# Why should we find new universal hash functions with good hardware implementation ?

Cédric Lauradoux, Marine Minier, Tanguy Risset, Wassim Znaidi

Lyon University - CITI Laboratory / SWING INRIA team
6, avenue des arts - 69621 Villeurbanne Cedex - France
first name.name@inrialpes.fr

**Abstract.** New techniques have emerged in information theory to improve the dissemination of information over a network. Many of this new results can be used in wireless sensor networks (WSNs) to preserve the nodes energy such as data aggregation (source coding, compressed sensing) or network-coding. Other algorithms like rateless codes (fountain codes) improve the resiliency of the transmission to packet losses. Many of these transformations have in common that the packets exchanged by the nodes are linear combination of the data to be transmitted. The consequence is that it is more difficult for the relaying nodes to know if a data received is legitimate or not. The obvious threat is therefore the pollution attack in which an adversary injects illegitimate data. The consequence of such an attack may vary depending on the applications ranging from an increased delay for data transmission to a total energy exhaustion of the WSN. Integrity policies need to be enforced to prevent pollution attacks. Message authentication codes can be used to preserve the data integrity from the emitter to the final receiver.
Two classes of algorithms are to be found to design message authentication codes (MACs). Algorithms based on classical cryptographic primitives such as hash functions (HMAC and MDx-MAC) or block ciphers (CBC-MAC). The other class of algorithms is based on universal hash functions (UHFs). In a motivation part, we will compare the performance in terms of delay and energy of schemes based on HMAC, CBC-MAC and UHFs for a classical network coding setup. All the implementations are done in software on MSP430 nodes. The conclusion is that UHFs are the only elegant solution that preserves the delay and the energy. The reason of this success is that homomorphic MAC can be designed from UHFs. For solution based on UHFs, there is an asymmetry between the data emitter and the relaying nodes. To reduce the energy gap between the emitter and the relaying nodes, we study the hardware implementation of universal hash functions. We particularly study the designs proposed by Hugo Krawczyk based on linear feedback shift register (LFSR). We discuss the various possibilities (*e.g.* fixed known key or variable key) to implement these schemes and how they can be adapted to reduce their hardware footprint.
**Keywords:** Integrity, MAC, universal hash functions.