2008 IEEE International Conference on RFID
The Venetian, Las Vegas, Nevada, USA
April 16-17, 2008

Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications

Srinivas Devadas[1], Edward Suh[2], Sid Paral, Richard Sowell, Tom Ziola, Vivek Khandelwal
{sdevadas, esuh, sparal, rsowell, tziola, vkhandelwal} @ pufcoinc.com
PUFCO, Inc. 2225 East Bayshore Road, Suite #231, Palo Alto, CA 94303

Abstract— **Physical Unclonable Functions (PUFs) exploit the physical characteristics of the silicon and the IC manufacturing process variations to uniquely characterize each and every silicon chip. Since it is practically impossible to model, copy, or control the IC manufacturing process variations, PUFs not only make these chips unique, but also effectively unclonable. Exploiting the inherent variations in the IC manufacturing process, PUFs provide a secure, robust, low cost mechanism to authenticate silicon chips. This makes PUFs attractive for RFID ICs where cost and security are the key requirements. In this paper we present the design and implementation of PUF enabled "unclonable" RFIDs. The PUF-enabled RFID has been fabricated in 0.18μ technology, and extensive testing results demonstrate that PUFs can securely authenticate an RFID with minimal overheads. We also highlight the advantages of PUF based RFIDs in anti-counterfeiting and security applications.**

I. Introduction

RFID technology makes it possible to provide each and every item, and not just the item type, a "unique identifier." Additionally, hundreds of these unique identifiers, on RFID tagged items, can be read simultaneously, without the need for a line of sight. Various industries are exploiting these characteristics of RFID technology to improve the ability to track and trace their physical goods – inventory, work-in-progress, tools, equipment, personnel, etc. Some industries, such as luxury brand goods, pharmaceutical, and government are also using RFID technology for authentication and anti-counterfeiting of products, drugs, government documents etc. For anti-counterfeiting of, say, a luxury brand product, a manufacturer notes the unique identifier of every RFID tagged item he ships, and then compares the identifier found on the product at the point-of-sale against the one he had recorded before shipping to establish the authenticity of the product.

RFID certainly has advantages over traditional authentication and anti-counterfeiting mechanisms, such as color shifting inks, holograms, 2D barcodes etc. RFID tags can be read without line of sight or physical contact with tagged items, hence RFID technology does not affect the supply chain throughput. But, RFID technology is primarily a track & trace technology, and in the context of applications like authentication, anti-counterfeiting, secure access, basic RFID technologies cannot provide truly secure solutions.

∞ Cloning of RFID tags: An adversary can easily copy the content ("unique identifier") of one tag to another tag. In simple RFIDs, cloned tags are indistinguishable from authentic ones.

∞ Replay attacks: Unauthorized readers can listen and record the communication between an authorized reader and a RFID tag, and then replay the communication to essentially achieve the same outcome that a legitimate reader and tag would have achieved even without copying a tag. Basic RFID tags do not provide any mechanisms to prevent such attacks.

RFID certainly raises the bar as an authentication or anti-counterfeiting measure, but the bar is only as high as the technical "skills" of counterfeiters, which unfortunately are reaching new highs every day. Customers and vendors are increasingly becoming more aware of the limitations in RFID technology, and have come up with various alternatives. Unfortunately none of these solutions are sufficient:

∞ Basic passive RFID tags include yet another number, a "factory" serial number in read-only memory on the chip. This serves as another line of defense. But all a counterfeiter needs to do is read and clone this number, in addition to the RFID tag contents, and record this data on another tag. An adversary can record this additional serial number, along with the unique identifier, and then replay it.

∞ Crypto RFID tags include a secret key on the chip, and use symmetric key or public key cryptography to encrypt/decrypt data being exchanged between the tag and the reader. This approach is essentially using encryption to achieve authentication. Severe first-order limitations with this approach are in the high cost of such tags and readers, and the complexity of the infrastructure required to embed and manage keys in the tags and readers throughout the supply chain. Crypto RFID tags are also vulnerable to cloning attacks by skilled adversaries.

∞ New printed electronic RFID tags are appearing on the horizon. These RFID tags use a different, and perhaps

[1] MIT, Cambridge, MA
[2] Cornell University, Ithaca, NY

difficult to duplicate manufacturing process. But at the core, the issue is not cloning of the manufacturing process, but cloning of the data stored in such a tag. Hence, this approach is vulnerable to cloning, side channel and replay attacks in much the same way as the other approaches.

