Low Energy Trusted Private Sensing Using Shared Hardware Random Number Generators

Saro Meguerdichian and Miodrag Potkonjak
Computer Science Department
University of California, Los Angeles
{saro, miodrag}@cs.ucla.edu

***Abstract*—For remote deployment of sensors in potentially hostile environments it is crucial to both ensure that the data is private and trust that the data originated from the sensor in question, at the alleged time and location of sensing, and without tampering. However, another critical requirement is to minimize energy consumption in computation and communication. We satisfy these often contradictory requirements by employing one set of matched public physical unclonable functions (PPUFs) to establish privacy and trust in data, time, and location and another to create a shared hardware random number generator (HRNG) for random challenge generation.**

I. Introduction

Security has been widely recognized as one of the most important metrics of many state-of-the-art and pending systems and applications. Traditional, algorithm-based cryptography has produced a spectrum of elegant and effective security approaches. However, the rapid change of modern applications, mainly due to extensive networking and more recently networked sensing, imposed a new generation of security desiderata and requirements. Specifically, remote trusted sensing where guarantees that particular collected data by a specific sensor is indeed collected by the sensor at the claimed time and claimed location are essential for almost all applications that include computational sensing components.

It has been proven that classical cryptography is not able to solve the remote sensing problem. Recently, hardware based cryptography produced two conceptually similar solutions: one using standard CMOS circuitry [1] and one using nanotechnologies such as III-V semiconductor trees [2]. Both of these solutions integrate public physical unclonable functions (PPUFs) compounded with real-time challenges to authenticate data from remote sensing systems. There are two main limitations of such systems. The first is that two way communication is continuously required between the sensing system and the remote consumer of the collected sensing data. The second equally important ramification is that the high and frequent level of communication induces high energy consumption. In addition, it is important to note that lossy links used by wireless communication equipment are more pronounced in low energy systems and that lossy links can be used by the attacker to mask several classes of security attacks.

Hardware-based security has emerged in the last decade as powerful and effective security mechanisms. A physical unclonable function (PUF) is a physical system with a complex relationship between its inputs and its outputs. Furthermore, due to technological and/or scientific reasons it is not possible to produce two identical PUFs. Hardware-based security has attracted a great deal of attention once it was realized that process variation in standard CMOS technology naturally creates integrated circuits with unique timing, power, and other metrics. Numerous structures, technologies, and PUF data processing techniques have been proposed and analyzed.

However, a PUF can be used only within the framework of secret key cryptography. The public PUF (PPUF) removes this restriction and enables the creation of a broad spectrum of public key cryptography. PPUFs preserve all advantages of PUF-based techniques over classical cryptography, including resiliency against physical and side channel attacks and much faster and lower energy execution of security protocols.

There are currently two main mechanisms for the creation of PPUFs. The first uses a large, preferably exponential, gap between execution on a unique integrated circuit and simulation. The key idea is that many questions related to the properties of the integrated circuit such as delay between an input and an output can be easily answered by the owner of the integrated circuit but require excessive time when these questions are answered using simulation. Essentially, the properties of each gate or transistor serve as a public key and the availability of the integrated circuit corresponds to a secret key. Numerous questions about PPUFs, including their operational and environmental stability, have been studied [3][4][5][6][7].

The second mechanism is device aging. For example, all transistors and in particular PMOS transistors are subject to increase of their threshold voltage if they are under stress, i.e. if they act as open switches. The increased threshold voltage has a number of consequences including reduced speed (increased delay) and reduced leakage energy. Therefore, now it is possible to match characteristics of a subset of gates on two different integrated circuits. The actual speed of aging follows exponential decay rules. The speed of device aging depends on the local temperature. Usually an hour or less of device aging is required to increase the threshold voltage by several millivolts and induce linearly proportional time delay.

Hardware random number generators have much longer history. However, all of the currently proposed hardware random generators have certain important limitations. Among them is the main obstacle for their use in security protocols: it was not possible to create two or more identical random number generators. We overcome this limitation by employing the device aging-based PPUF as the main component for the creation of hardware random number generators. A simple by powerful observation is that the PPUF can be used as the core for production of random number generators because there are no correlations between input and output bits.

