Chapter 1

Trust and Privacy in Medical Systems using Public Physical Unclonable Functions

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, tele-healthcare raises the importance of trust to an even higher level. For example, when a doctor wants to conduct gait diagnostics on a patient who has been wearing a medical smart shoe equipped with multiple pressure sensors and a mote capable of wireless trasmission, it is crucial that both he and the patient are convinced that the received pressure or other readings are actually from the deployed sensors, that the 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. In fact, it is difficult to imagine a domain in which guarantees of privacy are more important than in tele-healthcare, where intimate data about patients is being collected, stored, transmitted, and viewed. In the previous example, the patient and doctor should also be convinced that only they (or perhaps other authorized parties) are able to view the raw patient data sent from the patient to the doctor, the diagnoses sent from the doctor to the patient, or any other conversation between the patient and doctor that should demand confidentiality.

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. As a result, we have two primary objectives. The first is to present public key communication and other cryptographic protocols that induce low area, energy, and computation overheads such that they are suitable for deployment in medical sensing environments, where energy and power are crucial constraints. The second objective is to present a trusted medical sensing platform in all 3 dimensions of sensing trust (data, location, and time).

To address this problem we present three security primitives. The first security primitive leverages a recent new hardware-based technique for privacy of data (cryptography), the physical unclonable function (PUF). A PUF is a deterministic multiple-input multiple-output system that is hard to reverse engineer and simulate. Silicon PUFs are currently by far the most popular and most effective hardware-based security systems that are intrinsically resilient to physical and side channel attacks. Major PUF limitations include the use of secret key cryptography, large storage space requirements, and the ability to realize only a very limited set of security protocols. Recently developed public key PUF schemes such as public physical unclonable functions (PPUFs) and SIMPL remove all these limitations but require that at least one participating party is capable of conducting complex simulations. Therefore, low power and low latency applications cannot be realized using these techniques.

The most recently proposed matched public PUF (mPPUF) preserves all advantages of PPUFs but requires each party in a wide class of security protocols to conduct only a single cycle computation. Therefore, in a sense, the mPPUF is an ultimately low energy and low latency security approach that enables the device to operate in hostile environments. The key idea is to use device aging (e.g. transistor slowdown or wire electromigration) to create two completely identical PPUFs in such a way that the probability that a third PPUF can have the same characteristics is negligible. The mPPUF is the first cryptographic primitive and implementation that requires from all participating parties only a single cycle energy for security protocols such as authentication and public key communication. Also, it is the first scheme that requires only self-trust; each party has control over announcing its own public key using preliminary aging. Through public key elimination of storage and elimination of simulation, the mPPUF combines the best properties of both PUFs (single cycle operation and low energy) and PPUFs (public key security and no storage requirements).

The second conceptual enabler for trusted, private medical systems is interleaving (overlapping) of security (PUF) 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.

1.1 Related Research

In this section, we briefly summarize the most directly related literature in process variation, device aging, PUFs and PPUFs, and trust and privacy.

1.1.1 Process Variation

The primary basis for our approach is inherent PV and gate-level uniqueness in modern and future silicon CMOS technologies [1]. There are several difficult technological problems that preclude fabrication of ICs with the exact feature sizes of gates and wires and levels of doping. They include wafer lattice structure imperfections, non-uniform dopand distribution, mask alignment, and chemical/mechanical polishing [1].

PV exists among gates when gates across ICs are designed to be identical, but due to manufacturing limitations are different and unique in terms of structural and operational properties, such as timing delay and power consumption. As transistors have shrunk in size, the percentage difference in this property has grown. For example, identical gates may have up to 30% difference in timing delays in current 45 nm technology [2]. Furthermore, variability can be increased using intentional random doping and through light exposure. By leveraging PV between identically designed gates and ICs, we can develop a delay-based authentication technique that authenticates ICs, taking advantage of the near impossibility to manufacture two ICs with the same delay characteristics.

