2009 IEEE European Test Symposium, pp.143 -148, May 2009.

Partial Scan Approach for Secret Information Protection*

Michiko Inoue Tomokazu Yoneda Muneo Hasegawa Hideo Fujiwara
Nara Institute of Science and Technology(NAIST), Japan
{kounoe, yoneda, fujiwara}@is.naist.jp

Abstract

This paper proposes a secure scan design method which protects the circuits containing secret information such as cryptographic circuits from scan-based side channel attacks. The proposed method prevents the leakage of secret information by partial scan design based on a balanced structure. We also guarantee the testability of both the design under test and DFT circuitry, and therefore, realize both security and testability. Experiments for RSA circuit shows the effectiveness of the proposed method.

1. Introduction

Cryptographic circuits are often embedded in secure systems requiring high throughput. Since such cryptographic circuits include encryption and/or decryption keys in the circuits, their security is important issue.

Scan design is a widely used Design-for-Testability technique, which enables FFs in sequential circuits to be directly controlled and observed through scan chains. However, it is too vulnerable in scan-based side-channel attacks if test pins are still available after production tests for in-field test or debug. Several works have been done to achieve both security and testability for scan design.

Hely et al.[3] introduced an authentication mechanism. If the authentication is failed, FF order in a scan chain are periodically changed, and it makes the attackers impossible to analyze the circuits. They[2] also proposed a test controller which isolates registers with secret information and resets values of the other registers at the beginning of test mode to protect secret information to be leaked. However, the method has room for improvement on testability since the method cannot test secret registers and the test controller is tested by only checking whether all the registers are reset.

Lee et al.[4] presented a Lock & Key technique where a scan chain is divided into smaller subchains and access to subchains are randomized for unauthorized users. The method requires a large test controller including FSM for the authorization, LFSR to randomize the subchain order. Moreover, testability of the test controller is not mentioned.

Yang et al.[8] proposed a Mirror Key Register (MKR) that keeps a copy of secret key in normal mode. The proposed method introduced a test controller that can transfer the circuit to test mode only when it is powered on. That prevents attackers from extracting the data on the way of encryption or decryption. In test mode, the register storing the secret information is isolated from the remaining circuit, and the MKR is reset at the beginning of the test mode. Therefore, the secret information is never leaked in test mode. The proposed method enables the whole circuit to be tested except the register for the secret information and the signal lines between the register and the MKR.

Paul et al.[6] proposed a VIm-Scan which utilizes some FFs in a scan chain for authentication to move to test mode. In this method, the circuit can move to test mode only if the proper sequence of test keys are inputed to these FFs. This method is superior to the other methods in a sense that the test controller is testable. However, it needs a long test key sequence to move test mode.

In this paper, we propose a new secure scan method based on a balanced structure. The balanced structure is a structure for testable sequential circuits. We adopt a partial scan to make a *kernel* balanced, where a kernel is the portion of the circuit excluding the scan chains. The partial scan protects non-scan registers completely from scan-based attacks. In addition, we introduce a mechanism to confuse the kernel logic in test mode to protect scan registers. Our proposed method makes the circuit behavior in test mode completely different from normal mode. We use a test controller that transfers the circuit to test mode only when it is powered on like [8]. The proposed test controller is very small and fully testable. Therefore, the proposed partial scan method based on balanced structure guarantees high security and high testability simultaneously. Moreover, because of the nature of partial scan, the proposed method can achieve lower area overhead and reduce over-testing compared to full scan design.

*This work was supported in part by Japan Society for the Promotion of Science (JSPS) under Grants-in-Aid for Scientific Research ((B)20300018, (C)18500038).

The remainder of the paper is organized as follows. In Section 2, we assume the potential attackers and discuss the vulnerability of some well-used cryptographic circuits. Section 3 introduces a balanced structure, and we propose a new secure scan design and evaluate it in Sections 4 and 5. Finally, we conclude the paper in Section 6.

2. Assumption on Attackers

In general, the security requirements are varied with attackers' knowledge level. In this paper, we suppose the attackers who can use only generally obtainable knowledge, and assume the attackers as follows.

