[2016/477](http://eprint.iacr.org/2016/477)

**Shortening the Libert-Peters-Yung Revocable Group Signature Scheme by Using the Random Oracle Methodology**

**Abstract**:In EUROCRYPT 2012, Libert, Peters and Yung (LPY) proposed the first scalable revocable group signature (R-GS) scheme in the standard model which achieves constant signing/verification costs and other costs regarding signers are at most logarithmic in N, where N is the maximum number of group members. However, although the LPY R-GS scheme is asymptotically quite efficient, this scheme is not sufficiently efficient in practice. For example, the signature size of the LPY scheme is roughly 10 times larger than that of the RSA signature (in 160-bit security). In this paper, we propose a compact R-GS scheme secure in the random oracle model that is efficient not only in the asymptotic sense but also in practical parameter settings. We achieve the same efficiency as the LPY scheme in an asymptotic sense, and the signature size is nearly equal to that of the RSA signature (in 160-bit security). It is particularly worth noting that our R-GS scheme has the smallest signature size compared to those of previous R-GS schemes which enable constant signing/verification costs. Our technique, which we call parallel Boneh{Boyen{Shacham group signature technique, helps to construct a R-GS scheme without following the technique used in LPY, i.e., we directly apply the Naor–Naor–Lotspiech framework without using any identity-based encryption.

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

[2015/933](http://eprint.iacr.org/2015/933)

**Cryptanalysis of Provably Secure Certificateless Short Signature Scheme**

**Abstract**:Recently, Choi et al. proposed certificateless short signature scheme in random oracle model and the author claims that it is provably secure. Certificateless Public Key Cryptography is a new paradigm, where it allows resolving the inherent key escrow and key management problem. Attack to certificateless signature scheme are of two types as Type-I where the adversary can replace the public key of the user and cannot able to retrieve the master secret key from Key Generator Center (KGC). In Type-II, the adversary can able to obtain the master secret key and cannot replace the public key of the user. In this paper we have proven that, the proposed scheme is not secure against Type-I adversary. To prove, we solve linear Diophantine equation and obtain the partial-private key of the user.

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

[2015/830](http://eprint.iacr.org/2015/830)

**Unique Signature with Short Output from CDH Assumption**

**Abstract**:We give a simple and efficient construction of unique signature on groups equipped with bilinear map. In contrast to prior works, our proof of security is based on computational Diffie-Hellman problem in the random oracle model. Meanwhile, the resulting signature consists of only one group element. Due to its simplicity, security and efficiency, our scheme is suitable for those situations that require to overcome communication bottlenecks. Moreover, the unique signature is a building block for designing chosen-ciphertext secure cryptosystems and verifiable random functions, which have found many interesting applications in cryptographic protocol design.

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

[2015/826](http://eprint.iacr.org/2015/826)

**Programmable Hash Functions go Private:Constructions and Applications to (Homomorphic) Signatures with Shorter Public Keys**

**Abstract:**We introduce the notion of asymmetric programmable hash functions (APHFs, for short), which adapts Programmable Hash Functions, introduced by Hofheinz and Kiltz at Crypto 2008, with two main differences. First, an APHF works over bilinear groups, and it is asymmetric in the sense that, while only {\em secretly} computable, it admits an isomorphic copy which is publicly computable. Second, in addition to the usual programmability, APHFs may have an alternative property that we call programmable pseudorandomness. In a nutshell, this property states that it is possible to embed a pseudorandom value as part of the function's output, akin to a random oracle. In spite of the apparent limitation of being only secretly computable, APHFs turn out to be surprisingly powerful objects. We show that they can be used to generically implement both regular and linearly-homomorphic signature schemes in a simple and elegant way. More importantly, when instantiating these generic constructions with our concrete realizations of APHFs, we obtain: (1) the first linearly-homomorphic signature (in the standard model) whose public key is sub-linear in both the dataset size and the dimension of the signed vectors; (2) short signatures (in the standard model) whose public key is shorter than those by Hofheinz-Jager-Kiltz from Asiacrypt 2011, and essentially the same as those by Yamada, Hannoka, Kunihiro, (CT-RSA 2012).

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

[2015/743](http://eprint.iacr.org/2015/743)

**Short Group Signatures via Structure-Preserving Signatures: Standard Model Security from Simple Assumptions**

**Abstract**:Group signatures are a central cryptographic primitive which allows users to sign messages while hiding their identity within a crowd of group members. In the standard model (without the random oracle idealization), the most efficient constructions rely on the Groth-Sahai proof systems (Eurocrypt'08). The structure-preserving signatures of Abe et al. (Asiacrypt'12) make it possible to design group signatures based on well-established, constant-size number theoretic assumptions (a.k.a. ``simple assumptions'') like the Symmetric eXternal Diffie-Hellman or Decision Linear assumptions. While much more efficient than group signatures built on general assumptions, these constructions incur a significant overhead w.r.t. constructions secure in the idealized random oracle model. Indeed, the best known solution based on simple assumptions requires 2.8 kB per signature for currently recommended parameters. Reducing this size and presenting techniques for shorter signatures are thus natural questions. In this paper, our first contribution is to significantly reduce this overhead. Namely, we obtain the first fully anonymous group signatures based on simple assumptions with signatures shorter than 2 kB at the 128-bit security level. In dynamic (resp. static) groups, our signature length drops to 1.8 kB (resp. 1 kB). This improvement is enabled by two technical tools. As a result of independent interest, we first construct a new structure-preserving signature based on simple assumptions which shortens the best previous scheme by 25%. Our second tool is a new method for attaining anonymity in the strongest sense using a new CCA2-secure encryption scheme which is simultaneously a Groth-Sahai commitment.

