(12) **BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ**

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **1-0021128**

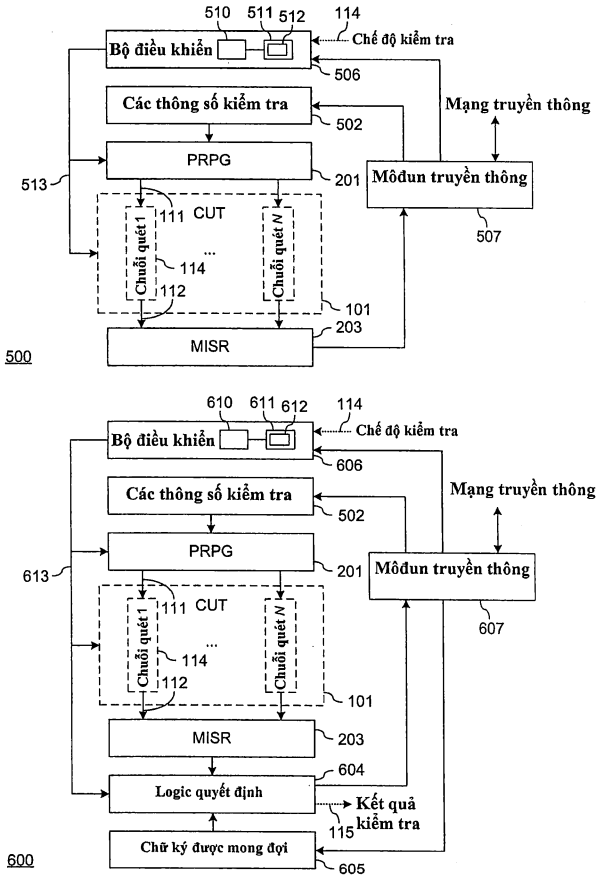
(51)[7] **G01R 31/3181**, 31/3183

(13) **B**

(21) 1-2016-03246
(22) 05.02.2014
(86) PCT/SE2014/050145 05.02.2014
(87) WO2015/119540 13.08.2015
(45) 25.06.2019 375
(43) 25.10.2016 343
(73) TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (SE)
SE-164 83, Stockholm, Sweden
(72) DUBROVA, Elena (SE), NASLUND, Mats (SE), CARLSSON, Gunnar (SE), FORNEHED, John (SE), SMEETS, Bernard (NL)
(74) Công ty Luật TNHH T&G (TGVN)

(54) THIẾT BỊ ĐIỆN TỬ VÀ PHƯƠNG PHÁP KIỂM TRA MẠCH LOGIC DẠNG SỐ

(57) Sáng chế đề cập tới các thiết bị điện tử (320) bao gồm mạch logic dạng số (101) và môđun kiểm tra (322) được làm thích ứng để nhận các thông số kiểm tra từ thiết bị quản lý kiểm tra từ xa (310), sinh ra các mẫu kiểm tra dựa trên các thông số kiểm tra, áp dụng các mẫu kiểm tra vào mạch logic dạng số, nhận các phản hồi kiểm tra từ mạch logic dạng số, cô đọng các phản hồi kiểm tra vào trong chữ ký kiểm tra, và hoặc là truyền chữ ký kiểm tra tới thiết bị quản lý kiểm tra từ xa hoặc xác định kết quả kiểm tra dựa trên so sánh của chữ ký được mong đợi nhận được từ thiết bị quản lý kiểm tra từ xa với chữ ký kiểm tra. Sáng chế còn đề cập tới thiết bị quản lý kiểm tra từ xa bao gồm các phương tiện được làm thích ứng để thu được các thông số kiểm tra thích hợp để sinh ra các mẫu kiểm tra cho mạch logic dạng số, thu được chữ ký được mong đợi tương ứng với các mẫu kiểm tra, truyền các thông số kiểm tra tới ít nhất một thiết bị điện tử bao gồm mạch logic dạng số, và hoặc nhận chữ ký kiểm tra từ ít nhất một thiết bị điện tử và xác định kết quả kiểm tra dựa trên so sánh của chữ ký được mong đợi với chữ ký kiểm tra, hoặc truyền chữ ký được mong đợi tới ít nhất một thiết bị điện tử.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập tới các thiết bị điện tử bao gồm mạch logic dạng số và môđun kiểm tra để kiểm tra mạch logic dạng số, các thiết bị quản lý kiểm tra từ xa để kiểm tra từ xa các mạch logic dạng số được chứa trong các thiết bị điện tử, các phương pháp tương ứng, các chương trình máy tính tương ứng, và các sản phẩm chương trình máy tính tương ứng.

Tình trạng kỹ thuật của sáng chế

Lỗi phần cứng trong mạch logic dạng số có thể có tác động xấu tới chức năng của nó. Cụ thể, nó áp dụng vào các mạch logic dạng số tạo ra chức năng mã hóa, do việc vận hành an toàn có thể bị ảnh hưởng xấu bởi các lỗi phần cứng. Do đó, mong muốn là các mạch logic dạng số thực hiện các việc tự kiểm tra được tạo ra ở bên trong (Built-In Self-Tests - BIST) trong suốt thời gian hoạt động của chúng. Các mạch tích hợp (Integrated circuit - IC) có chức năng BIST thường tích hợp logic trên chip cho việc sinh ra việc kiểm tra và phân tích phản hồi của việc kiểm tra.

BIST logic (Logic BIST - LBIST), được sử dụng để kiểm tra các mạch logic dạng số, thường áp dụng bộ sinh mẫu giả ngẫu nhiên (Pseudo-Random Pattern Generator - PRPG) để sinh ra các mẫu kiểm tra được áp dụng cho kiểm tra dưới mạch (circuit-under-test - CUT), và thanh ghi chữ ký nhiều đầu vào (Multiple Input Signature Register - MISR) để thu được phản hồi đã được cô đọng, còn được gọi là chữ ký, của CUT cho các mẫu kiểm tra này. Đầu ra MISR không chính xác sẽ chỉ thị lỗi trong CUT.

LBIST thường được sử dụng trong kết hợp với thiết kế quét, là kỹ thuật thiết kế cho kiểm tra, tạo ra cách đơn giản để thiết lập và quan sát từng ô, hoặc thành phần lưu trữ, trong mạch logic dạng số. Trong thiết kế quét, tất cả các thành phần lưu giữ của mạch logic dạng số được kết nối vào trong một hoặc nhiều thanh ghi dịch, được gọi là các chuỗi quét, bằng cách dồn kênh các đầu vào tương ứng của chúng để trợ giúp chế độ quét cho phép tải và dỡ tải nối tiếp của nội dung của chuỗi quét. Với mỗi chuỗi

quét, mẫu kiểm tra được tải vào trong chuỗi của các thành phần lưu giữ, và trạng thái của mọi thành phần lưu giữ sẽ được đọc ra. Trong chế độ vận hành bình thường, các chuỗi quét không ảnh hưởng tới việc vận hành của mạch.

LBIST thường được quản lý và được điều khiển chung bởi đơn vị điều khiển hoặc nằm trên CUT hoặc trên cùng một bảng mạch như là CUT. Đơn vị điều khiển khởi tạo LBIST bằng cách tạo ra các thông số kiểm tra tới PRPG, như trị số khởi tạo và số các mẫu kiểm tra cần được sinh ra, dựa trên đó PRPG sinh ra các mẫu kiểm tra mà sau đó được áp dụng cho CUT. Sau đó, các phản hồi kiểm tra được nhận được từ CUT được cô đọng bởi MISR vào trong chữ ký được so sánh với chữ ký được mong đợi để xác định kết quả kiểm tra. Các thông số kiểm tra và chữ ký được mong đợi được lưu giữ trong bộ nhớ hoặc được gắn cứng. Thông thường, LBIST được thực hiện một cách tự động khi bật nguồn hoặc khi khởi động lại, hoặc trong phản hồi với kích hoạt từ bên ngoài, tức là, nếu phần cứng hoặc phần mềm quan sát chip chỉ ra lỗi. Ngoài ra, LBIST có thể được khởi tạo bởi bộ phận vận hành, tức là, cho các mục đích gỡ lỗi khi chip lỗi được gửi đi sửa chữa.

Trong LBIST đã biết, cùng một bộ các mẫu kiểm tra được sử dụng cho mọi thời điểm mà việc kiểm tra được thực hiện. Đó là do thực tế là PRPG luôn bắt đầu từ cùng một trạng thái khởi tạo, được xác định bởi trị số khởi tạo được tạo ra trong suốt quá trình sản xuất, và một cách tương ứng sinh ra cùng một bộ các mẫu kiểm tra. Hơn nữa, chữ ký kiểm tra thu được bằng cách tích tụ và cô đọng các phản hồi kiểm tra được so sánh với cùng một chữ ký được mong đợi được lưu giữ hoặc được gắn cứng trong chip và được tạo ra trong quá trình sản xuất. Nó mở cửa cho các Trojan phần cứng, tức là các điều chỉnh có hại của các thành phần mạch trong suốt quá trình sản xuất, không thay đổi chữ ký được tạo bởi MISR. Điều này là có thể do các phản hồi kiểm tra của CUT được tích tụ và được cô đọng vào trong chữ ký, và khả năng mà mạch lỗi tạo ra cùng một chữ ký như mạch chính xác là khác không. Phần sau thường được được đề cập tới như là "lỗi sai số lấy mẫu - aliasing error". Hiệu quả của tấn công này hiện được minh họa cho bộ sinh số ngẫu nhiên phần cứng của Intel trong bộ xử lý Ivy Bridge, được xem xét là an ninh về mặt mã hóa và được bảo vệ bởi LBIST truyền thống (G. T. Becker, F. Regazzoni, C. Paar, and W. P. Burleson, "Stealthy Dopant-

Level Hardware Trojans", trong "Cryptographic Hardware and Embedded Systems - CHES 2013", ghi chú cho bài giảng trong tài liệu "Computer Science, Volume 8086, Springer Berlin Heidelberg, 2013", các trang 197–214).

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là để đề xuất cách cải tiến so với các các kỹ thuật nêu trên và so với tình trạng kỹ thuật của sáng chế.

Cụ thể hơn, mục đích của sáng chế là để đề xuất việc kiểm tra logic được xây dựng bên trong được cải tiến của các thiết bị điện tử bao gồm mạch logic dạng số, và cụ thể là việc kiểm tra logic xây dựng bên trong có khả năng phát hiện các biến đổi có hại của các thành phần mạch của mạch logic dạng số. Mục đích khác của sáng chế là để đề xuất việc che phủ kiểm tra được cải tiến và để cho phép kiểm tra từ xa cho lượng lớn tiềm tàng của các thiết bị điện tử có các mạch logic dạng số tương tự.

Có thể đạt được mục đích này và các mục đích khác của sáng chế nhờ các phương tiện của các khía cạnh khác nhau của sáng chế, như được xác định bởi các yêu cầu bảo hộ độc lập. Các phương án thực hiện của sáng chế khác biệt bởi các yêu cầu bảo hộ phụ thuộc.

Theo khía cạnh thứ nhất, sáng chế đề xuất thiết bị điện tử. Thiết bị điện tử bao gồm mạch logic dạng số và môđun kiểm tra. Môđun kiểm tra được làm thích ứng để nhận một hoặc nhiều thông số kiểm tra từ thiết bị quản lý kiểm tra từ xa và để sinh ra một hoặc nhiều mẫu kiểm tra dựa trên các thông số kiểm tra. Môđun kiểm tra còn được làm thích ứng để áp dụng các mẫu kiểm tra vào mạch logic dạng số, nhận một hoặc nhiều phản hồi kiểm tra từ mạch logic dạng số, cô đọng các phản hồi kiểm tra vào trong chữ ký kiểm tra, và truyền chữ ký kiểm tra tới thiết bị quản lý kiểm tra từ xa.

Theo khía cạnh thứ hai, sáng chế đề xuất thiết bị điện tử. Thiết bị điện tử bao gồm mạch logic dạng số và môđun kiểm tra. Môđun kiểm tra được làm thích ứng để nhận một hoặc nhiều thông số kiểm tra từ thiết bị quản lý kiểm tra từ xa và để sinh ra một hoặc nhiều mẫu kiểm tra dựa trên các thông số kiểm tra. Môđun kiểm tra còn được làm thích ứng để áp dụng các mẫu kiểm tra vào mạch logic dạng số, nhận một hoặc nhiều phản hồi kiểm tra từ mạch logic dạng số, cô đọng các phản hồi kiểm tra

vào trong chữ ký kiểm tra, nhận chữ ký mong đợi tương ứng với các mẫu kiểm tra từ thiết bị quản lý kiểm tra từ xa, và xác định kết quả kiểm tra. Kết quả kiểm tra được xác định dựa trên so sánh của chữ ký được mong đợi với chữ ký kiểm tra.

Theo khía cạnh thứ ba, sáng chế đề xuất thiết bị quản lý kiểm tra từ xa. Thiết bị quản lý kiểm tra từ xa bao gồm các phương tiện được làm thích ứng để thu được một hoặc nhiều thông số kiểm tra là thích hợp để sinh ra một hoặc nhiều mẫu kiểm tra cho mạch logic dạng số. Các phương tiện còn được làm thích ứng để thu được chữ ký được mong đợi tương ứng với các mẫu kiểm tra, và truyền các thông số kiểm tra tới ít nhất một thiết bị điện tử bao gồm mạch logic dạng số. Các phương tiện còn được làm thích ứng để nhận chữ ký kiểm tra từ ít nhất một thiết bị điện tử, và xác định kết quả kiểm tra dựa trên so sánh của chữ ký được mong đợi với chữ ký kiểm tra.

