

International Conference and Business Expo on

Wireless Communication & Network

September 21-23, 2015 Baltimore, USA

Applications of homomorphic cryptography to the internet of things

Mohamed M Hamdi

School of Communication Engineering (Sup'Com), Tunisia

Emerging applications based on the IoT are introducing new security challenges. They operate in a dynamic environment dominated by the evolution of the security threats and the variation of network features (e.g., network topology, energy level). One of the major challenges that should be tackled is the trade-off between robustness and energy-efficiency. This strengthens the need for in-network processing such as aggregation and compression to limit the computational, memory, and storage overhead. Existing cryptographic algorithms and protocols are not compliant with such processing and turn out to affect the lifetime of the mobile nodes being part of the IoT. To cope with this problem, homomorphic encryption is introduced in this talk as an alternative to improve the applicability of cryptographic solutions to IoT-based applications. Concrete examples are described and analyzed in order to illustrate the potential brought by homomorphic encryption in providing energy-effective protection of the IoT.

Biography

Mohamed M Hamdi is an Associate Professor at the School of Communication Engineering (Sup'Com, Tunisia) and Development Manager at Elgazala Technopark. His publications covered cyber security, wireless communications, optical communications and multimedia communications. He gave invited and keynote speeches at prestigious conferences including ITU World, IEEE CTS, and European Identity and Cloud. He has also co-chaired the elections committee of the IEEE CIS Technical Committee (2009 and 2011). Mohamed holds Eng, Master and Doctorate degrees in Telecommunications.

mmh@supcom.rnu.tn

Notes: