A New Event-driven Dynamic Vision Sensor based Physical Unclonable Function for Camera Authentication in Reactive Monitoring System

Yue Zheng*, Yuan Cao+, and Chip-Hong Chang*
*School of Electrical and Electronic Engineering, Nanyang Technological University
+College of Internet of Things Engineering, Hohai University, Changzhou, China
Email: yzheng015@e.ntu.edu.sg, ycao3@e.ntu.edu.sg, echchang@ntu.edu.sg.

***Abstract*—Surveillance footage has become an integral part of law enforcement as video cameras become ubiquitous, affordable and more reliable. Dynamic vision sensor (DVS) emerges as a new sensing technology that outsmarts existing static CMOS image sensors in vision-enabled traffic monitoring, assisted living and high-speed target tracking for its low latency, high temporal resolution and wide dynamic range under uncontrolled illumination. Instead of recording a steady stream of snapshots taken at a fixed rate, DVS responds only to temporal contrast and records only sparse asynchronous address-events with precise timing information. However, the accountability of the footage captured is incomplete if the cue is triggered by an unidentified device. One effective way to eliminate the anonymity is to build a random oracle out of the DVS sensor and use its authenticity as a root of trust to protect the integrity of the footage. In this paper, we present the first ever event-based physical unclonable function (PUF) for DVS camera identification and secret key generation in reactive monitoring system. A non-intrusive PUF response readout scheme is proposed by exploiting the two unique reset switches, one continuous-timed and one self-timed, of DVS pixel to enable simultaneous generation of PUF response with non-disruptive output of asynchronous address-events. Only three transistors are added to each pixel to isolate the PUF response readout and to prevent the spontaneously detected DVS events from interfering with the PUF operation, which is also triggered by the reflectance change in the scene. Our simulation results based on 1.8V 180nm CMOS technology show that the raw response generated by the proposed event-driven DVS-based PUF has near ideal uniqueness of 49.96%, and worst-case reliability of 96.3% and 99.2% for variations of temperature from −35∼115°C and supply voltage from 1.6∼2.0V, respectively. Its randomness has also been attested by the NIST tests.**

I. Introduction

Visual Sensor Network (VSN) [1] has become increasingly ubiquitous and pervasive as video cameras are made better, more reliable and substantially cheaper by technological advancements. Two prevalent applications where conventional frame-based imaging technology may be inadequate are traffic monitoring [2] and assisted living [3]. In the former public surveillance scenario, performance may be compromised by its limited dynamic range and bandwidth due to the short event latency while the latter private surveillance scenario may have implication on infringed privacy. In both cases, tremendous time and effort are needed to sit through endless hours of recorded video to find the clues of law violation or exceptions. The monitoring systems carry hidden cost of additional sensors for event detection such as radar or laser range finders and on-board processing units to analyze massive pixel data generated from the steady image stream. These problems can be eased by the use of emerging Dynamic Vision Sensor (DVS) [4] and its augmented Dynamic and Active Pixel Vision Sensor (DAVIS) [5]. DVS pixels respond asynchronously to relevant changes in intensity and output them in sparse address-event representation (AER). The reduction of data redundancy by event-based triggered focal-plane analog processing makes DVS more suited than conventional active pixel vision sensor to reactive surveillance system where images or videos are only recorded if a critical event has occurred.

Using reactive monitoring for law enforcement requires the guarantee of not only the integrity of collected evidence but also the authenticity of sensing device. In order that the footage captured by the camera can be used to hold the offender accountable for his misdeed, the trustworthiness of the DVS-based camera must be established. A few sensor level authentication approaches have been proposed to guarantee a real end point security, spanning from the data generator to the data receiver [1]. A majority of these approaches use a trusted computing platform enclosed within the monitoring facility to perform the encryption and authentication. For example, TrustEYE.M4 [6] used for secure sensing consists of an OmniVision OV5642 image sensor, a dedicated hardware security module and an ARM Cortex M4 processor. Such solutions are costly and the safekeeping and communication of private key for encryption and device authentication are vulnerable to invasive and semi-invasive attacks [7], [8]. Physical Unclonable Function (PUF) is a new security primitive that leverages the uncontrollable manufacturing process variations of identically designed circuits to assign an integrated device a unique fingerprint. In [9], a keyless camera authentication has been proposed by transforming the pixel array of a CMOS image sensor into a PUF. Its device signature is extracted from the fixed pattern noise (FPN) of reset image by bypassing the correlation double sampling (CDS) of active pixel sensor (APS). Such a device ID can only be regenerated when the device is powered on and upon stimulated by a challenge.

