Electronic elections, winter 2007

MICHAEL NÜSKEN

3. Exercise sheet
Hand in solutions until Sunday, 23 December 2007.

Exercise 3.1 (Security of a re-encryption mixnet). (12+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 $g, g^\alpha, g^\beta, g^\gamma \in G$ decide whether $\alpha\beta = \gamma$ (Tsiounis & Yung 1998).

We work in some (multiplicatively written) group G generated by an element g of order q, all this specified in the global setup. The receiver of the mixnet has the private key $\alpha \in \mathbb{Z}_q$ which defines the public key $a = g^\alpha \in G$. We use $\mathrm{enc}_a(x, \varrho) = (g^\varrho, a^\varrho x)$ and $\mathrm{dec}_\alpha(r, y) = yr^{-\alpha}$.

(i) Check that $\mathrm{dec}_\alpha \mathrm{enc}_a(x, \varrho) = x$. 1

- The attacker $\mathcal{A}$ is given input and output of one particular mix, ie. a list of encrypted messages $(g^{\varrho_i}, a^{\varrho_i} x_i)_{i\in I}$ and a re-encrypted and re-order list $(g^{\varrho'_i}, a^{\varrho'_i} x_{\sigma(i)})_{i\in I}$ where σ is a permutation of I. The random exponents ϱ_i, ϱ'_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 (g, a, g^ϱ, b) and tries to determine whether $b = a^\varrho$. 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 $c_0 = (g^{\varrho}, bx)$, $c_1 = (g^{\varrho_1}, a^{\varrho_1}x)$, and
  - the mix's output $c'_0 = (g^{\delta_0}g^{\varrho}, a^{\delta_0}bx)$, $c'_1 = (g^{\varrho'_1}, a^{\varrho'_1}x)$.

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 bx, and c_1 and c'_1 are both encryptions of x.

2 (iv) Decrypting c_0 we get $\mathrm{dec}_\alpha(c_0) = bxa^{-\varrho}$. Prove that this is equal to x if and only if $b = a^{\varrho}$.

1 (v) Prove that if $b \neq a^{\varrho}$ the attacker will answer that $\sigma^{-1}(1) = 1$.

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

Now, you play the above game twice (say), and answer "$b \neq a^{\varrho}$" 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 $\mathrm{prob}(\mathcal{A}(\dots) = \text{"}\sigma^{-1}(1) = 1\text{"}) > \frac{3}{4}$. (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 3.2 (Secret sharing). (2+4 points)

Fix $p = 1009$ and consider polynomials over the field $\mathbb{F}_p$ with p elements. Let u_i, $0 \leq i < 8$ be chosen at random but all different, say $u_0 = -1$, $u_1 = 5$, $u_2 = 17$, $u_3 = 42$, $u_4 = 97$, $u_5 = 127$, $u_6 = 571$, $u_7 = 800$. A polynomial of degree less than 8 has been determined with $f(0)$ being a secret key to a safe containing $1\,000\,000$€. Secret bearer i gets the share $(u_i, f(u_i))$. The secret bearers 1 through 7 collide and so together they know $f(u_1) = 1$, $f(u_2) = 120$, $f(u_3) = 712$, $f(u_4) = 95$, $f(u_5) = 761$, $f(u_6) = 20$, $f(u_7) = 841$. Only the secret bearer 0 stays honest.

(i) Suppose due to an indescretion the seven learn that $u_0 = -1$, yet not the value $f(u_0)$. Make (or prove) a statistics: For every value $s \in \mathbb{F}_p$ count the number of share values $f(u_0)$ leading to this secret. [2]

(ii) Suppose due to an indescretion the seven learn that $f(u_0) = 194$, yet not u_0. Make a statistics: For every value $s \in \mathbb{F}_p$ count the number of share nodes u_0 leading to this secret. [+2]

(iii) Compare the results: is one of the indiscretions a problem for scret bearer 0? Which one? Why? Can you describe "how much" information was disclosed? [+2]

Note that MuPAD has a function `interpolate` which also works over a finite field `Dom::GaloisField(p);`

References

YIANNIS TSIOUNIS & MOTI YUNG (1998). On the security of ElGamal based encryption. In *Public Key Cryptography*, HIDEKI IMAI & YULIANG ZHENG, editors, number 1431 in Lecture Notes in Computer Science, 117–134. Springer-Verlag, Berlin, Heidelberg. ISBN 3-540-64693-0. ISSN 0302-9743. URL `http://dx.doi.org/10.1007/BFb0054009`.