(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년08월31일
(11) 등록번호 10-1773490
(24) 등록일자 2017년08월25일

(51) 국제특허분류(Int. Cl.)
G06F 21/10 (2013.01) *G01R 31/30* (2006.01)
G01R 31/317 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
G06F 21/10 (2013.01)
G01R 31/3004 (2013.01)
(21) 출원번호 10-2015-7018765
(22) 출원일자(국제) 2013년12월20일
심사청구일자 2016년11월29일
(85) 번역문제출일자 2015년07월13일
(65) 공개번호 10-2015-0097624
(43) 공개일자 2015년08월26일
(86) 국제출원번호 PCT/US2013/077049
(87) 국제공개번호 WO 2014/100647
국제공개일자 2014년06월26일
(30) 우선권주장
61/740,333 2012년12월20일 미국(US)
13/752,215 2013년01월28일 미국(US)
(56) 선행기술조사문헌
US20110317829 A1
US20120044777 A1
US20110002461 A1
E. Suh et al "Physical Unclonable Functions for Device Authentication and Secret Key Generation", 2007 44th ACM/IEEE Design Automation Conference pp.9-14, 2007.06.

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
구오, 수
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인 남앤드남

전체 청구항 수 : 총 15 항 심사관 : 윤혜숙

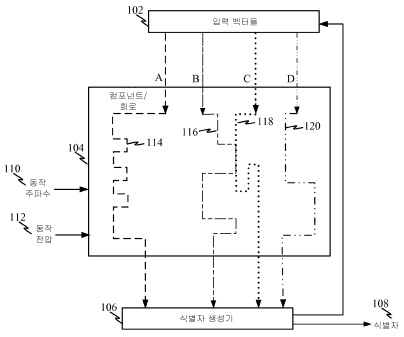
(54) 발명의 명칭 **데이터-의존 회로 경로 응답들을 이용하는 고유하고 복제불가한 플랫폼 식별자들**

(57) 요 약

고유 식별자를 생성하기 위한 방법 및 장치가 제공된다. 하나 또는 그 초과의 테스트들은 하나 또는 그 초과의 회로들에 대한 하나 또는 그 초과의 데이터-의존 회로 경로들에 대해 수행된다. 그후, 하나 또는 그 초과의 테스트들은, 하나 또는 그 초과의 회로들 각각에 대한 동작 주파수 및/또는 동작 전압을 조정하면서, 하나 또는 그

(뒷면에 계속)

대 표 도 - 도1



초과의 회로들에 대한 하나 또는 그 초과의 데이터-의존 회로 경로들에 대해 반복된다. 임계 주파수 및/또는 임계 전압은 하나 또는 그 초과의 데이터-의존 회로 경로들 각각에 대해 확인된다. 그후, 식별자는 하나 또는 그 초과의 데이터-의존 회로 경로들에 대해 확인된 복수의 임계 주파수들 및/또는 임계 전압들에 기초하여 발생될 수 있다.

(52) CPC특허분류
G01R 31/31725 (2013.01)
H04L 9/3278 (2013.01)

명 세 서

청구범위

청구항 1

고유 식별자를 생성하기 위해 프로세싱 회로에서 동작하는 방법으로서,

하나 또는 그 초과의 회로들에 대해 하나 또는 그 초과의 회로 경로들을 통한 하나 또는 그 초과의 테스트들을 수행하는 단계;

상기 하나 또는 그 초과의 회로들 각각에 대한 동작 주파수 및/또는 동작 전압을 조정하면서, 상기 하나 또는 그 초과의 회로들에 대해 상기 하나 또는 그 초과의 회로 경로들을 통한 상기 하나 또는 그 초과의 테스트들을 반복하는 단계;

상기 하나 또는 그 초과의 회로 경로들 각각에 대한 임계 주파수 및/또는 임계 전압을 확인하는 단계; 및

상기 하나 또는 그 초과의 회로 경로들에 대해 확인된 복수의 임계 주파수들 및/또는 임계 전압들에 기초하여 식별자를 생성하는 단계를 포함하는,

고유 식별자를 생성하기 위해 프로세싱 회로에서 동작하는 방법.

청구항 2

제 1 항에 있어서,

상기 식별자는 상기 프로세싱 회로를 포함하는 플랫폼과 연관되는,

고유 식별자를 생성하기 위해 프로세싱 회로에서 동작하는 방법.

청구항 3

제 1 항에 있어서,

상기 식별자에 소프트웨어 애플리케이션 설치를 연관시키는 단계; 및

상기 프로세싱 회로 상에서의 상기 소프트웨어 애플리케이션의 실행을 상기 식별자의 성공적인 검증에 바인딩(binding)하는 단계를 더 포함하는,

고유 식별자를 생성하기 위해 프로세싱 회로에서 동작하는 방법.

청구항 4

제 3 항에 있어서,

상기 식별자의 성공적인 검증은, 상기 식별자의 오리지널 인스턴스(instance)와 상기 식별자의 후속 생성된 인스턴스가 동일함을 확인하기 위해 이들을 비교하는,

고유 식별자를 생성하기 위해 프로세싱 회로에서 동작하는 방법.

청구항 5

제 1 항에 있어서,

상기 하나 또는 그 초과의 회로들은:

범용 계산(computational) 컴포넌트들;

비-식별자 특정 계산 컴포넌트들; 또는

비-저장 및/또는 비-메모리 회로들인,

고유 식별자를 생성하기 위해 프로세싱 회로에서 동작하는 방법.

청구항 6

제 1 항에 있어서,

상기 동작 주파수 및/또는 동작 전압은:

상기 테스트의 각각의 반복에 대해 상기 동작 주파수를 증가시키는 것;

상기 테스트의 각각의 반복에 대해 상기 동작 전압을 감소시키는 것; 및/또는

상기 테스트의 각각의 반복에 대해 상기 동작 주파수 및 상기 동작 전압의 조합을 조정하는 것

중 적어도 하나에 의해 조정되는,

고유 식별자를 생성하기 위해 프로세싱 회로에서 동작하는 방법.

청구항 7

제 1 항에 있어서,

상기 하나 또는 그 초과의 회로들은:

하나 또는 그 초과의 내부의 계산 컴포넌트들;

하나 또는 그 초과의 외부의 계산 컴포넌트들; 및/또는

내부 및 외부 계산 컴포넌트들의 조합

중 적어도 하나를 포함하는,

고유 식별자를 생성하기 위해 프로세싱 회로에서 동작하는 방법.

청구항 8

제 1 항에 있어서,

상기 임계 주파수는, 주어진(given) 회로 경로를 통한 테스트가 상기 테스트에 대한 부정확한(incorrect) 응답을 제공하는 주파수인,

고유 식별자를 생성하기 위해 프로세싱 회로에서 동작하는 방법.

청구항 9

제 1 항에 있어서,

상기 임계 주파수는, 주어진 회로 경로를 통한 테스트에 대해 예상되는 응답이 예상치못한(unexpected) 응답으로 변하는 주파수인,

고유 식별자를 생성하기 위해 프로세싱 회로에서 동작하는 방법.

청구항 10

제 1 항에 있어서,

상기 식별자는:

하나의 회로에 대한 2개 또는 그 초과의 상이한 회로 경로들에 대한 2개 또는 그 초과의 임계 주파수들 및/또는 임계 전압들에 기초하는,

고유 식별자를 생성하기 위해 프로세싱 회로에서 동작하는 방법.

청구항 11

제 1 항에 있어서,

상기 식별자는:

2개 또는 그 초과의 상이한 회로들에 대한 2개 또는 그 초과의 상이한 회로 경로들에 대한 2개 또는 그 초과의 임계 주파수들 및/또는 임계 전압들에 기초하는,

고유 식별자를 생성하기 위해 프로세싱 회로에서 동작하는 방법.

청구항 12

제 1 항에 있어서,

후속 검증을 위해 상기 식별자를 저장하는 단계를 더 포함하는,

고유 식별자를 생성하기 위해 프로세싱 회로에서 동작하는 방법.

청구항 13

제 1 항에 있어서,

이전에 저장된 식별자를 리트리브(retrieve)하는 단계; 및

상기 생성된 식별자와 상기 이전에 저장된 식별자가 동일한지 확인하기 위해 이들을 비교하는 단계를 더 포함하는,

고유 식별자를 생성하기 위해 프로세싱 회로에서 동작하는 방법.

청구항 14

장치로서,

하나 또는 그 초과의 회로들에 대해 하나 또는 그 초과의 회로 경로들을 통한 하나 또는 그 초과의 테스트들을 수행하기 위해 적응된 수단;

상기 하나 또는 그 초과의 회로들 각각에 대해 동작 주파수 및/또는 동작 전압을 조정하면서, 상기 하나 또는 그 초과의 회로들에 대해 상기 하나 또는 그 초과의 회로 경로들을 통한 상기 하나 또는 그 초과의 테스트들을 반복하기 위해 적응된 수단;

상기 하나 또는 그 초과의 회로 경로들 각각에 대한 임계 주파수 및/또는 임계 전압을 확인하기 위해 적응된 수단; 및

상기 하나 또는 그 초과의 회로 경로들에 대해 확인된 복수의 임계 주파수들 및/또는 임계 전압들에 기초하여 식별자를 생성하기 위해 적응된 수단을 포함하는,

장치.