978-1-5090-5701-6/16/$31.00 ©2016 IEEE

Without storing it in local memory or hardcoded, the ID cannot be easily stolen or replicated. The integrity of image sensor is assured as any attempts to tamper or reverse engineer the pixel array will render its PUF inoperable. Unfortunately, CDS bypass is not applicable to DVS due to their completely different sensing and reset mechanism. One drawback of current image sensor PUF [9] is its response is dependent solely on the input challenge. As no exposure can be made during PUF operation, the response to the input challenge is not event-driven.

In this paper, a new DVS-based PUF for on-chip identification and secret key generation is proposed. The PUF response is triggered by an address event and is dependent on both the input challenge and the temporal contrast of triggered event. This is made possible by devising a new readout scheme to take advantage of the continuous-timed and self-timed reset switches unique to DVS pixels. Both switches are made to work in tandem for PUF generation and address-event readout without intervening each other operations. The DVS sensor can continue to complete the detection and output precisely timed information about the motion of tracking target while in PUF operation triggered by the same event. This has greatly improved the responsiveness and cut down the cost of auxiliary non-vision based sensors in reactive monitoring system.

The rest of the paper is organized as follows. Section II introduces the fundamentals of DVS. Section III elaborates the entropy source of DVS, and the problems and solution for its exploitation for event-driven PUF response generation. Simulation results are presented and analyzed in Section IV. Section V concludes the paper.

II. Static and Dynamic Vision Sensor Preliminaries

An APS is the basic sensing circuit for a pixel of a frame-based image sensor. Fig. 1 shows the typical CMOS circuit implementation of a three-transistor APS (3T-APS). The photodiode is a sensing element that converts light intensity into electrical current. Even in the absence of illumination, or in uniform illumination, device mismatches and offset due to the manufacturing process variations can cause the individual photodiode to respond differently from pixels to pixels. This FPN can be suppressed by using a CDS circuit [5] to cancel the reset voltage from the signal voltage. The analog output voltage after CDS is then digitized by an ADC. To improve the image quality by CDS, all pixels need to be reset each time before an exposure is taken.

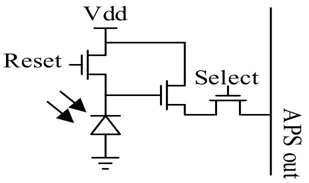
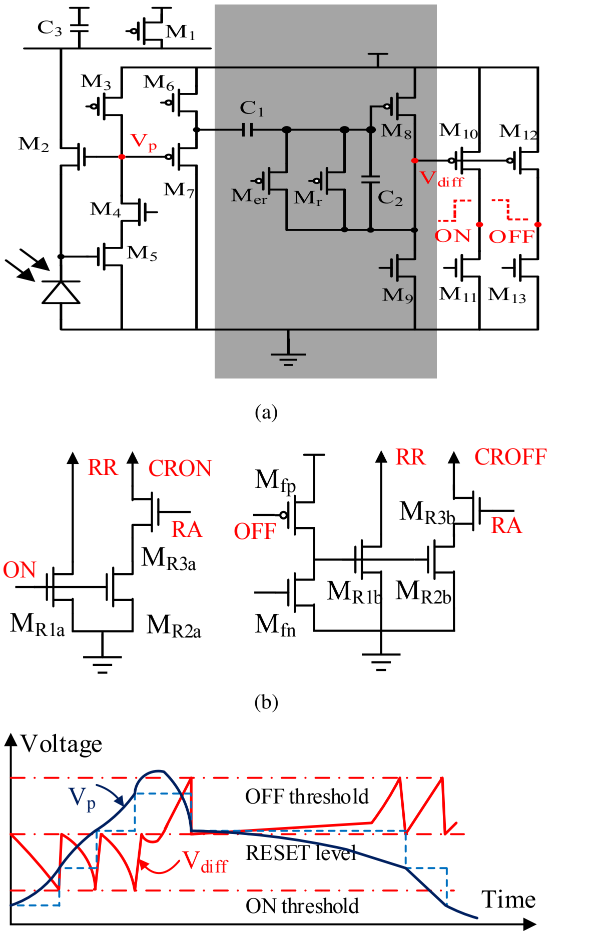


Fig. 1. Schematic of a typical 3T-APS for frame-based image sensor



(a)

(b)

(c)

Fig. 2. (a) Pixel schematic, (b) pixel AER logic and (c) operating principle of DVS [10].

