



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0112233
(43) 공개일자 2020년10월05일

(51) 국제특허분류(Int. Cl.)
G06F 21/14 (2013.01) G06F 21/76 (2013.01)
(52) CPC특허분류
G06F 21/14 (2013.01)
G06F 21/76 (2013.01)
(21) 출원번호 10-2019-0032385
(22) 출원일자 2019년03월21일
심사청구일자 2019년03월21일

(71) 출원인
국방과학연구소
대전광역시 유성구 북유성대로488번길 160 (수남동)
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
김희동
대전광역시 유성구 북유성대로488번길 160 (수남동)
이형민
서울특별시 성북구 안암로 145 (안암동5가)
(뒷면에 계속)
(74) 대리인
제일특허법인(유)

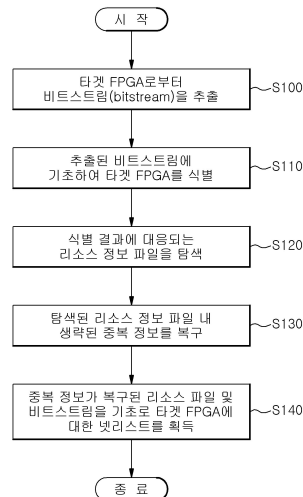
전체 청구항 수 : 총 9 항

(54) 발명의 명칭 FPGA 역공학 장치 및 방법

(57) 요약

본 발명의 일 실시예에 따른 FPGA 역공학 방법은, 타겟 FPGA(field programmable gate array)로부터 비트스트림(bitstream)을 추출하는 단계; 상기 추출된 비트스트림에 기초하여 상기 타겟 FPGA를 식별하는 단계; 상기 식별 결과에 대응되는 리소스 정보 파일을 탐색하는 단계; 상기 탐색된 리소스 정보 파일 내 생략된 중복 정보를 복구하는 단계; 및 상기 중복 정보가 복구된 리소스 파일 및 상기 비트스트림을 기초로 상기 타겟 FPGA에 대한 넷리스트(Netlist)를 획득하는 단계를 포함한다.

대표도 - 도3



(72) 발명자

김영민

서울특별시 노원구 광운로 20 (월계동)

이한솔

서울특별시 성북구 안암로 145 (안암동5가)

유호영

서울특별시 노원구 광운로 20 (월계동)

이상일

서울특별시 성북구 안암로 145 (안암동5가)

명세서

청구범위

청구항 1

타겟 FPGA(field programmable gate array)로부터 비트스트림(bitstream)을 추출하는 단계;
 상기 추출된 비트스트림에 기초하여 상기 타겟 FPGA를 식별하는 단계;
 상기 식별 결과에 대응되는 리소스 정보 파일을 탐색하는 단계;
 상기 탐색된 리소스 정보 파일 내 생략된 중복 정보를 복구하는 단계; 및
 상기 중복 정보가 복구된 리소스 파일 및 상기 비트스트림을 기초로 상기 타겟 FPGA에 대한 넷리스트(Netlist)를 획득하는 단계를 포함하는
 FPGA 역공학 방법.

청구항 2

제 1 항에 있어서,
 상기 중복 정보는,
 복수의 프리머티브(primitive)에 대해 지원 가능한 사이트(site) 정보를 포함하는
 FPGA 역공학 방법.

청구항 3

제 1 항에 있어서,
 상기 중복 정보를 복구하는 단계는,
 FPGA 캐드 툴(CAD tool)에 상기 탐색된 리소스 정보 파일을 입력하여 상기 생략된 중복 정보를 복구하는
 FPGA 역공학 방법.

청구항 4

제 1 항에 있어서,
 상기 넷리스트를 획득하는 단계는,
 상기 중복 정보가 복구된 리소스 파일 및 상기 비트스트림을 기초로 프로그램 가능 상호 접속점(programmable interconnect point) 정보와 프로그램 가능 로직 지점(programmable logic point) 정보를 복구하는 단계; 및
 상기 복구된 프로그램 가능 상호 접속점 정보와 프로그램 가능 로직 지점 정보를 기초로 상기 넷리스트를 획득하는 단계를 포함하는
 FPGA 역공학 방법.

