

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
25 January 2007 (25.01.2007)

PCT

(10) International Publication Number
WO 2007/011507 A2

(51) International Patent Classification:
G01R 31/28 (2006.01)

(21) International Application Number:
PCT/US2006/025178

(22) International Filing Date: 27 June 2006 (27.06.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/182,335 14 July 2005 (14.07.2005) US

(71) Applicant (for all designated States except US): **ATMEL CORPORATION** [US/US]; 2325 Orchard Parkway, San Jose, CA 95131 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **FAGAN, John** [US/US]; 7671 Pine Knob Road, Pasadena, MD 21122 (US).

(74) Agents: **SAWYER, Joseph, A.** et al.; SAWYER LAW GROUP LLP, P.O. Box 51418, Palo Alto, CA 94303 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR ENCRYPTION-BASED DESIGN OBFUSCATION FOR AN INTEGRATED CIRCUIT

(57) Abstract: Encryption-based design obfuscation for an integrated circuit includes creating multiple functional circuit paths for an integrated circuit design and selecting among the multiple functional circuit paths during scan testing. Encrypting selection data corresponding to an intended function of the integrated circuit design avoids revealing the intended function as a result of the scan testing.



WO 2007/011507 A2

METHOD AND SYSTEM FOR ENCRYPTION-BASED DESIGN OBFUSCATION FOR AN INTEGRATED CIRCUIT

FIELD OF THE INVENTION

The present invention relates to securing circuit design, and more particularly to encryption-based design obfuscation for integrated circuit designs.

5 BACKGROUND OF THE INVENTION

The development of integrated circuits (ICs) has become increasingly complex, due in large part to the ever increasing functionality offered by newly developed circuitry. Integrated circuits continue to surpass milestones in development, as more and more functionality is packaged into smaller sizes. This enhanced functionality and the
10 greater number of transistors packaged in an integrated circuit requires more rigorous testing requirements to insure reliability once the device is commercialized. Thus, new integrated circuit designs are repeatedly tested and debugged during the development process to minimize the number and severity of errors that may subsequently arise. Regardless of the rigor of the developmental testing, invariably a certain percentage of
15 manufactured devices will fail prematurely.

Thus, a problem existing in the semiconductor industry is in the testing of manufactured chips. Even assuming a good, error-free logic design, it is well known that various faults and errors can enter into the production process, which can result in functional defects in a manufactured chip. These faults can enter through a variety of
20 causes in the numerous manufacturing process steps and can affect any of the different gates, switches or lines on the chip. To prevent such devices from being sold or used in systems, typically some level of testing is performed on manufactured chips to identify those that may fail prematurely.

A number of different types of testing have been used to minimize the possibility
25 of premature failure of manufactured chips. One of the more popular types of testing is scan testing. Scan testing is a well recognized design-for-test ("DFT") technique used for addressing certain testing problems in very large scale integrated ("VLSI") circuits. A full scan design technique transforms a given sequential circuit into a combinational circuit and shift register (referred to as a scan register) for the purpose of testing. This
30 transformation makes it possible to obtain almost complete fault coverage using an Automatic Test Pattern Generation ("ATPG") program. Typically, as part of the scan

test, large circuits are partitioned into smaller combinational circuits to facilitate fault isolation and failure analysis.

The scan design technique implements all or most of the state elements in the device under test, such as flip-flops and latches, as scannable flip-flops, which often are referred to as scan-flops. An ATPG program can treat the state elements as pseudo inputs and outputs of the device. During typical testing, a scan-path is first tested by shifting a simple sequence of 1s and 0s through chained scan-flops. The ATPG program then generates test vectors that are applied to test the combinational logic. The device then returns to normal operational mode, typically for one clock cycle, to capture the response of the combinational circuit in the scan-flops. The captured response is unloaded via the scan-path and, at the same time, the state element values corresponding to the next test vector are loaded. This testing sequence repeats until all test vectors are applied.

Tools exist to help evaluate resulting data from the scan test and identify path(s)/logic gate(s) exhibiting stuck-at faults. While such analysis tools can provide a level of assistance in isolating faults, they also create a level of vulnerability, since use of such tools allows for reverse engineering of the integrated circuit design.

