ETH Zürich, D-INFK
Spring 2018

Prof. Ueli Maurer
Christian Badertscher
Fabio Banfi

Cryptography Foundations
Solution Exercise 4

4.1 The (In)security of the ElGamal Public-Key Cryptosystem

a) A ciphertext $(y_A, c) = (g^x, m \cdot g^{x \cdot x_B})$ is decrypted with the secret key x_B as follows:

$$c \cdot ((y_A)^{x_B})^{-1} = (m \cdot g^{x \cdot x_B}) \cdot ((g^x)^{x_B})^{-1} = m.$$

b) Let R^{DDH} be the system that (when interacting with a distinguisher) outputs a triple (g^a, g^b, g^{ab}) for uniformly distributed $a, b \in \mathbb{Z}_q$, S^{DDH} the system that outputs (g^a, g^b, g^c) for uniformly distributed $a, b, c \in \mathbb{Z}_q$, and S^{ind} the system implementing the IND-CPA game for the ElGamal encryption scheme.

From a distinguisher D for the bit-guessing problem $(S^{\mathsf{ind}}, \beta)$, we construct a distinguisher D' for the problem of distinguishing R^{DDH} and S^{DDH}. Upon obtaining a triple (A, B, C), D' first sends B to D as the public key. When D submits two challenge messages m_0 and m_1, D' chooses a bit β uniformly at random and sends $(A, m_\beta \cdot C)$ to D. When D issues a bit Z, D' outputs the bit $Z' := Z \oplus \beta$.

Note that when D' interacts with R^{DDH}, it perfectly emulates S^{ind} towards D.

Assume D' interacts with S^{DDH}; in this case, (A, B, C) are uniform and independent, and therefore $m_\beta \cdot C$ is distributed uniformly by Exercise 1.2. Moreover, A, B, and $m_\beta \cdot C$ are independent since

$$\begin{aligned}\Pr[A = x \wedge B = y \wedge m_\beta \cdot C = z] &= \Pr[A = x \wedge B = y \wedge C = m_\beta^{-1} \cdot z] \\ &= \Pr[A = x] \cdot \Pr[B = y] \cdot \Pr[C = m_\beta^{-1} \cdot z] \\ &= \Pr[A = x] \cdot \Pr[B = y] \cdot \Pr[m_\beta \cdot C = z],\end{aligned}$$

and therefore the bit Z output by D in this case is statistically independent of β, and thus Z equals β with probability $\frac{1}{2}$.

Finally, for the advantage of D' we have:

$$\begin{aligned}\Delta^{D'}(R^{\mathsf{DDH}}, S^{\mathsf{DDH}}) &= \Pr^{D'S^{\mathsf{DDH}}}[Z' = 1] - \Pr^{D'R^{\mathsf{DDH}}}[Z' = 1] \\ &= \Pr^{D'S^{\mathsf{DDH}}}[\underbrace{Z \oplus \beta = 1}_{Z \neq \beta}] - \Pr^{D'R^{\mathsf{DDH}}}[\underbrace{Z \oplus \beta = 1}_{Z \neq \beta}] \\ &= \frac{1}{2} - (1 - \Pr^{DS^{\mathsf{ind}}}[Z = \beta]) \\ &= \Pr^{DS^{\mathsf{ind}}}[Z = \beta] - \frac{1}{2} \\ &= \frac{1}{2} \cdot \Lambda^D\big((S^{\mathsf{ind}}, \beta)\big).\end{aligned}$$

c) The following adversary wins the IND-CCA game with advantage 1:

1. Receive the public key $y_B = g^{x_B}$.

2. Choose arbitrary m_0, m_1 with $|m_0| = |m_1|$ and $m_0 \neq m_1$ and receive a ciphertext $(y_A, c) = (g^x, m_b \cdot g^{x \cdot x_B})$ for a uniform $b \in \{0, 1\}$.
3. Ask for a decryption m' of $(y'_A, c') \coloneqq (y_A \cdot g, c \cdot y_B)$.
4. Guess $b' = 0$ if $m' = m_0$ and $b' = 1$ otherwise.

