Security Primitives and Protocols for Ultra Low Power Sensor Systems

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

***Abstract*— Security requirements in sensor systems include resiliency against physical and side-channel attacks, low energy for communication, storage, and computation, and the ability to realize a variety of public-key protocols. Furthermore, primitives and protocols that enable trusted remote operation in terms of data, time, and location are essential to guarantee secure sensing. By integrating physically unclonable functions (PUFs) directly into sensor hardware and using device aging to securely match groups of sensors, we enable a variety of ultra low power security protocols for trusted remote sensing, including authentication and public key communication.**

I. Introduction

Trust and privacy are becoming increasingly more important facets of communication following the ubiquity of distributed sensor networks, social networks, cloud computing, and mobile systems. As we move toward distributed processing, storage, and sensing as the platform of choice, trust in data integrity and guarantees of privacy become essential considerations in security. In the domain of sensor networks, trust has the following four components: sensing location, sensing time, sensor integrity, and the data origin. In other words, upon receiving data, the owner of the sensor must trust that the data originated from the correct sensor, that the sensor was in the correct location at the correct time, and that the sensor was functioning properly. A sensing platform that, for example, monitors a home to detect burglars becomes useless if the data cannot be trusted.

Privacy, on the other hand, is also essential for many applications. Public key cryptographic communication protocols have been heavily studied and proposed to create data privacy, but in general require high computational resources and power consumption. We have two primary objectives. The first is to enable public key communication and other cryptographic protocols that induce low area, energy, and computation overheads such that they are suitable for deployment in low-power distributed or embedded sensing systems. The second objective is to create a trusted sensing platform in all 4 dimensions of sensing trust (data, location, time, and sensing hardware).

To achieve both goals, we introduce a conceptually new class of public physically unclonable functions (PPUFs). A physically unclonable function (PUF), whose silicon implementation was introduced by Gassend et al. in 2002 [1], is a complex physical input-output mapping which cannot be predicted or replicated. PPUFs, introduced by Beckmann et al. more recently in 2009 [2], allow PUF characteristics to be published and used as a public key.

Traditional PUFs use process variation (PV) as the key mechanism for uniqueness. PV is the deviation of device parameters from nominal values due to natural imperfections in the manufacturing process. We propose a new security primitive that uses a combination of coordinated device aging and gate disabling to allow multiple parties to customize their PPUFs to the same exact configuration and therefore create the same input-output mapping, while making it impossible for any attacker to match the same configuration. Thus, the coordinated parties can communicate privately. To then enable trust, we interleave the new PPUF with the sensing hardware such that the sensor data, GPS output, and clock timestamp can each be communicated by the sensor to the sensor owner without possibility of tampering by an attacker.

II. Related Work

The sensor network as we know it today is a culmination of a decade of research in distributed wireless systems ranging from deployment and coverage to energy optimization and data integrity [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17]. PUFs [1] [18] and more recently PPUFs [2] [19] have emerged as promising security platforms, and a wide variety of architectures, applications, and protocols have been proposed [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32]. These devices leverage challenge randomization and other well studied cryptographic and system security principles [33] [34] [35] [36] [37]. Our work differs from previous efforts because for the first time we use coordinated device aging and gate disabling in addition to PV to create a trusted remote sensing platform.

III. Preliminaries

We use the gate-level delay model from Markovic et al. [38], shown in Equation 1, where k_{tp} is the delay-fitting parameter, C_L is load capacitance, V_{dd} is supply voltage, n is subthreshold slope, μ is mobility, C_{ox} is oxide capacitance, W is gate width, L is effective channel length, $\phi_t = kT/q$ is thermal voltage, k_{fit} is a model-fitting parameter, σ is the drain induced barrier lowering (DIBL) factor, and V_{th} is threshold voltage.

$$D = \frac{k_{tp} \cdot C_L \cdot V_{dd}}{2 \cdot n \cdot \mu \cdot C_{ox} \cdot \frac{W}{L} \cdot (\frac{kT}{q})^2} \cdot \frac{k_{fit}}{(\ln(e^{\frac{(1+\sigma)V_{dd} - V_{th}}{2 \cdot n \cdot (kT/q)}} + 1))^2} \tag{1}$$

We adopt the quad-tree model proposed by Cline et al. [39] for variations in L and the Gaussian distribution proposed by Asenov et al. [40] for variations in V_{th}, the two physical parameters that are impacted by PV [41].

$$\Delta V_{th} = A \cdot e^{\beta V_G} \cdot e^{-E_\alpha / kT} \cdot t^{0.25} \tag{2}$$

We use the negative bias temperature instability (NBTI) aging model proposed by Chakravarthi et al. [42], shown in Equation 2, where ΔV_{th} is threshold voltage shift, A and β are constants, V_G is the applied gate voltage, E_α is the measured activation energy of the NBTI process, T is the temperature, and t is time.

