Institut for Matematik og Datalogi
Syddansk Universitet

November 26, 2019
JFB

Cryptology – 2019 – Assignment 3

Assignment due Thursday, December 19, 13:00

Groups of up to three students are allowed (and encouraged) on this assignment. Note that this is part of your exam project, and it will count some towards the grade in the course, so you may not work with others not in your group. If it is late, it will not be accepted. Turn in the assignment through the SDU Assignment system in Blackboard, and remember to keep your receipt. Turn in one PDF file per group.

You may write your answers in either English or Danish. If you do it by hand, write very neatly and legibly. Remember to explain all answers.

1. In class we have discussed the discrete logarithm problem modulo a prime, which means that we have discussed them over fields of prime order. There are also finite fields of prime power order, so for any prime p and any exponent $e \geq 1$, there is a field with $q = p^e$ elements, $GF(q)$. The elements of such a field can be represented by polynomials over $GF(p)$ of degree no more than $e-1$. The operations can be performed by working modulo an irreducible polynomial of degree e. For example, $y = x + x^5 + x^7$ is an element of the field $GF(2^{10})$, represented by $GF(2)[x]/(x^{10} + x^3 + 1)$. One can calculate a representation for y^2, by squaring y and then computing the result modulo $x^{10} + x^3 + 1$, so one gets $x^2 + 2x^6 + 2x^8 + x^{10} + 2x^{12} + x^{14} \pmod{x^{10} + x^3 + 1} = 1 + x^2 + x^3 + x^4 + x^7$.

   Why would there be a preference for working in $GF(2^k)$ for some large k, rather than modulo a prime for some very large prime? Hint: think about how arithmetic is performed. Also think about security.

2. Consider the Shamir secret sharing scheme with $p = 37$. Let the threshold be $t + 1 = 3$. Suppose the shares are:

   - (1, f(1)) = (1,1)

- (2, f(2)) = (2,20)
- (3, f(3)) = (3,36)

which are distributed to the share recipients. Show how to compute the secret.

3. In class we used the Goldwasser-Micali encryption scheme to implement bit commitments, as follows: Assume that a modulus N, which is the product of two large, equal length primes is given, along with an element $y \in \mathbb{Z}_N^*$ such that $\left(\frac{y}{N}\right) = 1$, but y is a quadratic nonresidue modulo N.

   To commit to a bit $b \in \{0,1\}$, choose a random $r \in \mathbb{Z}_N^*$ and set $C(b,r) = y^b \cdot r^2 \pmod{N}$.

   To open a commitment $c \in J_N$ as a zero, reveal $r \in \mathbb{Z}_N^*$ such that $c = r^2 \pmod{N}$. To open a commitment $c \in J_N$ as a one, reveal $r \in \mathbb{Z}_N^*$ such that $c = y \cdot r^2 \pmod{N}$.

   (a) Show that, assuming the hardness of the QUADRES problem, these bit commitments are computationally concealing.

   (b) Show that these bit commitments are information-theoretically binding.

   (c) Show how a prover can show that two of these bit commitments are commitments to different bits, without revealing which is a commitment to a one and which is a commitment to a zero.

      i. What does the prover reveal and how does the verifier check it?

      ii. Call the output revealed when showing that commitments are to different bits r. Argue that the distribution of r is the same when $(b_1, b_2) = (0,1)$ as when $(b_1, b_2) = (1,0)$. This means that V learns nothing except that $b_1 \neq b_2$ (assuming the quadratic residuosity assumption).

      iii. Argue that if P has in fact committed in c_1, c_2 to the bit pairs $(0,0)$ or $(1,1)$, she cannot use this method to show that they are commitments to different bits.

   (d) Show how a prover can show that two of these bit commitments are commitments to the same bit. What does the prover reveal

and how does the verifier check it? (It's OK to skip writing the security arguments, but convince yourself that it is secure.)

4. In an undirected graph $G = (V, E)$, an independent set of size k is a subset $I \subseteq V$, $|I| = k$ such that no two vertices in I have an edge between them. The Independent Set Problem is to determine if there exists an independent set of size k in a given graph. (This problem is NP-Complete.)

   Give a zero-knowledge proof for Independent Set. Thus, your input is an undirected graph, $G = (V, E)$, and a positive integer k, where G has an independent set of size at least k. Assume that the Prover knows such an independent set. Assume that the graph is given as an incidence matrix (the rows and columns are indexed by the vertices and there is 1 in the cell if the two vertices indexing that cell have an edge between them and 0 if not).

   Note that you should do a direct proof, rather than a reduction to another NP-Complete problem and then doing the zero-knowledge proof for the other problem. Use Goldwasser-Micali bit commitments.

   Prove that your protocol has the following properties:

   - Completeness
   - Soundness
   - Zero-knowledge