Sensors and Materials, Vol. 31, No. 5 (2019) 1375–1386
MYU Tokyo

S & M 1864

Secure Circuit with Low-power On-chip Temperature Sensor for Detection of Temperature Fault Injection Attacks

Hyungseup Kim,[1] Byeoncheol Lee,[1] Jaesung Kim,[1] Kwonsang Han,[1]
Hyoungho Ko,[1] Dong Kyue Kim,[2] Byong-Deok Choi,[2] and Ji-Hoon Kim[3*]

[1]Department of Electronics Engineering, Chungnam National University,
Daejeon 34134, Republic of Korea
[2]Department of Electronic Engineering, Hanyang University,
Seoul 04763, Republic of Korea
[3]Department of Electronic and Electrical Engineering, Ewha Womans University,
Seoul 03760, Republic of Korea

(Received April 13, 2018; accepted March 13, 2019)

Keywords: secure circuit, hardware security, physical attack protection, fault injection attacks, temperature fault injection attacks

In this paper, we present a secure circuit with a low-power on-chip temperature sensor for the detection of temperature fault injection attacks. Such attacks stress an electronic circuit by heating it beyond the allowed operation temperature range, inducing random modifications of the data in the memory cell or limiting the function of the target device. The objective of the proposed secure circuit with an on-chip temperature sensor is to detect temperature-based fault injection attacks and protect the secure contents of the target device. The proposed secure circuit detects and allows the shutdown of the protected circuit when the temperature is below −10 °C or above 80 °C. The protected circuit operates normally in the operation temperature range from −10 to 80 °C and can be shut down by the control block of the secure circuit outside of this operation temperature range. The proposed secure circuit has a simple structure and a small active area, and consists of a low-power temperature sensor, two comparators, and an XOR gate. It is fabricated using a standard 0.18 μm complementary metal-oxide-semiconductor (CMOS) process with a small active area of 0.04 mm^2 and consuming 19.72 μW with a 1.8 V power supply.

1. Introduction

Recently, hardware-level physical security has been highly required, as secure data exchange via various communication networks and devices, such as a wireless sensor network, is increased.[1,2] Physical attacks are threats to the integrated circuits (ICs) implemented in electronic devices containing the secure information of the user, such as smartcards and smartphones. They can be classified into two categories: invasive and noninvasive attacks. Invasive attacks can be defined as attacks causing the physical modification and deformation of the attacked chip, such as reverse engineering, focused ion beam (FIB) chip editing, and

*Corresponding author: e-mail: jihoonkim@ewha.ac.kr
https://doi.org/10.18494/SAM.2019.2258

ISSN 0914-4935

microprobing attacks. Noninvasive attacks are attacks that do not physically damage the attacked chip, such as side channel and fault injection attacks. Noninvasive attacks can be initiated by several methods such as timing attacks, power analysis, electromagnetic analysis (EMA), glitch attacks, and operation temperature change. Fault injection attacks are highly dangerous because of their effectiveness and low cost. They are a threat to data security as they can extract the secure information stored in the target device. Fault injection attacks can be made to occur by several approaches such as clock glitching, voltage glitching, overclocking, electromagnetic (EM) pulses, and temperature.[3] A temperature fault injection attack changes the environment temperature of the attacked chip, causing it to operate outside of the allowed operating temperature range, and extracts the secure information stored. Various studies of temperature attacks have been presented.[4–13] Temperature attacks can be of two types: low- and high-temperature attacks. Low-temperature attacks are initiated by cooling the attacked chip and extracting the data under a freezing condition.[4–7] In previous works, a static random access memory (SRAM) was cooled below −50 °C to freeze the data, but its data could be recovered after a power outage.[4,5] High-temperature attacks are caused by heating the attacked chip, generating errors in the function of the target under the heated condition.[8–10] A fault injection with a 71.4% probability of causing memory errors was reported to be achieved by heating an IBM JVM up to 100 °C.[10] As shown in previous research, temperature fault injection attacks can result in severe problems in hardware security.

In this paper, a secure circuit with a low-power on-chip temperature sensor is presented for the detection of temperature fault injection attacks. The objective of the proposed secure circuit with the on-chip temperature sensor is to detect the temperature-based fault injection attacks and protect the secure contents of the target device. The proposed secure circuit detects and allows the shutdown of the protected circuit when the temperature is below −10 °C or above 80 °C. The protected circuit operates normally in the operation temperature range from −10 to 80 °C and can be shut down by the control block of the secure circuit outside of this operating temperature range. The proposed secure circuit has a simple structure and a small active area, and consists of a low-power temperature sensor, two comparators, and an XOR gate. The low-power temperature sensor generates two complementary to the absolute temperature (CTAT) characteristic voltages for comparison with the reference voltage through each of the two comparators. The XOR gate is implemented to detect and shut down the protected circuit when the temperature is below −10 °C or above 80 °C by using the two comparator output signals.

2. Circuit Implementation

2.1 Description of proposed secure circuit

The concept description of the proposed temperature detection secure circuit is shown in Fig. 1. It presents the operation of the proposed secure circuit when a temperature fault injection attack affects a chip. When a temperature fault injection attack is initiated to extract the secure data from the attacked chip, the fully integrated on-chip secure circuit detects the temperature of the attacking environment. Following this, the detected result is transmitted to

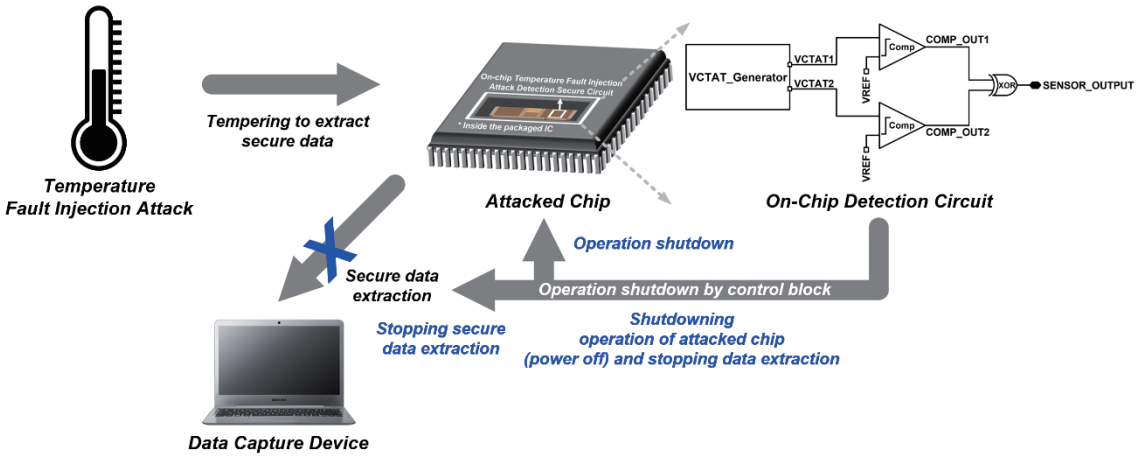


Fig. 1. (Color online) Concept description of the proposed secure circuit.

the control block of the secure system on-chip (SoC) platform. The on-chip secure detection circuit selects a specific temperature range and detects whether the outside temperature is in the normal operation range. On the basis of the detection result transmitted by the secure circuit, the detection block determines whether the chip is attacked. When the control block assesses a nonattacking condition, the secured chip continues to operate its normal function. When the control block confirms an attacking condition, the operation of the attacked chip and power are shut down. By shutting down the operation of the attacked chip, the secure data is protected and prevented from being extracted by the temperature fault injection attack. The proposed temperature detection secure circuit is one of the functional blocks forming the secure SoC platform. In this paper, we focus on the secure detection circuit for detecting temperature fault injection attacks. The control block is in the main secure SoC core, which will not be discussed in this paper.

