

# Final Steps of the NIST Lightweight Cryptography Standardization (Keynote Abstract)

Meltem Sonmez Turan<sup>1</sup>

<sup>1</sup> NIST

## Keywords

Cybersecurity, Cryptography standardization, Lightweight Cryptography, Ascon cryptographic protocol

## Topic

This talk includes an overview of the NIST Lightweight Cryptography Standardization process and explains the evaluation of the finalists, the selection of Ascon as the winner and the final steps in the standardization process.

## Biography


Dr. Meltem Sonmez Turan is a mathematician in the Computer Security Division of National Institute of Standards and Technology. Meltem co-leads the Lightweight Cryptography Standardization project at NIST. Her research interests include symmetric cryptography, random number generation and circuit complexity.

---

*C&ESAR'23: Computer & Electronics Security Application Rendezvous, Nov. 21-22, 2023, Rennes, France*

 <https://www.linkedin.com/in/meltem-sonmez-turan-847b024> (M. S. Turan)

© 2023 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)