CMOS Image Sensor Based Physical Unclonable Function for Smart Phone Security Applications

Yuan Cao, Siarhei S. Zalivaka, Le Zhang, Chip-Hong Chang and Shoushun Chen
School of Electrical and Electronic Engineering
Nanyang Technological University
50 Nanyang Avenue, Singapore 639798
Email: ycao3@e.ntu.edu.sg; zali0001@e.ntu.edu.sg; lzhang15@e.ntu.edu.sg; echchang@ntu.edu.sg; eechenss@ntu.edu.sg

***Abstract*—Recent years have seen the rapid growing market of smart phones. At the same time, pirated, knockoff or refurnished phones have also flooded into the worldwide market and inflicted great loss on the mobile phone industry. Existing anti-counterfeiting, authentification and identification methods, which rely on the verification of the IDs stored in the phone memory, are vulnerable to attack. This paper presents a new CMOS image sensor based physical unclonable function (PUF) for smart phone identification and anti-counterfeiting. The proposed PUF exploits the intrinsic imperfection during the image sensor manufacturing process to generate the unique signatures. With the proposed differential readout algorithm for the pixels of the fixed pattern noise, the effects of power supply and temperature variations are suppressed. Simulations on a typical 3-T CMOS image sensor in GF 65nm CMOS technology show that the proposed PUF can generate robust and reliable challenge-response pairs with an uniqueness of 50.12% and a reliability of 100% at temperature varying from 0°C to 100°C and supply voltage variation of $\pm 16.7\%$.**

***Index Terms*—Physical Unclonable Function, process variation, smart phone anti-counterfeiting, CMOS image sensor.**

I. Introduction

It is estimated that there are approximately 7 billion mobile subscribers all over the world by May 2014 [1]. With the emergence of "turnkey" solution provided by MediaTek (MTK), the entry threshold and costs for handset research and production have been significantly lowered, which open the floodgates for knockoff, counterfeited and refurnished mobile phones to permeate the global mobile phone market [2]. The mobile phone industry suffers a massive financial loss from a conservative estimate of 6 billion USD of knockoff phone sales reported in Feb. 2014 [3]. Presently, device-specific IDs such as IMEI (device ID), IMSI (subscriber ID), or ICC-ID (SIM card serial number) are used for the identification and authentication of the mobile phones. As these device IDs are normally kept in the storage elements of the mobile phones, the hackers can easily copy them to another low cost refurnished or knockoff cell phones [4]. These cloned phones are virtually indistinguishable from the authentic ones. To protect the user's privacy, a "cookie law" has been enforced in the US and Europe [5], which requires the programs to obtain the user's permission before uploading these IDs to the cloud. This law limits the third party programs to identify the users [6]. Some commercial companies, such as BlueCava and Iovation, have already started to identify devices based on other features, such as browser configuration or screen resolution [7]. Recently, the researchers try to utilize the imperfection of the accelerometer sensor to generate the stable device signatures in smart phones with precision and recall in access of 96% [7].

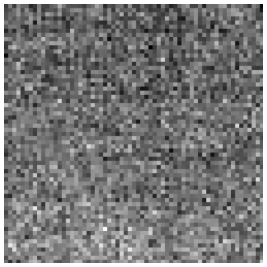

Fig. 1. A typical FPN image in a CMOS image sensor [13].

Physical Unclonable Function (PUF) is a circuit module that generates chip signatures relying on the uncontrollable and unpredictable process variations. It provides a secure and low cost solution for secure key generation, device authentication, counterfeit detection and prevention. Many PUFs have been proposed and successfully implemented in mobile applications [8]–[11]. Unlike the IDs stored in the non-volatile memory, the signatures produced by the PUF cannot be removed, copied or compromised. In this paper, we propose a new CMOS image sensor based PUF for smart phone authentication and identification. The proposed PUF exploits the fixed pattern noise (FPN) in a CMOS image sensor, which now becomes a standard component in smart phones, to produce a unique and reliable signature for device identification. The term FPN refers to the variations in output pixel values, under uniform illumination, due to device and interconnect mismatches across an image sensor [12]. A typical FPN image of a CMOS image sensor is shown in Fig. 1 [13]. Unfortunately, these patterns can be affected by the operating environments such as power supply voltage, temperature and so on. In this paper, we propose a differential readout solution to desensitize the supply voltage and temperature variations with a negligible hardware overhead. The simulation results obtained from a 65nm CMOS technology image sensor have demonstrated its viability to produce secure, robust and non-transferable unique fingerprint for smart phone authentication and identification.