청구항 5

타겟 FPGA(field programmable gate array)로부터 비트스트림(bitstream)을 추출하는 추출부;
 상기 추출된 비트스트림에 기초하여 상기 타겟 FPGA를 식별하는 식별부;
 상기 식별 결과에 대응되는 리소스 정보 파일을 탐색하는 탐색부;
 상기 탐색된 리소스 정보 파일 내 생략된 중복 정보를 복구하는 복구부; 및
 상기 중복 정보가 복구된 리소스 파일 및 상기 비트스트림을 기초로 상기 타겟 FPGA에 대한 넷리스트(Netlist)

를 획득하는 획득부를 포함하는

FPGA 역공학 장치.

청구항 6

제 5 항에 있어서,

상기 중복 정보는,

복수의 프리머티브(primitive)에 대해 지원 가능한 사이트(site) 정보를 포함하는

FPGA 역공학 장치.

청구항 7

제 5 항에 있어서,

상기 복구부는,

FPGA 캐드 툴(CAD tool)에 상기 탐색된 리소스 정보 파일을 입력하여 상기 생략된 중복 정보를 복구하는

FPGA 역공학 장치.

청구항 8

제 5 항에 있어서,

상기 획득부는,

상기 중복 정보가 복구된 리소스 파일 및 상기 비트스트림을 기초로 프로그램 가능 상호 접속점(programmable interconnect point) 정보와 프로그램 가능 로직 지점(programmable logic point) 정보를 복구하고,

상기 복구된 프로그램 가능 상호 접속점 정보와 프로그램 가능 로직 지점 정보를 기초로 상기 넷리스트를 획득하는

FPGA 역공학 장치.

청구항 9

제 1 항 내지 제 4 항 중 어느 한 항에 기재된 방법에 따른 각각의 단계를 수행하는 명령어를 포함하는 프로그램이 기록된 컴퓨터 판독 가능 기록매체.

발명의 설명

기술 분야

[0001] 본 발명은 비트스트림에 기초하여 FPGA에 대한 역공학을 수행하는 장치 및 방법에 관한 것이다.

배경 기술

[0002] FPGA (field programmable gate array)란 재프로그래밍 가능한 논리 소자의 집합을 의미할 수 있다. FPGA는 개발자의 의도대로 유연하게 프로그래밍 할 수 있다는 장점때문에, 자동차 산업, 항공, 국방 등 다양한 분야에서 널리 이용되고 있다.

[0003] FPGA 칩에는 비트 스트림을 통해 프로그래밍 되는 FPGA 기반의 시스템이 탑재될 수 있다. 만약, FPGA 기반의 시스템을 직접 구현하지 않고 외부 업체에 위탁하여 구현하는 경우, 구현된 시스템에는 임의의 공격자에 의해 오작동을 일으키거나 정보를 유출시키는 등의 하드웨어 악성 기능이 포함될 가능성이 있다. 또한, 국방, 범죄수사, 첩보전 등의 분야에서는 상대 측의 하드웨어 장비를 취득할 경우, 취득한 하드웨어 장비 내 FPGA 칩을 분석하여 그 목적과 기능, 저장된 데이터를 찾아낼 필요가 있다.

[0004] 따라서, 상대 측으로부터의 공격을 사전에 방지하거나, 취득한 상대 측의 하드웨어 장비를 분석하기 위해, FPGA 칩에 전달되는 비트 스트림을 통해 FPGA 내부 로직을 확인할 수 있는 단계까지 역공학을 수행할 수 있다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 미국 공개특허공보 US2002/0199110 (2002년12월26일 공개)

발명의 내용

해결하려는 과제

[0006] 본 발명의 일 실시예에 따른 FPGA 역공학 방법은, 타겟 FPGA(field programmable gate array)로부터 비트스트림(bitstream)을 추출하는 단계; 상기 추출된 비트스트림에 기초하여 상기 타겟 FPGA를 식별하는 단계; 상기 식별 결과에 대응되는 리소스 정보 파일을 탐색하는 단계; 상기 탐색된 리소스 정보 파일 내 생략된 중복 정보를 복구하는 단계; 및 상기 중복 정보가 복구된 리소스 파일 및 상기 비트스트림을 기초로 상기 타겟 FPGA에 대한 넷리스트(Netlist)를 획득하는 단계를 포함한다.

[0007] 또한, 상기 중복 정보는, 복수의 프리미티브(primitive)에 대해 지원 가능한 사이트(site) 정보를 포함할 수 있다.