Theo khía cạnh thứ tư, sáng chế đề xuất thiết bị quản lý kiểm tra từ xa. Thiết bị quản lý kiểm tra từ xa bao gồm các phương tiện được làm thích ứng để thu được một hoặc nhiều thông số kiểm tra là thích hợp để sinh ra một hoặc nhiều mẫu kiểm tra cho mạch logic dạng số. Các phương tiện còn được làm thích ứng để thu được chữ ký được mong đợi tương ứng với các mẫu kiểm tra, truyền các thông số kiểm tra tới ít nhất một thiết bị điện tử bao gồm mạch logic dạng số và truyền chữ ký được mong đợi tới ít nhất một thiết bị điện tử.

Theo khía cạnh thứ năm, sáng chế đề xuất phương pháp kiểm tra mạch logic dạng số được chứa trong thiết bị điện tử. Phương pháp được thực hiện bởi thiết bị điện tử. Phương pháp bao gồm bước nhận một hoặc nhiều thông số kiểm tra từ thiết bị quản lý kiểm tra từ xa và sinh ra một hoặc nhiều mẫu kiểm tra dựa trên các thông số kiểm tra. Phương pháp còn bao gồm bước áp dụng các mẫu kiểm tra cho mạch logic dạng số, nhận một hoặc nhiều phản hồi kiểm tra từ mạch logic dạng số, cô đọng các phản hồi kiểm tra vào trong chữ ký kiểm tra, và truyền chữ ký kiểm tra tới thiết bị quản lý kiểm tra từ xa.

Theo khía cạnh thứ sáu, sáng chế đề xuất phương pháp kiểm tra mạch logic dạng số được chứa trong thiết bị điện tử. Phương pháp được thực hiện bởi thiết bị điện tử. Phương pháp bao gồm bước nhận một hoặc nhiều thông số kiểm tra từ thiết bị quản lý kiểm tra từ xa và sinh ra một hoặc nhiều mẫu kiểm tra dựa trên các thông số kiểm tra.

Phương pháp còn bao gồm bước áp dụng các mẫu kiểm tra vào mạch logic dạng số, nhận một hoặc nhiều phản hồi kiểm tra từ mạch logic dạng số, cô đọng các phản hồi kiểm tra vào trong chữ ký kiểm tra, nhận chữ ký được mong đợi tương ứng với các mẫu kiểm tra từ thiết bị quản lý kiểm tra từ xa, và xác định kết quả kiểm tra dựa trên so sánh của chữ ký được mong đợi với chữ ký kiểm tra.

Theo khía cạnh thứ bảy, sáng chế đề xuất phương pháp kiểm tra mạch logic dạng số được chứa trong thiết bị điện tử. Phương pháp được thực hiện bởi thiết bị quản lý kiểm tra từ xa. Phương pháp bao gồm bước thu được một hoặc nhiều thông số kiểm tra là thích hợp để sinh ra một hoặc nhiều mẫu kiểm tra cho mạch logic dạng số. Phương pháp còn bao gồm bước thu được chữ ký được mong đợi tương ứng với các mẫu kiểm tra và truyền các thông số kiểm tra tới ít nhất một thiết bị điện tử bao gồm mạch logic dạng số. Phương pháp còn bao gồm bước nhận chữ ký kiểm tra từ ít nhất một thiết bị điện tử, và xác định kết quả kiểm tra dựa trên so sánh của chữ ký được mong đợi với chữ ký kiểm tra.

Theo khía cạnh thứ tám, sáng chế đề xuất phương pháp kiểm tra mạch logic dạng số được chứa trong thiết bị điện tử. Phương pháp được thực hiện bởi thiết bị quản lý kiểm tra từ xa. Phương pháp bao gồm bước thu được một hoặc nhiều thông số kiểm tra là thích hợp để sinh ra một hoặc nhiều mẫu kiểm tra cho mạch logic dạng số. Phương pháp còn bao gồm bước thu được chữ ký được mong đợi tương ứng với các mẫu kiểm tra, truyền các thông số kiểm tra tới ít nhất một thiết bị điện tử bao gồm mạch logic dạng số và truyền chữ ký được mong đợi tới ít nhất một thiết bị điện tử.

Theo các khía cạnh khác, sáng chế đề xuất các chương trình máy tính bao gồm các lệnh thực thi được bởi máy tính. Các lệnh thực thi được bởi máy tính làm cho thiết bị, khi được thực thi trên đơn vị xử lý được chứa trong thiết bị, thực hiện phương pháp theo khía cạnh bất kỳ trong số các khía cạnh thứ nhất, thứ hai, thứ ba hoặc thứ tư của sáng chế được mô tả ở trên.

Theo khía cạnh khác nữa, sáng chế đề xuất sản phẩm chương trình máy tính bao gồm môi trường lưu trữ đọc được bởi máy tính. Môi trường lưu trữ đọc được bởi máy tính có các chương trình máy tính theo các khía cạnh của sáng chế được chứa ở trên đó.

Theo văn cảnh này, thiết bị điện tử theo phương án thực hiện của sáng chế bao gồm mạch logic dạng số áp dụng ít nhất một phần của chức năng mà thiết bị điện tử cung cấp. Ví dụ, mạch logic dạng số có thể áp dụng chức năng mã hóa, như bộ sinh số giả ngẫu nhiên hoặc mật mã luồng. Thiết bị điện tử được tạo ra với môđun kiểm tra cho mục đích kiểm tra mạch logic dạng số và có thể còn bao gồm các loại mạch khác với mạch logic dạng số, mà các loại mạch khác không được kiểm tra bởi các phương án thực hiện của sáng chế. Môđun kiểm tra có thể được tích hợp với mạch logic dạng số, tức là, vào trong IC đơn, hoặc được tạo ra cùng nhau với mạch logic dạng số, tức là, trên bảng mạch chung. Thiết bị điện tử có thể được chứa trong thiết bị mã hóa, tức là mạch mã hóa. Thiết bị điện tử cũng có thể được chứa trong thiết bị đầu cuối di động, như thiết bị người sử dụng (User Equipment - UE), điện thoại di động, điện thoại thông minh, thẻ thông minh, máy tính bảng, hoặc loại thiết bị từ máy tới máy (Machine-to-Machine - M2M) hoặc loại vạn vật nối tới Internet (Internet-of-Things - IoT).

Sáng chế tạo ra việc sử dụng của việc sử dụng của LBIST truyền thống, sử dụng cùng một bộ các mẫu kiểm tra để kiểm tra mạch logic dạng số, CUT, và cùng một chữ ký được mong đợi cho mọi thời điểm kiểm tra được thực hiện, phục hồi CUT được giám sát có thể bị tổn tương cho các Trojan phần cứng khai thác lỗi sai số lấy mẫu của MISR. Đó là do thực tế là các điều chỉnh có hại của các thành phần mạch có thể được thực hiện trong suốt quá trình sản xuất mà không thay đổi chữ ký được tạo ra bởi MISR khi cô đọng các phản hồi kiểm tra của mạch được biến đổi, do chữ ký thể hiện phản hồi tích tụ của CUT tới toàn bộ bộ các mẫu kiểm tra.

Các phương án thực hiện của sáng chế làm giảm nhẹ vấn đề này bằng cách tạo ra thiết bị điện tử và thiết bị quản lý kiểm tra từ xa được làm thích ứng để thực hiện các kiểm tra logic theo cách phối hợp. Cụ thể hơn, có thể đạt được điều này bằng cách truyền các thông số kiểm tra từ thiết bị quản lý kiểm tra từ xa tới thiết bị điện tử và sinh ra các mẫu kiểm tra dựa trên các thông số kiểm tra nhận được từ thiết bị quản lý kiểm tra từ xa. Bên cạnh việc tạo ra các thông số kiểm tra, thiết bị quản lý kiểm tra từ xa cũng tạo ra chữ ký được mong đợi tương ứng với bộ các mẫu kiểm tra được sinh ra bởi thiết bị điện tử để phát hiện các lỗi phần cứng trong mạch logic dạng số, bao gồm

các điều chỉnh có tác động xấu của mạch logic dạng số. Có thể đạt được điều này bằng cách so sánh chữ ký kiểm tra, thu được bằng cách cô đọng các phản hồi kiểm tra từ mạch logic dạng số, với chữ ký được mong đợi. So sánh của chữ ký kiểm tra với chữ ký được mong đợi hoặc được thực hiện tại thiết bị quản lý kiểm tra từ xa hoặc tại thiết bị điện tử. Nếu nó được thực hiện tại thiết bị quản lý kiểm tra từ xa, thì chữ ký kiểm tra được truyền từ thiết bị điện tử tới thiết bị quản lý kiểm tra từ xa cho việc so sánh với chữ ký được mong đợi sau đó. Nếu được thực hiện tại thiết bị điện tử, thì chữ ký được mong đợi được truyền từ thiết bị quản lý kiểm tra từ xa tới thiết bị điện tử cho việc so sánh với chữ ký kiểm tra sau đó.

Các phương án thực hiện của sáng chế có lợi thế hơn so với LBIST truyền thống ở chỗ các bộ khác nhau của các mẫu kiểm tra có thể được sử dụng tại mọi thời điểm khi việc kiểm tra được thực hiện, nhờ đó cải thiện khả năng che phủ kiểm tra. Cụ thể, bằng cách sử dụng các trị số khởi tạo khác nhau, PRPG sinh ra các mẫu kiểm tra bắt đầu từ trạng thái khởi tạo khác, tạo thành các chuỗi khác nhau của các mẫu kiểm tra. Sẽ có lợi nếu việc cung cấp của các Trojan phần cứng trong suốt quá trình sản xuất bị cản trở, cho lý do trong đó đối thủ không có hiểu biết hoàn chỉnh về các mẫu kiểm tra sẽ được sinh ra trong suốt thời gian sống của mạch logic dạng số, CUT.

Cần đặc biệt chú ý là việc sinh ra của các chữ ký được mong đợi có nhu cầu về tính toán rất cao, do nó là dựa trên mô phỏng của mạch logic dạng số cần được kiểm tra, tức là, thiết kế của mạch logic dạng số. Do đó, sẽ không có lợi nếu sinh ra các chữ ký được mong đợi tại thiết bị điện tử, do cách tiếp cận này sẽ làm tăng một cách đáng kể độ phức tạp của thiết bị điện tử cũng như diện tích chip và việc tiêu tốn năng lượng của nó. Cũng không có lợi để lưu giữ một lượng lớn các chữ ký được mong đợi được sinh ra từ trước, tạo thành việc tăng đáng kể của các yêu cầu lưu giữ. Các khía cạnh này là rất quan trọng cho việc kiểm tra được tạo ra bên trong của các thiết bị đầu cuối di động, và cụ thể là cho các thiết bị M2M/IoT đặc trưng bởi các nguồn tài nguyên tính toán bị hạn chế và nói chung là được cấp nguồn pin bị hạn chế.

Các phương án thực hiện của sáng chế tạo ra kiểm tra logic của các mạch logic dạng số với việc bảo vệ được cải tiến chống lại các Trojan phần cứng cũng như khả năng che phủ kiểm tra được cải thiện. Bên cạnh đó, cách tiếp cận kiểm tra từ xa được

bộc lộ ở đây là có lợi trong các tình huống M2M/IoT do nó cho phép quản lý kiểm tra từ xa và phát hiện các lỗi trong số lượng lớn tiềm tàng các thiết bị. Nó áp dụng cụ thể là cho kiểm tra một đối nhiều của số lớn các thiết bị tương tự, hoặc số lượng lớn các thiết bị, bao gồm các mạch logic dạng số tương tự.

Theo một phương án thực hiện sáng chế, kết quả kiểm tra được xác định như là chỉ thị của lỗi trong mạch logic dạng số nếu chữ ký được mong đợi khác với chữ ký kiểm tra. Theo cách khác, nếu chữ ký kiểm tra thu được bằng cách cô đọng các phản hồi kiểm tra được tích tụ nhận được từ mạch logic dạng số là khác với chữ ký được mong đợi, thì lỗi sẽ được chỉ thị. Nghĩa là, kiểm tra đã thất bại. Trái lại, kết quả kiểm tra được xác định như là chỉ thị của việc đã vượt qua phần kiểm tra.

Theo một phương án thực hiện sáng chế, thông tin thuộc về kết quả kiểm tra được truyền từ thiết bị điện tử tới thiết bị quản lý kiểm tra từ xa. Nó áp dụng cho các phương án thực hiện của sáng chế thực hiện so sánh chữ ký kiểm tra với chữ ký được mong đợi trong thiết bị điện tử. Thông tin được truyền có thể bao gồm kết quả kiểm tra, tức là, thông tin chỉ thị xem liệu kiểm tra là thất bại hay đã được vượt qua.

Theo một phương án thực hiện sáng chế, môđun kiểm tra còn được làm thích ứng để thực hiện các bài tự kiểm tra logic trên mạch logic dạng số. Các kiểm tra này, có thể, tức là được thực hiện khi bật nguồn hoặc khi khởi động lại, hoặc trong phản ứng với kích hoạt từ bên ngoài. Về phía này, môđun kiểm tra sinh ra một hoặc nhiều mẫu kiểm tra dựa trên các thông số kiểm tra được lưu giữ hoặc được cài cứng, áp dụng các mẫu kiểm tra tới mạch logic dạng số, cô đọng các đầu ra kiểm tra nhận được từ mạch logic dạng số vào trong chữ ký kiểm tra, và so sánh chữ ký kiểm tra với chữ ký được mong đợi đã được lưu hoặc được cài cứng.

Theo một phương án thực hiện sáng chế, các phương tiện của thiết bị quản lý kiểm tra từ xa còn được làm thích ứng để thu được các chữ ký được mong đợi bằng cách tính toán các chữ ký được mong đợi dựa trên các thông số kiểm tra và thiết kế của mạch logic dạng số. Như được thảo luận ở trên, việc tính toán các chữ ký được mong đợi nhờ các phương pháp mô phỏng mạch logic dạng số là có yêu cầu về tính toán rất cao và do đó là không hiệu quả để được thực hiện tại thiết bị điện tử. Theo cách thay thế, các chữ ký được mong đợi được sinh ra từ trước có thể được lưu giữ,

tức là trong cơ sở dữ liệu, tại thiết bị quản lý kiểm tra từ xa hoặc tại bộ phận lưu trữ bên ngoài có thể truy cập được bởi thiết bị quản lý kiểm tra từ xa.

Mặc dù các ưu điểm của sáng chế trong một số trường hợp đã được mô tả với tham khảo tới các phương án thực hiện của khía cạnh cụ thể của sáng chế, nhưng lý do tương ứng cũng có thể áp dụng cho các phương án thực hiện của các khía cạnh khác của sáng chế.

Các mục đích khác, các đặc điểm khác và các ưu điểm với sáng chế sẽ trở nên rõ ràng khi nghiên cứu phần bộc lộ chi tiết dưới đây cùng với các hình vẽ và các yêu cầu bảo hộ kèm theo. Những người có hiểu biết trung bình trong lĩnh vực sẽ hiểu rõ rằng các dấu hiệu khác nhau của sáng chế có thể được kết hợp để tạo ra các phương án khác với các phương án được mô tả dưới đây.

Mô tả vắn tắt các hình vẽ

Các mục đích, đặc điểm và ưu điểm nêu trên cũng như các mục đích, đặc điểm và ưu điểm khác của sáng chế sẽ được hiểu rõ hơn nhờ phần minh họa kèm theo và phần mô tả chi tiết và không làm hạn chế của các phương án thực hiện sáng chế, với tham khảo tới các hình vẽ kèm theo, trong đó:

Fig.1 thể hiện giản đồ khối của IC đã biết với chức năng LBIST.

Fig.2 thể hiện giản đồ khối chức năng của môđun LBIST đã biết.

Fig.3 minh họa một cách sơ lược việc kiểm tra từ xa theo một phương án thực hiện của sáng chế.

Fig.4 thể hiện thiết bị điện tử theo một phương án thực hiện của sáng chế.

Fig.5 thể hiện môđun kiểm tra theo một phương án thực hiện của sáng chế.

Fig.6 thể hiện môđun kiểm tra theo một phương án thực hiện khác của sáng chế.

Fig.7 thể hiện phương pháp kiểm tra được thực hiện bởi thiết bị điện tử, theo một phương án thực hiện của sáng chế.

Fig.8 thể hiện phương pháp kiểm tra được thực hiện bởi thiết bị điện tử, theo một phương án thực hiện khác của sáng chế.

Fig.9 thể hiện phương pháp kiểm tra được thực hiện bởi thiết bị quản lý kiểm tra từ xa, theo một phương án thực hiện của sáng chế.

Fig.10 thể hiện phương pháp kiểm tra được thực hiện bởi thiết bị quản lý kiểm tra từ xa, theo một phương án thực hiện khác của sáng chế.

Fig.11 thể hiện IC, theo một phương án thực hiện của sáng chế.

Fig.12 thể hiện SoM, theo một phương án thực hiện của sáng chế.

Fig.13 thể hiện thiết bị đầu cuối di động, theo một phương án thực hiện của sáng chế.

Tất cả các hình vẽ là sơ lược, không nhất thiết phải cùng tỉ lệ, và thường chỉ thể hiện các phần cần thiết để làm rõ sáng chế, trong đó, các phần khác có thể bị bỏ qua hoặc đơn giản là được đề xuất.

Mô tả chi tiết sáng chế

Sáng chế sẽ được mô tả chi tiết hơn dưới đây có dựa vào các hình vẽ kèm theo, trong đó các phương án cụ thể của sáng chế sẽ được thể hiện. Tuy nhiên, sáng chế có thể được thể hiện dưới các dạng khác nhau và không nên được hiểu là chỉ giới hạn ở các phương án được trình bày trong bản mô tả này. Đúng hơn là, các phương án này được đưa ra theo cách ví dụ để giúp bản mô tả trở nên toàn diện và đầy đủ, và sẽ chuyển tải đầy đủ phạm vi của sáng chế đến các chuyên gia trong lĩnh vực.

Trên Fig.1, IC 100 được minh họa như là một ví dụ cho thiết bị điện tử với chức năng LBIST truyền thống. IC 100 có thể, tức là, là bộ vi xử lý, IC ứng dụng cụ thể (Application-Specific IC - ASIC), hoặc mạng cổng lập trình được bằng trường (Field-Programmable Gate Array - FPGA). Nó cũng có thể là một phần của IC lớn hơn, hệ thống trên chip (System-on-Chip - SoC), tức là, IC tích hợp tất cả các thành phần của hệ thống điện tử vào trong chip đơn, hệ thống trong gói (System-in-Package - SiP), là nhiều mạch tích hợp được bao trong một môđun hoặc gói đơn, hoặc hệ thống trên môđun (System-on-Module - SoM), là máy tính được nhúng toàn bộ được xây dựng trên một bảng mạch đơn. IC 100 bao gồm mạch logic dạng số 101, CUT, áp dụng ít nhất một phần của chức năng mà IC 100 tạo ra, và môđun LBIST 102 để thực hiện các kiểm tra logic trên CUT 101.

Môđun LBIST 102, được minh họa chi tiết hơn trên Fig.2, bao gồm PRPG 201, có thể dựa trên thanh ghi dịch phản hồi tuyến tính (Linear Feedback Shift Register - LFSR), để sinh ra các mẫu kiểm tra giả ngẫu nhiên mà trong suốt kiểm tra được áp dụng cho CUT 101 thông qua các đầu vào kiểm tra 111. Mẫu kiểm tra bao gồm nhiều trị số nhị phân, một trị số cho mỗi đầu vào kiểm tra 111. Các mẫu kiểm tra được sinh ra dựa trên một hoặc nhiều thông số kiểm tra được lưu giữ 202 hoặc được gắn cứng 202 trong môđun LBIST 102. Thông thường, các thông số kiểm tra bao gồm trị số khởi tạo, xác định trạng thái ban đầu của PRPG 201, và số các mẫu kiểm tra cần được tạo ra. Môđun LBIST 102 còn bao gồm MISR 203 để cô đọng các phản hồi kiểm tra nhận được từ CUT 101 thông qua các đầu vào kiểm tra 112, cùng được đề cập tới như là "dữ liệu trụ - stump data", vào trong chữ ký kiểm tra, và logic quyết định 204 để so sánh chữ ký kiểm tra thu được từ MISR 203 tới chữ ký được mong đợi được lưu giữ 205 hoặc được gắn cứng 205 trong môđun LBIST 102. Kết quả của so sánh này được tạo ra sẵn sàng nhờ các phương tiện của tín hiệu 115 chỉ thị kết quả kiểm tra tới mạch bên ngoài, tức là đơn vị giám sát lỗi được tạo ra cùng với IC 100. Môđun LBIST 102 còn bao gồm bộ điều khiển 206 để điều khiển việc vận hành của môđun LBIST 102 và CUT 101 nhờ các phương tiện của một hoặc nhiều tín hiệu điều khiển 113. Bộ điều khiển 206 tùy chọn thực hiện các chuỗi của các kiểm tra logic một cách tự trị, tức là, tại thời điểm bật nguồn hoặc khởi động lại, để đáp ứng lại với điều kiện lỗi được phát hiện, hoặc đáp ứng lại với kích hoạt từ bên ngoài nhận được thông qua đầu vào điều khiển tùy chọn 114. Đầu vào điều khiển 114 cũng có thể được sử dụng để đảo chiều IC 100 giữa chế động vận hành thông thường và chế độ kiểm tra, hoặc để khởi tạo chu kỳ kiểm tra, và có thể, tức là, được kết nối tới bộ phận giám sát lỗi được tạo ra cùng với IC 100.

LBIST thường được sử dụng trong kết hợp với thiết kế quét, là kỹ thuật thiết kế cho kiểm tra, tạo ra cách đơn giản để thiết lập và quan sát từng ô, hoặc thành phần lưu trữ, trong mạch logic dạng số như CUT 101. Trong thiết kế quét, các ô của mạch logic dạng số, như CUT 101, được kết nối vào trong một hoặc nhiều thanh ghi dịch, được gọi là các chuỗi quét 114. Các chuỗi quét 114 được tạo ra với các đầu vào kiểm tra 111 được dồn kênh (các bộ dồn kênh không được thể hiện trên Fig.2) để trợ giúp chế độ

quét cho phép tải và dỡ tại nối tiếp của các nội dung của các chuỗi quét 114 thông qua các đầu vào kiểm tra 111 và các đầu ra kiểm tra 112, một cách tương ứng. Các chuỗi quét được xác định trong suốt thiết kế mạch và là biểu diễn cho hiệu quả vận hành kiểm tra của các phần của CUT. Thông thường, các chuỗi quét được định vị trước và sau, tức là, xen kẽ với, các phần của các mạch chức năng của CUT theo cách mà mỗi phần chức năng có (i) "chuỗi quét trước đó" tạo ra các đầu vào cho các thành phần mạch của phần chức năng này, và (ii) "chuỗi quét sau đó" nhận các đầu ra của phần chức năng.

Chu kỳ kiểm tra thường bao gồm chế độ quét chọn và nạp nối tiếp mẫu kiểm tra vào trong các chuỗi quét 114 thông qua các đầu vào kiểm tra 111. Khi các chuỗi quét 114 được nạp đầy, chế độ vận hành thông thường của CUT 101 sẽ được chọn, thông qua các tín hiệu điều khiển 113, và một chu kỳ đồng hồ được áp dụng, nhờ đó áp dụng mẫu kiểm tra được tải cho các đầu vào của logic kết hợp được áp dụng bởi CUT 101. Phản hồi của CUT 101 với các trị số đầu vào được xác định bởi các mẫu kiểm tra được tạo ra sẵn sàng tại các đầu vào kiểm tra 112 của logic kết hợp. Cuối cùng, chế độ quét của CUT 101 được chọn lại lần nữa, và một chu kỳ đồng hồ được áp dụng để dỡ tải các trị số đầu ra của các chuỗi quét 114 qua các đầu ra kiểm tra 112. Trong khi các đầu ra bị dịch chuyển ra khỏi các chuỗi quét 114, mẫu kiểm tra tiếp theo có thể được tải vào trong các chuỗi quét 114. MISR 203 cô đọng và tích tụ các phản hồi kiểm tra nhận được thông qua các đầu vào kiểm tra 112 vào trong chữ ký kiểm tra mà sau đó được so sánh, bởi logic quyết định 204, tới chữ ký được mong đợi được lưu giữ 205 hoặc được gắn cứng 205 trong môđun LBIST 102. Đầu ra MISR không chính xác, tức là, chữ ký khác với chữ ký được mong đợi, tức là, chữ ký của CUT 101 không có lỗi, sẽ chỉ thị lỗi.

