An Efficient Technique to Protect AES Secret Key from Scan Test Channel Attacks

Jaehoon Song*, Taejin Jung, Jihun Jung***, and Sungju Park*****

Abstract—**Scan techniques are almost mandatorily adopted in designing current System-on-a-Chip (SoC) to enhance testability, but inadvertently secret keys can be stolen through the scan test channels of crypto SoCs. An efficient scan design technique is proposed in this paper to protect the secret key of an Advanced Encryption Standard (AES) core embedded in an SoC. A new instruction is added to IEEE 1149.1 boundary scan to use a fake key instead of user key, in which the fake key is chosen with meticulous care to improve the testability as well. Our approach can be implemented as user defined logic with conventional boundary scan design, hence no modification is necessary to any crypto IP core. Conformance to the IEEE 1149.1 standards is completely preserved while yielding better performance of area, power, and fault coverage with highly robust protection of the secret user key.**

Index Terms—**AES, key protection, scan design, IEEE 1149.1 boundary scan design, SoC**

Manuscript received Nov. 21, 2011; revised Jan. 9, 2012.
* TranSono Inc., Korea
** LG Electronics INC., Seoul, Korea
*** Computer Science and Engineering Department, Hanyang University, Ansan Korea
S. Park (parksj@mslab.hanyang.ac.kr) is a corresponding author.

Earlier version of this paper has been presented at the poster section in the International Test Conference 2008.

I. INTRODUCTION

Advanced Encryption Standard (AES) algorithm is widely adopted to secure data transfers among mobile products as well as high-end servers. The AES is especially implemented as an IP core embedded into an SoC for internet servers or smart cards [1, 2]. The leak of the secret user key from the system including AES core may result in great economical loss or social problem, thus it is imperative to protect the user key from any attack.

Scan designs are well known testable design techniques used not only to improve fault coverage but also to save test cost in production testing of SoCs [3]. By adopting scan based design, internal signals of an SoC can be controlled and observed to diagnose as well as detect any defect [4, 5]. Therefore scan test becomes a mandatory process to find faulty chips before shipping the chips to customers. In scan designed SoC including AES core, secret user key can be observed through the scan chains [6-12], hence a key protection mechanism must also be considered in adopting the scan technique. Several works have been proposed to protect the secret key from scan channel attacks. Scan chain structures are changed by scrambling the order of the flip-flops, inserting inverters, or modifying scan registers [9, 11, 12]. Instead of modifying scan structures, secure and insecure modes are provided to allow scan test mode through IEEE 1149.1 (JTAG) boundary scan controller [10, 13]. To achieve better productivity SoC designers are forced to reuse design modules from external sources of IP of which security is not well verified. To prevent the security failure in one module from being cascaded through test subsystems of chips, security enhanced test

access mechanisms are addressed to escape from the threat posed by untrustworthy cores [14, 15]. A protection scheme is proposed for serial JTAG channels which are prone to be downgraded by any threat of a malicious chip in a JTAG chain [16].

JTAG based secured scan design technique is proposed in this paper. The contributions of this paper compared with other approaches: This technique preserves compatibility with IEEE 1149.1 (JTAG) standards. No modification is needed to the AES core thus the AES IP can be reused in designing an SoC. The secret user key is completely protected. The circuit implementation requires less design penalties such as area overhead, power consumption, and fault coverage [9-11].

The paper is organized as follows. Section 2 gives a brief overview of current approaches on scan secured design. In Section 3, our secured scan design technique is described for an AES core. Experimental results are shown in Section 4 followed by the concluding remarks in Section 5.

II. PREVIOUS SCAN DESIGN TECHNIQUES TO PROTECT AES SECRET USER KEY

AES is a round-based, symmetric block cipher, standardized by National Institute of Standards and Technology (NIST) in 2001. Hardware implementations of the AES, taking advantage of requiring less memory space, are widely used in mobile applications as well as internet servers.