A need exists, therefore, for design obfuscation for an IC, including during scan testing. The present invention addresses such a need.

BRIEF SUMMARY OF THE INVENTION

Aspects of encryption-based design obfuscation for an IC are described. Encryption-based design obfuscation for an integrated circuit includes creating multiple functional circuit paths for an integrated circuit design and selecting among the multiple functional circuit paths during scan testing. Encrypting selection data corresponding to an intended function of the integrated circuit design avoids revealing the intended function as a result of the scan testing.

With the encryption-based design obfuscation of the present invention, the circuit function intended as a circuit design cannot be determined without knowledge of the encrypted select register data. Without the ability to determine the intended function, reverse engineering via scan test analysis is prevented. The present invention achieves this security while supporting scan testing for fault coverage of a circuit design in a straightforward and effective manner. These and other advantages of the aspects of the present invention will be more fully understood in conjunction with the following

detailed description and accompanying drawings.

BRIEF DESCRIPTION OF SEVERAL VIEWS OF THE DRAWINGS

Figure 1 illustrates a block diagram of an encryption based design obfuscation for an integrated circuit in accordance with the present invention.

Figure 2 illustrates a block diagram of the encryption based obfuscation design including a tamper detect block.

DETAILED DESCRIPTION OF THE INVENTION

The present invention relates to encryption-based design obfuscation for an integrated circuit. The following description is presented to enable one of ordinary skill in the art to make and use the invention and is provided in the context of a patent application and its requirements. Various modifications to the preferred embodiment and the generic principles and features described herein will be readily apparent to those skilled in the art. Thus, the present invention is not intended to be limited to the embodiments shown but is to be accorded the widest scope consistent with the principles and features described herein.

Figure 1 illustrates a block diagram of encryption based design obfuscation for an integrated circuit that avoids revealing the design/reverse engineering as a result of scan testing in accordance with the present invention. A 4:1 MUX (multiplexer) 25 is inserted for use with every flip-flop 26 in the scan test. One input connection of MUX 25 is for the actual functional path of the circuit logic 30 and three input connections can provide valid functional inputs but are not part of the functional path. An n-bit select register 27 is also provided. The number of functional circuits created is 2^n . Thus, if $n=10$, 1024 circuits that are deterministic (and non-trivial) input to output functions are provided. However, only one of those circuits is the intended function for the actual design.

In order to secure the design, the intended function selection data is encrypted with an encryptor 29, e.g., an encryption algorithm, such as DES (data encryption standard). The encrypted data provides the selection data for the one intended function that the design developer knows, but which the device tester does not know. Since other selection data selects a functional circuit input, scan testing can still be achieved for fault coverage without revealing actual intended device function. This could allow sensitive (ITAR) designs to be assembled and tested in non-ITAR compliant locations.

Through the utilization of encrypted selection data in accordance with the present

invention, the circuit function intended for the design cannot be determined without knowledge of the encrypted select register data. Without the ability to determine the intended function, reverse engineering is prevented. Further, in a preferred embodiment, the register select value for the intended function is lost if power is removed, resulting in all 2^n circuits being equally probable for selection. Figure 2 illustrates the block diagram of the encryption based obfuscation design including a tamper detect block 31. If the power is lost, the circuit will probably be disabled (1 chance in 2^n of powering up in operational state). Use of a power on reset circuit, and adding a reset function to the n-bit register 27 will guarantee powering up in a non-operational mode. In addition, if the tamper detection block 31 is added to the device or system, conditions such as overvoltage, undervoltage, illegal clock frequency, or sudden temperature change, can be used to reset the n-bit select register to a false state even while operating. If this occurs, the device continues to operate, in a benign fashion, with no apparent indication that tamper detection has occurred. Thus, the 'real' circuit can be disabled in the case of tamper detection. In addition, the selection bits do not have to be unique but can be shared among the registers in a circuit design, as is well appreciated by those skilled in the art.