청구항 15

명령들이 저장된 비-일시적인 머신-판독가능(machine-readable) 저장 매체로서,

상기 명령들은, 적어도 하나의 프로세서에 의해 실행될 때, 상기 적어도 하나의 프로세서로 하여금, 제 1 항 내지 제 13 항 중 어느 한 항에 따른 방법을 수행하게 하는,

비-일시적인 머신-판독가능 저장 매체.

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

청구항 36

삭제

발명의 설명

기 술 분 야

[0001] **35 U.S.C. § 119 하에서의 우선권 주장**

[0002] [0001] 본 특허 출원은 2012년 12월 20일자로 출원되고, 여기서 본원에 인용에 의해 명시적으로 포함되는, 발명의 명칭이 "Unique and Unclonable Platform Identifiers Using Data-Dependent Circuit Path Responses"인 미국 가출원 제61/740,333호를 우선권 주장한다.

[0003] **분야**

[0004] [0002] 다양한 특징들은, 고유하고 복제불가한(unique and unclonable) 식별자들을 생성하는 것에 관한 것이고, 더욱 구체적으로는 물리적 회로 또는 컴포넌트의 본질적인 특징들에 기초한 식별자에 관한 것이다.

배 경 기 술

[0005] [0003] 소프트웨어 보호는 소프트웨어의 허가되지 않은 카피를 방지하기 위해 이용되는 컴퓨터 보안 기법들의 패밀리이다. 다시 말해서, 소프트웨어는 사용자가, 이 소프트웨어를 사용하기 위해 적절하게 라이센싱되었는지 결정하고 그리고 이 소프트웨어가 적절하게 라이센싱된 경우에만 구동하도록 해야만 한다.

[0006] [0004] 소프트웨어 보호와 관련된 다른 문제는, 소프트웨어가 구동중인 칩(예를 들어, 반도체 디바이스) 또는 플랫폼이 위조(counterfeit) 칩인지 식별하는 방법에 있다. 위조 칩들은, 빠르게 확산되고 있고, 전자 공급 체인(electronics supply chain)에 대한 리스크이다. 위조 반도체들로부터의 제품 폴아웃(fallout)은, 드롭 콜(dropped call)과 같은 작은 문제들로부터 훨씬 더 큰 문제들까지 범위를 이룰 수 있다. 결과적으로, 전자 공급 체인에서 위조 칩들의 사용을 식별하고 제한하는 것은 필수적이다.

[0007] [0005] 소프트웨어 지적 재산권 및 컨텐츠 보호를 위한 가장 큰 난제들 중 하나는, 보호된 소프트웨어로 하여금 이 소프트웨어가 구동중인 하드웨어 플랫폼을 식별하게 하는 것이다. 기존의 칩 설계들에 추가의 로직을 부가할 필요가 없고 심지어 이미 제조된 칩들에 적용될 수 있는 제로-원가의 솔루션을 설계할 필요가 있다.

[0008] [0006] 따라서, 소프트웨어로 하여금, 추가의 로직 및/또는 식별 특정 회로 컴포넌트들을 필요로 하지 않고도 소프트웨어가 구동중인 하드웨어 플랫폼을 고유하게 식별하도록 허용하는 솔루션이 필요하다.

발명의 내용

[0009] [0007] 고유한 식별자를 생성하기 위해 프로세싱 회로에서 동작가능한 방법이 제공된다. 하나 또는 그 초과의 테스트들은, 하나 또는 그 초과의 회로들에 대한 하나 또는 그 초과의 데이터-의존 회로 경로들에 대해 수행될 수 있다. 다양한 예시들에서, 하나 또는 그 초과의 회로들은: (a) 범용 계산(computational) 컴포넌트들, (b) 비-식별자 특정 계산 컴포넌트들, 및/또는 (c) 비-저장 및/또는 비-메모리 회로들일 수 있다. 다른 예시들에서, 하나 또는 그 초과의 회로들은: (a) 하나 또는 그 초과의 내부의 계산 컴포넌트들; (b) 하나 또는 그 초과의 외부 계산 컴포넌트들; 및/또는 (c) 내부의 계산 컴포넌트들과 외부의 계산 컴포넌트들의 조합 중 적어도 하나를 포함할 수 있다.

[0010] [0008] 하나 또는 그 초과의 테스트들은, 하나 또는 그 초과의 회로들 각각에 대한 동작 주파수 및/또는 동작 전압을 조정하면서, 하나 또는 그 초과의 회로들에 대한 하나 또는 그 초과의 데이터-의존 회로 경로들에 대해 반복될 수 있다. 동작 주파수 및/또는 동작 전압은: (a) 테스트의 각각의 반복에 대한 동작 주파수를 증가시키는 것; (b) 테스트의 각각의 반복에 대한 동작 전압을 감소시키는 것; 및/또는 (c) 테스트의 각각의 반복에 대한 동작 주파수와 동작 전압의 조합을 조정하는 것 중 적어도 하나에 의해 조정된다.

[0011] [0009] 임계 주파수 및/또는 임계 전압은 하나 또는 그 초과의 데이터-의존 회로 경로들 각각에 대해 확인될 수

있다. 일 예시에서, 임계 주파수는, 주어진(given) 데이터-의존 회로 경로가 테스트에 부정확한 응답을 제공하는 주파수일 수 있다. 다른 예시에서, 임계 주파수는, 주어진 데이터-의존 회로 경로에 대한 테스트에 예상되는 응답이 예상밖의 응답으로 변하는 주파수일 수 있다.

[0012] [0010] 다음으로, 식별자는 하나 또는 그 초과의 데이터-의존 회로 경로들에 대해 확인된 복수의 임계 주파수들 및/또는 임계 전압들에 기초하여 생성될 수 있다. 일 예시에서, 식별자는 프로세싱 회로를 포함하는 플랫폼과 연관될 수 있다. 다른 예시에서, 방법은 추가로 (a) 소프트웨어 애플리케이션 설치를 식별자에 연관시키고; 및/또는 (b) 프로세싱 회로 상에서의 소프트웨어 애플리케이션의 실행을 식별자의 성공적인 검증에 바인딩(bind)할 수 있다. 식별자의 성공적인 검증은, 식별자의 오리지널 인스턴스와 식별자의 후속 생성된 인스턴스가 동일한지 확인하기 위해, 이들을 비교할 수 있다. 일부 예시들에서, 식별자는: (a) 하나의 회로에 대해 2개 그 초과의 상이한 회로 경로들에 대한 2개 또는 그 초과의 임계 주파수들 및/또는 임계 전압들, 또는 (b) 2개 또는 그 초과의 상이한 회로들에 대해 2개 또는 그 초과의 상이한 회로 경로들에 대한 2개 또는 그 초과의 임계 주파수들 및/또는 임계 전압들에 기초할 수 있다. 식별자는 후속 검증을 위해 저장될 수 있다. 검증 프로세스 동안, 이전에 저장된 식별자는 리트리브될 수 있다. 그후, 생성된 식별자는, 이전에 저장된 식별자와 비교되어 이들이 동일한지 확인될 수 있다.

[0013] [0011] 프로세싱 회로에 커플링된 하나 또는 그 초과의 회로들을 포함하는 장치가 고유한 식별자를 생성하기 위해 제공될 수 있다. 프로세싱 회로는: (a) 하나 또는 그 초과의 회로들의 하나 또는 그 초과의 데이터-의존 회로 경로들에 대해 하나 또는 그 초과의 테스트들을 수행하고; (b) 하나 또는 그 초과의 회로들 각각에 대해 동작 주파수 및/또는 동작 전압을 조정하면서, 하나 또는 그 초과의 회로들에 대한 하나 또는 그 초과의 데이터-의존 회로 경로들에 대해 하나 또는 그 초과의 테스트들을 반복하고; (c) 하나 또는 그 초과의 데이터-의존 회로 경로들 각각에 대해 임계 주파수 및/또는 임계 전압을 확인하고; 그리고/또는 (d) 하나 또는 그 초과의 데이터-의존 회로 경로들에 대해 확인된 복수의 임계 주파수들 및/또는 임계 전압들에 기초하여 식별자를 생성하도록 적응될 수 있다.

[0014] [0012] 일 예시에서, 식별자는 프로세싱 회로를 포함하는 플랫폼과 연관될 수 있다. 다른 예시에서, 소프트웨어 애플리케이션 설치는 식별자와 연관될 수 있고, 프로세싱 회로 상에서의 소프트웨어 애플리케이션의 실행은 식별자의 성공적인 검증에 바인딩된다. 식별자의 성공적인 검증은, 식별자의 오리지널 인스턴스와 식별자의 후속 생성된 인스턴스가 동일한지 확인하기 위해, 이들을 비교할 수 있다.

[0015] [0013] 다양한 실시예들에서, 하나 또는 그 초과의 회로들은: (a) 범용 계산 컴포넌트들, (b) 비-식별자 특정 계산 컴포넌트들, 및/또는 비-저장 및/또는 비-메모리 회로들일 수 있다.

[0016] [0014] 동작 주파수 및/또는 동작 전압은: (a) 테스트의 각각의 반복에 대해 동작 주파수를 증가시키는 것; (b) 테스트의 각각의 반복에 대해 동작 전압을 감소시키는 것; 및/또는 (c) 테스트의 각각의 반복에 대해 동작 주파수와 동작 전압의 조합을 조정하는 것 중 적어도 하나에 의해 조정될 수 있다.

[0017] [0015] 하나 또는 그 초과의 회로들은: (a) 하나 또는 그 초과의 내부의 계산 컴포넌트들, (b) 하나 또는 그 초과의 외부의 계산 컴포넌트들; 및/또는 (c) 내부의 계산 컴포넌트와 외부의 계산 컴포넌트의 조합 중 적어도 하나를 포함할 수 있다.