The pixel circuit for DVS is more complex. Fig. 2(a) shows a DVS pixel schematic excerpted from [10]. A transimpedance amplifier, consisting of transistors M_2, M_3, M_4 and M_5, converts the photocurrent logarithmically into a voltage V_p. V_p is buffered by a source follower composed of M_6 and M_7 to avoid the transimpedance amplifier from being loaded by the capacitive input of the differencing circuit in the shaded area of Fig. 2(a). The differencing circuit detects the temporal change in luminance. The direction of change is detected by two common-source static inverter comparators made up of $M_{10} \sim M_{13}$ with different bias voltages. The ON and OFF thresholds of the comparators are set up by the biasing circuits shown in Fig. 2(b). The common input voltage V_{diff} to the comparators can only cross either one of the two thresholds but not both simultaneously. When this happens, the transistor M_{R1a} or M_{R1b} will be switched on accordingly and a row-request signal RR will be generated to signify that an ON or an OFF event has occurred.

Different from the APS of frame-based image sensor, DVS pixels are not globally refreshed during operation as the address-events are generated locally and asynchronously by the pixels. A DVS sensor has unique readout circuits for asynchronous communication between the pixel array and its peripheral [10]. The row request RR signal is shared by all pixels in a row. When RR is acknowledged by the row acknowledge RA to enable the arbiter circuit of each pixel (see Fig. 2(b)) in the addressed row, the pixel that crosses the ON or OFF event generation threshold will send out a column request signal $CRON$ or $CROFF$ accordingly. The sparse and asynchronous events are then output in AER [11]. For a 128 × 128 DVS array, the AER of an address event consists of an 1-bit ON or OFF event state, a 7-bit row address and a 7-bit column address.

DVS adopts a self-timed reset mechanism. When an activated cell completes its communication, the transistor M_r in Fig. 2(a) will be pulled low to reset the pixel, so V_{diff} will be pulled back to a reset level between the ON and OFF threshold region and no event can be generated during this period. Since M_r is self-timed, it cannot be accessed externally. Fortunately, there is also a reset switch M_{er} in each pixel that can be externally accessed. M_{er} allows selected columns of pixels to be hold in reset to optimize the processing of pixels in the regions of interest. This reset switch offers an opportunity to implement an event-triggered PUF in DVS efficiently and differentiate it from the frame-based PUF.

III. Proposed Event-based PUF

A. Process Variation Analysis

The entropy of PUF is usually abstracted from mismatches stem from the manufacturing process variations of symmetrical or identical circuit structures. For the case of DVS, the differencing circuit in the shaded area of Fig. 2(a) is an ideal candidate. When M_r or M_{er} turns on, the DVS cell works in the reset mode. Without parametric mismatch, the voltage V_{diff} of the differencing circuit is expected to be the same for all identically designed cells. The process variation dependence of V_{diff} is derived as follows.

As transistors M_8 and M_9 are operated in the subthreshold region to reduce power consumption, their individual drain current can be expressed as:

$$I_D = I_0 e^{\frac{V_{gs}-V_{th}}{nV_T}} (1 - e^{\frac{-V_{ds}}{V_T}}) \tag{1}$$

where I_0 is the drain current at $V_{gs} = V_{th}$, V_{gs} is the gate-source voltage, V_{th} is the threshold voltage, V_{ds} is the drain-source voltage, n is the bulk junction emission coefficient and V_T is the thermal voltage.

If V_{ds} exceeds $4V_T$, the bracketed terms in (1) can be neglected [12]. When M_{er} is turned on, I_8 of M_8 can be expressed as:

$$I_8 = I_{0,8} e^{\frac{V_{DD}-V_{diff}-|V_{th,8}|}{V_T}} \tag{2}$$

Correspondingly, I_9 of M_9 can be expressed as:

$$I_9 = I_{0,9} e^{\frac{V_{gs,9}-V_{th,9}}{V_T}} \tag{3}$$

Without applying any body bias, i.e., when the body-source voltage V_{bs} is equal to zero, $V_{th,8}$ and $V_{th,9}$ of transistors M_8 and M_9 are given by [13]:

$$|V_{th8}| = |V_{th0,8}| - \lambda_D(V_{DD} - V_{diff}) \tag{4}$$

$$V_{th9} = V_{th0,9} - \lambda_D diff \tag{5}$$

where $V_{th0,8}$ and $V_{th0,9}$ are the threshold voltages at zero drain bias for M_8 and M_9, respectively. $\lambda_d = -\partial V_{th}/\partial V_{ds}$ is the drain induced barrier lowering (DIBL) coefficient.

By setting $I_8 = I_9$, V_{diff} can be derived as follows:

$$V_{diff} = \frac{1+\lambda_d}{1+2\lambda_d}V_{DD} + \frac{V_{th0,9} - |V_{th0,8}|}{1+2\lambda_d} - \frac{V_{gs,9} + nV_T ln\frac{I_{0,9}}{I_{0,8}}}{1+2\lambda_d} \tag{6}$$

Differentiating V_{diff} with respect to λ_d, we have:

$$\frac{\partial V_{diff}}{\partial \lambda_d} = -\frac{V_{DD} - 2(|V_{th0,8}| - V_{th0,9} + V_{gs,9} + nV_T ln\frac{I_{0,9}}{I_{0,8}})}{(1+2\lambda_d)^2} \tag{7}$$

As M_9 is in the subthreshold region, $V_{gs,9} \ll V_{DD}$, which makes V_{DD} dominates all terms in the numerator of (7). Since $\lambda_d \ll 1$, $(1+2\lambda_d)^2 \approx 1$. From (7), $\partial V_{diff} \approx -V_{DD}\partial\lambda_d$. As DIBL is a principal contributor to threshold voltage variation in short channel device, the proportional change in V_{diff} at reset with the change in λ_d implies that V_{diff} at reset is sensitive to manufacturing process variations. The variation in threshold voltage results in different V_{diff} output from even the matched devices in the neighboring pixels during row-reset.

B. Non-intrusive Readout for PUF Operation

Although the differencing circuit output at reset time is proven to be a good entropy source for PUF operation, there is no direct access to that analog pixel value. Therefore, a new readout mechanism is needed to feed the challenge of the PUF. As the DVS pixel is already more complex than the APS, each pixel can only afford to add a few transistors, which aggravates the design challenge.

In frame-based image sensor, the entire pixel array has to be reset and the CDS circuit has to be bypassed to extract the PUF response. During this period, image acquisition is prohibited. When a new exposure is made, the previously generated PUF response can then be used as device signature

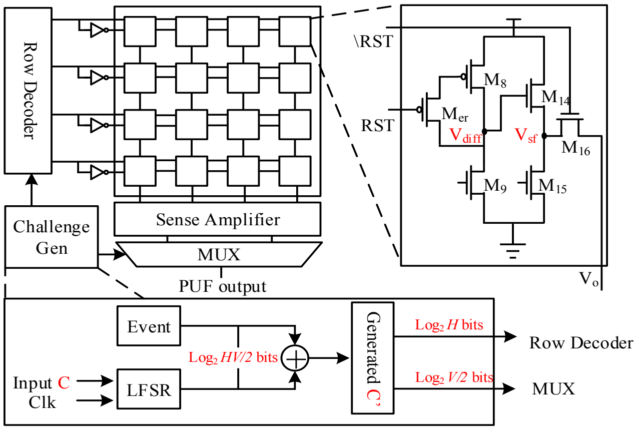


Fig. 3. Block diagram of the proposed PUF readout scheme

to encrypt or watermark the newly acquired image. Authentication can be done in the reverse order but still sequentially. This synchronized reset and the corresponding global refractoriness to absolute illumination have severely restricted the responsiveness of frame-based image sensor, increased the redundancy and prevented continuous monitoring of events happening in the scene while it is operating in the PUF mode [9]. It will be a welcoming feat if both processes can be carried out simultaneously with minimum intrusion into the existing pixel structure.

It turns out to be a blessing in disguise that the inaccessible self-timed reset switch M_r of DVS can be used to provide an undisruptive control for spontaneous firings of other pixels when the pixels reset by M_{er} are used for PUF response bit generation. As explained in Section II, the DVS pixels respond to relative changes in intensity asynchronously. Only those rows of pixels where an event is detected will be placed in the refractory period by M_r in order to output the address-events. All other pixels are allowed to fire if any reflectance changes in the scene are detected during this time. By resetting a particular row through the continuous-timed reset signal M_{er}, the RR signal cannot be produced to generate an event from this row but the pixels in all other rows are still responsive to temporal contrast.