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

[2015/525](http://eprint.iacr.org/2015/525)

**Short Randomizable Signatures**

**Abstract**:Digital signature is a fundamental primitive with numerous applications. Following the development of pairing-based cryptography, several taking advantage of this setting have been proposed. Among them, the Camenisch-Lysyanskaya (CL) signature scheme is one of the most flexible and has been used as a building block for many other protocols. Unfortunately, this scheme suffers from a linear size in the number of messages to be signed which limits its use in many situations.

In this paper, we propose a new signature scheme with the same features as CL-signatures but without the linear-size drawback: our signature consists of only two elements, whatever the message length, and our algorithms are more efficient. This construction takes advantage of using type 3 pairings, that are already widely used for security and efficiency reasons.

We prove the security of our scheme without random oracles but in the generic group model. Finally, we show that protocols using CL-signatures can easily be instantiated with ours, leading to much more efficient constructions.

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

[2015/248](http://eprint.iacr.org/2015/248)

**Verifiably Encrypted Signatures with Short Keys based on the Decisional Linear Problem and Obfuscation for Encrypted VES**

**Abstract**:Verifiably encrypted signatures (VES) are signatures encrypted by a public key of a trusted third party and we can verify their validity without decryption. This paper proposes a new VES scheme which is secure under the decisional linear (DLIN) assumption in the standard model. We also propose new obfuscators for encrypted signatures (ES) and encrypted VES (EVES) which are secure under the DLIN assumption.

All previous efficient VES schemes in the standard model are either secure under standard assumptions (such as the computational Diffie-Hellman assumption) with large verification (or secret) keys or secure under \emph{(non-standard) dynamic qq-type assumptions} (such as the qq-strong Diffie-Hellman extraction assumption) with short verification keys. Our construction is the first efficient VES scheme with short verification (and secret) keys secure under \emph{a standard assumption (DLIN)}.

As by-products of our VES scheme, we construct new obfuscators for ES/EVES based on our new VES scheme. They are more efficient than previous obfuscators with respect to the public key size. Previous obfuscators for EVES are secure under non-standard assumption and use zero-knowledge (ZK) proof systems and Fiat-Shamir heuristics to obtain non-interactive ZK, i.e., its security is considered in the random oracle model. Thus, our construction also has an advantage with respect to assumptions and security models. Our new obfuscator for ES is obtained from our new obfuscator for EVES.

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

[2015/169](http://eprint.iacr.org/2015/169)

**Short Schnorr signatures require a hash function with more than just random-prefix resistance**

**Abstract**:Neven, Smart and Warinschi (NSW) proved, in the generic group model, that full-length Schnorr signatures require only random-prefix resistant hash functions to resist passive existential forgery.

Short Schnorr signatures halve the length of the hash function, and have been conjectured to provide a similar level of security. The NSW result is too loose to provide a meaningful security for short Schnorr signatures, but Neven, Smart and Warinschi conjecture that this is mere artefact of the proof technique, and not an essential deficiency of the short Schnorr signatures. In particular, this amounts to a conjecture that short Schnorr signature are secure under the same set of assumptions, namely random-prefix resistance of the hash function.

This report provides a counterexample to the latter conjecture, in other words, a separation result. It finds a hash function that seems to suggest random-prefix resistance does not suffice for short Schnorr signatures. In other words, the loose reduction implicit in the NSW theorem is as tight as possible.

Obviously, this result does not preclude the possibility of another proof for short Schnorr signatures, based on different hash function security properties such as preimage resistance.

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

[2015/014](http://eprint.iacr.org/2015/014)

**Group Signatures from Lattices: Simpler, Tighter, Shorter, Ring-based**

**Abstract**:We introduce a lattice-based group signature scheme that provides several noticeable improvements over the contemporary ones: simpler construction, weaker hardness assumptions, and shorter sizes of keys and signatures. Moreover, our scheme can be transformed into the ring setting, resulting in a scheme based on ideal lattices, in which the public key and signature both have bit-size soft-O(n log N), for security parameter n, and for group of N users. Towards our goal, we construct a new lattice-based cryptographic tool: a statistical zero-knowledge argument of knowledge of a valid message-signature pair for Boyen's signature scheme (Boyen, PKC'10), which potentially can be used as the building block to design various privacy-enhancing cryptographic constructions.

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

[2014/495](http://eprint.iacr.org/2014/495)

**Improved Short Lattice Signatures in the Standard Model**

**Abstract**:We present a signature scheme provably secure in the standard model (no random oracles) based on the worst-case complexity of approximating the Shortest Vector Problem in ideal lattices within polynomial factors. The distinguishing feature of our scheme is that it achieves short signatures (consisting of a single lattice vector), and relatively short public keys (consisting of O(log n) vectors.) Previous lattice schemes in the standard model with similarly short signatures, due to Boyen (PKC 2010) and Micciancio and Peikert (Eurocrypt 2012), had substantially longer public keys consisting of &Omega;(n) vectors (even when implemented with ideal lattices). We also present a variant of our scheme that further reduces the public key size to just O(log log n) vectors and allows for a tighther security proof by making the signer stateful.