It has been widely recognized that modern ICs are unique due to factors such as line edge roughness, polysilicon granularity, and random discrete dopants [3]. Numerous transistor- and gate-level characterization (GLC) techniques have been proposed, including: (i) direct measurement approaches [4]; (ii) schemes that employ FPGA reconfiguration [5]; (iii) approaches that create and observe special IC structures and specialized circuitry [6]; and (iv) non-destructive techniques that construct global measurements and deduce scaling factors of each gate by solving a system of equations [7][8][9][10].

1.1.2 Device Aging

Negative bias temperature instability (NBTI) and hot carrier injection (HCI) are examples of intrinsic phenomena of deep submicron silicon technologies that have detrimental impacts on reliability and speed of operation [11]. Recently, they have attracted a great deal of attention mainly due to reliability issues. NBTI effects are in particular pronounced for PMOS transistors. Its impact continues to increase with each technology node [3].

1.1.3 PUFs and PPUFs

A great impetus for hardware based security was provided by a MIT paper that introduced the first PUF using a mesoscopic optical system [12]. Soon, again at MIT, Devadas and his group proposed the silicon PUF concept and demonstrated its ASIC realization [13].

More recently, Beckmann and Potkonjak proposed the first PPUF structure and used it to construct secure protocols for the exchange of secret keys and for public key cryptographic communication [14]. The essential idea is that the owner of a PPUF publishes its gate-level characteristics, such as delay or leakage energy, which serve as its public key. Therefore, anybody can simulate a small number of input vector challenges using significant run times, but only the owner of the PUF is capable of executing billions or more inputs in any reasonable amount of time. Their approach exploits signal glitching and requires ultra accurate, ultra high frequency clocks and long execution times, at least in the range of hours. A conceptually similar but technically drastically different approach was proposed at the University of Munich [15].

Traditional PUF and PPUF schemes leverage PV [16][17][18]. Recently proposed device aging-based PUFs and PPUFs leverage both PV and device aging [19][20][21]. The mPPUF ensures complete trust self-sufficiency, one cycle ultra low power operation, resiliency against physical and side channel attacks, and high security flexibility.

1.1.4 Trust and Privacy

The privacy preserving techniques are addressed using a variety of public key encryption algorithms [22] [23] [24] [25] [26] [27] [28] such as RSA and elliptical curves. There is significant work on a variety of reputation and transitive reputation schemes [29] [30] [31] [32] [33] [34], in peer-to-peer computing, WWW data filtering, and social networks [35] [36] [37] [38] [39] [40]. 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 [41] [42] [24] [43] [44] [45] [46]. There is also a wide variety of numerical, linear

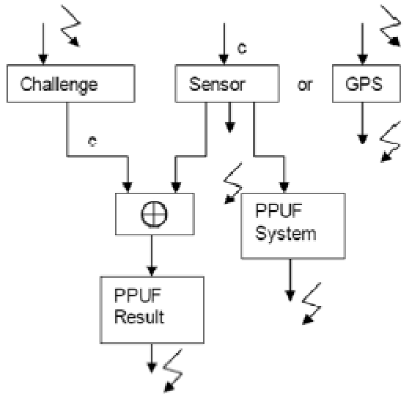


Figure 1.1: Trusted Sensing System and Flow.

algebra, and statistics techniques for gate level characterization that determine the delay, leakage power, or metrics of interest for the use of PPUFs [47] [48] [49] [50] [8] [7].