Note that $(y'_A, c') \neq (y_A, c)$, so the query in step 3. is allowed. The challenger decrypts (y'_A, c') to

$$\begin{aligned} m' &= c' \cdot \left(\left(y'_A\right)^{x_B}\right)^{-1} \\ &= (c \cdot y_B) \cdot ((y_A \cdot g)^{x_B})^{-1} \\ &= (c \cdot g^{x_B}) \cdot ((g^x \cdot g)^{x_B})^{-1} \\ &= (m_b \cdot g^{x \cdot x_B} \cdot g^{x_B}) \cdot (g^{x \cdot x_B} \cdot g^{x_B})^{-1} \\ &= m_b. \end{aligned}$$

Thus the adversary always guesses correctly.

4.2 On the (In)security of RSA

a) Let $\mathcal{M}_0 \coloneqq \{m \in \mathbb{N} \mid m^3 < n\}$. For any message $m \in \mathcal{M}_0$, the corresponding ciphertext equals $c = m^e \bmod n = m^3$. Since m^3 is not reduced modulo n, one can efficiently compute $m = c^{1/3}$ over the integers using numerical methods and hence recover the message from the ciphertext.

b) If the n_i are not pairwise coprime, one can find a nontrivial factor of one of the n_i with the extended Euclidean algorithm and hence compute the corresponding secret key. With the secret key, the corresponding ciphertext c_i can be decrypted to find the message.

Now assume the n_i are pairwise coprime and the following ciphertexts are intercepted:

$$\begin{aligned} c_1 &\equiv m^3 \pmod{n_1}, \\ c_2 &\equiv m^3 \pmod{n_2}, \\ c_3 &\equiv m^3 \pmod{n_3}. \end{aligned}$$

Using the Chinese Remainder Theorem, one can efficiently compute

$$c \equiv m^3 \pmod{n_1 n_2 n_3}.$$

Since $m < n_i$ for $i = 1, 2, 3$, we have $m^3 < n_1 n_2 n_3$, so $c = m^3$ is not reduced. Therefore, one can again recover m by calculating the cubic root of c in the integers.

This attack is called *Håstad attack*. It analogously works for any $e > 3$ if the same message is encrypted with at least e different public keys.

c) We have $n = pq$ and $\varphi(n) = (p-1)(q-1) = pq - p - q + 1$. This implies $p = n - q + 1 - \varphi(n)$ and therefore $n = nq - q^2 + q - \varphi(n)q$. Since n and $\varphi(n)$ are known, this quadratic equation can be solved efficiently for q, which also yields p.

4.3 Homomorphic Public-Key Encryption

a) For the ElGamal cryptosystem we have that the message space is a finite abelian (and cyclic) group $\langle \mathbb{G}; \circ \rangle$ of order $q \coloneqq |\mathbb{G}|$ with generator g. The ciphertext space is $\mathbb{G}^2$, on which we define $\otimes$ as the elementwise extension of $\circ$ (that is we consider the product group, where for $a, b \in \mathbb{G}^2$ with $a \coloneqq (a_1, a_2)$ and $b \coloneqq (b_1, b_2)$, we define $a \otimes b \coloneqq (a_1 \circ b_1, a_2 \circ b_2)$).

For any fixed public key $y_B := g^{x_B} \in \mathbb{G}$ (where $x_B \in \mathbb{Z}_q$ is the private key) and arbitrary messages m_1, m_2, let the ciphertexts be $c_i := E(m_i, y_B) = (g^{x_i}, m_i \circ y_B^{x_i})$, where $i \in \{1, 2\}$ and $x_i \in \mathbb{Z}_q$ are uniformly distributed. For $c_1 \otimes c_2$ we obtain

$$\begin{aligned} c_1 \otimes c_2 &= (g^{x_1}, m_1 \circ y_B^{x_1}) \otimes (g^{x_2}, m_2 \circ y_B^{x_2}) \\ &= (g^{x_1} \circ g^{x_2}, m_1 \circ y_B^{x_1} \circ m_2 \circ y_B^{x_2}) \\ &= (g^{x_1+x_2}, (m_1 \circ m_2) \circ y_B^{x_1+x_2}) \end{aligned}$$

where the last step follows since we assumed the group to be abelian.