2.2 Proposed secure circuit with on-chip temperature sensor

The schematic of the proposed secure circuit is shown in Fig. 2. This circuit with the low-power on-chip temperature sensor consists of a CTAT voltage generator, two comparators, an XOR gate, and two monitoring buffers. The CTAT voltage generator generates two CTAT characteristic voltages, *VCTAT*1 and *VCTAT*2. Both *VCTAT*1 and *VCTAT*2 are monitored by buffered output VCTAT1_MON and VCTAT2_MON signals. The generated *VCTAT*1 and *VCTAT*2 voltages are compared with the reference voltage (V_{REF}) by each comparator. The COMP_OUT1 signal of the first comparator detects the low-temperature range below −10 °C, whereas the COMP_OUT2 signal of the second comparator detects the high-temperature range above 80 °C. The outputs of both the comparators COMP_OUT1 and COMP_OUT2 are summed by the XOR gate. The output signal of the XOR gate, SENSOR_OUTPUT, is indicative of the detected temperature. When the output detection signal of the XOR gate is

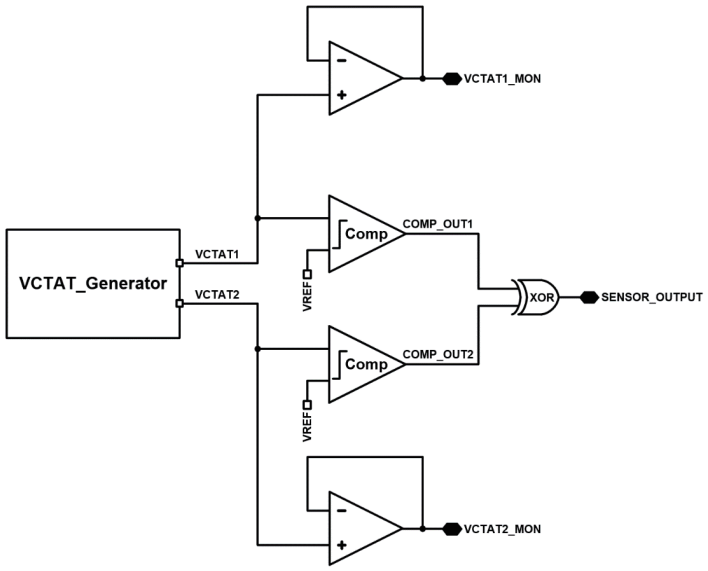


Fig. 2. Schematic of the proposed secure circuit with a temperature sensor.

high, the chip operates under a normal condition and is not prone to any temperature fault injection attack. The proposed secure circuit allows the protected chip to operate over a specific temperature range from −10 to 80 °C. When the output detection signal of the XOR gate is low, the chip operates under an attacked condition and is prone to temperature fault injection attacks. The detected attacked temperature range by the secure circuit is below −10 °C and above 80 °C. The proposed secure circuit detects the specific temperature and transmits the output detection signal to the control block in the main secure SoC core, which blocks the secure data from being extracted by the attacker by shutting down the operation of the protected chip.

The schematic of the comparator of the secure circuit is shown in Fig. 3. The proposed secure circuit is aimed to detect the temperature attacks. The complexity of the circuit increases the malfunction probability of the circuit during a severe temperature attack. Therefore, the secure circuit should have a simple scheme. Such a scheme as a latched comparator with additional clock signals requires an additional clock generator circuit that increases the circuit complexity. In severe temperature attack environments, the clock signal may be distorted and could lead to malfunction. The hysteresis comparator scheme is less sensitive to temperature than the latched comparator scheme. The comparator is implemented with a hysteresis comparator with a self-biased scheme without additional bias circuits and clock generators. The current consumption of the comparator is 1.36 μA at 1.8 V power supply.

The CTAT voltage generator is illustrated Fig. 4. It is based on a conventional beta-multiplier current reference circuit. It consists of a start-up circuit, a beta-multiplier current reference circuit, current mirrors, polysilicon resistors, and pseudo-resistors. The beta-multiplier current reference generates current I_1, which is the reference current (I_{REF}). This generated current is

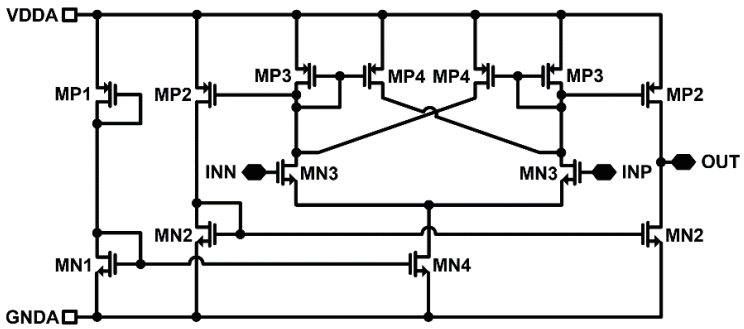


Fig. 3. Schematic of the comparator of the secure circuit.