[0008] 또한, 상기 중복 정보를 복구하는 단계는, FPGA 캐드 툴(CAD tool)에 상기 탐색된 리소스 정보 파일을 입력하여 상기 생략된 중복 정보를 복구할 수 있다.

[0009] 또한, 상기 넷리스트를 획득하는 단계는, 상기 중복 정보가 복구된 리소스 파일 및 상기 비트스트림을 기초로 프로그램 가능 상호 접속점(programmable interconnect point) 정보와 프로그램 가능 로직 지점(programmable logic point) 정보를 복구하는 단계; 및 상기 복구된 프로그램 가능 상호 접속점 정보와 프로그램 가능 로직 지점 정보를 기초로 상기 넷리스트를 획득하는 단계를 포함할 수 있다.

[0010] 본 발명의 일 실시예에 따른 FPGA 역공학 장치는, 타겟 FPGA(field programmable gate array)로부터 비트스트림(bitstream)을 추출하는 추출부; 상기 추출된 비트스트림에 기초하여 상기 타겟 FPGA를 식별하는 식별부; 상기 식별 결과에 대응되는 리소스 정보 파일을 탐색하는 탐색부; 상기 탐색된 리소스 정보 파일 내 생략된 중복 정보를 복구하는 복구부; 및 상기 중복 정보가 복구된 리소스 파일 및 상기 비트스트림을 기초로 상기 타겟 FPGA에 대한 넷리스트(Netlist)를 획득하는 획득부를 포함한다.

[0011] 또한, 상기 중복 정보는, 복수의 프리미티브(primitive)에 대해 지원 가능한 사이트(site) 정보를 포함할 수 있다.

[0012] 또한, 상기 복구부는, FPGA 캐드 툴(CAD tool)에 상기 탐색된 리소스 정보 파일을 입력하여 상기 생략된 중복 정보를 복구할 수 있다.

[0013] 또한, 상기 획득부는, 상기 중복 정보가 복구된 리소스 파일 및 상기 비트스트림을 기초로 프로그램 가능 상호 접속점(programmable interconnect point) 정보와 프로그램 가능 로직 지점(programmable logic point) 정보를 복구하고, 상기 복구된 프로그램 가능 상호 접속점 정보와 프로그램 가능 로직 지점 정보를 기초로 상기 넷리스트를 획득할 수 있다.

발명의 효과

[0014] 본 발명의 실시예에 의하면, 생략된 정보가 복구된 리소스 파일을 이용하므로, 타겟 FPGA에 대한 넷리스트 복원률과 복원의 정확성을 높일 수 있다. 이를 통해, 외부에서 구현된 FPGA 시스템을 이용하는 경우, 임의의 공격자에 의한 오작동 또는 정보 유출 등을 사전에 방지할 수 있다.

[0015] 또한, FPGA를 이용한 하드웨어 또는 임베디드 시스템을 기초로 이루어지는 각종 범죄에 대하여 본 발명의 FPGA 역공학 방법을 적용함으로써, 범죄 수사를 위한 증거 확보에도 큰 도움을 줄 수 있다.

[0016] 뿐만 아니라, 본 발명의 실시예와 같은 비침습적인 역공학은 그 외 수사, 증거수집, 군사 방어 등 타겟 FPGA를 손상시키지 않아야 하는 다양한 분야에 널리 사용될 수 있다. 특히, 상대 측의 하드웨어 장비를 취득한 경우, 본 발명의 실시예에 따라 취득한 하드웨어 장비 내 FPGA를 분석함으로써, 그 목적과 기능, 및 저장된 데이터를

용이하고 정확하게 복원할 수 있다.

도면의 간단한 설명

도 1은 본 발명의 일 실시예에 따른 FPGA 역공학 장치의 제어 블록도이다.

도 2는 본 발명의 일 실시예에 따른 FPGA 역공학 장치가 비트스트림을 추출하는 과정을 설명하기 위한 도면이다.

도 3은 본 발명의 일 실시예에 따른 FPGA 역공학 방법의 흐름도이다.

도 4는 본 발명의 일 실시예에 따른 FPGA 역공학 방법의 적용 예를 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명의 범주는 청구항에 의해 정의될 뿐이다.

