Institute of Computer Science, University of Bern
Cryptographic Protocols, FS 2023

Prof. Christian Cachin
Jovana Mićić

Exercise 11

11.1 Arithmetic circuits (5pt)

The BGW protocol for secure multiparty computation evaluates an arithmetic circuit among n parties. However, most computer hardware, hardware-layout compilers, and the familiar circuit model in theory operate with binary (Boolean) wires and gates.

Describe how to turn a binary circuit into an equivalent arithmetic circuit over $GF(q)$, for some prime q. To be concrete, represent FALSE and TRUE with values in $GF(q)$ and describe how to implement AND, OR, NOT, and XOR gates. Justify the operations of each gate.

11.2 Accumulator based on the strong RSA assumption (5pt)

Recall the Camenisch-Lysyanskaya (CL) RSA-based accumulator scheme. It uses a hash function $H : \{0,1\}^* \to \mathbb{N}$, which maps arbitrary bit strings to primes. How can H be implemented in a deterministic way?

Existing primality tests are probabilistic. Assume we are given an algorithm *isPrime*(n, k), which outputs a Boolean value indicating whether the integer n is prime; the value k is a security parameter. Let it be implemented by the Miller-Rabin test [KL21, Sec. 8.2], which has access to a random-number generator R. If n is prime, this method always returns TRUE; if n is composite, it returns TRUE with probability at most $O(4^{-k})$ and FALSE otherwise.

Suppose R is a pseudorandom generator with seed s, i.e., there is a method $R.$*setSeed*(s) and after every call of this, R outputs a deterministic sequence of values that only depends on s.

a) Describe an implementation of H with text or using pseudocode.

b) *(Bonus: +5pt)* Implement the complete CL accumulator including H in python or your favorite programming language.

If you submit a solution to the bonus question, please upload one ZIP file containing the source code and the solution in PDF.

References

[KL21] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography: Principles and Protocols*. CRC Press, 3rd edition, 2021.