In this paper we describe simple, inexpensive and "unclonable" RFID ICs based on Physical Unclonable Functions, and an authentication mechanism that is secure and robust against replay attacks. This RFID solution addresses the cost, complexity and security issues around the use of traditional RFIDs for anti-counterfeiting and security applications.

The rest of this paper is organized as follows. Section II describes the concept of Physical Unclonable Functions (PUFs) and presents a PUF circuit design. Section III applies PUF technology to RFIDs and describes our design and implementation of a PUF-enabled RFID. Section IV shows test results from PUF RFIDs fabricated in 0.18μ technology, and Section V summarizes the key characteristics of the PUF-enabled RFIDs. Finally, Section VI discusses the previous work and Section VII concludes the paper.

II. PHYSICAL UNCLONABLE FUNCTIONS

A Physical Random Function or Physical Unclonable Function (PUF) is a function that maps a set of challenges to a set of responses based on an intractably complex physical system; a challenge is an input to the function and a response is the output. The function can only be evaluated with the physical system, and is unique for each physical instance. Hence, the PUF function provides a static mapping between challenges and responses, which is a "random" assignment.

While PUFs can be implemented with various physical systems, this paper focuses on silicon PUFs that are based on the hidden timing and delay information of integrated circuits [4, 5]. Even with identical layout masks, the variations in the manufacturing process cause significant delay differences among different ICs. Silicon PUFs derive digital secrets from the complex delay characteristics of wires and transistors in integrated circuits (ICs).

Because silicon PUFs tap into the random variation that occurs during an the IC fabrication process, the secret(s) are intrinsic to the silicon itself, are extremely difficult to predict or "program" in advance of manufacture, and are essentially non-replicable from chip to chip. As a result, PUF technology provides several advantages over the conventional approach of storing digital secrets to customize each IC. First, PUFs significantly increase physical security by generating volatile secrets that only exist in a digital form when a chip is powered on and running. This means that an adversary, rather than merely examining an IC's memory to read its stored secret, instead would need to mount an attack while the chip is running and using the secret -- a significantly harder proposition than discovering non-volatile keys. An invasive physical attack would need to accurately measure PUF delays from transistor to transistor without changing the delays or discover volatile keys in registers without cutting power or tripping tamper-sensitive circuitry that clears out the registers. Second, even the IC manufacturer cannot clone a PUF-enabled IC. That is because the random component of manufacturing variation cannot be controlled or programmed in any conventional sense by the manufacturer - it is inherent to the process itself. Finally, PUFs also simplify key provisioning (which is necessary with crypto-chips) because manufacturers do not have to program the IC with secrets.

Figure 1 illustrates a silicon PUF delay circuit based on MUXes and an arbiter. The circuit has a multiple-bit input X and computes a 1-bit output Y based on the relative delay difference between two paths with the same layout length. The input bits determine the delay paths by controlling the MUXes. Here, a pair of MUXes controlled by the same input bit X[i] work as a switching box (dotted boxes in the figure). The MUXes pass through the two delay signals from the left side if the input control bit X[i] is zero. Otherwise, the top and bottom signals are switched. In this way, the circuit can create a pair of delay paths for each input X. To evaluate the output for a particular input, a rising signal is given to both paths at the same time, the signals race through the two delay paths, and the arbiter (latch) at the end decides which signal is faster. The output is one if the signal to the latch data input (D) is faster, and zero otherwise.

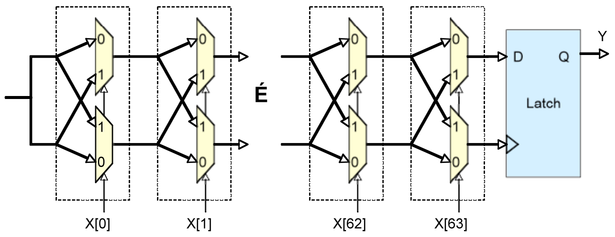

Figure 1. An arbiter PUF delay circuit. The circuit creates two delay paths with the same layout length for each input X, and produces an output Y based on which path is faster.

