NEW PARADIGMS IN SIGNATURE SCHEMES

Hovav Shacham, Ph.D.
Stanford University, 2006

Adviser: Dan Boneh

Digital signatures provide authenticity and nonrepudiation. They are a standard cryptographic primitive with many applications in higher-level protocols. Groups featuring a computable bilinear map are particularly well suited for signature-related primitives. For some signature variants the only construction known uses bilinear maps. Where constructions based on, e.g., RSA are known, bilinear-map–based constructions are simpler, more efficient, and yield shorter signatures. We describe several constructions that support this claim.

First, we present the Boneh-Lynn-Shacham (BLS) short signature scheme. BLS signatures with 1024-bit security are 160 bits long, the shortest of any scheme based on standard assumptions.

Second, we present Boneh-Gentry-Lynn-Shacham (BGLS) aggregate signatures. In an aggregate signature scheme it is possible to combine n signatures on n distinct messages from n distinct users into a single aggregate that provides nonrepudiation for all of them. BGLS aggregates are 160 bits long, regardless of how many signatures are aggregated. No construction is known for aggregate signatures that does not employ bilinear maps. BGLS aggregates give rise to verifiably encrypted signatures, a signature variant with applications in contract signing.

Third, we present Boneh-Boyen-Shacham (BBS) group signatures. Group signatures provide anonymity for signers. Any member of the group can sign messages, but the resulting signature keeps the signer's identity secret. Only the group manager can trace the signature, undoing its anonymity, using a special trapdoor. BBS group signatures are 1443 bits long, shorter than any previous scheme by an order of magnitude. The signing operation is also an order of magnitude more efficient than in previous schemes.

Finally, we consider variants and extensions of the BBS group signature scheme, including a group signature with a novel revocation mechanism that we call verifier-local revocation (VLR). In a VLR group signature, messages announcing the revocation of some users need only be processed by the verifiers; the signers are stateless. We present the Boneh-Shacham VLR group signature scheme, which has signatures even shorter than in BBS.

Approved for publication:

By: ____________________________

For Department of Computer Science