The rest of the paper is organized as follows. In Section II, the design and operations of the proposed PUF are elaborated.

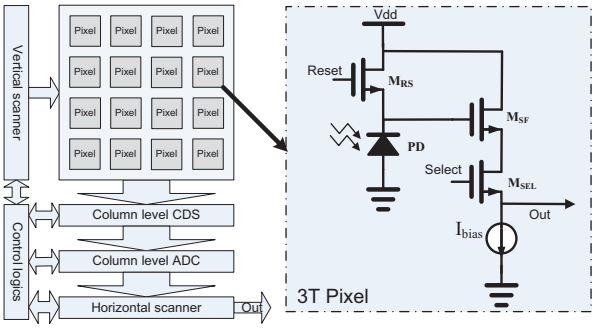

Fig. 2. Typical architecture of CMOS image sensor with 3T pixel.

The figure of merits and simulation results of the proposed PUF are presented and discussed in Section III. Finally, the conclusion is given in Section IV.

II. Circuits and Operations

A. 3T CMOS Image Sensor

Fig. 2 shows a typical architecture of 3T active pixel sensor (APS) and the pixel schematic [14]. Each pixel cell consists of a photodiode (PD), a reset transistor M_{RS}, a select transistor M_{SEL} and a source follower readout transistor M_{SF}. The operation of this pixel is explained as follows. When M_{RS} is turned on, the voltage on the photodiode (PD) is reset to the value:

$$V_{PD} = V_{dd} - V_{th,RS} + V_{KTC} \tag{1}$$

where $V_{th,RS}$ and V_{KTC} are the threshold voltage of the reset transistor M_{RS} and the thermal noise, respectively. V_{KTC} is the main random noise due to the reset operation [14].

Next, M_{RS} is turned off and the PD is electrically floated. The photocurrent I_{ph} due to the incident illumination discharges V_{PD} (omitting the small dark current). After an exposure time t, the select transistor M_{SEL} is turned on. The output voltage of this pixel is read. This voltage can be expressed as:

$$V_{out} = V_{dd} - V_{th,RS} + V_{KTC} - V_{th,SF} - \frac{I_{ph} \times t}{C_{PD}} \tag{2}$$

where $V_{th,SF}$ and C_{PD} are the threshold voltage of the source follower transistor M_{SF} and the PD junction capacitance, respectively.

It is noted that the the pixel voltage is preserved during readout, which makes it possible to read the pixel value multiple times. From (2), the variations in pixel output values (i.e., FPN) are caused by the variations in photodiode size, photodiode capacitance, and the threshold voltages of M_{RS} and M_{FS}. As the FPN can badly degrade the image qualities, noise cancelation circuits, such as correlated double sampling (CDS), are employed in the readout circuits. CDS is a method to measure electrical values such as voltages or currents by eliminating an undesired offset. The output of the pixel is measured twice to obtain the reference voltage of the pixel (the pixel voltage after it is reset) and the signal voltage of the pixel (the pixel voltage after the exposure). The reference voltage is then subtracted from the signal voltage.

B. Proposed Image Sensor based PUF

Each output bit of the proposed CMOS image sensor based PUF is obtained as a function of the two dimensional array of the pixels. As the CMOS image sensor has non-destructive readout, the original function will not be affected by the proposed PUF. In the proposed PUF, we bypass the CDS by inserting a bypass transistor in parallel with the CDS circuits, because the CDS may worsen the randomness by reducing the desirable effect of FPN for the generation of random PUF response. The pixel output voltage during the reset phase is directly read. During reset, based on (1), the output voltage of the pixel can be written as:

$$V_{rst} = V_{dd} - V_{th,RS} + V_{KTC} - V_{th,SF} \tag{3}$$

V_{rst} can be varied due to the variations of $V_{th,RS}$ and $V_{th,SF}$. The variations of V_{rst} generate a unique pattern for each pixel array. However, as V_{rst} is sensitive to the random reset noise and the variations of supply voltage and temperature, the IC signatures produced directly from V_{rst} are unstable. To obtain a more reliable signatures from the image sensor, a differential readout algorithm is proposed. The proposed challenge response pair (CRP) algorithm is shown in Fig. 3. First, the CDS is bypassed by turning the bypass transistor on. Then, V_{rst} of each pixel is scanned out. In this way, the entire image for V_{rst} (we call this image the "reset image") is readout and stored in the memory after it is digitized. Next, an n-bit challenge C is input to initialize an n-bit linear feedback shift register (LFSR) counter. n is expressed as:

$$n = \log_2 (H \times V) \tag{4}$$

where H and V are the numbers of the rows and columns of the image sensor, respectively.