There are two ways to construct a k-bit response from the 1-bit output of this PUF delay circuit. First, one circuit can be used k times with different inputs. A challenge is used as a seed for a pseudo-random number generator (such as a linear feedback shift register). Then, the PUF delay circuit is evaluated k times, using k different bit vectors from the pseudo-random number generator serving as the input X to configure the delay paths. It is also possible to duplicate the single-output PUF circuit multiple times to obtain k bits with a single evaluation.

PUF responses can either be directly used to authenticate a device or can serve as a secret key for cryptographic operations such as encryption and digital signatures to enhance security beyond authentication. This paper only focuses on the authentication with minimally-sized circuits in RFIDs, instead of authentication that relies on expensive cryptographic operations. For simple authentication, a verifier saves randomly selected challenge-response-pairs (CRPs) from a device when the device is known to be authentic, and later checks a response in the field to authenticate the device. We describe this protocol in more detail in the next section in the context of RFIDs.

To break the PUF-based authentication scheme without being able to create two identical PUFs, attackers may try to construct a precise timing model and learn the parameters for a particular PUF from many challenge-response pairs corresponding to that PUF [7]. To address this, we use a PUF circuit specifically designed to scramble its output which thwarts such “model building” attacks.

III. PUF-ENABLED UNCLONABLE RFIDs: DESIGN & IMPLEMENTATION

While traditional RFID technology has limitations in its use as a true anti-counterfeiting measure, it still is an almost ideal technology to talk to “things.” Unlike other anti-counterfeiting solutions, like special printing, holograms, tamper-evident seals etc, RFID does not require manual intervention, it need not slow down the supply chain throughput, and can leverage cost-reduction curves and scale economies associated with ICs and electronic components in general. A critical element that has been missing is a scalable, cost-effective way to prevent cloning. An RFID tag that has a secret that cannot be copied would allow one to immediately distinguish a counterfeit tag from the genuine one. Such a RFID tag would fit the requirements for anti-counterfeiting.

Now if this PUF-equipped IC is an RFID chip, the PUF would mean that such an RFID chip would have its own unique secrets (corresponding to an exponential number of challenge-response-pairs), derived from the silicon itself. And these secrets would be:

- ∞ Essentially impossible to predict or “control” in advance of manufacture
- ∞ Essentially impossible to duplicate or clone from one chip to the next

Therefore, the PUF can add a secure authentication feature to an RFID if it can be integrated into an RFID effectively (with minimal additional silicon area and power consumption).

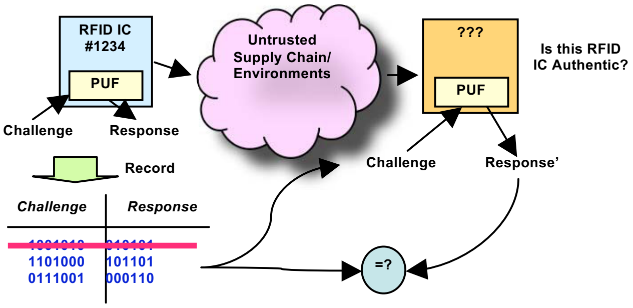

Figure 2. The overview of the PUF-based RFID authentication procedure.

Figure 2 illustrates the PUF-based authentication process for anti-counterfeiting. In our approach, each RFID contains a *chosen*, possibly unique, fixed-length identifier such as an EPC code in non-volatile memory for identification. Therefore, for identification purposes, PUF-enabled RFIDs are identical to conventional RFIDs. While PUF responses can also be used as an identifier given that they are unique for each IC (provided they are long enough), we choose to have a separate conventional identifier so that the PUF-enabled RFID can also be used for traditional track-and-trace applications and to enable conventional database lookups.

For secure authentication, the RFID contains a PUF circuit and exploits the fact that the PUF can have an exponential number of challenge-response pairs where the response is unique for each IC and each challenge.

Consider the authentication process shown in Figure 2. A trusted party such as a product vendor, when in possession of an authentic RFID with an authentic product, applies randomly chosen challenges to obtain unpredictable responses. The trusted party stores these challenge-response pairs in a database for future authentication operations. This database is indexed by the (unique) identifier normally associated with each RFID and/or product, for example, an EPC code that is stored in non-volatile memory on the RFID. The identification of the RFID and product is based on this conventional identifier. To check the *authenticity* of an RFID and the associated product later in the field, the trusted party selects a challenge that has been previously recorded but has never been used for an authentication check operation, and obtains the PUF response from the RFID. If the response matches (i.e., is close enough to) the previously recorded one, the RFID is authentic because only the authentic IC and the trusted party should know that challenge-response-pair. To protect against man-in-the-middle attacks, challenges are never reused. Therefore, the challenges and responses can be sent in the clear over the network during authentication operations. Note that the challenge-response database can be re-charged with new challenge-response-pairs to increase the number of authentication events.