AES is defined for a block size of 128 bits and key lengths of 128, 192, and 256 bits; accordingly the number of rounds becomes 10, 12, and 14. As shown in Fig. 1, the process of AES encryption consists of initial pre-round and normal rounds determined by the length of the user key. Pre-round takes user secret key and plain text to be encrypted, and the outputs transformed with KeyXOR operator are fed to the normal rounds. Then SubByte, ShiftRow, MixColumn, and KeyXOR operations are sequentially performed to generate intermediately transformed data to be stored to the Register R at each round.

By adopting scan design the AES register R becomes a part of scan chain of which the values can be observable and controllable thus the secret user key can be retrieved

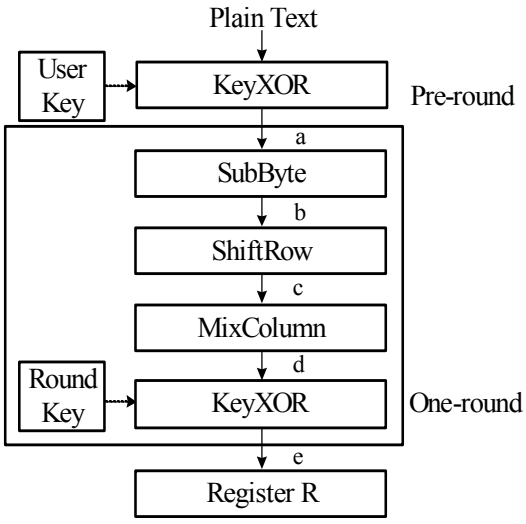

Fig. 1. Process of AES encryption.

in scan test mode [6-12].

M number of different matching keys of which the length is N have been defined to protect AES user key in scan test mode [9]. Only when the M matching keys are applied in predefined order the scan output ports are activated.

The matching keys are verified by comparing the output of scan flip-flops with the key matching block. However the increased number of scan fanout requires routing overhead with additional delay, and design reuse becomes difficult due to the modification on the AES core. More importantly any test engineer can use the pattern matching key values to activate the scan output ports to sniff the AES internal information.

In [10], AES core must pass through power-off operation whenever normal only secure mode is changed to insecure mode by adding a new state in JTAG standard Test Access Port (TAP) states. By resetting values remaining during the encryption process in normal mode, observation of the secret key through the scan port is prohibited. Mirror key register (MKR) is inserted to the AES core to avoid loading the user key during scan test mode. However, this technique is not compatible with JTAG standards, scan flip-flops have to be implemented with reset mode, and it is hard to reuse the predesigned AES core due to the MKR internally added.

Inverters are arbitrarily inserted to scan chains to protect keys, and the scan out data are further transformed through the S-box [11]. But, the S-box can also be regenerated by [17] if the structure of the S-box is

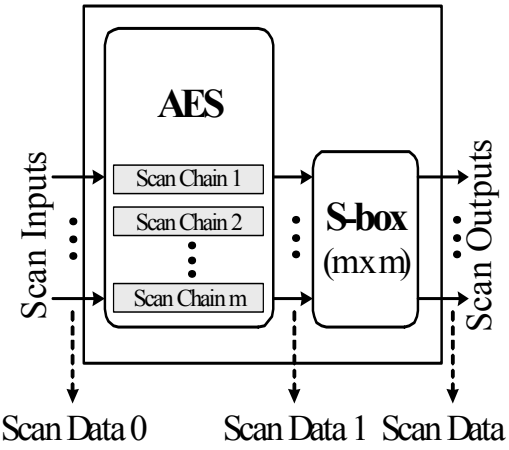

Fig. 2. Key Protection technique by using inverter and S-box.

exposed by the designer. As can be seen in Fig. 2, the scan data 1 can be retrieved from the scan data 2 through the S-box regenerated. Despite the sufficient number of inverters, their positions can still be identified by [10] in scan chains. Therefore if the structure of the S-box is exposed by the designer, this technique is not perfect for scan side channel attacks.

