A Lightweight Cryptographic System for Implantable Biosensors

Sara S. Ghoreishizadeh*, Tolga Yalçın†, Antonio Pullini‡,
Giovanni De Micheli*, Wayne Burleson§, and Sandro Carrara*
* EPFL, LSI - Lausanne - Switzerland † University for Information Science and Technology, Ohrid, Macedonia
‡ ETHZ, IIS- Zurich - Switzerland § Department of Electrical and Computer Engineering UMass, Amherst, MA, USA

***Abstract*—This paper presents a lightweight cryptographic system integrated onto a multi-function implantable biosensor prototype. The resulting heterogeneous system provides a unique and fundamental capability by immediately encrypting and signing the sensor data upon its creation within the body. By providing these security services directly on the implantable sensor, a number of low-level attacks can be prevented. This design uses the recently standardized SHA-3 Keccak secure hash function implemented in an authenticated encryption mode. The security module consists of the DuplexSponge security core and the interface wrapper. The security core occupies only 1550 gate-equivalents, which is the smallest authenticated encryption core reported to date. The circuit is fabricated using 0.18 μm CMOS technology and uses a supply voltage of 1.8 V. The simulated power consumption of the complete cryptosystem with a 500 KHz clock is below 7 μW.**

***Index Terms*—Lightweight encryption, Keccak hash function, Authentication, Privacy, Implantable biosensor.**

I. Introduction

Recently the development of new *Implantable Medical Devices* (IMD) has allowed blood tests to be performed in the patient's body anywhere and at any time instead of in the laboratories. The increased reliance on the IMD technology, especially in the case of potentially life-saving therapies, can introduce difficult trade-offs in reliability and security. Personal health information that was once restricted to the confines of a medical laboratory, can now potentially be accessible to various unauthorized parties.

Implantable biosensors are IMDs that measure biological phenomena and send data to a more powerful device for storage or analysis. They range from high-data-rate imaging devices for the eye or brain to extremely low-data-rate for glucose or other metabolites in the body. A subcutaneous sensor involves an implanted biosensor that acts as a lab on a chip, conducting a small experiment on a sensor at molecular or electrochemical level. More advanced subcutaneous sensors are under development now that can detect drugs and endogenous human metabolites, and simultaneously calibrate for temperature and pH. Recent examples of subcutaneous biosensors include injectable subcutaneous devices that are remotely powered by a bandage-like patch that also provides a data link to a higher level wearable device (as shown in Fig. 1), possibly a body area network or, eventually, a higher-level health information system [1].

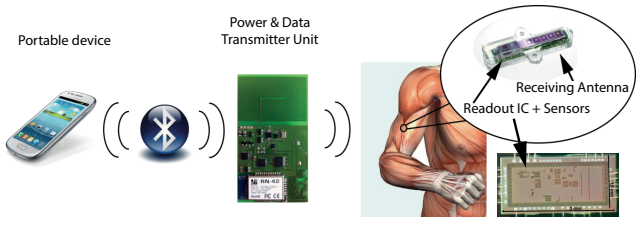

Fig. 1. Fully implantable subcutaneous medical device powered by a patch located on top of the skin. The patch is wirelessly connected to a smart phone for further data analysis and decision-making.

Subcutaneous biosensors require a special set of security and privacy [1]. A key problem with fully implanted sensors is that small infrequent wireless transmission poses a greater privacy risk than large or continuous transmissions. For example, a sensor may take several minutes to complete its task, then deliver only a few bytes of data; giving this information a high value per bit that may make it an attractive target. Short data transmissions necessitate careful use of a cipher, especially if the sensor data take only a few different values. On the other hand, when a biosensor includes a patch that is meant to pair with the sensor, additional risks arise. For example, the patch of an unconscious patient can be removed and replaced by another patch. Other challenges are low-power and low-cost implementation, potential side-channel attacks, and key management issues. Conventional key management schemes can be used to allow access to the data by authorized parties from physicians, to emergency personnel, insurance providers, and even the user.

In [2] a lightweight wireless protocol for IMDs is presented that leverages well-studied wireless and cryptographic technologies. In [3], [4], a hardware implementation of the stream cipher Hummingbird is presented. In [5], the use of block ciphers in IMD security is investigated. Recently, use of sponge-based hash functions for authenticated encryption was introduced [20]. Keccak, the winner of the SHA-3 competition [6], [7] is the best known and most analyzed sponge-based secure hash function. It allows various block sizes and different modes of operation.

