

Edge & 5G

FPGA community forums and blogs on community.intel.com are migrating to the new Altera Community and are read-only. For urgent support needs during this transition, please visit the FPGA Design Resources page or contact an Altera Authorized Distributor.

Intel Community / Blogs / Tech Innovation / Edge & 5G 100 Discussions

Intel Labs Researcher Spotlight: Christoph Dobraunig's Lightweight Cryptography Algorithms Selected

Subscribe Article Options



Scott Bair Employee 05-18-2023 2 0 11K

Scott Bair is a key voice at Intel Labs, sharing insights into innovative research for inventing tomorrow's technology.

Highlights

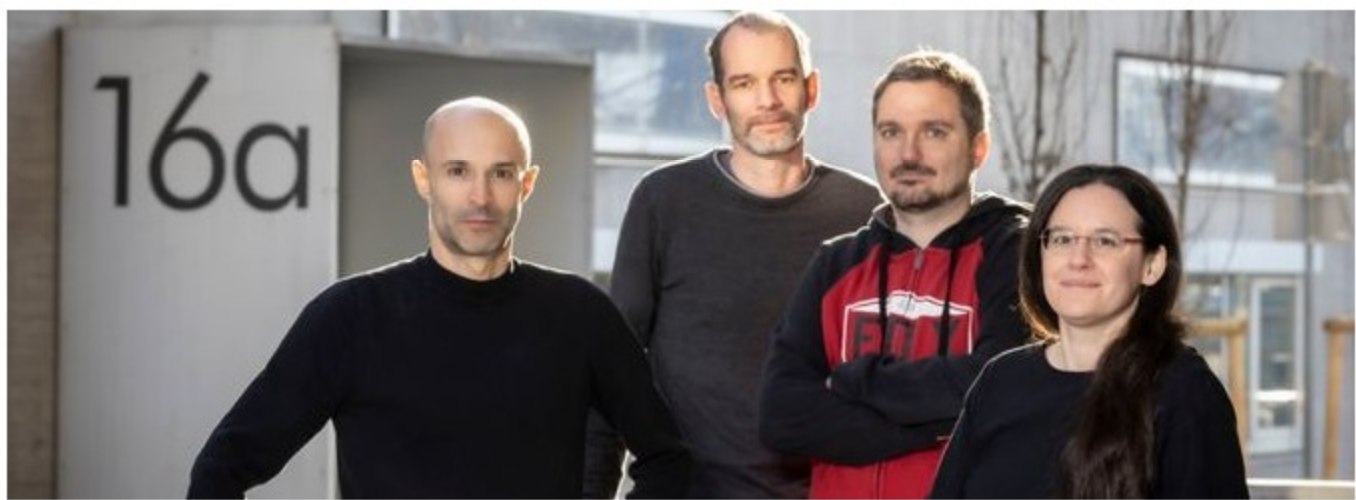
- Intel Labs research scientist Christoph Dobraunig's work on the cipher suite Ascon was selected as a new standard for lightweight cryptography by NIST.
- Dobraunig also worked on ISAP and Elephant, two other lightweight cryptography NIST candidates that were selected as top 10 finalists.
- Ascon will be featured at NIST's virtual [Sixth Lightweight Cryptography Workshop](#) on June 21-22.

Security standards for edge devices and small electronics just got stronger. Intel Labs research scientist Christoph Dobraunig's work on the cipher suite Ascon was selected as a new standard for lightweight cryptography by the National Institute of Standards and Technology (NIST) in February 2023. NIST initiated the competition to standardize algorithms for one or more authenticated encryption with associated data (AEAD) and hashing schemes for use in constrained environments, such as in radio frequency identification (RFID) tags and sensor networks. Ascon will be featured at NIST's virtual [Sixth Lightweight Cryptography Workshop](#) on June 21-22.

"NIST competitions do not happen very often and past selected standards, such as the 2000 competition winner Advanced Encryption Standard (AES), have had a huge worldwide impact on the cryptography and security industry," said Dobraunig, who works in the Security and Privacy Research lab. "This is a tremendous honor for the Ascon team."

The competition process began in February 2019 when 57 candidates were submitted to NIST for consideration. In March 2021, NIST announced 10 finalists to move forward to the final round of the selection process. Dobraunig also worked on [ISAP and Elephant](#), two other lightweight cryptography NIST candidates that were selected as top 10 finalists. For [ISAP](#), the team included Maria Eichlseder, Stefan Mangard, and Robert Primas from Graz University of Technology (TU Graz), Florian Mendel from Infineon Technologies, Bart Mennink from Radboud University, and Thomas Unterluggauer from Intel Labs. For [Elephant](#), the team included Tim Beyne and Yu Long Chen from KU Leuven and imec-COSIC, and Bart Mennink from Radboud University.

Among the seven algorithms in the Ascon suite, some or all may become part of [NIST's published lightweight cryptography standard](#) by the end of the year. The authenticated ciphers Ascon-128 and Ascon-128a previously were selected as the primary choice for lightweight authenticated encryption in the final portfolio of the [CAESAR competition](#) that took place from 2014 to 2019.