III. PROPOSED SECURED SCAN DESIGN

An efficient scan design technique is proposed in this paper to protect the secret key of an AES core embedded in an SoC. The focuses are given to preserve compatibility with JTAG standard, to reuse predesigned AES IP, and to completely protect the user key with less design penalties such as area, power, and testability. Whenever the normal mode is changed to scan test mode, an instruction newly added to JTAG standards is invoked. The data are encrypted with the Fake key instead of the user key by executing new instruction in scan test mode. Fig. 3 shows our secured scan design to protect AES secret user key from side channel attacks. No design change is needed to the internal logic of the AES core, thus any hard or soft AES IP can be reused in SoC design. Details of our technique are described in the following two subsections.

1. Fake Key Based Secure Scan Test Procedure

The procedures in applying our technique can be briefly summarized as follows.

(1) Invoke “SecureScanTest” instruction through JTAG boundary scan.

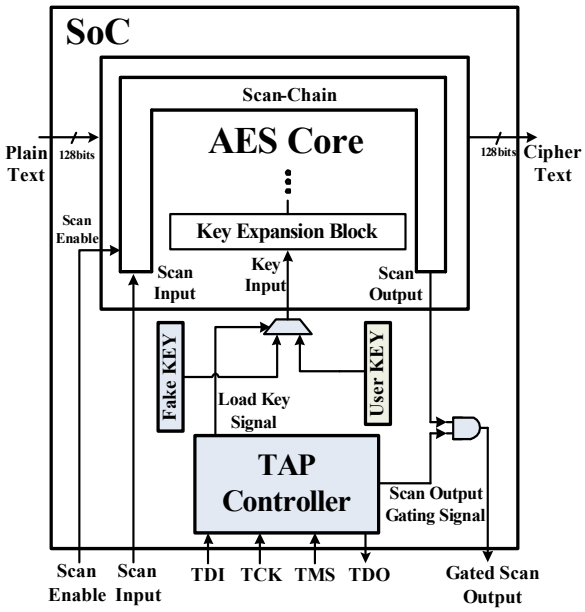

Fig. 3. Secured scan architecture by Fake Key insertion.

(2) By blocking scan output port, initially operate scan shift to flush out the scan chain possibly including encrypted data.

(3) In normal scan test mode, Fake key is loaded instead of user key with activating scan output port.

The data remaining in the internal registers becomes the target of attackers whenever normal mode is changed to another mode. An instruction named "SecureScanTest" newly added to JTAG standards is applied for scan testing. With the invocation of the instruction, initially the internal scan chains are shifted out to flush out the data without being observed by blocking scan output port. It is noted that in [10] secure mode is changed to insecure mode by power off the AES chip in which all the scan flip flops are assumed to have reset mode. Afterward the mode is changed to regular scan test mode with activating the scan output port, in which Fake key instead of the user key is loaded to the AES core as shown in Fig. 3. The Load Key signal from the instruction decoder is used to drive the Key values. The control block generating the Load Key and Scan Output Gating signals is shown in Fig. 4, where the counter initially activated tells the number of scan shifts to flush out the encrypted data. Internal structure of the AES core used in this paper is shown in Fig. 5 and the gate level logic simulation results are shown in Fig. 6. At time T13 when the

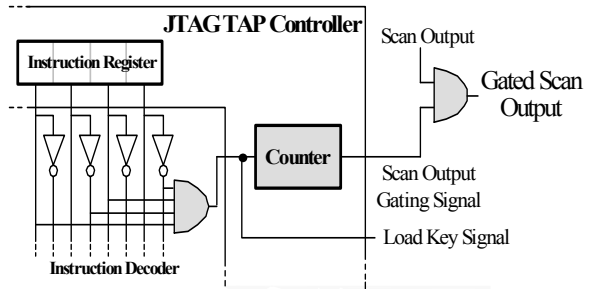

Fig. 4. Modified JTAG TAP Controller.