In order to prevent replacement of PPUFs and hardware random number generators, their gates are shared with the regular logic of the sensor and control systems. Note that the new technique is not restricted to use in sensing systems and can be also used in other systems such as computation and communication in such a way that trusted network processing is enabled.

A. Organization

The rest of the manuscript is organized in the following way. In the next section we summarize the most relevant related work in hardware-based security, in particular that which is related to the security of remote sensing systems. In Section III we introduce our

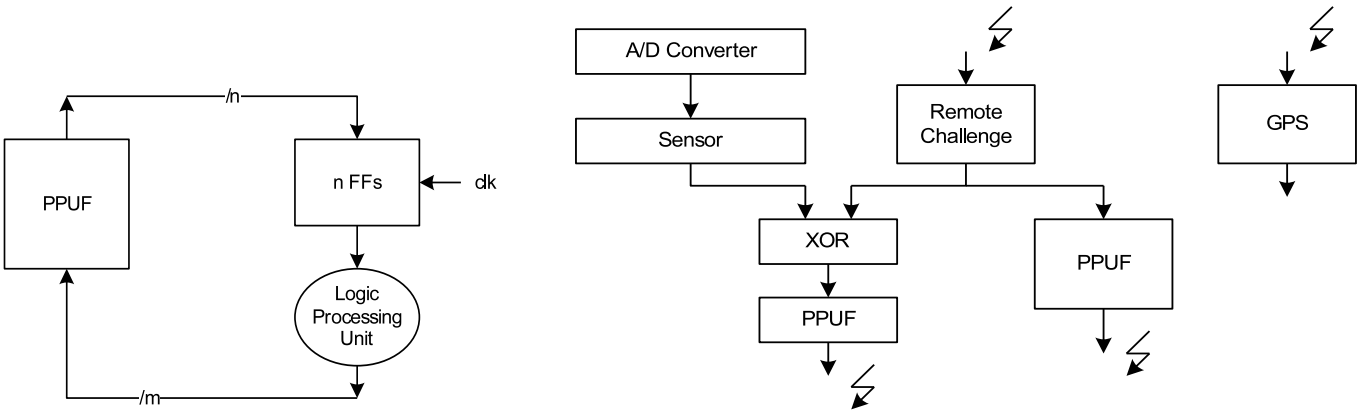

Fig. 1: (a) Basic architecture for the new HRNG and (b) challenge-based system architecture for trusted remote sensing [1].

key technical novelty, the PPUF-based hardware random number generator that is used in Section IV to create a new low energy approach for remote trusted sensing. We conclude in Section V.

II. Related Work

We now briefly survey the most relevant related previous research. The focus is on two broad topics: (i) embedded sensor networks and collection and processing of collected data; and (ii) trust and trust-related security techniques. In addition, we survey work on PUFs, PPUFs, and hardware random number generators.

Rapid development of low-energy sensor and wireless communication technologies resulted in a broad spectrum of research and development projects in the creation of a new type of distributed embedded system called the sensor network. Networked embedded sensing is a relatively new research area that studies the collection of sensor data. Embedded sensor networking addresses a wide spectrum of tasks such as deployment, coverage, energy efficient operation, data integrity, compression, and calibration [8][9][10][11][12][13][14][15][16][17][18].

There is a number of privacy preserving techniques [19][20][21][22][23][24] as well a variety of reputation preserving and transitive reputation schemes [25][26][27][28][29]. There are two previously proposed techniques from trusted remote sensing [1][3] that depend on the notion of random challenges that have been widely used in many cryptography and system security scenarios [19][30][31][32].

Since its introduction in 2009, the PPUF has been comprehensively studied [3][4][6][5][33][2][34][35][36]. Device aging and related gate level characterization techniques have been also used for other applications such as hardware Trojan horse detection [37][38][39][40][41][42][43][44][34].