The Ascon team began work on the suite of authenticated encryption and hashing algorithms in 2014. From left: Martin Schl ffer, Florian Mendel, Christoph Dobraunig, and Maria Eichlseder. Image credit: Lunghammer, TU Graz.

"As the number of Internet of Things (IoT) devices continues to grow, security at the edge in constrained environments is critical as these devices communicate via public networks and may be physically accessible, making the technology vulnerable to side-channel attacks and more," said Dobraunig, who worked with a team of cryptographers to develop Ascon, including Maria Eichlseder from TU Graz, and Florian Mendel and Martin Schl ffer from Infineon Technologies.

Ascon Designed to Withstand Real-World Threats

The [Ascon project](#) began in 2014 at TU Graz when Ph.D. students Dobraunig and Eichlseder worked with university researchers Mendel and Schl ffer on a submission for the CAESAR competition. Many constrained IoT devices gather information and transmit data to high-performance back-end servers, including devices such as motion sensors in buildings and other large-scale structures, odor detectors for hazardous chemical leaks, and networked medical devices for pacemaker patients. The Ascon team set out to improve lightweight authenticated encryption for communication from these types of devices.

For example, thieves can steal cars by exploiting a potential vulnerability in the vehicle's electronic control units (ECUs). These devices control different systems, such as headlights, engine control, and the smart key that unlocks and starts the vehicle. ECUs are connected through controller area network (CAN) buses. Using a [CAN injection hack](#) on certain car models, attackers can reach the smart key ECU from the wires connected to the headlight, which are on the same CAN bus. By sending a false key validation CAN message to the smart key receiver, thieves can then send a second CAN message to the door ECU to unlock the vehicle.

"While smart technology makes our lives easier, we need to be vigilant in protecting devices that seem secure but may actually be vulnerable to more sophisticated attacks," said Dobraunig.

Ciphers have to withstand real-world threats where the attacker may have physical access to the device. [Ascon's sponge-based authenticated encryption](#) has been designed to provide robustness against certain implementation mistakes and attacks. For example, even if an attacker manages to recover an internal state during data processing through a side-channel attack, this does not directly lead to the recovery of the secret key or trivial forgeries.

The Ascon suite provides 128-bit security and internally uses the same 320-bit permutation (with different round numbers) so that a single lightweight primitive is sufficient to implement both AEAD and hashing. Sharing a single primitive for all schemes not only reduces the area requirements for hardware implementations, but also allows restriction of the code base that must be maintained. This reduces the workload necessary for efficient and secure implementations.

Ascon's permutation is defined on 64-bit words using only bitwise Boolean functions (and, not, xor) and rotations within words. The permutation lends well to fast bitsliced implementations on 64-bit platforms, while bit interleaving allows for fast bitsliced implementations on 32-, 16-, and 8-bit platforms. Ascon's low-degree S-box allows masked implementations with a small overhead in hardware and software. Ascon works well with lightweight devices carrying out cryptographic operations.

Looking to the Future

Up to this point, Dobraunig's research has focused on cryptography, including the analysis and design of symmetric cryptography, and implementation security for side-channel and fault attacks. In the future, he would like to explore cryptography in the context of system security.

"While probably the main application of cryptography nowadays is to secure communication channels between devices and storage, I expect cryptography to move more and more into devices," said Dobraunig.

This device focus will enable new and creative usages for cryptography that increase the system's security, such as [Cryptographic Capability Computing](#) (C3) developed at Intel Labs.

Memory safety vulnerabilities have long been a major affliction for software written in loosely-typed languages such as C and C++. The most prevalent vulnerabilities violate either spatial or temporal safety. C3 is a stateless mechanism that enforces memory safety in a fully flexible memory layout without relying on any additional metadata beyond what is encoded in a 64-bit pointer. It replaces inefficient metadata memory accesses with efficient cryptography by assigning a unique and distinct cryptographically isolated space for each allocation, which is identified by information encoded in a novel cryptographic address (CA) format. No additional metadata is needed.

"C3 with its novel requirements on cryptographic algorithms provides an interesting opportunity to design tailored cryptographic algorithms and to explore new design methods," said Dobraunig.

Translate Tags: Intel_Labs

2 Kudos

About the Author



Scott Bair is a Senior Technical Creative Director for Intel Labs, chartered with growing awareness for Intel's leading-edge research activities, like AI, Neuromorphic Computing and Quantum Computing. Scott is responsible for driving marketing strategy, messaging, and asset creation for Intel Labs and its joint-research activities. In addition to his work at Intel, he has a passion for audio technology and is an active father of 5 children. Scott has over 23 years of experience in the computing industry bringing new products and technology to market. During his 15 years at Intel, he has worked in a variety of roles from R&D, architecture, strategic planning, product marketing, and technology evangelism. Scott has an undergraduate degree in Electrical and Computer Engineering and a Masters of Business Administration from Brigham Young University.

You must be a registered user to add a comment. If you've already registered, sign in. Otherwise, register and sign in. Comment

Community support is provided Monday to Friday. Other contact methods are available here. Intel does not verify all solutions, including but not limited to any file transfers that may appear in this community. Accordingly, Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade. For more complete information about compiler optimizations, see our Optimization Notice.