The last line corresponds to an encryption of $(m_1 \circ m_2)$ with the first element of the ciphertext having exponent $x := x_1 + x_2$. Therefore a valid encryption (with respect to the public key y_B) of $m_1 \circ m_2$ can be computed as $c_1 \otimes c_2$.

b) For the naïve RSA cryptosystem we have that both the message and ciphertext spaces are the finite multiplicative group $\mathbb{Z}_n^*$ of integers modulo $n := p \cdot q$ for p and q primes and with order $t := |\mathbb{Z}_n^*| = \varphi(n) = (p-1)(q-1)$.

For any fixed public key $e \in \mathbb{Z}_t^*$ (relative to some private key $d \in \mathbb{Z}_t^*$ such that $e \cdot d \equiv_t 1$) and arbitrary messages m_1, m_2, let the ciphertexts be $c_i := E(m_i, (n, e)) = [m_i^e]_n$ (for $i = 1, 2$ and where $[x]_n$ denotes the remainder of x when divided by n). We have:

$$\begin{aligned} c_1 \cdot c_2 &\equiv_n E(m_1, (n, e)) \cdot E(m_2, (n, e)) \\ &\equiv_n m_1^e \cdot m_2^e \\ &\equiv_n (m_1 \cdot m_2)^e \\ &\equiv_n E(m_1 \cdot m_2, (n, e)). \end{aligned}$$

Therefore the encryption of $[m_1 \cdot m_2]_n$ is computed as $[c_1 \cdot c_2]_n$.

c) Let $\langle \mathbb{G}; \circ \rangle$ be the group associated with the message space of (E, d). Due to the assumption of the exercise, we can assume the existence of an (efficiently computable) function γ that, given two encryptions c, c' of messages m, m' (with respect to pk), computes a valid encryption of $m \circ m'$ (with respect to pk).

Then the following distinguisher wins the CCA-game with probability 1: first, it chooses three messages m_0, m_1, m_2 that are (pairwise) different and m_2 not equal the neutral element. It first asks for the encryption of m_2, thus obtaining $c_2 := E(m_2, pk)$. Then it presents the challenge (m_0, m_1) to the challenger, thus obtaining $c := E(m_b, pk)$ for $b \in \{0, 1\}$ uniformly distributed. At this point the adversary can exploit the fact that (E, d) is homomorphic by computing $\widetilde{c} := \gamma(c, c_2)$, which is a valid encryption of $m_b \circ m_2$ relative to the public key pk.

Due to correctness of the encryption scheme, $\widetilde{c} \neq c$ and hence asking for the decryption of $\widetilde{c}$ is an allowed query to the decryption oracle. The decryption of $\widetilde{c}$ yields $m' := m_b \circ m_2$ and computing $m' \circ (m_2)^{-1} = m_b$ completely recovers m_b. This is sufficient to win the CCA game with probability 1.

d) There are two important use-cases for homomorphic encryption schemes.

- In electronic voting schemes, the homomorphic property can be used to count the votes. In a 0/1-vote (i.e., yes/no-votes without abstentions) for example, one could compute the sum of all encrypted votes without the need to decrypt each vote. This protects *voter privacy*. Only the final result will be decrypted in the end. Note that to make such a procedure sound, several other techniques are needed in combination, as treated for example in the lecture on *Cryptographic Protocols*. Homomorphic encryption is just one helpful tool to achieve the goal of a secure voting protocols.

- Assume a client wants to outsource a specific computation to a server. The server is trusted not to tamper with the data, but the client might be afraid that the data he sends to the server could leak to an intruder. So, the client sends his encrypted inputs for the computation to the server and the server then performs all operations on the respective ciphertexts. Thanks to the homomorphic property, this will translate to operations performed on plaintexts. The server returns the encrypted result and the client simply needs to decrypt the returned value to obtain the result of the computation. Note that for this to be even more powerful, one might need an encryption scheme that is homomorphic with respect to ring operations, such as addition and multiplication simultaneously. This topic however, which is typically referred to as *fully homomorphic encryption*, will not be of primary interest in this lecture.