To generate a stable response bit, the pixel value P_C in the "reset image" with the address C is acquired. Another challenge (address) C' is generated from the n-bit (LFSR) counter by shifting C in N ($N < 2^n - 1$) clock cycles. The pixel value of $P_{C'}$ is also read out and compared with P_C. The output bit is either 0 or 1 depending on which pixel value is larger. When the absolute value of $P_C - P_{C'}$ is larger than a predefined threshold P_{th}, which is determined empirically based on the process technology, the generated bit can be considered as stable. However , if this absolute value is smaller than or equal to P_{th}, another stable pair of pixels will be sought by shifting the content of the LFSR by one more clock cycle to generate a new C'. This procedure is repeated until the entire pixel array has been sought. In fact, P_{th} provides a knob to tune the noise margin of the pixel pairs to counteract the effect of the random KTC noise, temperature and voltage variations. Besides, the user can reconfigure this PUF by selecting a different value of N in the LFSR counter. With the reconfigurability, the security for the PUF can be greatly enhanced [15].

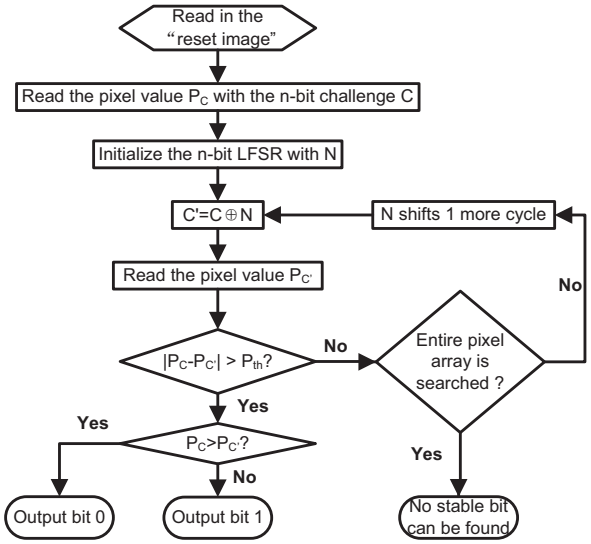

Fig. 3. CRP generation algorithm for the proposed PUF.

III. Simulation Results and Discussion

A. Figures of Merit of PUFs

Uniqueness and reliability are the most important figures of merit (FOMs) for the quality assessment of PUFs.

Uniqueness measures how different are the CRPs generated by one PUF from the other. Uniqueness can be estimated by the average inter-die Hamming Distance (HD) of the responses produced by different PUFs. Let R_u and R_v be the n-bit responses from two different chips, u and v, with the same input challenge C, the uniqueness U for m chips is formulated as:

$$U = \frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^{m} \frac{HD(R_u, R_v)}{n} \times 100\% \qquad (5)$$

The reliability measures how reproducible or stable are the CRPs of a PUF under different operating conditions. The different operating conditions can be the variations in temperature, supply voltage and so on. Let R_i be an n-bit response to an input challenge C produced by the PUF of a chip i under the nominal operating condition. The same set of challenges are then applied k times to the same PUF under varying environmental conditions to obtain the responses $R_{i,j}$ for $j = 1, 2, \cdots, k$. The reliability S for chip i can be expressed as:

$$S = 1 - \frac{1}{k} \sum_{j=1}^{k} \frac{HD(R_i, R_{i,j})}{n} \times 100\% \qquad (6)$$

Ideally, the uniqueness of a PUF is 50% for the highest distinguishability of the CRPs generated by the PUF. Meanwhile, the ideal value of reliability is 100% for PUF that can regenerate the correct responses to the same challenges at all time under all operating conditions. It is impossible to achieve these ideal values in practice. A properly designed PUF possesses acceptable quality to meet the security demand of the cryptosystem where it is applied.