We have designed and fabricated RFID ICs with the silicon PUF circuit based on MUXes and an arbiter. Our PUF-enabled RFID IC operates at 13.56MHz and is based on the ISO-14443 type A specification. This passive RFID IC operates just like a regular RFID IC for storing a unique identifier or EPC code; the PUF circuit is activated for authentication. The same PUF circuit is used many times for a given 64-bit challenge to produce a 64-bit or longer response.

To allow an RFID reader to access the PUF, our RFID tags support a new command: challenge. Also, the existing READ and WRITE commands in RFIDs can be used as the PUF commands. On a challenge command, the tag accepts a 64-bit challenge from the reader and sends a response for the given challenge back to the reader. A WRITE into a specific address is interpreted as the challenge command, and a READ from a specific address retrieves the PUF response.

Figure 3 shows the floorplan of the PUF-enabled PUF, which implements the ISO-14443A standard with a full anti-collision protocol. As shown in the figure, the majority of the silicon area is consumed by standard RFID components such as the RF front-end, OTP memory, digital logic to implement various commands. The PUF circuit and the linear feedback shift register (LFSR) that configures the circuit (highlighted by a red box) consume only a small portion of the chip. The PUF component has been implemented in less than 0.02mm^2 in our first chip that is designed in 0.18μ fabrication technology.

The PUF consumes dynamic power only during evaluation – when it generates the response. Outside of evaluation, which is most of the time, only traditional CMOS leakage currents are present. The power required during evaluation is small compared to the power stored in a typical RFID device such that the VDD drop is insignificant.

Although our current implementation of the PUF-enabled RFID uses a specific frequency (HF) and a command set, we note that the same PUF technology and its RFID commands can be integrated into RFIDs that operate at other frequencies. For example, the same PUF module can be used in passive UHF tags. We only use a HF tag as a vehicle to demonstrate that PUF technology enables strong authentication even in low-cost, low-power passive RFID tags. There is no difference between HF and UHF tags from the PUF authentication perspective.

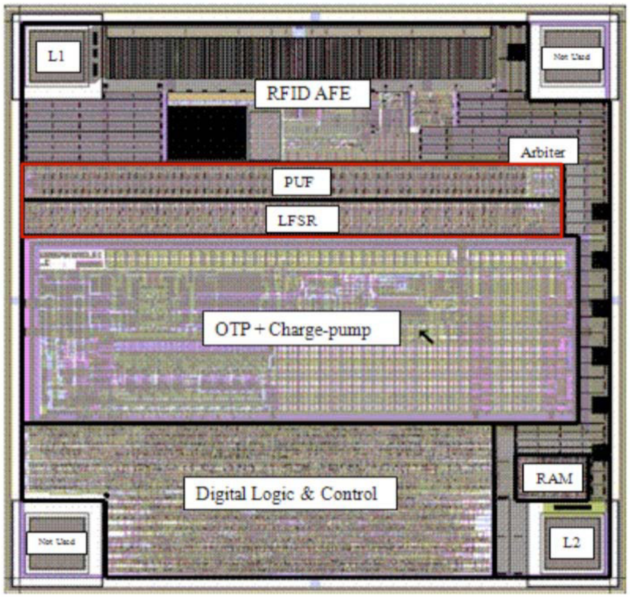

Figure 3. The floorplan of a PUF-enabled RFID.

IV. PUF-ENABLED UNCLONABLE RFID: TEST RESULTS

The RFID IC device was manufactured in 0.18μ fabrication technology and extensive testing and data collection has been performed on the RFID IC.

In order to quantify performance, it is required to determine if responses from PUF circuits are "unique" and "reproducible". We define the following two metrics for this purpose.

- **Intra-PUF Variation**: Defined as the number of bits in a PUF response, which vary when the response for a challenge is repeatedly generated on a given PUF device in a changing environment; commonly represented in the form of a statistical distribution. Also referred to as "Intra-chip Noise" or "Noise". Intra-PUF Variation is a measure of the reproducibility of responses from an individual PUF circuit.