4.4 The Rabin Trapdoor One-Way Permutation

a) The quadratic residues (modulo 35) in $\mathbb{Z}_{35}$ are

$$0, 1, 4, 9, 11, 14, 15, 16, 21, 25, 29, 30.$$

b) Recall the Chinese remainder theorem: The map $\phi\colon \mathbb{Z}_n \to \mathbb{Z}_p \times \mathbb{Z}_q$ given by

$$\phi(x) = (x \bmod p, x \bmod q)$$

is an isomorphism of rings. Concretely, ϕ is a bijection that is compatible with addition and multiplication so that

$$\begin{aligned}\phi(x+y) &= ((x+y) \bmod p, (x+y) \bmod q)\\ &= (x \bmod p, x \bmod q) + (y \bmod p, y \bmod q) = \phi(x) + \phi(y),\\ \phi(xy) &= (xy \bmod p, xy \bmod q)\\ &= (x \bmod p, x \bmod q)(y \bmod p, y \bmod q) = \phi(x)\phi(y).\end{aligned}$$

We say that $\mathbb{Z}_n$ is (canonically) isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_q$ and write $\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q$. It follows that an element $x \in \mathbb{Z}_n$ is a unit, which means that x has a multiplicative inverse, $x \in \mathbb{Z}_n^*$, if and only if the corresponding elements $x \bmod p$ and $x \bmod q$ are units in $\mathbb{Z}_p$ and $\mathbb{Z}_q$, respectively. Therefore, the restriction of ϕ to $\mathbb{Z}_n^*$ gives an isomorphism $\mathbb{Z}_n^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Similarly, $x \in \mathbb{Z}_n^*$ is a quadratic residue modulo n if and only if $x \bmod p$ and $x \bmod q$ are quadratic residues modulo p and q. We write $QR_n = \{x^2 \mid x \in \mathbb{Z}_n^*\}$ for the quadratic residues in $\mathbb{Z}_n^*$, which is a subgroup of $\mathbb{Z}_n^*$. Then, $QR_n \cong QR_p \times QR_q$. Counting the quadratic residues in $\mathbb{Z}_n^*$ is thus reduced to counting the quadratic residues in $\mathbb{Z}_p^*$ and the quadratic residues in $\mathbb{Z}_q^*$. Consider the map

$$x \mapsto x^2\colon \mathbb{Z}_p^* \to QR_p. \tag{1}$$

It is clearly surjective. Moreover for every x, $-x$ is mapped to the same quadratic residue $x^2 = (-x)^2$ and $-x \neq x$ because otherwise $2x \equiv 0 \pmod p$, which would imply that p divides 2. On the other hand, from $x^2 = (x')^2$ it follows that $(x'x^{-1})^2 = 1$. The latter implies that $x'x^{-1} = \pm 1 \Leftrightarrow x' = \pm x$ as the polynomial $X^2 - 1 = (X+1)(X-1)$ only has the two roots ± 1. We thus have established that the map (1) is 2-to-1 and that the number of quadratic residues in $\mathbb{Z}_p^*$ is $\frac{1}{2}$ of the number of elements in $\mathbb{Z}_p^*$, i.e. $|QR_p| = \frac{p-1}{2}$. With the same argument we get that there are $\frac{q-1}{2}$ quadratic residues in $\mathbb{Z}_q^*$. Finally, we see that there are $\frac{p-1}{2}\frac{q-1}{2}$ quadratic residues in $\mathbb{Z}_n^*$, which are $\frac{1}{4}$ of its elements.

c) Observe that $p+1 \equiv 0 \pmod 4$ is divisible by 4 and set $z = x^{\frac{p+1}{4}}$. As x is a quadratic residue modulo p we have an integer y such that $y^2 \equiv x \pmod p$. We find

$$z^2 \equiv x^{\frac{p+1}{2}} \equiv x^{\frac{p-1}{2}} x \equiv (y^2)^{\frac{p-1}{2}} x \equiv y^{p-1} x \equiv x \pmod p,$$

where we have used that the order of y modulo p must divide $p-1$ so that $y^{p-1} \equiv 1 \pmod p$. Hence, z is a square root of x modulo p.