Two contention problems remain to be resolved. Firstly, the readout of PUF response and that of DVS event should be isolated from each other. Secondly, the self-timed reset of events should not corrupt, override or be mismaken as PUF output. They can be resolved by adding three additional transistors $M_{14} \sim M_{16}$ to each DVS pixel for reading out the PUF response. M_{14} and M_{15} constitute a source follower to buffer the analog reset value V_{diff}, and M_{16} is a pass transistor to transfer the output voltage under the control of $\overline{RST}$ signal. $\overline{RST}$ is asserted only when the continuous-timed reset switch M_{er} is turned on. Therefore, when a reset occurs after the firing of an event in a DVS row, M_{16} will remain in the off state as long as M_{er} is turned off, i.e., $RST = 1$. This will prevent the asynchronous DVS self-timed reset M_r from interfering with the generation and output of PUF response.

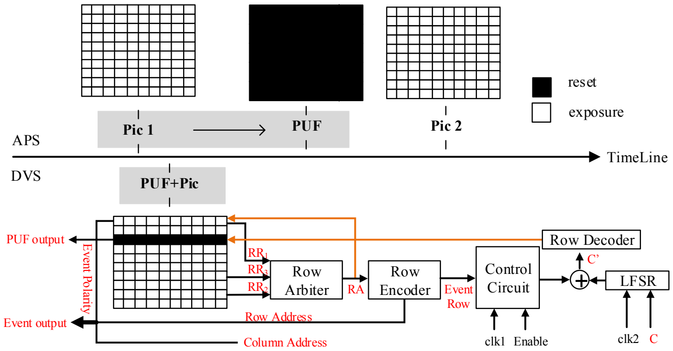


Fig. 4. Timeline of frame-based (APS) and event-based (DVS) PUF

For the PUF response to be triggered by an event and generated spontaneously with the event, the input challenge is first loaded as a seed into the LFSR. When the ON and OFF events are communicated to the peripheral, the row address acknowledged by the signal RA mentioned in Section II is XORed with the output of the LFSR to generate an M-bit signature C'. The upper $log_2(H)$ bits of C' is used to select a row of cells for response bit generation, where H is the number of rows of DVS pixel array. This way the actual challenge applied is unpredictable by the adversary, and the cells that are selected for PUF generation will not be the event request row that triggers the PUF operation. The event that triggers the PUF generation can continue to be read out concurrently with the PUF response. Fig. 4 shows the timelines for the frame-based APS-PUF readout and the asynchronous DVS-based PUF readout.

To generate a response bit, V_{diff} of two neighboring cells are compared using a column sense amplifier. $V/2$ response bits will be generated from the row reset by M_{er}, where V is the number of columns of DVS pixel array. One of the generated response bits will be selected using a multiplexer with the lower $log_2(V/2)$ bits of C' as its data select input, as shown in the bottom inset of Fig. 3. To generate a L-bit response, the M-bit LFSR is clocked L times to obtain a new signature C' for the generation and selection of each response bit. The row address will be latched during this period. As the average DVS event rate is tens of thousands of events per second [5], the monitoring authority has full prerogative to limit the number of different PUF responses to be collected for a critical incidence by changing Clk_2 to control when the next earliest address event is allowed to mix with the output of LFSR to produce C'. By reloading the LFSR with a new challenge seed C, a new L-bit response can be generated.

C. Camera Identification for Reactive Monitoring

A possible use scenario of the proposed DVS PUF for camera identification is illustrated in Fig. 5. During the enrolment phase, all the challenge-response pairs (CRPs) of DVS sensor are recorded by a trusted party and stored in a secure database. The camera is then deployed in the field to collect evidence of law violation. An input challenge (which can be refreshed periodically by the monitoring authority) is loaded as a seed N to the LFSR. When a dubious event is detected, the PUF will be triggered by one of the instantaneous address events to generate a response. Multiple responses may be generated from different address events depending on the interval between Clk_1 and Clk_2 as well as the duration of the incident of offence. For example, in the case of traffic monitoring, DVS can also be leveraged to estimate the event speed with high quality and low computational cost compared to conventional speed detection methods [14], [15]. Its real-time speed measurement can be used to trigger an offence and enable the address latch in Fig. 4 to generate the PUF responses until the speed alarm is released. The generated responses are sent back along with their address events and the footage. The internal challenge C' of each collected response can be regenerated by the authority from its address event and the input challenge used by the monitoring authority at the time of offence. The camera can be successfully authenticated