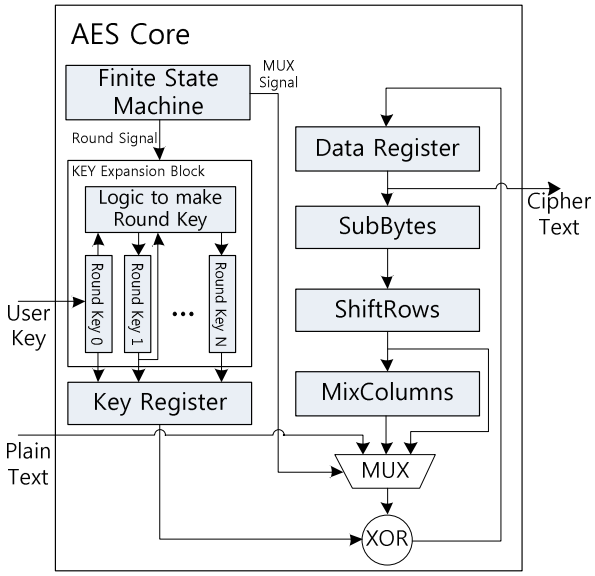

Fig. 5. AES core architecture.

"ScanSecure Test" instruction of which OPCODE is "0010" is loaded, the mode is changed to scan test mode by activating the SE signal. But until T78 no data is observed through the SO scan output port since the SO is deactivated during initial scan shifts to flush out internal data. Then from T79 normal scan operations are performed with activating the SO while the Fake key instead of the User key is inserted to the AES core. Different from the approach [10], our technique does not require the flip-flops to have reset mode, hence the area and power can also be saved.

2. Fake Key for Secure and Testabilitake Key for Secure and Testability

Meticulous care must be taken in determining the value of the Fake key not only to protect the secret key but also at least to give no harm to test coverage. Instead of inserting separate MKR register to the AES core [10], Fake key values are driven from the external logic of the AES core through the MUX controlled by the Load Key signal in Fig. 3. Since our technique does not require any change in the internal logic, it can be generically adopted to design any secured SoC. This fixed Fake key may lower the fault coverage, however it has been experimentally observed that by taking 100 different Fake key values even better fault coverage was able to be achieved than the User Key. Synopsys TetraMax automatic test pattern generation tool has been extensively used to check the fault coverage of the circuit embedding AES core with external Fake key, and it was found over 99.6% fault coverage was achievable.

IV. EXPERIMENTAL RESULTS

For 100 Fake keys of which values are randomly chosen, the fault coverages range from 99.85% to

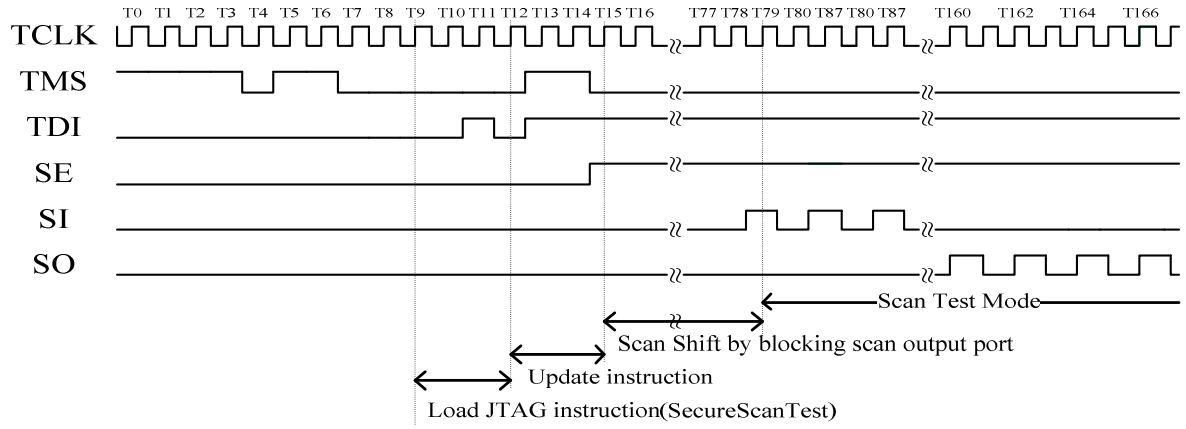

Fig. 6. Timing diagram for AES key application.