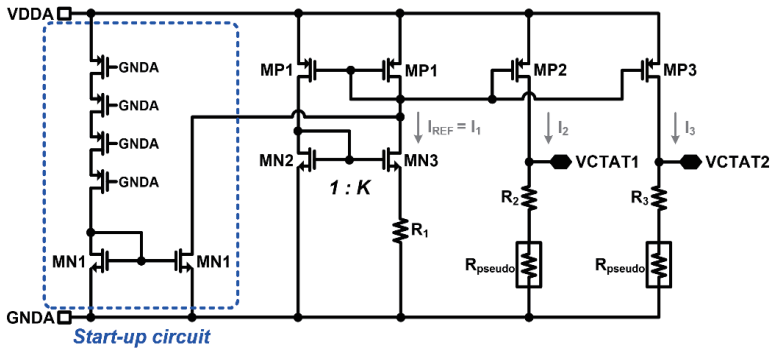


Fig. 4. (Color online) Schematic of the CTAT voltage generator.

proportional to the absolute temperature (PTAT). The generated PTAT current of the beta-multiplier current reference can be expressed as

$$I_{REF} \approx \frac{n \cdot \ln(K) \cdot U_T}{R_1}, \tag{1}$$

where n is the slope factor, K is the multiplier ratio of the n-channel metal-oxide-semiconductor (NMOS) device, U_T is the thermodynamic voltage, and R_1 is the reference resistance of the beta-multiplier current reference.[14] The generated I_{REF} is copied to I_2 and I_3 by the diode-connected current mirrors MP2 and MP3. The CTAT voltages $VCTAT1$ and $VCTAT2$ are generated by the copied current and resistors. The temperature-dependent voltage change does not require a specific value and only needs to be detected when the temperature is below −10 °C and above 80 °C. Therefore, the circuit design was carried out by setting the appropriate value through simulating the voltage change according to the temperature. The current consumption of the CTAT generator is 5.4 μA at 1.8 V power supply. The simulation result of the pseudo-resistor with temperature is exhibited in Fig. 5. It shows that the temperature increase corresponds to

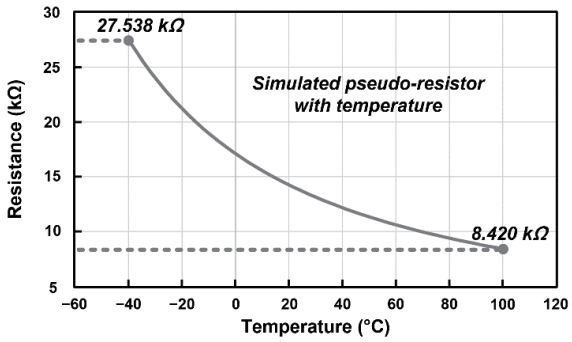


Fig. 5. Simulation result of the pseudo-resistor with temperature.

a decrease in the resistance of the designed pseudo-resistor. The resistance of the polysilicon resistors also decreases with the increase in temperature.[15] Therefore, even if the reference current generated by the beta-multiplier current reference has a PTAT characteristic, the polysilicon resistors and designed pseudo-resistors have a higher factor corresponding to the resistance decrement with temperature. This enables the generation of the CTAT characteristic voltages *VCTAT*1 and *VCTAT*2. The generated *VCTAT*1 and *VCTAT*2 can be expressed as

$$VCTAT1 = I_2 \cdot (R_2 + R_{pseudo}), \tag{2}$$

$$VCTAT2 = I_3 \cdot (R_3 + R_{pseudo}). \tag{3}$$

The monitoring buffer is implemented using a self-biased inverter-based amplifier. The self-biased inverter-based amplifier scheme is implemented to not use an additional bias block. The phase margin of the buffer is 69.29° with 6.38 MHz bandwidth. The current consumption of the monitoring buffer is 1.42 μA at 1.8 V power supply.