d) From **b)** we know that every $y \in QR_n \cong QR_p \times QR_q$ has exactly 4 different square roots in $\mathbb{Z}_n^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$. We need to show that one of them is in QR_n. Then the map $f\colon QR_n \to QR_n$ on the exercise sheet is surjective and thus also injective, as QR_n is finite. That is, f is a permutation. We do this by giving an efficient algorithm that computes such a square root of y. From **c)** we know how to compute square roots modulo p and q. Let $a = y^{\frac{p+1}{4}} \bmod p$ and $b = y^{\frac{q+1}{4}} \bmod q$. Then, $(a,b) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ is a square root of $\phi(y) = (y \bmod p, y \bmod q) \in QR_p \times QR_q$. But in fact, $(a,b) \in QR_p \times QR_q \cong QR_n$ because QR_p and QR_q are groups and a, b are powers of elements in QR_p and QR_q, respectively. We can also see this directly by observing that the $\frac{p+1}{4}$-th power of a square root modulo p of y will be a square root modulo p of a. In summary, the inverse $f^{-1}\colon QR_n \to QR_n$ is given by

$$f^{-1}(y) = \phi^{-1}\left(y^{\frac{p+1}{4}} \bmod p, y^{\frac{q+1}{4}} \bmod q\right)$$

and is efficiently computable if p and q are known.

e) The idea here is to find two square roots x, y modulo n of $z = f(x) = x^2$ such that $x \not\equiv \pm y \pmod n$. Then $x^2 - y^2 = (x+y)(x-y) \equiv 0 \pmod n$ and it follows that $\gcd(x-y, n)$ is one of the prime divisors of n. Let A be the algorithm from the exercise sheet that inverts f with probability α. We choose a uniformly distributed $x \in \mathbb{Z}_n^*$ and run $A(x^2)$. We show that this yields a y as above with probability $\frac{1}{2}\alpha$.

Let X be a uniformly distributed random variable over $\mathbb{Z}_n^*$. Then, $Z = X^2$ is uniformly distributed over QR_n since $x \mapsto x^2\colon \mathbb{Z}_n^* \to QR_n$ is 4-to-1. Z remains uniformly distributed when we condition on $\pm X \notin QR_n$ as $x \mapsto x^2\colon \mathbb{Z}_n^* \setminus \pm QR_n \to QR_n$ is 2-to-1. So if $Y = A(Z) = A(X^2)$, then

$$\Pr(Y \in QR_n \wedge Y^2 \equiv X^2) = \alpha.$$

With the help of A we succeed in factoring n with probability

$$\begin{aligned}
&\Pr(Y \in \mathbb{Z}_n^* \wedge Y \not\equiv \pm X \wedge Y^2 \equiv X^2) \\
&\quad \geq \frac{1}{2} \Pr(Y \in \mathbb{Z}_n^* \wedge Y \not\equiv \pm X \wedge Y^2 \equiv X^2 \mid \pm X \notin QR_n) \\
&\quad \geq \frac{1}{2} \Pr(Y \in QR_n \wedge Y^2 \equiv Z \mid \pm X \notin QR_n) \\
&\quad = \frac{1}{2} \Pr(Y \in QR_n \wedge Y^2 \equiv Z) \\
&\quad = \frac{1}{2}\alpha,
\end{aligned}$$

where we used in the second step that $Y \in QR_n$ and $\pm X \notin QR_n$ implies that $Y \in \mathbb{Z}_n^* \wedge Y \not\equiv \pm X \pmod n$.

The success probability can be amplified as follows. The probability that we succeed in finding a prime divisor of n with k independent runs of our algorithm is equal to $1 - (1 - \frac{1}{2}\alpha)^k$. This can be made arbitrarily close to 1 for sufficiently large k.