

## Cryptology – F08 – Week 12

### **Lecture, April 22**

We covered the Blum-Goldwasser Public-key Cryptosystem from section 8.4 and began on zero-knowledge (from the notes by Ivan Damgård and Jesper Buus Nielsen, available through the course's homepage).

### **Lecture, April 24**

We continued with zero-knowledge from the notes and slides.

### **Lecture, April 30**

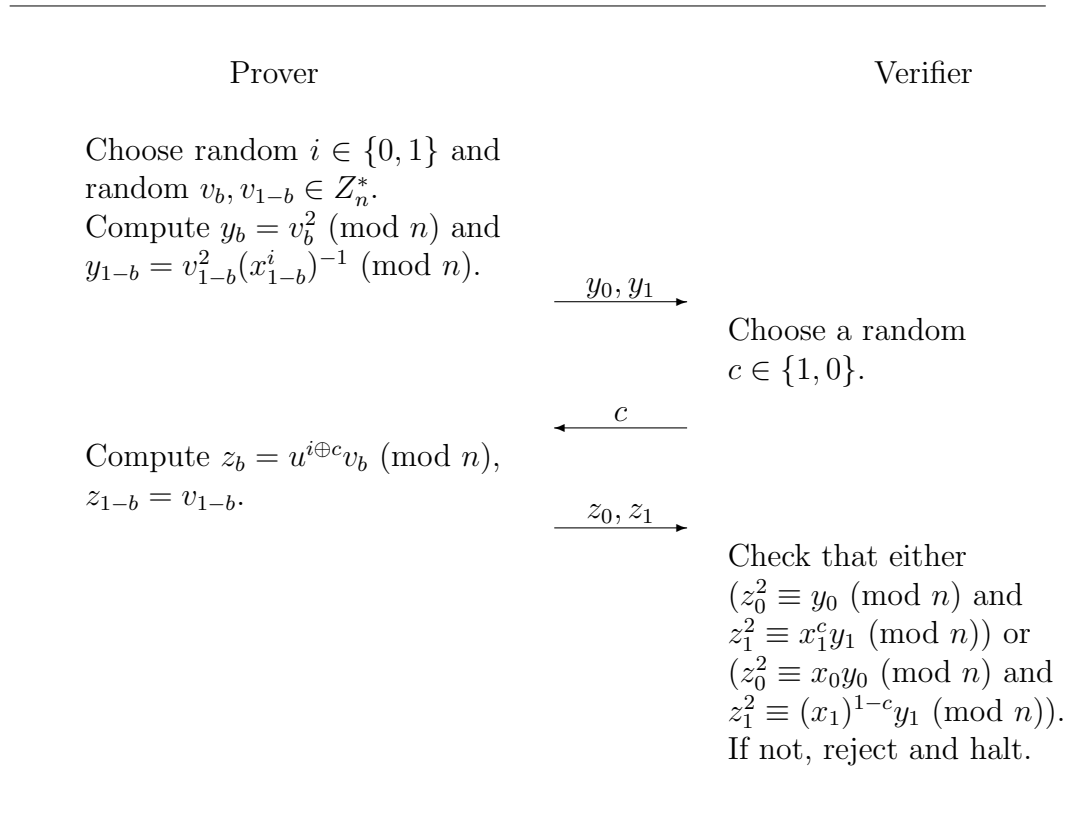
We will continue with zero-knowledge, from the notes and slides, and cover chapter 9 in the textbook.

### **Lecture, May 7**

We will cover sections 10.1, 10.2, and 10.5.4 of chapter 10, section 11.2 of chapter 11, and section 13.1 of chapter 13..

