



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0090841
(43) 공개일자 2023년06월22일

(51) 국제특허분류(Int. Cl.)
G06F 9/38 (2006.01) G06F 11/14 (2006.01)
G06F 12/0802 (2016.01)
(52) CPC특허분류
G06F 9/3861 (2013.01)
G06F 11/1471 (2013.01)
(21) 출원번호 10-2021-0179950
(22) 출원일자 2021년12월15일
심사청구일자 2021년12월15일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암
동5가)
(72) 발명자
서태원
경기도 남양주시 순화궁로 18, 4110동 902호(별내
동, 신안인스빌아파트)
구건재
경기도 남양주시 불암로 337, 5103동 2004호(별내
동, 남양주별내 유승 한내들)
(74) 대리인
이대호, 박건홍

전체 청구항 수 : 총 12 항

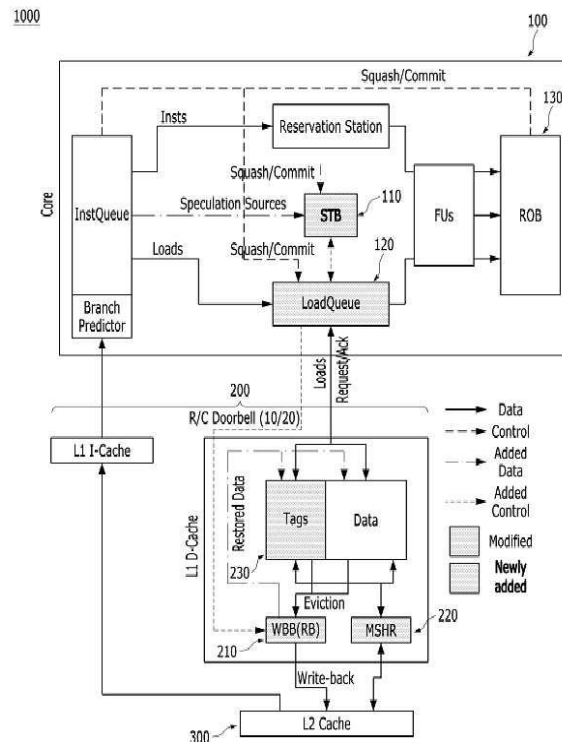
(54) 발명의 명칭 라이트-백 버퍼를 이용하여 캐시 메모리 상태를 복구하는 프로세서 및 그 동작

(57) 요약

비순차 실행(Out-of-order execution)을 위한 예측 실행(Speculative Execution)을 수행하는 프로세서가 개시된다. 상기 프로세서는 코어 및 L1 캐시 메모리를 포함하고, 상기 코어는: 예측 명령이 리오더 버퍼(reorder buffer, ROB)에 기록되는 경우, 상기 예측 명령을 추적하기 위해 예측 추적 정보를 저장하는 예측 추적 버퍼

(뒷면에 계속)

대표도 - 도1



(speculative track buffer, STB); 및 상기 예측 명령에 포함되는 제 1 예측 명령의 예측 성공 또는 예측 실패가 결정되는 경우, 상기 제 1 예측 명령의 제 1 예측 추적 정보에 기초하여 상기 제 1 예측 명령이 속하는 제 1 예측 블록에 대한 확정 초인종 신호(Commit Doorbell) 또는 복구 초인종 신호(restore doorbell)를 상기 L1 캐시 메모리로 송신하는 로드큐(LoadQueue, LQ);를 포함하고, 상기 L1 캐시 메모리는: 라이트 버퍼(write buffer);를 포함하고, 상기 라이트 버퍼는: 상기 예측 명령에 의해 발생한 요청이 상기 L1 캐시 메모리로 반환됨에 따라 상기 L1 캐시 메모리의 태그 및 데이터 영역으로부터 추출되는 추출 캐시블록을 저장하고, 그리고 상기 제 1 예측 블록에 대한 확정 초인종 신호 또는 복구 초인종 신호를 수신하는 경우에, 상기 제 1 예측 블록에 대응하는 추출 캐시블록에 대한 확정 동작 또는 복구 동작을 수행할 수 있다.

