Cryptology ePrint Archive: Report 2011/438

Short Transitive Signatures for Directed Trees

Philippe Camacho and Alejandro Hevia

Abstract: A transitive signature scheme allows to sign a graph in such a way that, given the signature of edges (a,b) and (b,c), it is possible to compute the signature for the edge (or path) (a,c) without the Signer's secret. Constructions for undirected graphs are known but the case of directed graphs remains open. A first solution for the easier case of directed trees (DTTS) was given by Yi at CT-RSA 2007. In Yi's construction, the signature for an edge is O(n (\log (n \log n))) bits long in the worst case. A year later, Neven designed a simpler scheme where the signature size is reduced to O(n \log n) bits. Although Neven's construction is more efficient, handling O(n \log n) still remains impractical for large n.

In this work, we design a new $DTTS$ scheme where for any value \lambda \geq 1 and security parameter \kappa, we have:

* A signature for an edge is only $O(\kappa \lambda)$ bits long.

* Signing or verifying the signature for an edge requires O(\lambda) cryptographic operations.

* Computing a signature for an edge requires \lambda n^{1/\lambda} cryptographic operations.

To the best of our knowledge this is the first construction with such trade off. In particular, we achieve O(\kappa\log(n)) bits signatures, as well as O(\log(n)) time to generate edge signatures, verify or even compute edge signatures. Our construction relies on hashing with common-prefix proofs, a new variant of collision resistance hashing. A family \HashFam is collision resistant hashing with common-prefix proofs if for any H \in \HashFam, given two strings X and Y equal up to position i, a Combiner can convince a Verifier that X[1..i] is a prefix of Y by sending only H(X),H(Y), and a small proof. We believe that this new primitive will lead to other interesting applications.

Category / Keywords: cryptographic protocols / transitive signatures; authenticated data structures; collision resistant hashing;

Date: received 12 Aug 2011, last revised 20 Aug 2011

Contact author: philippe camacho at gmail com

Available formats: PDF | BibTeX Citation

Note: Minor corrections.

Version: 20110821:003404 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]