2.3 Simulation results

The simulation results of the proposed secure circuit consisting of an on-chip temperature sensor are shown in Fig. 6. The simulation results of *VCTAT*1 and *VCTAT*2 with temperature are exhibited in Fig. 6(a). They reveal that the generated *VCTAT*1 and *VCTAT*2 have different voltages and slopes with temperature for temperature detection over the temperature range. The simulation results of each comparator output are displayed in Fig. 6(b), showing the possibility of detecting the temperature. The generated *VCTAT*1 detects the lower range of temperature, i.e., below −10 ℃, by the first comparator by comparison with the VREF. The first comparator outputs a high signal in this temperature range but a low signal when the temperature is above −10 ℃. In addition, *VCTAT*2 detects a high temperature range above 80 ℃ by the second comparator by comparison with the V_{REF}. The second comparator outputs a high signal when

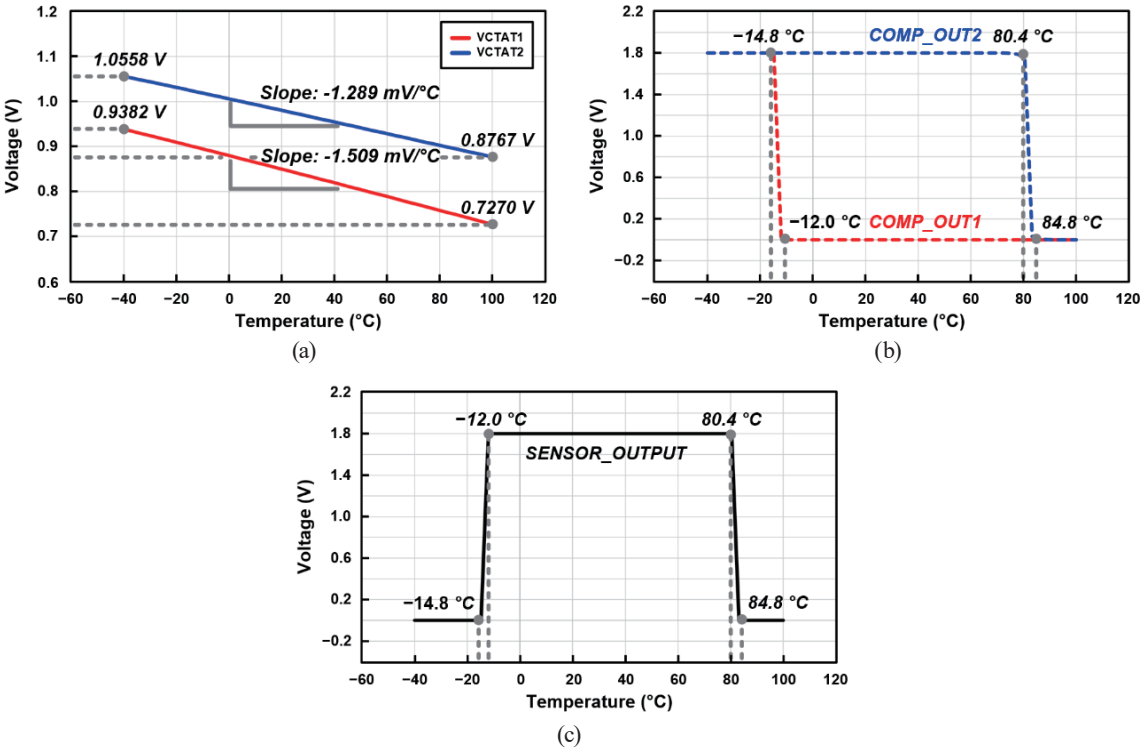


Fig. 6. (Color online) Simulation results of the proposed secure circuit with on-chip temperature sensor.

the temperature is below 80 °C and a low signal when the temperature is above 80 °C. The outputs of the two comparators COMP_OUT1 and COMP_OUT2 are used for detecting the outside temperature. The output simulation result of the proposed secure circuit is shown in Fig. 6(c). The outputs of both the comparators COMP_OUT1 and COMP_OUT2 are transferred to the XOR gate that outputs SENSOR_OUTPUT signal, which is exclusive-or of COMP_OUT1 and COMP_OUT2. The detection output SENSOR_OUTPUT detects whether the temperature is in the normal operation range from −10 to 80 °C. When the outside temperature is out of the normal operation range, the secure circuit detects an abnormal temperature and transmits the detected signal to the main secure SoC core to shut down the attacked chip and block the secure data from being extracted.