(52) CPC특허분류

G06F 12/0802 (2013.01)

(72) 발명자

이종민

서울특별시 강북구 덕릉로 26-9, 201호(수유동)

이준연

경기도 수원시 영통구 봉영로 1410-17, 105동 180
2호(망포동, e편한세상 영통2차 1단지)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711126288
 과제번호 2019-0-00533-003
 부처명 과학기술정보통신부
 과제관리(전문)기관명 정보통신기획평가원
 연구사업명 정보보호핵심원천기술개발(R&D, 정보화)
 연구과제명 컴퓨터 프로세서의 구조적 보안 취약점 검증 및 공격 탐지 대응
 기 여 율 50/100
 과제수행기관명 고려대학교 산학협력단
 연구기간 2019.04.01 ~ 2022.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호 1711131696
 과제번호 2021R1C1C1012172
 부처명 과학기술정보통신부
 과제관리(전문)기관명 한국연구재단
 연구사업명 개인기초연구(과기정통부)(R&D)
 연구과제명 대규모 그래프 구조의 신경망 처리를 위한 효율적인 프로세서 및 메모리 구조에 대

한 연구

기 여 율 20/100
 과제수행기관명 고려대학교 산학협력단
 연구기간 2021.03.01 ~ 2026.02.28

이 발명을 지원한 국가연구개발사업

과제고유번호 1711125781
 과제번호 2019-0-01343-003
 부처명 과학기술정보통신부
 과제관리(전문)기관명 정보통신기획평가원
 연구사업명 융합보안핵심인재양성사업
 연구과제명 융합보안핵심인재양성사업
 기 여 율 20/100
 과제수행기관명 한국인터넷진흥원
 연구기간 2019.05.01 ~ 2024.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호 1711126325
 과제번호 2020-0-01819-002
 부처명 과학기술정보통신부
 과제관리(전문)기관명 정보통신기획평가원
 연구사업명 정보통신방송혁신인재양성(R&D)
 연구과제명 ICT명품인재양성(고려대학교)
 기 여 율 10/100
 과제수행기관명 고려대학교 산학협력단
 연구기간 2020.07.01 ~ 2023.12.31

명세서

청구범위

청구항 1

비순차 실행(Out-of-order execution)을 위한 예측 실행(Speculative Execution)을 수행하는 프로세서에 있어서, 상기 프로세서는 코어 및 L1 캐시 메모리를 포함하고,

상기 코어는:

예측 명령이 리오더 버퍼(reorder buffer, ROB)에 기록되는 경우, 상기 예측 명령을 추적하기 위해 예측 추적 정보를 저장하는 예측 추적 버퍼(speculative track buffer, STB); 및

상기 예측 명령에 포함되는 제 1 예측 명령의 예측 성공 또는 예측 실패가 결정되는 경우, 상기 제 1 예측 명령의 제 1 예측 추적 정보에 기초하여 상기 제 1 예측 명령이 속하는 제 1 예측 블록에 대한 확정 초인종 신호(Commit Doorbell) 또는 복구 초인종 신호(restore doorbell)를 상기 L1 캐시 메모리로 송신하는 로드큐(LoadQueue, LQ);

를 포함하고,

상기 L1 캐시 메모리는:

라이트 버퍼(write buffer);

를 포함하고,

상기 라이트 버퍼는:

상기 예측 명령에 의해 발생한 요청이 상기 L1 캐시 메모리로 반환됨에 따라 상기 L1 캐시 메모리의 태그 및 데이터 영역으로부터 추출되는 추출 캐시블록을 저장하고, 그리고

상기 제 1 예측 블록에 대한 확정 초인종 신호 또는 복구 초인종 신호를 수신하는 경우에, 상기 제 1 예측 블록에 대응하는 추출 캐시블록에 대한 확정 동작 또는 복구 동작을 수행하는,

프로세서.

청구항 2

제 1 항에 있어서,

상기 라이트 버퍼는:

상기 추출 캐시블록을 저장하는 경우에, 상기 추출 캐시블록의 예측 명령 추출 정보(SPE), 상태 데이터 정보, 교체 주소 정보를 설정하는,

프로세서.

청구항 3

제 2 항에 있어서,

상기 제 1 예측 명령의 예측 실패가 결정되는 경우, 상기 로드큐는:

상기 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값을 포함하는 복구 초인종 신호를 상기 L1 캐시 메모리로 송신하는,

프로세서.

