# The ZK-SSH Project
# The Zero-Knowledge Identification Protocol

Andreas Gaupmann Christian Schausberger Ulrich Zehl

September 7, 2005

## Contents



# 1 The Ohta-Okamoto Zero-Knowledge Identification Protocol

The zero-knowledge protocol used by the ZK-SSH project is due to Ohta and Okamoto [OO88]. It is a modification and generalization of the well-known Fiat-Shamir scheme [FS86], but has one crucial advantage: It is, to the best of our knowledge, not encumbered by patents.

Ohta and Okatomo present a sequential version in some detail, and discuss the security of a parallel scheme, but they do not present the parallel protocol's actions. Therefore, we will do this ourselves.

## 1.1 Setup

A prover P chooses a RSA-like modulus $n$ (the product of two secret large primes) and $k$ random integers $S_i \in \mathbb{Z}_n$ as his private identity keys, and a small integer $L$. His overall private key is $((S_1, \ldots, S_k), n, L)$.

P now computes his public identity keys $I_i = {S_i}^L$ for all $1 \leq i \leq k$, and publishes $((I_1, \ldots, I_k), n, L)$ as his overall public identity key.

## 1.2 Proof of Identity and Verification

The proving party P wants to prove their purported identity to the verifying party V. To do this, the following protocol is carried out over $t$ rounds until V is convinced of the correctness.

1. P chooses a random $R \in \mathbb{Z}_n$ and sends the witness $X = R^L$ to V.
2. V picks $(e_1, \ldots, e_k) \in \mathbb{Z}_L$ at random, and sends the resulting challenge vector to P.

3. P computes Y as

$$Y = R \cdot \prod_{j=1}^{k} (S_j)^{e_j} \pmod{n}$$

and sends Y as his response.

4. V accepts the round iff the following equation holds.

$$Y^L = X \cdot \prod_{j=1}^{k} (I_j)^{e_j} \pmod{n}$$

After $t$ successful rounds, V accepts the proof. The probability that a cheating prover can successfully fool an honest verifier is then only $L^{-kt}$, a significant gain over the sequential protocol's $L^{-t}$.

## 2 Concrete Parameters

In the ZK-SSH project, we will work in a remote attacher scenario where no reasonable assumptions about his power—beyond being polynomially bounded—are possible. Therefore, the probability that a cheater can successfully fool an honest verifier should be

$$\frac{1}{2^{80}}$$

or less.

Chosing $L := 4$, $k := 10$ as the number of secret identitiy keys, and $t := 4$ as the number of rounds and substituting in the respective equations yields

$$\left(\frac{1}{4}\right)^{10 \cdot 4} = \left(\left(\frac{1}{2}\right)^{2}\right)^{40} = \left(\frac{1}{2}\right)^{80}$$

which statisfies the above requirement.

For the length of the modulus $n$, we propose to use at least 2048 bits to have a margin of security for future developments in factorization and cryptanalysis.

## References


[FS86] Amos Fiat and Adi Shamir, *How to prove yourself: Practical solutions to identification and signature problems*, Advances in Cryptology – CRYPTO 1986 (Andrew M. Odlyzko, ed.), Lecture Notes in Computer Science, vol. 263, Springer, 1986, pp. 186–194.

[OO88] Kazuo Ohta and Tatsuaki Okamoto, *A modification of the Fiat-Shamir scheme*, Advances in Cryptology – CRYPTO 1988 (Shafi Goldwasser, ed.), Lecture Notes in Computer Science, vol. 403, Springer, 1988, pp. 232–243.