

Esecurity: secure internet & e-voting, summer 2013

MICHAEL NÜSKEN

12. Exercise sheet

Hand in solutions until Monday, 8 July 2013, 08:00

Exercise 12.1 (Security of a re-encryption mixnet). (14+3 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.

Note that the security of the ElGamal encryption scheme is equivalent to the so-called decisional Diffie-Hellman problem for the underlying group G , which is given four elements $P, aP, bP, cP \in G$ decide whether $ab = c$.

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 $\text{enc}_A(X, t) = (tP, tA + X)$ and $\text{dec}_a(T, Y) = Y - aT$.

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

- The attacker \mathcal{A} is given input and output of one particular mix, ie. a list of encrypted messages $(r_iP, r_iA + X_i)_{i \in I}$ and a re-encrypted and re-order list $(r'_iP, r'_iA + X_{\sigma(i)})_{i \in I}$ 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 $i_0 \in I$.
- Suppose that he can always do so.
- The reducer, that is you, is given four elements (P, 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 $c_0 = (rP, B + X)$, $c_1 = (r_1P, r_1A + X)$, and
- the mix's output $c'_0 = (\delta_0P + rP, \delta_0A + B + X)$, $c'_1 = (r'_1P, r'_1A + X)$.

- 3 (ii) Argue that we can execute all operations in polynomial time. (Where a call to the attacker only counts as a single time unit.)
- 3 (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 $B + X$, and c_1 and c'_1 are both encryptions of X .
- 2 (iv) Decrypting c_0 we get $\text{dec}_a(c_0) = B + X - rA$. 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 $\text{prob}(\mathcal{A}(\dots) = \sigma^{-1}(1) = 1) > \frac{3}{4}$. (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.