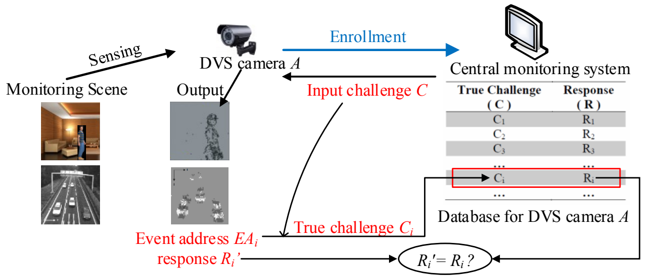


Fig. 5. An identification scheme using the proposed sensor based PUF

if the collected CRPs match those in the database.

It should be noted that DVS events are timestamped automatically [10]. Thanks to the non-disruptive PUF operation, the address events of an entire offence are recorded continuously. As long as the address events that trigger the PUF responses fit seamlessly into the set of address events recorded throughout the offence, the collected evidence is indisputable as the proven authenticity of the camera is tightly bound to the footage and time of offence.

IV. Performance Evaluation and Discussions

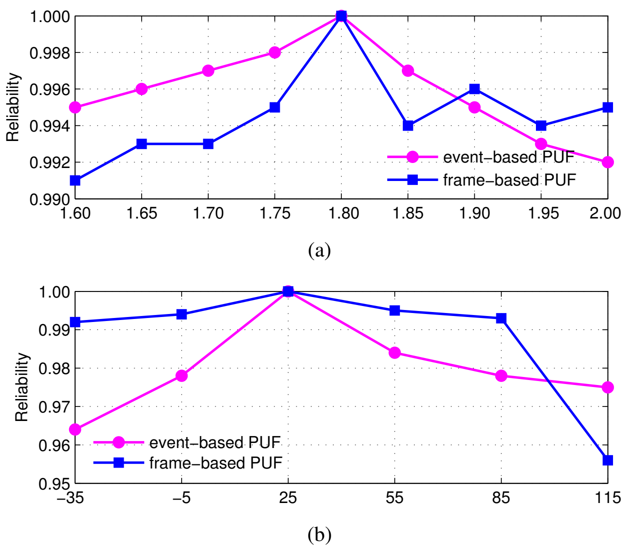
The proposed DVS-based PUF is simulated in Cadence using the process design kit (PDK) of TSMC 180nm CMOS technology. Monte Carlo method is used to introduce the random process variations according to the device characterization provided by the foundry. Each iteration of Monte Carlo simulation represents a unique set of variations applied to a PUF instance. Its performance is evaluated in term of *Reliability*, *Uniqueness*, and *Randomness*.

A. Reliability

The reliability of a PUF instance measures the reproducibility of its CRPs under different environmental conditions. It is usually evaluated by calculating the intra-die hamming distances (HD) between a reference response obtained under the nominal voltage or temperature and the regenerated responses to the same challenge under different voltages or temperatures.

A total number of 2000 responses of 128 bits each were collected. The reference responses were generated at a nominal voltage of 1.8 V and room temperature of 25°C. Each response was subsequently regenerated at supply voltage ranges from 1.6 V to 2 V with a step size of 0.05 V at room temperature. These 2000 responses were also regenerated at different temperatures varying from -35°C to 115°C with the PUF operating at 1.8V. For comparison, the frame-based image sensor PUF proposed in [16] were also simulated under the same technology and environmental variations. The reliabilities of frame-based and event-based image sensor PUFs are shown in Fig. 6. The results show that both PUFs have comparably high reliability. Overall, the responses of the proposed event-based PUF are generally more reliable against supply voltage variations but slightly less reliable against temperature variations.

To improve the reliability of raw PUF responses, error correction code (ECC) is used. The specifications of ECC is determined by the worst case reliability of the PUF. From Fig. 6, the worst-case reliability of the proposed DVS-based image sensor PUF is 96.3% at -35°C and 99.2% at 2V. Both are higher than those of the frame-based image sensor PUF. Table. I shows the worst case reliabilities of both PUFs and their BERs after applying the same ECC. The BER after ECC of DVS-based PUF is found to be about eight times smaller than that of [16].