IV. New Security Primitive

We have developed a new class of PPUF that leverages the intrinsic process variation inherent in silicon devices as well as user-controlled, coordinated device-aging and gate-disabling to enable trusted remote sensing and ultra low power public key protocols between groups of sensor nodes. The device architecture is shown in Figure 1a. The design is derived from the following 3 main components:

(i) *Racing signals.* The device output is not based on traditional functionality, but rather on the relative timing delays between an exponential number of paths from input to output. Conceptually, input signals ”race” through gates with different timing delays and arrive at output arbiters (A), which output 0 or 1 depending on which input arrives first (e.g. which signal ”won” the race).

(ii) *Alternating booster (B) and repressor (R) cells for exponential simulation complexity*. Output unpredictability and device simulation complexity depend on the logic gates through which the input signals propagate. The role of a booster cell is to exponentially increase the switching frequency. We use, for example, a 4-input XOR gate as a booster cell whose output switches each time any of its inputs switches. In other words, the booster cell's output switching frequency is on average 4 times the switching frequency of any of its inputs. A 4-input NAND gate is an example of a repressor cell that switches for 12.5% of input switches, on average. We use the following four alternating repressor cells which maintain the 12.5% repression rate while maximizing unpredictability:

$$\begin{aligned} y_1 &= x_1' \cdot x_2 \cdot x_3 \cdot x_4 \\ y_2 &= x_1 \cdot x_2' \cdot x_3 \cdot x_4 \\ y_3 &= x_1 \cdot x_2 \cdot x_3' \cdot x_4 \\ y_4 &= x_1 \cdot x_2 \cdot x_3 \cdot x_4' \end{aligned}$$

Conceptually, due to maximal boosting and unpredictable repressing of signals, increasing the height (number of levels) of the circuit exponentially increases simulation complexity while linearly increasing delay and power.

Algorithm 1 PPUF Coordination

```
1: The sensor determines which of its PPUF's gates are within a $\Delta delay$ faster than the corresponding gate on the owner's PPUF such that aging of the gate to match delay is possible.
2: The sensor calculates from Equations 1 and 2 the $\Delta V_{th}$ and aging time required to match the owner's PPUF gate, and ages it for the required time.
3: The owner repeats the same process for those gates which are faster than those on the sensor's PPUF.
4: All remaining unmatched gates are disabled on both PPUFs.
```

Algorithm 2 Public Key Communication

```
1: The sensor and sensor owner conduct the PPUF coordination protocol to obtain identical PPUFs.
2: The sensor chooses a random challenge and computes the PPUF response to that challenge.
3: The sensor combines the PPUF response with the data to be sent using a simple XOR.
4: The sensor sends both the random challenge and the combined response/data message to the sensor owner.
5: The sensor owner computes the PPUF response to the challenge. Because the PPUFs are identical after coordination, the response will also be identical.
6: The sensor owner recovers the original data by computing the XOR of the combined response/data message and the computed PPUF response.
```