1. Attackers know the cryptographic algorithm to be implemented as a circuit, and can suppose some candidates for RTL design.
2. Attackers can identify the test pins if scan design is adopted as DFT.
3. Attackers do not know detailed information on the gate level design or DFT including the order of FFs in the scan chains.

Some scan-based side-channel attacks are reported for DES(Data Encryption Standard)[7] and AES(Advanced Encryption Standard)[8]. These attacks identify the order of scan FFs by applying input patterns repeatedly, and discover the secret information from the analysis of registers.

RSA needs a secret key for decryption in which modulo-multiply operations and modulo-square operations are repeatedly executed. The executions of modulo-multiply operations depends on a bit pattern of the secret key, and it can be discovered by analyzing scan FFs repeatedly.

3. Balanced Structure

We use a balanced structure[1] as a testable sequential circuit structure. To use the structure, we give some definition according as [1].

A synchronous sequential circuit S consists of blocks of combinational logic and registers. A register is a collection of one or more FFs controlled by the same control signal. There are two kinds of registers. A LOAD register is a register whose FFs have no explicit LOAD ENABLE control signal, and a HOLD register is a register whose FFs have an explicit LOAD ENABLE control signal. The LOAD ENABLE control signals must be controlled primary inputs. The combinational logic in S are partitioned into clouds, each of which is a maximal region of connected combinational logic such that its inputs are either primary inputs or outputs of FFs and its outputs are either primary outputs or inputs to FFs.

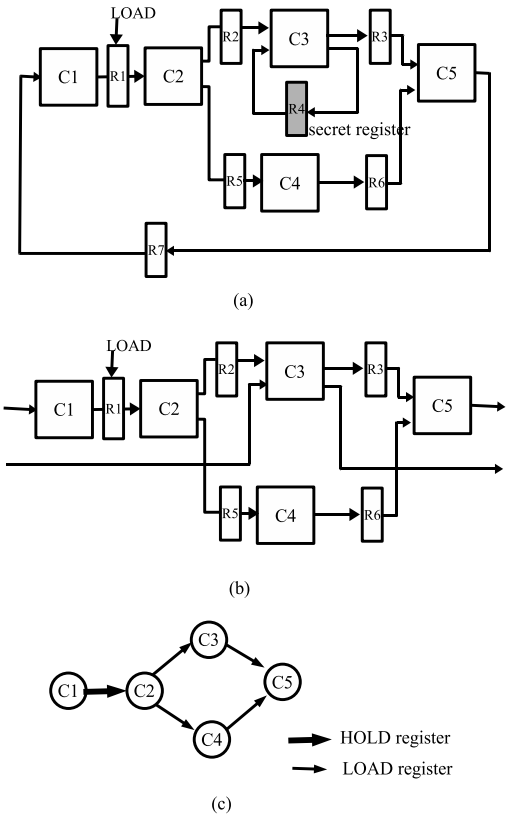

Figure 1. (a)Sequential circuit S, (b)Balanced sequential circuit S', (c)Topology graph.

A *topology graph* of a sequential circuit is a directed graph $G = (V, A, H, w)$ in which V is a set of clouds, A is a set of registers between clouds, $H \subset A$ is a set of HOLD registers, and $w : A \rightarrow Z^+$ (positive integers) denotes the number of FFs in each register. The weight $w(a)$ of a register a represents the cost of converting the register a into a scan register.

Definition 1 (balanced structure[1]) *Let S be a synchronous sequential circuit with a topology graph $G = (V, A, H, w)$. S is said to be balanced structure if*

1. *G is acyclic,*
2. *$\forall v_1, v_2 \in V$, all directed paths from v_1 to v_2 are of equal length, and*
3. *$\forall h \in H$, if h is removed from G, the resulting graph is disconnected.*

Figure 1(a) shows an example of a sequential circuit S. The sequential circuit consists of clouds $C1, \cdots, C5$,

a HOLD register $R1$ and LOAD registers $R2, \cdots, R7$. The sequential circuit S' is obtained from S by replacing two registers $R4$ and $R7$ with primary inputs and outputs. Figures 1(b),(c) show the sequential circuit S' and its topology graph. The topology graph satisfies Definition 1 and S' is a balanced structure.