(a)

(b)

Fig. 6. Reliability against (a) voltage (V) variation and (b) temperature (°C) variation.

TABLE I
Worst Case Reliability of Image Sensor Based PUFs

raw PUF	worst case reliability	BER after ECC*
ISICIR [16]	0.956(115°C)	1.5445e-04
This work	0.963(-35 °C)	2.0343e-05

* Bit error rate (BER) after applying BCH(127,36,15) code.

B. Uniqueness

The responses generated from a PUF device should be distinguishable from those generated from other devices for the same challenge. This quality is commonly evaluated by the inter-die hamming distance of responses collected from different PUF instances to the same challenge.

For the uniqueness test, a set of 64-bit responses were obtained by simulating 2000 DVS-based PUF instances at 1.8 V and 25°C. The uniqueness of these 2000 instances is calculated to be 49.96%. Fig. 7 shows the probability mass function of inter-die hamming distances. It fits almost perfectly with the ideal binomial distribution (the red curve) with equal probability of success and failure of each trial for 64 trials per experiment.

C. Randomness

The cryptographic randomness of the proposed PUF is evaluated by the NIST test [17]. Altogether 100000 response bits were generated from the DVS-based PUF. They were divided

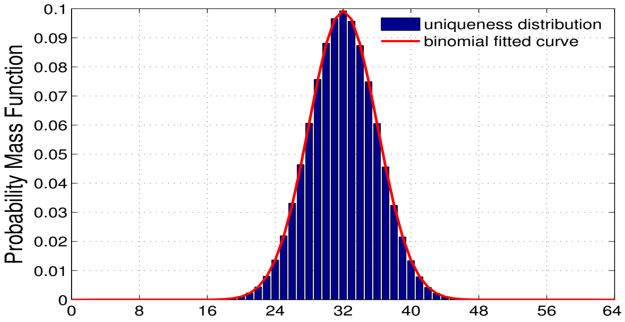


Fig. 7. Simulated inter-die variation (Ave = 31.98 bits out of 64 bits, 49.96%).

into 20 blocks of 5000 bits each for the test. Statistical tests that performed are showed in the first column. The second and third columns indicate the P-value obtained via the application of a chi-square test at the 1% level and the proportion of binary sequences that passed the tests respectively. A P-value larger than 0.01 and a minimum pass rate of 18/20 is required to certify that the generated bitstream is random. The NIST test results shown in Table. II validate that the proposed PUF can be used as a generator of cryptographic nonces or random numbers.

TABLE II
RESULTS OF NIST TESTS ON RANDOM SEQUENCES GENERATED BY PROPOSED DVS-BASED PUF

Statistical	P VAL	PROP	RESULT
Frequency	0.025193	19/20	Pass
BlockFrequency	0.637119	19/20	Pass
CumulativeSums(forward)	0.350485	19/20	Pass
CumulativeSums(backward)	0.213309	19/20	Pass
Runs	0.637119	20/20	Pass
LongestRun	0.739918	20/20	Pass
Rank	0.025193	20/20	Pass
FFT	0.213309	19/20	Pass
OverlappingTemplate	0.035174	20/20	Pass
ApproximateEntropy	0.275709	19/20	Pass
Serial(forward)	0.964295	20/20	Pass
Serial(backward)	0.350485	20/20	Pass
LinearComplexity	0.350485	18/20	Pass

V. Conclusion

This paper presents the first ever proposal on vision sensor based PUF that has coherently unified device authenticity, event integrity and acquisition time to achieve trustworthiness and non-repudiation of captured evidence. To prevent the use of forged, fabricated or tainted electronic vision evidence to sway the verdict in a court case, the responses of vision sensor PUF are controlled not only by the input challenge but also triggered and influenced by the events happened in the scene. By exploiting the unique properties of DVS sensor, time-stamped target tracking in busy scene can be recorded spontaneously as the PUF responses are generated. To overcome the contention of concurrent response bit generation and address-event acquisition due to the mandatory pixel reset in both operations, a new non-intrusive readout scheme is proposed. The method requires only three additional transistors per pixel to isolate the continuous-timed reset from the self-timed reset. Event-driven PUF eliminates voluminous amount of redundant and irrelevant background data when used in reactive monitoring system for law enforcement. Our simulation results have also corroborated its good cryptographic properties and quality as unique device identifier and secret key generator.