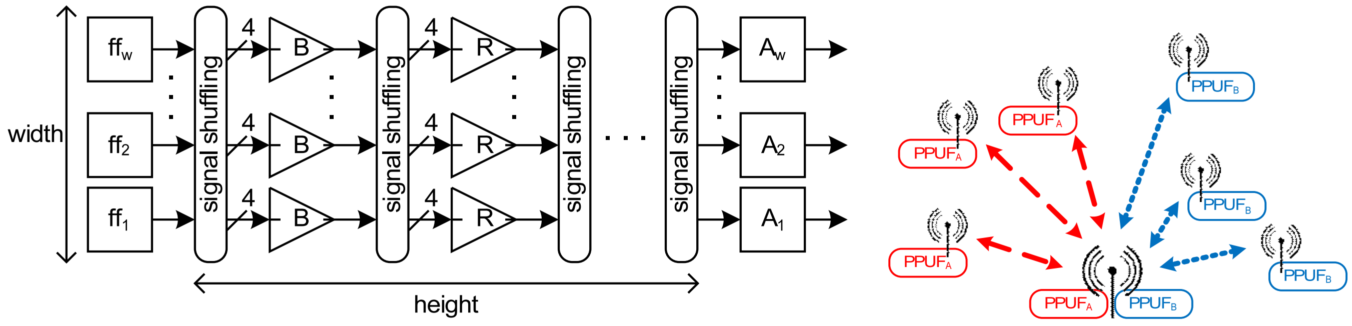
(iii) *Maximally mixing interconnection network to enable gate disabling*. The interconnection network between levels of gates is crucial in maximizing output unpredictability and simulation complexity while maintaining the ability to disable some gates without sacrificing security (Section V-A). Therefore, we use interconnection networks that are both balanced (each gate in one level drives the same number of gates in the next level) and interleaved (each output depends on each input).

These components enable all of our desiderata for a secure sensing platform: (i) low power, delay, and area overheads; (ii) resilience to a variety of statistical, simulation, emulation, and protocol attacks; and (iii) the ability to realize a variety of public key cryptographic protocols.

A. Resilience Against Attacks

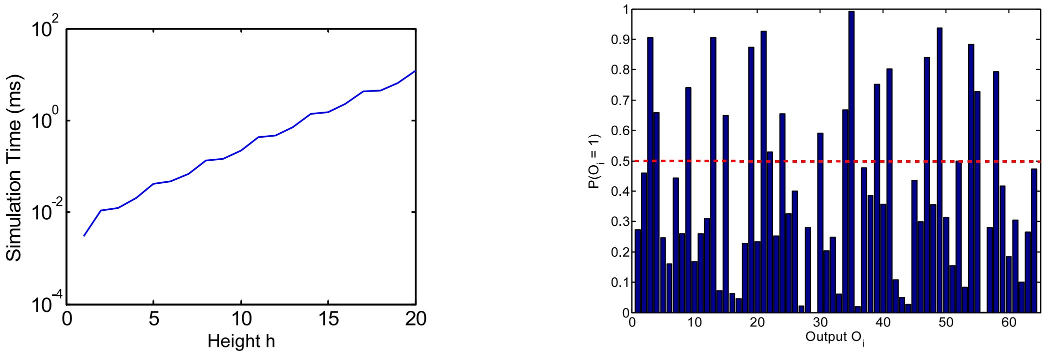
1) Simulation: Figure 2a shows the simulation effort vs. PPUF height on a logarithmic scale, for a coordinated PPUF of width 1024. Clearly, the simulation time grows exponentially with height, rendering simulation intractable for even modest PPUF sizes.

2) Prediction: If the outputs are predictable, an attacker could attempt to subvert the security protocols by correctly



(a) (b)

Fig. 1: (a) New PPUF architecture that enables multi-party PPUF coordination. Input signals race from flip-flops (FF) through alternating levels of booster (B) and repressor (R) cells to arbiters (A), whose outputs depend on which input signal arrives first. (b) Conceptual sensor network with coordinated PPUF matching. A sensor owner uses one PPUF (A, red dashed line) to communicate with some sensors and another (B, blue dotted line) to communicate with others.



(a) (b)

Fig. 2: (a) Simulation time of a coordinated PPUF vs. height, for $w = 1024$. (b) Probability that a particular output bit of a coordinated PPUF equals 1, shown for a representative subset of outputs for $w = 1024$ and $h = 21$.

guessing PPUF outputs. Figure 2b shows the probability that each output will be equal to 1 for a representative set of outputs of a coordinated PPUF with width 1024 and height 21. Ideally, each output will be 1 50% of the time, shown by the red dashed line. We can see that the PPUF output has reasonably high entropy, with a large number of outputs at or near the ideal point.

V. Protocols

A. PPUF Coordination

The key protocol which enables ultra low power public key protocols is coordination of PPUFs owned by multiple parties. The protocol proceeds as described in Algorithm 1 for a sensor and sensor owner, and results in each party having an identical PPUF without the possibility of any attacker being able to match the same configuration. To allow this functionality, we add additional gate control logic to our PPUF primitive. This allows for (i) the gate to be aged with its maximally aging inputs and (ii) the gate to be disabled (prevented from switching). One additional input and multiplexer for each gate is sufficient to achieve these goals. Note that this protocol need only be conducted once during calibration.

