A MAC Mode for Lightweight Block Ciphers

A MAC Mode for Lightweight Block Ciphers

Lightweight cryptography strives to protect communication in constrained environments without sacrificing security. However, security often conflicts with efficiency, shown by the fact that many new lightweight block cipher designs have block sizes as low as 64 or 32 bits. Such low block sizes lead to impractical limits on how much data a mode of operation can process per key. MAC (message authentication code) modes of operation frequently have bounds which degrade with both the number of messages queried and the message length. We present a MAC mode of operation, LightMAC, where the message length has no effect on the security bound, allowing an order of magnitude more data to be processed per key. Furthermore, LightMAC is incredibly simple, has almost no overhead over the block cipher, and is parallelizable. As a result, LightMAC not only offers compact authentication for resource-constrained platforms, but also allows high-performance parallel implementations. We highlight this in a comprehensive implementation study, instantiating LightMAC with PRESENT and the AES. Moreover, LightMAC allows flexible trade-offs between rate and maximum message length. Unlike PMAC and its many derivatives, LightMAC is not covered by patents. Altogether, this makes it a promising authentication primitive for a wide range of platforms and use cases.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, KU Leuven, NTT Corporation
Contributors: Luykx, A., Preneel, B., Tischhauser, E. W., Yasuda, K.
Pages: 43-59
Publication date: 2016

Host publication information
Title of host publication: Revised Selected Papers of the 23rd International Conference on Fast Software Encryption (FSE 2016)
Publisher: Springer
ISBN (Print): 978-3-662-52992-8
(Lecture Notes in Computer Science, Vol. 9783).
Keywords: Lightweight, MAC, LightMAC, Message length, Birthday bound, Integrity, Verification
Electronic versions:
Luykx_et_al_A_MAC_Mode_for_Lightweight_Block_Ciphers.pdf. Embargo ended: 20/07/2017
DOIs:
10.1007/978-3-662-52993-5_3
Source: Findit
Source-ID: 2307542633
Research output: Research - peer-review; Article in proceedings – Annual report year: 2016