Monash University
FIT 5124: Advanced Topics in Security
Week 7 Tutorial Sheet

Ron Steinfeld, 22 April 2015

In this week's tutorial we will look at some aspects of Zero Knowledge (ZK) Proofs and their applications.

Problems

1 **OR Composition of ZK 'Sigma' protocols.** Generalize the 1-of-2 OR combination method for ZK 'Sigma' protocols to a 1-of-ℓ combination for any ℓ. Using this method, give a ZK proof protocol for the relation

$$R_{(1,\ell)} = \{(h_1, \ldots, h_\ell; x) : \exists i \in [\ell] : h_i = g^x\}.$$

2 **Application to Build Revocable Anonymous Identification.** Anonymous identification protocols allow a user who belongs to a group of N users to prove that he belongs to the group, without reveaing his identity within the group. On the other hand, in a *revocable* anonymous identification protocol, if a user 'misbehaves', the user's identity can be revealed (thus revoking the user's anonymity) by a trusted authority called a group manager.

(a) Show how to combine the 1-of-ℓ OR method from problem (2) with the EQ and AND combining methods (see Schoenmaker's lecture notes Chapter 5) to construct a ZK proof protocol for the relation

$$R'_{(1,\ell)} = \{((A, B, h_0, h_1, \ldots, h_\ell); (u, x)) : A = g^u, B = h_0^u g^x, \exists i \in [\ell] : h_i = g^x\}.$$

(b) Explain how to apply this protocol to construct a revocable anonymous identification protocol. Explain: (1) Why it is infeasible for a malicious misbehaving user in this protocol to prevent the group manager from revealing the user's identity, using a recorded successful identification conversation for this user recorded by an honest verifier. (2) Why it is infeasible for a verifier to impersonate as a user after observing the protocol responses from the user. (3) Is this protocol secure against a cheating *group manager* that tries to frame a user, and why?

(c) Read about the *group signature* variant of the above group identification protocol, as described in pages 57-58 of Schoenmaker's lecture notes (see link on Moodle). Explain how this signature variant defends against a cheating group manager that tries to frame a user.

3 **Other Applications of ZK proofs.** Read about and explore other applications of ZK proofs, such as anonymous credentials and anonymous e-cash. A starting point is the presentation available at https://courses.engr.illinois.edu/cs598man/fa2009/slides/AC-F09-Lect19-20.pdf, and the references referred to there, and the IBM 'Identity Mixer' site, at http://www.zurich.ibm.com/idemix/.