NISTIR 8369

Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process

Meltem Sönmez Turan
Kerry McKay
Donghoon Chang
Çağdaş Çalık
Lawrence Bassham
Jinkeon Kang
John Kelsey

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8369

National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8369

Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process

Meltem Sönmez Turan
Kerry McKay
Donghoon Chang
Çağdaş Çalık
Lawrence Bassham
Jinkeon Kang
John Kelsey

Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8369

July 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology
Interagency or Internal Report 8369
Natl. Inst. Stand. Technol. Interag. Intern. Rep. 8369, 81 pages (July 2021)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8369

require hashing functionality, the following four candidates will be considered: ASCON, PHOTON-Beetle, SPARKLE, and Xoodyak.

Eight of the finalists, namely ASCON, Elephant, GIFT-COFB, Grain-128AEAD, ISAP, PHOTON-Beetle, Romulus, and SPARKLE, rely on thoroughly-analyzed, and previously-published building blocks and components. ASCON, GIFT-COFB, ISAP, PHOTON-Beetle, Romulus, SPARKLE, TinyJAMBU, and Xoodyak demonstrated performance advantages over NIST standards in software benchmarks and are under consideration for software applications. For hardware applications, the finalists ASCON, Elephant, GIFT-COFB, PHOTON-Beetle, Romulus, TinyJAMBU, and Xoodyak demonstrated performance advantages over NIST standards. ISAP provides promising features for applications requiring side-channel resistance.

6. Next Steps

It is estimated that the third round of evaluation and review will take approximately 12 months. The selection will consider the security of the candidates and performance on software and hardware platforms, including the performance of protected implementations. During the final round, NIST is planning to host the fifth workshop to support the standardization process.

NIST encourages further analysis of the candidates that did not advance to the final round. The candidates that proposed new modes of operation instantiated with AES might still be beneficial for general-purpose applications. The modes of operations of these candidates may be considered later under NIST's mode development project [277].