X-ray and Proton Radiation Effects on 40 nm CMOS Physically Unclonable Function Devices

P. F. Wang, E. X. Zhang, *Senior Member, IEEE*, K. H. Chuang, W. Liao, *Student Member, IEEE*, H. Gong, *Student Member, IEEE*, P. Wang, *Student Member, IEEE*, C. N. Arutt, *Student Member, IEEE*, K. Ni, *Member, IEEE*, M. W. McCurdy, *Senior Member, IEEE*, I. Verbauwhede, *Fellow, IEEE*, E. Bury, D. Linten, *Senior Member, IEEE*, D. M. Fleetwood, *Fellow, IEEE*, R. D. Schrimpf, *Fellow, IEEE*, and R. A. Reed, *Fellow, IEEE*

***Abstract*—Total ionizing dose effects are investigated on a physically unclonable function (PUF) based on CMOS breakdown. Devices irradiated to 2.0 Mrad(SiO_2) show less than 11% change in current ratio at 1.2 V. The read-out window of programmed PUFs decreases significantly at high dose proton irradiation, and then recovers back to the original value after annealing. The proton test results for the *p*FET selector, the *unbroken n*FET, and the *broken n*FET indicate that the threshold voltage shift of the *p*FET selector contributes mainly to the degradation of the PUF.**

***Index Terms*— Hardware security, physically unclonable function, oxide breakdown, X-ray, proton, total ionizing dose.**

I. Introduction

Space systems require integrated circuits to perform operations such as protection of ground-to-spacecraft command and control communications in a reliable and highly secure way. New research and development in the commercial electronics sector on approaches to secure communication between systems may prove to be useful for low-cost, space-based applications. The current practice in commercial electronic systems is to place a secret key in non-volatile memory, and use cryptographic primitives such as digital signature and encryption to protect confidential information. While analogous approaches may be useful in larger space systems, such approaches are difficult and expensive to implement in low-cost, small-satellite communication systems.

In this paper, we evaluate the possibility of using a physically unclonable function (PUF) to meet the secure communication needs of space systems. A PUF is “an expression of an inherent and unclonable instance-specific feature of a physical object,” e.g., similar to fingerprints of human beings [1]. Ideally, PUFs are low-cost cryptographic primitives for secure-key generation and storage of chip IDs for device authentication and data security [2]-[5]. Silicon PUFs are a major subclass of electronic PUFs [1],[6], which use process-related variation of transistor characteristics to get a unique data pattern that is unpredictable and reproducible. An example of how PUFs might be used in space applications is to encrypt data transmission between spacecraft or between spacecraft and ground stations. To be able to function in this role in space, the PUF must be resilient to the space radiation environment. In this work, the radiation response of a CMOS-based PUF device, which utilizes the randomness of breakdown (BD) positions in transistors (BD-PUF), is evaluated using 10-keV X-rays and 1.8-MeV protons.

II. Experimental Details

The test structure for the BD-PUF examined consists of two minimum sized *n*FETs, each with shorted source and drain, and a *p*FET selector fabricated in a commercial 40 nm CMOS technology, as shown in Fig. 1 [6]. A forming step is used to establish the PUF unit by (random) breakdown of the gate dielectric in one of the two *n*FETs. In practice, a high voltage is applied to the gates of the *n*FETs by enabling the *p*FET compliance transistor. The high voltage applied to the *n*FET gate generates random defects within the gate oxide until hard failure occurs. As soon as one of the *n*FETs experiences breakdown, the current through the broken oxide will create a voltage drop on the *p*FET selector, which now acts as a compliance FET in saturation mode [7], limiting the stress voltage and current. The breakdown path in the *broken n*FET will further wear-out during this condition, in a current-limited way [8]. The *unbroken n*FET, however, will not accumulate additional

This work was supported by AFRL and AFOSR through the Hi-REV program and by the Defense Threat Reduction Agency through its Basic Research program.

P. F. Wang, E. X. Zhang, W. Liao, H. Gong, P. Wang, C. N. Arutt, K. Ni, M. W. McCurdy, D. M. Fleetwood, R. D. Schrimpf, and R. A. Reed are with the Department of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN 37235 USA (e-mail: pengfei.wang@vanderbilt.edu; enxia.zhang@vanderbilt.edu; mike.mccurdy@vanderbilt.edu; dan.fleetwood @vanderbilt.edu; ron.schrimpf@vanderbilt.edu; robert.reed@vanderbilt.edu).

K. H. Chuang, E. Bury and D. Linten are with Imec, Kapeldreef 75, Leuven B-3001, Belgium (e-mail: Kai.Hsin.Chuang@imec.be; Erik.Bury@imec. be; Dimitri.Linten@imec.be).

