Comments on Hlinovsky's survey "Zero Knowledge Proofs of Identity and Proofs of Knowledge".

Lauri Tarkkala

October 17, 2001

1 Introduction

I have a mostly cosmetic gripe with the introduction section. The section basically does not state anything incorrect. The motivation for using zero knowledge protocols in authentication schemes is correct as such, but the zero knowledge protocol of identity presented has one minor "feature".

The Feige-Fiat-Shamir protocol requires at least three participants, Victor the verifier, Peggy the prover and Trent the trusted third party. Trent is relied on to create and publish the Blum integer n, and neither Peggy nor Victor should know the factors of n.

If Victor knows the factors of n, the protocol is not zero-knowledge and the secret can be broken.

If Peggy knows the factors of n, he can act as a malicious verifier towards an unsuspecting Peggy-Prime, and discover the secret.

The obvious solution for deploying the protocol in an authentication scheme without Trent is to have a separate n for each 'Peggy,Victor' which is generated by Victor. This has the obvious implication that Victor can only proove herself to Peggy and no others, and as such the fact that Peggy learns nothing from the proof is of dimnished value.

This makes the Feige-Fiat-Shamir protocol unusable for use in a 'web-of-trust' environment such as PGP or an environment requiring 'leaps of faith'-style enrollment such as the SSH protocol.

This can also present some interesting logistical problems, as n must be known by Peggy at the time of key-generation.

These are not problems with all zero-knowledge protocols, but as the only protocol presented in the paper, I feel that it might have been prudent to mention these features, especially as zero knowledge proofs of identity where contrasted to other schemes.

The section otherwise provides a nice and brief introduction to the survey.

2 Proofs of knowledge

The definition of an interactive proof system of knowledge is slightly clumsy and in my opinion incomplete. I personally had trouble understanding what "There exists an M (with complete control over cheater P') actually means.

Does this mean that M actually places characters on the private and common tapes of P' at will (and hence there is no need for a separate P' in the definition) or does it mean that M merely controls the inputs to P' and would this include the coin-tosses P' makes as it is a probabilistic machine.

I ended up guessing at this point in the survey, and unfortunately had a slightly unsecure feeling reading the rest of the results in the survey.

This section also omitted defining the difference between a proof of knowledge and a proof identity. The section does however enlighten the reader to the subtleties and problems involved in defining knowledge briefly, but one is left wondering how these differ from a proof of knowledge.

The obvious conclusion could be that proofs of identity are those where the proof system has a public key which the prover can publish prior to the verification, but then the question arises that can all proofs of knowledge be adapted into proofs of identity (or is this an open problem?).

3 Feige-Fiat-Shamir identitication scheme

The section states that the Feige-Fiat-Shamir protocol is two or four orders of magnitude of faster than RSA-based identity schemes. This is a dubious statement at best.

The performance of RSA is related directly to one parameter, which is the size of the primes used to generate the modulus.

The performance of the Feige-Fiat-Shamir identification scheme is related to several parameters: the size of the primes used to generate the modulus, the number of secret/public random number pairs k and the number of rounds the protocol is executed t.

The size of n must be same as for a RSA protocol, as they both depend on the difficulty of factoring it. The security parameters k and t should be configured such that factoring the modulus can not be done with effort less than 2^{tk} mystical operations.

Assuming that a 1024-bit modulus n could be factored with effort relative to 2^{100}. This would assume values for k and t such that $kt > 100$.

The statement regarding the performance of the Feige-Fiat-Shamir scheme hence seems quite unclear. A noteworthy point though, is that the Feige-Fiat-Shamir protocol would suffer less than a RSA-based scheme from an increase in modulus length required if some new marginal improvements to factoring techniques were discovered (if better than marginal improvements are discovered, then the situation is obviously different).

I also might want to comment on the notation used in step 2 of the key generation. The meaning I derived is $(-1)^b S_j^{-2} \bmod 2$, in the notation I am familiar with. The modulus could at least have been stated. The rest of the survey did make the meaning clear.

The proof of the protocol being an interactive proof system and zero-knowledge is readable and understandable, with one exception. I had a slight problem in relating it to the definition of zero-knowledge in the previous section.

The machine M is said to be probabilistic polynomial time. This is obviously in regard to the input, and the size of the messages $\mathcal{O}(2^k)$ is considered constant. k however is defined by the key, and chosen by the prover. I am personally not convinced by the fact, that the simulation can produce with indistinguishable probability distribution the requested view, if the keysize is not previously known (hence contradicting the definition). Fixing the k to a constant for all keys obviously corrects this.

4 Conclusion

The survey is a good walk-through of the Feige-Fiat-Sahmir identification scheme. A nice background and context for evaluating the protocol is shown, and it's place in this context is proven in a readable manner.

The survey contained some minor quirks, but in my opinion these were minor fallacies (as they could be noticed by a reader of my limited understanding $;-)$, and overall the survey was good.