Advanced Cryptography — Final Exam

Serge Vaudenay

16.6.2009

- all documents are allowed
- a pocket calculator is allowed
- communication devices are not allowed
- answers to the exercises must be provided on a separate sheet
- readability and style of writing will be part of the grade
- do not forget to put your name on the sheet!

1 A Distinguisher

We consider an oracle A which, upon a query x which is a vector of k bits, behaves as follows:

Input: x
1: compute the vector $\bar{x}$ by flipping all bits of x
2: set $u = \bar{x} \| x$
3: pick a random permutation σ over $\{1, 2, \ldots, 2k\}$
4: apply transposition σ on u to get a vector v
namely, if $u = u_{2k} \| \cdots \| u_2 \| u_1$ we have $v = u_{\sigma(2k)} \| \cdots \| u_{\sigma(2)} \| u_{\sigma(1)}$
5: set y to the k rightmost bits of v
Output: y

We denote $y = A(x)$. (We stress that $A(x)$ is a random variable.)

1. Given a random variable X we define its distribution function $P_X(x) = \Pr[X = x]$. Show that for any x and y we have
$$P_{A(x)}(y) = \frac{\binom{k}{k-w(y)}}{\binom{2k}{k}}$$
where $w(y)$ is the Hamming weight of y (i.e. the number of bits set to 1 in y). Deduce it does not depend on x.
As an application, compute the table of $P_{A(x)}$ with $k = 2$.
2. Deduce the best advantage of a distinguisher limited to a single query x for distinguishing A from a random oracle.
For $k = 2$, compute the advantage.
3. Given a function $f : \{0, 1\}^k \to \mathbf{R}$ we define its discrete Fourier transform
$$\hat{f}(a) = \sum_x (-1)^{a \cdot x} f(x)$$
Let r be the Hamming weight of the bitwise AND of a and x and let s be such that $r + s$ is the Hamming weight of x. Show that $a \cdot x$ can be expressed as a function in terms of r and s. By grouping the x's with same values of r and s in the sum, show that there is a function g such that $\hat{P}_{A(x)}(a) = g(w(a))$.
Compute the table of $\hat{P}_{A(x)}$ for $k = 2$.

To fix the bias, we consider the following oracle B.

Input: x

for i=1 to r **do**

  query $A(x)$ and get y_i

end for

set $y = y_1 \oplus \cdots \oplus y_r$

Output: y

Again, we denote $B(x)$ the random output from x.

4. Given two independent random variables X and Y, show that

$$P_{X \oplus Y}(z) = \sum_{x,y \text{ s.t. } x \oplus y = z} P_X(x) P_Y(y)$$

   Deduce that

$$P_{B(x)}(y) = \sum_{\substack{y_1,\ldots,y_r \text{ s.t.} \\ y_1 \oplus \cdots \oplus y_r = y}} \prod_{i=1}^{r} P_{A(x)}(y_i)$$

   If we had to compute the table of $P_{B(x)}$ form this formula, what would be the complexity, roughly? Is it doable for $k = 10$ and $r = 10$?

5. Show that for all a we have

$$\hat{P}_{X \oplus Y}(a) = \hat{P}_X(a) \times \hat{P}_Y(a)$$

   i.e. the discrete Fourier transform of the distribution of $X \oplus Y$ is obtained by multiplying the discrete Fourier transforms of X and Y.
   Deduce that

$$\hat{P}_{B(x)}(a) = \left(\hat{P}_{A(x)}(a) \right)^r$$

   If we had to compute the table of $\hat{P}_{B(x)}$ form this formula, what would be the complexity, roughly? Is it doable for $k = 10$ and $r = 10$? How about $k = 128$ and $r = 10$?

6. For any function $f : \{0,1\}^k \to \mathbf{R}$ such that $\sum_x f(x) = 1$, show that

$$\sum_x \left(f(x) - 2^{-k} \right)^2 = 2^{-k} \sum_{a \neq 0} \left(\hat{f}(a) \right)^2$$

   Hint: think about Parseval.

7. Deduce that the square Euclidean imbalance of $B(x)$ is

$$\mathsf{SEI}(B(x)) = \sum_{a \neq 0} \left(\hat{P}_{A(x)}(a) \right)^{2r}$$

   Finally deduce that

$$\mathsf{SEI}(B(x)) = \sum_{w=1}^{k} \binom{k}{w} (g(w))^{2r}$$

   Is it feasible to compute it for $k = 128$ and $r = 10$?

8. Deduce an estimate on the number of samples to distinguish $B(x)$ from a uniformly distributed random variable.

9. As an application, compute this estimate for $k = 2$. How large r must be so that this is higher than 2^{80}?

2 Σ-Protocol for Cubic Residues

We consider an integer $n = p \times q$ where p and q are two primes numbers, 3 divides $p - 1$ but not $q - 1$.

1. Show that -3 is a quadratic residue modulo p.
2. Deduce that $X^2 + X + 1$ has 2 roots in $\mathbf{Z}_p$.
3. Show that $X^3 - 1$ has exactly 3 different roots in $\mathbf{Z}_p$.
   Deduce that for all $s \in \mathbf{Z}_p^*$ the polynomial $X^3 - s$ has either no root or exactly 3 different roots.
4. By using the Chinese remainder theorem, show that any element of $\mathbf{Z}_n^*$ has either exactly 3 cubic roots or none. Those with cubic roots will be called *cubic residues*. We denote by CR_n the set of all cubic residues from $\mathbf{Z}_n^*$.
5. Inspire by the Fiat-Shamir Σ-protocol and propose a Σ-protocol for the relation

$$R((n, v), s) \Leftrightarrow vs^3 \bmod n = 1$$

   Be careful to go through the check list which has been given in the course, describe all components of the Σ-protocol and prove it satisfies the required properties.

3 The GQ Protocol

Σ-protocols are made with some components satisfying a list of requirements as explained in the course. We consider here Σ-protocols with the extra property of uniqueness of response: using the notations from the course, for each x, a, e, there exists a unique z such that the verification $V(x, a, e, z)$ holds.

1. Show that the Schnorr Σ-protocol provides uniqueness of response.

Let (N, e) be an RSA public key. We consider the following GQ protocol with relation

$$R((N, e, X), x) \Longleftrightarrow x^e \bmod N = X$$

$$\begin{array}{rcl}
\textbf{Prover} & & \textbf{Verifier} \\
\textbf{witness}: x & \textbf{input}: (N, e, X) & \\
 & & \\
\text{pick } y \in \mathbf{Z}_N^* & & \text{pick } c \in \{0, 1, \ldots, 2^\ell - 1\} \\
Y \leftarrow y^e \bmod N & \xrightarrow{\quad Y \quad} & \\
 & \xleftarrow{\quad c \quad} & \\
z \leftarrow yx^c \bmod N & \xrightarrow{\quad z \quad} & z^e \stackrel{?}{\equiv} YX^c \pmod{N}
\end{array}$$

Warning: in the GQ protocol, notations are somewhat different from usual.

2. Assuming that GQ is a Σ-protocol, formalize all components except the extractor.
3. Show (except special soundness) that all properties are satisfied.
4. Show that GQ provides response uniqueness.
5. When $\mathsf{gcd}(c_1 - c_2, e) = 1$, show that we can extract a witness from two transcripts (Y, c_1, z_1) and (Y, c_2, z_2).
   Hint: use the extended Euclid algorithm to find two integers a and b such that $ae + b(c_1 - c_2) = 1$.
6. Deduce that we have an extractor which might fail sometimes. Estimate the probability of failure for $e = 65\,537$.