DLP Zero-Knowledge Identification Protocol with Multichallenges

Sergey Hovhannisyan
State Engineering University of Armenia
Yerevan, Armenia
Email: ogser@seua.am

Ashot Khachaturov
State Engineering University of Armenia
Yerevan, Armenia
Email: ashotian@gmail.com

ABSTRACT

A DLP (discrete logarithmic problem) zero-knowledge protocol with multichallenges is presented. The protocol is base on computational impossibility of finding discrete logarithm, where the base is a primitive (generating) element of the multiplicative group.

Keywords

Zero-knowledge identification protocol, cryptography, information security, multichallenge, discrete logarithm problem, probability of forgery.

1. INTRODACTION

A disadvantage of simple password protocols is that when a claimant A gives the verifier B her password, B can later impersonate A. Challenge-response protocols are improved on this issue, though they might reveal some partial information about the claimant's secret [1].

Zero-knowledge (ZK) protocols are designed to address these concerns of revealing some partial information about the claimant's secret, by allowing a prover to demonstrate knowledge of a secret while revealing no information whatsoever (beyond what the protocol run) of use to the verifier in conveying this demonstration of knowledge to others. The point is that only a single bit of information need be conveyed-namely, that the prover actually does know the secret [2].

More generally, a zero-knowledge protocol allows a proof of the truth of an assertion, while

conveying no information whatsoever (this notion can be quantified in a rigorous sense) about the assertion itself other than its actual truth. In this sense, a zero-knowledge proof is similar to answer obtained from a (trusted) *oracle*.

2. PROTOCOL DESCRIPTION

Let us describe the general idea of the new zero-knowledge identification protocol with multichallenges.

The objective is for A to identify itself by proving knowledge of a secret $\mathbf{s} = (s_1, s_2, \ldots, s_k)$ (associated with A through authentic public data) to any verifier B, without revealing any information about **s** not known or computable by B prior to execution of the protocol. The security relies on the difficulty of finding discrete logarithmic value, belonging to the multiplication group of, $Z^*{}_p$ where p is a prime number.

The challenge (or exam) $\mathbf{e} = (e_1, e_2, \ldots, e_k)$ requires that A be capable of answering two these questions, one of which demonstrates her knowledge of the secret **s** and the other on easy question (for honest provers) to prevent cheating. An adversary impersonating A might try to cheat by selecting any y^* and setting $x = \alpha^{y^*} / v$, where α and v are public data, then answering the challenge $\mathbf{e} = 1$ with the correct answer $\mathbf{e} = 0$ which requires knowing a discrete logarithm of $\mathbf{x} \bmod \mathbf{p}$. Prover A knowing $\mathbf{s}$ can answer both questions, but otherwise can at best answer one of the two questions, and so had probability only $1/2$ of escaping detection.

To decrease the probability of cheating arbitrarily to an acceptable small value of 2^{-tk}, the protocol is iterated $\mathbf{t}$ times, with B accepting A's identity only if all $\mathbf{t}$ questions are successfully answered.

A must respond to at most one challenge (question) for a given witness, and shouldn't reuse any witness; in many protocols security may be compromised if either of these conditions is violated.

The security relies on the difficulty of solving discrete logarithm problem (DLP); given a prime $\mathbf{p}$, a generator, α of $Z^*{}_p$, and an element $\beta \in Z^*{}_p$ find the integer x, $0 \le x \le p-2$ such that $\alpha^x \equiv \beta \bmod p$.

3. MULTICHALLENGES PROTOCOL STEPS

Summary: A proves knowledge of $\mathbf{s}$ to B in $\mathbf{t}$ execution of a 3 pass protocol.

1. One-time setup.

a) A trusted center T selects a large random prime $\mathbf{p}$ and generator α of the multiplicative group $Z^*{}_p$ of the integers modulo $\mathbf{p}$.

b) Each claimant A selects k random integers $s_1, s_2, \ldots, s_k$ in the range $1 \le s_i \le p-1$ and computes $v_i = \alpha^{s_i} \bmod p_i$ for $1 \le i \le k$.

c) As public key is $(p, \alpha, \bar{v})$, where $\bar{v} = \{v_1, v_2, \ldots, v_k\}$. A's private key is $\bar{s}$, where $\bar{s} = \{s_1, s_2, \ldots, s_k\}$.

2. Protocol messages: Each of $\mathbf{t}$ rounds has three messages with from as follows.

$A \to B$	$x = \alpha^r \bmod p$ witness
$A \leftarrow B$	$\{e_1, e_2, \ldots, e_r\}$ $\quad e_i \in \{0,1\}$
$A \to B$	$y = r + \sum_{i=1}^{k} s_i e_i \bmod p$

3. Protocol actions. The following steps are iterated $\mathbf{t}$ times (sequentially and independently). B accepts the proof if all rounds succeed.

a) A choose a random (commitment) $\mathbf{r}$, $1 \le r \le p-1$ and sends (the witness) $x = \alpha^r \bmod p$ to B.

b) B randomly selects multichallenge

$$e = \{e_1, e_2, \ldots, e_k\}$$

$$e_i \in \{0,1\} \text{ for } 1 \le i \le k$$

c) A computes and sends to B (response) y.

$$\overline{y} = r + \sum_{i=1}^{k} e_i s_i$$

d) B accepts upon verifying $x \cdot \prod_{i=1}^{k} v_i^{e_i} = \alpha^y$

Protocol is provably secure against chosen message attack and the best attack has a probability of forgery 2^{-tk} .

4. CONCLUSION

From theoretical point of view the derived result is of some great interest, but is not applicable on device with low-powered processing units (ex. chip card processors)

REFERENCES

[1] A. Menezes, P. Van Orschot, and S. Vanstone, “Handbook Applied Cryptography”, CRC Press, 1997.

[2] U.Feige, A. Fiat, A. Shamir, “Zero-Knowledge proofs of identity”, Journal of Cryptography 1, 77-94, 1990.

[3] Hovhannisyan S., Ghazaryan H. “DLP Zero-Knowledge identification protocol” Proceeding of the Computer Science and Information Technologies, Conference Yerevan p 312-322 2007