1.2 Preliminaries

1.2.1 Gate Delay, Power, and Process Variation

We use the gate-level delay and power models from Markovic et al. [51]. The delay model is reproduced in Equation (1.1), where k_{tp} is the delay-fitting parameter, C_L is load capacitance, V_{dd} is supply voltage, n is substreshold 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. Load capacitance C_L is defined in Equation (1.2), where γ is the logical effort of the gate and W_{fanout} is the sum of the widths of the load gates.

$$D = \frac{k_{tp} \cdot C_L \cdot V_{dd}}{2 \cdot n \cdot \mu \cdot C_{ox} \cdot \frac{W}{L} \cdot (\frac{kT}{q})^2} \cdot \frac{k_{fit}}{(\ln(e^{\frac{(1+\sigma)V_{dd}-V_{th}}{2\cdot n \ \ cdot(kT/q)}}))^2} \tag{1.1}$$

$$C_L = C_{ox} \cdot L \cdot (\gamma \cdot W + W_{fanout}) \tag{1.2}$$

There are two parameters that are directly impacted by PV: effective channel length (L) and threshold voltage (V_{th}) [52]. For V_{th}, we adopt the Gaussian distribution proposed by Asenov et al. [53]. Note that gates are not correlated in terms of V_{th}. For L, however, we follow the quad-tree model proposed by Cline et al. [54], which considers the spatial correlations among gates.

In the quad-tree model, the gate-level property (e.g. effective channel length) subject to PV is distributed into multiple levels, with a different number of grids allocated on each level. The grids on each level are assigned variation values that follow a normal distribution. We calculate the total value of the target gate-level property as the sum of the variations on each level of the grids to which the corresponding gate belongs.

We show the quad-tree model for effective channel length L in Equation (1.3), where ΔL_{ij} is the quantitative variation of the i-th level and j-th grid to which the gate belongs; μ_i and σ_i are parameters of the normal distribution at level i.

$$\Delta L = \sum i \Delta L_{ij}, \qquad \textit{where} \qquad \Delta L_{ij} \approx N(\mu_i, \sigma_i) \tag{1.3}$$

Equation (1.4) decribes the leakage power model, and Equation (1.5) describes the gate-level switching power model [51], where α is the activity factor and f is the frequency.

$$P_{leakage} = 2 \cdot n \cdot \mu \cdot C_{ox} \cdot \frac{W}{L} \cdot (\frac{kT}{q})^2 \cdot V_{dd} \cdot e^{\frac{\sigma \cdot V_{dd} - V_{th}}{n \cdot (kT/q)}} \tag{1.4}$$

$$P_{switching} = \alpha \cdot C_L \cdot V_{dd}^2 \cdot f \tag{1.5}$$

Gate-level delay and physical properties can be recovered post-silicon by gate-level characterization [7] and stored as a public key. For the evaluation of presented approach and the presentation of simulation results, we select 45 nm technology and the variabilities in terms of effective channel length and threshold voltage (level of doping) as indicated by these two models.

1.3 Device Aging

We use the aging model proposed by Chakravarthi et al. [55] and shown in Equation (1.6) for the effect of device aging due to NBTI on V_{th} shift, where 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.

$$\Delta V_{th} = A \cdot e^{\beta V_G} \cdot e^{-E_\alpha/kT} \cdot t^{0.25} \tag{1.6}$$

For mPPUF matching, we use static (DC) aging, which can be reversed by removing the applied stress [11]. Note that the model follows a fractional power law; in other words, a relatively large amount of aging happens in a relatively short amount of time, when the input vectors are first applied.

1.4 Basic Idea, Design, and Operational Flow

When designing a tele-healthcare system, numerous design metrics must be considered, such as system lifetime, accuracy, deployment on the body, 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 and in particular tele-healthcare trust is a new security area which requires the development of new mechanisms and protocols. We present 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 mPPUF 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 1.2 illustrates the mPPUF 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 mPPUF propagates a challenge vector through the booster and repressor components and through maximally mixing interstage networks, to produce a physically unique response vector. Each physically unique mPPUF, due to process variations, will produce different response vectors. However, two or more instances of the mPPUF can be matched to each other using combined coordinated aging and gate disabling. For example, one or more motes sampling and transmitting data from sensors across a patient's body can be equipped with a mPPUF that can be matched to a mPPUF in a receiving device at the doctor's office.

