The art of cryptography, summer 2016

MICHAEL NÜSKEN

12. Exercise sheet
Hand in solutions until Monday, 11 July 2016, 11:59

Exercise 12.1 (Another game hopping). (12 points)

We select globally

- a group G with element g of order q and
- a function $\mathrm{prf}\colon \mathcal{K} \to \left\{\{0,1\}^* \to \{0,1\}^\ell\right\}$ with some specified set $\mathcal{K}$ of keys.

We now have the public parameters $\pi = ((G,g,q),\mathcal{K})$. Consider the following variant of ElGamal encryption:

- KeyGen$\colon \pi \mapsto (\mathrm{pk},\mathrm{sk})$:
  $a \xleftarrow{\$} \mathbb{Z}_q$, $k \xleftarrow{\$} \mathcal{K}$, $A \leftarrow g^a$. Return public key (A,k) and private key (a,k).
- Enc$\colon (\pi,\mathrm{pk},m) \mapsto c$:
  $t \xleftarrow{\$} \mathbb{Z}_q$, $T \leftarrow g^t$, $h \leftarrow \mathrm{prf}_k(A^t)$. Return $(T, h \oplus m)$.
- Dec$\colon (\pi,\mathrm{sk},c) \mapsto m'$:
  Parse $c = (T,c_1)$. Return $\mathrm{prf}_k(T^a) \oplus c_1$

The security game is $G^{\text{IND-POA}}$. Prove the following theorem and fix t', ε' in terms of t, ε. 12

Theorem. *If DDH of (G,g,q) is (t,ε)-secure and the function* prf *is (t,ε)-pseudo-random then the above encryption scheme is (t',ε')-IND-POA.*

Exercise 12.2 (Security of a re-encryption mixnet). (0+14 points)

We want to prove that the security of a re-encryption mixnet based on ElGamal can be reduced to the security of the underlying ElGamal encryption scheme. In other words: if we can break the anonymity of the mixnet then we can also break ElGamal encryption.

In the entire exercise we only consider a key-only attack, ie. the attacker only gets the setup.

We work in some (additively written) group G generated by an element P of order q, all this specified in the global setup. The receiver of the mixnet has the private key $a \in \mathbb{Z}_q$ which defines the public key $A = aP \in G$. We use $\mathrm{enc}_A(X,t) = (tP, tA + X)$ and $\mathrm{dec}_a(T,Y) = Y - aT$.

+1 (i) Check that $\mathrm{dec}_a \mathrm{enc}_A(X,t) = x$ if $A = aP$.

A mixnet consists of several servers, called mixes. Each mix obtains a sorted list of ciphertexts, the ordering on the ciphertexts is fixed somehow, eg. by lexicographical ordering as bitstrings. It reencrypts them and sorts the results. The security claim is: As long as at least two ciphertexts are involved and one server is uncompromomised the attacker cannot do any better than guesseing which output ciphertext corresponds to which input ciphertext.

The security game is this:

- The attacker $\mathcal{A}$ is given input and output of one particular mix, ie. a list of encrypted messages $(r_i P, r_i A + X_i)_{i\in I}$ and a re-encrypted and re-order list $(r'_i P, r'_i A + X_{\sigma(i)})_{i\in I}$ where σ is a permutation of I. The random coefficients r_i, r'_i and the permutation σ are unknown to the attacker.
- The attacker tries to determine $\sigma^{-1}(i_0)$ for some element $i_0 \in I$.

For simplicity, suppose that he can always do so.

The reducer, that is you, is given the setup (G, P) and three elements (A, rP, B) and tries to determine whether $B = rA$. The reducer is allowed to query the attacker and prepare the attacker's entire environment, ie. all its inputs, also those coming from oracles. You feed the attacker with

- the mix's input $c_0 = (rP, B + X)$, $c_1 = (r_1 P, r_1 A + X)$, and
- the mix's output $c'_0 = (\delta_0 P + rP, \delta_0 A + B + X)$, $c'_1 = (r'_1 P, r'_1 A + X)$.

+2 (ii) Argue that we can execute all operations in polynomial time. (Where a call to the attacker only counts as a single time unit.)

+2 (iii) Prove that the ciphertext c'_i is a re-encryption of ciphertext c_i. In other words, c_0 and c'_0 are both encryptions of $X + B - rA$, and c_1 and c'_1 are both encryptions of X.

+1 (iv) Decrypting c_0 we get $\mathrm{dec}_a(c_0) = B + X - rA$. Prove that this is equal to X if and only if $B = rA$.

+1 (v) Prove that if $B \neq rA$ the attacker will answer that $\sigma^{-1}(1) = 1$.

+1 (vi) Prove that if $B = rA$ the attacker can only guess and will answer $\sigma^{-1}(1) = 0$ or $\sigma^{-1}(1) = 1$ at random. (Assume that the attacker chooses uniformly if there is an ambiguity.)

Now, you play the above game twice (say), and answer "$B \neq rA$" if and only if the attacker answers $\sigma^{-1}(1) = 1$ in both queries.

+3 (vii) Prove that you give the correct answer with probability at least 75%.

+3 (viii*) Suppose that the attacker only succeeds with a considerable advantage over guessing, say prob($\mathcal{A}(\dots) =$ "$\sigma^{-1}(1) = 1$") $> \frac{3}{4}$. (Here, n is the security parameter, say the length q in bits, and c is some constant depending on $\mathcal{A}$ only.) Prove that you still answer correctly with probability at least $\frac{9}{16}$.

Refining all this leads to the theorem:

Theorem. *Assume that at least one mix of an ElGamal re-encryption mixnet is uncorrupted.*

If the decisional Diffie-Hellman problem is intractable, then the mixnet is (computationally) anonymous.

If ElGamal encryption is secure against a key-only attacker trying to distinguish the encryptions of (one of) two self-chosen plaintexts, then the mixnet is (computationally) anonymous.

Exercise 12.3 (Civitas). (0 points)

Study the Civitas election scheme as embedded in the course' notes.