Table 1. Comparison of general technical aspects

	[9]	[10]	[11]	Prop.
Reusability of hard AES IP	N	N	N	Y
Compatibility with JTAG	Y	N	Y	Y
Direct applicability of ATPG	Y	Y	N	Y
Complete protection of AES user key	N	Y	N	Y

99.61%, and the Fake key with all 0 s provide the highest fault coverage. Therefore the design experiment was performed with this Fake key value of all 0s. The design includes AES core, JTAG TAP controller and additional control circuits with the Fake key. All cores are implemented with Magna 0.18 um process, and commercial power analysis and automatic test pattern generation CAD tools are used to analyze the peak power and the fault coverage of the proposed secure AES core.

Table 1 compares the technological characteristics with previous approaches [9-11]. AES core with [9] can not be reused in designing an SoC, [10] is not compatible with JTAG standards, and in [11] test patterns generated for the AES core can not be directly applicable unless converted through the S-box. Mode based [10] and our approach only provide complete protection of AES key.

Table 2, 3, 4, and 5 compare area overhead, functional power, scan test power, and fault coverage. The M in [9] indicates the number of matches for the activation of scan output ports, and the N tells the number of bits of the matching key. The experiment for [11] implements 4 scan chains (lengths of scan chains={66,66,65,65}) with 10 inverters for each scan chain. As can be seen in Table 2, the area overhead is relatively smaller than any other technique. Cell area can be smaller in [9], but increased routing overhead according to the length of the matching key bits N results in more area overhead. Additional inverters and S-box logic in [11] requires relatively more area overhead.

Power consumptions in normal mode are compared in Table 3. Proposed technique does not need extra register as MKR and flip-flops with reset mode in [10], and 1.92% power saving was achieved. In [9] additional interconnects to matching blocks for the activation of scan output ports asks more power. Due to the inverters and S-box logic, about 3.14% more power is needed in [11].

Table 4 compares the scan test power. Because of the MKR register, a considerable amount of dynamic scan

Table 2. Comparison of area overhead

		Cell Area (um^2)	Routing Area (um^2)	Total Area (um^2)	Total Area Inc. (%)
AES	-	185221	215166	400387	Non
[10]	-	201786	219351	421137	5.18
[9] (M/N)	256/1	188948	215535	404483	1.02
	128/2	187624	215746	403370	0.75
	32/8	187647	217001	404648	1.06
	16/16	187467	219364	406831	1.61
	4/64	187920	223057	410977	2.64
	1/256	188212	227594	415806	3.85
[11]	-	188467	218430	406897	1.63
Prop.	-	185397	215886	401283	0.22

Table 3. Power consumption in functional mode

		Dynamic (e-02 w)	Leakage (e-06 w)	Total (e-02 w)	Total Inc. (%)
AES	-	1.1272	5.285	1.1277	Non
[10]	-	1.1498	9.739	1.1508	2.04
[9] (M/N)	256/1	1.1301	5.464	1.1306	0.26
	128/2	1.1331	5.452	1.1336	0.52
	32/8	1.1397	5.434	1.1402	1.11
	16/16	1.1444	5.424	1.1449	1.53
	4/64	1.1538	5.407	1.1543	2.36
	1/256	1.1695	5.391	1.1700	3.75
[11]	-	1.1750	7.328	1.1757	4.26
Prop.	-	1.1285	5.435	1.1290	0.12

Table 4. Power consumption in scan test mode

		Dynamic (e-03 w)	Leakage (e-06 w)	Total (e-03 w)	Total Inc. (%)
AES	-	1.9546	5.285	1.9599	Non
[10]	-	2.1918	9.739	2.2015	12.33
[9] (M/N)	256/1	1.9688	5.464	1.9743	0.73
	128/2	1.9750	5.452	1.9805	1.05
	32/8	1.9861	5.434	1.9915	1.61
	16/16	1.9997	5.424	2.0051	2.31
	4/64	2.0232	5.407	2.0286	3.51
	1/256	2.0494	5.391	2.0548	4.84
[11]	-	2.0628	7.328	2.0701	5.62
Prop.	-	1.9877	5.435	1.9931	1.70

