Univ.Prof. Dr. Dominique Schröder
Paul Gerhart
Version: 14. November 2024

Exercise: Privacy Enhancing Technologies (B.Sc.)

Theoretical Deepening

1 Security of El Gamal

In this exercise, we will prove the security of El Gamal using a security Reduction. I.e., we will prove Theorem 1. For your convenience, we depict the construction for El Gamal Encryption in Figure 1, and both the security game for public-key CPA security and the game for the DDH problem in Figure 2. In addition, you can assume that Lemma 1.1 holds *without* proving it. After the exercise class, we will provide proof for both Lemma 1.1 and Theorem 1.

$\mathsf{KGen}(\lambda)$	$\mathsf{Enc}(\mathsf{pk}, m)$	$\mathsf{Dec}(\mathsf{sk}, (c_1, c_2))$
1 : $\mathsf{sk} \leftarrow\!\!\$\ \mathbb{Z}_p$	1 : $r \leftarrow\!\!\$\ \mathbb{Z}_p$	1 : $m = c_2 / c_1^{\mathsf{sk}}$
2 : $\mathsf{pk} \leftarrow g^{\mathsf{sk}}$	2 : $c_1 \leftarrow g^r$	2 : **return** m
3 : **return** $(\mathsf{sk}, \mathsf{pk})$	3 : $c_2 \leftarrow \mathsf{pk}^r \cdot m$	
	4 : **return** (c_1, c_2)	

Figure 1: ElGamal public-key encryption scheme.

Theorem 1. *If the DDH problem is hard relative to $\mathbb{G}$, then the El Gamal encryption scheme is CPA secure.*

Lemma 1.1. *Let $\mathbb{G}$ be a finite group, and let $m \in \mathbb{G}$ be arbitrary. Then choosing uniform $k \leftarrow\!\!\$\ \mathbb{G}$ and setting $k' := k \cdot m$ results in the same distribution for k' as choosing uniform $k' \leftarrow\!\!\$\ \mathbb{G}$. Put differently, for any $g'' \in \mathbb{G}$ we have*

$$\Pr[k \cdot m = g''] = \frac{1}{|\mathbb{G}|},$$

where the probability is taken over the uniform choice of k.

Exercise 1. *Prove Theorem 1 using a security reduction from the CPA security of El Gamal to the hardness of DDH.*

$\mathsf{PubK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(\lambda)$	$\mathsf{DDH}_{\mathcal{A},\mathsf{GGen}}(\lambda)$
1 : $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\lambda)$	1 : $(\mathbb{G}, [1], q) \leftarrow \mathsf{GGen}(1^\lambda)$
2 : $(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk}), \quad \lvert m_0\rvert = \lvert m_1\rvert$	2 : $x, y, z_1 \leftarrow\!\!\$\ \mathbb{Z}_q$
3 : $b \leftarrow\!\!\$\ \{0,1\}$	3 : $z_0 := xy$
4 : $c_b \leftarrow \mathsf{Enc}(\mathsf{pk}, m_b)$	4 : $b \leftarrow\!\!\$\ \{0,1\}$
5 : $b' \leftarrow \mathcal{A}(c_b)$	5 : $b' \leftarrow \mathcal{A}(\mathbb{G}, q, [1], [x], [y], [z_b])$
6 : **if** $b' = b$	6 : **return** $(b = b')$
7 : **return** 1	
8 : **else return** 0	

Figure 2: Security game of CPA encryption and the DDH game.

Univ.Prof. Dr. Dominique Schröder
Paul Gerhart
Version: 14. November 2024

Exercise: Privacy Enhancing Technologies (B.Sc.)

Theoretical Deepening

2 Security of PRFs

In this exercise, we will prove the security of PRFs. For your convenience, we recall the definition of pseudorandom functions. Let $Func_n = \{f | f : \{0,1\}^n \to \{0,1\}^n\}$ be the set of all functions mapping n-bit strings to n-bit strings.