청구항 4

제 3 항에 있어서,

상기 라이트 버퍼는:

상기 제 1 예측 명령의 상기 복구 초인종 신호를 수신하는 경우에, 추출 캐시블록 중에서 상기 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값에 대응하는 복구 캐시블록을 결정하고, 그리고

상기 복구 캐시블록을 상기 복구 캐시블록의 상기 교체 주소 정보에 기초하여 상기 태그 및 데이터 영역에 복구하는,

프로세서.

청구항 5

제 4 항에 있어서,

상기 L1 캐시 메모리는;

상기 예측 명령에 의해 발생한 요청에 따라 상기 L1 캐시 메모리로 반환된 갱신 캐시블록을 상기 L1 캐시 메모리의 태그 및 데이터 영역에서 추출되는 캐시블록의 위치에 저장하고, 상기 갱신 캐시블록에 대하여 예측 명령 갱신 정보(SPI)를 설정하고, 그리고

상기 제 1 예측 블록에 대한 복구 초인종 신호를 수신하는 경우에, 상기 복구 캐시블록을 상기 태그 및 데이터 영역에 복구하기 위해 상기 복구 캐시블록의 교체 주소 정보에 대응하는 갱신 캐시블록을 상기 복구 캐시블록으로 교체하고, 그리고 상기 복구 캐시블록의 예측 명령 갱신 정보(SPI)를 해제하는,

프로세서.

청구항 6

제 5 항에 있어서,

상기 L1 캐시 메모리는:

상기 제 1 예측 명령의 복구 초인종 신호를 수신하는 시점에 상기 제 1 예측 명령에 의해 발생한 요청이 L1 캐시 메모리로 반환되지 않은 경우, 상기 제 1 예측 명령에 대한 스쿼시 정보(SQ)를 설정하는 MSHR(Miss Status Holding Register);

을 포함하는,

프로세서.

청구항 7

제 6 항에 있어서,

상기 MSHR은:

상기 제 1 예측 명령에 대한 추출 정보(SQ)가 설정되어 있는 경우, 상기 제 1 예측 명령에 의해 반환된 요청을 무시하는,

프로세서.

청구항 8

제 2 항에 있어서,

상기 제 1 예측 명령의 예측 성공이 결정되는 경우, 상기 예측 추적 버퍼는:

상기 리오더 버퍼로부터 상기 제 1 예측 명령에 대한 확정 신호를 수신하는 경우, 상기 제 1 예측 명령의 유효 비트가 설정되어 있는지 결정하고; 그리고

상기 제 1 예측 명령의 유효 비트가 설정되어 있는 경우, 상기 제 1 예측 명령의 식별 정보를 상기 로드큐로 송신하고,

상기 로드큐는:

상기 제 1 예측 명령의 식별정보를 수신하는 경우, 상기 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값을 포함하는 확정 초인종 신호를 상기 L1 캐시 메모리로 송신하는,

프로세서.

청구항 9

제 8 항에 있어서,

상기 로드큐는:

상기 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 예측 명령 로드 정보(SPL)가 설정되어 있는 경우에 상기 확정 초인종 신호를 송신하는,

프로세서.

청구항 10

제 9 항에 있어서,

상기 라이트 버퍼는:

상기 제 1 예측 명령의 상기 확정 초인종 신호를 수신하는 경우에, 추출 캐시블록 중에서 상기 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값에 대응하는 확정 캐시블록을 결정하고,

상기 L1 캐시 메모리는:

상기 확정 캐시블록의 교체 주소 정보에 대응하는 상기 태그 및 데이터 영역의 위치에 있는 갱신 캐시블록의 예측 명령 갱신 정보(SPI)를 해제하는,

프로세서.

청구항 11

제 10 항에 있어서,

상기 라이트 버퍼는:

상기 확정 캐시블록의 상태 데이터가 'clean'으로 설정된 경우에, 상기 확정 캐시블록을 무효화하고, 또는

상기 확정 캐시블록의 상태 데이터가 'dirty'로 설정된 경우에, 상기 확정 캐시블록의 예측 명령 추출 정보(SPE)를 해제하는,

프로세서.

청구항 12

제 1 항에 있어서,

상기 라이트 버퍼는 라이트-백 버퍼(write-back buffer)인,

프로세서.