본 발명의 실시예들을 설명함에 있어서 공지 기능 또는 구성에 대한 구체적인 설명은 본 발명의 실시예들을 설명함에 있어 실제로 필요한 경우 외에는 생략될 것이다. 그리고 후술되는 용어들은 본 발명의 실시예에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

이하 사용되는 '...부', '...기' 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어, 또는, 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

도 1은 본 발명의 일 실시예에 따른 FPGA 역공학 장치의 제어 블록도이다.

본 발명의 FPGA 역공학 장치는 FPGA에 대한 넷리스트(netlist)를 복원하는 장치를 의미한다. 여기서, 넷리스트란 HDL(hardware description language)과 같은 하드웨어 기술 언어에 기초한 회로 합성 결과 또는 CAD 툴에 의해 작성된 회로 자체에 대한 정보를 포함하는 파일로서, 이를 기초로 레이아웃(layout) 과정을 수행하면 해당 FPGA 칩의 내부를 이해할 수 있다.

반도체 칩의 경우 내부 회로가 물리적으로 결정되어 있어, 반도체 칩의 상단을 황산이나 사포 등을 이용하여 제거한 후 반도체 칩을 노출시킨다면 직접 물리적으로 역공학이 가능할 수 있다. 하지만 이러한 침습적(invasive)인 방법을 사용하여 역공학을 시도하면, 해당 반도체 칩은 더 이상 사용할 수 없으며 다시 역공학을 시도하는 것도 불가능할 수 있다. 따라서, 획득한 하드웨어의 수가 적은 경우에는 침습적인 역공학 방법을 시도하기 어렵다.

그 결과, 최근에는 비침습적인 방법을 사용한 역공학을 수행하는 것에 대한 연구가 활발히 진행되고 있다. 예를 들어, FPGA는 초기에 전원이 인가된 후 프로그래밍 데이터를 통해서 내부 논리회로가 정해지기 때문에, 프로그래밍을 위해 내부로 전달되는 비트스트림을 추출하면 비침습적으로 FPGA의 논리회로를 추측하는 것이 가능할 수 있다. 이하에서는 도 2를 참조하여 비트스트림을 이용하여 FPGA를 역공학 하는 방법에 대해 설명한다.

도 2는 본 발명의 일 실시예에 따른 FPGA 역공학 장치가 비트스트림을 추출하는 과정을 설명하기 위한 도면이다.

도 2를 참조하면, FPGA 칩(F_C)내부의 메모리는 SRAM과 같은 휘발성 메모리 (M_S)이기 때문에 프로그래밍을 위해 컴퓨터에서 제공된 논리 정보를 저장하지 못할 수 있다. 즉, FPGA 칩(F_C)은 전원이 제거되면 메모리에 저장된 모든 논리회로가 사라질 수 있다. 컴퓨터를 통해 매번 논리회로와 관련된 논리 정보를 제공받을 수 없기 때문에, FPGA 칩(F_C)을 포함하는 FPGA(F)는 PROM과 같은 비휘발성 메모리(M_P)를 추가적으로 구비하고, 구비된 비휘발성 메모리(M_P)에 프로그래밍을 위한 논리 정보를 저장할 수 있다. 비휘발성 메모리(M_P)는 FPGA(F)에 전원이 제공되면 프로그래밍 논리 정보를 FPGA 칩(F_C) 내부의 휘발성 메모리(M_S)에 전달하고, 휘발성 메모리(M_S)는 FPGA 칩(F_C)에 논리 정보를 제공함으로써, FPGA 칩(F_C) 내부에 논리회로가 구성될 수 있다.