Trong LBIST truyền thống, như được mô tả ở đây với tham khảo tới các hình vẽ Fig. 1 và Fig.2, cùng một bộ các mẫu kiểm tra được áp dụng cho CUT 101 mọi lần mà các kiểm tra logic được thực hiện, tức là mọi lần mà chu kỳ kiểm tra được thực thi. Đó là do thực tế là các thông số kiểm tra, trạng thái khởi tạo của PRPG 201 và số các mẫu kiểm tra cần được tạo ra, cũng như chữ ký tương ứng được mong đợi, cần phải được lưu giữ hoặc gắn cứng trong IC 100. Các nhược điểm của cách tiếp cận của tình trạng

kỹ thuật của sáng chế bị gấp đôi. Thứ nhất, do cùng một bộ các mẫu kiểm tra được sử dụng mọi thời điểm khi các kiểm tra logic được thực hiện trong suốt thời gian tồn tại của IC 100, và bộ các mẫu kiểm tra là đã biết khi chip được sản xuất, chip là dễ bị tổn thương cho các Trojan phần cứng khai thác lỗi sai số lấy mẫu của MISR 203. Đối thủ có thể khai thác hiểu biết của các mẫu kiểm tra và chữ ký được mong đợi tương ứng cho việc biến đổi có hại các thành phần mạch trong suốt quy trình sản xuất, sao cho chữ ký kiểm tra được tạo ra bởi MISR cho kiểm tra của bộ các véctơ là giống như của thiết kế mạch ban đầu. Thứ hai, do các mẫu kiểm tra được sinh ra theo cách giả ngẫu nhiên, nên một số lớn các mẫu kiểm tra được yêu cầu để đạt được việc che phủ kiểm tra đáp ứng yêu cầu, thường là ở cỡ 10.000 mẫu kiểm tra hoặc nhiều hơn. Hạn chế trong kích cỡ của bộ kiểm tra xuất phát từ yêu cầu rằng chu kỳ kiểm tra được mong đợi được hoàn thành trong thời gian hợp lý, phụ thuộc vào ứng dụng hiện có. Ví dụ, với trạm cơ sở vô tuyến hoặc nút khác của mạng truy cập vô tuyến, chu kỳ kiểm tra cho việc kiểm tra tại chỗ thường được mong đợi để hoàn thiện trong khoảng thời gian ít hơn mười giây. Do đó, sẽ không có lợi để tăng một cách đáng kể kích cỡ của bộ kiểm tra, tức là bộ kiểm tra của các mẫu kiểm tra, như nó sẽ tạo thành việc tăng đáng kể của thời gian thực thi chu kỳ kiểm tra. Sử dụng các bộ kiểm tra khác nhau cho từng chu kỳ kiểm tra để cải thiện việc che phủ kiểm tra là không có lợi do mỗi bộ các mẫu kiểm tra yêu cầu chữ ký được mong đợi tương ứng để xác định xem liệu chip có vượt qua kiểm tra hay không. Trong khi sinh ra các mẫu kiểm tra bởi PRPG là không có quá nhiều yêu cầu về mặt tính toán, việc sinh ra chữ ký được mong đợi tương ứng tạo thành nỗ lực tính toán đáng kể, do nó yêu cầu việc mô phỏng logic tổ hợp được áp dụng bởi CUT trong phần mềm, và để tính toán phản hồi của logic tổ hợp được mô phỏng tới từng mẫu kiểm tra. Theo nghĩa khác, bên cạnh CUT, chip sẽ yêu cầu các phương tiện xử lý đủ phức tạp để mô phỏng logic tổ hợp được áp dụng bởi CUT và để tính toán các phản hồi đầu ra của CUT cho các mẫu kiểm tra như là đầu vào. Rõ ràng là, nó sẽ tạo thành việc tăng đáng kể của độ phức tạp của chip. Cũng sẽ hiểu rằng sẽ không có lợi để lưu các chữ ký được sinh ra từ trước cho các bộ kiểm tra thay đổi hoặc lớn, do có việc tăng tương ứng trong các nguồn tài nguyên lưu trữ được yêu cầu.

Trong phần dưới đây, và tham khảo tới các hình vẽ từ Fig. 3 đến Fig.13, việc kiểm tra từ xa theo một phương án thực hiện của sáng chế sẽ được mô tả.

Fig.3 minh họa hệ thống 300 bao gồm thiết bị quản lý kiểm tra từ xa 310 và một hoặc nhiều thiết bị điện tử 320 được sắp xếp để liên lạc với nhau qua mạng truyền thông 301. Thiết bị quản lý kiểm tra từ xa 310 có thể, tức là, là máy tính cá nhân được tạo ra với chương trình máy tính theo một phương án thực hiện của sáng chế, hoặc đơn vị giám sát lỗi dành riêng, như được mô tả chi tiết hơn bên dưới. Thiết bị quản lý kiểm tra từ xa 310 cũng có thể được áp dụng như là máy ảo để thực thi trong môi trường điện toán đám mây.

Mỗi thiết bị trong các thiết bị điện tử 320 bao gồm mạch logic dạng số, CUT 101, và môđun kiểm tra (TM) 322 để thực hiện các kiểm tra logic trên CUT 101, như được mô tả chi tiết hơn bên dưới. Sẽ hiểu rằng, mặc dù các thiết bị điện tử 320 được minh họa trên Fig.3 như là liên lạc trực tiếp với thiết bị quản lý kiểm tra từ xa 310, nhưng các thiết bị điện tử 320 có thể được chứa trong các thiết bị đầu cuối di động, tức là, các UE, các máy tính, các máy tính bảng, các thiết bị M2M, mà qua liên lạc của thiết bị quản lý kiểm tra từ xa 310 được thực hiện qua đó. Mạng truyền thông 301 có thể, tức là, là thành phần bất kỳ, hoặc là tổ hợp của, mạng diện cục bộ (Local Area Network - LAN), LAN không dây (Wireless LAN - WLAN), mạng diện rộng (Wire Area Network - WAN), Internet, mạng của tập đoàn, mạng vô tuyến dạng ô như hệ thống toàn cầu cho liên lạc di động (Global System for Mobile Communications - GSM), hệ thống liên lạc viễn thông di động toàn cầu (Universal Mobile Telecommunications System - UMTS), hoặc cải tiến dài hạn (Long term Evolution - LTE), hoặc mạng bột phát, mạng dạng lưới, hoặc mạng mao dẫn. Liên lạc giữa thiết bị quản lý kiểm tra từ xa 310 và các thiết bị điện tử 320 có thể bị ảnh hưởng bởi các phương tiện của giao thức truyền thông thích hợp bất kỳ trong tình trạng kỹ thuật của sáng chế, tức là, giao thức điều khiển truyền (Transmission Control Protocol - TCP), giao thức gói thông tin người sử dụng (User Datagram Protocol - UDP), hoặc giao thức quản lý thiết bị bất kỳ như TR.069 (Broadband Forum - diễn đàn băng rộng), quản lý thiết bị liên hiện di động mở (Open Mobile Alliance - OMA), hoặc M2M trọng lượng nhẹ OMA (OMA Lightweight M2M).

Các phương án thực hiện của sáng chế thực hiện liểm tra logic của CUT 101 theo cách phân tán, hơn là theo cách tự trị như trong tình trạng kỹ thuật của sáng chế. Về phía này, thiết bị quản lý kiểm tra từ xa 310 thu được các thông số kiểm tra, dựa trên bộ các mẫu kiểm tra nào có thể được sinh ra sử dụng PRPG, và chữ ký được mong đợi tương ứng với bộ các mẫu kiểm tra. Các thông số kiểm tra được truyền, qua mạng truyền thông 301, tới ít nhất một thiết bị trong các thiết bị điện tử 320. Dựa trên các thông số kiểm tra nhận được, thiết bị điện tử 320 sinh ra các mẫu kiểm tra và thực hiện các kiểm tra logic tương tự như LBIST truyền thống được mô tả với tham khảo tới các hình vẽ Fig. 1 và Fig.2. Nghĩa là, các mẫu kiểm tra được sinh ra được áp dụng cho CUT 101 và các phản hồi kiểm tra từ CUT 101 được cô đọng vào trong chữ ký kiểm tra, mà sau đó sẽ được so sáng với chữ ký được mong đợi tương ứng để xác định kết quả kiểm tra, tức là, xem liệu CUT 101 đã qua hay bị thất bại với bộ các mẫu kiểm tra. So sánh có thể hoặc được thực hiện tại thiết bị quản lý kiểm tra từ xa 310 hoặc tại thiết bị điện tử 320. Nếu so sánh được thực hiện tại thiết bị quản lý kiểm tra từ xa 310, thì chữ ký kiểm tra được truyền từ thiết bị điện tử 320 tới thiết bị quản lý kiểm tra từ xa 310, trong đó nó được so sánh với chữ ký được mong đợi và kết quả kiểm tra được xác định một cách tương ứng. Nếu so sánh được thực hiện tại thiết bị điện tử 320, thì chữ ký được mong đợi được truyền từ thiết bị quản lý kiểm tra từ xa 310 đến thiết bị điện tử 320, trong đó nó được so sánh với chữ ký kiểm tra và kết quả kiểm tra được xác định một cách tương ứng.

Bằng cách chọn một cách phù hợp các thông số kiểm tra, các vấn đề được kết hợp với LBIST truyền thống sẽ được làm giảm. Cụ thể, bằng cách truyền các trị số khởi tạo khác nhau xác định trạng thái ban đầu của PRPG, có thể thực hiện các kiểm tra logic sử dụng các bộ kiểm tra khác nhau cho mọi thời điểm mà kiểm tra được thực hiện, đơn giản bằng cách sử dụng các trị số khởi tạo khác nhau, nhờ đó cải thiện việc phát hiện của các Trojan phần cứng. Ngoài ra, kích cỡ của kiểm tra có thể được tăng, trong khi giữ phần đầu liên lạc thấp, bằng cách truyền thông số kiểm tra tới hiệu ứng này, ra lệnh các thiết bị điện tử 320 sinh ra bộ kiểm tra có kích thước mong muốn. Theo cách này, khả năng che phủ kiểm tra có thể được cải thiện. Về phía này, các thông số kiểm tra bao gồm ít nhất một trong số trị số khởi tạo, số các mẫu kiểm tra cần

được tạo ra, và một hoặc nhiều số chuỗi của các mẫu kiểm tra cần được sinh ra. Bằng cách truyền danh sách của một hoặc nhiều số chuỗi tới các thiết bị điện tử theo một phương án thực hiện của sáng chế, bên cạnh trị số khởi tạo, các mẫu kiểm tra cụ thể có thể được chọn và được sinh ra, do đặc điểm tất định của các chuỗi được sinh ra bởi các PRPG. Nhờ đó, các kiểm tra logic có thể được tùy chỉnh cho các phần cụ thể của mạch logic dạng số.

Các phương án thực hiện của sáng chế có ưu điểm ở chỗ nhu cầu về độ phức tạp được tăng cho các IC trợ giúp kiểm tra logic được xây dựng ở trong sẽ thay đổi các bộ kiểm tra, và/hoặc các bộ kiểm tra tạo ra khả năng che phủ kiểm tra sẽ được làm giảm. Bằng cách để thiết bị quản lý kiểm tra từ xa 310, hơn là thiết bị điện tử 320, tính toán hoặc lưu giữ các chữ ký được mong đợi, các hạn chế trong các nguồn tài nguyên tính toán, lưu giữ và pin của thiết bị điện tử 320 sẽ được khắc phục.

Sẽ hiểu rằng việc quản lý kiểm tra từ xa theo các phương án thực hiện của sáng chế có thể được thực hiện theo cách một đối một, như được mô tả ở đây với tham khảo tới Fig.3, hoặc theo cách một đối nhiều. Trong trường hợp sau, các thông số kiểm tra được truyền tới nhiều thiết bị điện tử 320 hoặc là giống nhau hoặc ít nhất là bao gồm các CUT 101 giống nhau, như bộ chung của các mẫu kiểm tra và chữ ký được mong đợi tương ứng có thể được sử dụng. Nếu so sánh của chữ ký kiểm tra với chữ ký được mong đợi được thực hiện tại thiết bị quản lý kiểm tra từ xa 310, thì từng thiết bị điện tử 320 sẽ truyền chữ ký kiểm tra của nó tới thiết bị quản lý kiểm tra từ xa 310, trong đó chúng được so sánh với chữ ký được mong đợi trên cơ sở mỗi thiết bị. Một cách tương ứng, nếu so sánh được thực hiện tại các thiết bị điện tử 320, thì chữ ký được mong đợi sẽ được truyền tới các thiết bị điện tử 320. Kiểm tra một đối nhiều có ưu điểm phụ là ở chỗ chữ ký được mong đợi, việc tính toán của nó là yêu cầu nhiều tính toán, có thể được sử dụng cho việc kiểm tra một số lớn tiềm tàng các thiết bị điện tử giống nhau 320. Nó là đặc biệt quan trong cho các tình huống M2M/IoT trong đó các lượng lớn của các thiết bị nhỏ được triển khai với khả năng tính toán, khả năng lưu trữ và các nguồn tài nguyên pin bị hạn chế. Trong phần sau, sáng chế sẽ được thảo luận trong văn cảnh của kiểm tra một đối một, tức là, thiết bị quản lý kiểm tra từ xa 310 quản lý thiết bị điện tử đơn 320 từ xa. Tuy nhiên, các phương án thực hiện không bị

hạn chế vào việc kiểm tra một đối một và các phương án thực hiện tương ứng cho kiểm tra một đối nhiều có thể được dự tính một cách dễ dàng.

Đề cập tới Fig.3, phương án thực hiện của thiết bị quản lý kiểm tra từ xa 310 hiện được mô tả. Thiết bị quản lý kiểm tra từ xa 310 bao gồm các phương tiện xử lý, như đơn vị xử lý 311 và bộ nhớ 312 bao gồm chương trình máy tính 313, và giao diện mạng (NI) 314, được làm thích ứng để thu được một hoặc nhiều thông số kiểm tra thích hợp để sinh ra một hoặc nhiều mẫu kiểm tra cho mạch logic dạng số, CUT101, được chứa trong một hoặc nhiều thiết bị điện tử 320, và để thu được chữ ký được mong đợi tương ứng với bộ các mẫu kiểm tra. Các thông số kiểm tra có thể, tức là, được cung cấp bởi bộ phận vận hành của thiết bị quản lý kiểm tra từ xa 310 hoặc được truy hồi từ cơ sở dữ liệu 315 mà thiết bị quản lý kiểm tra từ xa 310 được cung cấp với hoặc truy cập vào. Các thông số kiểm tra có thể được thu khi việc kiểm tra được khởi tạo, tức là, được yêu cầu bởi người vận hành, được kích hoạt bởi chỉ thị lỗi nhận được từ một trong số các thiết bị điện tử 320 hoặc từ đơn vị giám sát lỗi, hoặc dựa trên lịch biểu. Các phương tiện còn được làm thích ứng để truyền các thông số kiểm tra tới thiết bị điện tử 320 trong đó chúng được sử dụng để sinh ra các mẫu kiểm tra, như được mô tả chi tiết hơn bên dưới. Các thông số kiểm tra được truyền tới thiết bị điện tử 320 nhờ giao diện mạng 314, thông qua mạng liên lạc 301. Các phương tiện còn được làm thích ứng để nhận chữ ký kiểm tra tương ứng với chữ ký được mong đợi từ thiết bị điện tử 320, và để xác định kết quả kiểm tra dựa trên so sánh của chữ ký được mong đợi với chữ ký kiểm tra nhận được. Chữ ký kiểm tra được nhận từ thiết bị điện tử 320 bởi giao diện mạng 314, thông qua mạng truyền thông 301. Tùy chọn là các phương tiện còn được làm thích ứng để xác định kết quả kiểm tra như là chỉ thị của lỗi trong CUT 101 nếu chữ ký được mong đợi khác với chữ ký kiểm tra nhận được từ thiết bị điện tử 320.

