**The Shortest Signatures Ever**

**Abstract**:Multivariate Cryptography is one of the main candidates for creating post quantum public key cryptosystems. Especially in the area of digital signatures, there exist many practical and secure multivariate schemes. In this paper we present a general technique to reduce the signature size of multivariate schemes. Our technique enables us to reduce the signature size of nearly all multivariate signature schemes by 10 to 15 % without slowing down the scheme significantly. We can prove that the security of the underlying scheme is not weakened by this modification. Furthermore, the technique enables a further reduction of the signature size when accepting a slightly more costly verification process. This trade off between signature size and complexity of the verification process can not be observed for any other class of digital signature schemes. By applying our technique to the Gui signature scheme, we obtain the shortest signatures of all existing digital signature schemes.

= = = = = = = = = = = = = = = = = = = =

**Short and Adjustable Signatures**

**Abstract**:Motivated by the problem of one-time password generation with security against server breaches, we introduce the notion of {\em adjustable signature schemes} that allow the length of a signature to be adjusted---at the setup, signing or verification stages, depending on the application. Defining security for such schemes poses several challenges, such as: (i) different signature lengths should provide different levels of security, and (ii) the effort required for forging a very short signature (e.g., 6 bytes) should not be reusable for forging additional signatures. We provide security definitions that concretely capture the trade-off between signature length, number of forgeries and level of security provided by the scheme.

The above requirements rule out all existing solutions for short signatures. In this paper, as a feasibility result, we provide the first instantiation of all variants of adjustable signatures based on indistinguishability obfuscation. Our starting point is the state-of-the-art construction by Ramchen and Waters [ACM CCS 2014]. We observe that their scheme fails to meet our requirements for an adjustable signature scheme, and enhance it to obtain adjustable signatures with {\em shorter} signatures, {\em faster} signing and {\em strong} unforgeability. We also employ new proof techniques in order toobtain the above-mentioned notions of security.

For the simpler case where adversarial effort does not grow with the number of forgeries, we also provide a concrete construction based on the BLS signature scheme, by instantiating it using smaller group sizes that yield shorter signature lengths while providing reasonable security. We implement this scheme for various signature sizes an report on its efficiency.

= = = = = = = = = = = = = = = = = = =

**Certificateless Aggregate Short Signature Scheme**

**Abstract:** An aggregate signature scheme is the aggregation of multiple signatures into a single compact signature of short string that can convince to any arbitrary verifier participating in the scheme. The aggregate signature scheme is very useful for real-world cryptographic applications such as secure routing, database outsourcing etc where the signatures on several distinct messages generated by many distinct users requires to be compact. In this paper, we presented an aggregate signature scheme using Certificateless Public Key Cryptography(CL-PKC). The scheme is provably secure with strongest security and shortest length. We have proven the scheme is existentially unforgeable under adaptive chosen message attack, assuming the hardness of computational Diffie-Hellman(CDH) Problem.

= = = = = = = = = = = = = = = = = = =

**A Provably Secure Short Signature Scheme from Coding Theory**

**Abstract:**Signatures with partially message recovery in which some parts of messages are not transmitted with signatures to make them shorter are useful where bandwidth is one of the crucial concern and especially in case of signing short messages in applications such as time stamping, certified email services and identitybased cryptosystems. In this paper, to have quantum-attackresistant short signatures, a signature scheme with partially message recovery from coding theory is proposed. The security of the proposed scheme is proved under Goppa Parametrized Bounded Decoding and the Goppa Code Distinguishing assumptions in the random oracle model. Relying on the partially message recovery property, the proposal is shorter than the Dallot signature scheme, the only provably secure and practical code-based signature scheme. We should highlight that our scheme can be used as a building block of code-based signature schemes with additional properties since it compared to Dallot signature scheme not only improves its communication overhead but also it preserves its signature efficiency.