**LITERATURAL SUVERY**

**Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps**

An approach of membership revocation in group signatures is verifier-local revocation (VLR for short). In this approach, only verifiers are involved in the revocation mechanism, while signers have no involvement. Thus, since signers have no load, this approach is suitable for mobile environments. Although Boneh and Shacham recently proposed a VLR group signature scheme from bilinear maps, this scheme does not satisfy the backward unlikability. The backward unlikability means that even after a member is revoked, signatures produced by the member before the revocation remain anonymous. In this paper, we propose VLR group signature schemes with the backward unlinkability from bilinear maps.

**Group signatures with verifier-local revocation. Acm Conference on Computer & Communications Security**

Group signatures have recently become important for enabling privacy-preserving attestation in projects such as Microsoft's ngscb effort (formerly Palladium). Revocation is critical to the security of such systems. We construct a short group signature scheme that supports Verifier-Local Revocation (VLR). In this model, revocation messages are only sent to signature verifiers (as opposed to both signers and verifiers). Consequently there is no need to contact individual signers when some user is revoked. This model is appealing for systems providing attestation capabilities. Our signatures are as short as standard RSA signatures with comparable security. Security of our group signature (in the random oracle model) is based on the Strong Diffie-Hellman assumption and the Decision Linear assumption in bilinear groups. We give a precise model for VLR group signatures and discuss its implications.

**Wallet Databases with Observers**

Previously there have been essentially only two models for computers that people can use to handle ordinary consumer transactions: (1) the tamper-proof module, such as a smart card, that the person cannot modify or probe; and (2) the personal workstation whose inner working is totally under control of the individual. The first part of this article argues that a particular combination of these two kinds of mechanism can overcome the limitations of each alone, providing both security and correctness for organizations as well as privacy and even anonymity for individuals.

Then it is shown how this combined device, called a wallet, can carry a database containing personal information. The construction presented ensures that no single part of the device (i.e. neither the tamper-proof part nor the workstation) can learn the contents of the database — this information can only be recovered by the two parts together.

**Hierarchical Identity Based Encryption with Constant Size Ciphertext**

We present a Hierarchical Identity Based Encryption (HIBE) system where the ciphertext consists of just three group elements and decryption requires only two bilinear map computations, regardless of the hierarchy depth. Encryption is as efficient as in other HIBE systems. We prove that the scheme is selective-ID secure in the standard model and fully secure in the random oracle model. Our system has a number of applications: it gives very efficient forward secure public key and identity based cryptosystems (with short ciphertexts), it converts the NNL broadcast encryption system into an efficient public key broadcast system, and it provides an efficient mechanism for encrypting to the future. The system also supports limited delegation where users can be given restricted private keys that only allow delegation to bounded depth. The HIBE system can be modified to support sublinear size private keys at the cost of some ciphertext expansion.

**Constant-Size Commitments to Polynomials and Their Applications**

We introduce and formally define polynomial commitment schemes, and provide two efficient constructions. A polynomial commitment scheme allows a committer to commit to a polynomial with a short string that can be used by a verifier to confirm claimed evaluations of the committed polynomial. Although the homomorphic commitment schemes in the literature can be used to achieve this goal, the sizes of their commitments are linear in the degree of the committed polynomial. On the other hand, polynomial commitments in our schemes are of constant size (single elements). The overhead of opening a commitment is also constant; even opening multiple evaluations requires only a constant amount of communication overhead. Therefore, our schemes are useful tools to reduce the communication cost in cryptographic protocols. On that front, we apply our polynomial commitment schemes to four problems in cryptography: verifiable secret sharing, zero-knowledge sets, credentials and content extraction signatures.

**Verifiable Delegation of Computation over Large Datasets**

We study the problem of computing on large datasets that are stored on an untrusted server. We follow the approach of amortized verifiable computation introduced by Gennaro, Gentry, and Parno in CRYPTO 2010. We present the first practical verifiable computation scheme for high degree polynomial functions. Such functions can be used, for example, to make predictions based on polynomials fitted to a large number of sample points in an experiment. In addition to the many noncryptographic applications of delegating high degree polynomials, we use our verifiable computation scheme to obtain new solutions for verifiable keyword search, and proofs of retrievability. Our constructions are based on the DDH assumption and its variants, and achieve adaptive security, which was left as an open problem by Gennaro et al (albeit for general functionalities). Our second result is a primitive which we call a verifiable database (VDB). Here, a weak client outsources a large table to an untrusted server, and makes retrieval and update queries. For each query, the server provides a response and a proof that the response was computed correctly. The goal is to minimize the resources required by the client. This is made particularly challenging if the number of update queries is unbounded. We present a VDB scheme based on the hardness of the subgroup membership problem in composite order bilinear groups.