[6] T.P. Pedersen. Distributed provers with applications to undeniable signatures. *Lecture Notes in Computer Science (Eurocrypt '90)*, 473:221–238, 1991.

[7] T.P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. *Lecture Notes in Computer Science (Crypto '91)*, 576:129–140, 1992.

[8] T.P. Pedersen. A threshold cryptosystem without a trusted party. *Lecture Notes in Computer Science (Eurocrypt '91)*, 547:522–526, 1992.

[9] L. Pintsov and S. Vanstone. Postal revenue collection in the digital age. In *Proc. Financial Cryptography '00*, 2000.

[10] D. Pointcheval and J. Stern. Security proofs for signature schemes. *Lecture Notes in Computer Science (Eurocrypt '96)*, 1070:387–399, 1996.

[11] H. Krawczyk R. Gennaro, S. Jarecki and T. Rabin. Secure distributed key generation for discrete-log based cryptosystems. *Lecture Notes in Computer Science (Eurocrypt '99)*, 1592:295–310, 1999.

[12] C.P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4:161–174, 1991.

[13] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.