The art of cryptography: security, reductions, and group cryptography

Prof. Dr. Joachim von zur Gathen, Konstantin Ziegler

5. Assignment

(Due: Thursday, 10 May 2012, 13^{00})

Exercise 5.1 (Distinguisher to test)**.** Let N be a Blum integer and $\mathcal{B}$ be an algorithm that on input $a \in \square_N \cup \boxtimes_N$ outputs "$a \in \square_N$" or "$a \in \boxtimes_N$". Furthermore, for $a \in \square_N \cup \boxtimes_N$ *chosen uniformly at random*, the algorithm is correct with probability at least $1/2 + \varepsilon$. Consider the following derived algorithm $\mathcal{C}$.

Algorithm $\mathcal{C}$ Weak squareness test from squareness distinguisher $\mathcal{B}$

Input $a \in \square_N \cup \boxtimes_N$.

Output "$a \in \square_N$" or "$a \in \boxtimes_N$".

1. $r \xleftarrow{\$} \mathbb{Z}_N^\times$.
2. $s \xleftarrow{\$} \{0,1\}$.
3. Compute $b \in (-1)^s r^2 a$ in $\mathbb{Z}_N$.
4. Call $\mathcal{B}$ with input b, and let $t \in \{0,1\}$ be the output bit $t = (\mathcal{B}(b) = \text{"}b \in \square_N\text{"})$. [Thus t is 1 if and only if $\mathcal{B}$ answers "$b \in \square_N$".]
5. If $s \oplus t = 1$ then return "$a \in \square_N$" else return "$a \in \boxtimes_N$".

(i) (2 points) Show that $\mathcal{C}$ answers correctly if and only if $\mathcal{B}$ answers correctly in step 4.

(ii) (2 points) Show that for any input $a \in \square_N \cup \boxtimes_N$, the element b computed in step 3 is a uniform random element of $\square_N \cup \boxtimes_N$.

(iii) (2 points) Conclude that the probability that $\mathcal{C}$ answers correctly is at least $1/2 + \varepsilon$ *for any input*.

Exercise 5.2 (Amplifying)**.** Given a Monte-Carlo algorithm $\mathcal{C}$ that answers correctly for any input with probability at least $1/2 + \varepsilon$. Consider a test $\mathcal{T}$ which runs $\mathcal{C}$ exactly $k = 2m + 1$ times independently and outputs the majority answer.

(i) (2 points) Provide an exact expression for the probability that $\mathcal{T}$ answers incorrectly.

(ii) (2 points) Show that the expression in (i) is bounded above by $(1 - 4\varepsilon^2)^m/2$. [Hint: Let $s = 1/2 + \varepsilon$ and $t = 1/2 - \varepsilon$ and use $t/s \leq 1$.]

(iii) (2 points) For ε equal to 0.01, 0.1, and 0.25 determine k such that $\mathcal{T}$ is correct with probability at least 97%.

Exercise 5.3 (Blum-Blum-Shub Generator)**.** Given the Blum integer $N = 1333 = 31 \cdot 43$.

(i) (1 points) How many elements do $\square_{1333}$ and $\boxtimes_{1333}$ have?

(ii) (4 points) Determine the sets $\square_{1333}$ and $\boxtimes_{1333}$ with a programming language of your choice and verify that squaring (modulo N) defines a bijection $\square_{1333} \to \square_{1333}$ and a bijection $\boxtimes_{1333} \to \square_{1333}$. Give a bijection $\square_{1333} \to \boxtimes_{1333}$.

(iii) (2 points) Compute the the smallest primes p and q with $p \geq 2^9$, $q \geq 2^{11}$, and $p \equiv q \equiv 3 \bmod 4$. Let $N = p \cdot q$ and $x_0 = 100\,001$.

(iv) (5 points) Implement the Blum-Blum-Shub generator in a programming language of your choice and compute the first 50 bits with the generator.

Carry out a few statistical tests.

(v) (2 points) For each possible possible pair (z_{2i}, z_{2i-1}), $i = 1..2^{13}$, determine the number of times they occur. Compare with the theoretical values for a truly random generator.

(vi) (3 points) What is the mean value and the standard deviation for 2^{13} bits. Compare with the theoretical values for a truly random generator.

(vii) (+4 points) Plot 1 000 points (u, v), where the binary representation of u and v consists of 10 consecutive bits out of the produced series of bits each. Can any regularities be seen in the picture? Compare with a simple linear congruential generator: $x_i \leftarrow 313 \cdot x_{i-1} \bmod 2053$, $z_i \leftarrow x_i \bmod 1024$, where each value gives a coordinate of u or v.