Trusted Sensors and Remote Sensing

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

Jennifer L. Wong
Computer Science Department
SUNY Stony Brook University
jwong@cs.sunysb.edu

Abstract— **Remote trusted operation is essential for many types of sensors in an even greater number of applications. It is often crucial to secure guarantees that a particular sensor sample is taken by a specific sensor at a particular time and stated location. We present the first generic system architecture and security protocol that provides low cost, low power, and low latency trusted remote sensing. The approach employs already known randomized challenges and public physically unclonable function with a new concept of interleaved operational and security circuitry.**

I. Motivation and Problem Formulation

Trust plays an essential role in many types of systems and applications ranging from peer-to-peer computing, filtering of information on the web, and recommendation systems to many branches of social networks and e-commerce. Trust is bound to achieve even higher levels of importance because of its increasing use in data centers, mobile systems, and embedded sensing. In mobile systems, due to energy and power restrictions, in many situations it is advantageous to delegate computation to desktop systems, clusters, or data centers. Finally and maybe most importantly, distributed embedded sensing raises the importance of trust to an even higher level. For example, when a home owner goes to a Hawaii conference and wants to observe sensors in his house, it is crucial that he is convinced that the received sensor readings are actually from the deployed sensors, that sensors have not been repositioned, and that the timestamp associated with the data is correct. Without this trust the data is of little value. In addition to trust, in many applications privacy is of the highest importance. However, unlike trust, the privacy of data is easily addressed using state-of-the-art public key encryption techniques.

Our primary objective is the creation of a new conceptual approach for trusted remote sensing that leverages a recent new hardware-based technique for privacy of data (cryptography). To answer this problem we use three security primitives. As the first security primitive, we use the recently introduced public physical unclonable function (PPUF) [1]. A PUF is a complex physical system with a large number of inputs and outputs, where the mapping from the inputs to the outputs cannot be predicted in any reasonable time, and the system can not be reproduced due to scientific or technological difficulties [2]. A PPUF is a PUF in which all parameters of the system are published as a public key, and where one can compute any output for a given input but only using algorithms of high computational complexity that are many orders slower than the execution of the input vector on the PPUF physical system. For example, the execution time may be less than one nanosecond while the simulation time is many seconds. PPUFs realize public key cryptographic protocols and simultaneously are resilient against physical and side channel attacks. The second conceptual enabler for trusted remote sensing is interleaving (overlapping) of security (PPUF) and sensing, computation, and communication circuitry that ensures trusted information flow. Finally, in order to prevent replay attacks, we employ randomized challenges.

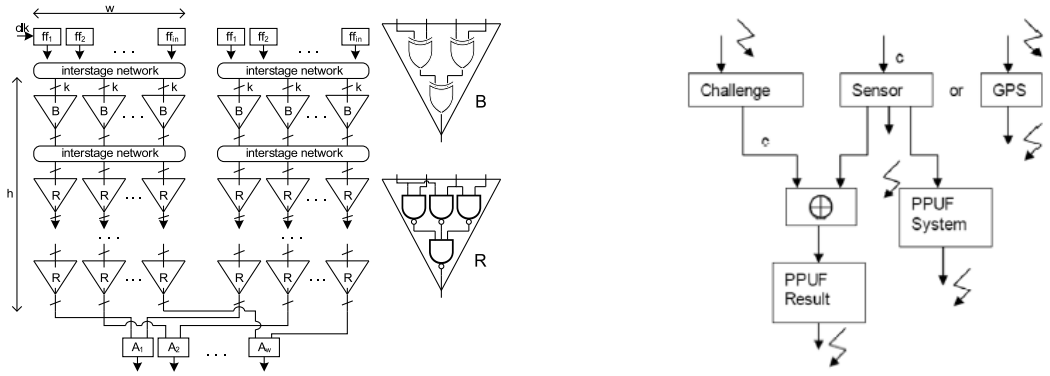
In summary, our goal is to design distributed unattended sensors and accompanying security protocols in such a way that they are simultaneously provably secure and practical (low hardware overhead, low energy, and low realization costs), and that they support fast and easy verification while still posing exponentially difficult tasks on attackers. In addition, we seek resiliency against an arbitrary side channel or physical attack.

