modified signature scheme to issue a certificate – one has to make sure that no information about the CA's or the user's private key is leaked.

We first present a distributed Schnorr signature scheme and prove it to be as secure as the non distributed version, i.e., existentially unforgeable under adaptively chosen message attacks. Second, this scheme is incorporated into the construction of a distributed implicit certificate scheme.

Our digital signature threshold scheme is based on two primitives: Pederson's Verifiable Secret Sharing Scheme and Pederson's multi-party protocol to generate a random shared secret [8, 6]. These primitives are briefly discussed in Section 2. In Section 3 we recall Schnorr's signature scheme [12]. Then we propose in Section 4 a (t, n) threshold version of this signature scheme. We prove the security of the scheme in Section 5, adapting the proof techniques used in [5]. The non-distributed implicit certificate scheme is introduced in Section 6. The (t, n) threshold version of this scheme is presented in Section 7, and a security proof is presented in Section 8.

In all proofs, we use the random oracle model as described in [1]. For all protocols we assume a synchronous communication model, where all players are connected via private channels and a global broadcast channel.

2 Secret Sharing Schemes

2.1 Parameters

We use elliptic curve notation for the discrete logarithm problem. Suppose q is a large prime and G, H are generators of a subgroup of order q of an elliptic curve E. We assume that E is chosen in such a way that the discrete logarithm problem in the subgroup generated by G is hard, so it is infeasible to compute the integer d such that $G = dH$.

2.2 Shamir's Secret Sharing Scheme

In a (t, n) secret sharing scheme, a dealer distributes a secret s to n players $P_1, \cdots, P_n$ in such a way that any group of at least t players can reconstruct the secret s, while any group of less than t players do not get any information about s. In [13], Shamir proposes a (t, n) threshold secret sharing scheme as follows. In order to distribute $s \in Z_q$ among $P_1, ..., P_n$ (where $n < q$), the dealer chooses a random polynomial f over Z_q of degree at most $t - 1$ satisfying $f(0) = s$. Each participant P_i receives $s_i = f(i)$ as his share.

There is one and only one polynomial of degree at most $t - 1$ satisfying $f(i) = s_i$ for t values of i. Therefore, an arbitrary group $\mathcal{P}$ of t participants can reconstruct the polynomial $f()$ by using Lagrange's interpolation formula:

$$f(u) = \sum_{i \in \mathcal{P}} f(i)\omega_i(u) \ , \text{ where } \ \omega_i(u) = \prod_{\substack{j \in \mathcal{P} \\ j \neq i}} \frac{u - j}{i - j} \bmod q.$$

Since it holds that $s = f(0)$, the group $\mathcal{P}$ can reconstruct the secret directly, using the formula

$$s = f(0) = \sum_{i \in \mathcal{P}} f(i)\omega_i \ , \text{ where } \ \omega_i = \omega_i(0) = \prod_{\substack{j \in \mathcal{P} \\ j \neq i}} \frac{j}{j - i} \bmod q.$$