If a sequential circuit is a balanced structure, we can obtain a test sequence for the circuit using test patterns for its combinational equivalent. A combinational equivalent for a balanced sequential circuit S is a combinational circuit obtained from S by replacing each FF in every register in S with a wire. Let d be the longest directed path length in a topology graph of S. If some fault f is detected when applying an input pattern t to S in continuous d clocks, t is said to be a single-pattern test for f.

Theorem 1 ([1]) *Let S and C be a balanced sequential circuit and its combinational equivalent, respectively. Then any complete test set for all detectable stuck-at faults in C is a complete single-pattern test set for all detectable stuck-at faults in the combinational logic of S.*

In [1], a partial scan method BALLAST that obtains a balanced sequential circuit as a *kernel* is proposed. A heuristic algorithm is also proposed to select scan registers resulting in the minimum area overhead.

4. Balanced Secure Scan

4.1 Outline

We propose a new secure scan method based on a balanced structure, called *balanced secure scan*. The proposed balanced secure scan protects secret information stored in some registers in a circuit under test. We call the registers which keep the secret information or whose values depend on the secret information *secret registers*. In this paper, we assume that secret registers are designated in advance. The outline of the proposed method is shown as follows.

1. Select scan registers so that the kernel becomes a balanced structure and the number of FFs in secret registers selected as scan registers is minimized.

2. If some secret registers are selected as scan registers, add confusion circuits into the kernel to confuse the values of the secret registers in test mode while preserving balanced structure.

The proposed method protects some secret registers by partial scan, and protects the other secret registers by kernel logic confusion. The kernel logic confusion realizes different behaviors between normal and test modes and prevents the secret information from leakage from the scannable secret registers in test mode. Moreover, we propose a test controller that transfers the circuit to test mode only when the circuit is powered on, so that that the scan shift operation is unavailable once the circuit becomes normal mode. The proposed confusion circuit and test controller are testable, and therefore, the proposed method guarantees that the additional circuit does not reduce the security by their malfunction.

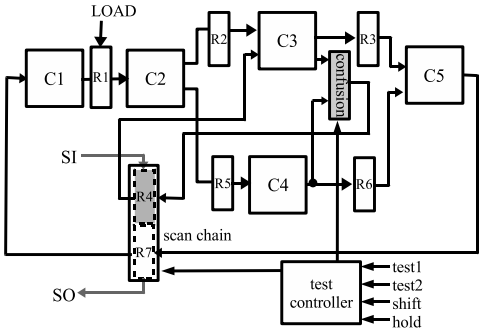

Figure 2. Proposed method.

Figure 2 shows an example where the proposed method is applied to a sequential circuit in Fig.1(a). We first make the kernel balanced by selecting $R4$ and $R7$ as scan registers. Since the selected $R4$ is a secret register, we then confuse the input of $R4$ using the output of a cloud $C4$.

4.2 Scan Register Selection

For a given sequential circuit, we first select scan registers so that the kernel becomes a balanced structure, where we try to minimize the number of FFs in the secret registers selected as scan register and then minimize the number of FFs in the scan registers.

We select scan registers by an enhanced method of the scan register selection proposed in [1]. The method[1] selects scan registers for a given topology graph $G = (V, A, H, w)$ to make the kernel balanced, where the total weight $\sum_{r \in SR} w(r)$ of selected scan registers is minimized, where SR is a set of selected registers.

In the proposed method, we first replace the weight $w(r)$ of each secret register r with $C \cdot w(r)$ by multiplying a sufficient large value C, then apply the scan register selection method in [1]. Consequently, we select a small number of scan FFs in secret registers and a small number of scan FFs.

4.3 Kernel Logic Confusion

If some secret registers are selected as scan registers, we confuse values of the registers only in test mode. In the

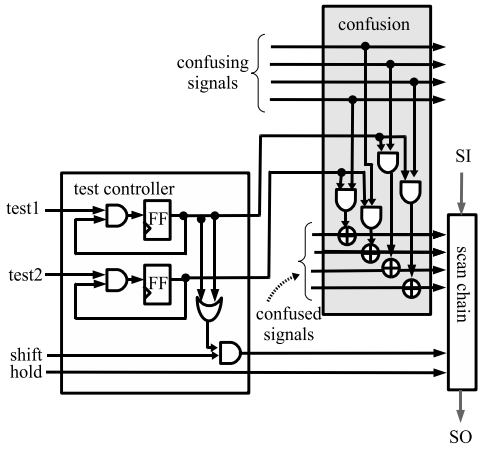

Figure 3. Confusion circuit and test controller.

kernel logic confusion, the inputs of the secret registers are exclusive-ORed with other signals(Fig.3). The additional connections are chosen while preserving balanced structure. In the current version, we randomly choose the signals that confuse the secret scan registers within the range that preserves a balanced structure.