We present 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 1.1. 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.

1.5 The Matched Public PUF

We present 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 1.2. 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

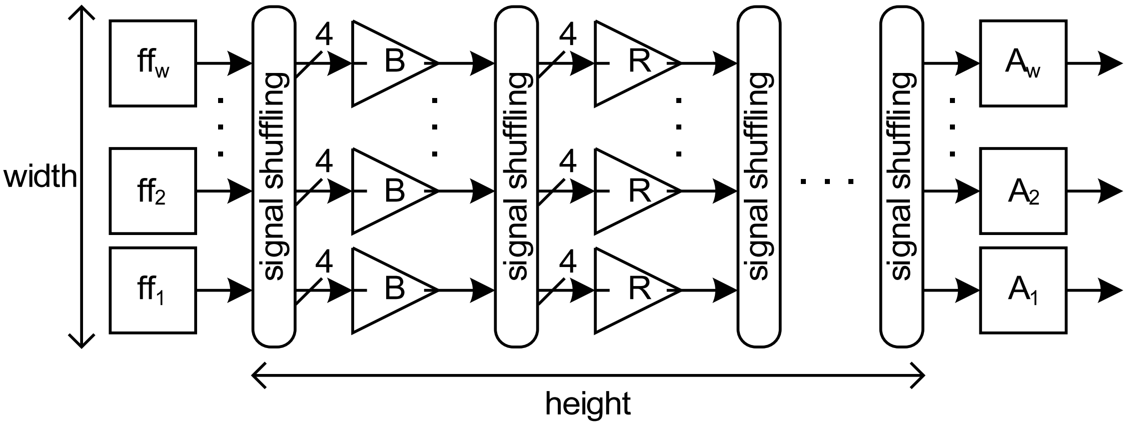


Figure 1.2: New mPPUF architecture that enables multi-party PPUF coordination. Input signals race from flip-flops (FF) through alternating levels of booster (B) and repressor (R) cells to arbiters (A), whose outputs depend on which input signal arrives first.

complexity while linearly increasing delay and power.

(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 1.6.1). 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.

1.5.1 Resilience Against Attacks

Simulation

Figure 1.4 shows the simulation effort vs. PPUF height on a logarithmic scale, for a mPPUF of width 1024. Clearly, the simulation time grows exponentially with height, rendering simulation intractable for even modest PPUF sizes.

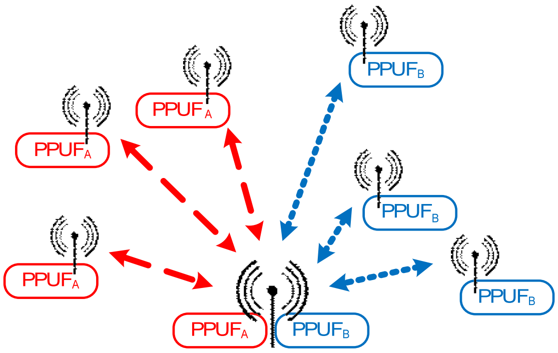


Figure 1.3: Conceptual sensor network with mPPUF matching. A doctor uses one mPPUF (A, red dashed line) to communicate with some sensor nodes on one patient and another (B, blue dotted line) to communicate with sensor nodes on another.

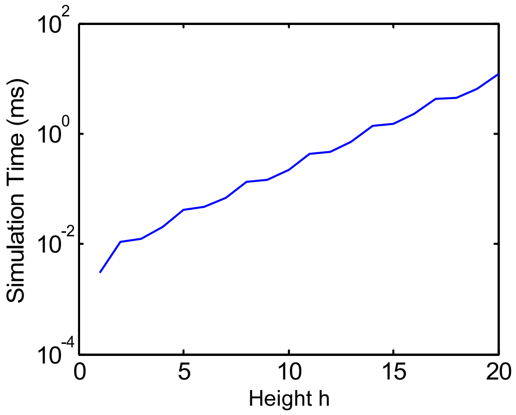


Figure 1.4: Simulation time of a mPPUF vs. height, for $w = 1024$.