Various types of hardware random number generators have been developed, based on clocking of random pulse generators, quantum mechanical properties, or other physical sources of variation such as temperature fluctuations, with multiple silicon implementations [45][46][47][48][49]. Due to general instability and high overheads in implementing hardware random number generators, a common practice is to use the hardware random number generator to generate a seed for a pseudorandom number generator. To the best of our knowledge, our work is the first to create a seeded hardware random number generator whose randomness is derived from process variation while maintaining difficulty to predict the generated random number even if the seed is known.

III. Hardware Random Number Generator

We introduce a new type of hardware random number generator (HRNG). The new HRNG has two new noble properties that enable its usage for remote trusted sensing and many other security tasks. The first property is that it can be easily integrated with standard CMOS logic. The second is that it is possible to create exactly k identical HRNGs in such a way that the creation of a $(k+1)$th HRNG is not possible due to process variation.

Figure 1a shows the basic architecture that is used for the new HRNG. The key basic component of new HRNG is a PPUF that is placed in the feedback loop. The feedback loop also includes a certain amount of processing logic that is used for further improvement of the randomness of the HRNG. The use of a PPUF as the basic building block has several advantages. First, we can use device aging-based techniques for the matching of two PPUFs: one at the sensor device and one at the system that communicates with the sensing system. Several such techniques are presented in [3]. Even more importantly, it is well known that PPUFs produce very difficult to predict output for any given input.

Given a random seed s_i, the PPUF computes the response $R(s_i)$ and generates the next seed s_{i+1}. One simple value for s_{i+1} is $R(s_i)$ itself. However, it is crucial to note that one of the inherent properties of our architecture is that responses to two challenges are more likely to differ if the challenges themselves differ greatly. In other words, the Hamming distance of two responses is likely to increase as the Hamming distance of their challenges increases.

Therefore, one powerful method that is still simple in terms of hardware overhead is to use either $R(s_i)$ or $\overline{R(s_i)}$, depending on which one results in a higher Hamming distance between s_{i+1} and s_i. Additionally, standard unbiasing techniques first proposed by Von Neumann in 1951 can be applied to essentially increase the entropy (i.e. decrease the compressibility) of the generated numbers in terms of passing all statistical tests [50].

The crucial observation is that because PPUFs are difficult to predict and simulate and impossible to clone, no attacker can generate the same sequence of random numbers given the same seed. However, because a pair of PPUFs can be matched, two parties can match their PPUF-HRNGs. As a result, by sharing an initial seed (which does not have to be kept secret), the two parties can generate the same sequence of random numbers that they can then securely consider to be shared secrets.

There are several important observations about the new approach. The first is that it requires exactly one clock cycle for all processing

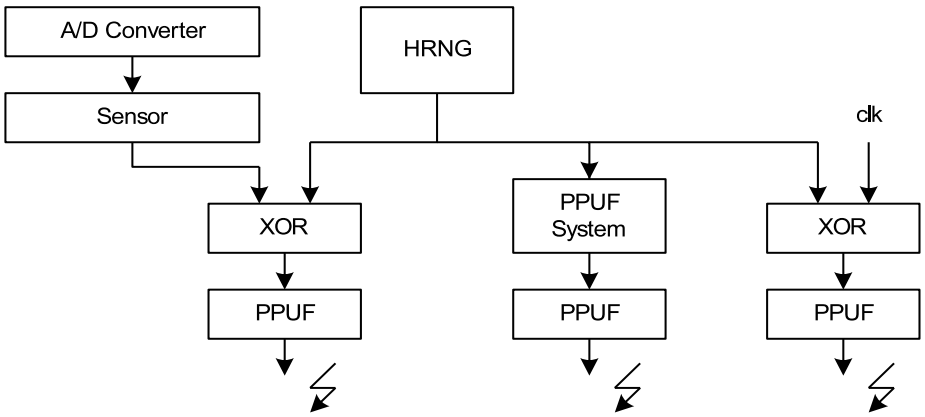

Fig. 2: The new approach for trusted remote sensing.

required for generation and one clock cycle for its verification. Therefore, in a sense this is the ultimate efficiency. The integration of the hardware random number generator with processing logic of the sensing and controlling system is done exactly in the same way that it was done in the integration of the PPUF with combinational logic presented in [1]. The overall system is symmetric in a sense that not only can the control system authenticate data from the sensing system but the authentication can be also conducted in the other direction, where the sensing system authenticates data from the control system. This can be very important in secure real-time control applications.