Since the kernel logic confusion is needed only in test mode, we mask the signals which confuse the secret scan registers in normal mode. These mask elements are controlled by a test controller.

4.4 Test Controller

We propose a test controller to switch normal mode and test mode (Fig.3). The test controller has 4 inputs: $test1$, $test2$, $shift$, and $hold$, where $test1$ and $test2$ control the mode of the circuit, and $shift$ and $hold$ control the scan chains. The shift operation is available only when $shift = 1$ holds in test mode. The test controller has two FFs, and the circuit is said to be in test mode when at least one FF in the test controller has a value 1. The proposed test controller has the following features.

1. We adopt power-on set FFs to the test controller, and this brings the circuit to be test mode when it is powered on and once the circuit moves to normal mode it cannot go back to test mode while being powered on.

2. Values of registers in normal mode cannot be shifted out through scan chains. Since the circuit cannot be transferred from a normal mode to test mode, it is impossible to make the circuit operate for several clock cycles in normal mode and then shift out the register values using the scan operation.

3. The kernel logic confusion and scan shift operation are available only in test mode.

4. The test controller and the kernel logic confusion circuit are testable. Since the circuit is in test mode if at least one FF in the test controller has a value 1, two FFs can have value 0 exclusively. That is, we can fully control each FF value in test mode. Since the circuit under test including the confusion circuits is a balanced structure, and in addition, the test controller has a quite simple structure, both the test controller and the confusion circuits are testable.

5. Evaluation

5.1 Security

In general, scan-based side-channel attacks analyze the circuits with secret information based on the implemented algorithm and shifted-out FF values. The known attack methods for AES or DES repeat normal operations and scan operations, identify the order of FFs in a scan chain, and then analyze the secret information. That is, information on the implemented algorithm and/or all the FF values are necessary to analyze secret information.

In the proposed method, a part of registers are protected as non-scan registers. Even if some secret registers are selected as scan registers, their values are confused in test mode. In addition, the circuit cannot go back to test mode once it moves to normal mode, and hence, any attacker cannot extract FF values in normal mode. Since attackers are assumed to have no knowledge on gate level design, they cannot know the algorithm implemented by confusion circuits. In addition, a part of FF values are not shifted out and the attackers cannot know all the FF values. From these facts, it is impossible to analyze secret information.

The test controller and the confusion circuits are testable, and this testability avoids a risk of secret information leakage due to some malfunction of these additional circuit.

5.2 Testability

We evaluated the proposed method using an RSA decryption circuit. We use the 1024-bit RSA decryption circuit available as an open source IP core[5].

We first modified the circuit according to the assumption in [1]. We modified the circuit so that the registers have explicit LOAD ENABLE control signals if the registers have HOLD function.

We applied the proposed balanced secure scan and full scan methods to the modified circuit, and compared area overhead and testability. We used Design Compiler (Synopsys) for logic synthesis, DFT Complier (Synopsys) to in-

Table 1. Area overhead

	confusion (%)	area (gates)				area overhead (gates)					
		total	comb.	register	TC	total	total(%)	confusion	MUX	scan	TC
original		331,566	206,042	125,524	0	0	0	0	0	0	0
full scan		359,378	206,042	153,336	0	27,812	8.39	0	0	27,812	0
proposed	100	361,578	218,466	143,088	24	30,012	9.05	12,288	136	17,564	24
	50	355,434	212,322	143,088	24	23,868	7.20	6,144	136	17,564	24
	25	352,362	209,250	143,088	24	20,796	6.27	3,072	136	17,564	24