- [0027] 이 때, FPGA 보드에 전원 제공 시, 비휘발성 메모리에서 휘발성 메모리로 제공되는 비트스트림을 추출함으로써 비트스트림 기반의 역공학이 가능할 수 있다. 특히, FPGA 리소스 정보 파일과 비트스트림의 상관관계를 기초로 FPGA에 대한 역공학을 수행할 수 있다.
- [0028] 그러나, 상술한 역공학 방법에서 이용하는 FPGA 리소스 정보 파일은 용량을 최소화하기 위해 중복 정보를 생략하여 생성될 수 있다. 그 결과, 기존의 FPGA 리소스 정보 파일을 그대로 이용할 경우, FPGA에 대한 정보 중 일부에 대해서만 역공학이 가능할 수 있다.
- [0029] 이를 해결하기 위해, 본 발명의 일 실시예에 따른 FPGA 역공학 장치(100)는 타겟 FPGA의 리소스 정보 파일 내 생략된 정보를 복구하고, 생략된 정보가 복구된 리소스 파일과 추출된 비트스트림을 이용하여 타겟 FPGA의 넷리스트를 획득하는 FPGA 역공학 장치(100) 및 방법을 제공할 수 있다.
- [0030] 다시 도 1을 참조하면, 본 발명의 일 실시예에 따른 FPGA 역공학 장치(100)는 추출부(110), 식별부(120), 탐색부(130), 복구부(140) 및 획득부(150)를 포함할 수 있다.
- [0031] 추출부(110)는 타겟 FPGA로부터 비트스트림을 추출할 수 있다. 여기서, 타겟 FPGA는 넷리스트(Netlist)를 획득하고자 하는 대상 FPGA를 의미할 수 있다. 또한, 추출부(110)는 타겟 FPGA로부터 추출된 비트스트림으로부터 비트 파일을 획득할 수 있다.
- [0032] 식별부(120)는 추출된 비트 파일에 기초하여 타겟 FPGA를 식별할 수 있다. 구체적으로, 식별부(120)는 추출된 비트 파일을 분석하고, 분석 결과에 기초하여 비트 파일에 대응되는 타겟 FPGA를 식별할 수 있다.
- [0033] 탐색부(130)는 식별 결과에 대응되는 리소스 정보 파일을 탐색할 수 있다. 예를 들어, 일 실시예에 따른 탐색부(130)는 복수의 FPGA에 대응되는 리소스 정보 파일 리스트를 저장하고, 식별부(120)에 의해 타겟 FPGA가 식별되면, 식별된 타겟 FPGA에 대응되는 리소스 정보 파일을 리소스 정보 파일 리스트로부터 탐색할 수 있다. 이와는 달리, 다른 실시예에 따른 탐색부(130)는 식별부(120)에 의해 타겟 FPGA가 식별되면, 식별 결과를 기초로 FPGA 리소스 정보 파일 탐색 틀을 이용하여 식별된 FPGA에 대한 리소스 정보 파일을 탐색할 수도 있다.
- [0034] 복구부(140)는 탐색된 리소스 정보 파일 내 생략된 중복 정보를 복구할 수 있다. 여기서, 중복 정보는 복수의 프리머티브(primitive)에 대해 지원 가능한 사이트(site) 정보를 포함할 수 있다. 복구부(140)는 FPGA 캐드 툴(CAD tool)에 상기 탐색된 리소스 정보 파일을 입력하여 상기 생략된 중복 정보를 복구할 수 있다.
- [0035] 획득부(150)는 중복 정보가 복구된 리소스 파일 및 비트 파일을 기초로 타겟 FPGA 칩에 대한 넷리스트를 획득할 수 있다. 이를 위해, 획득부(150)는 중복 정보가 복구된 리소스 파일 및 비트 파일을 기초로 프로그램 가능 상호 접속점(programmable interconnect point) 정보와 프로그램 가능 로직 지점(programmable logic point) 정보를 복구하고, 복구된 프로그램 가능 상호 접속점 정보와 프로그램 가능 로직 지점 정보를 기초로 넷리스트를 획득할 수 있다.
- [0036] 도 1을 참조하면, 본 발명의 일 실시예에 따른 FPGA 역공학 장치(100)의 각 구성은 마이크로프로세서(Microprocessor)를 포함하는 연산 장치로 구현될 수 있고, 예를 들어 중앙 처리 장치(Central Processing Unit, CPU), 그래픽 처리 장치(Graphic Processing Unit, GPU) 등으로 구현될 수 있다. 이와는 달리, FPGA 역공학 장치(100)의 복수의 구성이 하나의 SOC(System On Chip)으로 구현되는 것도 가능할 수 있다.
- [0037] 지금까지는 FPGA 역공학 장치(100)의 구성에 대하여 설명하였다. 이하에서는 상술한 FPGA 역공학 장치(100)에 의해 수행되는 FPGA 역공학 방법에 대해 설명한다.
- [0038] 도 3은 본 발명의 일 실시예에 따른 FPGA 역공학 방법의 흐름도이다.
- [0039] 먼저, FPGA 역공학 장치(100)는 타겟 FPGA로부터 비트스트림(bitstream)을 추출할 수 있다(S100). 구체적으로, FPGA 역공학 장치(100)의 추출부(110)는 FPGA 칩 외부의 비휘발성 메모리로부터 FPGA 칩 내부의 휘발성 메모리로 전송되는 비트스트림을 추출할 수 있다. 나아가, FPGA 역공학 장치(100)의 추출부(110)는 추출된 비트스트림으로부터 비트 파일을 획득할 수 있다.
- [0040] 그 다음, FPGA 역공학 장치(100)는 추출된 비트스트림에 기초하여 타겟 FPGA를 식별할 수 있다(S110). 구체적으로, FPGA 역공학 장치(100)의 식별부(120)는 추출부(110)에 의해 비트스트림으로부터 획득된 비트 파일을 분석하여, 타겟 FPGA를 식별할 수 있다.
- [0041] 이를 위해, FPGA 역공학 장치(100)의 식별부(120)는 비트 파일을 분석하여 FPGA에 대한 구성 데이터를 획득할

