Feige-Fiat-Shamir Identification Scheme

Ivan Gorbunov & Vsevolod Nagibin & Nikita Andrusov
MIPT

May 2024

1 Introduction

This document contains a description of an identification scheme originally presented by Uriel Feige, Amos Fiat and Adi Shamir in 1988 [1]. The scheme is a zero-knowledge proof allowing one party, the Prover, to prove to another party, the Verifier, that they possess secret information without revealing the secret itself. Due to such wonderful properties, the scheme is incredibly useful in cryptography.

2 Interaction Protocol

The scheme assumes the existence of a trusted centre, whose only purpose is to publish a modulus N which is a Blum integer (a product of two prime numbers of the form $4k+3$). No one else should know the factorization of N.

At first, Prover generates a private and a public key:

- Choose k random numbers S_1 ... S_k in $\mathbb{Z}_n$
- Choose each I_j (randomly and independently) as $\pm\frac{1}{S_j^2}(modN)$
- Publish $I_1...I_k$ and keep $S_1...S_k$ secret

Prover will try to convince the Verifier that he possesses the square roots of I_j, and the S_j are hidden by the difficulty of extracting square roots.

The following protocol is a proof of identity (which is repeated t times)

- Prover picks random $R \in \mathbb{Z}_n$ and sends $X = \pm R^2(modN)$
- Verifier picks random boolean vector $(E_1...E_k)$
- Prover sends the value $Y = R \cdot \Pi_{E_j=1} S_j(modN)$
- Verifier checks that $X = \pm Y^2 \cdot \Pi_{E_j=1} I_j(modN)$

If all the t Verifier's checks were successful, he accepts the proof.

The following theorem was proved by Feige, Fiat and Shamir, showing that the protocol has the desired properties.

Theorem 1. *The above protocol is an unrestricted input zero knowledge relative to a trusted center, for $k = O(\log\log N)$ and $t = \Theta(\log N)$.*

References

[1] Uriel Feige, Amos Fiat & Adi Shamir — ”Zero-knowledge proofs of identity”