IV. Trusted Remote Sensing

In this section we introduce a new HRNG-based approach for trusted remote sensing with reduced communication cost. We start by summarizing previously introduced techniques for trusted remote sensing that utilize randomly and remotely generated challenges to ensure security. After that we introduce a new system architecture that eliminates the need for remote generation of challenges through the usage of synchronized HRNGs. Finally, we analyze and compare the new approach with the two previous techniques.

A. Traditional Trusted Remote Sensing

Figure 1b shows a challenge-based system architecture for trusted remote sensing [1]. The key idea is to communicate from a remote location to the sensor a challenge that consists of 32 or 64 or some other number of bits. The challenge is XOR-ed with the input to the sensor. Since the challenge is not known in advance to the potential attacker and since the simulation of the PPUF takes prohibitively long time, the integrity of the reported sensed information is ensured. In addition to checking the sensing information, one can also check if the reported sensing data was indeed sensed by the claimed sensing system. For that purpose, one can either independently use the challenge for verification that the claimed system indeed is what was deployed or use it simultaneously to verify a particular reported sample. Signals from a global positioning system (GPS) are used for the establishment and authentication of the time when a particular sample is collected. Our final remark is that for secure generation of authentication data and its secure flow it is mandatory that the PPUF is merged with the actual logic of the sensor system.

B. Synchronized HRNG-based Trusted Remote Sensing

Figure 2 presents a graphical illustration of the new approach for trusted remote sensing. At a very high level of abstraction it is similar to the system presented in the previous subsection. The key difference is that all requirements for external communication to the sensing system is eliminated through the use of the synchronized random number generators. In principle, the three PPUFs at the bottom of the figure can be eliminated. However, that may greatly facilitate statistical security attacks. When the PPUFs are employed, security of communicated data is ensured.

It is interesting and important to analyze the new system architecture for remote trusted sensing. It uses a total of four PPUFs. It has been shown that less than a thousand gates are more than sufficient for the creation of high quality unclonable devices. Also note that one can exploit trade-offs between the width and height of a PPUF to balance its randomness and its correlation.

Finally, we conclude this subsection by explaining the matching of delays of corresponding gates in two different integrated circuits. The idea is simple. We first conduct gate-level characterization, where we measure the delay of each gate. The next step is that the faster gate is intentionally made subject to device aging so that its delay is matched to the delay of the slow gate. The key observation is that by using this technique only of a subset of gates can be matched, due to the limited impact of NBTI-based device aging. In the final phase all gates that are not matched are isolated from the PPUFs using either hardware or software techniques.

C. Comparison of the New PPUF HRNG-based Approach with Previous Techniques for Remote Trusted Sensing

There are only two major differences from the two previous architectures for remote trusted sensing. The new approach uses synchronized PPUF-based hardware random number generators for simultaneous issuing of random challenges both at the sensing and remote controlling systems. This technique implies that after initial synchronization of the two hardware number generators there is no need for further communication of the challenges. Therefore, there is no more communication overhead, i.e. the communication requirements are exactly equal to ones in regular unsecured approaches for remote data collection. Finally, the PPUF-based hardware number generators can be used in conjunction with synchronized system clocks at the control and the sensor system for time authentication without employment of GPS signals that additionally significantly reduces energy consumption and the overall cost of secure remote sensing while increasing the scope of deployment to locations that are not exposed to GPS signals.

The second difference is that the use of synchronized PPUFs completely eliminates the need for simulation. In other words, there is no more need for simulation and essentially the security latency is eliminated. This property is of high importance in many distributed

systems such as ones where real-time control is required and used.

V. Conclusion

Trusted remote sensing, which provides guarantees that a particular sample collected by an unsecured remote sensing system was indeed collected by that hardware placed at a specific location at a claimed time, is of fundamental importance for essentially any embedded sensing application. We have developed a new approach for trusted remote sensing that does not only guarantee security requirements but also drastically reduces communication requirements and minimizes energy consumption. The essential enabling new concept is a pair of matched PPUF-based hardware random number generators. The matching of delay-based PPUFs is accomplished through NBTI-based device aging of transistors. The PPUF-based hardware random number generator is designed in such a way that it does not allow reading or injection of its inputs and outputs. The main next step includes experimental demonstration of the approach for trusted remote sensing.

