A 415 nW Physically and Mathematically Secure Electro-Quasi-static HBC Node in 65nm CMOS for Authentication and Medical Applications

Shovan Maity, Nirmoy Modak, David Yang, Shitij Avlani, Mayukh Nath, Josef Danial, Debayan Das, Parikha Mehrotra, Shreyas Sen
Purdue University

Abstract—Applications such as secure authentication, remote health monitoring require secure, low power communication between devices around the body. Radio wave communication protocols, such as Bluetooth, suffer from the problem of signal leakage and high power requirement. Electro QuasiStatic Human Body Communication (EQS-HBC) is the ideal alternative as it confines the signal within the body and also operates at order of magnitude lower power. In this paper, we design a secure HBC SoC node, which uses EQS-HBC for physical security and an AES-256 core for mathematical security. The SoC consumes 415nW power with an active power of 108nW for a data rate of 1kbps, sufficient for authentication and remote monitoring applications. This translates to 100x improvement in power consumption compared to state-of-the-art HBC implementations while providing physical security for the first time.


I. INTRODUCTION

Secure Communication around the Human Body is critical for applications like connected healthcare through physiological signal monitoring and secure authentication using wearable key, primarily needing data-rates (DR) <50kbps (Fig. 1). For example 256b key transfer with 50ms latency requires a data rate of 5.12kbps, or I-ch EMG data acquisition with 16b resolution at 500sps results in a data rate of 8kbps. Perpetual battery-free operation or years of operating lifetime with small batteries for wearable patches calls for sub µW power consumption for these low-Data Rate communication, while simultaneously calling for end to end security. Human Body Communication (HBC) is the most promising technique for body area network communication achieving orders of magnitude lower power than traditional Bluetooth low energy [1], [2]. However, previous implementation used MHz frequency range leading to 1) > 40µW power 2) lack of physical security, i.e. signals are snoopable by nearby attackers. Recently, in [3], the authors have described the physics of containing the transmission within the human body using low frequency (10kHz-1MHz) Electro-QuasiStatic (EQS) signals. While encryption provides strong-resistance against brute-force attacks, they are still vulnerable and the strongest security is achieved if the attacker doesn’t have access to the physical signal itself. In this paper, we demonstrate end-to-end secure communication SoC through combination of AES 256 providing mathematical security and the first EQS-HBC IC implementation, providing physical security, all within 415nW total power, leveraging the low frequency operation of EQS-HBC.

The frequency used for HBC heavily impacts the signal leakage (Fig. 2) and hence the vulnerability to a nearby attacker. Signal transmission in the EQS regime (f < 10s of MHz) enables signal confinement within a range of <1cm around most of the body and <15 cm near transmitting device, providing physical security.

Previous HBC implementations primarily used 50Ω termination at the receiver, resulting in a high loss at low frequencies (f < \(\frac{1}{\text{R}_{\text{int}} C_{\text{load}}}\)) due to the capacitive return path (Fig. 3a). Hence, the frequency range of operation for those implementations were generally >10MHz ( [1], [2], [4], [5]) leading to significant signal leakage out of the body. Capacitive high impedance termination enables flat band HBC channel

Authorized licensed use limited to: Purdue University. Downloaded on April 08,2021 at 05:08:25 UTC from IEEE Xplore. Restrictions apply.
II. SYSTEM ARCHITECTURE

The overall SoC has a digital transmitter, AES-256 core and a mixed signal receiver (Fig. 4). Low-DK broadband implementation will suffer from high loss (< 100kHz), imposing stringent sensitivity requirements, motivating narrowband modulation to improve sensitivity. Also, it is necessary to choose a \( f_c < 10 \text{MHz} \) for EQS physical security. A narrowband architecture with low carrier frequency and low baseband-frequency (for low-DR), minimizes overall system power. Along with EQS physical security an AES-256 core enables strong end-to-end security by providing mathematical security. Since, the signal leakage in EQS-HBC is very close to or below the noise floor, it is only possible for an attacker to sniff the signal through averaging over a long time. Frequency Hopping (FH) at the transmitter enhances the physical security of EQS-HBC by denying the attacker averaging capability over a narrow band of frequencies.