Theo cách khác, các phương tiện được chứa trong thiết bị quản lý kiểm tra từ xa 310 có thể được làm thích ứng để truyền chữ ký được mong đợi đến thiết bị điện tử 320 và, tùy chọn, để nhận thông tin thuộc về kết quả kiểm tra cho các mẫu kiểm tra từ thiết bị điện tử 320, hơn là nhận chữ ký kiểm tra từ thiết bị điện tử 320 và xác định kết quả kiểm tra tại thiết bị quản lý kiểm tra từ xa 310.

Tùy chọn là, các phương tiện được chứa trong thiết bị quản lý kiểm tra từ xa 310 có thể được làm thích ứng để mã hóa liên lạc với thiết bị điện tử 320, tức là, sử dụng vỏ an ninh (Secure Shell - SSH), lớp các khe an ninh (Secure Sockets Layer - SSL), tính an ninh lớp vận chuyển (Transport Layer Security - TSL), IPsec, hoặc dạng tương tự, như đã biết trong tình trạng kỹ thuật của sáng chế. Nghĩa là, các phương tiện được làm thích ứng để mã hóa các thông số kiểm tra, và, tùy chọn là, chữ ký được mong đợi, được truyền tới thiết bị điện tử 320, và để giải mã chữ ký kiểm tra hoặc kết quả kiểm tra được nhận từ thiết bị điện tử 320. Ngoài ra, thiết bị quản lý kiểm tra từ xa 310 có thể được làm thích ứng để xác thực liên lạc với thiết bị điện tử 320, như đã biết trong tình trạng kỹ thuật của sáng chế, nhờ đó loại bỏ các tấn công loại có người tham gia ở giữa và loại mạo nhận.

Tùy chọn nữa là, các phương tiện được làm thích ứng để tính toán chữ ký được mong đợi dựa trên mô phỏng của thiết kế mạch của CUT 101, tức là, logic tổ hợp nằm dưới, sử dụng các mẫu kiểm tra như là đầu vào, như đã biết trong tình trạng kỹ thuật của sáng chế. Theo cách thay thế, chữ ký được mong đợi có thể được lưu giữ trong cơ sở dữ liệu 315 và được truy hồi khi kiểm tra với bộ các mẫu kiểm tra tương ứng với chữ ký được mong đợi được lưu, được thực hiện.

Đề cập tới các hình vẽ Fig. 4 đến Fig.6, các phương án thực hiện của thiết bị điện tử 320 sẽ được mô tả. Tương tự như IC 100 được mô tả với tham khảo tới các hình vẽ Fig. 1 và Fig.2, thiết bị điện tử 320 bao gồm mạch logic dạng số 101, CUT, áp dụng ít nhất một phần của chức năng mà thiết bị điện tử 320 tạo ra, và môđun kiểm tra 322 để thực hiện các kiểm tra logic trên CUT 101. Thiết bị điện tử 320 có thể, tức là, là IC 1100 được minh họa trên Fig.11, bao gồm mạch logic dạng số 1101 và môđun kiểm tra 1102, như bộ vi xử lý, ASIC, hoặc FPGA. Nó cũng có thể là một phần của IC lớn hơn, SoC, SiP 1200, hoặc SoM 1200, được minh họa trên Fig.12, bao gồm mạch logic dạng số 1201 và môđun kiểm tra 1202. Phương án thực hiện của thiết bị điện tử 320 có thể, tức là, được chứa trong mạch mã hóa như là mạch hoặc mật mã luồng để mã hóa và/hoặc giải mã. Hơn nữa, phương án thực hiện của thiết bị điện tử 320 cũng có thể được chứa trong thiết bị đầu cuối di động như điện thoại di động 1300, được minh họa trên Fig.13, bao gồm mạch logic dạng số 1301 và môđun kiểm tra 1302.

Phương án thực hiện 500 của môđun kiểm tra 322 được minh họa trên Fig.5. Tương tự như môđun LBIST 102, môđun kiểm tra 500 bao gồm PRPG 201 để sinh ra các mẫu kiểm tra giả ngẫu nhiên và MISR 203 để cô đọng các phản hồi kiểm tra nhận được từ CUT 101 thông qua các đầu ra kiểm tra 112 vào trong chữ ký kiểm tra. Trái với môđun LBIST 102, các thông số kiểm tra không được lưu giữ hoặc được gắn cứng mà được nhận từ thiết bị quản lý kiểm tra từ xa 310. Về phía này, môđun kiểm tra 500 bao gồm môđun liên lạc 507 được định cấu hình để liên lạc với thiết bị quản lý kiểm tra từ xa qua mạng liên lạc, như thiết bị quản lý kiểm tra từ xa 310 được minh họa trên Fig.3. Cụ thể hơn, môđun liên lạc 507 được định cấu hình để nhận các thông số kiểm tra và cung cấp các thông số kiểm tra nhận được tới PRPG 201, tức là, thông qua môđun 502 được định cấu hình để lưu giữ một cách tạm thời các thông số kiểm tra. Môđun liên lạc 507 còn được định cấu hình để nhận chữ ký kiểm tra từ MISR 203 và để truyền chữ ký kiểm tra tới thiết bị quản lý kiểm tra từ xa.

Bộ điều khiển 506 của môđun kiểm tra 500 bao gồm các phương tiện xử lý, như bộ nhớ 511 lưu giữ chương trình máy tính 512, và đơn vị xử lý 510 thực thi chương trình máy tính 512, mà tại đó bộ điều khiển 506 là vận hành được để điều khiển môđun kiểm tra 500 để thực hiện các kiểm tra logic trong phản hồi để nhận các thông số kiểm tra từ thiết bị quản lý từ xa. Cụ thể hơn, môđun kiểm tra 500 là vận hành được để nhận một hoặc nhiều thông số kiểm tra từ thiết bị quản lý kiểm tra từ xa, thông qua môđun liên lạc 507, sinh ra một hoặc nhiều mẫu kiểm tra dựa trên các thông số kiểm tra nhận được, sử dụng PRPG 201, áp dụng các mẫu kiểm tra cho CUT 101, nhận các phản hồi kiểm tra từ CUT 101, cô đọng các phản hồi kiểm tra vào trong chữ ký kiểm tra, sử dụng MISR 203, và truyền chữ ký kiểm tra tới thiết bị quản lý kiểm tra từ xa, sử dụng môđun liên lạc 507.

Tùy chọn là, bộ điều khiển 506 có thể còn được định cấu hình để thực hiện các kiểm tra logic tự trị, tức là, tại thời điểm bật nguồn hoặc khởi động lại, đáp ứng lại với điều kiện lỗi, hoặc đáp ứng lại với kích hoạt từ bên ngoài nhận được thông qua đầu vào điều khiển tùy chọn 114. Đầu vào điều khiển 114 cũng có thể được sử dụng để đảo chiều thiết bị điện tử 320 giữa chế động vận hành thông thường và chế độ kiểm tra,

hoặc để khởi tạo chu kỳ kiểm tra, và có thể, tức là, được kết nối tới bộ phận giám sát lỗi được tạo ra cùng với thiết bị điện tử 320.

Phương án thực hiện thay thế 600 của môđun kiểm tra 322 hiện sẽ được mô tả với tham khảo tới Fig.6. Tương tự như môđun kiểm tra 500, môđun kiểm tra 600 bao gồm PRPG 201 để sinh ra các mẫu kiểm tra giả ngẫu nhiên và MISR 203 để cô đọng các phản hồi kiểm tra nhận được từ CUT 101 thông qua các đầu ra kiểm tra 112 vào trong chữ ký kiểm tra. Tiếp theo, môđun kiểm tra 600 cũng bao gồm môđun liên lạc 607 được định cấu hình để liên lạc với thiết bị quản lý kiểm tra từ xa qua mạng liên lạc, như thiết bị quản lý kiểm tra từ xa 310 được minh họa trên Fig.3. Tương tự như môđun liên lạc 507, môđun liên lạc 607 được định cấu hình để nhận các thông số kiểm tra và cung cấp các thông số kiểm tra nhận được tới PRPG 201, tức là, thông qua môđun 502 được định cấu hình để lưu giữ một cách tạm thời các thông số kiểm tra.

Môđun kiểm tra 600 còn bao gồm logic quyết định 604 được định cấu hình để so sánh chữ ký kiểm tra thu được từ MISR 203 với chữ ký được mong đợi, như đã biết trong tình trạng kỹ thuật của sáng chế. Tuy nhiên, khác với môđun LBIST 102, chữ ký được mong đợi không được lưu giữ hoặc được gắn cứng trong môđun kiểm tra 600 mà được nhận từ thiết bị quản lý từ xa, thông qua môđun liên lạc 607. Về phía này, môđun liên lạc 607 được định cấu hình để nhận chữ ký được mong đợi và cung cấp chữ ký được mong đợi nhận được tới logic quyết định 604, tức là, thông qua môđun 605 được định cấu hình để tạm thời lưu giữ chữ ký được mong đợi. Logic quyết định 604 có thể còn được định cấu hình để cung cấp kết quả của so sánh, tức là, kết quả kiểm tra, tới môđun liên lạc 607 có thể còn được định cấu hình để truyền thông tin thuộc về kết quả kiểm tra tới thiết bị quản lý từ xa. Còn tùy chọn nữa, logic quyết định 604 có thể được định cấu hình để tạo ra sự sẵn có cho kết quả kiểm tra tới mạch bên ngoài, tức là, đơn vị giám sát lỗi cùng với thiết bị điện tử 320, nhờ các phương tiện của tín hiệu 115.

Bộ điều khiển 606 của môđun kiểm tra 600 bao gồm các phương tiện xử lý, như bộ nhớ 611 lưu giữ chương trình máy tính 612, và đơn vị xử lý 610 thực thi chương trình máy tính 612, mà tại đó bộ điều khiển 606 là vận hành được để điều khiển môđun kiểm tra 600 để thực hiện các kiểm tra logic trong phản hồi để nhận các thông số kiểm tra từ thiết bị quản lý từ xa. Cụ thể hơn, môđun kiểm tra 600 là vận hành được để nhận

một hoặc nhiều thông số kiểm tra từ thiết bị quản lý kiểm tra từ xa, thông qua môđun liên lạc 607, sinh ra một hoặc nhiều mẫu kiểm tra dựa trên các thông số kiểm tra nhận được, sử dụng PRPG 201, áp dụng các mẫu kiểm tra cho CUT 101, nhận các phản hồi kiểm tra từ CUT 101, cô đọng các phản hồi kiểm tra vào trong chữ ký kiểm tra, sử dụng MISR 203, nhận chữ ký được mong đợi tương ứng với bộ các mẫu kiểm tra từ thiết bị quản lý kiểm tra từ xa, thông qua môđun liên lạc 607, và xác định kết quả kiểm tra dựa trên so sánh của chữ ký được mong đợi nhận được với chữ ký kiểm tra, sử dụng logic quyết định 604.

Tùy chọn là, bộ điều khiển 606 có thể còn được định cấu hình để thực hiện các kiểm tra logic tự trị, tức là, tại thời điểm bật nguồn hoặc khởi động lại, đáp ứng lại với điều kiện lỗi, hoặc đáp ứng lại với kích hoạt từ bên ngoài nhận được thông qua đầu vào điều khiển tùy chọn 114. Đầu vào điều khiển 114 cũng có thể được sử dụng để đảo chiều thiết bị điện tử 320 giữa chế động vận hành thông thường và chế độ kiểm tra, hoặc để khởi tạo chu kỳ kiểm tra, và có thể, tức là, được kết nối tới bộ phận giám sát lỗi được tạo ra cùng với thiết bị điện tử 320.

Các phương án thực hiện của môđun kiểm tra 322, như các môđun kiểm tra 500 và 600, và cụ thể là các môđun liên lạc 507 và 607, còn có thể được định cấu hình để mã hóa liên lạc với thiết bị quản lý kiểm tra từ xa, tức là, sử dụng SSH, SSL, TSL, IPsec, hoặc dạng tương tự, như đã biết trong tình trạng kỹ thuật của sáng chế. Nghĩa là, các thông số kiểm tra và, tùy chọn là, chữ ký được mong đợi, nhận được từ thiết bị quản lý kiểm tra từ xa sẽ được giải mã. Một cách tương ứng, chữ ký kiểm tra và kết quả kiểm tra được mã hóa trước khi truyền tới thiết bị quản lý kiểm tra từ xa. Ngoài ra, thiết bị điện tử 320 có thể được làm thích ứng để xác thực liên lạc với thiết bị quản lý kiểm tra từ xa 310, như đã biết trong tình trạng kỹ thuật của sáng chế, nhờ đó loại bỏ các tấn công loại có người tham gia ở giữa và loại mạo nhận.