- **Inter-PUF Variation**: Defined as the number of bits in a PUF response, which vary between different devices for a set of shared challenges; commonly represented in the form of a statistical distribution. The Inter-PUF Variation is a measure of the uniqueness of an individual PUF circuit.

For secure authentication that ensures different PUF instances are distinguished, the inter-PUF variation must be high, ideally 50% on average. For reliable authentication of authentic PUF instances, the intra-PUF variation must be low, ideally being zero.

Figure shows the distribution of intra-PUF and inter-PUF variations when 128-bit responses are produced and compared. The intra-PUF variation is represented by the curves on the left. Here, the X axis represents the code distance, the number of bits that are different between two evaluations for a given challenge on a PUF instance, and the Y axis represents the number of comparisons that resulted in a particular code distance. The thin circled line (dark blue curve) shows results when the temperature is fixed at 25°C, and the thick light blue line shows aggregate results when the temperature changes from -25 to +85°C. As illustrated by the graphs, the intra-chip variation becomes worse (higher) when the temperature changes.

The inter-PUF variation is shown by the curves on the right. Here, the X-axis represents the number of bits differing between responses produced by two different PUF instances for the same challenge. Similar to the intra-PUF variation cases, the thin circled line (brown curve) represents results at a fixed temperature at 25°C and the thick orange line represents results over -25 to +85°C. As observed from the graph, inter-PUF variation is more stable with respect to temperature than intra-PUF variation. Other observations show that the inter-PUF variation distribution is centered in the neighborhood of the code distance of 64, very close to the ideal value of (response size)/2.

In summary, the experiments show that identical PUF circuits, on multiple RFID chips, produce 128-bit responses that differ according to the inter-PUF variation distribution with a mean centered close to the ideal 64 bits. On the other hand, repeated challenges to the same PUF device differ according to the intra-PUF variation distribution centered in the vicinity of 12 to 16 bits. By utilizing the “chasm” between the two Intra-PUF and Inter-PUF distributions, it is possible to differentiate one PUF device from another; this differentiation can be used

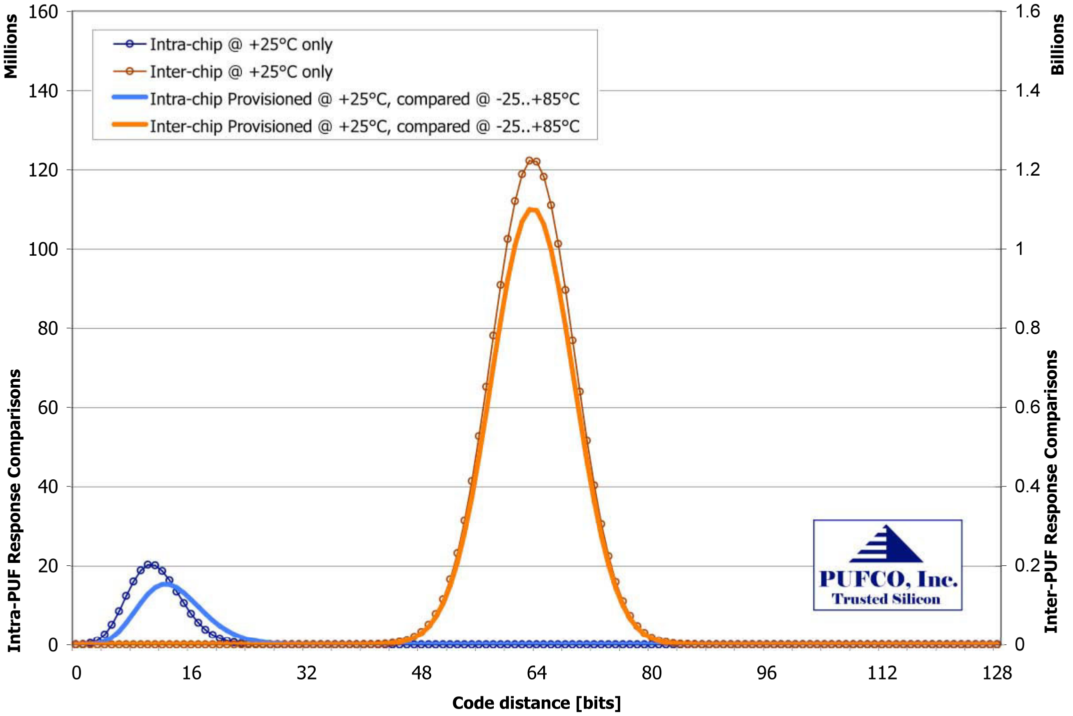

Figure 4. Code distance distribution of 128-bit PUF responses.

for authentication of RFIDs. For example, the authentication scheme can set a threshold at 32 bits so that an RFID is considered authentic if it can produce a response that is less than 32 bits different from the one that is recorded in the database.

