IEEE 802 PLENARY TUTORIAL SESSIONS

MONDAY, 11 March 2024

Hyatt Regency Denver at Colorado Convention Center

SESSION 1 6:15 PM - 7:35 PM MOUNTAIN STANDARD TIME

TITLE OF TUTORIAL: **Ascon: The Lightweight Cryptography Standard for IoT**

NAME OF PRESENTERS, THEIR AFFLIATIONS AND CONTACT INFO:

Presenter Name	Affiliation
FLORIAN MENDEL	**Infineon Technologies**

ABSTRACT: **Implementing strong encryption is often not affordable for small and resource-constrained devices. To address this gap, NIST has recently selected Ascon as the new standard for lightweight authenticated encryption and hashing. In a multi-year international competition Ascon was selected as the winner among 56 candidates. Similar competitions led to the selection of the NIST standards AES and SHA-3. Ascon can provide the same security and combined functionality as AES-128 and SHA3-256 at a much lower cost.**

Wireless security is becoming increasingly important, and the weakest link is often the most vulnerable. Ascon will lower the bar for devices with little energy and computing power to implement security. In this tutorial, we will consider Ascon for next generation wireless standards, specifically 802.11 and 802.15, which are heavily used to serve many IoT applications. We will give an overview of Ascon, provide benchmarking results, and show how Ascon can be easily integrated into these wireless standards.

SESSION 2 7:35 PM - 8:50 PM MOUNTAIN STANDARD TIME

NO TUTORIAL SCHEDULED FOR THIS TIME SLOT

SESSION 3 9:00 PM - 10:30 PM MOUNTAIN STANDARD TIME

NO TUTORIAL SCHEDULED FOR THIS TIME SLOT

TUTORIAL ROOM: TO BE ADDED