3. Measurement Results

3.1 Prototype IC implementation

The prototype IC of the proposed secure circuit was fabricated with a standard 0.18 μm complementary metal-oxide-semiconductor (CMOS) process with a small active area of 0.04 mm2. The die photograph is shown in Fig. 7. The total power consumption is 19.72 μW with 1.8 V power supply.

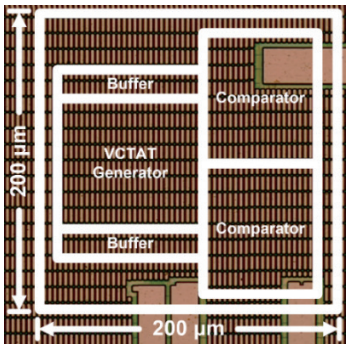


Fig. 7. (Color online) Die photograph of the proposed secure circuit.

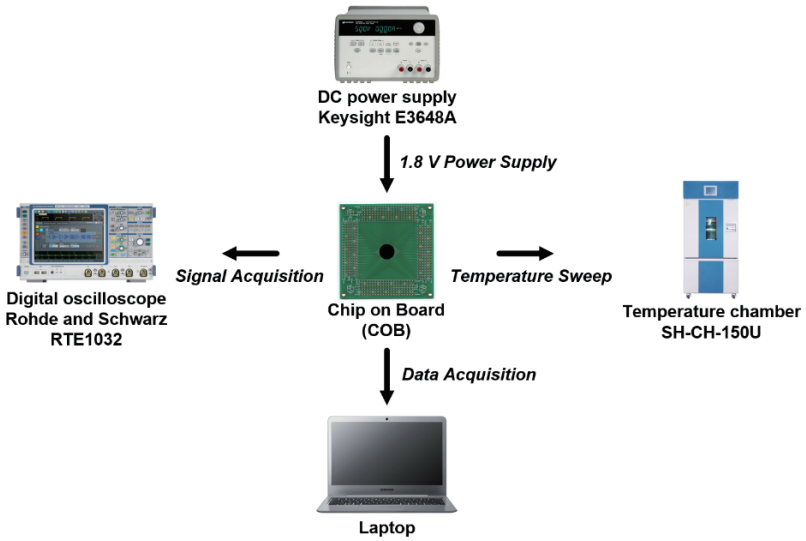


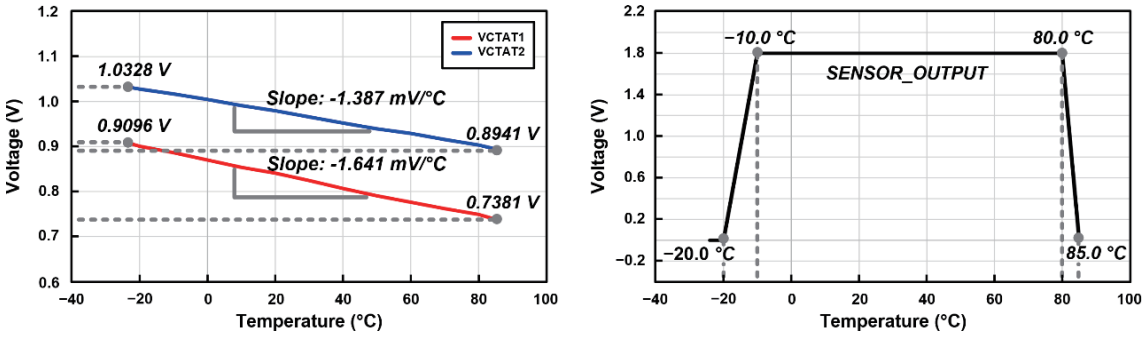
Fig. 8. (Color online) Measurement environment of the proposed secure circuit.