Acknowledgment

This work was supported in part by the NSF under awards CNS-0958369, CNS-1059435, and CCF-0926127, and is based upon research performed in collaborative facilities renovated with funds from the National Science Foundation under Grant No. 0963183, an award funded under the American Recovery and Reinvestment Act of 2009 (ARRA).

References

[1] M. Potkonjak, S. Meguerdichian, and J. L. Wong, "Trusted sensors and remote sensing," *Sensors*, pp. 1104–1107, 2010.

[2] J. B. Wendt and M. Potkonjak, "Nanotechnology-based trusted remote sensing," *Sensors*, pp. 1213–1216, 2011.

[3] S. Meguerdichian and M. Potkonjak, "Security primitives and protocols for ultra low power sensor systems," *Sensors*, pp. 1225–1228, 2011.

[4] S. Meguerdichian and M. Potkonjak, "Device aging-based physically unclonable functions," *DAC*, pp. 288–289, 2011.

[5] S. Meguerdichian and M. Potkonjak, "Matched public PUF: ultra low energy security platform," *ISLPED*, pp. 45–50, 2011.

[6] M. Potkonjak et al., "Differential public physically unclonable functions: architecture and applications," *DAC*, pp. 242–247, 2011.

[7] S. Meguerdichian and M. Potkonjak, "Using standardized quantization for multi-party PPUF matching: foundations and applications," *ICCAD*, 2012.

[8] S. Meguerdichian et al., "Coverage problems in wireless ad-hoc sensor networks," *InfoCom*, vol. 3, pp. 1380–1387, 2001.

[9] S. Meguerdichian et al., "Localized algorithms in wireless ad-hoc networks: location discovery and sensor exposure," *MobiHoc*, pp. 106–116, 2001.

[10] S. Slijepcevic and M. Potkonjak, "Power efficient organization of wireless sensor networks," *ICC*, pp. 472–476, 2001.

[11] S. Slijepcevic, S. Megerian, and M. Potkonjak, "Location errors in wireless embedded sensor networks: sources, models, and effects on applications," *SIGMOBILE MC2R*, vol. 6, no. 3, pp. 67–78, 2002

[12] J. Feng, F. Koushanfar, and M. Potkonjak, "System-architectures for sensor networks: issues, alternatives, and directions," *ICCAD*, pp. 112–121, 2002.

[13] F. Koushanfar, et al., "Low power coordination in wireless ad-hoc networks," pp. 475–480, *ISLPED*, 2003.

[14] J. Feng, S. Megerian, and M. Potkonjak, "Model-based calibration for sensor networks," *Sensors*, pp. 737–742, 2003.

[15] G. Veltri et al., "Minimal and maximal exposure path algorithms for wireless embedded sensor networks," *SenSys*, pp. 40–50, 2003.

[16] J. L. Wong, R. Jafari, and M. Potkonjak, "Gateway placement for latency and energy efficient data aggregation," *LCN*, pp. 490–497, 2004.

[17] J. Adriaens, S. Megerian, and M. Potkonjak, "Optimal worst-case coverage of directional field-of-view sensor networks," *SECON*, pp. 336–345, 2006

[18] F. Koushanfar, N. Taft, and M. Potkonjak, 'Sleeping coordination for comprehensive sensing using isotonic regression and domatic partitions," *InfoCom*, pp. 1–13, 2006.

[19] W. Diffie and M. Hellman, "New directions in cryptography," *TIT*, vol. 22, no. 6, pp. 644–654, 1976.

[20] I. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography*, Cambridge Univ Pr, 1999.

[21] D. Boneh and H. Shacham, "Fast variants of RSA," *Cryptobytes*, pp 1–8, 2002.

[22] K. Paterson, "ID-based signatures from pairings on elliptic curves," *Electronics Letters*, vol. 38, no. 18, pp. 1025–1026, 2002.

