Advanced Topics in Cryptography – Exercise Set 2

June 15, 2011

Exercise 1

An electronic check stating "Pay 10000 yen to Mr. Tarou Kyudai" is encrypted using the one-time pad, where both the message and the key are represented as binary vectors. Suppose that the adversary does not know the key. Describe a possible attack.

Exercise 2

Consider the set of users $\{U_1, U_2, U_3, U_4\}$. Construct a secret sharing scheme with a (monotone) access structure $\{\{U_1, U_2\}, \{U_3, U_4\}\}$. In other words, the sets $\{U_1, U_2\}$ and $\{U_3, U_4\}$ can reconstruct the secret, while any other set not containing them have no information on the secret.

Example: $\{U_1, U_2\}$, or $\{U_1, U_2, U_3\}$, or $\{U_1, U_2, U_3, U_4\}$ can reconstruct the secret, while $\{U_1, U_4\}$ cannot.

Exercise 3

Consider the $(k+1, n)$ Shamir secret sharing scheme. There are n users and any $k+1$ of them can reconstruct the secret Z.

The scheme is defined by the polynomial $f(X) = H_0 + H_1X + \ldots + H_{k-1}X^{k-1} + ZX^k$ of degree k over the field $\mathbb{Z}_p$, where p is prime and $p \geq n$. For all $0 \leq i \leq k-1$, H_i are mutually independent and uniform over $\mathbb{Z}_p$. For simplicity, we take the secret $Z \in \mathbb{Z}_p$.

Every user U_i, $1 \leq i \leq n$ receives a share $Y_s := f(s_i)$, where all $s_i \in \mathbb{Z}_p$ are distinct, i.e. $s_i \neq s_j$, for all $1 \leq i, j \leq n$ such that $i \neq j$.

Question 1) Explain, why s_i must be distinct.

In the classical Shamir scheme, the secret is placed as a free coefficient,
i.e. $f(X) = Z + H_1X + \ldots + H_{k-1}X^{k-1} + H_kX^k$.

In other words, $Z = f(0)$. However, it must hold that $p > n$ (as opposed to "$p \geq n$" in the above scheme).

Question 2) Explain, why the classical Shamir scheme is insecure, if the number of players $n = p$.