I. Verbauwhede is with imec-COSIC, KU Leuven, Belgium (e-mail: ingrid.verbauwhede@esat.kuleuven.be).

damage in this phase due to the reduced stress voltage. As a result, a “soft” breakdown path only will have been generated in one *n*FET [6],[9].

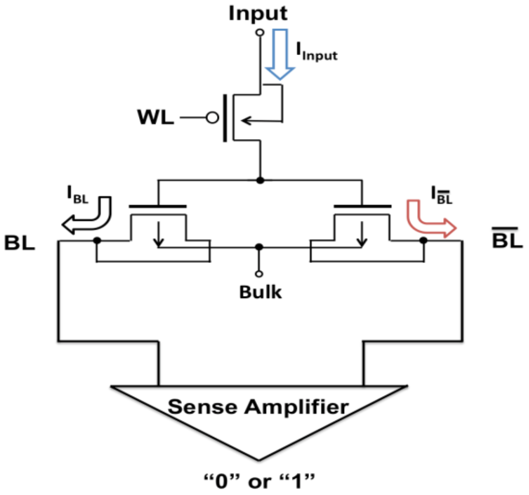

Fig. 1. BD-PUF structure, consisting of two minimum sized *n*FETs (*W* x *L* = 120 x 40 nm^2) and a *p*FET selector. Breakdown can be generated on one of the *n*FETs randomly.

The forming step and measurement of the I_D-V_G characteristics were performed using a HP4156 semiconductor parameter analyzer. Forming currents vs. time are shown in Fig. 2. The forming step was accomplished by applying 2 V to the *input*, 1 V on the *word line WL*, and -2 V on the *bit line BL*, $\overline{BL}$, and *bulk* contacts for 5 seconds. A straightforward method to recognize the device in which breakdown occurs is to compare the current of *BL* and $\overline{BL}$. In this example, $\overline{BL}$ experiences breakdown after 0.25 s of stress. Breakdown in the *BL n*FET is represented by a logical “0;” conversely, if breakdown occurs on the $\overline{BL}$ *n*FET, it is represented as a logical “1.”

In an actual application, a readout circuit applies a pulsed voltage to BL and $\overline{BL}$, and the resulting currents flow through a sense amplifier (Fig. 1). Whether the state is “0” or “1” is determined by comparing the current differences. Readout values are compared with expected values to determine whether a query or command is authentic. To simulate the sensing portion of this process, in this work we apply 1.2 V to the *input* and evaluate the resulting BL and $\overline{BL}$ currents.

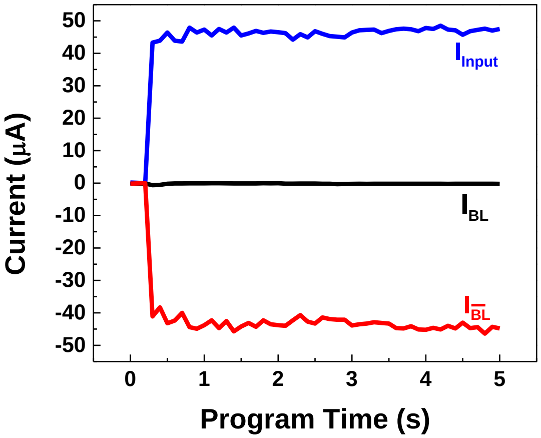

Fig. 2. Forming step of a BD-PUF. The $\overline{BL}$ *n*FET experiences breakdown at ~ 0.25 s.

III. EXPERIMENTAL RESULTS

This section describes the results of X-ray and proton irradiation experiments on the BD-PUF structure after forming.

A.X-ray Irradiation

X-ray irradiation was performed on unlidded packaged parts using an ARACOR 4100 10-keV X-ray system with a dose rate of 31.5 krad(SiO_2)/min. All terminals of the device under test (DUT) were grounded during exposure. The current read-out is done by sweeping the input voltage from 0 V to 1.5 V with all other terminals grounded. The pre-irradiation behavior of the PUF is stable, as shown in Fig. 3(a). The currents associated with $\overline{BL}$ breakdown show no significant variation during 20 subsequent sweeps. Fig. 3(b) shows *I-V* read curves of the BD-PUF before and after 10-keV X-ray irradiation up to 2 Mrad(SiO_2). Less than 11% change in current ratio at 1.2 V was observed with low-dose X-ray exposure, i.e., the BD-PUF stability is not affected significantly by X-ray irradiation.