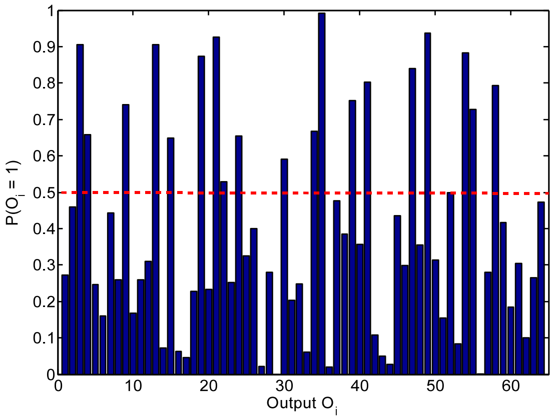


Figure 1.5: Probability that a particular output bit of a mPPUF equals 1, shown for a representative subset of outputs for $w = 1024$ and $h = 21$.

Prediction

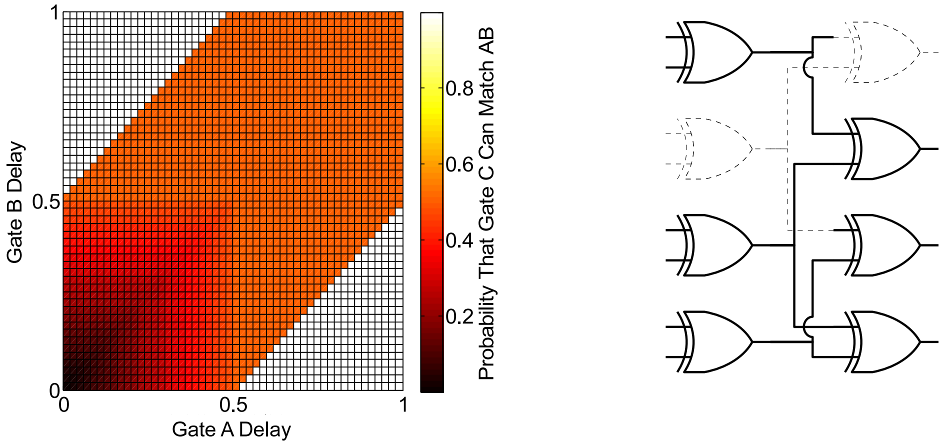
If the outputs are predictable, an attacker could attempt to subvert the security protocols by correctly guessing PPUF outputs. Figure 1.5 shows the probability that each output will be equal to 1 for a representative set of outputs of a mPPUF with width 1024 and height 21. Ideally, each output will 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.

1.6 Protocols

Consider, for example, a doctor, Alice, and a patient, Bob, who want to match their PPUFs. Assume a very simple PV model for delay where individual gate delays follow a uniform random distribution between 0 and 1, and an aging model where maximal aging of a gate increases its delay by 0.5. Without loss of generality, consider the following cases when aging a gate A with delay D_A on Alice's PPUF to match its corresponding gate B with delay D_B on Bob's PPUF:

1. $D_A = D_B$. This is the trivial case. Gates A and B have equal delay, so they are already matched.
2. $D_B - 0.5 \leq D_A < D_B$. Here, gate A is faster than gate B, but not by more than 0.5. To match the gates, Alice ages gate A by $\Delta D_A = D_B - D_A$ such that $D_A + \Delta D_A = D_B$.
3. $D_A < D_B - 0.5$. In this case, gate A is faster than gate B by more than 0.5. Hence, gates A and B cannot be matched and must be disabled.

To match their PPUFs, Alice and Bob both follow the same aging and disabling procedure outlined above. Therefore, the only cases for which gate A and gate B cannot be matched are when $D_A < D_B - 0.5$ or $D_B < D_A - 0.5$. It is easy to see that the probability of either of these events occurring is 1/4, shown as the white regions in Figure 1.6a. Therefore, Alice and Bob are able to match 75% of their gates, on average.



