Schnorr's Protocol

Author(s): C. P. Schnorr 1991

Summary: The Schnorr protocol is described by R. Cramer, I. Damgård and B. Schoenmakers in [CDS94].

Protocol specification (in common syntax)

```
A, B :             principal
Na, Nb :           fresh number
Sa :               private key
Pa = exp(g,Sa) :   public key
```

```
A chooses Na and computes a = exp(g,Na)

 1.    A  ->  B   :     a

B chooses Nb

 2.    B  ->  A   :     Nb

A computes r = Na + Nb × Sa

 3.    A  ->  B   :     r

B checks that exp(g, r) = a × exp(Pa,Nb)
```

Description of the protocol rules

A zero-knowledge protocol is designed for convincing the verifier of the validity of a given statement, without releasing any knowledge beyond the validity of the statement. This concept was introduced in [GMR85]. An overview can be found in [Gol01]. We present the Schnorr protocol which is described by R. Cramer, I. Damgård and B. Schoenmakers in [CDS94] and which uses this method.

The `+`, × and `exp` symbols denote respectively addition, multiplication and modular exponentiation.

Details of the computation done by `B` at the last step of the protocol:

```
    a × exp(Pa,Nb)
 =  exp(g,Na) × exp(exp(g,Sa),Nb)
 =  exp(g,Na) × exp(g,Sa × Nb)
 =  exp(g,Na + Sa × Nb)
 =  exp(g, r)
```

Requirements

A wants to prove his identity to B by showing him that he knows Sa without revealing it.

References

[CDS94]

Citations

[CDS94] R. Cramer, I. Damgård, and B. Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *Proc. 14th Annual International Cryptology Conference (CRYPTO'94)*, volume 963 of *LNCS*, pages 174–187, Santa Barbara (California, USA), 1994. Springer-Verlag.

[GMR85] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. In *Proc. 17th annual ACM Symposium on Theory of Computing*, pages 291–304. ACM Press, 1985.

[Gol01] O. Goldreich. *Foundations of Cryptography.* Cambridge University Press, 2001.