

TP 03: El-Gamal and Cramer-Shoup Encryption

Jean-Sébastien Coron

Université du Luxembourg
www.jscoron.fr

1 El-Gamal encryption

Let consider the following variant of the El-Gamal encryption scheme.

Key Generation: Let G be a subgroup of prime order q of \mathbb{Z}_p^* for prime p and let g be a generator of G . Let $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$ be a hash-function. Let x be a random integer between 0 and $q - 1$. Let $h = g^x$. The public-key is (g, h) and the private-key is x

Encryption: Given $m \in \{0, 1\}^n$, generate a random integer r between 0 and $q - 1$ and let :

$$c = (g^r, H(h^r) \oplus m)$$

1. Explain how decryption works.
2. Implement this variant of El-Gamal.
3. Describe and implement a chosen-ciphertext attack against this variant.

2 The Cramer-Shoup public-key encryption scheme

1. Explain why decryption work in Cramer-Shoup's cryptosystem.
2. Let consider the following "lite" version of Cramer-Shoup.

Key-Generation:

Let G a group of prime order q . Generate random $g_1, g_2 \in G$ and randoms $x_1, x_2, z \in \mathbb{Z}_q$. Let $c = g_1^{x_1} g_2^{x_2}$ and $h = g_1^z$. Then $pk = (g_1, g_2, c, h)$ and $sk = (x_1, x_2, z)$

Encryption:

Let $m \in G$. Generate a random $r \in \mathbb{Z}_q$. Then

$$C = (g_1^r, g_2^r, h^r m, c^r)$$

Decryption:

Given $C = (u_1, u_2, e, v)$, check that $v = u_1^{x_1} u_2^{x_2}$. In this case, outputs $m = e / (u_1)^z$. Otherwise, output "reject".

This version is secure against non-adaptive chosen-ciphertext attack; that is, the adversary is only allowed to make decryption queries *before* he receives the challenge ciphertext, not after (IND-CCA1 security). Show that this "lite" version is not secure against adaptive chosen-ciphertext attack (IND-CCA2 security), where the adversary can make decryption queries both before and after receiving the challenge ciphertext.