II. Related Research

In this section, we briefly survey the most directly related work. The emphasis is on one side on sensor networks and computational sensing and on another on trust and trust related security techniques.

Progress in sensor and wireless communication technologies in the last decade resulted in comprehensive efforts in the creation of a new type of distributed embedded systems–the sensor network. Computational sensing is a new discipline that processes, interprets, and enables decision making using data provided by embedded sensor networks. Numerous topics including deployment, coverage, energy efficient operation, data integrity, compression, and calibration have been studied [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16]. A comprehensive survey of many sensing and wireless communication issues in embedded sensing is given in [17].

The privacy preserving techniques are addressed using a variety of public key encryption algorithms [18] [19] [20] [21] [22] [23] [24] such as RSA and elliptical curves. There is significant work on a variety of reputation and transitive reputation schemes [25] [26] [27] [28] [29] [30], in peer-to-peer computing, WWW data filtering, and social networks [31] [32] [33] [34] [35] [36]. Partly, the newly proposed techniques for trusted sensing depend on the notion of random challenges that have been widely used in many contexts in cryptography and system security [37] [38] [20] [39] [40] [41] [42]. There is also a wide variety of numerical, linear algebra, and statistics



(a) (b)

Fig. 1: (a) PPUF Architecture (b) Trusted Sensing System and Flow.

techniques for gate level characterization that determine the delay, leakage power, or metrics of interest for the use of PPUFs [43] [44] [45] [46] [47] [48].

III. Basic Idea, Design, and Operational Flow

When designing a sensor system, numerous design metrics must be considered, such as system lifetime, accuracy, deployment, low power, costs, etc. One of the most important aspects, which is also the most difficult to address in the physical world, is privacy and trusted operation of the sensing system. Users request information privacy at all levels of the system: data collection, transmission, processing, and storage. In addition, users are typically remotely accessing the system and require authentication of the data in terms of its sensor origin, location, and collection time. This amount of sensing trust is crucial in order to protect the user from physical attacks. As previously discussed, privacy is typically resolved using cryptographic methods. However, sensing trust is a new security area which requires the development of new mechanisms and protocols. We propose the first approach for the operation of trusted devices and sensors by utilizing PPUFs as the trust mechanism. This new method of integrating PPUFs along with existing hardware in the design creates a trusted information flow within the system. The system, which requires minimal hardware overhead (less than one thousand gates) and minimal computational power, is resilient to physical, side channel, and software attacks.

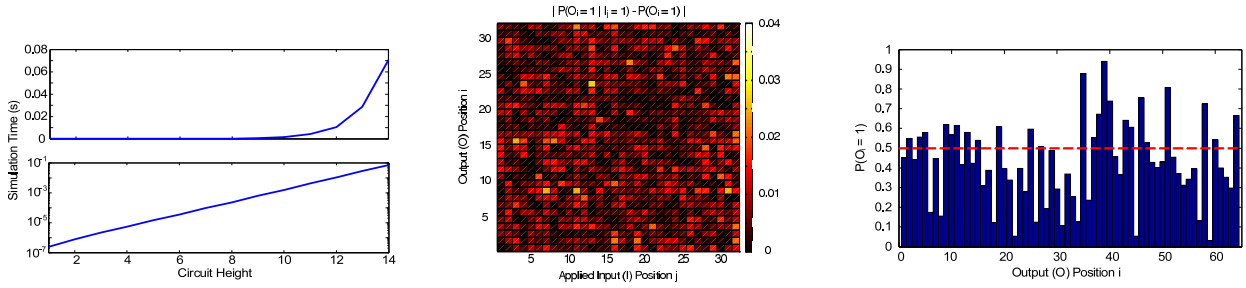
The proposed PPUF architecture consists of a multiple-input, multiple-output physical system. The system produces pairs of input and output vectors that are sufficiently large such that they are difficult to guess. Figure 1a illustrates the proposed structure which consists of booster (B) and repressor (R) cells. Booster cells are used to increase the switching frequency of the output with respect to the input. Repressor cells perform the opposite function, to reduce the switching frequency. The PPUF propagates a challenge vector through the booster and repressor components and through partially random interstage networks, to produce a physically unique response vector. Each physically unique PPUF, due to process variations, will produce different response vectors. This differential PPUF (dPPUF) architecture is described in detail in the technical report [49].