[23] D. Hankerson, S. Vanstone, and A. Menezes, *Guide to Elliptic Curve Cryptography*, Springer-Verlag New York Inc., 2004.

[24] J. Fry and M. Langhammer, "RSA and public key cryptography in FPGAs," *Tech. Report TR CF-032305-1.0*, Altera Corporation, 2005.

[25] P. Resnick et al., "Reputation systems," *CACM*, vol. 43, no. 12, pp. 45–48, 2000.

[26] P. Resnick and R. Zeckhauser, "Trust among strangers in Internet transactions: empirical analysis of eBay's reputation system," *Advances in Applied Microeconomics*, vol. 11, pp. 127–157, 2002.

[27] S. Buchegger and J. Le Boudec, "A robust reputation system for mobile ad-hoc networks," *P2PEcon*, 2004.

[28] M. Nowak and K. Sigmund, "Evolution of indirect reciprocity," *Nature*, vol. 437, no. 7063, pp. 1291–1298, 2005.

[29] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *DSS*, vol. 43, no. 2, pp. 618–644, 2007.

[30] A. Menezes, P. Van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[31] D. Stinson, *Cryptography: Theory and Practice*, CRC press, 2006

[32] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley Publishing, 2008.

[33] S. Wei, F. Koushanfar, and M. Potkonjak, "Integrated circuit digital rights management techniques using physical level characterization," *Workshop on DRM*, pp. 3–14, 2011.

[34] J. Zheng and M. Potkonjak, "Securing netlist-level FPGA design through exploiting process variation and degradation," pp. 129–139, *FPGA*, 2012.

[35] S. Wei and M. Potkonjak, "Wireless security techniques for coordinated manufacturing and on-line hardware trojan detection," *WISEC*, 2012.

[36] . F. Koushanfar et al., "Can EDA combat the rise of electronic counterfeiting?" *DAC*, 2012.

[37] F. Koushanfar and M. Potkonjak, "CAD-based security, cryptography, and digital rights management," *DAC*, pp. 268–269, 2007.

[38] . Y. Alkabani, F. Koushanfar, and M. Potkonjak, "Remote activation of ICs for piracy prevention and digital right management," *ICCAD*, pp. 674–677, 2007.

[39] Y. Alkabani et al., "Trusted integrated circuits: a nondestructive hidden characteristics extraction approach," *IH*, pp. 102–117, 2008.

[40] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Lightweight secure PUFs," *ICCAD*, pp. 670–673, 2008.

[41] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Testing techniques for hardware security," *ITC*, pp. 1–10, 2008.

[42] A. Vahdatpour and M. Potkonjak, "Leakage minimization using self sensing and thermal management," *ISLPED*, pp. 265–270, 2010.

[43] S. Wei, S. Meguerdichian, and M. Potkonjak, "Gate-level characterization: foundations and hardware security applications," *DAC*, pp. 222–227, 2010.

[44] S. Wei, A. Nahapetian, and M. Potkonjak, "Robust passive hardware metering," *ICCAD*, pp. 802–809, 2011.

[45] G. W. Brown, *History of RAND's Random Digits*, RAND Corporation, 1949.

[46] R. C. Fairfield, R. L. Mortenson, and K. B. Coulthart, "An LSI random number generator (RNG)", *Advances in Cryptography*, pp. 203–230, 1984.

[47] A. Gerosa, R. Bernardini, and S. Pietri, "A fully integrated 8-bit, 20Mhz, truly random numbers generator, based on a chaotic system," *SSMSD*, pp. 87–92, 2001.

[48] T. Stojanovski, J. Pil, and L. Kocarev, "Chaos-based random-number generators. Part II: practical realization," *TCSZ*, vol. 48, no. 3, pp. 382–385, 2001.

[49] V. Fischer and M. Drutarovsky, "True random number generator embedded in reconfigurable hardware," *CHES*, pp. 415–430, 2002.

[50] J. Von Neumann, "Various techniques used in connection with random digits," *Applied Mathematics Series*, no. 12, pp. 36–38, 1951.