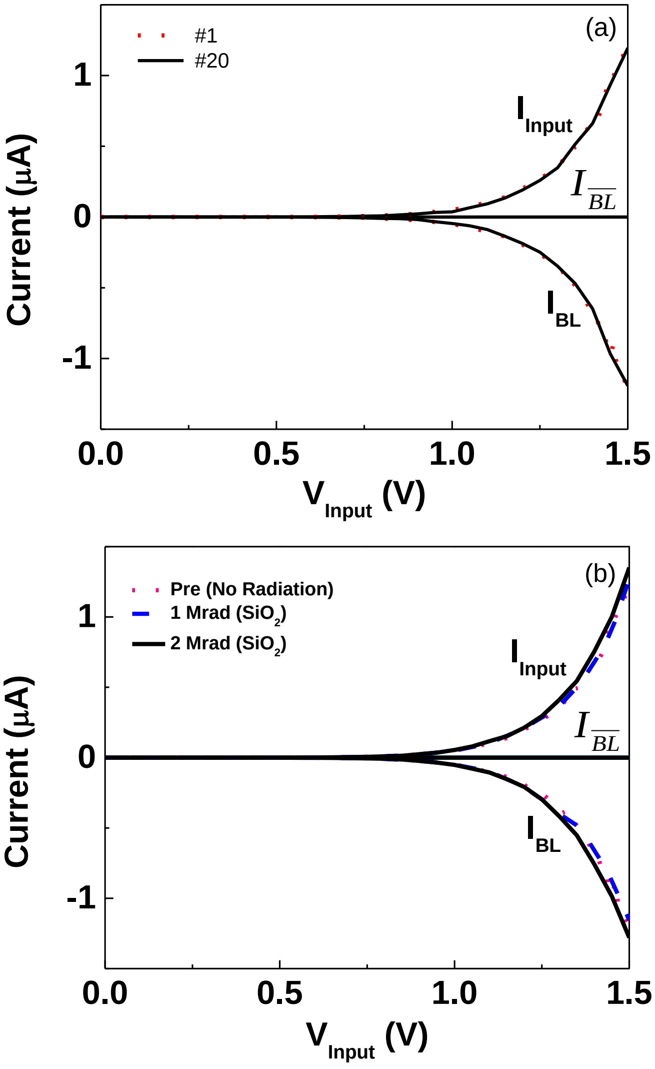

Fig. 3. Input/output currents vs. input voltage for (a) 20 cycles, demonstrating little cycle-to-cycle variation, and (b) a BD-PUF at different TID levels for 10-keV X-ray irradiation. V_{Input} is the voltage of the terminal “*input”* defined in Fig. 1.

B. 1.8 MeV Proton Irradiation

1.8 MeV proton irradiation experiments were conducted using the Pelletron accelerator at Vanderbilt University. The beam size was sufficient to irradiate the entire die uniformly. BD-PUFs were irradiated with all terminals grounded. The TID levels for proton fluences of 3 x 10^{13}, 5 x 10^{13}, 7 x 10^{13} and 1 x 10^{14} cm^{-2} are 58, 96, 134 and 192 Mrad(Si), respectively [10]. Fig. 4(a) plots the measured electrical response of the BD-PUF before and after proton exposure. Below a fluence of 3 x 10^{13} cm^{-2}, there is no radiation-induced change of the input and BL currents. However, the input currents and BL currents decrease with fluences above 3 x 10^{13} cm^{-2}. In contrast, the $\overline{BL}$ current Fig. 4(b) *increases* significantly, and already noticeably at the lowest radiation dose. Note that the $\overline{BL}$ current, which is quite small, is plotted on a log scale for visibility.

