Advanced cryptography: Cloud & More, winter 2013/14

MICHAEL NÜSKEN

9. Exercise sheet
Hand in solutions until Wednesday, 22 January 2014, 23:59

Exercise 9.1 (Zero-Knowledge). (12 points)

Read Quisquater, Quisquater, Quisquater, Quisquater, Guillou, Guillou, Guillou, Guillou, Guillou, Guillou & Berson (1989) to one of your children. Alternatively take one of your fellow students.

(i) Write down the protocol in a form appropriate for computer science students rather than for children. [4]

(ii) Prove for this protocol the following three properties:

- Completeness: If the prover's claim is true, the verification returns true — always. [2]
- Soundness: If the prover's claim is false, the verification fails — with high probability. [2]
- Zero-knowledge: The verifier does not learn anything about the private information. [4]

Exercise 9.2 (Usage of $\mathcal{ZK}$). (8+3 points)

There is a theorem that says that for any (first-order) logical statement φ there is a zero-knowledge proof where PAULA claims the truth of φ and convinces VICTOR of that without revealing a truth assigment to the variables occuring in φ.

(i) Explain how to use that to indentify PAULA under the assumption that VICTOR has her certificate including, say, a public ElGamal encryption key. [4]

Why is this approach problematic? [+3]

(ii) What kind of statement should the cloud prove to the user regarding verifiability of a computation? [4]

Exercise 9.3 ($\mathcal{NP} \subseteq \mathcal{IP}$). (4 points)

Let X be a problem (language) in $\mathcal{NP}$. Describe a one-round interactive proof for it and show that it is complete and sound. 4

Note: The previous proof cannot be (computational) zero-knowledge. To achieve that you would need a commitment scheme, a zero-knowledge proof for one NP-complete problem and a stronger reduction notion than usual to enable transforming problems to the reference problem (as usual) and back (this is the extra).

References

JEAN-JACQUES QUISQUATER, MYRIAM QUISQUATER, MURIEL QUISQUATER, MICHAËL QUISQUATER, LOUIS GUILLOU, MARIE ANNICK GUILLOU, GAÏD GUILLOU, ANNA GUILLOU, GWENDOLÉ GUILLOU, SOAZIG GUILLOU & TOM BERSON (1989). How to Explain Zero-Knowlegde Protocols to Your Children. In *Advances in Cryptology: Proceedings of CRYPTO 1989*, Santa Barbara, CA, number 435 in Lecture Notes in Computer Science, 628–631. Springer-Verlag. ISSN 0302-9743. URL `http://dx.doi.org/10.1007/0-387-34805-0_60`.