Efficient Identification and Signatures for Smart Cards[1]

C.P. Schnorr

Universität Frankfurt

Abstract[2]

We present an efficient interactive identification scheme and a related signature scheme that are based on discrete logarithms and which are particularly suited for smart cards. Previous cryptosystems, based on the discrete logarithm, have been proposed by El Gamal (1985), Chaum, Evertse, van de Graaf (1988), Beth (1988) and Günther (1989). The new scheme comprises the following novel features.

1. We propose an efficient algorithm to preprocess the exponentiation of random numbers. This preprocessing makes signature generation very fast. It also improves the efficiency of the other discrete log-cryptosystems. The preprocessing algorithm is based on two fundamental principles *local randomization* and *internal randomization.*

2. We use a prime modulus p such that $p-1$ has a prime factor q of appropriate size (e.g. 140 bits long) and we use a base α for the discrete logarithm such that $\alpha^q = 1 (\mathrm{mod} p)$. All logarithms are calculated modulo q. The length of the signatures is about 212 bits, i.e. it is less than half the length of RSA and Fiat-Shamir signatures. The number of communication bits of the identification scheme is less than half that of other schemes.

---

[1] European patent application 89103290.6 from 24.2.1989.

[2] Extended abstract: C.P. Schnorr, "Efficient Identification and Signatures for Smart Cards", *Advances in Cryptology: Proceedings of CRYPTO '89 (Lecture Notes in Computer Science; 435)*, G. Brassard, Ed., Springer Verlag, 1990, pp. 239–252.

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 688-689, 1990.

The new scheme minimizes the work to be done by the smart card for generating a signature or for proving its identity. This is important since the power of current processors for smart cards is rather limited. Previous signature schemes require many modular multiplications for signature generation. In the new scheme signature generation costs about 12 modular multiplications, and these multiplications do not depend on the message/identification, i.e. they can be done in preprocessing mode during idle time of the processor.

The security of the scheme relies on the one-way property of the exponentiation $y \longrightarrow \alpha^y (\bmod p)$, i.e. we assume that discrete logarithms with base α are difficult to compute. The security of the preprocessing is established by information theoretic arguments.