[0018] [0016] 임계 주파수는: (a) 주어진 데이터-의존 회로 경로에 대한 테스트가 테스트에 대한 부정확한 응답을 제공하고, 그리고/또는 (b) 주어진 데이터-의존 회로 경로에 대한 테스트에 대해 예상되는 응답이 예상밖의 응답으로 변하는 주파수일 수 있다.

[0019] [0017] 식별자는: (a) 하나의 회로에 대한 2개 또는 그 초과의 상이한 회로 경로들에 대해 2개 또는 그 초과의 임계 주파수들 및/또는 임계 전압들, 및/또는 (b) 2개 또는 그 초과의 상이한 회로들에 대한 2개 또는 그 초과의 상이한 회로 경로들에 대해 2개 또는 그 초과의 임계 주파수들 및/또는 임계 전압들에 기초할 수 있다.

도면의 간단한 설명

[0020] [0018] 다양한 특징들, 속성 및 이점들은, 도면과 관련하여 고려될 때 이하 설명된 상세한 설명으로부터 명백하게 될 수 있으며, 여기서 동일한 참조 문자들은 명세서 전반에 걸쳐 이에 대응하게 식별한다.

[0019] 도 1은 온-보드 또는 오프-보드 컴포넌트 또는 회로에 대해 데이터-의존 회로 경로 응답 정보를 활용함으로써 식별자(ID)를 추출하는 방법을 예시한다.

[0020] 도 2는 다수의 온-보드 또는 오프-보드 컴포넌트들 또는 회로들로부터 데이터-의존 회로 경로 응답 정보를 활용함으로써 플랫폼 식별(ID)을 추출하는 방법을 예시한다.

[0021] 도 3은 상이한 동작 주파수들에서 일 세트의 입력 벡터들에 대한 예시적인 결과들을 예시하는 표이다.

[0022] 도 4는 상이한 동작 전압들에서 일 세트의 입력 벡터들에 대한 예시적인 결과들을 예시하는 표이다.

[0023] 도 5는 상이한 동작 주파수-전압 쌍들에서 일 세트의 입력 벡터들에 대한 예시적인 결과들을 나타내는 표를 예시한다.

[0024] 도 6은 데이터-의존 회로 경로들에 기초하여 고유의 복제불가한 식별자를 컴퓨팅하도록 적응될 수 있는 예시적인 프로세싱 회로를 예시한다.

[0025] 도 7은 하나 또는 그 초과의 온-보드 및/또는 오프-보드 컴포넌트들, 회로들, 및/또는 반도체들에 대해 데이터-의존 회로 경로 응답 정보를 활용함으로써 고유의 복제불가한 플랫폼 식별자(ID)를 컴퓨팅하기 위한 방법을 예시한다.

발명을 실시하기 위한 구체적인 내용

[0021] [0026] 이하의 설명에서, 본 개시물의 다양한 양상들의 전반적인 이해를 제공하기 위해 특정 세부사항들이 주어진다. 그러나, 양상들이 이러한 특정 세부사항들 없이도 실행될 수 있다는 것이 당업자에 의해 이해될 것이다. 예를 들어, 회로들은 양상들을 불필요한 세부사항으로 모호하게 하는 것을 회피하기 위해 블록도들로 나타낼 수 있다. 다른 경우들에서, 잘-알려진 회로들, 구조들 및 기법들은 본 개시물의 양상들을 모호하게하지 않기 위해 상세하게 나타내지 않을 수 있다.

[0022] [0027] 단어 "예시적인"은 본원에서 "예, 예시, 또는 예증으로서 기능하는 것"을 의미하도록 사용된다. "예시적인"으로서 본원에 설명된 임의의 구현 또는 양상은 반드시 본 개시물의 다른 양상들보다 바람직하거나 유리한 것으로서 해석되지는 않는다. 유사하게, 용어 "양상들"은, 본 개시물의 모든 양상들이 논의된 특징, 이점 또는 동작의 모드를 포함하도록 요구하지 않는다.

[0023] 개관

[0024] [0028] 제 1 양상은, 예상된 또는 의도된 반도체 회로 상에서 소프트웨어가 구동중인지 여부 또는 그 대신에 시뮬레이터 환경 또는 위조 플랫폼상에서 소프트웨어가 구동중인지 여부를 판정하도록 이용될 수 있는 그리고 런타임에 프로세서에 의해 추출될 수 있는 고유하고 복제불가한 플랫폼 식별자를 생성하기 위해 각각의 반도체 회로에서의 고유한 고유 특징들을 이용하는 것을 제공한다. 반도체 제조에 있어서의 변동들로 인해, 동일한 반도체 회로의 2개의 인스턴스들 내의 동일한 회로 경로가 상이한 응답(예를 들어, 경로 지연, 주파수 응답, 전압 응답 등)을 가질 수 있다. 예를 들어, (그러나, 상이한 반도체 회로들 내에서) 동일한 설계의 각각의 데이터-의존 경로에 대한 안정적인 동작을 위해 임계 주파수는 변할 수 있다. 동일한 설계를 갖는 반도체 회로들 사이에서의 이러한 변동들은, 각각의 반도체 회로를 특징화하고 그리고 고유하고 복제불가한 식별자를 생성하기 위해 활용/이용될 수 있다.

[0025] [0029] 제 2 양상은, 상이한 데이터-의존 회로 경로들을 시뮬레이팅하기 위해 상이한 입력 벡터들을 생성하고 적용하는 것, 그리고 그후 각각의 데이터-의존 회로 경로에 대해 주파수 특징들을 추출하는 것을 제공한다. 일 예시에서, 일 세트의 명령들은 다양한 동작들(예를 들어, 상이한 수학적 동작들 등)을 수행하기 위해 주어진 입력을 이용할 수 있다. 이용되는 입력에 의존하여, 수행된 동작들은 상이한 회로 경로들(즉, 데이터-의존 경로들)을 이용할 수 있다. 따라서, 입력 벡터들은 고유하고 복제불가한 플랫폼 식별자를 생성하도록 특징화될 수 있는 복수의 데이터-의존 경로들을 도입하도록 기능할 수 있다. 복수의 입력 벡터들을 이용함으로써, 각각의 회로 경로에 대한 결과들이 불안정해질 때까지(예를 들어, 테스트 결과들이 이전의 테스트들로부터 변화하거나 부정확해질 때까지) 각각의 데이터-의존 회로 경로가 반복적으로 테스트되었다. 각각의 사전-정의된 테스트에 대해 최종 알려진 안정적인 전압/주파수가 고유한 식별자를 생성하는데 이용된다.

[0026] [0030] 제 3 양상은, 복수의 상이한 반도체 회로들 사이에서, 그리고/또는 다수의 내부의 및/또는 외부의 서브-회로들 또는 컴포넌트들에 대해 데이터-의존 회로 경로들을 특징화하는 것을 제공한다. 그후, 상이한 반도체 회로들, 서브-회로들, 및/또는 컴포넌트들에서의 2개 또는 그 초과의 데이터-의존 회로 경로들의 특징화가 고유하고 복제불가한 식별자를 생성하는데 이용된다.

[0027] **고유하고 복제불가한 식별자의 예시적인 생성**

[0028] [0031] 데이터-의존 회로 경로들의 이용 및 물리적 컴포넌트들(예를 들어, 반도체 디바이스들, 전기적 경로들, 전기적 컴포넌트들 등)의 본질적 변동들에 기초하여 하드웨어 디바이스에 대한 고유하고 복제불가한 식별자를 생성하기 위한 메커니즘이 제공된다. 예를 들어, 다수의 반도체 디바이스들이 제조될 때, 복합 반도체 프로세스는 제조업자 또는 설계자의 제어 하에 약간의 변동들을 도입한다. 2개의 반도체 디바이스들이 동일한 실리콘 웨이퍼로부터 제조된다고 하더라도, 동일하게 설계된 전기 배선들/경로들은 그 폭이 아마도 수 나노미터들정도 상이할 것이다. 실리콘의 표면에서의 미시한(microscopic) 차이들은 또한 전기 경로들의 곡률(curvature)에 거의 미미한 변동들을 도입할 수 있다. 추가적으로, 인쇄 회로 보드 상에서의 반도체 디바이스들의 솔더링은 커패시턴스들/임피던스 등에서의 차이들을 야기할 수 있다. 이 고유한 특징들은 물리적 컴포넌트(예를 들어, 반도체 디바이스)에 대해 제어불가하고 고유하기 때문에, 이들을 정량화하는 것은 본질적인, 고유하고 복제불가한 식별자를 생성할 수 있다. 추가적으로, (예를 들어, 하나 또는 그 초과의 반도체 디바이스들을 통해) 하나 또는 그 초과의 데이터-의존 회로 경로들은 식별자의 고유함을 추가로 개선하기 위해 이용될 수 있다.

[0029] [0032] 본 접근방식은, 추가의 로직(예를 들어, 회로 컴포넌트들, 트랜지스터들 등)을 반도체 설계에 부가할 필요가 없고 그리고 심지어는 이미 제조된 반도체 디바이스들에도 적용가능한 제로 원가 솔루션을 제공할 수 있다.