We have developed the first trusted architecture for remote sensing. This architecture combines standard sensing hardware with two PPUFs and a challenge generation system as shown in Figure 1b. The challenge generation system obtains a binary key from the trusted authority and produces a pseudo-random bit string on demand. This bit string is XORed with the sensor data/output. The first PPUF block, PPUF Result, is used to authenticate the collected sensor data. In addition, the second PPUF, PPUF System, is used to authenticate the time and location of the sensor data either through the sensor clock itself in the case of time or from an integrated GPS subsystem.

IV. Trusted Sensor Information Flow in the Remote Sensor

In addition to the trusted sensor architecture, Figure 1b also shows the trusted information flow. The three-piece arrows pointing to the right indicate information coming from the authenticating party (AP), and the three-piece arrows pointing to the left show the information flowing from the trusted sensor (TS) to the AP. The AP sends to the TS a binary string that serves as a challenge. It is combined with the sensor output using the XOR block. The purpose of this block is to create completely unpredictable input values for the PPUF Result system. This is a completely sufficient approach for this task, but one can employ other non-linear and unpredictable functions to combine the challenge and sensor signals in such a way as to further improve security. For example, one potential such approach is to use classical one-way trap door cryptographic functions.

The PPUF Result sends the data back to the AP. The key observation about PPUF Result is that this functional component should have a large number of outputs in order to maximize the advantage of the sensor and system over any attacker. This is due to the fact that the owner must check only a subset of the PPUF result outputs, while the attacker must compute all of them. Each sensor component standardly



(a) (b) (c)

Fig. 2: (a) Exponential growth of simulation time for 1 GHz processor to simulate a PPUF with w=64, in linear and log scales. (b) Conditional probability estimated correlation map between an output bit O_i and input bit I_j. (c) Likelihood of output bit O_i being 1 for a PPUF (w=64, h=10), demonstrating the infeasibility of a random guessing attack.

consists of two main components: a signal transducer and a digital analog converter with other integrated circuits for processing the signal (e.g. denoising and amplification). The PPUF System is used to authenticate the sensor or GPS data. Authentication is performed by the AP by using the original sensor and PPUF Result output.

In addition to authenticating the sensor itself, we have to answer two other questions about its location and the time at which a particular sample was taken. For these two purposes we use exactly the same approach as for the trusted sensor, except that the sensor is replaced with the Global Positioning System (GPS) signal. In principle the GPS can be replaced with any other position and time system, for example distance measurements in circuitry for sensor networks. The GPS signal is completely integrated with other circuitry on the trusted sensor integrated circuit in order to prevent alterations by the attacker. Recall that a GPS signal receives information from at least four satellites for 3D positioning, and timing information originates from the satellite. Therefore, we can authenticate this information in exactly the same way as performed for the sensing circuitry.

There are several advantages that the AP has over any potential attacker. First, the AP has a significantly larger amount of time for computation and verification, whereas the attacker must produce the PPUF outputs in real-time or within a specified time. Note that the attacker can not pre-compute the PPUF outputs prior to the challenge generation. Figure 2a illustrates the exponential growth of simulation time for a 64-bit wide PPUF. Second, the attacker must compute all PPUF outputs for all samples, while the AP can check a relatively small number of challenges and randomly selected bits of each to verify correct operation. Third, the AP can select challenge bits in such a way that they facilitate rapid computation of a subset of the PPUF outputs, reducing required verification computation overhead.

