

Homework 4

Instructor: abhi shelat

You may collaborate with other students on the homework but you must submit your own individually written solution. Please identify your collaborators and any other external sources you use. Do not submit a problem solution which you cannot explain orally to me.

Problem 1 *Many-message Encryption*

Provide a definition for many-message CPA-secure public key encryption. Prove that single-message CPA-secure public key encryption implies many-message CPA-secure public key encryption.

Problem 2 *Bob and his socks*

Bob is color-blind. His sister always teases him before going to school by telling him “Your socks are mismatched! Quick! Go change them before the bus comes.” Bob is thus always chasing after the bus in the morning. At some point, however, he realizes that his sister is more interested in making him run than in keeping his feet properly matched. Help Bob design a protocol he can use with his sister to tell whether his sister is teasing him or is telling him the truth about his mismatched socks.

Problem 3 *Commitments*

Design a multi-bit commitment scheme that uses a single RSA modulus n and exponent e for all of the commitments. (Hint: you might have to modify the standard strong RSA assumption in order to prove that your scheme is binding.)

Problem 4 *Zero Knowledge Proofs*

Consider the following zero-knowledge protocol for proving that a value a is a quadratic residue modulo n . The idea of this construction is to simply parallelize the simpler ZKP for quadratic residuosity.

Input: n and a . Let α such that $\alpha^2 \equiv a \pmod n$ be given to P .

1. P chooses a random prime $p = 2q + 1$ where q is a random k -bit prime, a random g of order q in \mathbb{Z}_p^* , a random $\beta \leftarrow \mathbb{Z}_q^*$, and sets $h = g^\beta \pmod p$. P sends p, q, g, h to V .
2. V computes a random string c of length k and a random $r \leftarrow \mathbb{Z}_q^*$, and sends $x = g^r h^c$ to P .
3. P chooses k random values $r_1, \dots, r_k \pmod n$, computes $s_i = r_i^2 \pmod n$, and sends s_1, \dots, s_k to V .
4. V sends r and c to P .

5. P checks that $x = g^r h^c$. If so, P sends to V , for each i , the value $t_i = r_i \alpha^{c_i}$, where c_i is the i th bit of c . P also sends β to V
6. V checks that $t_i^2 \equiv s_i a^{c_i}$ for each i , and that $h = g^\beta$. If so, V accepts, otherwise V rejects.

This defines a P, V which you will prove is a zero-knowledge proof system. It should be clear that P, V has completeness 1. In order to achieve the zero-knowledge property, we added the commitment x into the protocol, as you will see when proving this.

1. Prove that P, V has negligible soundness (ie, V can only be convinced with negligible probability if a is a quadratic non-residue modulo n).
2. Prove that if the discrete logarithm problem is hard, then P, V is computational zero-knowledge (i.e., the simulated transcript is *indistinguishable* from a real one).