Although the present invention has been described in accordance with the embodiments shown, one of ordinary skill in the art will readily recognize that there could be variations to the embodiments and those variations would be within the spirit and scope of the present invention. For example, although DES is described for use as the encryption algorithm, other encryption algorithms may be used according to design needs, as is well understood in the art. Accordingly, many modifications may be made by one of ordinary skill in the art without departing from the spirit and scope of the appended claims.

CLAIMS

We Claim:

1. A method for encryption-based design obfuscation for an integrated circuit, the method comprising:

creating multiple functional circuit paths for an integrated circuit design;

selecting among the multiple functional circuit paths during scan testing; and

encrypting selection data corresponding to an intended function of the integrated circuit design to avoid revealing the intended function as a result of the scan testing.

2. The method of claim 1 wherein selecting further comprises selecting with an n-bit select register.

3. The method of claim 2 wherein encrypting selection data further comprises encrypting the data of the n-bit select register with a data encryption standard (DES) algorithm.

4. The method of claim 2 wherein creating multiple functional paths further comprises creating 2^n functional paths.

5. The method of claim 1 wherein the encrypted selection data is lost upon circuit tamper detection.

6. The method of claim 5 wherein loss of the encrypted circuit selection data results in an equal probability of selection of each of the multiple functional paths.

7. The method of claim 1 wherein creating multiple functional paths further comprises creating a plurality of deterministic, non-trivial, input to output functions.

8. A system for encryption-based design obfuscation for an integrated circuit, the system comprising:

functional path logic of an integrated circuit;

a selection device for storing selection data to direct selection of one of a plurality of circuit designs for the functional path logic; and

an encryptor for encrypting selection data corresponding to an intended function of the integrated circuit, wherein potential reverse engineering of the intended function as a result of scan testing is avoided.

5 9. The system of claim 8 wherein the selection device further comprises an n-bit select register.

10 10. The system of claim 9 wherein the selection device further stores encrypted selection data from the encryptor as data encrypted in accordance with a data encryption standard (DES) algorithm.

11. The system of claim 9 wherein the selection device further directs selection of one of 2^n circuit designs.

15 12. The system of claim 8 wherein the selection device loses the encrypted selection data upon circuit tamper detection.

13. The system of claim 12 wherein loss of the encrypted selection data results in an equal probability of selection of each of the plurality of circuit designs.

20 14. The system of claim 8 wherein each of the plurality of circuit designs further comprises a deterministic, non-trivial, input to output functional circuits.

25 15. A method for encryption-based design obfuscation for an integrated circuit, the method comprising:

encrypting data that identifies an intended function for an integrated circuit design; and

selecting the intended function from a plurality of functions based on the encrypted data.

30 16. The method of claim 15 wherein the encrypted data further comprises encrypted data in an n-bit select register.

17. The method of claim 16 wherein selecting the intended function further

comprises selecting the intended function from 2^n functions.

18. The method of claim 15 further comprising losing the encrypted data upon
tamper detection to result in equal probability for selection of each of the plurality of
functions.