3.2 Measurement environment

The measurement environment of the prototype IC of the proposed secure circuit is shown in Fig. 8. The evaluation of the prototype IC proceeds with the implementation of the IC into the printed circuit board (PCB) by a chip-on-board (COB) process. The temperature detection is tested by sweeping the temperature by using a temperature chamber. The output signals are acquired by using a digital oscilloscope.

3.3 Measurement results

The measurement results of the prototype IC of the proposed secure circuit are shown in Fig. 9. The measured *VCTAT*1 and *VCTAT*2 with temperature are shown in Fig. 9(a). The



(a) (b)

Fig. 9. (Color online) Measurement results of the proposed secure circuit.

Table 1
Performance summary.

Specification	This work
Process (μm)	0.18
Supply voltage (V)	1.8
Power consumption (μW)	19.72
Temperature attack detection range	below −10 °C and above 80 °C
Active area (mm^2)	0.04

figure shows that the generated *VCTAT*1 and *VCTAT*2 results agree well with simulation results in Fig. 6(a). There are slight differences in voltage and slope as revealed by comparing the measurement and simulation results, but the overall tendency confirms that the designed CTAT voltages are generated as intended. The output measurement results of the proposed secure circuit are presented in Fig. 9(b). The detection output SENSOR_OUTPUT detects whether the temperature is in the normal operation range from −10 to 80 °C. The measurement results indicate that the prototype IC detects the temperature range below −10 °C and above 80 °C as low signals, which is the attacking temperature range. The measurement results of the detection output SENSOR_OUTPUT show that the proposed secure circuit performs the functions as designed. A slight error in the temperature range is noted by comparing the measurement and simulation results because of the process variation; however, it is verified that the overall tendency and operation are identical to those of the designed circuit as intended. The performance summary of the secure circuit is presented Table 1.

4. Conclusions

In this paper, a secure circuit with a low-power on-chip temperature sensor for the detection of temperature fault injection attacks is presented. The proposed secure circuit detects and allows the protected circuit to shut down when the temperature is below −10 °C and above 80 °C. The protected circuit operates normally in the operation temperature range from −10 to 80

℃ and can be shut down by the control block of the secure circuit outside of this temperature range. The proposed scheme has the advantages of being simple without additional complex circuitry, having a small active area, and the ability to detect a temperature range below −10 ℃ and above 80 ℃ for protecting secure data from temperature-based attacks. The prototype IC is fabricated using a standard 0.18 μm CMOS process with a simple structure, a small active area of 0.04 mm^2, and a consumption of 19.72 μW using a 1.8 V power supply including monitoring buffers.

Acknowledgments

This work was supported by the Samsung Research Funding Center of Samsung Electronics under Project Number SRFC-IT1601-01. The chip fabrication and EDA tool were supported by the IC Design Education Center (IDEC), Republic of Korea.

References

1 U. Umar, M. U. H. Al Rasyid, and S. Sukaridhoto: Int. J. Eng. Technol. Innovation **8** (2018) 157.
2 A. Sudarsono, S. Huda, N. Fahmi, M. U. H. Al-Rasyid, and P. Kristalina: Int. J. Eng. Technol. Innovation **6** (2016) 103.
3 N. Sklavos, R. Chaves, G. D. Natale, and F. Regazzoni: Hardware Security and Trust, N. Sklavos, R. Chaves, G. D. Natale, and F. Regazzoni, Eds. (Springer International Publishing, Switzerland, 2017) Chap. 2.
4 S. Skorobogatov: Technical Report, University of Cambridge Computer Laboratory No. UCAM-CL-TR-536 (2002).
5 D. Samyde, S. P. Skorobogatov, R. J. Anderson, and J.-J. Quisquater: IEEE Security in Storage Workshop 2002 (SISW02) (IEEE, 2002) 65
6 T. Muller and M. Spreitzenbarth: 11th Int. Conf. Applied Cryptography and Network Security (ACNS) (Springer, 2013) 373.
7 J. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten: 17th USENIX Security Symp. (USENIX, 2008) 45.
8 M. Hutter and J. M. Schmidt: 12th Int. Conf. Smart Card Research and Advanced Applications (Springer, 2013) 219.
9 J. J. Quisquater and D. Samyde: Proc. 3rd Int. Conf. Research in Smart Cards (E-Smart'02, 2002) 185.
10 S. Govindavajhala and A. W. Appel: Proc. IEEE Symp. Security and Privacy (2003) 154.
11 R. Kumar, P. Jovanovic, and I. Polian: 2014 IEEE 20th Int. On-Line Testing Symp. (IOLTS) (IEEE, 2014) 43.
12 H. Martin, T. Korak, E. S. Millan and M. Hutter: IEEE Trans. Inf. Forensics Secur. **10** (2015) 266.
13 E. Tena-Sanchez and A. J. Acosta: 2018 28th Int. Symp. Power and Timing Modeling, Optimization and Simulation (PATMOS, 2018) 163.
14 D. Djekic, G. Fantner, J. Behrends, K. Lips, M. Ortmanns, and J. Adners: 43rd IEEE European Solid State Circuits Conf. (ESSCIRC) (IEEE, 2017) 79.
15 Z. Tan, S. H. Shalmany, G. C. M. Meijer, and M. A. P. Pertijs: IEEE Trans. Electron Devices **50** (2003) 1413.