One can define and address a number of security and trust attacks. Nevertheless, it is easy to see that two most likely and most important attacks are infeasible. The first one is random guessing. Random guessing is infeasible because the number of PPUF output bits is rather large, and therefore correct selection of even a subset of the bits is highly unlikely.

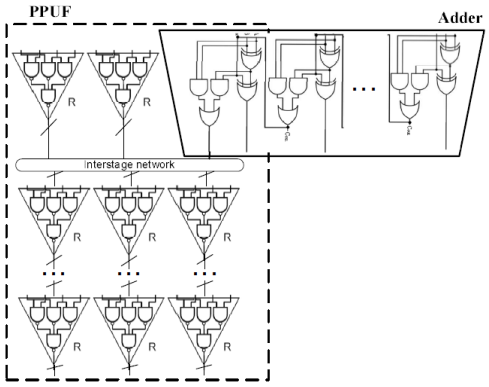


Fig. 3: Interleaved PPUF with Sensor/GPS component (e.g. Adder Used in A/D Circuitry).

Figure 2c illustrates for a given PPUF circuit the likelihood of guessing each of the 64 outputs correctly based on observation of previous challenges. For many of the outputs, the probability is close to the ideal case, demonstrating that the PPUF output is difficult to predict. Figure 2b shows a correlation map between the probability of input and output bits both being 1 for a 32-bit wide PPUF. Note that the map illustrates the probability the output bit is 1 when the input bit is 1.

Another potentially powerful attack is substitution of previously gathered sensor data into the XOR circuit. This attack does not work for the GPS circuitry because its data can be directly routed to the AP. More importantly, it does not work for the sensor circuitry, as shown in Figure 3. The figure illustrates an interleaved PPUF and senor component, such as the adder used in the analog-to-digital converter. By integrating a portion of the sensor circuitry into the PPUF circuitry, any modifications to the sensor itself will impact the delay, leakage power, or other essential properties of the PPUF, making the attack easily recognizable by the AP. In addition, note that the attacker would have to do this alteration in the field while continuing to conduct sensing.

V. Discussion

It is important to observe that all ideas, architectures, and mechanisms of trusted sensing can be directly applied to data

processing or data storage components. Therefore, we can authenticate whether particular information is coming from main memory or coming from a particular processor.

We believe that this research will create new security mechanisms, primitives, and protocols that would greatly increase the application range and applicability of PPUF structures. It also opens the door for combining research in fields like digital signal processing, control theory, information theory, and thermal dynamics with ICs, CAD, and in particular security and cryptography.

VI. Conclusion

We have introduced the first hardware-based system architecture and security protocols for trusted remote sensing that allow information about the source of sensed data and the location and sampling time of the remote sensor to be authenticated with arbitrarily high probability. The approach leverages the concept of randomized challenges and the recently introduced public physically unclonable functions with a new concept of overlapping sensing and security circuitry. The approach is generic and can be applied in various sensing and other applications. Our simulations indicate that it results in very low hardware, delay, and energy overheads.

References

[1] N. Beckmann and M. Potkonjak, "Hardware-based public-key cryptography with public physically unclonable functions," *IH*, pp. 206-220, 2009.

[2] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," *CCS*, pp. 148-160, 2002.

[3] S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M. Srivastava, "Coverage problems in wireless ad-hoc sensor networks," *Infocom*, vol. 3, pp. 1380-1387, 2001.

[4] S. Megerian, F. Koushanfar, M. Potkonjak, and M. B. Srivastava, "Worst and best-case coverage in sensor networks," *TMC*, vol. 4, no. 1, pp. 84-92, 2005.

[5] S. Meguerdichian, S. Slijepcevic, V. Karayan, and M. Potkonjak, "Localized algorithms in wireless ad-hoc networks: location discovery and sensor exposure," *MobiHoc*, pp. 106-116, 2001.

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

[7] G. Veltri, Q. Huang, G. Qu, and M. Potkonjak, "Minimal and maximal exposure path algorithms for wireless embedded sensor networks," *SenSys*, pp. 40-50, 2003.