Liên lạc giữa các môđun liên lạc 507 và 607 và các bộ điều khiển 506 và 606, một cách tương ứng, có thể bị ảnh hưởng theo tiêu chuẩn IEEE 1149.1 "Cổng truy cập kiểm tra tiêu chuẩn và kiến trúc quét biên - Standard Test Access Port and Boundary-Scan Architecture", dưới đây được đặt tên chung là nhóm hoạt động kiểm tra liên hợp (Joint Test Action Group - JTAG).

Trong phần sau, các phương án thực hiện khác của sáng chế được mô tả liên quan tới các hình vẽ từ Fig. 7 đến Fig.10.

Trên Fig.7, phương án thực hiện của phương pháp 700 để kiểm tra mạch logic dạng số được chứa trong thiết bị điện tử, như CUT 101 được chứa trong thiết bị điện tử 320, sẽ được minh họa. Phương pháp 700 được thực hiện bởi thiết bị điện tử và bao gồm bước nhận 701 một hoặc nhiều thông số kiểm tra từ thiết bị quản lý kiểm tra từ xa, như thiết bị quản lý kiểm tra từ xa 310, và sinh ra 702 một hoặc nhiều mẫu kiểm tra dựa trên các thông số kiểm tra nhận được. Phương pháp 700 còn bao gồm bước áp dụng 703 mẫu kiểm tra tới mạch logic dạng số, nhận 704 một hoặc nhiều phản hồi kiểm tra từ mạch logic dạng số, một phần cho mỗi mẫu kiểm tra, cô đọng 705 các phản hồi kiểm tra nhận được từ mạch logic dạng số vào trong chữ ký kiểm tra, và truyền 706 chữ ký kiểm tra tới thiết bị quản lý kiểm tra từ xa. Phương pháp 700 còn có thể bao gồm các bước bổ sung theo phần được mô tả ở trên, cụ thể là đề cập tới các hình vẽ từ Fig. 3 tới Fig.6.

Trên Fig.8, phương án thực hiện của phương pháp 800 khác để kiểm tra mạch logic dạng số được chứa trong thiết bị điện tử, như CUT 101 được chứa trong thiết bị điện tử 320, sẽ được minh họa. Phương pháp 800 được thực hiện bởi thiết bị điện tử và bao gồm bước nhận 801 một hoặc nhiều thông số kiểm tra từ thiết bị quản lý kiểm tra từ xa, như thiết bị quản lý kiểm tra từ xa 310, và sinh ra 802 một hoặc nhiều mẫu kiểm tra dựa trên các thông số kiểm tra nhận được. Phương pháp 800 còn bao gồm bước áp dụng 803 các mẫu kiểm tra tới mạch logic dạng số, nhận 804 một hoặc nhiều phản hồi kiểm tra từ mạch logic dạng số, một phần cho mỗi mẫu kiểm tra, cô đọng 805 các phản hồi kiểm tra nhận được từ mạch logic dạng số vào trong chữ ký kiểm tra, nhận 806 chữ ký được mong đợi tương ứng với các mẫu kiểm tra từ thiết bị quản lý kiểm tra từ xa, và xác định 807 kết quả kiểm tra dựa trên so sánh của chữ ký được mong đợi nhận được với chữ ký kiểm tra. Tùy chọn là phương pháp 800 còn có thể bao gồm bước truyền 808 thông tin thuộc về kết quả kiểm tra tới thiết bị quản lý kiểm tra từ xa. Phương pháp 800 còn có thể bao gồm các bước bổ sung theo phần được mô tả ở trên, cụ thể là đề cập tới các hình vẽ từ Fig. 3 tới Fig.6.

Các phương án thực hiện của các phương pháp 700 hoặc 800 có thể được áp dụng bởi chương trình máy tính 512 (hoặc 612) bao gồm các lệnh thực thi được bởi máy tính để làm cho thiết bị, như môđun kiểm tra 500 (hoặc 600) để thực hiện một cách tương ứng, khi các lệnh thực thi được bởi máy tính được thực thi trên đơn vị xử lý 510 (hoặc 610) được chứa trong thiết bị. Với tham khảo tới phần được mô tả ở trên, sẽ thấy rằng một số hoặc tất cả các bước của phương pháp 700 (hoặc 800) được thực hiện trong phối hợp với các phần chức năng khác của môđun kiểm tra 500 (hoặc 600). Ví dụ, bước nhận 701 một hoặc nhiều thông số kiểm tra từ thiết bị quản lý kiểm tra từ xa được thực hiện trong phối hợp với môđun liên lạc 507, và bước sinh ra 702 một hoặc nhiều mẫu kiểm tra dựa trên các thông số kiểm tra nhận được được thực hiện trong phối hợp với PRPG 201.

Trên Fig.9, phương án thực hiện của phương pháp 900 để kiểm tra mạch logic dạng số được chứa trong thiết bị điện tử, như CUT 101 được chứa trong thiết bị điện tử 320, sẽ được minh họa. Phương pháp 900 được thực hiện bởi thiết bị quản lý kiểm tra từ xa, như thiết bị quản lý kiểm tra từ xa 310. Phương pháp bao gồm bước thu được 901 một hoặc nhiều thông số kiểm tra thích hợp để sinh ra một hoặc nhiều mẫu kiểm tra cho mạch logic dạng số, thu được 902 chữ ký được mong đợi tương ứng với các mẫu kiểm tra, và truyền 903 các thông số kiểm tra tới ít nhất một thiết bị điện tử bao gồm mạch logic dạng số. Phương pháp 900 còn bao gồm bước nhận 904 chữ ký kiểm tra từ ít nhất một thiết bị điện tử, và xác định 905 kết quả kiểm tra dựa trên so sánh của chữ ký được mong đợi với chữ ký kiểm tra nhận được. Phương pháp 900 còn có thể bao gồm các bước bổ sung theo phần được mô tả ở trên, cụ thể là đề cập tới các hình vẽ từ Fig. 3 tới Fig.6.

Trên Fig.10, phương án thực hiện của phương pháp 1000 khác để kiểm tra mạch logic dạng số được chứa trong thiết bị điện tử, như CUT 101 được chứa trong thiết bị điện tử 320, sẽ được minh họa. Phương pháp 1000 được thực hiện bởi thiết bị quản lý kiểm tra từ xa, như thiết bị quản lý kiểm tra từ xa 310. Phương pháp 1000 bao gồm bước thu được 1001 một hoặc nhiều thông số kiểm tra thích hợp để sinh ra một hoặc nhiều mẫu kiểm tra cho mạch logic dạng số, thu được 1002 chữ ký được mong đợi tương ứng với các mẫu kiểm tra, truyền 1003 các thông số kiểm tra tới ít nhất một thiết

bị điện tử bao gồm mạch logic dạng số, và truyền 1004 chữ ký được mong đợi tới ít nhất một thiết bị điện tử. Tùy chọn là, phương pháp 1000 có thể còn bao gồm bước nhận 1005 thông tin thuộc về kết quả kiểm tra cho các mẫu kiểm tra từ ít nhất một thiết bị điện tử. Phương pháp 1000 còn có thể bao gồm các bước bổ sung theo phần được mô tả ở trên, cụ thể là đề cập tới các hình vẽ từ Fig. 3 tới Fig.6.

Các phương án thực hiện của các phương pháp 900 hoặc 1000 có thể được áp dụng bởi chương trình máy tính 313 bao gồm các lệnh thực thi được bởi máy tính để làm cho thiết bị thực hiện một cách tương ứng, khi các lệnh thực thi được bởi máy tính được thực thi trên đơn vị xử lý 311 được chứa trong thiết bị.

Người có hiểu biết trung bình trong lĩnh vực kỹ thuật sẽ nhận ra rằng sáng chế không bị hạn chế vào các phương án thực hiện đã được mô tả ở trên. Trái lại, nhiều biến đổi và phương án thay thế là có thể được thực hiện mà vẫn nằm trong phạm vi bảo hộ của các yêu cầu bảo hộ kèm theo. Cũng thấy rằng các phương án thực hiện của sáng chế có thể được áp dụng trong phần cứng, tức là các loại khác nhau của mạch điện tử, phần mềm, tức là các phương tiện xử lý thực thi chương trình máy tính thích hợp, hoặc tổ hợp bất kỳ của chúng.

Yêu cầu bảo hộ

1. Thiết bị điện tử (320; 1100; 1200; 1300) bao gồm:

mạch logic dạng số (101), và

môđun kiểm tra (322; 600) được làm thích ứng để:

nhận một hoặc nhiều thông số kiểm tra thích hợp để sinh ra một hoặc nhiều mẫu kiểm tra cho mạch logic dạng số từ thiết bị quản lý kiểm tra từ xa,

sinh ra một hoặc nhiều mẫu kiểm tra dựa trên các thông số kiểm tra,

áp dụng các mẫu kiểm tra vào mạch logic dạng số,

nhận một hoặc nhiều phản hồi kiểm tra từ mạch logic dạng số và,

cô đọng các phản hồi kiểm tra vào trong chữ ký kiểm tra,

thiết bị điện tử, khác biệt ở chỗ, môđun kiểm tra còn được làm thích ứng để:

nhận chữ ký được mong đợi tương ứng với các mẫu kiểm tra từ thiết bị quản lý kiểm tra từ xa, và

xác định kết quả kiểm tra dựa trên so sánh của chữ ký được mong đợi với chữ ký kiểm tra.

2. Thiết bị điện tử theo điểm 1, trong đó môđun kiểm tra được làm thích ứng để xác định kết quả kiểm tra như là chỉ thị của lỗi trong mạch logic dạng số nếu chữ ký được mong đợi khác với chữ ký kiểm tra.

3. Thiết bị điện tử theo điểm 1 hoặc 2, trong đó môđun kiểm tra còn được làm thích ứng để truyền thông tin thuộc về kết quả kiểm tra tới thiết bị quản lý kiểm tra từ xa.

4. Thiết bị điện tử theo điểm bất kỳ trong số các điểm từ 1 đến 3, còn bao gồm bộ sinh giả ngẫu nhiên (201) để sinh ra các mẫu kiểm tra dựa trên các thông số kiểm tra.

5. Thiết bị điện tử theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó, các thông số kiểm tra bao gồm ít nhất một trong số trị số khởi tạo, số các mẫu kiểm tra cần được tạo ra, và một hoặc nhiều số chuỗi của các mẫu kiểm tra cần được sinh ra.

6. Thiết bị điện tử theo điểm bất kỳ trong số các điểm từ 1 đến 5, là một trong số mạch tích hợp (Integrated Circuit) (1100), hệ thống trên chip (System-on-Chip) (1100), hệ thống trong gói (System-in-Package) (1200), hoặc hệ thống trên môđun (System-on-Module) (1200).

7. Thiết bị mã hóa bao gồm thiết bị điện tử theo điểm bất kỳ trong số các điểm từ 1 đến 6.

8. Thiết bị đầu cuối di động (1300) bao gồm thiết bị điện tử theo điểm bất kỳ trong số các điểm từ 1 đến 6, hoặc thiết bị mã hóa theo điểm 7.

9. Thiết bị quản lý kiểm tra từ xa (310) để kiểm tra mạch logic dạng số (101) được chứa trong thiết bị điện tử (320), thiết bị quản lý kiểm tra từ xa bao gồm các phương tiện (311–315) được làm thích ứng để:

thu được một hoặc nhiều thông số kiểm tra là thích hợp để sinh ra một hoặc nhiều mẫu kiểm tra cho mạch logic dạng số,

thu được chữ ký được mong đợi tương ứng với các mẫu kiểm tra, và

truyền các thông số kiểm tra tới ít nhất một thiết bị điện tử bao gồm mạch logic dạng số,

thiết bị quản lý kiểm tra từ xa, khác biệt ở chỗ, các phương tiện còn được làm thích ứng để:

truyền chữ ký được mong đợi tới ít nhất một thiết bị điện tử.

10. Thiết bị quản lý kiểm tra từ xa theo điểm 9, trong đó các phương tiện còn được làm thích ứng để nhận thông tin thuộc về kết quả kiểm tra cho các mẫu kiểm tra từ ít nhất một thiết bị điện tử.

11. Thiết bị quản lý kiểm tra từ xa theo điểm 9 hoặc 10, trong đó các phương tiện còn được làm thích ứng để thu được chữ ký được mong đợi bằng cách tính toán chữ ký được mong đợi dựa trên các thông số kiểm tra và thiết kế của mạch logic dạng số.

12. Thiết bị quản lý kiểm tra từ xa theo điểm bất kỳ trong số các điểm từ 9 đến 11, trong đó, các thông số kiểm tra bao gồm ít nhất một trong số trị số khởi tạo, số các

mẫu kiểm tra cần được tạo ra, và một hoặc nhiều số chuỗi của các mẫu kiểm tra cần được sinh ra.