From the intra-PUF and inter-PUF variations, we can compute associated false-positive and false-negative probabilities for a given authentication threshold when PUF responses are used to uniquely authenticate a device. We define the false-positive and false-negative as follows.

- **False-positive:** The statistical probability of an erroneous identification of a device as authentic when it is actually an impostor.
- **False-negative:** The statistical probability of an erroneous rejection of an authentic device as an impostor when it is actually authentic.

False-positive and false-negative probabilities can be balanced and traded-off against each other by setting the appropriate authentication code distance threshold. 128-bit PUF response data show that the intersection of false-positive and false-negative probabilities can be made to be in the range of few parts per billion or lower. Wider response sizes or repeated authentication events can improve this range.

We also note that while 128 bits were generated from each PUF, it is possible to generate larger and smaller response sizes with corresponding performance characteristics. In general, a longer response allows lower false positive and negative rates by increasing the "chasm" between the inter-PUF variation and the intra-PUF variation.

V. PUF-ENABLED UNCLONABLE RFID APPLICATIONS

PUF-based unclonable RFIDs provide the following advantages over basic passive RFIDs with simple identifiers or secure RFIDs based on conventional cryptographic operations:

- **Highly Secure:** The RFID chip itself cannot be cloned. The responses to challenges are generated dynamically, and are volatile. Volatile information is much harder to extract than non-volatile information. With practically unlimited numbers of challenge-response pairs available, each pair can be used only once. This essentially serves as a one-time pad. A replay attack would fail since the adversary cannot predict the challenge and responses to be used for next authentication event.
- **Low Cost, Low Power Consumption: A** PUF circuit is a fairly lightweight addition to the RFID chip. The initial implementation of a basic 64-stage PUF circuit with a linear feedback shift register (LRSR) added less than 0.02mm^2 in the 0.18μ technology and consumes little extra power. Chip size, cost and power consumption are key market acceptance parameters for RFID. PUF based RFID enhances the capabilities of basic RFID in the most cost effective way, even for item level use.
- **Simple, Robust Authentication:** PUFs provide strong authentication of an RFID tag unlike traditional tags that can be easily cloned. Therefore, a PUF RFID tagged product can be authenticated at each end-point of a supply chain (or anywhere in between) by simply comparing the response generated during an authentication event with the response recorded at the secure location. Also, PUF challenge response pairs can be generated and stored by multiple independent parties that do not share information.

PUF based unclonable RFIDs provide simple and robust anti-counterfeiting mechanism compared to item level e-predigree, as proposed in pharmaceutical industry. Since the PUF RFID chips cannot be cloned, a simple authentication at the point-of-sale ensures only a genuine product is sold to the customer. This can even be achieved without serialization (providing unique serial # to each saleable unit), by using the PUF RFID tag identifier and PUF authentication. While this simple PUF authentication does not identify the weak link in the supply chain, where a compromise might have been made, it certainly ensures only a genuine product is sold to the customer. PUF RFIDs do not prevent building a complex e-pedigree, but can certainly be the first step in ensuring consumer safety. Additionally, PUF authentication is a much faster operation compared to e-pedigree, which can be of significance when responding to pandemics and other urgent situations.

The low cost and power consumption of PUF based RFIDs make them suitable for item level use, a significant advantage over cryptographic techniques. For cryptographic approaches, significant investment needs to be made to securely store secrets in the chips, and in complex infrastructure (hardware and software) to do authentication. PUF based RFIDs do not store any secrets, and do not need complex infrastructure for authentication.

VI. RELATED WORK

Researchers have studied the implementation of PUFs exploiting physical characteristics other than timing and delay information of silicon circuits. For example, Pappu proposed an optical PUF, which uses the speckle patterns of optical medium for laser light [8]. Coating PUFs and acoustic PUFs [9, 11] measure the capacitance of a coating layer covering an IC and the acoustic reflections of a token, respectively. This paper focuses on silicon PUFs which are very easy to integrate into ICs including RFIDs unlike other types of PUFs.

