Mathematical Cryptology 2019

Dept. of EIT
Lund University
Box 118, 221 00 Lund, Sweden

WEEK 6,

Reading instructions:

- Chapter 19 (partly repetition)
- Chapter 20-22

There will be 2-4 hours of lectures covering the above.

Last programming exercise:

- Implement the Somewhat Homomorphic Encryption scheme given in the guest lecture (SHE over the integers, 2009 van Dijk et. al., PUBLIC KEY scheme; course webpage for slides) so that you can do homomorphic addition and multiplication for single bit messages. How many multiplications can your SHE do? Choose suitable parameters for the problem below.
- Implement a solution to the following problem: Alice and Bob would like to compare their LTH grades on a recent course. However, they do not want to tell their grade to anyone, they only want to know who has the highest grade. Alice's grade is represented in binary by $x = (x_1, x_0)$ and Bob's is similarly $y = (y_1, y_0)$. Now the LTH grades are represented as $00 = U$ (did not pass), $01 = 3$, $10 = 4$, $11 = 5$. Find the Boolean function that computes "$x < y$" and express it in ANF (using addition and multiplication in $\mathbb{F}_2$).
- In order for Alice and Bob to solve their problem, they use the help of two friends. Viktor sets up the secret/public key for the SHE ϕ. Alice and Bob encrypt their grades using the public key and each of them gives their encrypted information $\phi(x), \phi(y)$ to Claude Cloud. Claude computes the expression for f implementing "$x < y$" on the encrypted information to obtain $\phi(b = "x < y")$. He gives this to Viktor who decrypts and announces the result b to Alice and Bob. Run one more round to check also "$y < x$" and give the final result. Implement and run the solution.

Note: If you think the public key version is too complicated to implement, it is ok to implement the symmetric version, but then you need to assume that Viktor is giving the secret key to each of Alice and Bob.
Maximum 15 hours of work!

Ch 17: Standard exercises:
17.4 Show that in our definition of $\mathcal{BPP}$ one can replace the constant 2/3 by any proportion in the range $(1/2, 1)$. 17.5 Show that if one-way functions exist then $\mathcal{P} \neq \mathcal{NP}$.

Ch 20-21: Review exercises:
20.1 What is a committment scheme?
20.2 What does it mean for a committment scheme to be binding or concealing?
20.3 How can a zero-knowledge protocol for proof of knowledge be used as an identification scheme?
20.4 In the protocol for graph isomorphism, show that if Peggy produces the same graph H in two different runs of the protocol, then Victor can determine the secret graph isomorphism.
20.5 How do you turn an interactive zero-knowledge identification scheme into a digital signature scheme?

Ch 20-21: Standard exercises:
20.6 Given a group G and four elements g_1, g_2, h_1, h_2, suppose Peggy knows that

$$log_{g_1}(h_1) = log_{g_2}(h_2) = x$$

and that Peggy knows x. Give a protocol for Peggy to convince Victor that not only she knows the discrete logarithm but that the two discrete logarithms are equal.
20.7 Show that the zero-knowledge proof of validity for the committment $B_a(x)$ given in the text for when $x \in \{-1, 1\}$ satisfies the three requirements.

EXAM: Friday March 25, 8.00-13.00 at E:3139
First three programming exercises must have be approved before the exam! The last programming exercise from week 6 may be approved up to one week after the exam.

The exam will be review exercises (40%) and problem solving exercises (60%). Not the same as your hand-in exercises, but similar. See the course webpage, where you find old exams.

The book is not allowed on the exam, but complicated formulas will be given on the exam if they are needed. Do not forget to bring a good calculator.