[0030] [0033] 도 1은 온-보드 또는 오프-보드 컴포넌트 또는 회로에 대한 데이터-의존 회로 경로 응답 정보를 활용함으로써 식별자(ID)를 추출하는 방법을 예시한다. 본 예시에서, 컴포넌트 또는 회로(104)는 입력 벡터들(102) 및 식별자 생성기(106)를 포함하는 식별자 생성 모듈에 의해 테스트되고 있다. 몇몇 예시들에 따르면, 컴포넌트 또는 회로는: (a) 전기적으로 패시브 및 액티브인 컴포넌트들을 갖는 인쇄 회로 보드, (b) 반도체 디바이스, 및/또는 (c) 프로세싱 디바이스를 포함할 수 있다. 컴포넌트 또는 회로(104)는 자신의 동작 주파수(118) 및/또는 자신의 동작 전압(120)을 조정함으로써 동적으로 구성가능할 수 있다.

[0031] [0034] 여기 예시된 바와 같이, 컴포넌트 또는 회로(104)는 다수의 데이터-의존 회로 경로들(A(114), B(116), C(118), 및 D(120))을 포함할 수 있다. 예를 들어, 컴포넌트 또는 회로(104)는, 제공된 입력 데이터에 상이하게 의존하여 동작들을 수행하는 신호 프로세서, 산술(arithmetic) 모듈 등일 수 있다. 예를 들어, 가산 및 승산 동작들은 산술 모듈에서 상이한 경로들을 취할 수 있다. 추가적으로, 더 많은 수의 추가적인 동작은 더 적은 수의 가산 동작과는 상이한 경로를 취할 수 있다. 이러한 "경로"는, 예를 들어, 트랜지스터(들)을 지칭할 수 있고, 그리고/또는 특정 동작을 통한 전기 트레이스(electrical trace)들은 컴포넌트 또는 회로(104)에서 수행된다.

[0032] [0035] 입력 벡터들(102)은, 특정한 동작들 및/또는 계산들로 하여금 컴포넌트 또는 회로(104)에 의해 수행되게 하는 하나 또는 그 초과의 명령들 및/또는 데이터 입력을 포함할 수 있다. 입력 벡터의 다양한 예시들은, 동작들, D1 및/또는 D2에 대한 더욱 복잡한 동작들 중에서도, D1+D2, D1×D2, D1/D2, log(D1), 비트단위의 D1 AND D2, D1 XOR D2을 수행하는 것(여기서, D1 및 D2는 데이터 입력들(예를 들어, 수들, 비트 스트링들 등)임)을 포함한다. 입력 벡터들은 상이한 모드들의 동작들에서 컴포넌트 런(component run)을 행하는 임의의 제어 신호들 또는 구성들일 수 있다.

[0033] [0036] 단일 입력 벡터는, 컴포넌트 또는 회로(104)에 대한 동작 주파수(110) 및/또는 전압(112)이 각각의 반복시에 조정되기(예를 들어, 주파수를 증가시키거나 전압을 감소시키는 식임) 때문에, 여러 번 수행될 수 있다. 각각의 반복 이후에, 컴포넌트/회로(104)가 또한 안정적임(예를 들어, 예상되는 또는 정확한 응답/결과를 입력 벡터에 제공함)을 보장하기 위해, 체크가 수행된다. 이 프로세스는, 데이터-의존 회로 경로 응답/결과가 변하는 임계 동작 주파수(또는 임계 동작 전압)가 식별될 때까지, 반복된다. 임계 주파수 및/또는 임계 전압이 식별되면, 데이터-의존 회로 경로에 대한 특정 입력 벡터의 실행은 중단되거나 또는 종결된다. 그후, 컴포넌트 또는 회로에 대한 식별자를 생성하기 위해 (예를 들어, 하나 또는 그 초과의 다른 입력 벡터들에 대해 입력 주파수들과 조합하여) 그 특정 입력 벡터에 대한 이러한 임계 주파수가 이용될 수 있다.

[0034] [0037] 임계 주파수 및/또는 임계 전압은 수많은 방법들에서 확인될 수 있다. 제 1 예시에서, 동작 주파수(110)는 증분적으로 증가되면서, 동작 전압(112)은 고정되어 유지된다. 임계 전압 및/또는 임계 주파수는, 입력 벡터에 대한 응답/결과가 변하거나 또는 부정확한 것들이다.

[0035] [0038] 제 2 예시에서, 동작 전압(112)은 증분적으로 감소되고, 이는 동작 주파수(110)의 대응하는 감소를 야기한다. 예를 들어, 동작 전압(112)은 증분적으로 감소(저하)될 수 있고, 결과들/응답이 변할 때까지 입력 벡터의 각각의 반복이 행해진다. 동작 전압(112)이 감소되기 때문에, 이는 또한 동작 주파수를 감소시킬 수 있다는 것을 주목한다. 특정 입력 벡터에 대한 정확한 결과/응답을 제공하는 마지막 최소 전압(또는 결과 동작

주파수)은, 컴포넌트 또는 회로에 대한 식별자를 생성하는데 (예를 들어, 하나 또는 그 초과의 다른 입력 벡터들에 대한 최소 전압과 조합하여) 이용된다.

[0036] [0039] 제 3 예시에서, 동작 전압(112)은 증분적으로 감소되면서, 동작 주파수(110)는 증분적으로 증가된다. 예를 들어, 주파수와 전압 둘 다의 조합은, 임계 주파수/전압(예를 들어, 특정 데이터 경로가 불안정해지는 주파수/전압 쌍)이 식별될 때까지 (예를 들어, 사전정의된 주파수/전압 쌍에 따라) 조정될 수 있다.

[0037] [0040] 식별자 생성기(106)는, 각각의 테스트 벡터에 대해 최대 안정적인 동작 주파수(또는 가장 낮은 안정 동작 전압)를 파악할 수 있고, 그후 이들을 이용하여 컴포넌트, 회로, 또는 반도체에 대한 고유하고 복제불가한 식별자를 컴퓨팅할 수 있다.

[0038] [0041] 일 예시에서, 컴포넌트, 회로, 또는 반도체의 최대 동작 주파수는 가장 긴(중요) 회로 경로 딜레이(예를 들어, 최대 레이턴시를 갖는 체인 내에서 연결된 일련의 상이한 게이트들 또는 로직 디바이스들)에 의해 결정될 수 있다. 이는 또한, 컴포넌트, 회로, 또는 반도체가, 특정 테스트 벡터에서 컴퓨팅하는 데이터 값들에 의존하는 상이한 경로 딜레이들을 갖는 더 짧은 경로들을 갖는다는 것을 의미한다. 회로 경로 딜레이에 대한 반도체 프로세스 변동들의 영향으로 인해, 동일한 설계이지만 상이한 컴포넌트들, 회로들, 또는 반도체들에서의 각각의 데이터-의존 임계 경로의 최대 주파수/최소 전압은 불규칙 변동(random variation)들을 가질 것이다. 이는 또한, 각각의 데이터-의존 회로 경로의 이러한 최대 주파수(또는 가장 낮은 전압) 정보의 특징화가 특정 컴포넌트, 회로 및/또는 반도체에 대한 식별 정보의 양호한 소스인 것으로 함축한다.

[0039] [0042] 일부 구현들에서, 데이터-의존 회로 경로들은 입력을 수신하고 출력을 제공하는 동적 회로 경로들일 수 있다. 그래서, 이들은 비-저장 및/또는 비-메모리 회로 경로들이다.

[0040] [0043] 도 2는 다수의 온-보드 또는 오프-보드 컴포넌트들 또는 회로들로부터의 데이터-의존 회로 경로 응답 정보를 활용함으로써 플랫폼 식별(ID)를 추출하는 방식을 예시한다. 이 양상은, 도 1에 설명된 접근방식과 유사하지만 하나 또는 그 초과의 입력 벡터들(202)을 구동하기 위해 이용되는 복수의 컴포넌트들 또는 회로들(204, 206, 및 208)을 갖는다. 각각의 컴포넌트 또는 회로(204, 206, 및 208)에 대해, 각각의 컴포넌트 또는 회로(204, 206, 및 208)에 대해 대응하는 동작 전압 및/또는 동작 주파수를 반복적으로 조절하면서, 입력 벡터가 구동될 수 있다.

[0041] [0044] 일 구현에서, 제 1 컴포넌트 또는 회로(204)의 동작 주파수는, 제 1 컴포넌트 또는 회로(204) 내의 하나 또는 그 초과의 데이터-의존 경로들에 대한 최대 안정 주파수를 확인하기 위해 증가될 수 있다. 한편, 제 2 컴포넌트 또는 회로(206)의 동작 전압은, 제 2 컴포넌트 또는 회로(206)에서 하나 또는 그 초과의 데이터-의존 경로들에 대한 최소 안정 전압을 확인하기 위해 감소될 수 있다. 유사하게, 제 3 컴포넌트 또는 회로(208)의 동작 주파수/전압 쌍은 제 3 컴포넌트 또는 회로(208) 내의 하나 또는 그 초과의 데이터-의존 경로들에 대한 임계 안정 주파수/전압 쌍을 확인하도록 조정될 수 있다. 식별자 생성기는 그후 플랫폼(예를 들어, 컴포넌트들 또는 회로들의 조합)에 대한 고유하고 복제불가한 본질적인 식별자를 컴퓨팅하기 위해 복수의 컴포넌트들 또는 회로들(204, 206, 및 208)에 대한 이러한 응답 정보를 이용할 수 있다.

