Title: Aggregate Signatures for BGPsec
Authors: Kyle Brogle, Sharon Goldberg, Leonid Reyzin (Boston University)
Emerging Technology Space: Secure Routing
Cryptographic Requirements: Aggregate Signatures

The Border Gateway Protocol (BGP), the protocol currently used for global route discovery on the Internet, is notoriously insecure. In BGP, autonomous systems (ASes) send routing announcements listing the ASes on the path to a particular destination. Cryptographically signing these announcements has been proposed as way of securing BGP. The proposal is known as BGPsec.

An announcement for a path that is n hops long will contain n digital signatures, added in sequence by each AS on the path. Sequential aggregate signature schemes seem particularly well suited for this application: they allow n signers, in order, to sign a message each, at a lower total cost than the cost of n individual signatures.

However, BGPsec requires routers to have access to a large number of public keys; indeed, a routing announcement can contain information from any of the 36,000 ASes in the Internet. Given the difficulty of storing, retrieving, and verifying certificates for over 36,000 public keys, the BGPsec protocol must give routers the option to perform lazy verification: that is, to immediately sign the routing announcement with its own public key, and to delay verification until a later time, e.g. when (a) it has time to retrieve the public keys of the other signers, or (b) when the router itself is less overloaded and can devote resources to verification.

We thus design, prove security for, and evaluate the performance of a new sequential aggregate scheme that supports lazy verification. Our scheme is based on trapdoor permutations like RSA. Unlike prior RSA-based proposals, which were insecure under lazy verification, our scheme does not require a signer to retrieve the keys of other signers and verify the aggregate-so-far before adding its own signature. Indeed, we do not even require a signer to know the public keys of other signers!