13. Phương pháp (800) kiểm tra mạch logic dạng số (101) được chứa trong thiết bị điện tử (320), phương pháp được thực hiện bởi thiết bị điện tử và bao gồm các bước:

nhận (801) một hoặc nhiều thông số kiểm tra thích hợp để sinh ra một hoặc nhiều mẫu kiểm tra cho mạch logic dạng số từ thiết bị quản lý kiểm tra từ xa (310),

sinh ra (802) một hoặc nhiều mẫu kiểm tra dựa trên các thông số kiểm tra,

áp dụng (803) các mẫu kiểm tra vào mạch logic dạng số,

nhận (804) một hoặc nhiều phản hồi kiểm tra từ mạch logic dạng số, và

cô đọng (805) các phản hồi kiểm tra vào trong chữ ký kiểm tra, phương pháp, khác biệt ở chỗ, nó còn bao gồm bước:

nhận (806) chữ ký được mong đợi tương ứng với các mẫu kiểm tra từ thiết bị quản lý kiểm tra từ xa, và

xác định (807) kết quả kiểm tra dựa trên so sánh của chữ ký được mong đợi với chữ ký kiểm tra.

14. Phương pháp theo điểm 13, trong đó, bước xác định kết quả kiểm tra bao gồm việc chỉ thị lỗi trong mạch logic dạng số nếu chữ ký được mong đợi khác với chữ ký kiểm tra.

15. Phương pháp (800) theo điểm 13 hoặc 14, còn bao gồm bước truyền (808) thông tin thuộc về kết quả kiểm tra tới thiết bị quản lý kiểm tra từ xa.

16. Phương pháp theo điểm bất kỳ trong số các điểm từ 13 đến 15, trong đó, các mẫu kiểm tra được sinh ra dựa trên các thông số kiểm tra sử dụng bộ sinh giả ngẫu nhiên được chứa trong thiết bị điện tử.

17. Phương pháp theo điểm bất kỳ trong số các điểm từ 13 đến 16, trong đó, các thông số kiểm tra bao gồm ít nhất một trong số trị số khởi tạo, số các mẫu kiểm tra cần được tạo ra, và một hoặc nhiều số chuỗi của các mẫu kiểm tra cần được sinh ra.

18. Phương pháp (1000) kiểm tra mạch logic dạng số (101) được chứa trong thiết bị điện tử (320), phương pháp được thực hiện bởi thiết bị quản lý kiểm tra từ xa (310), phương pháp bao gồm các bước:

thu được (1001) một hoặc nhiều thông số kiểm tra thích hợp để sinh ra một hoặc nhiều mẫu kiểm tra cho mạch logic dạng số,

thu được (1002) chữ ký được mong đợi tương ứng với các mẫu kiểm tra, và

truyền (1003) các thông số kiểm tra tới ít nhất một thiết bị điện tử bao gồm mạch logic dạng số,

phương pháp, khác biệt ở chỗ, nó còn bao gồm bước:

truyền (1004) chữ ký được mong đợi tới ít nhất một thiết bị điện tử.

19. Phương pháp theo điểm 18, còn bao gồm bước nhận (1005) thông tin thuộc về kết quả kiểm tra cho các mẫu kiểm tra từ ít nhất một thiết bị điện tử.

20. Phương pháp theo điểm 18 hoặc 19, trong đó, bước thu được chữ ký được mong đợi bao gồm việc tính toán chữ ký được mong đợi dựa trên các thông số kiểm tra và thiết kế của mạch logic dạng số.

21. Phương pháp theo điểm bất kỳ trong số các điểm từ 18 đến 20, trong đó, các thông số kiểm tra bao gồm ít nhất một trong số trị số khởi tạo, số các mẫu kiểm tra cần được tạo ra, và một hoặc nhiều số chuỗi của các mẫu kiểm tra cần được sinh ra.

22. Vật ghi đọc được bởi máy tính có chương trình máy tính (313) được lưu ở đó, chương trình máy tính bao gồm các lệnh thực thi được bởi máy tính để làm cho thiết bị (310) thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 13 đến 21, khi các lệnh thực thi được bởi máy tính được thực thi trên đơn vị xử lý (311) được chứa trong thiết bị.

Fig. 1

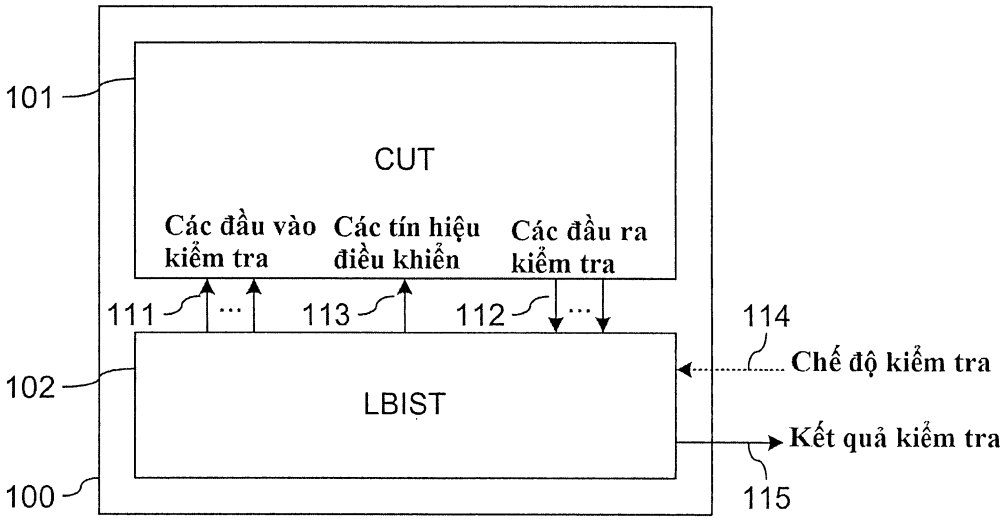

101
CUT
Các đầu vào kiểm tra
Các tín hiệu điều khiển
Các đầu ra kiểm tra
111
113
112
114
Chế độ kiểm tra
102
LBIST
Kết quả kiểm tra
100
115

Fig. 2

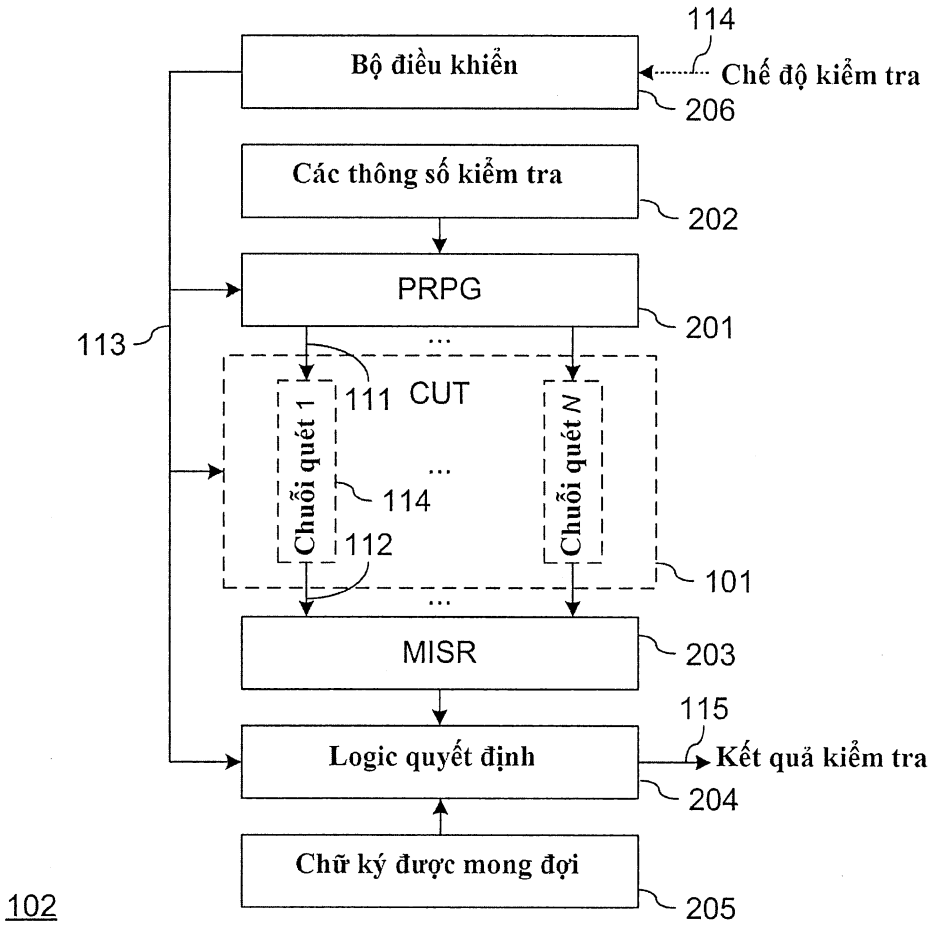

114
Bộ điều khiển
Chế độ kiểm tra
206
Các thông số kiểm tra
202
PRPG
201
113
111
CUT
Chuỗi quét 1
Chuỗi quét N
114
112
101
MISR
203
115
Logic quyết định
Kết quả kiểm tra
204
Chữ ký được mong đợi
205
102

Fig. 3

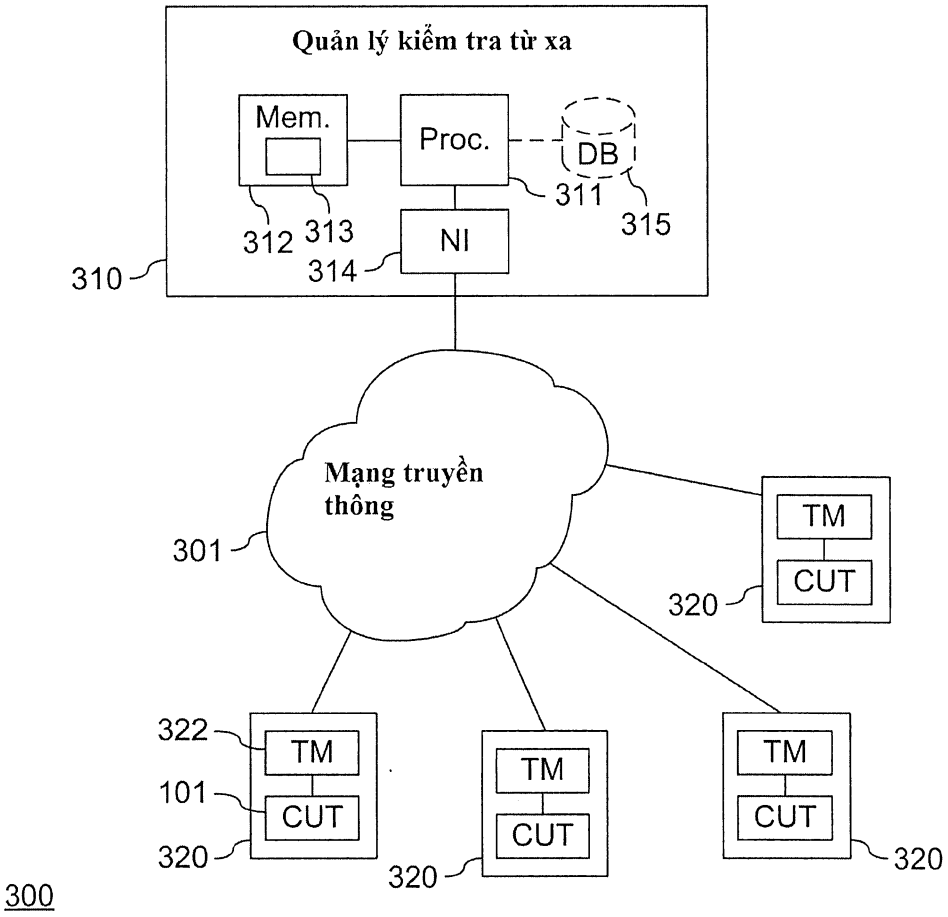

Quản lý kiểm tra từ xa
Mem.
Proc.
DB
311
315
312
313
NI
314
310
Mạng truyền thông
301
TM
CUT
320
322
TM
101
CUT
320
TM
CUT
320
TM
CUT
320
300

Fig. 4

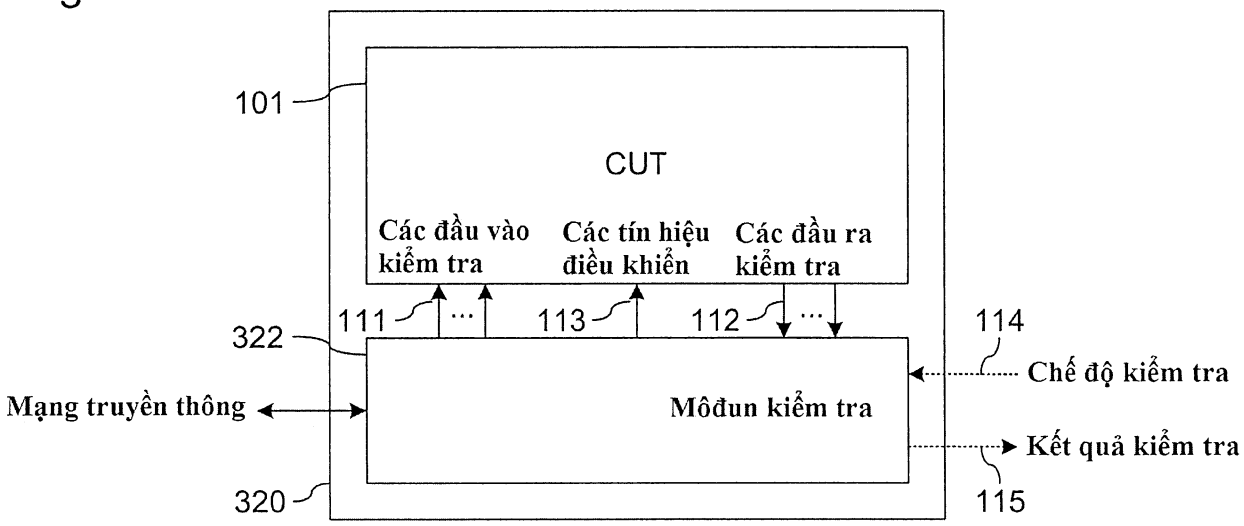

101
CUT
Các đầu vào kiểm tra
Các tín hiệu điều khiển
Các đầu ra kiểm tra
111
113
112
114
322
Chế độ kiểm tra
Mạng truyền thông
Môđun kiểm tra
Kết quả kiểm tra
320
115

