Sufficient conditions for sound tree hashing modes (Abstract)

Guido Bertoni[1], Joan Daemen[1], Michaël Peeters[2], and
Gilles Van Assche[1]

[1] STMicroelectronics
[2] NXP Semiconductors

Tree hashing has several advantages over sequential hashing such as parallelism and a lower cost of hash value recomputation when only a small part of the input changes. In this paper we consider the general case of tree hashing modes that make use of an underlying (sequential) hash function. We formally define tree hashing modes as algorithms for constructing *tree templates* that are independent of the message content and only depend on its length and hashing mode parameters. Such a tree template consists of a number of *node templates* arranged in a tree. Each node is a sequence of three types of *template bits*: message-independent frame bits, message bits and chaining bits.

In our template framework, we formulate a set of four simple conditions for a tree hashing mode to be *sound*. For the soundness, we base ourselves on the indifferentiability framework introduced by Maurer et al. in [2] and applied to hash functions by Coron et al. in [1]. We can prove that for any tree hashing mode satisfying these four conditions, the advantage in differentiating it from an ideal monolithic hash function is upper bounded by $q^2/2^n$ with q the number of queries to the underlying hash function and n the length of the chaining values.

Our result allows readily constructing either general-purpose or adhoc tree hashing modes that are provably sound. Moreover, we show how to take the union of tree hashing modes that preserves soundness. Finally, application to sequential hashing modes calling a fixed-input-length compression function provides some interesting new insights.

References

1. J. Coron, Y. Dodis, C. Malinaud, and P. Puniya, *Merkle-Damgård revisited: How to construct a hash function*, Advances in Cryptology – Crypto 2005 (V. Shoup, ed.), LNCS, no. 3621, Springer-Verlag, 2005, pp. 430–448.
2. U. Maurer, R. Renner, and C. Holenstein, *Inidifferentiability, impossibility results on reductions, and applications to the random oracle methodology*, Theory of Cryptography - TCC 2004 (M. Naor, ed.), Lecture Notes in Computer Science, no. 2951, Springer-Verlag, 2004, pp. 21–39.

Dagstuhl Seminar Proceedings 09031
Symmetric Cryptography
http://drops.dagstuhl.de/opus/volltexte/2009/1946