Cryptography

Problem set 5

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 $ed \equiv 1 \bmod \varphi(N)$)?

   (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.

11. Explain the difference between *proof of work*, *proof of space* and *proof of stake*. Provide examples.

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

13. Consider the following solution to the Socialist Millionaire problem. What is wrong with this solution? Participants: A has $x \in \{1, \dots, M\}$ and B has $y \in \{1, \dots, M\}$. A group G with prime order p is selected, g is a generator of G. Let $H : G \to \{0,1\}^n$ be a collision-resistant hash function, and $\mathsf{Enc}_k(x)$ denotes symmetric encryption with n-bit long key.

    A selects at random $s \in Z_p$, computes $\alpha = g^{sx}$ and sends α to B

    B selects at random $t \in Z_p$, computes $\beta = g^{ty}$ and sends β to A

    A derives a symmetric key $K_A := H(\beta^x)$

    B derives a symmetric key $K_B := H(\alpha^y)$

    A selects a random $r \in \{0,1\}^n$ and sends to B: $c = \mathsf{Enc}_{K_A}(r)$ and commitment to r

    B decrypts c with K_A, sends back the decrypted message

    A opens the commitment to r

14. How two parties can shuffle a deck of cards? See [2]

15. Describe kleptographic attack on ElGamal encryption.

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.

[2] Adi Shamir, Ronald L Rivest, and Leonard M Adleman. Mental poker. In *The mathematical gardner*, pages 37–43. Springer, 1981.