

Department of Applied Mathematics and Statistics  
The Johns Hopkins University

SEMINAR

Susan Hohenberger  
Department of Computer Science  
The Johns Hopkins University

November 15, 2007  
304 Whitehead Hall  
Refreshments: 3:30 p.m.  
Seminar: 4:00 p.m.

BATCH VERIFICATION OF SHORT SIGNATURES

ABSTRACT

With the rapid spread of computer networks, devices from vehicles to dog collars may soon be expected to communicate with their environments in an authenticated fashion. Several of these applications require that the cryptographic overhead be kept small and that many messages be processed at the same time. In this work, we consider the suitability of public key signatures in this scenario. That is, we want signatures that (i) are short and (ii) can be verified quickly. Signatures such as RSA have property (ii), but not (i); whereas short (pairing-based) signatures have property (i), but not (ii).

In this work, we focus on speeding up the verification of short signatures by batching the verification of many signatures from (possibly) different signers on (possibly) different messages. Prior work focused almost exclusively on batching signatures from the same signer. We present two results. First, we describe a batch verifier for a known scheme with a verification time where the dominant operation depends on the security parameter and not on the number of signatures to verify. Second, we design a new signature scheme (with some usage restrictions) that requires only a constant number of dominant operations to verify an arbitrary number of signatures. Preliminary results show that our techniques drastically improve performance in practice.

We will end with a discussion of privacy concerns and how these might be mitigated. A background in cryptography will not be assumed.

[This is joint work with Jan Camenisch (IBM Zurich Research) and Michael Ostergaard Pedersen (University of Aarhus) that appeared in Eurocrypt 2007.]