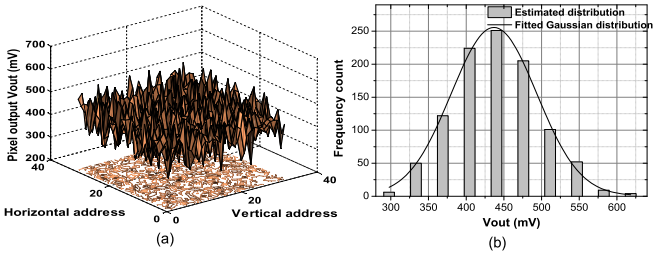

Fig. 4. The Monte Carlo simulation result for the pixel output V_{rst}: (a) in 32×32 pixel array, (b) frequency distribution.

B. Quality Analysis for the Proposed PUF

The transistor-level simulations are carried out by Cadence Virtuoso Spectre using the design kit (PDK) of GF 65nm 1.2V CMOS process technology. Monte Carlo simulation method [16] is used to introduce randomly sampled device parameter variations from a normal distribution. Each iteration of the Monte Carlo simulation represents a unique set of variations applied to a PUF instance. The PDK provided by the foundry contains the variation profile of key parameters in the GF 65nm CMOS technology, which can well represent the ranges of parameter values of the physical design due to the manufacturing process variations. The simulated CRPs of the proposed PUF based on a 32×32 3T image sensor (with the architecture of Fig. 2) are then collected and processed by the MATLAB scripts.

Fig. 4 shows the V_{rst} variations in the 32×32 3T image sensor and the histogram diagram of V_{rst}. The frequency distribution can be fitted by a Gaussian distribution of mean $\mu = 437mV$ and standard deviation $\sigma = 114mV$.

Based on the CRPs collected from 50 image sensor based PUF instances, with 120 CRPs generated for each instance, the frequency distribution of the inter-die HDs is obtained in Fig. 5. The uniqueness of these 50 instances is calculated to be 49.62%. The best fit Gaussian curve to the histogram diagram plotted in Fig. 5 has a mean of $\mu = 50.12\%$ and a standard deviation of $\sigma = 9.99\%$.

The reliability is simulated under varying supply voltages and temperatures. Fig. 6(a) shows the average reliability of the 50 PUF instances against the voltage variations. The 1000 CRPs collected under $1.2V$ are used as the reference. The supply voltage is varied from $1V$ to $1.4V$. The worst reliability of the CRPs is 99.1% when $P_{th} = 0$. The 1000 CRPs generated at $27°C$ are used as the reference to calculate the reliability of the proposed PUF against temperature variations. The average reliability calculated from the CRPs of all the 50 PUF instances at different temperatures are shown in Fig. 6(b). The worst reliability is found to be 97.6% at 100°C. Higher reliability can be obtained by increasing P_{th}. In Fig. 6, the reliability reaches 100% when $P_{th} = 10mV$ for temperature ranges from 0°C to 100°C and supply voltage ranges from $1V$ to $1.4V$.

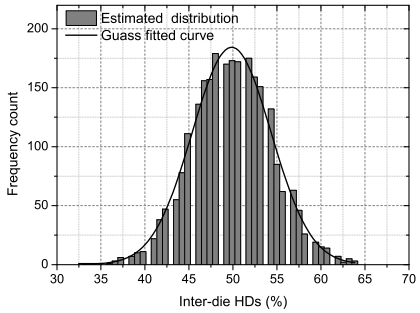

Fig. 5. Frequency distribution of the simulated inter-die HDs.

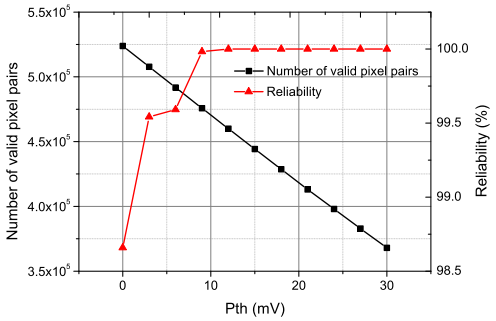

Fig. 7. Relationship between P_{th}, the number of valid pixels and the reliability of the PUF.

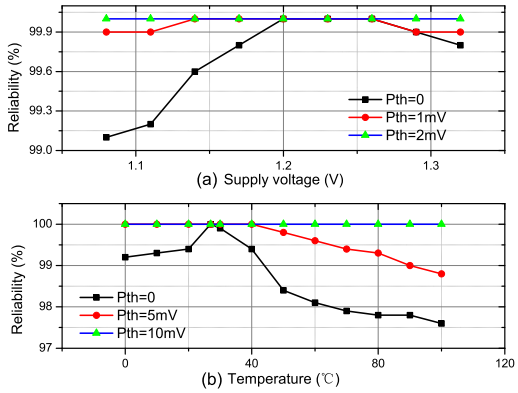

Fig. 6. Reliability of the proposed PUF with different P_{th} at (a) different voltages and (b) different temperatures.