수 있다. 여기서, 구성 데이터란 FPGA의 제품 정보 및 논리 정보가 텍스트로 기록된 파일을 의미할 수 있다.

- [0042] 구성 데이터를 획득한 후, 식별부(120)는 획득된 구성 데이터에 대응되는 FPGA를 구성 데이터베이스를 이용하여 확인할 수 있다. 여기서, 구성 데이터베이스란 비트스트림을 통해 획득된 구성 데이터와 다양한 FPGA 제품들 간의 상호상관 관계를 정리한 구성 데이터베이스를 의미할 수 있다. 식별부(120)는 이렇게 확인된 FPGA를 타겟 FPGA로서 식별할 수 있다.
- [0043] 그 다음, FPGA 역공학 장치(100)는 식별 결과에 대응되는 리소스 정보 파일을 탐색할 수 있다(S120). 여기서, 리소스 정보 파일이란 FPGA 내부의 모든 리소스에 대한 정보를 텍스트로 기록한 파일을 의미하며, FPGA 제조사에서 배포할 수 있다.
- [0044] 일 실시예에 따른 FPGA 역공학 장치(100)의 탐색부(130)는 복수의 FPGA 각각에 대한 리소스 정보 파일 중 식별된 타겟 FPGA에 대응되는 리소스 정보 파일을 탐색할 수 있다. 이와는 달리, 다른 실시예에 따른 FPGA 역공학 장치(100)의 탐색부(130)는 복수의 FPGA 각각에 대한 리소스 정보 파일의 탐색이 가능한 FPGA 리소스 정보 파일 탐색 틀에 식별된 타겟 FPGA를 입력하여, 타겟 FPGA에 대응되는 리소스 정보 파일을 탐색할 수도 있다.
- [0045] 리소스 정보 파일이 탐색되면, FPGA 역공학 장치(100)는 탐색된 리소스 정보 파일 내 생략된 중복 정보를 복구할 수 있다(S130). 상술한 바와 같이, 리소스 정보 파일은 제조사에서 배포하는데, 파일의 용량을 낮추기 위해 중복 정보를 생략하도록 제작될 수 있다. 예를 들어, FPGA 내부의 타일(tile) 1과 타일 2가 동일한 구조를 가질 경우, 해당 FPGA에 대한 리소스 정보 파일에서는 타일 2를 타일 1의 기술 내용을 인용하는 형식으로 기술할 수 있다. 이와 같이, 불완전한 리소스 정보 파일을 이용하여 역공학을 수행할 경우, 최종 획득되는 넷리스트의 복원률과 복원의 정확도가 낮아질 수 있다.
- [0046] 따라서, FPGA 역공학 장치(100)의 복구부(140)는 리소스 정보 파일의 생략된 중복 정보를 복구하여 완전한 리소스 정보를 제공할 수 있다. 이 때, 복구부(140)에 의해 복구되는 중복 정보는 복수의 프리머티브에 대해 지원 가능한 사이트 정보를 포함할 수 있다.
- [0047] 중복 정보의 복구를 위해, 복구부(140)는 FPGA 캐드 틀에 상기 탐색된 리소스 정보 파일을 입력하여 상기 생략된 중복 정보를 복구할 수 있다. 특히, 복구부(140)는 소스코드가 무상으로 공개된 오픈소스 캐드 틀을 이용하여 리소스 정보 파일의 생략된 중복 정보를 복구할 수 있다.
- [0048] 마지막으로, FPGA 역공학 장치(100)는 중복 정보가 복구된 리소스 파일 및 비트스트림을 기초로 타겟 FPGA에 대한 넷리스트를 획득할 수 있다(S140). 구체적으로, FPGA 역공학 장치(100)의 획득부(150)는 중복 정보가 복구된 리소스 파일 및 비트스트림을 기초로 프로그램 가능 상호 접속점 정보와 프로그램 가능 로직 지점 정보를 복구하고, 복구된 프로그램 가능 상호 접속점 정보와 프로그램 가능 로직 지점 정보를 기초로 넷리스트를 획득할 수 있다.
- [0049] 이를 위해, 획득부(150)는 비트스트림에 상호상관 알고리즘을 적용하여 중복 정보가 복구된 리소스 파일로부터 프로그램 가능 상호 접속점 정보와 프로그램 가능 로직 지점 정보를 복구할 수 있다. 획득부(150)는 비교를 통해 복구된 프로그램 가능 상호 접속점 정보와 프로그램 가능 로직 지점 정보를 타일 타입, 타일 위치 등으로 복구된 구성 데이터로 출력할 수 있다. 마지막으로, 획득부(150)는 복구된 구성 데이터를 기초로 FPGA에 대한 넷리스트를 획득할 수 있다.
- [0050] 지금까지는 본 발명의 일 실시예에 따른 FPGA 역공학 방법에 대하여 설명하였다. 이하에서는 상술한 FPGA 역공학 방법을 시중에 유통되는 Xilinx사(社)의 FPGA에 적용하는 실시예를 설명한다.
- [0051] 도 4는 본 발명의 일 실시예에 따른 FPGA 역공학 방법의 적용 예를 설명하기 위한 도면이다. 도 4에서 S₁은 종래의 역공학 방법에 따른 블록이고, S₂는 본 발명의 일 실시예에 따른 FPGA 역공학 방법에 따라 새롭게 추가된 블록을 의미한다.
- [0052] Xilinx사에서는 FPGA에 대한 구성 데이터로서 XDL 파일을 제공하고, FPGA에 대한 리소스 파일로서 XDLRC 파일을 제공한다. Xilinx사의 FPGA에 대한 종래의 역공학 방법은 XDL 파일을 복원하기 위해 Debit의 상관관계법에 기초한 BIL이라는 기존 역공학 도구를 사용하였다. BIL 역공학 도구를 통해 생성된 XDL 파일은 부분적인 정보만 가지고 있기 때문에 넷리스트 획득 시 극히 일부의 정보만이 복원되었다.
- [0053] 이를 개선하기 위해, 본 발명의 일 실시예에 따른 FPGA 역공학 방법은 비트 파일로부터 타겟 FPGA를 자동으로 식별하고, 타겟 FPGA에 대한 XDLRC 파일을 자동으로 탐색한 후, RapidSmith라는 오픈소스 캐드 틀을 이용하여