[0042] [0045] 도 3은, 상이한 동작 주파수들에서 일 세트의 입력 벡터들에 대한 예시적인 결과들을 도시하는 표이다. 이러한 입력 벡터들은, 하나 또는 그 초과의 컴포넌트들, 회로들, 및/또는 반도체 디바이스들에 대해 수행되었을 수도 있다. 입력 벡터들 각각(예를 들어, 테스트-a, 테스트-b, 테스트-c, 테스트-d)은, 하나 또는 그 초과의 주파수들(주파수-A, 주파수-B, 주파수-C, 주파수-D, 주파수-E, 및/또는 주파수-F)에 걸쳐 동작 주파수가 증분적으로 조절(예를 들어, 증가)되기 때문에, 반복적으로 실행될 수 있다. 인식될 수 있는 바와 같이, 각각의 입력 벡터에 대한 데이터-의존 회로 경로에 의존하여, 입력 벡터는 최대/임계 동작 주파수까지(up to) 통과(Pass) 또는 실패(Fail)할 수 있다. 통과는, 데이터-의존 회로 경로가 특정 동작 주피수에서의 예상되는 또는 정확한 응답을 입력 벡터에 제공했다는 것을 의미한다. 실패는, 데이터-의존 회로 경로가 특정 동작 주파수에서 부정확한, 예상밖의, 또는 변화된 응답을 입력 벡터에 제공했다는 것을 의미한다. 예를 들어, 테스트-c에서, 통과로부터 실패로의 천이는, 주파수-C와 주파수-D 사이에서 발생한다. 따라서, 임계 주파수는 주파수-C 또는 주파수-D로서 선택될 수 있다. 입력 벡터가 통과에서 실패로 천이하는 이러한 임계 주파수는, 플랫폼과 연관된 고유한 복제가능한 식별자를 생성하기 위해 기록되고 이용될 수 있다.

[0043] [0046] 도 4는, 상이한 동작 전압들에서 일 세트의 입력 벡터들에 대한 예시적인 결과들을 나타내는 표이다. 이러한 입력 벡터들은 하나 또는 그 초과의 컴포넌트들, 회로들, 및/또는 반도체 디바이스들 상에서 수행되었을 수도 있다. 입력 벡터들(예를 들어, 테스트-a, 테스트-b, 테스트-c, 테스트-d) 각각은, 동작 전압이 하나 또는

그 초과의 전압들(전압-A, 전압-B, 전압-C, 전압-D, 전압-E, 및/또는 전압-F)을 걸쳐 증분적으로 조정(예를 들어, 감소)될 수 있기 때문에 반복적으로 실행될 수 있다. 인식될 수 있는 바와 같이, 각각의 입력 벡터에 대한 데이터-의존 회로 경로에 의존하여, 입력 벡터는 최소/임계 동작 전압까지(up to) 통과 또는 실패할 수 있다. 통과는, 데이터-의존 회로 경로가 특정 동작 전압에서 예상되는 또는 정확한 응답을 입력 벡터에 제공했다는 것을 의미한다. 실패는, 데이터-의존 회로 경로가 특정 동작 전압에서 부정확한, 예상밖의, 또는 변화된 응답을 입력 벡터에 제공했다는 것을 의미한다. 예를 들어, 테스트-a에서, 통과로부터 실패로의 천이는 전압-D 및 전압-E 사이에서 발생한다. 이에 따라, 임계 전압은 전압-D 또는 전압-E로서 선택될 수 있다. 입력 벡터가 통과에서 실패로 천이하는 이러한 임계 전압은, 플랫폼과 연관된 고유하고 복제불가한 식별자를 생성하기 위해 기록되고 이용될 수 있다.

[0044] [0047] 도 5는, 상이한 동작 주파수-전압 쌍들에서 일 세트의 입력 벡터들에 대한 예시적인 결과들을 나타내는 표를 예시한다. 이러한 입력 벡터들은, 하나 또는 그 초과의 컴포넌트들, 회로들, 및/또는 반도체 디바이스들에 대해 수행되었을 수도 있다. 입력 벡터들(예를 들어, 테스트-a, 테스트-b, 테스트-c, 테스트-d) 각각은, 동작 주파수/전압 쌍이 하나 또는 그 초과의 주파수/전압 쌍들(주파수/전압-A, 주파수/전압-B, 주파수/전압-C, 주파수/전압-D, 주파수/전압-E, 및/또는 주파수/전압-F)에 걸쳐 증분적으로 조정(예를 들어, 증가 또는 감소)되기 때문에, 반복적으로 실행될 수 있다. 인식될 수 있는 바와 같이, 각각의 입력 벡터에 대한 데이터-의존 회로 경로에 의존하여, 입력 벡터는 임계 동작 주파수-전압 쌍까지(up to) 통과 또는 실패할 수 있다. 통과는, 데이터-의존 회로 경로가 특정 동작 주파수/전압 쌍에서 예상된 또는 정확한 응답을 입력 벡터에 제공했다는 것을 의미한다. 실패는, 데이터-의존 회로 경로가 특정 동작 주파수/전압 쌍에서 부정확한, 예상밖의, 또는 변화된 응답을 입력 벡터에 제공했다는 것을 의미한다. 예를 들어, 테스트-d에서, 통과로부터 실패로의 천이는 주파수/전압-B와 주파수/전압-C 사이에서 발생한다. 따라서, 임계 주파수/전압 쌍은 전압-B 또는 전압-C로서 선택될 수 있다. 입력 벡터가 통과에서 실패로 천이하는 이러한 임계 주파수/전압 쌍은, 플랫폼과 연관된 고유하고 복제불가한 식별자를 생성하기 위해 기록되고 이용될 수 있다.

[0045] [0048] 도 6은 데이터-의존 회로 경로들에 기초하여 고유하고 복제불가한 식별자를 컴퓨팅하도록 적응될 수 있는 예시적인 프로세싱 회로를 예시한다. 일 예시에서, 프로세싱 회로(602)는 하나 또는 그 초과의 데이터-의존 회로 경로들에 대한 특징들에 기초하여 고유한 식별자의 생성을 유발하기 위한 명령들을 포함하는 외부의 저장 디바이스(604)에 커플링될 수 있다. 다른 예시에서, 저장 디바이스(604)는 하나 또는 그 초과의 데이터-의존 회로 경로들에 대한 특징들에 기초하여 고유한 식별자의 생성을 유발하기 위해 프로세싱 회로(602)와 통합될 수 있다. 프로세싱 회로(602)는 또한, 하나 또는 그 초과의 내부의 서브-회로들(610, 612, 및/또는 614) 및/또는 하나 또는 그 초과의 외부 컴포넌트들(616, 618, 및 620)에 대한 동작 주파수를 조정하는 것을 허용하는 프로그래머블 주파수 모듈(622)(예를 들어, 클록 발생기 등)을 포함할 수 있다. 추가적으로, 프로세싱 회로(602)는 또한 하나 또는 그 초과의 내부 서브-회로들(610, 612, 및/또는 614) 및/또는 하나 또는 그 초과의 외부 컴포넌트들(616, 618, 및 620)에 대한 동작 전압을 조정하는 것을 허용하는 프로그래머블 전압 모듈(624)을 포함할 수 있다.

[0046] [0049] 프로세싱 회로(602)는 하나 또는 그 초과의 내부 서브-회로들(610, 612, 및/또는 614) 및/또는 하나 또는 그 초과의 외부 컴포넌트들(616, 618, 및 620)에 대한 데이터-의존 경로 응답 정보를 확인하기 위해 저장 디바이스(604)로부터 하나 또는 그 초과의 명령들을 포함 또는 획득할 수 있다. 하나 또는 그 초과의 입력 벡터들(606)은, 서브-회로들(610, 612, 614) 및/또는 컴포넌트들(616, 618, 620) 상에서 하나 또는 그 초과의 동작들을 실행 또는 수행하기 위해 프로세싱 회로에 의해 이용될 수 있다. 이러한 입력 벡터들은, 임계 주파수 및/또는 임계 전압이 각각의 데이터-의존 회로 경로에 대해 확인될 때까지 테스트되고 있는 서브-회로들(610, 612, 614) 또는 컴포넌트들(616, 618, 620) 각각의 동작 주파수 및/또는 동작 전압을 증분적으로 조절하면서 다수 회 구동될 수 있다. 식별자 생성기(608)는 다음으로 고유한 식별자(622)를 생성하도록 테스트된 복수의 데이터-의존 경로들에 대한 결과 임계 주파수들 및/또는 임계 전압들을 이용한다.

[0047] [0050] 일 예시에서, 고유한 식별자는, 프로세싱 회로(602), 내부/외부 회로들(610, 612, 614) 및/또는 컴포넌트들(616, 618, 620)을 포함하는 플랫폼과 연관된다.

[0048] [0051] 다른 예시에서, 고유한 식별자는 프로세싱 회로 상에서의 소프트웨어 애플리케이션 설치 또는 실행과 연관된다.

[0049] [0052] 또 다른 예시에서, 프로세싱 회로(602) 상에서의 소프트웨어 애플리케이션의 실행은 고유한 식별자의 성공적인 검증에 바인딩될수 있다. 예를 들어, 소프트웨어 애플리케이션이 실행되는 매번, 고유한 식별자에 기초

하여 설치되었을 때와 동일한 플랫폼상에서 여전히 실행되고 있다는 것을 확인하기 위해 검증이 수행된다. 고유한 식별자의 성공적인 검증은, 고유한 식별자의 오리지널 인스턴스와 고유한 식별자의 후속 생성된 인스턴스가 동일한지 확인하기 위해, 이들을 비교할 수 있다.