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

[9] F. Koushanfar, M. Potkonjak, and A. Sangiovanni-Vincentelli, "Fault tolerance techniques in wireless ad-hoc sensor networks," *Sensors*, pp. 1491-1496, 2002.

[10] J. L. Wong and M. Potkonjak, "Search in sensor networks: challenges, techniques, and applications," *ICASSP*, vol. 4, pp. 3752-3755, 2002.

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

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

[13] 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

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

[15] F. Koushanfar, N. Taft, and M. Potkonjak, "Sleeping coordination for comprehensive sensing using isotonic regression and domatic partitions," *INFOCOM*, pp. 1-13, 2006.

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

[17] S. Megerian and M. Potkonjak, *Wireless Sensor Networks*. Wiley Encyclopedia of Telecommunications. Wiley-Interscience, New York, NY, 2003.

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

[19] D. Boneh and H. Shacham, "Fast variants of RSA," *Cryptobytes (RSA Laboratories)*, pp 1-8, 2002.

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

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

[22] N. Gura, et al., "Comparing elliptic curve cryptography and rsa on 8-bit CPUs," *CHES*, pp. 119-132, 2004.

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

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

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

[26] 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.

[27] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," *WWW*, pp. 640-651, 2003.

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

[29] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," *CACM*, vol. 43, no. 12, pp. 45-48, 2000.

[30] P. Resnick and R. Zeckhauser, "Trust among strangers in Internet transactions: Empirical analysis of eBays reputation system," *Advances in Applied Microeconomics*, vol. 11, pp. 127-157, 2002.

[31] L. Adamic and E. Adar, "How to search a social network," *Social Networks*, vol. 27, no. 3, pp. 187-203, 2005.

[32] S. Androutsellis-Theotokis and D. Spinellis, "A survey of peer-to-peer content distribution technologies," *CSUR*, vol. 36, no. 4, p. 371, 2004.

[33] J. Kleinberg, "The convergence of social and technological networks," *CACM*, vol. 51, no. 11, pp. 66-72, 2008.

[34] R. Kumar, J. Novak, and A. Tomkins, "Structure and evolution of online social networks," *SIGKDD*, p. 617, 2006.

[35] D. Liben-Nowell, J. Novak, R. Kumar, P. Raghavan, and A. Tomkins, "Geographic routing in social networks," *PNAS*, vol. 102, no. 33, page. 11623, 2005.

[36] B. Zhou and J. Pei, "Preserving privacy in social networks against neighborhood attacks," *ICDE*, pp. 506-515, 2008.

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

[38] R. Anderson and M. Kuhn, "Tamper resistance: a cautionary note," *USENIX EC*, vol. 2, p. 1, 1996.

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

[40] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. A1bazaar, 2007.

[41] F. Stajano, "The resurrecting duckling," *Security Protocols*, pp. 215-222, 2000.

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

[43] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Techniques for design and implementation of secure reconfigurable PUFs," *TRETS*, vol. 2, no. 1, 2009, pp. 1-33.

[44] Y. Alkabani, F. Koushanfar, N. Kiyavash, and M. Potkonjak, "Trusted integrated circuits: a nondestructive hidden characteristics extraction approach," *IH*, pp. 102-117, 2008.

[45] F. Koushanfar, P. Boufounos, and D. Shamsi, "Post-silicon timing characterization by compressed sensing," *ICCAD*, pp. 185-189, 2008.

[46] M. Nelson, A. Nahapetian, F. Koushanfar, and M. Potkonjak, "SVD-based ghost circuitry detection," *IH*, pp. 221-234, 2009.

[47] M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey, "Hardware Trojan horse detection using gate-level characterization," *DAC*, pp. 688-693, 2009.

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

[49] S. Meguerdichian, M. Potkonjak, A. Nahapetian, and S. Wei, "Differential public physically unclonable functions," UCLA Tech. Report, 2010.