doi:10.1093/comjnl/bxm092

Capsule reviews

FAIROUZ KAMAREDDINE

The Capsule Reviews are intended to provide a short succinct review of each paper in the issue in order to bring the content to a wider readership. The Capsule Reviews were compiled by Fairouz Kamareddine. Professor Kamareddine is an Associate Editor of *The Computer Journal* and is based in the Department of Mathematical and Computer Sciences at Heriot-Watt University, Edinburgh, UK.

Analysis and Detection of Errors in Implementation of SHA-512 Algorithms on FPGAs. I. AHMAD AND A.S. DAS
Hash functions have a number of useful applications and advantages. In particular, the secure Hash Algorithm SHA-512 is widely used in real applications and in essential security services, and makes concurrent error detection (CED) extremely important. This paper analyses the propagation of single and multiple errors occurring at different operations of a digest round in the hardware implementation of SHA-512. First, the SHA-512 algorithm is discussed in detail and so is the propagation of error in SHA-512 including the error analysis of a digest round and a block round and those representing single, transient and permanent faults at all stages of hash value computation. Then, the method of predicting and checking parity bits for each performed operation is discussed where the paper proposes a parity scheme and error detection techniques and carries out a number of experimental results testing different types of expected errors. These tests show good results for the fault coverage.

Efficient and Provably Secure IP Multimedia Subsystem Authentication for UMTS. C.-M. HUANG AND J.-W. LI
Efficieny and security studies in mobile systems is a flourishing area of computer science (see for example, [1] and [2]). This paper carries out efficiency and security studies in Universal Mobile Telecommunications Systems (UTMSs). The paper proposes an evolutionary IP multimedia subsystem authentication and key agreement (E-IMS AKA) for the authentication of IP multimedia subsystems in UMTSs. The E-IMS AKA does not need duplicated AKA operations to maintain efficiency and can withstand security attacks. First, UTMSs are presented and the relevant background to authentication is given. Then, the proposed E-IMS AKA and IMS authentication are described in detail. The security analysis of E-IMS AKA is demonstrated through a number of analysis points. The paper further demonstrates that the E-IMS authentication can keep the efficiency of the one-pass authentication by comparing the delivery costs between the E-IMS authentication and the one-pass authentication. Computation and storage space of IMS AKA and E-IMS AKA are evaluated and the paper concludes that the storage complexity of E-IMS AKA is less than that of IMS AKA and furthermore, E-IMS AKA can save at least 42.9% of the computation cost of IMS AKA.

REFERENCES

[1] Tseng, Y.-M. (2007) A secure Authenticated Group Key Agreement Protocol for Resource-Limited Mobile Devices. *Computer Journal* **50**, 41–52.
[2] Choo, (2007) A proof of Revised Yahalom Protocol in the Bellare and Rogaway (1993) Model. *Computer Journal* **50**, 591–601.