This paper presents a lightweight cryptographic system integrated onto a multi-function subcutaneous biosensor prototype. This design uses the recently standardized Keccak secure hash function implemented in an authenticated encryption mode. The resulting heterogeneous system provides a unique and fundamental capability by immediately encrypting and signing

978-1-4799-2346-5/14/$31.00 ©2014 IEEE

the sensor data upon its creation within the body. To the best of our knowledge, this is the first cryptographic system for implantable biosensors until now.

Section II describes the implantable device and its system level design. The threat models are presented in Section III. In Section IV we present the implemented encryption system.

II. System overview

The conceptual view of a subcutaneous IMD that receives power via the inductive link is shown in Fig. 2 [8]. It consists of a molecular sensor array for metabolite detection, a pH and a temperature sensor for calibration, a multi-layer inductor for powering and communication, and the front-end IC. The front-end IC controls and reads out the sensor array and transmits the measured data back to the patch. The front-end IC is where the encryption and authentication system is implemented so that the sensor data is signed and encrypted upon its creation inside the body.

Fig. 3 shows the block diagram of the front-end IC. The IC consists of a control and readout unit that can be configured, according to the received commands from the patch, to perform different types of electrochemical measurements on different sensing sites of the sensor array. The detailed description of the control and readout part of the IC are presented in [9] and [10]. An analog to digital converter is implemented in the IC to digitize the measured data. The digital data goes through the data preparation unit to form a 16-bit size data. This data then goes through the encryption unit. The encryption unit takes four consequent data to form a 64-bit plaintext, and outputs a 64-bit ciphertext. The ciphertext, which is also divided in four words, is streamed out by the Tx/Rx interface. The streamed-out data can be sent out by backscattering through the inductive link. The external inductor is on a wearable patch described in [11] which is placed on top of the device. The design of the inductive link is presented in [12]. The parameters of the Encryption/Decryption unit can be set through JTAG.

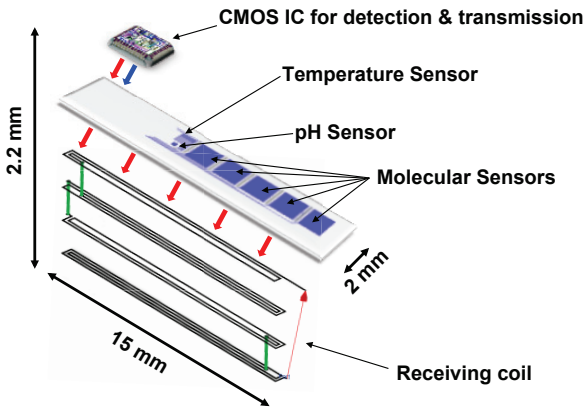

Fig. 2. The conceptual view of the subcutaneous IMD of Fig. 1. It receives power via an inductive link (reprinted from [8]). It consists of a sensor array for metabolite detection and calibration. The front-end IC controls and reads out the sensor array and transmits the measured data back to the patch. The front-end IC is where the encryption system is implemented.

The patch sends the data to a higher-level system like a smart phone of a laptop through Bluetooth, for decryption, data analysis, display, and decision-making. The patch is fully controllable from the higher-level system. The system commands the patch to start/stop sending power to the subcutaneous IMD, as well as the configuration commands.

III. Threat models

Personal health data has the potential to be misused for financial gain, discrimination, tracking or violence among others [13]. However the implementation of strong security is at odds with the low-cost and low-power system described in this paper. Hence we take a somewhat non-traditional and asymmetric approach by relying on the trust of standard key distribution in higher levels of the system where cost is not so important.

The key classes of IMD vulnerabilities researchers have identified are control vulnerabilities, in which an unauthorized person can gain control of an IMD's operation or even disable its therapeutic services, and privacy vulnerabilities, in which an IMD exposes patients data to an unauthorized party. Both kinds of vulnerability may be harmful to patients' health outcome, and are avoidable [1].

