Advanced Cryptography — Final Exam

Serge Vaudenay

24.5.2022

- duration: 3h
- any document allowed
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will <u>**not**</u> answer any technical question during the exam
- readability and style of writing will be part of the grade

1 Σ Protocol for Discrete Log Equality

We assume that public parameters pp describe a group, how to do operations and comparison in the group, and also give its prime order p. We use additive notation and 0 denotes the neutral element in the group. We define the relation $R((\mathsf{pp}, G, X, Y, Z), x)$ for group elements G, X, Y, Z and an integer x which is true if and only if $G \neq 0$, $X = xG$, and $Z = xY$. We construct a Σ-protocol for R with challenge set $\mathbf{Z}_p$. The prover starts by picking $k \in \mathbf{Z}_p$ with uniform distribution, computing and sending $A = kG$ and $B = kY$. Then, the prover gets a challenge $e \in \mathbf{Z}_p$. The answer is an integer z to be computed in a way which is a subject of the following question. The final verification is also a subject of the following question. The protocol looks like this:

Prover		**Verifier**
witness: x	instance: $(\mathsf{pp}, G, X, Y, Z)$	
$(X = xG$ and $Z = xY)$		
pick $k \in \mathbf{Z}_p$		
$A = kG,\ B = kY$	$\xrightarrow{A,B}$	
	$\xleftarrow{e}$	pick $e \in \mathbf{Z}_p$
??	$\xrightarrow{z}$	??

Q.1 Inspired by the Schnorr proof, finish the specification of the prover and the verifier.
Q.2 Specify the extractor and the simulator.
Q.3 Fully specify another Σ-protocol for the relation $R((\mathsf{pp}, G, X, Y, Z, U, V), (a, b))$ which is true if and only if $U = aG + bY$ and $V = aX + bZ$.

2 Distinguisher for Lai-Massey Schemes

The Lai-Massey scheme is an alternate construction to the Feistel scheme to build a block cipher from round functions. Let n be the block size and r be the number of rounds. We denote by $\oplus$ the bitwise XOR operation over bistrings. Let the F_i be secret functions from

$\{0,1\}^{\frac{n}{2}}$ to itself and π be a fixed public permutation over $\{0,1\}^{\frac{n}{2}}$. Let $x, y \in \{0,1\}^{\frac{n}{2}}$ and $x\|y$ denote the concatenation of the two bitstrings. We define

$$\varphi(F_1, \ldots, F_r)(x\|y) = \varphi(F_2, \ldots, F_r)(\pi(x \oplus F_1(x \oplus y))\|(y \oplus F_1(x \oplus y)))$$

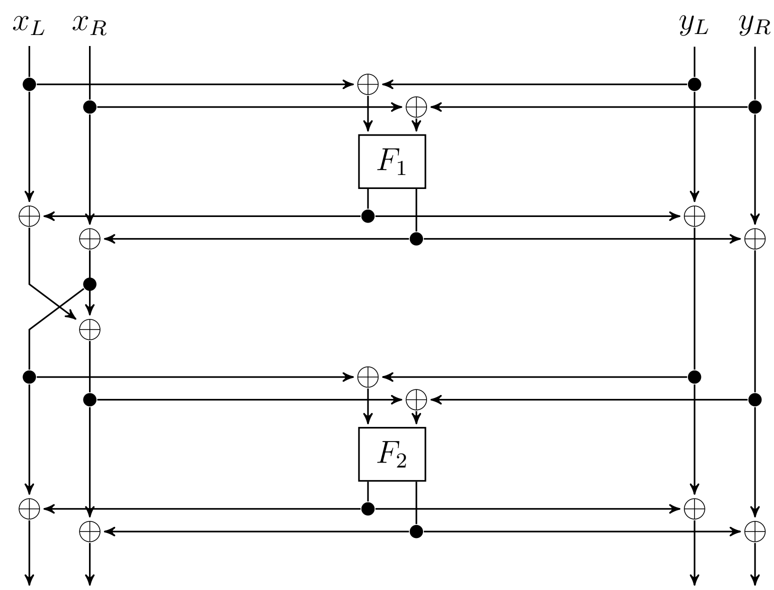
for $r > 1$ and

$$\varphi(F_r)(x\|y) = (x \oplus F_r(x \oplus y))\|(y \oplus F_r(x \oplus y))$$

when there is a single round. In what follows, we assume that the permutation π is defined by

$$\pi(x_L\|x_R) = (x_R\|(x_L \oplus x_R))$$

where $x_L, x_R \in \{0,1\}^{\frac{n}{4}}$. For example, a 2-round Lai-Massey scheme is represented as follows:



Q.1 If $\varphi(F_1, \ldots, F_r)$ is the encryption function, what is the decryption function?

Q.2 Give a distinguisher between $\varphi(F_1)$ and a random permutation with a single known plaintext and advantage close to 1. (Compute the advantage.)

Q.3 Give a distinguisher between $\varphi(F_1, F_2)$ and a random permutation with two chosen plaintexts and advantage close to 1. (Compute the advantage.)

3 Bias in the Modulo p Seed

We assume a setup phase $\mathsf{Setup}(1^\lambda) \to p$ to determine a public prime number p with security parameter λ. We consider the following generators:

Generator $\mathsf{Gen}_0(1^\lambda, p)$:

pick $y \in_U \mathbf{Z}_p$

return y

Generator $\mathsf{Gen}_1(1^\lambda, p)$:

$\ell \leftarrow \lceil \log_2 p \rceil$

pick $x \in_U \{0, 1, \ldots, 2^\ell - 1\}$

$y \leftarrow x \bmod p$

return y

Generator $\mathsf{Gen}_2(1^\lambda, p)$:

$\ell \leftarrow \lceil \log_2 p \rceil$

pick $x \in_U \{0, 1, \ldots, 2^{\ell+\lambda} - 1\}$

$y \leftarrow x \bmod p$

return y

Here, "pick $x \in_U E$" means that we sample x from a set E with uniform distribution. The value ℓ is the bitlength of p. In what follows, we consider distinguishers with unbounded complexity but limited to a single query to a generator.

Q.1 Estimate how ℓ is usually fixed to have λ-bit security for typical cryptography in a (generic) group of order p. (For instance, in an elliptic curve.)

Q.2 Compute the advantage of the best distinguisher between Gen_0 and Gen_1. Could it be large?

Q.3 Compute the advantage of the best distinguisher between Gen_0 and Gen_2.
Hint: use the Euclidean division $2^{\ell+\lambda} = qp + r$.

Q.4 Based on the computations, what do you conclude about the generator algorithms?