[0050] [0053] 도 7은 하나 또는 그 초과의 온-보드 및/또는 오프-보드 컴포넌트들, 회로들, 및/또는 반도체들에 대한 데이터-의존 회로 경로 응답 정보를 활용함으로써 고유하고 복제불가한 플랫폼 식별자(ID)를 컴퓨팅하기 위한 방법을 예시한다. 하나 또는 그 초과의 테스트들(예를 들어, 입력 벡터들, 계산 동작들 등)은, 하나 또는 그 초과의 회로들(702)에 대한 하나 또는 그 초과의 데이터-의존 회로 경로들에 대해 수행될 수 있다. 하나 또는 그 초과의 회로들은 식별자-특정 회로들이라기 보다 오히려 범용 회로들일 수도 있다는 점에 주목한다. 일부 예시들에서, 하나 또는 그 초과의 회로들은 비-저장 및/또는 비-메모리 회로들이다.

[0051] [0054] 하나 또는 그 초과의 테스트들은, 하나 또는 그 초과의 회로들(704) 각각에 대한 동작 주파수 및/또는 전압을 조정하면서 하나 또는 그 초과의 회로들에 대한 하나 또는 그 초과의 데이터-의존 회로 경로들에 대해 반복될 수 있다. 예를 들어, 하나 또는 그 초과의 회로들 각각에 대한 동작 주파수는 증가될 수 있고, 그리고/또는 하나 또는 그 초과의 회로들에 대한 동작 전압은 감소될 수 있다. 임계 주파수 및/또는 전압은 하나 또는 그 초과의 데이터-의존 회로 경로들(706) 각각에 대해 확인될 수 있다. 예를 들어, 이러한 임계 주파수 또는 전압은, 특정 테스트가 실패하기 시작하는(예를 들어, 결과/응답이 변하는) 최대 주파수 또는 최소 전압일 수 있다.

[0052] [0055] 식별자는 그후 하나 또는 그 초과의 데이터-의존 회로 경로들(708)에 대해 확인된 복수의 임계 주파수들 및/또는 전압들에 기초하여 생성될 수 있다. 일 예시에서, 식별자는 하나의 회로에 대한 2개 또는 그 초과의 상이한 회로 경로들에 대해 2개 또는 그 초과의 임계 주파수들 및/또는 임계 전압들에 기초(예를 들어, 생성)할 수 있다. 다른 예시에서, 식별자는 2개 또는 그 초과의 상이한 회로들에 대해 2개 또는 그 초과의 상이한 회로 경로들에 대한 2개 또는 그 초과의 임계 주파수들 및/또는 임계 전압들에 기초할 수 있다.

[0053] [0056] 식별자가 초기에 생성되는 경우, 식별자는 후속 검증을 위해 (예를 들어, 비-휘발성 메모리에) 저장될 수 있다(710). 예를 들어, 소프트웨어 애플리케이션은 이것이 플랫폼 상에 설치될 때 제 1 식별자를 획득 및 저장할 수 있고, 이에 의해 플랫폼에 대한 하나 또는 그 초과의 특정 회로들, 마이크로프로세서들, 및/또는 반도체 디바이스들에 이 소프트웨어 설치를 바인딩한다.

[0054] [0057] 식별자가 검증되고 있는 경우, 이전에 저장된 식별자는 리트리브된다(712). (단계(708)로부터) 새롭게 생성된 식별자는 그후, 이전에 저장된 식별자와 비교되어 이들이 동일한지가 확인된다(714). 이들이 동일하다면, 저장된 식별자와 새롭게 생성된 식별자 둘 다를 생성하기 위해 이용된 플랫폼은 동일하고 그리고 검증은 성공적인 것으로 결론 내려질 수 있다. 이와 달리, 새롭게 생성된 식별자 및 저장된 식별자가 상이하다면, 검증은 실패한다. 예를 들어, 소프트웨어 애플리케이션의 후속 스타트-업 시에, 이전에 저장된 식별자에 대해 새롭게 생성된 식별자를 검증함으로써 자신의 오리지널 플랫폼상에서 여전히 실행되고 있고, 이에 의해 플랫폼에 대한 하나 또는 그 초과의 특정 회로들, 마이크로프로세서들, 및/또는 반도체 디바이스들에 이 소프트웨어 설치를 바인딩한다고 검증할 수 있다.

[0055] [0058] 시스템-온-칩 플랫폼에 대해 2개의 예시적인 구현 시나리오들이 정의될 수 있다. 제 1 예시에서, 프로세서는, 프로세서와 통신하기 위해 온-칩 버스에 커플링된 플랫폼 식별자 추출 제어 소프트웨어, 프로그래머블 클록 생성기, 및 온-칩 계산 컴포넌트를 갖는다. 온-칩 계산 컴포넌트는, 식별자를 생성하기 위해 식별자 추출 제어 소프트웨어에 의해 이용될 수 있는 하나 또는 그 초과의 데이터-의존 회로 경로들을 제공할 수 있다. 제 2 예시에서, 프로세서는, 프로세서와 통신하기 위해 플랫폼 식별자 추출 제어 소프트웨어, 프로그래머블 클록 생성기, 및 오프-칩 계산 컴포넌트를 갖는다. 여기서, 오프-칩 계산 컴포넌트는, 식별자를 생성하기 위해 식별자 추출 제어 소프트웨어에 의해 이용될 수 있는 하나 또는 그 초과의 데이터-의존 회로 경로들을 제공할 수 있다.

[0056] [0059] 예시적인 구현 시나리오들 둘 다에서, 프로세서는 안정 상태의 지정 주파수에서 동작할 수 있고, 그리고 수개의 단계들을 실행할 수 있다. 먼저, 제어 소프트웨어는 제 1 동작 주파수에서 온/오프-칩 계산 컴포넌트들을 테스트하기 위해 상이한 데이터-의존 회로 경로들을 어드레싱할 수 있는 테스트(입력) 벡터들의 수집으로 구동/실행될 수 있다. 두 번째로, 제어 소프트웨어는 그후 테스트(while) 벡터들을 통해 구동/실행될 수 있으면서, 동시에 클록 주파수 생성기는 각각의 데이터-의존 회로 경로에 대한 임계 주파수(예를 들어, 최대 주파수)가 확인 및/또는 기록될 때까지 테스트 중인 계산 컴포넌트에 공급된 클록 주파수(예를 들어, 동작 주파수)를 증가 또는 감소시키도록 조정된다. 비교 및 양자화 절차는 그후, 또한 플랫폼 식별자일 수도 있는 고유한 식별

자를 생성하는데 이용될 수 있다. 플랫폼이 다수의 온-칩 및/또는 오프-칩 계산 컴포넌트들을 가지면, 다수의 추출된 식별자들은 단일의 플랫폼 식별자로 조합될 수 있다.

[0057] [0060] 이러한 접근방식은 기존의 프로세서들, 반도체들, 및/또는 칩들에 적용가능할 수 있고, 이들 중 대부분은 이미 저전력 소모를 위해 인에이블되는 플렉서블 클록 주파수 제어 메커니즘을 갖는다. 추가적으로, 고유한 식별자를 생성하기 위한 이러한 접근방식은, 외부의 고가의 테스팅 셋업들 및 절차들을 이용할 필요가 없는 하드웨어에 바인딩된다. 더욱이, 소프트웨어 요청들에 의해 이용가능하게 될 수 있는 추가의 하드웨어 로직 및 그 기능을 부가함으로써 현재 칩 설계를 개정할 필요는 없으며, 그로 인해 이것은 제로 원가 솔루션이다.

[0058] [0061] 도면들에 예시된 컴포넌트들, 단계들, 특징들 및/또는 기능들 중 하나 또는 그 초과는, 단일 컴포넌트, 단계, 특징 또는 기능으로 재배열 및/또는 조합될 수 있거나 또는 몇몇 컴포넌트들, 단계들, 또는 기능들로 구현될 수 있다. 본 발명으로부터 벗어나지 않고 추가적인 엘리먼트들, 컴포넌트들, 단계들, 및/또는 기능들이 또한 부가될 수 있다. 도면들에 예시된 장치, 디바이스들, 및/또는 컴포넌트들은, 도면들에 설명된 방법들, 특징들, 또는 단계들 중 하나 또는 그 초과를 수행하도록 구성될 수 있다. 본원에 설명된 알고리즘들이 또한 소프트웨어로 효율적으로 구현될 수 있고 그리고/또는 하드웨어에 내장될 수 있다.

[0059] [0062] 더욱이, 본 개시물의 일 양상에서, 도면들에 예시된 프로세싱 회로(들)는 도면들에 설명된 알고리즘들, 방법들, 및/또는 단계들을 수행하기 위해 특정하게 설계 및/또는 하드-와이어링된 특수목적 프로세서(예를 들어, ASIC(application specific integrated circuit))일 수 있다. 따라서, 이러한 특수목적 프로세서(예를 들어, ASIC)는 도면들에 설명된 알고리즘들, 방법들, 및/또는 단계들을 실행하기 위한 수단의 일례이다. 컴퓨터-판독가능 저장 매체는 또한, 특수목적 프로세서(예를 들어, ASIC)에 의해 실행될 때, 특수목적 프로세서로 하여금, 도면들에 설명된 알고리즘들, 방법들, 및/또는 단계들을 수행하게 하는 프로세서 판독가능 명령들을 저장할 수 있다.