발명의 설명

기술 분야

[0001] 본 발명은 캐시 메모리의 타이밍 부채널(side-channel)을 이용한 공격을 방어하기 위한 구조를 가지는 프로세서에 관한 것으로, 특히 비순차 실행(Out-of-order execution)을 위한 예측 실행(Speculative Execution)을 이용하여 캐시 메모리의 데이터를 유출하는 일시적 실행 공격(transient execution attack)을 방어하기 위한 구조를 가지는 프로세서 및 그 동작에 관한 것이다.

배경 기술

[0002] 스펙터(Spectre)와 멜트다운(Meltdown)과 같은 일시적 실행 공격(transient execution attack)은 최근에 발견된 프로세서의 구조적 취약점을 이용한 보안 공격 방식이다. 예를 들어, 일시적 실행 공격(transient execution attack)은 현재 많이 사용되고 있는 비순차(out-of-order, OoO) 프로세서의 예측 실행(speculative execution)과 캐시 메모리의 타이밍 부채널을 사용하여 비밀 데이터를 탈취하는 공격 방법이다. 공격자는 예측 실행(speculatively executed)된 데이터 로드(load) 명령어를 활용해 비밀 데이터를 접근하기 위해 예측분기 목적지를 조작한다. 예를 들어, Spectre-NG의 경우, 예측 분기 목적지를 조작하기 위해 예측 스토어(store) 회피 방식을 사용한다. 공격자는 캐시 부채널 공격을 통해 캐시에 남겨진 비밀 정보를 해석할 수 있다. Prime+Probe 방식은 미리 구성된 캐시블록들 중 비밀데이터로 인해 추출된 블록을 탐지하는 방식이다. 반면, Flush+Reload 방식은 비밀 데이터에 접근한 예측 로드 명령어에 의해 캐시에 갱신된 정보를 탐지하는 방식이다. 결과적으로 대부분의 일시적 실행 공격은 예측 로드 명령어에 의해 변경된 캐시 상태를 이용한다.

[0003] 인텔은 아마존 웹서비스(AWS), 마이크로소프트(MS), 구글, 레드햇 등과 협력해 멜트다운을 해결할 수 있는 패치를 개발했다. 이 패치는 문제가 된 비순차적 명령어 처리 기술을 비활성화한 것이다. 다만, 멜트다운 문제 해결을 위해 해당 비순차적 명령어 처리 기술을 비활성화함에 따라 CPU의 성능이 저하되는 문제가 발생했다. 비순차적 명령어 처리는 중앙처리장치 기술의 핵심이다. 영국의 IT전문지 레지스터에 따르면 비순차적 명령어 처리를 비활성화함으로써 인텔 CPU는 최대 30%까지 성능이 저하될 수 있다고 발표하였다.

[0004] 라이트-백 버퍼(Write-Back Buffer, WBB)는 국내 특허 출원번호 제1995-0014663호에서 개시되는 바와 같이 저레벨(low level) 캐시로 갱신되어야 하는 데이터를 임시로 저장하는 데이터 버퍼이다. 라이트-백 버퍼 없이 저레벨로 전달되는 쓰기 명령어를 수행하는 경우, 저레벨 캐시가 쓰기 요청을 처리할 수 없는 상태라면 캐시의 동작이 방해받을 수 있다. 라이트-백 버퍼는 대부분의 프로세서에 사용되며, 라이트-컴바이닝 버퍼(write-combining buffer) 또는 라인-필 버퍼(line-fill buffer) 등과 결합하여 다양한 형태로써 존재한다. 라이트-백 버퍼는 캐시 동작이 방해받지 않으면서 동작하기 위해 필수적인 요소이지만, 우리가 관찰해본 결과 대부분의 경우 활용률이 낮았다.

[0005] 본 개시는 라이트-백 버퍼에서 활용되지 않고 남은 공간들을 예측 실행에 따른 캐시 메모리의 상태를 복구하기 위한 공간으로 활용하여 일시적 실행 공격(transient execution attacks)을 효과적으로 방어하기 위한 구조적 해결 방법을 제시하고자 한다.

발명의 내용

해결하려는 과제

[0006] 본 개시는 전술한 배경기술에 대응하여 안출된 것으로, 프로세서의 구조적인 변경 및 이에 따른 캐시 메모리 상태 복구 동작을 통하여 기존의 소프트웨어 방식보다 빠르고 적은 비용으로 일시적 실행 공격을 효과적으로 방어

할 수 있는 프로세서를 제공하는 것을 목적으로 한다.