(a)

(b)

Figure 1.6: (a) Probability that a third, malicious gate C can match two honestly matched gates A and B; (b) small mPPUF with 6 matched and 2 disabled gates.

Now, assume that a third, malicious PPUF owner, Chuck, wants to match his PPUF to the same configuration as that matched by Alice and Bob. The following two cases are possible, for a gate C with delay D_C on Chuck's PPUF:

1. *Gates A and B were not able to match and were disabled.* In this case, Chuck must simply disable gate C to match the configuration.

2. *Gates A and B were matched.* Here, Chuck will only be able to age gate C to match if it is faster than the slowest gate between A and B, but not by more than 0.5 (i.e. $\max(D_A, D_B) - 0.5 \leq D_C < \max(D_A, D_B)$).

Figure 1.6a shows the probability that Chuck is able to match an unwelcome gate C with two honestly matched gates A and B for various delays D_A and D_B. This occurs with probability 7/12; in other words, Chuck is able to match only 58.33% of the configuration matched honestly by Alice and Bob.

After matching their PPUFs (e.g. Figure 1.6b), Alice and Bob now have PPUFs that realize the same complex function. In other words, both PPUFs (and no other PPUFs) will produce exactly the same unique response to any challenge in a single cycle. Therefore,

Algorithm 1 PPUF Matching

```
1: The patient determines which of its PPUF's gates are within a $\Delta delay$ faster than the corresponding gate on the doctor's PPUF such that aging of the gate to match delay is possible.
2: The patient calculates from Equations 1.1 and 1.6 the $\Delta V_{th}$ and aging time required to match the doctor's PPUF gate, and ages it for the required time.
3: The doctor repeats the same process for those gates which are faster than those on the patient's PPUF.
4: All remaining unmatched gates are disabled on both PPUFs.
```

Algorithm 2 Public Key Communication

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

Alice can issue Bob a challenge and verify his response by executing it on her own PPUF, enabling a myriad of low-energy cryptographic protocols that require neither high storage nor simulation.

1.6.1 PPUF Matching

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 patient and doctor, 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.

1.6.2 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 patient and doctor have coordinated their PPUFs to match an identical configuration. The protocol proceeds as specified in Algorithm 2, for a patient that is sending data to a doctor.

In the domain of tele-healthcare, 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 one party to the other.

1.7 Trusted Sensor Information Flow in the Remote Sensor

In addition to the trusted sensor architecture, Figure 1.1 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 consists of two main components: a signal transducer and a digital analog converter with other integrated circuits for processing

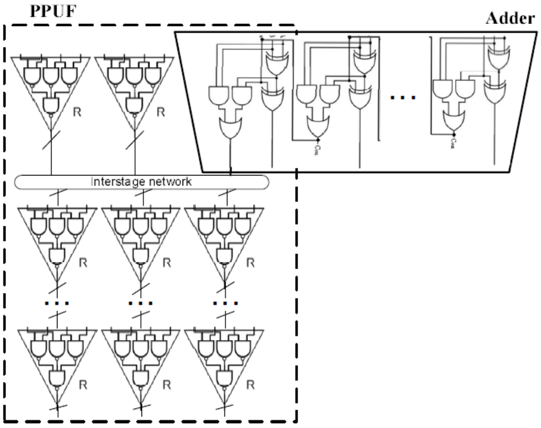


Figure 1.7: Interleaved PPUF with Sensor/GPS component (e.g. Adder Used in A/D Circuitry).

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.

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 1.7. The figure illustrates an interleaved PPUF and sensor 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.

