T-79.5501 Cryptology

Lecture 10 (Nov 22, 2005):

- The ElGamal Cryptosystem (6.1)
- Homomorphic encryption and how to sell digital goods
- The discrete logarithm problem (6.2)
- Shanks' algorithm (6.2.1)
- The Pohlig-Hellman algorithm (6.2.3)
- Elliptic curves (6.5.2)

Homomorphic encryption

Given ElGamal encryptions of m_1 and m_2 :

$(\alpha^{k_0}, \beta^{k_0} m_0)$ and $(\alpha^{k_1}, \beta^{k_1} m_1)$

one can generate valid ElGamal encryptions for $m_1 m_2$:

$$(\alpha^{k_0+k_1}, \beta^{k_0+k_1} m_0 m_1)$$

and and m_1 / m_2 :

$$(\alpha^{k_0-k_1}, \beta^{k_0-k_1} \frac{m_0}{m_1})$$

even without knowledge of the public key.

One-out-of-Two Oblivious Transfer

Alice has two digital products m_0 and m_1. Bob wants to buy one of them, and Alice is willing to sell just one.

The protocol (Aiello et al, Eurocrypt 2001)

1. Alice and Bob agree on a group G where ElGamal cryptosystem is secure, and a generator $\alpha \in G$ of order n.
2. Bob generates a key pair $(a, \beta = \alpha^a)$ for ElGamal cryptosystem and selects the product m_b he wants to buy. He represents his choice as bit as $B = \alpha^b$ and computes an encryption of it: $C = (\alpha^k , \beta^k B)$. Bob sends C, β to Alice.
3. Alice verifies that β is a valid public key and C is a valid ciphertext (there are cryptographic methods for doing this.)

One-out-of-Two Oblivious Transfer (2)

4. Alice draws four integers k_j, r_j, $j = 0,1$, $0 < k_j, r_j < n$, uniformly at random and computes encryptions of α^j, $j = 0,1$:

$$C_j = (\alpha^{k_j}, \beta^{k_j}\alpha^j),\ j = 0,1$$

and further encryptions of $\alpha^j / B = \alpha^{j-b}$ using homomorphic encryption. (Note that Alice does not know B but she knows the encryption C of it.)

$$(\frac{\alpha^{k_j}}{\alpha^k}, \frac{\beta^{k_j}\alpha^j}{\beta^k B}) = (\alpha^{k_j - k}, \beta^{k_j - k}\alpha^{j-b})$$

Then she raises both parts to power r_j and creates encryptions of $\alpha^{(j-b)rj}\, m_j$:

$$(\alpha^{(k_j - k)r_j}, \beta^{(k_j - k)r_j}\alpha^{(j-b)r_j} m_j),\ j = 0,1$$

And sends both encryptions to Bob.

One-out-of-Two Oblivious Transfer (3)

5. Bob takes the one with j = b, and is able to decrypt m_b as

$$(\alpha^{(k_b-k)r_b}, \beta^{(k_b-k)r_b}\alpha^{(b-b)r_b}m_b)$$

is a proper El Gamal encryption of m_b , since $\alpha^{b-b} = 1$.

If Bob selects $j \neq b$, and decrypts he gets $\alpha^{(j-b)\, rj}\, m_j = \alpha^{\pm rj}\, m_j$, which is random data.