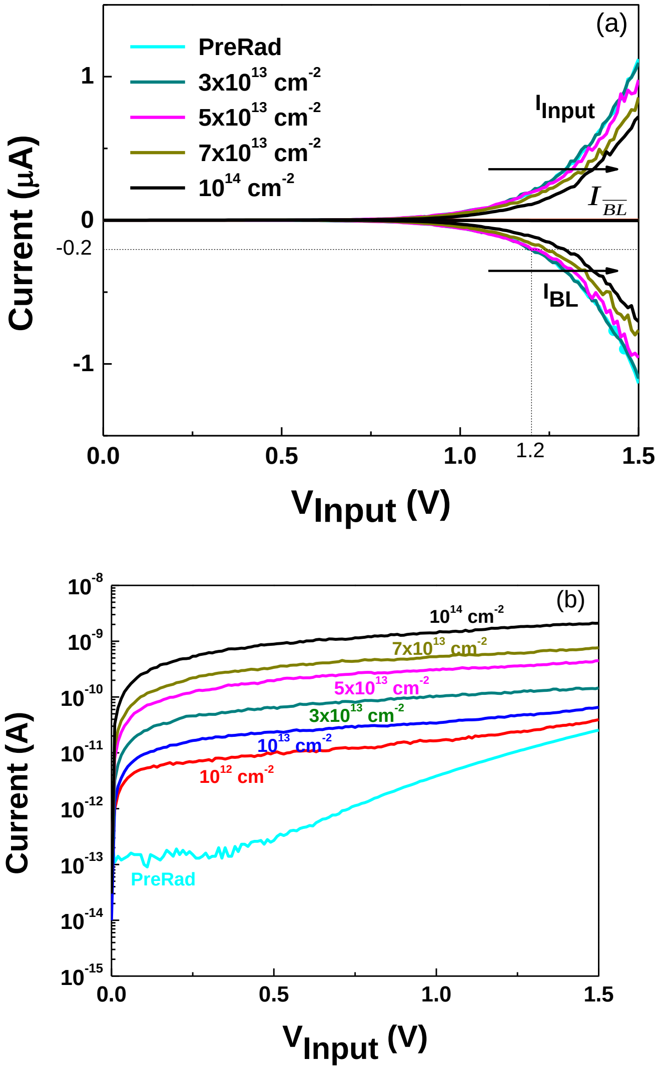

Fig. 4. (a) Current read-out of BD-PUF, and (b) $\overline{BL}$ current before and after 1.8 MeV proton irradiation. V_{Input} is the voltage of the terminal "*input*" defined in Fig. 1.

The BL current (I_{BL}) is -0.2 μA at 1.2 V for the pre-irradiation test, as shown in Fig. 4(a). For a fixed value of I_{BL}, the corresponding input voltage increases as the fluence becomes larger. This increase is characterized as ΔV_{BD}. Fig. 5(a) shows ΔV_{BD} as a function of fluence and the percentage decrease of the BL-current magnitude. ΔV_{BD} first increases with fluence and subsequently shows signs of recovery. Moreover, after enhanced recovery by annealing at high temperature (100 °C), ΔV_{BD} returns to its value prior to irradiation. Finally, the memory ratio ($I_{BL}/I_{BL\text{-}bar}$), the crucial application parameter to distinguish between a "0" or a "1," is extracted in Fig. 5(b). Similar to what is observed with ΔV_{BD}, the memory ratio between the I_{BL} and $I_{BL\text{-}bar}$ at 1.2 V decreases with fluence, then partially recovers at room temperature, and finally recovers back to the original value after annealing.

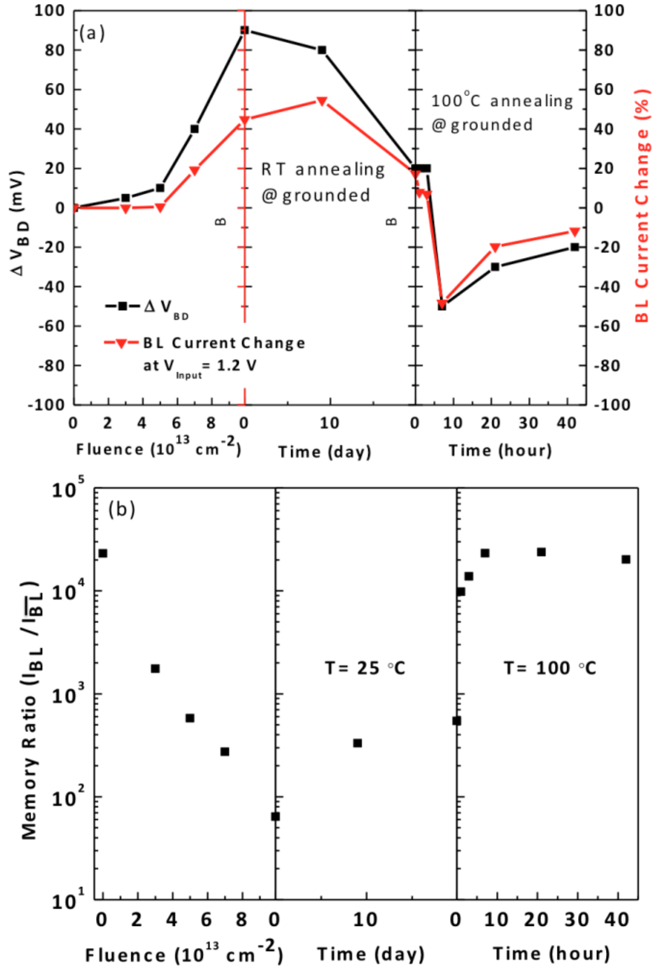

Fig. 5. (a) The change of input voltage when the BL current is -0.2 μA, and percentage decrease of BL current at 1.2 V, and (b) memory ratio as a function of fluence and annealing time.

