An Interactive Proof Based Identification and Signature Scheme Using Euler's Totient Function

DaeHun Nyang
Dept. of Computer Science
Yonsei University
Seoul, 120-749 Korea
Email nyang@emerald.yonsei.ac.kr

JooSeok Song
Dept. of Computer Science
Yonsei University
Seoul, 120-749 Korea
Email jssong@emerald.yonsei.ac.kr

Abstract — **Zero-knowledge interactive proof is a useful tool for designing identification and digital signature schemes. In this paper, we propose a new interactive proof based identification and signature scheme.**

I. Introduction

Since 1984, considerable attention has been paid to ZKIP, which is useful in identification and digital signature[1]. In this paper, we propose a new interactive proof based identification scheme and digital signature. The scheme uses discrete logarithm over the ring Z/nZ and Euler's totient function to get its security. A prover keeps a signed subgroup generator provided by a trusted center as its secret information.

II. Interactive Identification Scheme

Our interactive protocol is a proof of knowledge of a predicate

$$P(s,x) = [s^x \equiv g \bmod pq],$$

where $\gcd(x, \lambda(pq)) = 1$, and g is a generator of a subgroup of $Z/nZ(\lambda$ is the Carmichael function). Like other identification schemes, our protocol is composed of two phases. The first phase is the smart card issuing step, and the second is interactive proof.

A trusted center randomly chooses two large primes, p and q. The two primes are kept securely by the trusted center. We assume that the factorization of $n = pq$ is infeasible. Another public value g is also chosen by the trusted center. g is a generator of a sufficiently large subgroup of Z/nZ. It should be selected by the trusted center to satisfy $g^k \equiv 1 \bmod n$ where k is the order of g mod n. The trusted center publishes $(n = pq, g)$ in the public directory, which will be shared among a group of users. When an eligible user applies for a smart card, the trusted center issues a string I which contains information about the user and the card. And now the trusted center performs the following steps to compute the secret information s_i and a public-key v_i for user i.

1. For a user i who requests a trusted center of its secret value, the trusted center chooses v_i, where v_i is a prime and $\gcd(v_i, \lambda(n)) = 1$.
2. The center computes $s_i \equiv g^{1/v_i} \bmod n$. s_i can be easily obtained by computing $g^{d_i} \bmod n$ where $v_i d_i \equiv 1 \bmod \phi(n)$.
3. The center generates a signature $S = signature(I, v_i)$, and the certificate $C(\text{User } i) = (I, v_i, S)$.
4. A smart card containing the user's certificate is issued.

After the preparatory steps, a prover has a secret number s_i and can prove its identity to a verifier by the following interactive proof.

1. Prover sends its certificate $C(\text{Prover})$ to Verifier.
2. Verifier checks Prover's $C(\text{Prover}) = (I, v_i, S)$.
3. Prover picks a random number $r \in \{2, \ldots, n-1\}$ and sends $x \equiv r^{v_i} \bmod n$ as a test to Verifier.
4. Verifier sends a random number $e \in \{1, \ldots, 2^t\}$ as a question to Prover, where $2^t < v_i$. The size of 2^t represents a compromise between speed and security.
5. Prover sends to Verifier as a witness: $y \equiv r s_i^e \bmod n$
6. Verifier checks that $x \equiv y^{v_i} g^{-e} \bmod n$ and accepts the proof as valid only when the above result is correct.

Using an interactive proof based identification scheme and a hash function, one can construct a secure digital signature scheme[2]. Switching the identification scheme to a signature scheme, we replace the verifier's role by the hash function h.

III. Performance Evaluation

In the identification protocol and the signature scheme, precomputations reduce the verifier's burden as well as the prover's. A prover can pre-compute the value $x \equiv r^{v_i} \bmod n$ in its idle time. Also a verifier can prepare $g^{-e} \bmod n$ in advance.

# of mult.	Prover	Verifier	# of bytes(x, e, y)
Fiat-Shamir	t(k+2)/2	t(k+2)/2	12 + 3 + 256
Schnorr	1	$1.5t + 0.25t$	3 + 3 + 17.5
GQ	$1.5t$	$3t$	3 + 3 + 64
Our Scheme	$1.5t$	$1.5t$	3 + 3 + 64

Tab. 1: Comparison with the other schemes

Comparisons with other schemes in terms of the number of multiplications and the required storage amount are shown in Table 1(t and k are the security parameters in [2].).

IV. Conclusion

The scheme in the paper is very efficient both in verification and in proving steps owing to the pre-computable protocol structure. The interactive proof system proposed in this paper will be a primitive building block of various protocols such as payment protocols of digital cash, authentications in personal communications systems, and cookies in world wide web.

References

[1] S. Goldwasser, S. Micali, and C. Rackoff, The knowledge complexity of interactive proof systems, Proc. 17th Annual ACM Symp. Theory of Computing, (1986) pp. 291–304.

[2] Amos Fiat and Adi Shamir, How To Prove Yourself: Practical Solutions to Identification and Signature Problems, Advances in Cryptology : Proceedings of Crypto 86, Lecture Notes in Computer Science, Springer-Verlag, New York, (1987) pp. 186–194.

0-7803-5000-6/98/$10.00 © 1998 IEEE.