Two threat scenarios we consider are: *(i)* trusted patch is removed and placed on a rogue implant (e.g. falsified data for insurance fraud) *(ii)* rogue patch is used to extract data from a trusted implant. (e.g. stealing of personal health data)

Our scheme also avoids potential weaknesses in the patch or in the Bluetooth link and higher levels. The patch is a low-cost device that cannot afford expensive tamper-proofing. Thus we must avoid storing secrets on the patch that could be somehow extracted and then used to clone the patch or otherwise impersonate the patch. The lightweight Bluetooth link does not need to be secure in our scenario either. Our approach avoids the need for two-way authentication by automatically encrypting and signing all outgoing data. This avoids potential replay or relay attacks, both recently demonstrated in automotive and smart-card applications [14]. We do not protect against potentially malicious control of the device. This is a topic for future research, but we expect standard authentication techniques to be used as a defence. Malicious control could either destroy or falsify biosensor data.

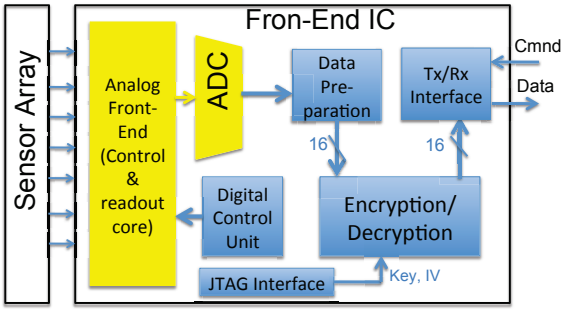

Fig. 3. The block diagram of the front-end IC. The analog blocks are coloured in yellow and the digital blocks in blue.

By selecting the newly standardized Keccak scheme, we benefit from the large amount of analysis and testing performed during the standardization process. In contrast, proprietary cryptographic schemes are often quickly broken due to their lack of exposure to the academic community.

An open topic is the possibility of side-channel attacks due to implementation issues. These could take the form of power, timing of electromagnetic analysis, or more active fault injection techniques. These will be similar to recent work on RFID side-channels [15]. It has become generally accepted that publishing of attacks and vulnerabilities provides more general insights about the security of systems [16].

IV. Security Module

Security of biosensor data has to be guaranteed in various levels: During measurement and processing, from outside observers (also known as side-channel attackers [17]), during communication from third parties, and during storage from unauthorized users. There are several algorithms and standards designed and extensively analysed to achieve these targets. The internationally accepted *Advanced Encryption Standard*, AES, is perhaps the most widely used encryption algorithm. It is very well-analysed, tested, and proved to be secure. However, encryption alone is not sufficient. Another important operation that has to be performed on the secure data is authentication, which is also very well-established and standardized by *National Institute of Standards and Technology* (NIST). Authenticated encryption combines both authentication and encryption in order to provide confidentiality, integrity and authenticity of the data, simultaneously. It has proven to be much more effective, especially on resource-limited devices, than simultaneous use of an encryption algorithm and an authentication algorithm.

Block cipher based special modes of operation, such as CCM, CWC, OCB, EAX and GCM [22], are the most popular authenticated encryption schemes. More recently, use of sponge-based hash functions as authenticated encryption primitives has been proposed [18]. A sponge function or a sponge construction is a class of algorithms with finite internal state that takes an input bit stream of any length and produces an output bit stream of any desired length. It is built from three components: *(i) A state memory*, S, containing b bits: It is divided into two parts, R of size r bits and C of size $c = b - r$ bits. The parameter r is called the bitrate and c is the capacity. *(ii) A function*, f, of fixed length that permutes or transforms the state memory. *(iii) A padding function* P: It appends enough bits to the input string so that the length of the padded input is a whole multiple of the bitrate, r. The padded input can thus be broken into r-bit blocks.

With its arbitrarily long input and output sizes, the sponge construction allows construction of various cryptographic primitives such as a hash function, a stream cipher or a *message authentication code* (MAC) [19]. Keccak is the best known and most thoroughly analysed sponge-based hash function [6] and it offers a very lightweight construction, especially for hardware implementations [21]. Keccak can also be tweaked to operate with reduced state size, which make it even more lightweight and the ideal choice for our application.

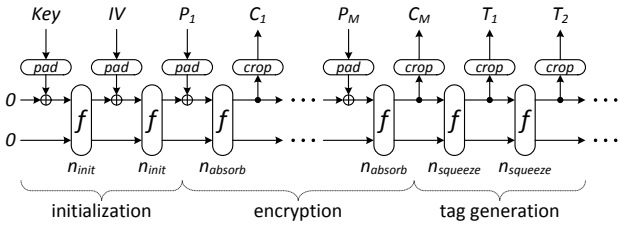

Fig. 4. DuplexSponge construction for authenticated encryption

We use Keccak in DuplexSponge configuration, which is based on the SpongeWrap run in duplex mode [20]. In this mode, the key and the *Initialization Vector* (IV) are added to the zero initial state as a whole or in chunks. This process is known as the initialization phase, where the internal state of the cipher is initialized with both secret key and non-secret IV. Following this phase, duplex operation begins, where the incoming plaintext is processed in blocks defined by the bit rate, r. The sponge function absorbs each incoming data block into its internal state, while the corresponding ciphertext block is generated in parallel. Upon completion of processing of all plaintext data, the authenticated tag is squeezed from the internal state in the finalization phase.