Recently, there have been significant efforts to develop techniques to securely authenticate RFID tags and associated products to prevent counterfeits. As discussed by Lehtonen et al. [6], current techniques can be generally put into three categories. First, traditional RFIDs simply rely on a unique identifier such as a serial number in an RFID tag to authenticate the tag. While this approach is simple and inexpensive, the identifiers cannot provide high security because an adversary can easily clone a tag. Second, the identifiers can be used with a track-and-trace technique where a back-end database keeps the history of each RFID tag so that suspicious activities can be detected. However, the track-and-trace requires massive infrastructure to record the detailed history of a tag in each and every step in the supply chain, and still cannot completely prevent cloning attacks. Finally, to resist cloning, each tag must be securely authenticated. Today's cryptographic primitives, however, are often too expensive for low-cost RFID tags and have not been demonstrated in fabricated RFID ICs. Even minimalist implementations of AES and SHA-1 take thousands of (or tens of thousand) gates and thousands of clock cycles [2, 3]. In this paper, we described the PUF-based technique that can be applied even to low-cost RFIDs and reported the experimental results from fabricated RFID tags.

Thanks to its security and cost effectiveness, researchers have recently proposed to apply PUF technology to RFID tags. For example, Tuyls et al. propose to combine coating PUFs with elliptic curve cryptography to authenticate a tag off-line [10]. Bolotnyy et al. study how to build a message authentication code with PUFs [1]. Unlike the previous studies, our PUF RFID uses a simple challenge-response protocol focusing on tag authentication and, to the best of our knowledge, is the first PUF-enabled RFID tag to be fabricated.

VII. CONCLUSION

This paper describes how PUFs can enable unclonable RFID tags for anti-counterfeiting and secure access. Compared to traditional approaches based on track-and-trace or cryptographic operations, PUF-enabled RFIDs provide strong authentication with minimal overheads and can be applied even to low-cost passive RFID tags. A HF RFID tag has been fabricated in a 0.18μ technology and the results demonstrate that the PUF circuit can indeed be integrated into a small passive RFID tag and authenticate each tag in a secure and reliable fashion.

REFERENCES

[1] L. Bolotnyy and G. Robins. Physically Unclonable Function -Based Security and Privacy in RFID Systems. Proc. IEEE International Conference on Pervasive Computing and Communications (PerCom 2007), New York, March, 2007, pp. 211-218.

[2] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, Strong Authentication for RFID Systems Using the AES Algorithm, Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES), Springer LNCS 3156, pp. 357-370, 2004.

[3] M. Feldhofer and C. Rechberger. A Case Against Currently Used Hash Functions in RFID Protocols, Workshop on RFID Security (RFIDSEC), 2006.

[4] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas. Silicon physical random functions. In Proceedings of the Computer and Communication Security Conference, November 2002.

[5] J.-W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas. A technique to build a secret key in integrated circuits with identification and authentication applications. In Proceedings of the IEEE VLSI Circuits Symposium, June 2004.

[6] M. Lehtonen, T. Staake, F. Michahelles and E. Fleisch, From Identification to Authentication – A Review of RFID Product Authentication Techniques. RFIDSec 2006.

[7] D. Lim. Extracting secret keys from integrated circuits. Master's thesis, Massachusetts Institute of Technology, May 2004.

[8] R. Pappu. Physical One-Way Functions. PhD thesis, Massachusetts Institute of Technology, 2001.

[9] B. Skoric, P. Tuyls, and W. Ophey. Robust key extraction from physical unclonable functions. In Proceedings of the Applied Cryptography and Network Security Conference 2005, volume 3531 of Lecture Notes in Computer Science, 2005.

[10] P. Tuyls and L. Batina. RFID-Tags for Anti-counterfeiting. Topics in Cryptology – CT-RSA 2006. Volume 3860 of Lecture Notes in Computer Science, 2006.

[11] P. Tuyls, B. Skoric, S. Stallinga, A. Akkermans, and W. Ophey. Information theoretical security analysis of physical unclonable functions. In Proceedings of Conference on Financial Cryptography and Data Security 2005, volume 3570 of Lecture Notes in Computer Science, 2005.