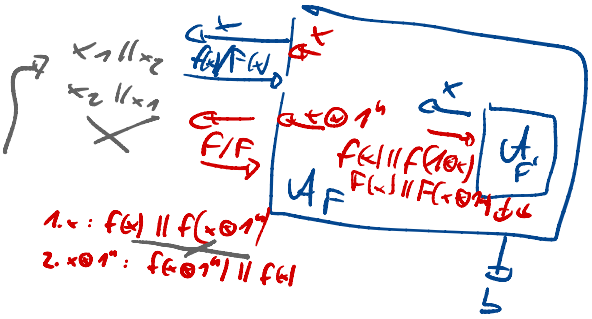
Definition 1 (Pseudorandom Functions)**.** Let $F : \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^n$ be an efficient, length-preserving, keyed function. F is a *pseudorandom function (PRF)* if for all PPT distinguishers D, there exists a negligible function negl such that

$$\left|\Pr\left[D^{F(k,\cdot)}(1^\lambda) = 1\right] - \Pr\left[D^{f(\cdot)}(1^\lambda) = 1\right]\right| \leq \mathsf{negl}(\lambda),$$

where the first probability is taken over uniform choice of $k \in \{0,1\}^\lambda$ and the randomness of D, and the second probability is taken over uniform choice of $f \in Func_n$ and the randomness of D.

Exercise 2. *Let F be a PRF. Prove or disprove that the following constructions are then also pseudorandom:*

1. $F'(k,x) := F(k, x \oplus 1^n)$
2. $F'(k,x) := F(k,x)||F(k, x \oplus 1^n)$
3. $F'(k, x_1||x_2) := F(k,x_1)||F(k,x_2)$
4. $F'(k,x) := F(k, 0||x)||F(k, 1||x)$



3 Mistakes in Proofs

In this exercise, we will examine common mistakes that arise when proofs are written unprecise. Let F be a PRF. We define $F'(k,x)$ via $F'(k,x) :=$ truncate last m bits of $F(k,x)$, $m < |F(k,x)|$.

Exercise 3. *We made the following approaches toward proving the security or the insecurity of F'. Which of these approaches is correct, and where is the mistake in the incorrect ones?*

1. F' is a PRF. We show this by reduction: Let's assume towards contradiction that there exists an adversary $\mathcal{A}$ that could distinguish F' from a random function with non-negligible probability. Then we construct an adversary $\mathcal{B}$ against F as follows: $\mathcal{B}$ invokes $\mathcal{A}$ and answers any query x by first computing $x' = trunc_m(x)$, asking x' to its own oracle and forwarding the answer to $\mathcal{A}$. Eventually, $\mathcal{A}$ outputs a bit b, which $\mathcal{B}$ also outputs. Obviously, $\mathcal{B}$ is efficient if $\mathcal{A}$ is. To analyze the success, consider the two cases: In the case where the oracle is F, $\mathcal{B}$ perfectly simulates F'. In the case where the oracle is a random function, $\mathcal{B}$ also simulates a random function, as f is obviously a random function. It follows, that $\mathcal{B}$ can distinguish whenever $\mathcal{A}$ can. As this would contradict the security of F, such an A cannot exist.

2. F' is a PRF. We show this by reduction: Let's assume towards contradiction that there exists an adversary $\mathcal{A}$ that could distinguish F' from a random function with non-negligible probability. Then we construct an adversary $\mathcal{B}$ against F as follows: $\mathcal{B}$ invokes $\mathcal{A}$ and

answers any query x by first computing $x' = trunc_m(x)$, asking x' to its own oracle and forwarding the answer to $\mathcal{A}$. Eventually, $\mathcal{A}$ outputs a bit b, which $\mathcal{B}$ also outputs. Obviously $\mathcal{B}$ is efficient if $\mathcal{A}$ is. To analyze the success, consider the two cases: In the case where the oracle is F, $\mathcal{B}$ perfectly simulates F'. In the case where the oracle is a random function, $\mathcal{B}$ also simulates a random function, as the simulation does not influence the distribution, it just switches one random function for another. It follows, that $\mathcal{B}$ can distinguish whenever $\mathcal{A}$ can. As this would contradict the security of F, such an $\mathcal{A}$ cannot exist.

3. F' is not a PRF: an adversary $\mathcal{A}$ queries $x||0$ and $x||1$. If $m \geq 1$, $\mathcal{A}$ receives the same output for both queries which would not be the case for a truly random function.