C. Transistor Results

Fig. 6(a) shows the I_D-V_G characteristics for proton tests on a *p*FET selector. Threshold-voltage shifts for different proton fluences and annealing times are shown in Fig. 6(b). Two *p*FETs were used for the proton measurements, and all package terminals were grounded for the *p*FET selector during exposure. ΔV_{th} increases significantly with fluence as a result of hole trapping in the gate dielectric and the generation of radiation-induced interface traps [11]. This leads to a decrease in drive current within the *p*FET selector. The value of ΔV_{th} recovers partially during annealing. The change of the *p*FET Δ

V_{th} here is therefore consistent with the response of ΔV_{BD} observed in Fig. 5(a).

The I_D-V_G characteristics are shown in Fig. 7 as a function of proton fluence for broken and unbroken *n*FETs. The off-state leakage currents of both the broken and unbroken *n*FET increase as the fluence becomes larger. One obvious reason that off-state leakage currents might increase for either the broken or unbroken *n*FET is increased gate leakage current due to proton-induced defect formation [12],[13]. However, Fig. 8 shows the I_G-V_G characteristics for the (a) broken and (b) unbroken *n*FET, and in neither case does the gate leakage current change significantly with proton irradiation. Hence, the increased leakage current in Figs. 7(a) and 7(b) must have a different origin.

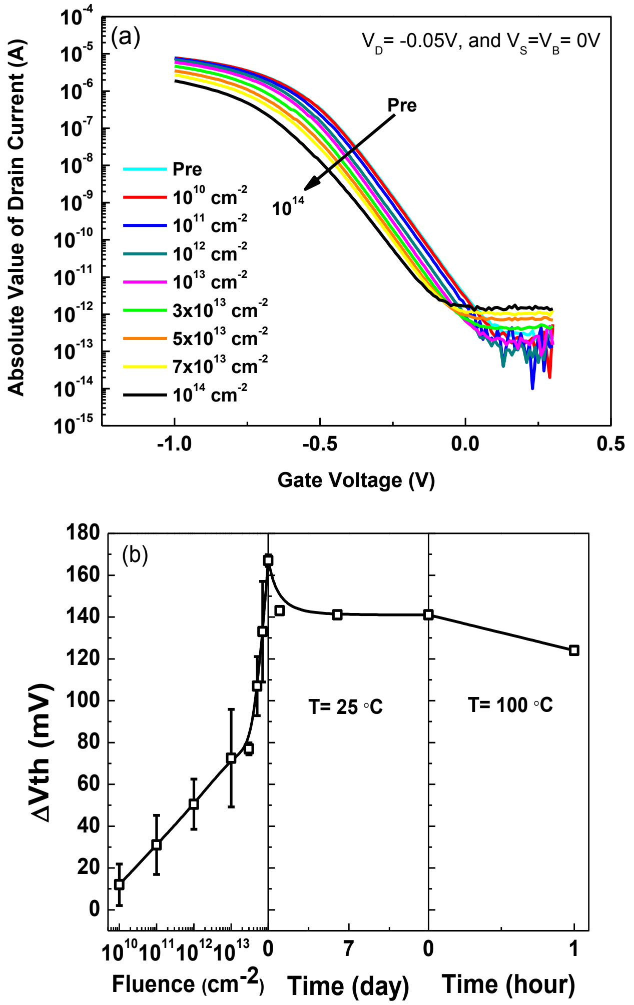

Fig. 6. (a) Semi-log plot of $I_D - V_G$ curve as a function of fluence; (b) threshold voltage shifts as a function of fluence and annealing time. Error bars here show the full range of variation observed.

