

# Cryptography

## Problem set 6

1. Present a proof of GMW algorithm [1] with “NAND” gate.
2. Show how to transform RSA blind signature scheme into  $\binom{2}{1}$ -OT (1-out-of-2 oblivious transfer) protocol.
3. GMW protocol needs  $\binom{4}{1}$ -OT, propose one.
4. (a) For the Chaum-Pedersen commitment scheme with  $p = 37, g = 13, h = 35$ , a commitment  $c(x, r) = g^x h^r \bmod p = 29$  was published. Find value  $x$  to which  $c(x, r)$  commits to.  
(b) For the commitment scheme based on DL in  $Z_p$ , with parameters  $p = 37, g = 13$  a commitment  $c(x) = g^x \bmod p = 29$  was published. Find  $x$ .

What can you say about binding and hiding of each scheme – which of the properties is unconditional and which is computational?

5. Show that (in fact) a single round of (simplified) Fiat-Shamir identification scheme reveals 1-bit of information.

Prove security of Feige-Fiat-Shamir identification scheme. Why it is better than Fiat-Shamir identification scheme?

6. Is the following protocol a zero-knowledge proof of knowledge of RSA key  $d$  (with public key  $\langle N, e \rangle$  where  $ed \equiv 1 \pmod{\varphi(N)}$ )?
  - (a) Victor sends a challenge  $x \in Z_N^*$ ,
  - (b) Peggy replies with an  $c := x^d \bmod N$ ,
  - (c) Victor encrypts  $c$  with a public key and checks if the result  $c^e \bmod N$  is equal to  $x$ .

Check completeness, soundness and zero-knowledge properties of the described protocol.

7. Consider the following protocol for  $n = 3$  participants. A participant of a protocol ( $\mathbf{P}_i$ ) has a secret  $s_i$ . To share a secret, a participant chooses at random a prime  $p$ , and then picks uniformly at random  $r_{i,1}, r_{i,2} \in Z_p$ , and computes

$$r_{i,3} = s_i - r_{i,1} - r_{i,2} \bmod p.$$

Then  $\mathbf{P}_i$  sends  $r_{i,a}, r_{i,b}$  (for  $a, b \neq j$ ) to a participant  $\mathbf{P}_j$  (i.e.,  $\mathbf{P}_1$  sends  $r_{1,1}, r_{1,3}$  to  $\mathbf{P}_2$ ).

Show that neither  $\mathbf{P}_2$  nor  $\mathbf{P}_3$  learn  $s_1$ . How any two participants are able to compute  $s_i$ ?

Assuming that  $s$  is an ElGamal’s private signature key (and  $\langle g, h, p \rangle$  is a corresponding public key with  $h = g^s \bmod p$ ) show how  $\mathbf{P}_i$  i  $\mathbf{P}_j$  can cooperate to sign a message  $m$ .

8. Present problem statement, solution and security analysis of Yao’s Millionaire problem.
9. Present problem statement, solution and security analysis of Socialist Millionaire problem.
10. Present problem statement, solution and security analysis of Chaum’s Dining Cryptographers.

## References

- [1] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 218–229. ACM, 1987.