중복 정보가 생략된 불완전한 XDLRC 파일을 보완하여, 생략된 중복 정보가 모두 복구된 완전한 XDLRC 파일을 역공학 과정에서 이용할 수 있다. 이처럼, 본 발명의 일 실시예에 따른 FPGA 역공학 방법은 종래의 BIL 역공학 도구에 비트스트림 파일 뿐 아니라 완전한 XDLRC 파일을 입력으로 줄 수 있기 때문에 XDL 파일 복원률을 높일 수 있으며, 그 결과 역공학의 정확도를 개선할 수 있다.

[0054] 상술한 FPGA 역공학 장치 및 방법은, 생략된 정보가 복구된 리소스 파일을 이용하므로, 타겟 FPGA에 대한 넷리스트 복원률과 복원의 정확성을 높일 수 있다. 이를 통해, 외부에서 구현된 FPGA 시스템을 이용하는 경우, 임의의 공격자에 의한 오작동 또는 정보 유출 등을 사전에 방지할 수 있다.

[0055] 또한, FPGA를 이용한 하드웨어 또는 임베디드 시스템을 기초로 이루어지는 각종 범죄에 대하여 본 발명의 FPGA 역공학 방법을 적용함으로써, 범죄 수사를 위한 증거 확보에도 큰 도움을 줄 수 있다.

