Provably Secure Distributed Schnorr Signatures and a (t, n) Threshold Scheme for Implicit Certificates

D.R. Stinson and R. Strobl
Certicom Corporation
5520 Explorer Drive
Mississauga ON, L4W 5L1
Canada

January 23, 2001

Abstract

In a (t, n) threshold digital signature scheme, t out of n signers must co-operate to issue a signature. We present an efficient and robust (t, n) threshold version of Schnorr's signature scheme. We prove it to be as secure as Schnorr's signature scheme: i.e., existentially unforgeable under adaptively chosen message attacks. The signature scheme is then incorporated into a (t, n) threshold scheme for implicit certificates. We prove the implicit certificate scheme to be as secure as the distributed Schnorr signature scheme.

1 Introduction

Traditional certificates contain a signature on some data, usually a public key and an identity string. To issue a traditional certificate, a Certification Authority (CA) first verifies the authenticity of this data and then simply issues a digital signature on it. The certificate is therefore as secure as the signature scheme: certificates cannot be forged because signatures cannot be forged.

When issuing implicit certificates, the situation is somewhat different. Implicit certificates also contain some data, usually some public reconstruction data and an identity string, but no public key or signature. The public key itself must be computed from the public reconstruction data and the public key of the CA who issued the certificate. Clearly, the advantage of implicit certificates is their size: they only contain some public reconstruction data, where as traditional certificates contain instead a public key and a digital signature. A survey of various types of implicit certificates is given in [9].

In contrast to traditional certificates, where the security lies directly on the underlying signature scheme, there are special security issues concerning implicit certificates. In general, any public reconstruction data and identity string, together with a CA's public key, would yield a public key. However, it should be hard to choose the public reconstruction data and compute the private key corresponding to the implied public key, without knowing the CA's private key. Another issue is that – since one usually uses a slightly