[0060] [0063] 또한, 본 개시물의 양상들이 플로우차트, 흐름도, 구조도, 또는 블록도로 도시된 프로세스로서 설명될 수 있음이 주목된다. 플로우차트가 순차적 프로세스로서 동작들을 설명할 수 있지만, 수많은 동작들이 병행하여 또는 동시에 수행될 수 있다. 이에 더해, 동작들의 순서는 재-바열될 수 있다. 프로세스는, 자신의 동작들이 완료될 때 종결된다. 프로세스는, 방법, 함수, 절차, 서브루틴, 서브프로그램 등에 대응할 수 있다. 프로세스가 함수에 대응하는 경우, 자신의 종결은 호 함수 또는 메인 함수로의 함수의 복귀에 대응한다.

[0061] [0064] 더욱이, 저장 매체는, 판독-전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 자기 디스크 저장 매체들, 광학 저장 매체들, 플래시 메모리 디바이스들 및/또는 다른 머신-판독가능 매체들및 프로세서-판독가능 매체들, 및/또는 정보를 저장하기 위한 컴퓨터-판독가능 매체들을 포함하는, 데이터를 저장하기 위한 하나 또는 그 초과의 디바이스들을 나타낼 수 있다. 용어들 "머신-판독가능 매체", "컴퓨터-판독가능 매체", 및/또는 "프로세서-판독가능 매체"는, 휴대용 또는 고정형 저장 디바이스들과 같은 비-일시적 매체들, 광학 저장 디바이스들, 및 명령(들) 및/또는 데이터를 저장하거나 포함하거나 또는 반송할 수 있는 다양한 다른 매체들을 포함할 수 있다(그러나, 이에 제한되지 않음). 따라서, 본원에 설명된 다양한 방법들은, "머신-판독가능 매체", "컴퓨터-판독가능 매체", 및/또는 "프로세서-판독가능 매체"에 저장될 수 있고 그리고 하나 또는 그 초과의 프로세서들, 머신들, 및/또는 디바이스들에 의해 실행될 수 있는 명령들 및/또는 데이터에 의해 완전하게 또는 부분적으로 구현될 수 있다.

[0062] [0065] 게다가, 본 개시물의 양상들은 하드웨어, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드, 또는 이들의 조합에 의해 구현될 수 있다. 소프트웨어, 펌웨어, 미들웨어 또는 마이크로코드로 구현될 때, 필수적인 태스크들을 수행하기 위한 프로그램 코드 또는 코드 세그먼트들이 저장 매체 또는 다른 저장소(들)과 같은 머신-판독가능 매체에 저장될 수 있다. 프로세서는 필수적인 태스크들을 수행할 수 있다. 코드 세그먼트는 프로시져, 함수, 서브프로그램, 프로그램, 루틴, 서브루틴, 모듈, 소프트웨어 패키지, 클래스, 또는 명령들, 데이터 구조들, 또는 프로그램 스테이트먼트들의 임의의 조합을 나타낼 수 있다. 코드 세그먼트는 정보, 데이터, 인수(argument)들, 파라미터들, 또는 메모리 컨텐츠들을 전달 및/또는 수신함으로써 다른 코드 세그먼트 또는 하드웨어 회로에 커플링될 수 있다. 정보, 인수들, 파라미터들, 데이터 등은 메모리 공유, 메시지 전달, 토큰 전달, 네트워크 송신 등을 포함하는 임의의 적절한 수단을 통해서 전달, 포워딩, 또는 송신될 수 있다.

[0063] [0066] 본원에 개시된 예시들에 관련하여 설명된 다양한 예시적인 로지컬 블록들, 모듈들, 회로들, 엘리먼트들, 및/또는 컴포넌트들은 범용 프로세서, 디지털 신호 프로세서(DSP), 주문형 집적 회로(ASIC), 필드 프로그램가능 게이트 어레이(FPGA) 또는 다른 프로그램 가능 로직 컴포넌트, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본원에 설명된 기능들을 수행하도록 설계된 이들의 임의의 조합으로 구현되거나 수행될 수

있다. 범용 프로세서는 마이크로프로세서일 수 있지만, 대안적으로 이 프로세서는 임의의 종래의 프로세서, 컨트롤러, 마이크로컨트롤러, 또는 상태 머신일 수 있다. 또한, 프로세서는 컴퓨팅 디바이스들의 조합, 예를 들면, DSP와 마이크로프로세서의 조합, 다수의 마이크로프로세서들, DSP 코어와 협력하는 하나 또는 그 초과의 마이크로프로세서들, 또는 임의의 다른 이러한 구성으로서 구현될 수 있다.

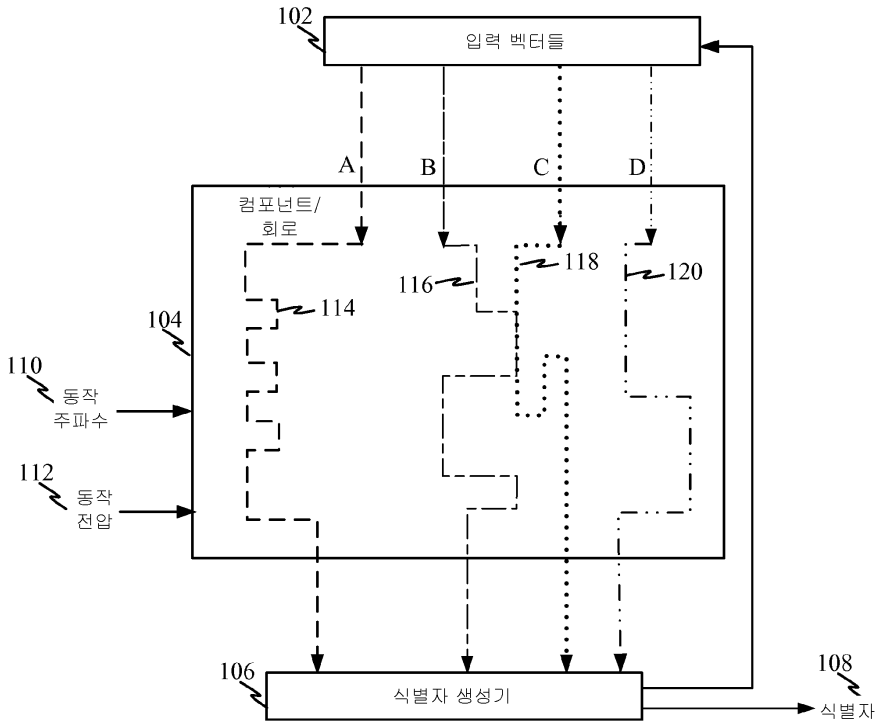
[0064] [0067] 본원에 개시된 예시들과 관련하여 설명된 방법들 또는 알고리즘들은 직접 하드웨어로 구현되거나, 프로세서에 의해 실행가능한 소프트웨어 모듈로 구현되거나, 또는 이 둘의 조합으로, 프로세싱 유닛, 프로그래밍 명령들, 또는 다른 지시들의 형태로 구현될 수 있고, 그리고 단일 디바이스에 포함될 수 있거나 또는 다수의 디바이스들에 걸쳐 분포될 수 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드 디스크, 탈착식 디스크, CD-ROM, 또는 당업계에 공지된 임의의 다른 형태의 저장 매체에 상주할 수 있다. 저장 매체는, 프로세서가 저장 매체로부터 정보를 판독하고 저장 매체에 정보를 기록할 수 있도록, 프로세서에 커플링될 수 있다. 대안적으로, 저장 매체는 프로세서에 통합될 수 있다.

[0065] [0068] 본원에 개시된 양상들과 관련하여 설명되는 다양한 예시적인 로지컬 블록들, 모듈들, 회로들 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 이들 둘의 조합들로서 구현될 수 있다는 점을 당업자들은 더 이해할 것이다. 하드웨어 및 소프트웨어의 상호 교환 가능성을 명시적으로 설명하기 위해, 다양한 예시적 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 그들의 기능과 관련하여 일반적으로 앞서 설명되어 있다. 이러한 기능이 하드웨어로 구현되는지 또는 소프트웨어로 구현되는지는 특정 애플리케이션 및 전체 시스템에 부과되는 설계 제약들에 의존한다.

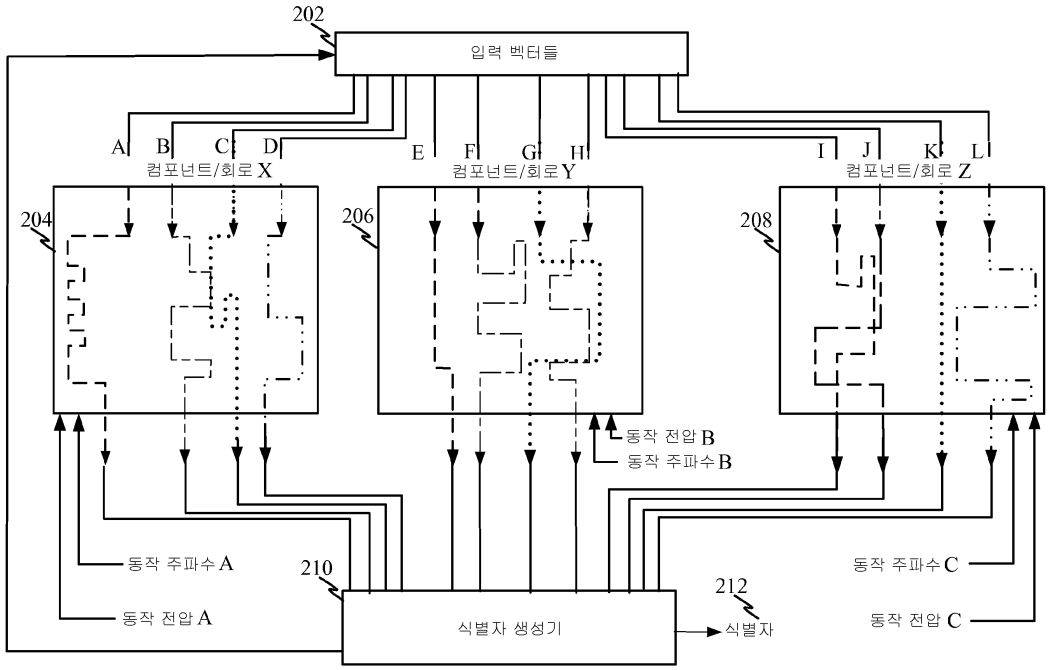
[0066] [0069] 본원에 설명된 본 발명의 다양한 특징들은, 본 발명으로부터 벗어나지 않고 상이한 시스템들로 구현될 수 있다. 본 개시물의 전술한 양상들은 단지 예시들이며 본 발명을 제한하는 것으로서 해석되어서는 안된다는 점에 주의해야 한다. 본 개시물의 양상들의 설명은 예시적이며 청구항들의 범위를 제한하지 않는 것으로 의도된다. 이와 같이, 본 교시들은 다른 유형들의 장치들에 쉽게 적용될 수 있으며, 수많은 대안들, 변형들, 및 변화들이 당업자들에게는 명백하게 될 것이다.