[0056] 뿐만 아니라, 본 발명의 실시예와 같은 비침습적인 역공학은 그 외 수사, 증거수집, 군사 방어 등 타겟 FPGA를 손상시키지 않아야 하는 다양한 분야에 널리 사용될 수 있다. 특히, 상대 측의 하드웨어 장비를 취득한 경우, 본 발명의 실시예에 따라 취득한 하드웨어 장비 내 FPGA를 분석함으로써, 그 목적과 기능, 및 저장된 데이터를 용이하고 정확하게 복원할 수 있다.

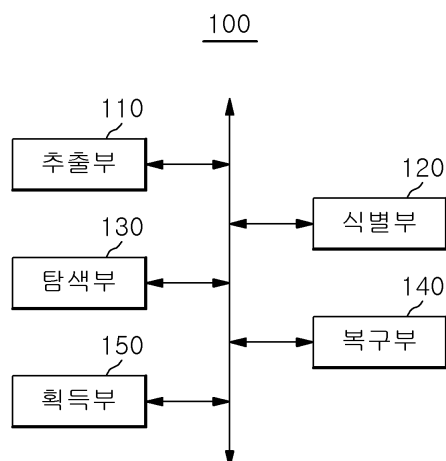
[0057] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 품질에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 명세서에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 균등한 범위 내에 있는 모든 기술사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

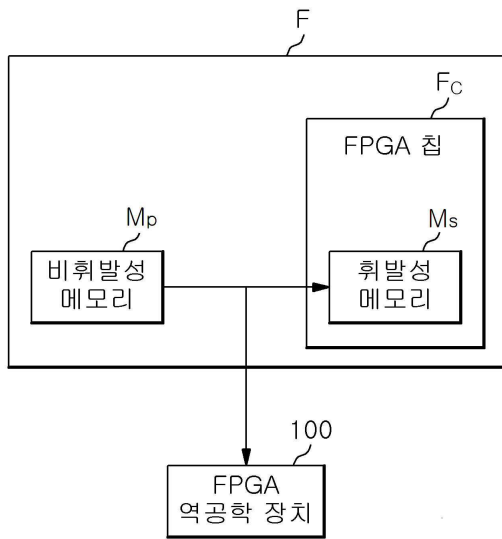
[0058] 100: FPGA 역공학 장치
110: 추출부
120: 식별부
130: 탐색부
140: 복구부
150: 획득부

도면

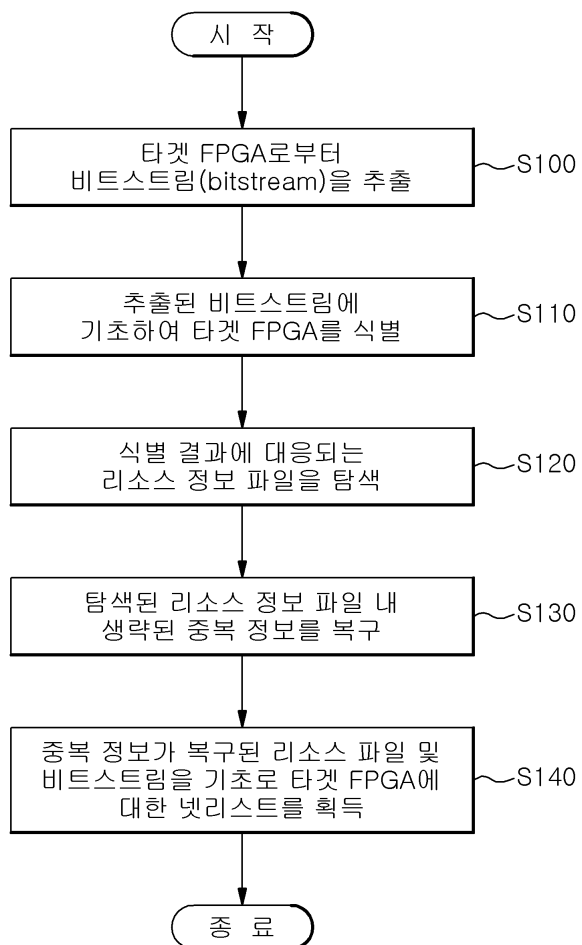
도면1



도면2



도면3



도면4