1.8 Beyond CMOS: Nanotechnology-based Trust and Privacy

Many potential nanotechnologies promise to be faster, smaller, and demand less power than their semiconductor counterparts. Additionally, the random synthesis methods with which many nanotechnology devices are fashioned generate impossible to clone components. By capitalizing on the analog nature of these new nanotechnology devices we are able to eradicate the need for high resolution measurements while still retaining robust security.

The development of nanotechnology research continues to lead to advances in medical science and material science, and has recently spread into computer engineering and electrical engineering. Current trends in nanotechnology-based computing focus on synthesizing molecular electronic devices in an attempt to obtain systematic results from disorderly chemical processes. Dick, et. al. [11] demonstrate promising results controlling the production of three-dimensional networks of Indium Arsenide (InAs) nanowires that display non-linear current-voltage (I-V) characteristics that could be harnessed in molecular electronic logic devices [11] [12]. However, the self-assembled nature of these networks remains innately random. For application of this nanotechnology (and others like it) to PUFs, this randomness is desirable.

Our target nanotechnology is the nanocell, effectively a non-linear two-dimensional network of randomly distributed metallic particles connected by self-assembled molecules, called monolayers, that exhibit I-V characteristics with negative differential resistance (NDR) [37] [38] [39]. Other similar nanotechnologies, such as the InAs nanowires also posses similar non-linear and network-like characteristics; however they have not been studied in the same capacity as the nanocell. Using the nanocell as a PPUF is possible in part due to the non-linearity of the I-V curve of the monolayers that connect its network.

The analog nature of the nanocell allows for the device to grow to an arbitrary size while maintaining a constant and practical authentication time. This is accomplished by dividing the network into partitions and authenticating the challenge-response pair over only one or a few of the partitions. The nanocell remains a connected network, while arbitrary lines are drawn throughout to partition the space. An attacker does not know which set of partitions the authenticating party will test, thus he must simulate the entire nanocell in order to attempt an attack.

Unique to nanocells that has not yet been realized in CMOS-based PUFs is the ability to not only dynamically choose input values, but to also dynamically choose input pins. As with the majority of integrated circuits, CMOS-based PUFs are one-way devices that have statically assigned input pins on which only the input values can vary. Utilizing the nanocell as an analog device offers the freedom to dynamically choose input pins each time a challenge is administered, effectively increasing the input space exponentially with the number of pins.

1.9 Conclusion

We have presented 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 matched public physically unclonable functions with a new concept of overlapping sensing and security circuitry. We have shown that PPUF matching between patient and doctor can enable ultra fast, ultra low power public key communication. The approach is generic and can be applied in various sensing and other applications, most importantly in tele-healthcare. Our simulations indicate that it results in very low hardware, delay, and energy overheads, and can be made even more efficient in terms of all of these metrics with the advancement of nanotechnology-based PUFs.

References

[1] S. Nassif et al., "High-performance CMOS variability in the 65nm regime and beyond," *IEEE International Electron Devices Meeting*, pp. 569–571, 2007.

[2] S. Borkar et al., "Parameter variations and impact on circuits and microarchitecture," *IEEE/ACM Design Automation Conference*, pp. 338–342, 2003.

[3] A. R. Brown, V. Huard, and A. Asenov, "Statistical simulation of progressive NBTI degradation in a 45-nm technology pMOSFET," *IEEE Transactions on Electron Devices*, vol. 57, no. 9, pp. 2320–2323, 2010.

[4] S. Smith et al., "Comparison of measurement techniques for linewidth metrology on advanced photomasks," *IEEE Transactions on Semiconductor Manufacturing*, vol. 22, no. 1, pp. 72–79, 2009.

[5] J. S. J. Wong, P. Sedcole, and P. Y. K. Cheung, "Self-characterization of combinatorial circuit delays in FPGAs," *IEEE International Conference on Field-Programmable Technology*, pp. 245–251, 2007.

[6] A. Keshavarzi, et al., "Measurements and modeling of intrinsic fluctuations in MOSFET threshold voltage," *IEEE/ACM International Symposium on Low Power Electronics and Design*, pp. 26–29, 2005.

