Cryptology ePrint Archive: Report 2011/620

Provable Security of BLAKE with Non-Ideal Compression Function

Elena Andreeva and Atul Luykx and Bart Mennink

Abstract: We analyze the security of the SHA-3 finalist BLAKE. The BLAKE hash function follows the HAIFA design methodology, and as such it achieves optimal preimage, second preimage and collision resistance, and is indifferentiable from a random oracle up to approximately $2^{n/2}$ assuming the underlying compression function is ideal. In our work we show, however, that the compression function employed by BLAKE exhibits a non-random behavior and is in fact differentiable in only $2^{n/4}$ queries. Our attack on the indifferentiability of the BLAKE compression function seriously undermines the security strength of BLAKE not only with respect to its overall indifferentiability, but also its collision and (second) preimage security in the ideal model. Our next contribution is the restoration of the security results for BLAKE in the ideal model by refining the level of modularity and assuming that BLAKE's underlying block cipher is an ideal cipher. We prove that BLAKE is optimally collision, second preimage, and preimage secure (up to a constant). We go on to show that BLAKE is still indifferentiable from a random oracle up to the old bound of $2^{n/2}$ queries, albeit under a weaker assumption: the ideality of its block cipher.

Available formats: PDF | BibTeX Citation

Version: 20111121:155316 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]