### **Problem sessions May 6 and May 8.**

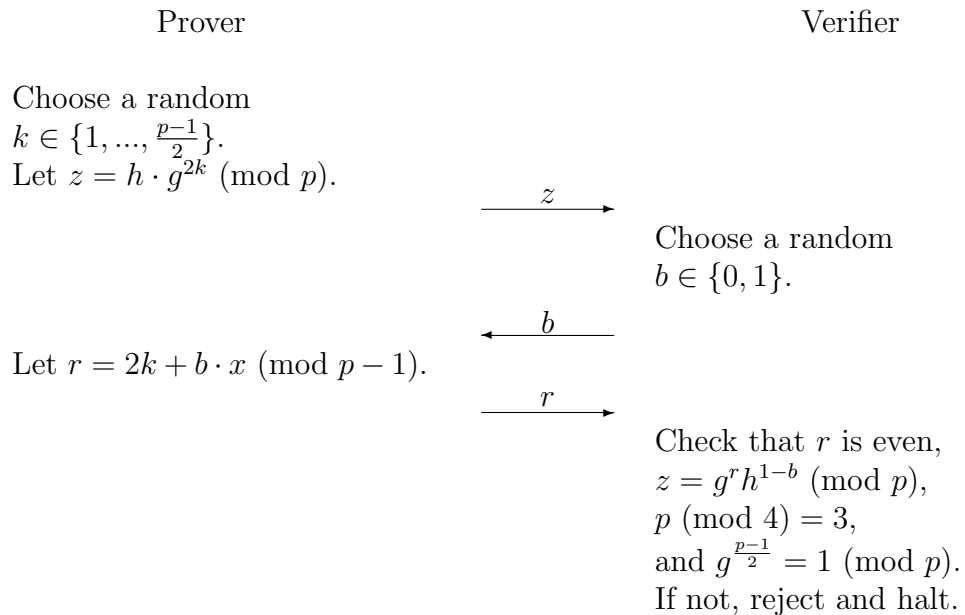
1. Let  $n$  be an integer with unknown factorization  $n = pq$ , where  $p$  and  $q$  are prime, and let  $x_0, x_1 \in Z_n^*$  be such that at least one of  $x_0$  and  $x_1$  is a quadratic residue modulo  $n$ . Assume that both  $x_0$  and  $x_1$  have Jacobi symbol  $+1$  modulo  $n$ . (Assume that it is  $x_b$  and  $u^2 \equiv x_b \pmod{n}$ ). Suppose that  $x_0, x_1$ , and  $n$  are given as input to a Prover and Verifier. Consider the interactive protocol in which the following is repeated  $\log_2 n$  times:



Note that  $\oplus$  is addition modulo 2.

- a. Prove that the above protocol is an interactive proof system showing that at least one of  $x_0$  and  $x_1$  is a quadratic residue modulo  $n$ .
  - b. Suppose that  $x_{1-b}$  is also a quadratic residue. What is the distribution of the values  $y_0, y_1, z_0, z_1$  sent by a Prover following the protocol?
  - c. Suppose that  $x_{1-b}$  is a quadratic nonresidue. What is the distribution of the values  $y_0, y_1, z_0, z_1$  sent by a Prover following the protocol?
  - d. Prove that the above protocol is perfect zero-knowledge.
2. Give a zero-knowledge interactive proof system for the Subgroup Non-membership Problem (showing that  $\beta$  is not in the subgroup generated by  $\alpha$ ). Prove the your protocol is an interactive proof system. Prove that it is zero-knowledge.

3. Let  $p = 4k + 3$  be a prime, and let  $g$  and  $h$  be quadratic residues modulo  $p$ . Assume that  $h$  is in the subgroup generated by  $g$  and that the Prover knows an  $x$  such that  $g^x = h \pmod{p}$ . Suppose that  $p$ ,  $g$ , and  $h$  are given as input to a Prover and Verifier. Consider the interactive protocol in which the following is repeated  $\log_2 p$  times:




---

(Actually, the last two checks only need to be done once and could be done before the first round of the protocol. Don't let their placement here confuse you.)

- a. Prove that the above protocol is an interactive proof system showing that  $h = g^{2y} \pmod{p}$  for some integer  $y$ .
- b. Suppose that  $h = g^{2y} \pmod{p}$  for some integer  $y$ . What is the probability distribution of the values  $(z, r)$  sent by a Prover following the protocol?
- c. Prove that the above protocol is perfect zero-knowledge.
- d. Suppose  $p = 4k + 3$ . Note that any quadratic residue  $g$  modulo  $p$  has odd order. Use this fact to show that if  $h$  is in the subgroup

generated by a quadratic residue  $g$ , then it is always possible to write  $h$  as  $h = g^{2y} \pmod{p}$  for some integer  $y$ . (Thus, the above protocol is an alternative zero-knowledge proof of subgroup membership for this special case.)

**e.** Suppose  $p = 4k + 3$ ,  $g \neq 1$  is a quadratic residue modulo  $p$ , and  $q = \frac{p-1}{2} = 2k + 1$  is a prime. Then, there is a more efficient secure way, than using the above protocol, to convince the Verifier that  $h = g^y \pmod{p}$  for some integer  $y$ . What is it? (Hint: no Prover is necessary.)

4. Do problem 9.1.
5. Do problem 9.2.
6. Do problem 9.6.
7. Do problem 9.7.
8. Do problem 9.8a.
9. Do problem 9.13.