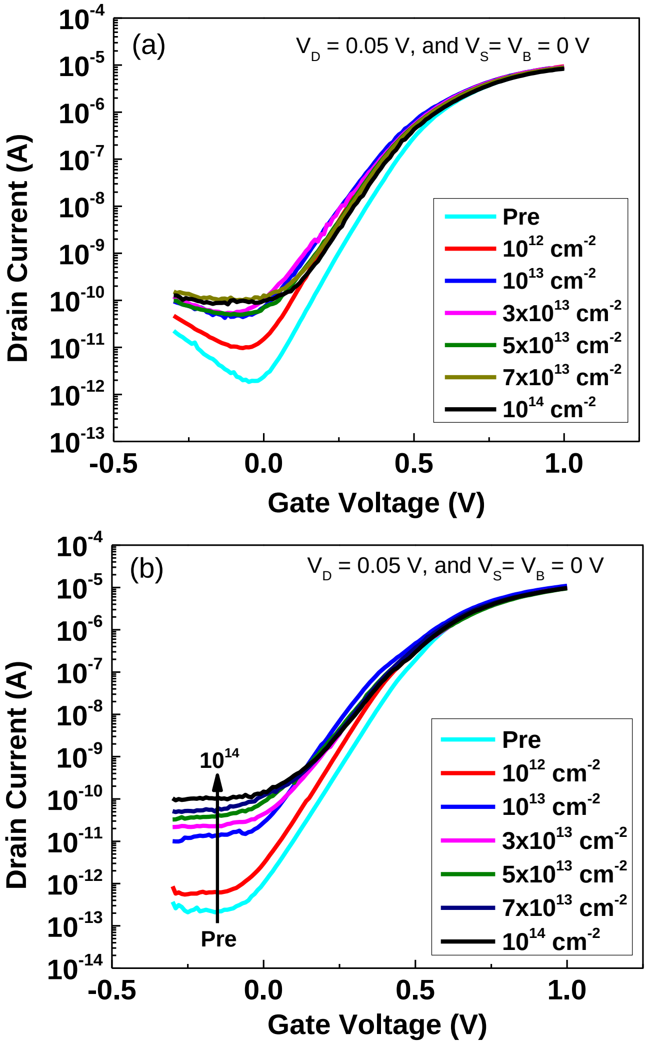

Fig. 7. Semi-log plots of $I_D - V_G$ curves for (a) the *broken* *n*FET, and (b) the *unbroken* *n*FET as a function of fluence.

IV. Discussion

Fig. 9 shows a schematic diagram of the current through the PUF after its forming step and proton irradiation. Current from the *Input* flows through the *p*FET selector, and then through the parallel combination of the broken and unbroken *n*FETs. The resistance of the broken *n*FET is much lower than that of the unbroken *n*FET, so before and after proton irradiation, nearly all of the current flows through the broken *n*FET. Fig. 6(a) shows that the current through the *p*FET selector decreases with proton fluence, as a result of the buildup of radiation-induced charge and the corresponding negative V_{th} shift [11],[14]. This leads to the overall decrease in read-out current of the BD-PUF in Fig. 4(a).

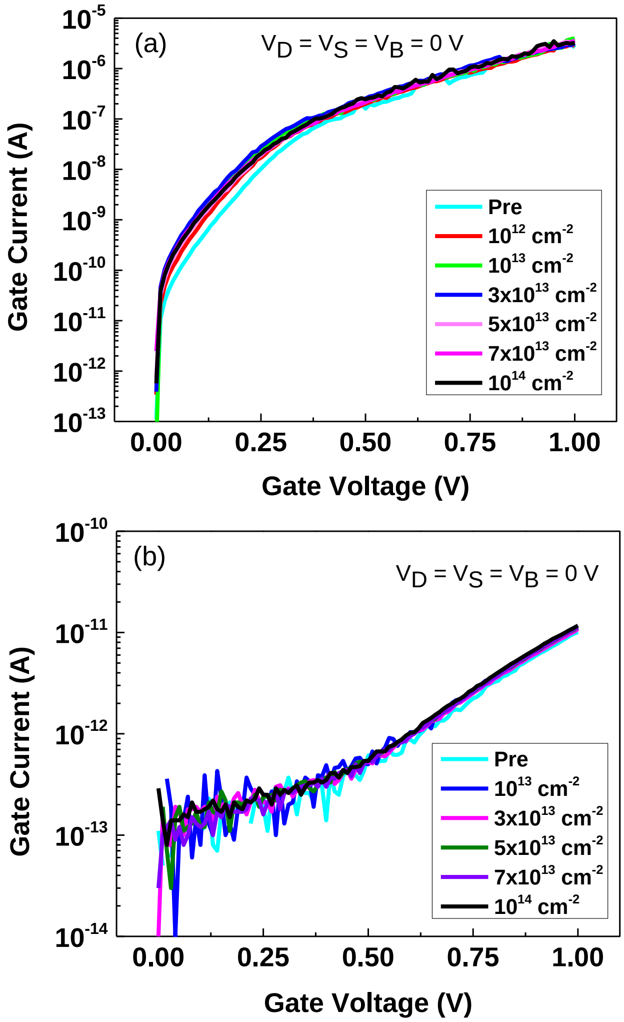

Fig. 8. $I_G - V_G$ curves for (a) the *broken n*FET, and (b) the *unbroken n*FET as a function of fluence.

To understand the increase in the $\overline{BL}$ current in Fig. 4(b), we must consider the parallel combination of the broken and unbroken *n*FETs in Fig. 9. While the majority of current still flows through the broken *n*FET, an increasing amount of leakage is observed in Fig. 7(b) after proton irradiation through the *unbroken n*FET, which shares a common body junction with the *broken n*FET. This leakage is independent of gate voltage, and due most likely to proton-induced displacement damage and interface traps at the body to *S/D* junctions [10]. The strong correlation of the $\overline{BL}$ current in Fig. 4(b) and the increased off-state leakage of the *unbroken n*FET therefore suggests that a small percentage (~ 0.1 to 1% in this case) of the total current flows through the body-to-*S/D* contacts of the unbroken *n*FET at the highest observed proton fluence. While this does not significantly affect the measured read-out current of the BD-PUF in Fig. 4(a), it does account for the increased $\overline{BL}$ current in Fig. 4(b).

