The Cost of Cryptography: Is Low Budget Possible?

Ingrid Verbauwhede
ESAT/COSIC, K.U. Leuven, Leuven, Belgium
E-mail: ingrid.verbauwhede@esat.kuleuven.be
Website: www.esat.kuleuven.be/cosic

ABSTRACT:
Ambient intelligence, the future internet, smart dust, all lead to the immersion of electronics in the human environment. E-health applications are one example: patients will carry intelligent sensors and actuators which are wireless connected to monitoring devices and health professionals. All these applications carry heavy security and privacy risks. Strong authentication is needed such that the correct medical doses can be administered or that the settings of brain stimulants cannot be modified. On top, these devices have typically an extremely limited power, energy and area budget.
So, the question is: can we provide secure implementations of cryptographic algorithms for these next generation applications? Cost can be expressed in memory footprint or gate count, number of clock cycles or time budget, power and energy budgets. On top, making implementations secure against physical attacks has an extra cost. In this presentation, we will discuss the implementation cost of several cryptographic algorithms, including public key, secret key and hash examples. We will indicate future directions in this field.

ACKNOWLEDGMENT:
The author gratefully acknowledges support from the IAP Programme P6/26 BCRYPT of the Belgian State, by the European Commission under contract number ICT-2007-216676 E-CRYPT NoE phase II, by EU Project UNIQUE (FP7) and by the K.U. Leuven-GOA TENSE (GOA/11/007).