Table 5. Comparison of fault coverage

		FC(%)	FC Inc.(%)	Scan Chain Length
AES	-	99.62	Non	262
[10]	-	99.68	0.06	390
[9] (M/N)	256/1	99.62	0	262
	128/2	99.62	0	262
	32/8	99.62	0	262
	16/16	99.62	0	262
	4/64	99.62	0	262
	1/256	99.62	0	262
[11]	-	99.62	0	262
Prop.	-	99.85	0.23	262

power is consumed, hence compared with our approach 10.63% more power is needed in [10]. In [9] scan test power is increased according the number of fanouts, that is more bits of the matching keys. [11] also requires considerably more scan test power due to the inverters and S-box.

Fault coverages are compared in Table 5. All the techniques [9-11] show high fault coverages as our proposed technique. Increased length of scan chains due to additional MKR in [10] require more time to generate test patterns. Test patterns for the AES core have to be transformed using the S-box in [11].

V. CONCLUSIONS

An efficient scan secured design technique is proposed for AES core to protect the user key from side channel scan attack. Scan test is allowed only with invoking new JTAG instruction. Initially the scan chain possibly including encrypted data is flushed out by blocking the scan output port. Fake key is loaded instead of user key in scan test mode. Compared with other techniques complete protection is guaranteed with less area overhead, less power consumption, and better fault coverage. Compatibility with JTAG standards and no change of internal AES core give another advantage for design reusability. Since the technique proposed in this paper does not require any change in internal scan chain as well as core internal logic, it can be generally adopted to any cryptographic hardware design.

ACKNOWLEDGMENTS

This research was supported in part by the National Research Foundation of Korea (NRF) grant (MEST) (No. 2010-0026822) and Ministry of Knowledge Economy (MKE) and IDEC Platform Center(IPC) at Hanyang Univ.

REFERENCES

[1] Mangard, M. Aigner and S. Dominikus, “A Highly Regular and Scalable AES Hardware Architecture”, *IEEE Transactions on Computer*, vol. 52, no. 1, pp. 483-491, April, 2004.

[2] C. Lee, “Smart Bus Arbiter for QoS control in H.264 decoders”, *Journal of Semiconductor Technology and Science*, pp. 33-39, Vol. 11, No. 1, Mar., 2011.

[3] Josephson and S. Poehhnan, “Debug methodology for the McKinley processor”, *International Test Conference(ITC)*, pp. 451-460, Baltimore, MD, USA, Oct. 30- Nov. 1, 2001.

[4] J. Lee, M. Teharanipoor, C. Patel and J. Plusquellic, “Securing Designs Against Scan-Based Side-Channel Attacks”, *IEEE Transations on Depedable and Secure Computing*, Vol. 4, no. 4, pp. 325-336, Oct.-Dec., 2007.

[5] M. L. Bushnell and V. D. Agrawal, Essentials of Electronic Testing, Kluwer Academic Publishers, 2000.

[6] R. Kapoor, “Security vs. test quality: Are they mutually exclusive?”, *in Proc. ITC*, pp. 1414, Charlotte, NC, USA, Oct. 26–28, 2004.

[7] J. Lee, M. Teharanipoor, and J. Plusquellic, “A Low-Cost Solution for Protecting IPs Against Scan-Based Side-Channel Attacks”, *VLSI Test Symposium*, pp. 94-99, Berkeley, CA, USA, Apr. 30-May 4, 2006.

[8] Yang, K. Wu and R. Karri, “Scan Based Side Channel Attack on Dedicated Hardware Implementations of Data Encryption Standard”, *International Test Conference(ITC)*, pp. 339-344, Charlotte, NC, USA, Oct. 26–28, 2004.

