 \cdot m_2)$$

- **Goldwasser-Micali Encryption** is homomorphic with $\mathbb{M} = \{0,1\} = \mathbb{Z}_2$.

$$Enc(b_1) \cdot Enc(b_2) = x^{b_1} r_1^2 x^{b_2} r_2^2 \bmod n = x^{b_1+b_2}(r_1 r_2)^2 \bmod n = Enc(b_1 \oplus b_2)$$

- **ElGamal Encryption** is homomorphic with $pk = \langle G, q, g, h \rangle, \mathbb{M} = G, \mathbb{C} = G \times G$.

$$Enc(m_1) \cdot Enc(m_2) = (g^{r_1}, m_1 \cdot h^{r_1})(g^{r_2}, m_2 \cdot h^{r_2}) = (g^{r_1+r_2}, (m_1 \cdot m_2) h^{r_1+r_2}) = Enc(m_1 \cdot m_2)$$