A. Transmitter Design

The fully-synthesized EQS-HBC transmitter (Fig. 5) has a programmable PRBS generator along with external data loading capability. the input data is deserialized, encrypted through an AES-256 core, serialized and subsequently used for OOK modulation, chosen for simplicity and low power. Direct Digital Synthesis (DDS) of the OOK signal is done by utilizing the baseband data as a control signal to a multiplexer

B. Receiver Design

The EQS-HBC receiver front-end (Fig. 6) utilizes a 2-stage current starved self-biased common source amplifier, which is ultra-low power due to the low carrier frequency of EQS-HBC. A passive, gate biased, tunable, 4 stage envelope detector (ED) [6] is used for demodulation due to the relatively relaxed sensitivity requirements. This is also suitable for reception...
of the transmitted signal with variable carrier frequency due to frequency hopping. Since the carrier to data rate ratio is 100 in this work compared to 10^6 in [6], a 4-stack ED was adopted. The ED restricts the maximum baseband data rate for a fixed carrier frequency, requiring tunability through bias control. A resettable integrator provides low pass filtering to reject the carrier feedthrough on the ED output and high gain at low power, utilizing the low-DR. A regenerative latch-based sampler is used to digitize the signal. An integrating Mueller-Muller CDR is used to provide phase alignment between data and clock from a digitally synthesized 16-phase clock generator, which uses off-chip crystal based reference without PLL, suitable for low carrier frequency operation.

C. AES 256 Encryption Core

The AES 256 core has a parallel data path implementation with 16 parallel sbox look up tables for each byte operation (Fig. 3b). The input data is deserialized over 128 cycles for 128 bit plain text input. The 14 encryption rounds creates an additional 14 cycle latency. The ciphertext is serialized and transmitted over 128 cycles at the transmitter end.

III. MEASUREMENT RESULTS

A. Power, Performance Results

The EQS-HBC SoC node, fabricated in 65nm CMOS technology, takes a 0.17mm^2 active area. The transmitter power, dominated by the output buffer dynamic power, varies from 38nW (Data Rate=1kbps,f_c=100kHz) to 240nW (DR=10kbps,f_c=1MHz) (Fig. 7a). The AES core runs at baseband clock and its power consumption is dominated by leakage power for such low data rates. Hence, power is minimized by running the transmitter at a supply voltage of 0.4V achieving 42nW active power operation (Fig. 7c). Fig.7 shows the EQS-HBC receiver performance with 0.54UI timing margin for a BER of 10^{-5} at 10 kbps data rate. To minimize power, the carrier frequency is reduced keeping data rate constant and shows acceptable BER of 10^{-4} at 10 kbps DR and 500kHz carrier frequency, as shown in Fig. 7d . The receiver shows a sensitivity of 400µV (64dBm with 50Ω for comparison) for minimum power operation at 0.5V supply, providing enough sensitivity even for 60dB EQS-HBC channel-loss with 0.4V transmitted voltage. With a higher supply voltage operation of 0.7V the receiver shows a sensitivity of -72dBm at 1 kbps and -63dBm at 10 kbps DR (Fig. 7e). Operating at the lowest power mode requires 227nW for physical security, with an additional 188nW for mathematical security through encryption (Fig. 7f).

B. Secure Key Transfer Demonstration

The feasibility of secure EQS-HBC is shown through a demonstration of authentication by secure key transfer between a wearable node with EQS-HBC IC and a PC. Fig. 8 shows the block diagram of the Tx/Rx PCB(5x5cm), through body received signal, out of body leakage waveforms during EQS-HBC transmission. The transmitter board, worn by the user on the wrist, sends the key at 5kbps data rate with carrier frequency of 500kHz and is decoded by an EQS-HBC receiver at the PC end, which is communicated to the PC through USB. The data reception shows a transmission latency of 0.4ms, sufficiently low for authentication applications. Out
IV. Conclusion

This paper presents a low power EQS-HBC SoC with a complete transceiver and AES 256 core for applications like secure authentication, remote health monitoring. The primary design focus has been on providing security (physical, mathematical) and minimizing the total power for low data rate applications instead of energy efficiency (done for higher data rates). The current design achieves 100X lower power while providing stronger security both physically (private space <15cm) and mathematically (AES 256 encryption), opening new possibilities in medical/authentication applications.

REFERENCES