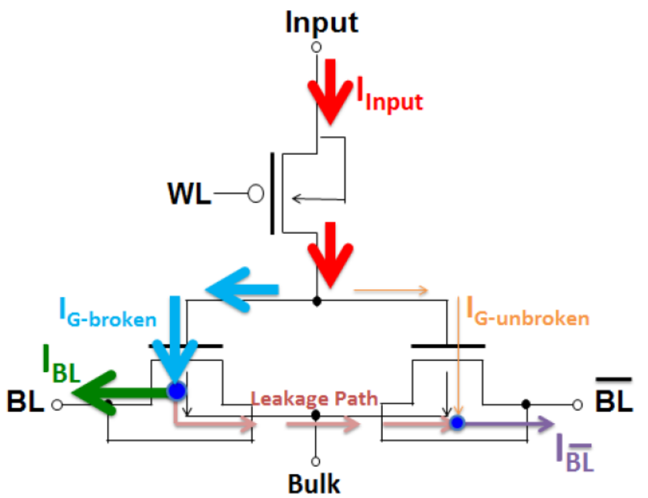

Fig. 9. Current in the BD-PUF after its forming step and proton irradiation. Current from the *Input* flows through the *p*FET selector, and then through the parallel combination of the broken and unbroken *n*FETs. The resistance of the broken *n*FET is much lower than that of the unbroken *n*FET, so before and after proton irradiation, nearly all of the current flows through the broken *n*FET. While the majority of current still flows through the broken *n*FET after proton irradiation, an increasing amount of leakage current flows through the *unbroken n*FET, which shares a common body junction with the *broken n*FET.

Finally, Fig. 10 shows the I_D-V_D characteristics of the selector and the I_G-V_G curve (load line) of the *broken n*FET as a function of proton fluence. The gate voltage of the *broken n*FET is equal to the drain voltage of the *p*FET selector in the BD-PUF. The cross points shown in Fig. 10 are operating points of the BD-PUF in typical circuit operation. The voltage drop across the *p*FET selector increases as the fluence becomes larger, and the maximum voltage drop is 0.11 V at a fluence of 10^{14} cm^{-2}, leading to the observed drop in read-out current of the BD-PUF.

Whether the observed reduction in value of the observed memory ratio will inhibit its operation in an application of interest depends not only on the fluence, but also on the sensitivity of the readout circuitry and the ambient conditions (temperature, noisiness, etc.). Because the non-ionizing energy loss of 1.8-MeV protons is much higher than that of the higher-energy protons that typically result in the degradation in space systems [15],[16], the equivalent displacement damage doses in this study are quite high compared with most realistic space environments [10]. For example, a 10 year mission with circular orbit around the earth at an altitude of 7000 km and a shielding of 100 mils Al would experience an equivalent 1.8 MeV proton fluence of ~7 x 10^{11} cm^{-2} [10], [15]-[19]. Thus, these types of BD-PUFs may well exhibit excellent radiation tolerance in most space environments of interest.

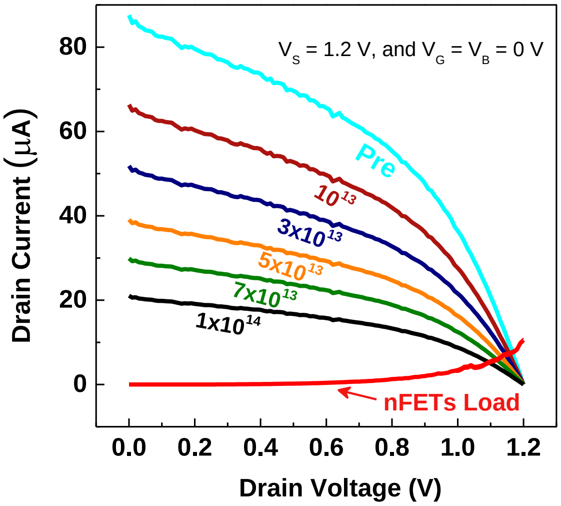

Fig. 10. The I_D-V_D curves of the *p*FET selector and the *n*FETs load line as a function of fluence.

V. Conclusions

The radiation response of a BD-PUF has been evaluated. The BD-PUF works well in X-ray irradiation environments. The characteristics of the BD-PUF show significant degradation at high fluence proton irradiation, attributed primarily to a threshold voltage shift of the *p*FET selector, thereby reducing the memory ratio. This mechanism was also confirmed by annealing experiments. These BD-PUFs likely will perform well in typical low-fluence space environments, but their suitability for high-fluence environments must be evaluated carefully, relative to system requirements.