[7] S. Wei, S. Meguerdichian, and M. Potkonjak, "Gate-level characterization: foundations and hardware security applications," *IEEE/ACM Design Automation Conference*, pp. 222–227, 2010.

[8] M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey, "Hardware Trojan horse detection using gate-level characterization," *IEEE/ACM Design Automation Conference*, pp. 688-693, 2009.

[9] S. Wei, S. Meguerdichian, and M. Potkonjak, "Malicious circuitry detection using thermal conditioning," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1136–1145, 2011.

[10] A. Vahdatpour, S. Meguerdichian, and M. Potkonjak, "A gate level sensor network for integrated circuits temperature monitoring," *IEEE Sensors*, pp. 652–655, 2010.

[11] M. A. Alam and S. Mahapatra, "A comprehensive model of PMOS NBTI degradation," *Microelectronics Reliability*, vol. 45, pp. 71–81, 2005.

[12] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions,"

Science, vol. 297, no. 5589, pp. 2026–2030, 2002.

[13] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, “Silicon physical random functions,” *ACM Conference on Computer and Communications Security*, pp. 148–160, 2002.

[14] N. Beckmann and M. Potkonjak, “Hardware-based public-key cryptography with public physically unclonable functions,” *Information Hiding Conference*, pp. 206–220, 2009.

[15] U. Rührmair, “SIMPL systems, or: can we design cryptographic hardware without secret key information?” *International Conference on Current Trends in Theory and Practice of Computer Science*, vol. 6543, pp. 26–45, 2011.

[16] M. Potkonjak, S. Meguerdichian, A. Nahapetian, and S. Wei, “Differential public physically unclonable functions: architecture and applications,” *IEEE/ACM Design Automation Conference*, pp. 242–247, 2011.

[17] M. Potkonjak, S. Meguerdichian, and J. L. Wong, “Trusted sensors and remote sensing,” *IEEE Sensors*, pp. 1104-1107, 2010.

[18] M. Majzoobi, F. Koushanfar, and M. Potkonjak, “Lightweight secure PUFs,” *IEEE/ACM International Conference on Computer Aided Design*, pp. 670-673, 2008.

[19] S. Meguerdichian and M. Potkonjak, “Device aging-based physically unclonable functions,” *IEEE/ACM Design Automation Conference*, pp. 288–289, 2011.

[20] S. Meguerdichian and M. Potkonjak, “Matched public PUF: ultra low energy security platform,” *IEEE/ACM International Symposium on Low Power Electronics and Design*, pp. 45–50, 2011.

[21] S. Meguerdichian and M. Potkonjak, ‘Security primitives and protocols for ultra low power sensor systems,” *IEEE Sensors*, 2011.

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

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

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

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

[26] N. Gura, et al., “Comparing elliptic curve cryptography and rsa on 8-bit CPUs,” *CHES*,

pp. 119-132, 2004.

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

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

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

[30] 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.

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

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

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

[34] 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.

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

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

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

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

[39] 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.

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

[41] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Sys-*

tems. Wiley Publishing, 2008.

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

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

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

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

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

[47] 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.

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

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

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

[51] D. Markovic, C. Wang, L. Alarcon, T.-T. Liu, and J. Rabaey, "Ultralow-power design in near-threshold region," *Proceedings of the IEEE*, vol. 98, no. 2, pp. 237–252, 2010.

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

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

[54] B. Cline, K. Chopra, D. Blaauw, and Y. Cao, "Analysis and modeling of CD variation for statistical static timing," *IEEE International Conference on Computer-Aided Design*, pp. 60–66, 2006.

[55] S. Chakravarthi, A. Krishnan, V. Reddy, C. F. Machala, and S. Krishnan, "A comprehensive framework for predictive modeling of negative bias temperature instability,"

IEEE International Reliability Physics Symposium, pp. 273–282, 2004.