B. Ultra Low Power Public Key Communication

The other protocol which is essential for trusted remote sensing is public key communication. The protocol requires that the sensor and sensor owner have coordinated their PPUFs to match an identical configuration. The protocol proceeds as specified in Algorithm 2, for a sensor that is sending data to a sensor owner.

In the domain of sensor networks, low power is key for long sensing lifetime and low cost. Because the PPUF response can be computed in a single cycle, only a very small number of cycles for either party is required to conduct the public key communication protocol to securely send data from the sensor to the sensor owner.

VI. Trusted Remote Sensing: Interleaving Sensing and Security Hardware

Our main goal for trusted remote sensing is to establish trust in the following 4 dimensions related to data delivery:

(i) *Data origin.* Received data is from the actual sensor.
(ii) *Sensor location.* The sensor has not been repositioned.
(iii) *Sensing time.* The data's timestamp is correct.

(iv) *Sensor integrity.* The sensor itself has not been modified.

We achieve the first three desiderata using the PPUF primitive described in Section IV. The overall system and flow is shown in Figure 1b. Essentially, sensor data, GPS data, and clock data are each transmitted to the recipient using the public key communication protocol described in Section V-B. Because the protocol requires only a very small number of clock cycles of computation, there is negligible time and power overhead in computation.

Sensor integrity can be realized by directly interleaving sensing hardware with the PPUF security primitive. In other words, if the functionality of the security hardware (e.g. the delay characteristics of a PPUF) is derived from the physical sensing hardware, then any tampering with the sensor will essentially change the PPUF input-output mapping. This would render the public key communication protocol ineffective and would be immediately detected during the next exchange of messages.

VII. Conclusion

We have presented a new security primitive that enables coordinated PPUF matching by multiple parties to create a shared PPUF instance that cannot be matched by any attacker. We have shown that PPUF coordination between sensor nodes and a sensor owner can enable ultra fast, ultra low power public key communication. Ultimately, we have proposed a generic framework for interleaving sensing and security using PPUF coordination to establish trusted remote sensing in terms of data origin, location, time, and sensor integrity. Simulation results show that the approach maintains a high level of security while inducing low delay, energy, and space overheads.

References

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

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

[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] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[19] U. Rührmair, "SIMPL systems, or: can we design cryptographic hardware without secret key information?" *SOFSEM*, vol. 6543, pp. 26–45, 2011.

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

[21] 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.

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

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

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

[25] M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey, "Hardware Trojan horse detection using gate-level characterization," *DAC*, pp. 688-693, 2009.
26

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

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

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

[29] M. Potkonjak et al., "Differential public physically unclonable functions: architecture and applications," *DAC*, 2011.

[30] S. Meguerdichian and M. Potkonjak, "Device aging-based physically unclonable functions," *DAC*, 2011.

[31] S. Meguerdichian, "Device aging-based PPUFs: architecture and protocols," M.S. thesis, Computer Science Dept., UCLA, 2011.

[32] S. Meguerdichian, "Matched Public PUF: Ultra Low Energy Security Platform," *ISLPED*, 2011.

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

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

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

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

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

[38] D. Markovic et al., "Ultralow-power design in near-threshold region," *Proceedings of the IEEE*, vol. 98, no. 2, pp. 237–252, 2010.

[39] B. Cline, K. Chopra, D. Blaauw, and Y. Cao, "Analysis and modeling of CD variation for statistical static timing," *ICCAD*, pp. 60–66, 2006.

[40] A. Asenov, "Random dopant induced threshold voltage lowering and fluctuations in sub-0.1 um MOSFETs: a 3-D atomistic simulation study," *T-ED*, vol. 45, no. 12, pp. 2505–2513, 1998.

[41] S. Sarangi et al., "VARIUS: a model of process variation and resulting timing errors for microarchitects." *SM*, vol. 21, no. 1, pp. 3–13, 2008.

[42] S. Chakravarthi et al., "A comprehensive framework for predictive modeling of negative bias temperature instability," *IRPS*, pp. 273–282, 2004.