About the Authors

Hyungseup Kim received his B.S. degree in Electronics Engineering from Chungnam National University, Daejeon, Republic of Korea, in 2014, where he is currently pursuing his Ph.D. degree. His current research interests are in the design of sensor interface circuits, biosignal acquisition circuits, secure integrated circuits, data converters, and mixed-mode integrated circuits.

Byeoncheol Lee received his B.S. degree in Electronics Engineering from Chungnam National University, Daejeon, Republic of Korea, in 2017, where he is currently pursuing his M.S. degree. His current research interests are in the design of CMOS analog and mixed-mode integrated circuits.

Jaseung Kim received his B.S. degree in Electronics Engineering from Chungnam National University, Daejeon, Republic of Korea, in 2018, where he is currently pursuing his M.S. degree. His current research interests are in the design of CMOS analog and mixed-mode integrated circuits.

Kwonsang Han received his B.S. degree in Electronics Engineering from Chungnam National University, Daejeon, Republic of Korea, in 2018, where he is currently pursuing his M.S. degree. His current research interests are in the design of CMOS analog and mixed-mode integrated circuits.

Hyoungho Ko received his B.S. and Ph.D. degrees in Electrical Engineering from Seoul National University, Republic of Korea, in 2003 and 2008, respectively. From 2008 to 2010, he worked with Samsung Electronics as a senior engineer. In 2010, he joined the Department of Electronics Engineering at Chungnam National University, Republic of Korea, where he is currently an associate professor. His current research interests are in the design of CMOS analog integrated circuits.

Dong Kyue Kim received his B.S., M.S., and Ph.D. degrees in Computer Engineering from Seoul National University in 1992, 1994, and 1999, respectively. From 1999 to 2005, he was an assistant professor in the Division of Computer Science and Engineering at Pusan National University. He is currently a full professor in the Department of Electronic Engineering at Hanyang University, Republic of Korea. His research interests are in the areas of system on chip (SoC) security, crypto-coprocessors, and information security.

Byong-Deok Choi received his B.S., M.S., and Ph.D. degrees in Electronics Engineering from Hanyang University, Seoul, Republic of Korea, in 1994, 1996, and 2002, respectively. Since 2005, he has been with Hanyang University, where he is currently a professor in the Department of Electronic Engineering. His current research interests include driving methods and circuits for flat panel displays, low-power circuit and analog circuit design, and power IC design.

Ji-Hoon Kim received his B.S. (summa cum laude) and Ph.D. degrees in Electrical Engineering and Computer Science from KAIST, Daejeon, Republic of Korea, in 2004 and 2009, respectively. In 2009, he joined Samsung Electronics. In 2018, he joined the faculty of the Department of Electronic and Electrical Engineering, Ewha Womans University, where he is currently an associate professor. His current interests include CPU/DSP, communication modem, and low-power SoC design for security/biomedical systems. Dr. Kim is a technical committee member of the circuits and systems for communications and VLSI systems and applications in the IEEE Circuits and Systems Society. He was a recipient of the best design award at DongbuHiTek IP Design Contest in 2007 and the first place award at the International SoC Design Conference Chip Design Contest in 2008.