SIMON and SPECK Information Paper

NSA stands firmly behind the Simon and Speck algorithms and hopes that they will contribute to improved security for constrained devices. NSA has funded prototyping efforts to explore U. S. National Security Systems (NSS) use on such platforms.

NSA attests that it is not aware of any cryptanalytic technique that would allow NSA or any other entity to exploit Simon or Speck. Both algorithms have been deemed by NSA to have security commensurate with their block and key sizes, and the 128/256 variants have been certified to provide the security necessary for NSS.

Prompted by potential U.S. government requirements for lightweight ciphers, a team of designers within NSA's Research Directorate began work on the Simon and Speck block ciphers in 2011. This work continues NSA’s long history of designing secure cryptography to protect NSS. The algorithms were published in the summer of 2013. To facilitate the U.S. Department of Defense's ability to procure secure computing equipment through the commercial marketplace, the U.S. National Body proposed Simon and Speck in the fall of 2014 for inclusion in the ISO/IEC SC27 WG2 lightweight cryptography standard, ISO/IEC 29192-2.

More than 70 security analysis papers from some of the world's best cryptographers support NSA's own conclusion that the algorithms are secure. Regarding performance, Simon and Speck have ranked at or near the top of most every performance comparison. A number of algorithms have been proposed with the explicitly-stated goal of being competitive with Simon and/or Speck, and thus providing viable security primitives for the lowest-end devices.

The ISO proposal progressed from a Study Period, to a Working Draft, to a Preliminary Draft Amendment, and at each of three ballot stages a solid majority of the participating national bodies voted in favor of its inclusion. The proposal did not reach the effective 75% favorable vote required as part of the ISO Process. However, according to official ISO documents, the outcome was “not a statement about the security or quality of the algorithms.” Our work supporting the amendment has now concluded. We continue to advocate for further research into lightweight ciphers and their adoption by ISO and other standards organizations.

For more information, please see https://nsacyber.github.io/simon-speck.