References

[1] R. Maes, “Physically unclonable functions: Construction, properties and applications,” Ph.D. dissertation, Dept. Elect. Eng., Katholieke Universiteit Leuven, Leuven, Belgium, Aug. 2012.
[2] 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*, pp. 406-408, 2007.
[3] K. Lofstrom, W. R. Daasch, and D. Taylor, “IC identification circuit using device mismatch,” in *Proc. IEEE Int. Solid-State Circuits Conf*, pp. 372-373, 2000.
[4] N. Liu, S. Hanson, D. Sylvester, and D. Blaauw, “OxID: On-chip one-time random ID generation using oxide breakdown,” in *Proc. IEEE VLSI Circuits Symp*., pp. 231–232, Jun. 2010.
[5] J. W. Lee, D. Lim, B. Gassend, et al., “A technique to build a secret key in integrated circuits for identification and authentication applications,” in *Proc. IEEE VLSI Circuits Symp*., pp. 176–179, Jun. 2004.
[6] K. H. Chuang, E. Bury, R. Degraeve, et al., “Physically unclonable function using CMOS breakdown position,” in *Proc. IEEE Int. Reliab. Phys. Symp.*, pp. 4C1.1-6, 2017.
[7] P. Y. Chen, R. Fang, R. Liu, et al., “Exploiting resistive cross-point array for compact design of physical unclonable function,” in *Proc. IEEE Int. Symp. Hardw.-Oriented Security Trust*, pp. 26–31, May 2015.
[8] B. Kaczer, R. Degraeve, M. Rasras, et al., “Impact of MOSFET gate oxide breakdown on digital circuit operation and reliability,” *IEEE Trans. Electron Devices*, vol. 49, no. 3, pp. 500-506, Mar. 2002.
[9] R. Degraeve, G. Groeseneken, R. Bellens, et al., “New insights in the relation between electron trap generation and the statistical properties of oxide breakdown,” *IEEE Trans. Electron Devices,* vol. 45, no. 4, pp. 904–911, Apr. 1998.
[10] M. Caussanel, A. Canals, S. K. Dixit, M. J. Beck, A. D. Touboul, R. D. Schrimpf, D. M. Fleetwood, and S. T. Pantelides, “Doping-type dependence of damage in silicon diodes exposed to X-ray, proton, and He+ irradiations,” *IEEE Trans. Nucl. Sci*., vol. 54, no. 6, pp. 1925-1930 Dec. 2007.
[11] D. M. Fleetwood, “Total ionizing dose effects in MOS and low-dose-rate sensitive linear-bipolar devices,” *IEEE Trans. Nucl. Sci.*, vol. 60, no. 3, pp. 1706–1730, Jun. 2013.
[12] F. W. Sexton, D. M. Fleetwood, M. R. Shaneyfelt, et al., “Precursor ion damage and angular dependence of single event gate rupture in thin oxides,” *IEEE Trans. Nucl. Sci*., vol. 45, no. 6, pp. 2509-2518, Dec. 1998.
[13] M. Ceschia, A. Paccagnella, M. Turrini, et al., “Heavy ion irradiation of thin gate oxides,” *IEEE Trans. Nucl. Sci.*, vol. 47, no. 6, pp. 2648-2655, Dec. 2000.
[14] P. Paillet, J. Schwank, M. Shaneyfelt, V. Ferlet-Cavrois, R. Jones, O. Flarrient, and E. Blackmore, “Comparison of charge yield in MOS devices for different radiation sources,” *IEEE Trans. Nucl. Sci.*, vol. 49, no. 6, pp. 2656–2661, Dec. 2002.
[15] G. P. Summers, E. A. Burke, P. Shapiro, and S. R. Messenger, “Damage correlations in semiconductors exposed to gamma, electron, and proton irradiations,” *IEEE Trans. Nucl. Sci.*, vol. 40, no. 6, pp. 1372-1379. Dec. 1993.
[16] M. A. Xapsos, P. M. O’Neill, and T. P. O’Brien, “Near-Earth space radiation models,” *IEEE Trans. Nucl. Sci.*, vol. 60, no. 3, pp. 1691-1705, Jun. 2014.
[17] E. G. Stassinopoulos and J. P. Raymond, “The space radiation environment for electronics,” in *Proc. IEEE*, vol. 76, no. 11, pp. 1423–1442, Nov. 1988.
[18] G. P. Ginet, S. L. Huston, C. J. Roth, T. P. O’Brien, and T. B. Guild, “The trapped proton environment in medium earth orbit (MEO),” *IEEE Trans. Nucl. Sci.*, vol. 57, no. 6, pp. 3135-3142, Dec. 2010.
[19] www.spenvis.oma.be.