Schnorr signature

From Wikipedia, the free encyclopedia

In cryptography, a **Schnorr signature** is a digital signature produced by the Schnorr signature algorithm. Its security is based on the intractability of certain discrete logarithm problems. It is considered the simplest digital signature scheme to be provably secure in a random oracle model. It is efficient and generates short signatures. It is covered by U.S. Patent 4,995,082 (http://www.google.com/patents?vid=4995082) , which expired in February 2008.

Contents

Algorithm

Choosing parameters

- All users of the signature scheme agree on a group G with generator g of prime order q in which the discrete log problem is hard. Typically a Schnorr group is used.
- All users agree on a cryptographic hash function H.

Key generation

- Choose a private key x such that $0 < x < q$.
- The public key is y where $y = g^x$.

Signing

To sign a message M:

- Choose a random k such that $0 < k < q$
- Let $r = g^k$
- Let $e = H(M||r)$, (where || denotes concatenation)
- Let $s = (k - xe) \bmod q$

The signature is the pair (e,s). Note that $0 \leq e < q$ and $0 \leq s < q$; if a Schnorr group is used and $q < 2^{160}$, then the signature can fit into 40 bytes.

Verifying

- Let $r_v = g^s y^e$
- Let $e_v = H(M||r_v)$

If $e_v = e$ then the signature is verified.

Public elements: G,g,q,y,s,e,r. Private elements: k,x.

See also

- DSA
- ElGamal signature scheme

References

- C.P. Schnorr, Efficient identification and signatures for smart cards, in G. Brassard, ed. Advances in Cryptology—Crypto '89, 239-252, Springer-Verlag, 1990. Lecture Notes in Computer Science, nr 435
- Claus-Peter Schnorr, Efficient Signature Generation by Smart Cards, J. Cryptology 4(3), pp161–174 (1991) (PS) (http://www.mi.informatik.uni-frankfurt.de/research/papers/schnorr.smartcardsig.1991.ps) .
- Menezes, Alfred J. et al. *Handbook of Applied Cryptography* CRC Press. 1996.