도면

도면1



도면2



도면3

입력 벡터	주파수-A	주파수-B	주파수-C	주파수-D	주파수-E	주파수-F
테스트-a	통과	통과	통과	통과	실패	실패
테스트-b	통과	통과	통과	통과	통과	실패
테스트-c	통과	통과	통과	실패	실패	실패
테스트-d	통과	통과	실패	실패	실패	실패

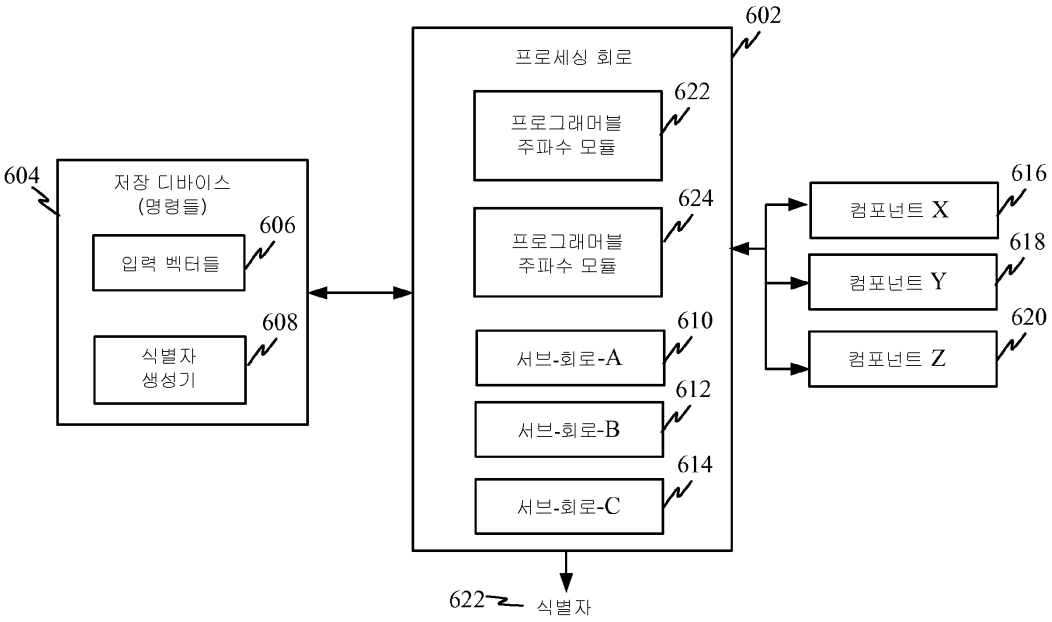
도면4

입력 벡터	전압-A	전압-B	전압-C	전압-D	전압-E	전압-F
테스트-a	통과	통과	통과	통과	실패	실패
테스트-b	통과	통과	통과	통과	통과	실패
테스트-c	통과	통과	통과	실패	실패	실패
테스트-d	통과	통과	실패	실패	실패	실패

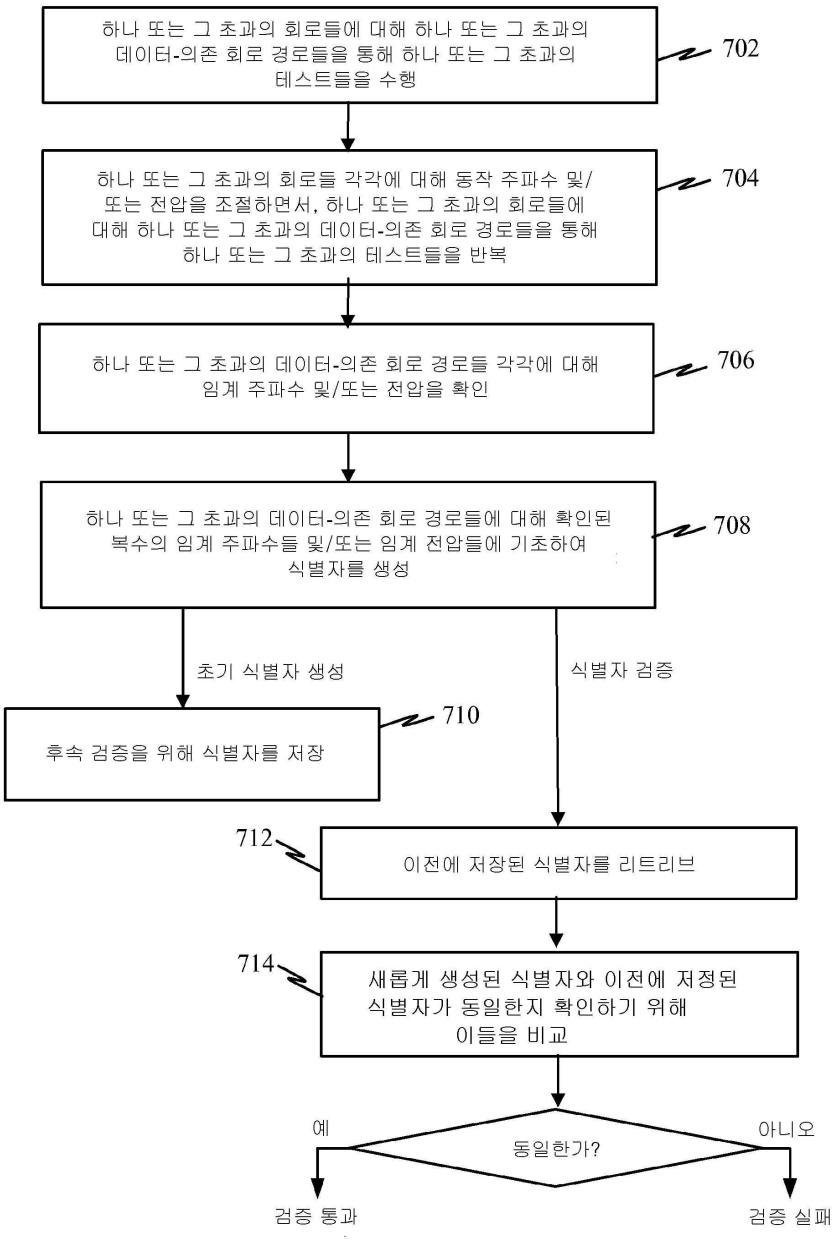
도면5

입력 벡터	주파수/전압-A	주파수/전압-B	주파수/전압-C	주파수/전압-D	주파수/전압-E	주파수/전압-F
테스트-a	통과	통과	통과	통과	실패	실패
테스트-b	통과	통과	통과	통과	통과	실패
테스트-c	통과	통과	통과	실패	실패	실패
테스트-d	통과	통과	실패	실패	실패	실패

도면6


602
프로세싱 회로
622
프로그래머블
주파수 모듈
624
프로그래머블
주파수 모듈
610
서브-회로-A
612
서브-회로-B
614
서브-회로-C
622
식별자
604
저장 디바이스
(명령들)
606
입력 벡터들
608
식별자
생성기
616
컴포넌트 X
618
컴포넌트 Y
620
컴포넌트 Z

도면7


하나 또는 그 초과의 회로들에 대해 하나 또는 그 초과의 데이터-의존 회로 경로들을 통해 하나 또는 그 초과의 테스트들을 수행
702
하나 또는 그 초과의 회로들 각각에 대해 동작 주파수 및/또는 전압을 조절하면서, 하나 또는 그 초과의 회로들에 대해 하나 또는 그 초과의 데이터-의존 회로 경로들을 통해 하나 또는 그 초과의 테스트들을 반복
704
하나 또는 그 초과의 데이터-의존 회로 경로들 각각에 대해 임계 주파수 및/또는 전압을 확인
706
하나 또는 그 초과의 데이터-의존 회로 경로들에 대해 확인된 복수의 임계 주파수들 및/또는 임계 전압들에 기초하여 식별자를 생성
708
초기 식별자 생성
식별자 검증
후속 검증을 위해 식별자를 저장
710
712
이전에 저장된 식별자를 리트리브
714
새롭게 생성된 식별자와 이전에 저정된 식별자가 동일한지 확인하기 위해 이들을 비교
예
동일한가?
아니오
검증 통과
검증 실패