NEWS

CAST

CAST Releases First Commercial SNOW-V Stream Cipher IP Core

High-throughput key stream generator enables fast cryptographic mechanisms for 5G and beyond high-speed communication systems

Woodcliff Lake, New Jersey — **March 3, 2025** — Semiconductor intellectual property core provider CAST today announced a new IP core that implements the SNOW-V stream cipher algorithm to meet the security and performance demands of modern communication systems. Available now for ASICs or FPGAs, the company believes it to be the first such commercial IP core.

The new **SNOW-V Stream Cipher Engine** provides a flexible and reusable hardware implementation of the official SNOW-V mechanism as published in 2019 by the IACR Transactions on Symmetric Cryptology. SNOW-V revises the SNOW 3G stream cipher algorithm to help satisfy the high-speed, low-latency security requirements of 5G, 6G, and future mobile networks. The core:

- Is optimized for ultra-high-speed communication, delivering throughput rates of over 140 Gbps in ASIC and 65 Gbps in FPGA implementations,
- Ensures confidentiality and integrity with AEAD (Authenticated Encryption with Associated Data) capabilities by easily interoperating with a GMAC (Galois Message Authentication Code) security framework in a GCM (Galois/Counter mode) topology, and
- Seamlessly upgrades existing 4G/5G network encryption as a drop-in replacement for SNOW 3G.

“Security safeguards struggle to keep up with the dramatic increases in the speed and bandwidth of cellular communications, multimedia streaming capabilities, and Internet of Things communication complexity,” said Dr. George Athanasiou, security product manager for CAST. “This new SNOW-V core joining CAST’s proven, low-risk

more

IP cores line means system designers can now establish high-speed security with practically no effort or performance impact."

About the SNOW-V IP Core

Developed by CAST partner Ocean Logic, the core accepts a secret 256-bit Key and a 128-bit Initialization Vector and produces a stream of secure 128-bit keys. These stream keys can be combined with a plaintext message to create secure ciphertext (and vice versa).

The new core helps future-proof security in a variety of applications, including current and future mobile communications systems, secure IoT device communication, high-speed encrypted data storage, and secure multimedia streaming. It can also be used for pseudo-random number generation and general data encryption.

The SNOW-V Stream Cipher Engine IP core is available now for ASICs and FPGAs, with flexible licensing including royalty-free. Visit the SNOW-V product page or contact CAST Sales for more information.

About CAST

Computer Aided Software Technologies, Inc. (CAST) is a silicon IP provider founded in 1993. The company's ASIC and FPGA IP product line includes security primitives and comprehensive SoC security modules; microcontrollers and processors; compression engines for data, images, and video; interfaces for automotive, aerospace, and other applications; and various common peripheral devices. Learn more by visiting www.cast-inc.com.

# # #

Media Contact: Artemis Couroupaki, a.couroupaki@cast-inc.com