Acknowledgment

This research is supported by Singapore Ministry of Education AcRF Tier 1 Grant No. RG186/14.

References

[1] T. Winkler and B. Rinner, "Security and privacy protection in visual sensor networks: A survey," *ACM Computing Surveys (CSUR)*, vol. 47, no. 1, pp. 2:1–2:42, Jul. 2014.

[2] T. Semertzidis, K. Dimitropoulos, A. Koutsia, and N. Grammalidis, "Video sensor network for real-time traffic monitoring and surveillance," *IET Intelligent Transport Syst.*, vol. 4, no. 2, pp. 103–112, Jun. 2010.

[3] D. Sunehra and A. Bano, "An intelligent surveillance with cloud storage for home security," in *Proc. IEEE Annual India Conf. (INDICON)*, Pune, India, Dec. 2014, pp. 1–6.

[4] T. Serrano-Gotarredona and B. Linares-Barranco, "A 128 × 128 1.5% contrast sensitivity 0.9% FPN 3 μs latency 4 mW asynchronous frame-free dynamic vision sensor using transimpedance preamplifiers," *IEEE J. Solid-State Circuits*, vol. 48, no. 3, pp. 827–838, Mar. 2013.

[5] C. Brandli, R. Berner, M. Yang, S.-C. Liu, and T. Delbruck, "A 240× 180 130 dB 3 μs latency global shutter spatiotemporal vision sensor," *IEEE J. Solid-State Circuits*, vol. 49, no. 10, pp. 2333–2341, Oct. 2014.

[6] T. Winkler and B. Rinner, "Sensor-level security and privacy protection by embedding video content analysis," in *Proc. IEEE Digital Signal Process. (DSP)*, Fira, Greece, July 2013, pp. 1–6.

[7] J. Delvaux and I. Verbauwhede, "Key-recovery attacks on various RO PUF constructions via helper data manipulation," in *Proc. IEEE Design, Automation and Test in Europe Conf. (DATE)*, Dresden, Germany, Mar. 2014, pp. 72:1 – 6.

[8] S. P. Skorobogatov, "Semi-invasive attacks: a new approach to hardware security analysis," Ph.D. dissertation, Uni. Cambridge, Cambridge, England, 2005.

[9] Y. Cao, L. Zhang, S. S. Zalivaka, C. H. Chang, and S. Chen, "CMOS image sensor based physical unclonable function for coherent sensor-level authentication," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 11, pp. 2629–2640, Nov. 2015.

[10] P. Lichtsteiner, C. Posch, and T. Delbruck, "A 128× 128 120 dB 15 μs latency asynchronous temporal contrast vision sensor," *IEEE J. Solid-State Circuits*, vol. 43, no. 2, pp. 566–576, Feb. 2008.

[11] K. A. Boahen, "A burst-mode word-serial address-event link-I: Transmitter design," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 51, no. 7, pp. 1269–1280, Jul. 2004.

[12] M. Alioto, "Understanding DC behavior of subthreshold CMOS logic through closed-form analysis," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 57, no. 7, pp. 1597–1607, Jul. 2010.

[13] H. Ghitani, "DIBL coefficient in short-channel NMOS transistors," in *Proc. of the 16th Nat. Radio Sci. Conf.(NRSC)*, Cairo, Egypt, Feb. 1999, pp. D4–1.

[14] M. Litzenberger and et. al, "Estimation of vehicle speed based on asynchronous data from a silicon retina optical sensor," in *Proc. IEEE Intelligent Transportation Syst. Conf. (ITSC)*, Toronto, Canada, Sept. 2006, pp. 653–658.

[15] E. Mueggler, C. Forster, N. Baumli, G. Gallego, and D. Scaramuzza, "Lifetime estimation of events from Dynamic Vision Sensors," in *Proc. IEEE Int. Conf. on Robotics and Automation (ICRA)*, Seattle, USA, May 2015, pp. 4874–4881.

[16] Y. Cao, S. S. Zalivaka, L. Zhang, C. H. Chang, and S. Chen, "CMOS image sensor based physical unclonable function for smart phone security applications," in *Proc. Int. Symp. on Integrated Circuits (ISIC)*, Singapore, Dec. 2014, pp. 392–395.

[17] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," DTIC Document, Tech. Rep., 2001.