1/1

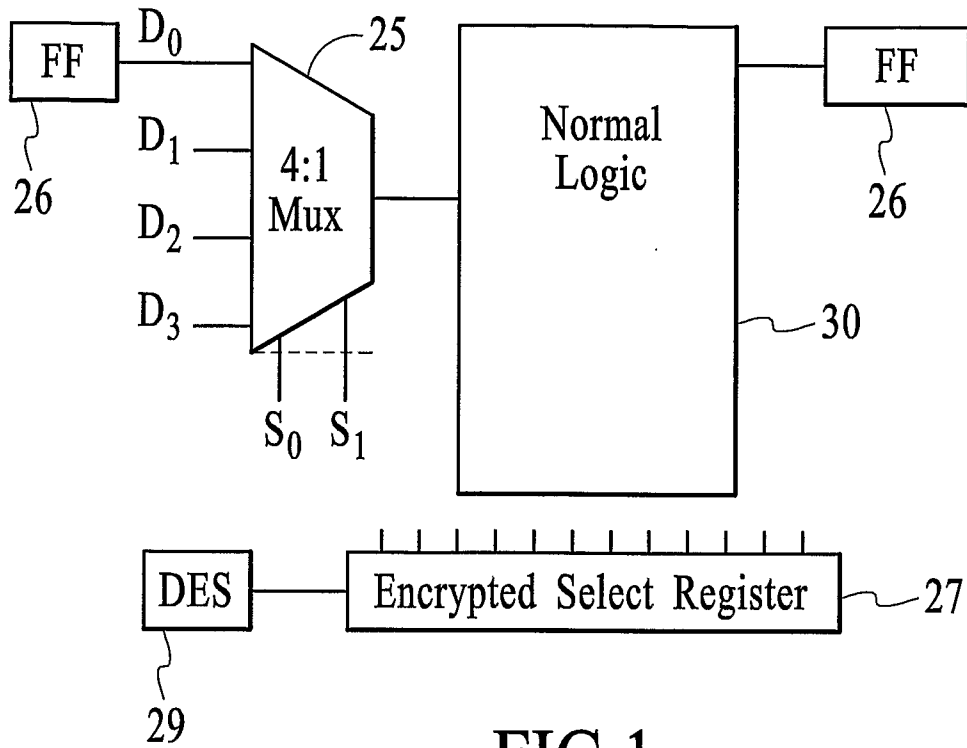


FIG.1

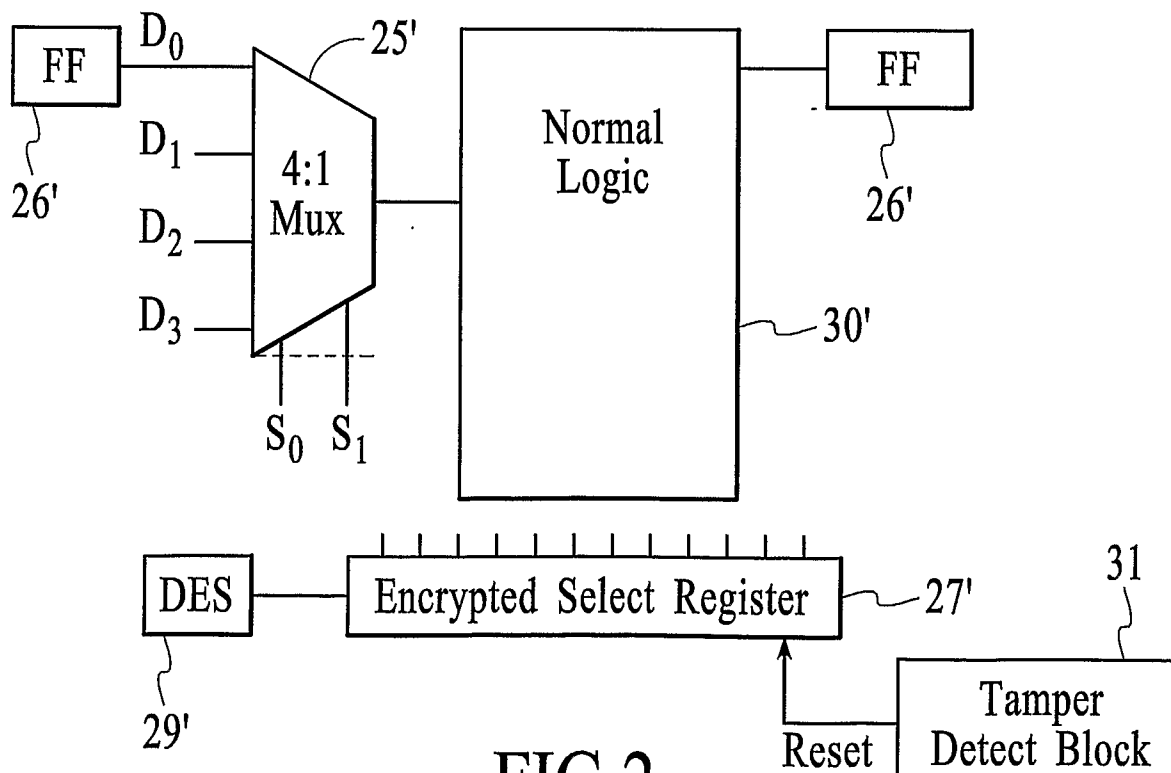


FIG.2