UNIVERSITY OF WATERLOO

TECHNOLOGY SUMMARY

"Lightweight" Security Algorithm for 4G /5G Networks

Reference
8810-7328/7325

Sectors
Telecommunication
Mobile Phones
E-Commerce
Information Security

Patent status
U.S. 8,953,784 and
Canadian 2,864,227

Stage of development
Implementations on smart phones are in progress
Seeking industrial partner for 4G networks
Studies for additional markets are on-going

Contact
Scott Inwood
Director of Commercialization
Waterloo Commercialization Office
519-888-4567, ext. 33728
sinwood@uwaterloo.ca
uwaterloo.ca/research

Description of the invention

As newer fourth generation (4G) wireless telecommunication systems are introduced, such as "LTE" (Long Term Evolution) and IEEE 802.16m (i.e., Wi-MAX), more robust security algorithms are required to comply with the associated 3GPP security standards. Typically the implementation of higher security cryptography methods are computationally more complex and thus have a negative impact on bandwidth efficiency, throughput and processing efficiency, storage, and power consumption, due to the complicated architecture.

University of Waterloo researchers associated with the world renowned Communications Security Lab have developed a new and "lightweight" stream cipher, referred to as "WG-16", that is targeted for resource-constrained mobile platforms, such as smart phones. The WG-16 stream cipher is based on the well-known Welch-Gong (WG) transformation, which has mathematically proved randomness properties such as ideal two-level autocorrelation, balance, long period, ideal tuple distribution, and high and exact linear complexity. These randomness properties uniquely overcome the disadvantages of state-of-the art cryptography approaches and thus significantly enhance the security confidence. Equally important, the WG-16 stream cipher complies with the existing 3GPP security standards.

The initial development of the WG-16 stream cipher has been focused on achieving the unique randomness properties. More recent development efforts have been focussed on optimizing the software and hardware implementations on various low-power and low-cost embedded platforms. Moreover, a suite of security protocols based on the WG-16 stream cipher is being developed and analyzed, which will be seamlessly integrated into the communication architecture of the 4G networks.

Advantages

- Only stream cipher method with mathematically proved randomness, thus guaranteeing security, and compliant with 3GPP security standard.
- Suitable for both hardware and software platforms.
- Low power consumption on resource-constrained devices.

Potential applications

- Cell/smart phones/tablets.
- Smart cards/mobile payment systems (e-commerce).
- Smart meters/wireless sensor networks.