[9] S. Paul, R. S. Chakraborty and S. Bhunia, “VIm-Scan : A Low Overhead Scan Design Approach for Protection of Secret Key in Scan-Based Secure Chips”, *VLSI Test Symposium*, pp. 455-460, Berkeley, CA, USA, May 6-10, 2007.

[10] Yang, K. Wu and R. Karri, “Secure Scan : A Design-for-Test Architecture for Crypto Chips”, *IEEE Transaction Computer-Aided Design of Integrated Circuits and systems*, Vol. 25, No. 10, pp. 2287-2293, Oct. 2006.

[11] G. Sengar, D. Mukhopadhyay and D. R. Chowdhury, “Secured Flipped Scan-Chain Model for Crypto-Architecture”, *IEEE Transaction Computer-Aided Design of Integrated Circuits and Systems*, Vol. 26, No. 11, pp. 2080-2084, Nov.2007.

[12] H. Fujiware and M. E. Obien “Secure and Testable Scan Design Using Extended de Bruijn Graphs”, *Proc. 15th Asia and South Pacific Design Automation Conference (ASP-DAC),* pp. 413-418,

2010

[13] J. Song, T. Jung, J. Lee, H. Jeong, B. Kim, S. Park, "An Efficient Secure Scan Design for an SoC Embedding AES Core", *International Test Conference(ITC)*, Oct. 26-28, 2008

[14] J. Da Rolt, G. Di Natale, M.-L Fkittes, and B. Rouzeyre "New security threats against chips containing scan chain structures", *Proc. IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 105-110, 2011

[15] K. Rosenfield and R. Karri "Security-Aware SoC Test Access Mechanisms", *Proc. IEEE VLSI Test Symposium (VTS)*, pp. 100-104, 2011

[16] K. Rosenfield and R. Karri "Attacks and Defenses for JTAG", *IEEE Design & Test of Computers*, pp. 36-47, 2010

[17] J. Seberry, X. M. Zhang and Y, Zheng, "Systematic generation of cryptographically robust S-boxes", *The 1st ACM Conference on Computer and Communications Security*, pp. 171-182, Fairfax, Virginia, USA, Aug. 10, 1993.

Jaehoon Song received the B.S., M.S., and Ph.D. degrees in computer science and engineering from Hanyang University, Kyeonggi-do, Korea in 2000, 2002, and 2009 respectively. Since 2009 he has been working for TranSono Inc., Seoul, Korea. In 2003, he worked for the System-on-a-Chip (SoC) Design Center at Seoul National University in Korea, where he was on the Development Staff in charge of platform-based design. His main research interests are in Design-for-Testability (DfT), signal integrity, and low-power design. Mr. Song is a member of the Institute of Electronics Engineers of Korea and the Korea Information Science Society. He received the Best Paper Award from the Korea Test Association at the Korea Test Conference in 2007.

Taejin Jung received the B.S. and M.S. degrees in Computer Science and Engineering from Hanyang University. Kyeonggi-do, Korea, in 2007 and 2009, respectively. He worked for C&S Technology from 2009 to 2011. Now he is working for LG Electronics. His interests include Design for Testability, Memory Test, and SoC Design.

Jihun Jung received the B.S. in computer science and engineering from Hanyang University, Kyeonggi-do, Korea in 2009. Since 2010 he has been working toward the M.S. and Ph.D. degree in computer science and engineering at the same University. His interests include Design for Testability, Memory Test, Memory ECC, and NoC Design.

Sungju Park received the B.S. degree in electronics from Hanyang University, Korea, in 1983 and the M.S and Ph.D. degrees in electrical and computer engineering from the University of Massachusetts at Amherst in 1988 and 1992, respectively. From 1983 to 1986, he was with the Gold Star Company in Korea. From 1992 to 1995, he worked for IBM Microelectronics, Endicott, NY as a Development Staff in charge of boundary scan and LSSD scan design. Since then, he has been a Professor in the department of computer science and engineering in Hanyang University, Korea. His research interests lie in the area of VLSI testing including scan design, built-in self test, test pattern generation, fault simulation, and synthesis of test. Additional interests include graph theory and design verification.