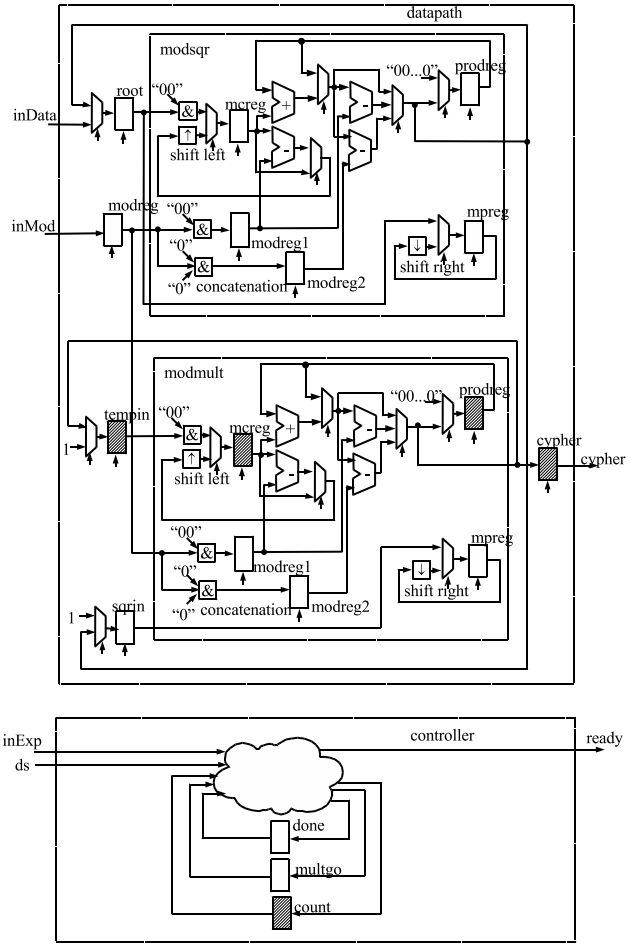

Figure 4. RSA decryption circuit.

sert scan chains, and TetraMAX (Synopsys) for test generation on SunFireV4100(3GHz AMD Opteron256, 16GB memory).

Figure 4 shows the RSA decryption circuit, which is composed of a datapath and a controller. The datapath has a modulo-square part (modsqr), and a modulo-multiply part(modmult). The RSA decryption circuit decodes an encrypted text y to a plaintext x using a secret key d and a public key m as $x = y^d \bmod m$. These keys d and m are stored in inMod and inExp in Fig.4, respectively. The modulo-square part calculates $y^{2^0} \bmod m, y^{2^1} \bmod m, y^{2^2} \bmod m, \cdots$ in this order. The module-multiply part calculates a modulo-multiply operation with the output of the modulo-square part as needed. For example, for $d = 5 = 101_{(2)}$, the plain text x is obtained as $x = y^{101_{(2)}} \bmod m = (y^{2^0} \bmod m) \times (y^{2^2} \bmod m) \bmod m$. That is, the operation of the module-multiply part depends on a bit pattern of the secret key d. Since the modulo-square part is not related with secret information, only the registers prodreg, mcreg in modmult, and registers count, cypher and tempin are designated as secret registers.

In the proposed method, we first separated the datapath and the controller by inserting primary input with MUXes and primary output to the signals between them to make the LOAD ENABLE control signals directly controllable from the primary inputs. This modification is to apply DFT for balanced structure[1]. We then selected scan registers to make the kernel balanced. As a result, registers mcreg, mpreg, modreg1, prodreg in both modsqr and modmult, and registers done, multgo, count are selected as scan registers. The secret registers selected as scan registers are mcreg and prodreg in modmult and count in the controller, and we confuse the inputs of these 3 registers. The bit-width of mcreg, prodreg and count are 1026, 1026 and 1024, respectively. In the experiment, we confused 1024(100%), 512(50%) and 256(25%) bits of the input of each register, and compared these area overhead and testability.

