This is not an issue with traditional certificates. However, whenever implicit certificates are used to authenticate a public key for some application, a specific security proof for the particular application is necessary. For example, in [2], a proof is given in the random oracle model that it is secure to use implicit certificates as authentication for public keys that verify Schnorr signatures.

9 Acknowledgments

We would like to thank Simon Blake-Wilson for his ideas on the general concepts. We also would like to thank Mingua Qu for reviewing the security proofs and for pointing out the special security issues that arise in the context of implicit certificates.

10 Summary

Based upon various secret sharing primitives and Schnorr's signature scheme, we have presented an implicit certificate scheme, a (t, n) threshold signature scheme, and a (t, n) threshold scheme for implicit certificates. All schemes are efficient, robust and provably secure in the random oracle model.

From a practical point of view, implicit certificate schemes have the following drawbacks. We suggest these points as open research problems.

- The implicit certificate schemes itself generate a key pair for the user. Therefore, the schemes cannot be used to generate a public reconstruction data for a given key pair of the user. To the best of our knowledge, no scheme based on the elliptic curve discrete logarithm problem exists that can issue an implicit certificate for a given key pair.
- The implicit certificate schemes produce a key pair which is defined over the same group as the CA's key pair is. Therefore, the security parameters for the certified public keys are always inherited from the certifying CA. This might not always be desirable in practice.

[1] M. Bellare and P. Rogaway. Random oracles are practical: a paradigm for designing efficient protocols. In *First Annual ACM Conference on Computer and Communications Security*, pages 62–73, 1993.

[2] D. Brown. Implicitly certifying signatures securely. manuscript.

[3] R. Gallant D. Brown and S. Vanstone. Provably secure implicit certificate schemes. In *Proc. Financial Cryptography '01*, to appear.

[4] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In *Proc. 28th FOCS*, pages 427–437, 1987.

[5] C. Park and K. Kurosawa. New elgamal type threshold digital signature scheme. *IEICE Trans.*, E79-A:86–93, 1996.