The generalized scheme is illustrated in Fig. 4, where *pad* and *crop* functions are simple as bit addition and bit removal, respectively. In modified forms of the scheme, such as donkeySponge or monkeyDuplex, it is also possible to use to the whole state input size b rather than the bitrate r for key and IV absorption. These specific forms even allow different round counts for n_{init}, n_{absorb} and $n_{squeeze}$ in order to increase the average throughput. In our case, we have used the same number of rounds for all in order to guarantee the security claim of the Keccak proposal.

However, instead of using the standard sizes for bitrate and capacity, we reduced the overall state size in order to achieve a compact implementation with a security level that would not have been possible at this cost with any other authenticated encryption scheme. The data block size and state size are selected as 4 and 100 bits, respectively. Together with 2 bits of padding and one bit of parity, this corresponds to a datarate $r = 7$, which provides first order preimage security of 86 bits ($= b - 2 \times r$) and second order preimage security of 46 bits ($= (b - r)/2$). The corresponding round number is chosen as 16, as stated in the Keccak specification.

The circuit for the security module is shown if Fig. 5. It is composed of the security core and the interface wrapper. Upon start, the 80-bit parallel key is read from the key register in 4-bit packages. It then starts receiving 16-bit data packages (48-bit IV followed by 64-bit sensor data – plaintext) from the sensor interface, which it also processes in 4-bit packages. All the key, IV and plaintext data are absorbed into the sponge state. IV and ciphertext are sent to the transmitter. Finally, the internal state is squeezed from the security core in 4-bit packages in order to extract the 32-bit message authentication tag. All the 4-bit extracted data are converted

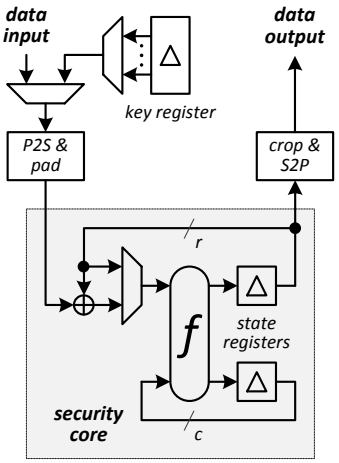

Fig. 5. The implementation of the biosensor security module: permutation based authenticated encryption

to 16-bit parallel data at the output serial-to-parallel converter. Each 4-bit package is processed in 16 rounds.

In order to achieve low power, we opted for a low bandwidth tweak of the Keccak secure hash function used in authenticated encryption mode. We also made aggressive utilization of bit-serial architectures in an effort to reduce combinational logic and minimize switching activity. While it may be argued that such an approach might be risky from a power analysis security point-of-view, we believe that the low data rates of the system will make it impractical to mouth a power analysis side-channel attack. Yet, this claim is to be tested, which in fact is one of our future targets.

The security core alone occupies only 1550 gate-equivalents (GE), which is the smallest authenticated encryption core reported up-to-date. Together with the interface wrapper, total area becomes 2280 GE. The simulated power consumption of the whole design is below 7 μW at 500 KHz system clock. Processing of each 4-bit block takes 20 clock cycles, resulting in a total of 640 cycles for initialization, 320 cycles for encryption and 160 cycles for tag generation.

V. Conclusions

To protect the wireless data transmission and to provide security and privacy for the IMD information, we designed and implemented a lightweight security system that uses a tweaked version of the Keccak secure hash function implemented in an authenticated encryption mode. The system is implemented in 0.18 μm standard CMOS technology and is fully integrated with the frontend electronics of the IMD. It consumes only 7 μW with a throughput of 100 Kbps. Tests on the hardware are planned soon. The implemented cryptosystem takes into consideration the unique threat models and constraints of the implantable biosensors. Therefore, it is a suitable cryptosystem to be integrated into the future IMDs to avoid vulnerabilities in both control and privacy.