Table 1 shows the area and the area overhead for the proposed method and the full scan design. We used the circuit after modification on LOAD ENABLE signals as an original circuit. The column $confusion$ denotes confusion ratio. The column $comb.$ denotes the combinational logic area including confusion circuits and MUXes for the datapath-controller isolation. The column $register$ denotes the area for non-scan and scan registers. The column TC denotes the area for a test controller. The proposed method achieves a little bit larger area overhead than the full scan when confusing all the bits of input of the secret registers selected as scan register. Practically, it is not considered that we need to confuse all the bits to protect such registers. Our method

Table 2. Test generation result (inMod and inExp are fixed)

	confusion(%)	fault	FC(%)	FE(%)	redundant	abort	TGT(s)
full scan	-	459,342	98.66	100.00	6,156	0	30.47
proposed	100	496,268	96.10	100.00	19,374	0	80.81
	50	477,836	95.95	100.00	19,374	0	72.66
	25	468,620	95.87	100.00	19,373	0	68.31

Table 3. Test generation result (inMod and inExp are primary inputs)

method	confusion(%)	fault	FC(%)	FE(%)	redundant	abort	TGT(s)
full scan	-	459,342	99.999	100.000	4	0	29.51
proposed	100	496,268	99,999	100.000	1	0	7.64
	50	477,836	99.999	100.000	1	0	6.98
	25	468,620	99.999	99.999	0	4	8.19

achieve lower area overhead than the full scan design when we confuse a part of these bits.

Table 2 shows the test generation result for the combinational logic parts, where two keys in inMod and inExp are set to some fixed random values. The columns $confusion$, $fault$, FC, FE $redundant$, $abort$ and TGT are confusion ratio, the numbers of total stuck-at faults, fault coverage, fault efficiency, the number of identified redundant and aborted faults, and test generation time, respectively. The combinational part for the proposed methods include the confusion circuits and therefore the number of faults are increased. We achieved complete (100%) fault efficiency for all the cases with reasonable test generation time. However, the proposed methods identified more redundant faults than the full scan. We considered this is because the register modreg is not selected as a scan register and there are redundant faults at both input and output of modreg which is connected with inMod with the fix value. However, in the case of the full scan design, modreg is selected as a scan register, and this makes the output of modreg testable.

To confirm this prediction, we gave an additional experiment for the case where inMod and inExp are primary inputs. Table 3 shows the result. In this case, there are little redundant faults for both the proposed method and the full scan design. That is, the most redundant faults are caused by the embedded fixed values. This implies that the proposed method can avoid over-testing.

6. Conclusion

In this paper, we proposed a partial scan method to make sequential circuits testable without sacrificing security. The proposed method protects secret registers through partial scan and the kernel logic confusion, and hence guarantees high security of the circuits. On the other hand, a partial scan method based-on the balanced structure guarantees high testability. In addition, the proposed method guarantees the testability of additional circuits, and this testability avoids a risk of secret information leakage due to some malfunction of these additional circuits.

Though full scan design is a de-facto standard for DFT method, this paper demonstrated a potential of partial scan design which can protect the secret information from scan-based side-channel attacks. The proposed method may affect the design flow, but it is very powerful and area-efficient method when highly security level is required for circuits.

References

[1] R. Gupta, R. Gupta, and M. Breuer. The BALLAST methodology for structured partial scan design. *IEEE Transactions on Computers*, 39(4):538–544, April 1990.

[2] D. Hely, F. Bancel, M.-L. Flottes, and B. Rouzeyre. Securing scan control in crypto chips. *Journal of Electronic Testing - Theory and Applications*, 23(5):457–464, Oct. 2007.

[3] D. Hely, M.-L. Flottes, F. Bancel, B. Rouzeyre, and N. Berard. Scan design and secure chip. In *Proceedings of 10th IEEE International On-Line Testing Symposium (IOLTS'04)*, pages 219–224, 2004.

[4] J. Lee, M. Tehranipoor, C. Patel, and J. Plusquellic. Securing designs against scan-based side-channel attacks. *IEEE Transactions on Dependable and Secure Computing*, 4(4):325–336, Oct.-Dec. 2007.

[5] OPENCORES. Rsa processor. http://www.opencores.org/projects.cgi/web/rsa/overview.

[6] 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. In *Proceedings of 25th IEEE VLSI Test Symposium(VTS'07)*, pages 455–460, 2007.

[7] B. Yang, K. Wu, and R. Karri. Scan based side channel attack on dedicated hardware implementations of data encryption standard. In *Proceedings of International Test Conference 2004 (ITC'04)*, pages 339–344, 2004.

[8] B. Yang, K. Wu, and R. Karri. Secure scan: A design-for-test architecture for crypto chips. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 25(10):2287–2293, Oct. 2006.