The high reliability of the proposed PUF is achieved at the expense of reducing the number of valid pixels. Originally, in the 32×32 sensor, there are $C_{1024}^2 = 523776$ pairs of pixels that can be used for the CRPs with $P_{th} = 0$. This corresponds to 511 CRPs for each pixel . The reliability is 98.66% with this setting. By increasing the threshold voltage P_{th}, only the pixel pairs with large distance are selected. Fig. 7 shows the relationship between the threshold P_{th} versus the number of valid pixels and the reliability of the PUF. P_{th} controls the trade-off between the reliability and the hardware efficiency. Benefiting from the large number of pixels in a modern CMOS image sensor, our proposed PUF will still have a huge CRP space while achieving a very high reliability.

IV. Conclusion

This paper presents a new CMOS image sensor based PUF. The proposed method has been simulated with GF 65nm CMOS technology. The intrinsic IDs generated from the imager cores have an uniqueness of 50.12%. A high reliability of 100% with supply voltage of $1 \sim 1.4V$ and temperature range of $0 \sim 100°C$ can be attained by tuning the differential threshold P_{th}. As a standard and indispensable component of the smart phones and tablets, the use of this security primitive for device identification and authentication has not only enhanced the security of existing mobile applications but also open out an avenue for exciting new development in mobile application security.

References

[1] "The world in 2014: ICT facts and figures," International Telecommunication Union, Tech. Rep., April 2014. [Online]. Available: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf

[2] D. Barboza, "In China, knockoff cellphones are a hit," April 2009. [Online]. Available: http://www.nytimes.com/2009/04/28/technology/28cell.html?_r=0

[3] "Counterfeit mobile phones a US$6 billion a year drain on global economy," Feb. 2014. [Online]. Available: http://www.mmfai.org/public/docs/eng/PR_MMF_Counterfeit.pdf

[4] "Free tool can change SN and IMEI to unlock iphone," http://yjjhen.sinaapp.com/, 2013.

[5] E. P. Council, "Directive 2002/58 on privacy and electronic communications," http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF, 2011.

[6] N. Nikiforakis *et al.*, "Cookieless monster: Exploring the ecosystem of webbased device fingerprinting," in *Proc. IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, May 2013, pp. 541–555.

[7] S. Dey *et al.*, "AccelPrint: Imperfections of accelerometers make smartphones trackable," in *Proc. of the Network and Distributed System Security Symposium (NDSS)*, San Diego, USA, Feb. 2014.

[8] R. S. Pappu, "Physical one-way functions," Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, 2001.

[9] G. Suh and S. Devadas, "Physical unclonable function for device authentication and secret key generation," in *Proc. Design Automation Conf. (DAC 07)*, San Diego, USA, June 2007, pp. 9–14.

[10] K. Lofstrom, W. Daasch, and D. Taylor, "IC identification circuit using device mismatch," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, San Francisco, USA, Feb. 2000, pp. 372–373.

[11] Y. Su, J. Holleman, and B. Otis, "A 1.6 pj/bit 96% stable chip-ID generating circuit using process variations," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, San Francisco, USA, Feb. 2007, pp. 406–407.

[12] H. Tian *et al.*, "Analysis of temporal noise in CMOS photodiode active pixel sensor," *IEEE Journal of Solid-State Circuits*, vol. 36, no. 1, pp. 92–101, 2001.

[13] A. E. Gamal *et al.*, "Modeling and estimation of FPN components in CMOS image sensors," in *Proc. the international society for optics and photonics (SPIE)*, San Jose, USA, Jan. 1998, pp. 168–177.

[14] J. Ohta, *Smart CMOS Image Sensors and Applications*. London, New York: CRC Press, 2007.

[15] S. Katzenbeisser *et al.*, "Recyclable PUFs: logically reconfigurable PUFs," *Journal of Cryptographic Engineering*, vol. 1, no. 3, pp. 177–186, 2011.

[16] L. Lang *et al.*, "Design and validation of arbiter-based PUFs for sub-45-nm low-power security applications," *IEEE Trans. Inform. Forensics and Security*, vol. 7, no. 4, pp. 1394–1403, Aug. 2012.