VI. Acknowledgement

The research has been funded in part by the project IronIC++ that is financed with a grant from the Swiss Nano-Tera.ch initiative and evaluated by the Swiss National Science Foundation. This work was supported in part by SRC task 1836.074, US NSF grants 0923313 and 0964641 and US DHHS grant 90TR0003/01.

References

[1] W. Burleson and S. Carrara (Eds.), *Security and Privacy for Implantable Medical Devices,* Springer, 2014.

[2] S. Hosseini-Khayat, *A lightweight security protocol for ultra-low power ASIC implementation for wireless Implantable Medical Devices,* International Symposium on Medical Information and Communication Technology (ISMICT), pp. 6-9, 2011.

[3] X. Fan et al, *Lightweight implementation of Hummingbird cryptographic algorithm on 4-bit microcontrollers,* International Conference on Internet Technology and Secured Transactions, pp.1-7, 2009.

[4] X. Fan et al, *FPGA implementations of the Hummingbird cryptographic algorithm* IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 48-51, 2010.

[5] C. Beck, D. Masney, W.Geiselmann, G. Bretthauer, *Block cipher based security for severely resource-constrained implantable medical devices,* International Symposium on Applied Sciences in Biomedical and Communication Technology, (ISABEL), pp. 62:1-62:5, 2011.

[6] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, *The Keccak SHA-3 Submission, submission to NIST (Round 3)*, 2011.

[7] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, The Keccak sponge function family, http://keccak.noekeon.org (17 June 2014).

[8] S. Carrara, A. Cavallini, S. Ghoreishizadeh, J. Olivo, G. De Micheli, *Developing highly integrated subcutaneous biochips for remote monitoring of human metabolism,* IEEE Sensors conference, 2012.

[9] S. Ghoreishizadeh, S. Carrara and G. De Micheli, *A configurable IC to control, readout, and Calibrate an array of biosensors,* European conference in circuit theory and design (ECCTD), 2013.

[10] S. Ghoreishizadeh, C Boero, A. Pullini, C. Baj-Rossi, S. Carrara and G. De Micheli, *Sub-mW reconfigurable interface IC for electrochemical sensing,* Submitted to the Biomedical Circuits and Systems Conference, (BioCAS), 2014.

[11] J. Olivo, S. Carrara, G. De Micheli, *IronIC Patch: A Wearable Device for the Remote Powering and Connectivity of Implantable Systems,* Proceedings of the IEEE Instrumentation and Measurement Technology Conference (I2MTC), pp. 286-289, 2012.

[12] J.Olivo, S.Carrara, and G.De Micheli, *A study of multi-layer spiral inductors for remote powering of implantable sensors,* IEEE Transactions on Biomedical Circuits and Systems, vol.7, no.4, pp. 536-547, 2013.

[13] W. Burleson, S.S. Clark, B. Ransford, K. Fu, *Design challenges for secure implantable medical devices,* Proceedings of the 49th Annual Design Automation Conference (DAC), 2012.

[14] A. Francillon, B. Danev, S. Capkun, *Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars,* In Proceedings of the Network and Distributed System Security Symposium (NDSS), 2011.

[15] T. Kasper et al, *New Methods for Cost- Effective Side-Channel Attacks on Cryptographic RFIDs,* In Workshop on RFID Security, 2009.

[16] D. Basin, S. Capkun, *The Research Value of Publishing Attacks,* Communications of the ACM, vol. 55 no. 11, 2012.

[17] S. Mangard, E. Oswald, T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security),* Springer-Verlag New York Inc., 2007.

[18] G. Bertoni et al, *Duplexing the Sponge: Single-Pass Authenticated Encryption and Other Applications*, 18th international workshop on Selected Areas in Cryptography (SAC), pp. 320-337, 2011.

[19] M.O. Saarinen, D. W. Engelz, *A Do-It-All-Cipher for RFID: Design Requirements,* IACR Cryptology ePrint Archive, 2012.

[20] J. Daemen, *Permutation-based Encryption, Authentication and Authenticated Encryption,* Directions in Authenticated Ciphers, (DIAC), 2012.

[21] L. Henzen et al, *Developing a Hardware Evaluation Method for SHA-3 Candidates,* Cryptographic Hardware and Embedded Systems, 2010.

[22] M. J. Dworkin, *Recommendtation for Block Cipher Modes of Operation – Methods and Techniques,* NIST Special Publication SP 800-38A, 2001