Fig. 5

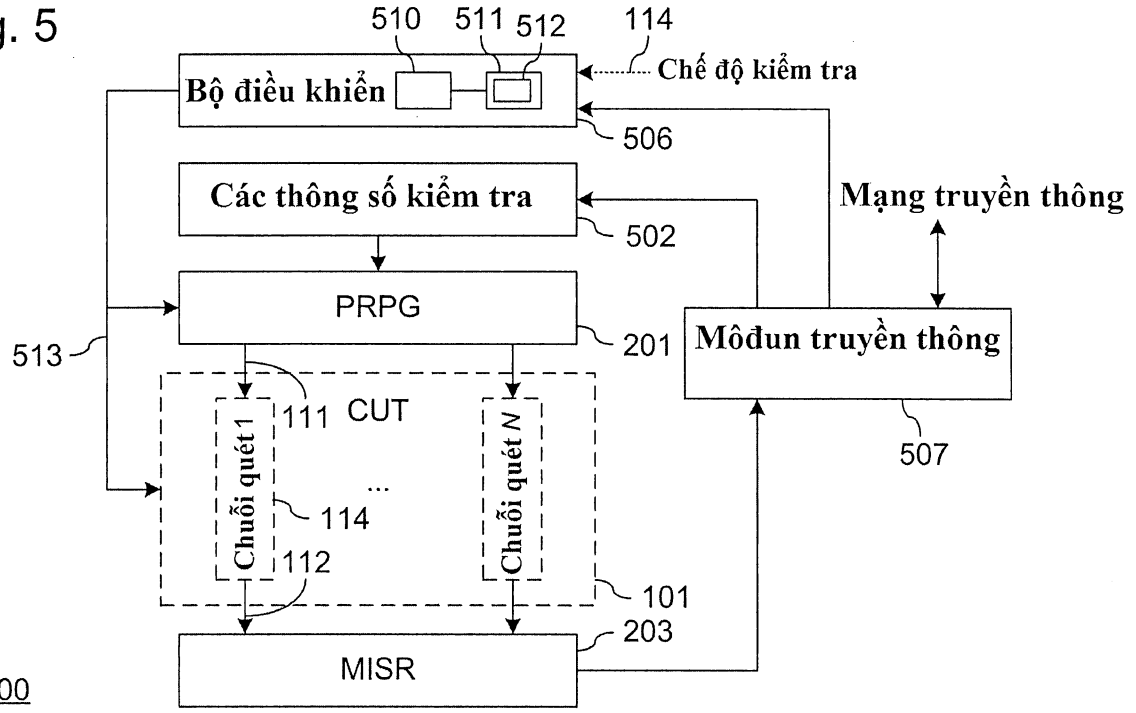

510
511
512
114
Chế độ kiểm tra
Bộ điều khiển
506
Các thông số kiểm tra
502
Mạng truyền thông
PRPG
201
Môđun truyền thông
513
111
CUT
Chuỗi quét 1
...
Chuỗi quét N
114
112
101
507
203
MISR
500

Fig. 6

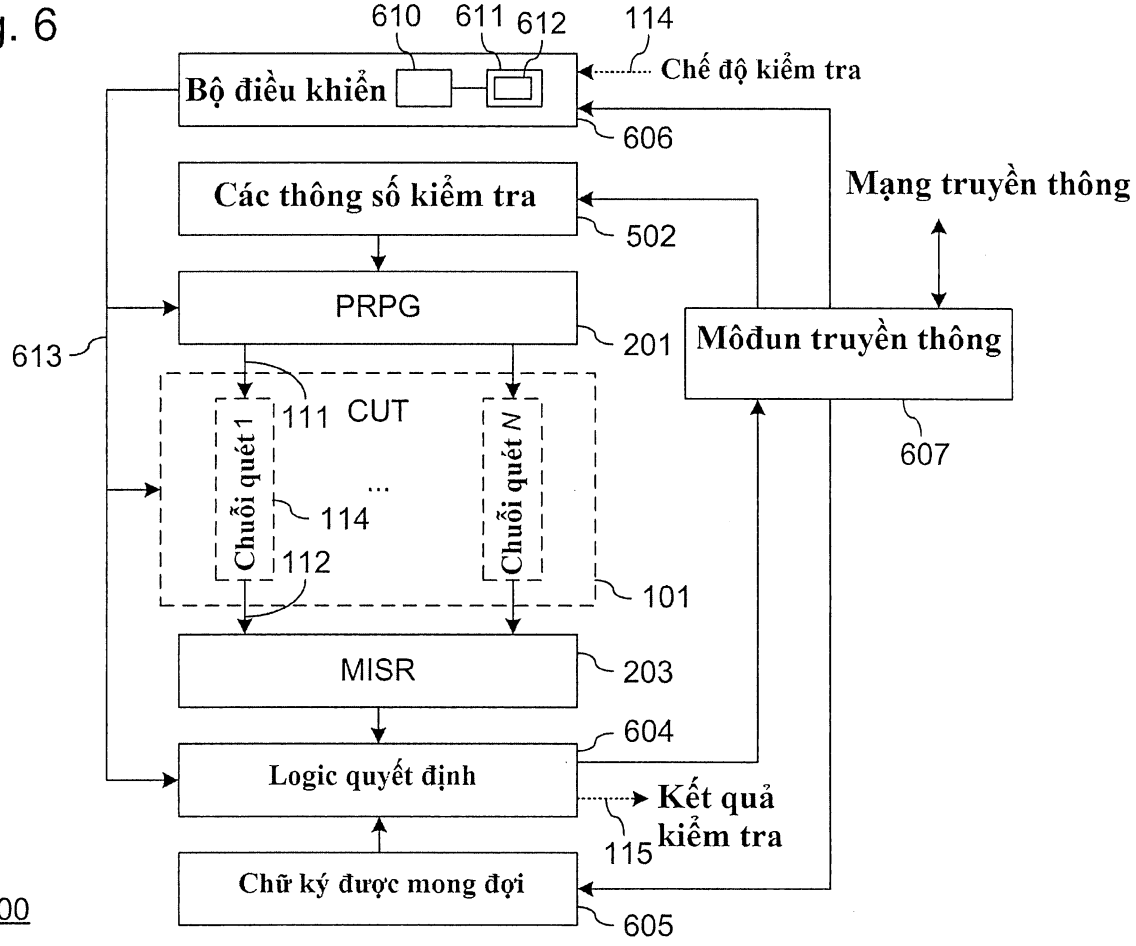

610
611
612
114
Chế độ kiểm tra
Bộ điều khiển
606
Mạng truyền thông
Các thông số kiểm tra
502
PRPG
201
Môđun truyền thông
613
111
CUT
Chuỗi quét 1
...
Chuỗi quét N
114
112
101
607
MISR
203
604
Logic quyết định
Kết quả kiểm tra
115
Chữ ký được mong đợi
605
600

Fig. 7

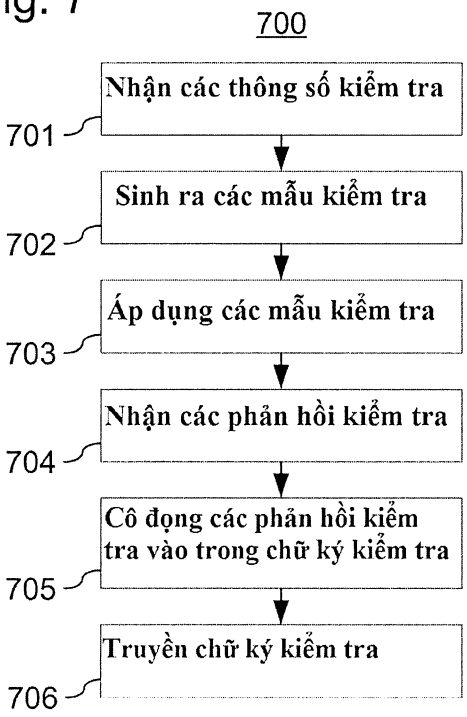


Fig. 8

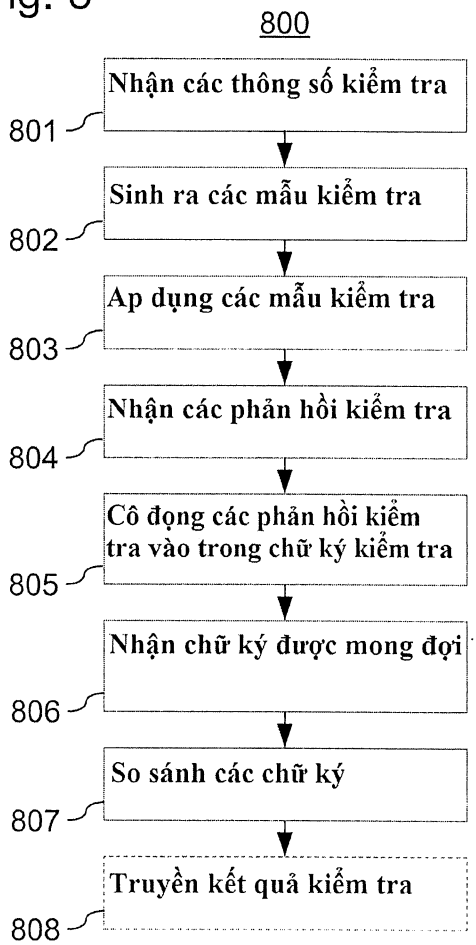


Fig. 9

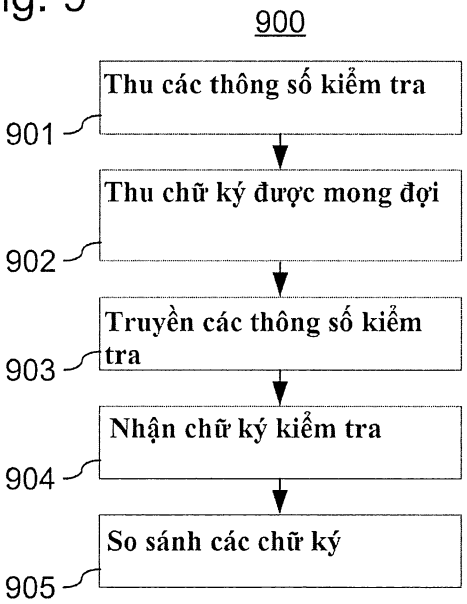


Fig. 10

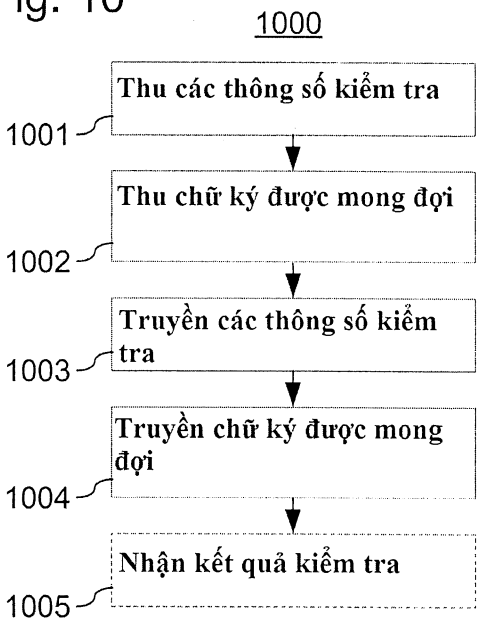


Fig. 11

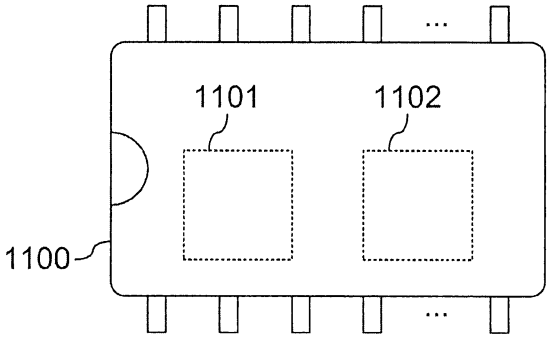


Fig. 12

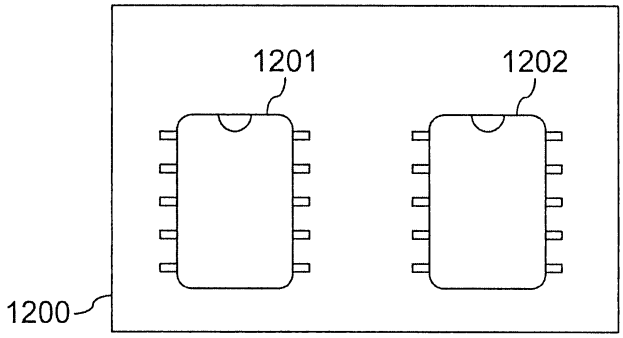


Fig. 13