ETH Zürich, D-INFK
Spring 2019

Prof. Ueli Maurer
Fabio Banfi
Daniel Jost
Jiamin Zhu

Cryptography Foundations

Exercise 4

4.1 The ElGamal Public-Key Cryptosystem

Goal*: The ElGamal public-key cryptosystem uses the Diffie-Hellmann protocol to build a PKE scheme. We prove that this scheme is IND-CPA secure.*

The Diffie-Hellman protocol can be used as a PKE scheme, as discussed in the lecture. In this task we consider one such scheme, the well-known ElGamal public-key cryptosystem. Let $G = \langle g \rangle$ be fixed and $q = |G|$ be publicly known. The ElGamal scheme then works as follows:

Key generation: Choose x_B uniformly at random from $\mathbb{Z}_q$. The secret key is x_B, the public key is $y_B := g^{x_B}$.

Encryption: On input a message $m \in G$, choose $x \in \mathbb{Z}_q$ uniformly at random. The ciphertext for a message $m \in G$ is the pair $(g^x, m \cdot y_B^x)$.

a) Describe the decryption of the ElGamal scheme, i.e., show how to obtain the message m given $(g^x, m \cdot y_B^x)$ and the secret key x_B.

b) Show that the ElGamal cryptosystem is IND-CPA secure under the DDH-assumption. More precisely, given a distinguisher D for the IND-CPA bit-guessing problem for public-key encryption $[\![S^{\textsf{pke-cpa}}; B]\!]$, design a new distinguisher D' for $\langle \mathsf{DDH}^0 \mid \mathsf{DDH}^1 \rangle$ such that

$$\Lambda^D([\![S^{\textsf{pke-cpa}}; B]\!]) = 2 \cdot \Delta^{D'}(\mathsf{DDH}^0, \mathsf{DDH}^1).$$

4.2 On the (In)security of RSA

Goal*: We discuss attacks on the naïve version of the RSA cryptosystem and prove a related reduction.*

a) Consider the naïve RSA public-key cryptosystem (Figure 2.12 in the lecture notes). This cyrptosystem is deterministic and therefore, as discussed in the lecture, given a ciphertext c an eavesdropper can test whether c encrypts a message from any given small set. Show that in the case of the naïve RSA cryptosystem with $e = 3$ in Bob's public key, there even exists a "large" subset of the message space such that an eavesdropper can recover any message of this set from a corresponding ciphertext and the public key more directly.

b) We now show that any message from the message space can be recovered by an eavesdropper, if this message is sent to three different users who all use the exponent $e = 3$. More precisely, consider the naïve RSA public-key cryptosystem with three different users, who have distinct moduli n_1, n_2, n_3, but all use the exponent $e = 3$. Assume some message m is encrypted for these users and an attacker observes the resulting ciphertexts. Show how the attacker can efficiently compute m from these ciphertexts and the public keys.

c) It is clear that one can efficiently compute $\varphi(n)$ from a factorization of n (and thus compute the private exponent d and therefore decrypt all messages). Show that conversely, computing $\varphi(n)$ is as hard as factoring n,[1] i.e., show that given n and $\varphi(n)$, one can efficiently find the two prime factors of n.

[1]Note that this does not exclude computing the e-th root (decrypting) to be easier than computing $\varphi(n)$.

4.3 Homomorphic Public-Key Encryption

Goal: *We discuss encryption schemes with a homomorphic property and their limitations and use-cases.*

Let (E, d) denote the pair consisting of the encryption function E and the decryption function d of a public-key encryption scheme. We assume that the message space is identified with a finite abelian group $\langle \mathbb{G}; \circ \rangle$ (with $|\mathbb{G}| \geq 3$).

(E, d) is said to be *homomorphic* if for all key pairs $(pk, sk) \in \mathcal{P} \times \mathcal{S}$ in the support of the key-pair distribution, given two ciphertexts $c_1 := E(m_1, pk)$ and $c_2 := E(m_2, pk)$, one can efficiently compute a valid ciphertext c (with respect to the same public key pk) for the message $m' := m_1 \circ m_2$. This means that c is such that $d(c, sk) = m_1 \circ m_2$ (and in particular no secret key is required to obtain such a c).

a) Show that the ElGamal cryptosystem is homomorphic.

b) Show that the naïve RSA cryptosystem is homomorphic.

c) Assume a homomorphic encryption scheme (E, d). Show a concrete attacker for the CCA bit-guessing problem that guesses the bit correctly with probability 1.

d) Describe in words an application scenario that makes reasonable use of a homomorphic encryption scheme (note that being homomorphic does not exclude CPA security, as the ElGamal system shows).

4.4 The Rabin Trapdoor One-Way Permutation

Goal: *We present a trapdoor one-way permutation provably based on the hardness of factoring.*

A quadratic residue modulo an integer n is an integer x such that there exists an integer y with $y^2 \equiv x \pmod{n}$. We write $\mathcal{QR}_n = \{x^2 \mid x \in \mathbb{Z}_n^*\}$ for the set of quadratic residues in $\mathbb{Z}_n^*$.

a) Let $p > 2$ be a prime. Show that half of the elements in $\mathbb{Z}_p^*$ are quadratic residues, i.e., show that $|\mathcal{QR}_p| = \frac{1}{2}|\mathbb{Z}_p^*|$.

Hint: Show that $x \mapsto x^2 \colon \mathbb{Z}_p^* \to \mathcal{QR}_p$ is a 2-to-1 mapping.

b) Now let p be a prime such that $p \equiv 3 \pmod{4}$. Describe an efficient algorithm that, given $x \in \mathcal{QR}_p$ and p, computes $y \in \mathcal{QR}_p$ such that $y^2 \equiv x \pmod{p}$.

Hint: To show that your y lies in $\mathcal{QR}_p$ (and not just in $\mathbb{Z}_p^*$), show that $\mathcal{QR}_p$ is a subgroup of $\mathbb{Z}_p^*$.

In the following, let p, q two primes such that $p \equiv q \equiv 3 \pmod{4}$, and let $n = pq$.

c) Show that $\frac{1}{4}$ of the elements in $\mathbb{Z}_n^*$ are quadratic residues modulo n.

Hint: Use the Chinese remainder theorem.

d) Show that the function $f \colon x \mapsto x^2 \bmod n$ is a trapdoor permutation on $\mathcal{QR}_n$. That is, show that it is a permutation and give an efficient algorithm that computes the inverse of f when the prime factors p and q of n are known.

e) Show that the permutation f of **d)** is one-way assuming that factoring is hard. That is, show that if you have an algorithm that inverts the permutation with probability $\alpha > 0$ for uniformly chosen inputs x, then you can factor n with probability $1 - \varepsilon$ for every $\varepsilon > 0$ (where the efficiency of the factoring algorithm depends on ε and α).

Hint: Consider the equation $x^2 - y^2 = kn$.