과제의 해결 수단

- [0007] 전술한 바와 같은 과제를 실현하기 위한 비순차 실행(Out-of-order execution)을 위한 예측 실행(Speculative Execution)을 수행하는 프로세서가 개시된다. 상기 프로세서는 코어 및 L1 캐시 메모리를 포함하고, 상기 코어는: 예측 명령이 리오더 버퍼(reorder buffer, ROB)에 기록되는 경우, 상기 예측 명령을 추적하기 위해 예측 추적 정보를 저장하는 예측 추적 버퍼(speculative track buffer, STB); 및 상기 예측 명령에 포함되는 제 1 예측 명령의 예측 성공 또는 예측 실패가 결정되는 경우, 상기 제 1 예측 명령의 제 1 예측 추적 정보에 기초하여 상기 제 1 예측 명령이 속하는 제 1 예측 블록에 대한 확정 초인종 신호(Commit Doorbell) 또는 복구 초인종 신호(restore doorbell)를 상기 L1 캐시 메모리로 송신하는 로드큐(LoadQueue, LQ);를 포함하고, 상기 L1 캐시 메모리는: 라이트 버퍼(write buffer); 를 포함하고, 상기 라이트 버퍼는: 상기 예측 명령에 의해 발생한 요청이 상기 L1 캐시 메모리로 반환됨에 따라 상기 L1 캐시 메모리의 태그 및 데이터 영역으로부터 추출되는 추출 캐시블록을 저장하고, 그리고 상기 제 1 예측 블록에 대한 확정 초인종 신호 또는 복구 초인종 신호를 수신하는 경우에, 상기 제 1 예측 블록에 대응하는 추출 캐시블록에 대한 확정 동작 또는 복구 동작을 수행할 수 있다.
- [0008] 대안적으로, 상기 라이트 버퍼는: 상기 추출 캐시블록을 저장하는 경우에, 상기 추출 캐시블록의 예측 명령 추출 정보(SPE), 상태 데이터 정보, 교체 주소 정보를 설정할 수 있다.
- [0009] 대안적으로, 상기 제 1 예측 명령의 예측 실패가 결정되는 경우, 상기 로드큐는: 상기 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값을 포함하는 복구 초인종 신호를 상기 L1 캐시 메모리로 송신할 수 있다.
- [0010] 대안적으로, 상기 라이트 버퍼는: 상기 제 1 예측 명령의 상기 복구 초인종 신호를 수신하는 경우에, 추출 캐시블록 중에서 상기 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값에 대응하는 복구 캐시블록을 결정하고, 그리고 상기 복구 캐시블록을 상기 복구 캐시블록의 상기 교체 주소 정보에 기초하여 상기 태그 및 데이터 영역에 복구할 수 있다.
- [0011] 대안적으로, 상기 L1 캐시 메모리는: 상기 예측 명령에 의해 발생한 요청에 따라 상기 L1 캐시 메모리로 반환된 갠 캐시블록을 상기 L1 캐시 메모리의 태그 및 데이터 영역에서 추출되는 캐시블록의 위치에 저장하고, 상기 갠 캐시블록에 대하여 예측 명령 갠 정보(SPI)를 설정하고, 그리고 상기 제 1 예측 블록에 대한 복구 초인종 신호를 수신하는 경우에, 상기 복구 캐시블록을 상기 태그 및 데이터 영역에 복구하기 위해 상기 복구 캐시블록의 교체 주소 정보에 대응하는 갠 캐시블록을 상기 복구 캐시블록으로 교체하고, 그리고 상기 복구 캐시블록의 예측 명령 갠 정보(SPI)를 해제할 수 있다.
- [0012] 대안적으로, 상기 L1 캐시 메모리는: 상기 제 1 예측 명령의 복구 초인종 신호를 수신하는 시점에 상기 제 1 예측 명령에 의해 발생한 요청이 L1 캐시 메모리로 반환되지 않은 경우, 상기 제 1 예측 명령에 대한 스쿼시 정보(SQ)를 설정하는 MSHR(Miss Status Holding Register); 을 포함할 수 있다.
- [0013] 대안적으로, 상기 MSHR은: 상기 제 1 예측 명령에 대한 추출 정보(SQ)가 설정되어 있는 경우, 상기 제 1 예측 명령에 의해 반환된 요청을 무시할 수 있다.
- [0014] 대안적으로, 상기 제 1 예측 명령의 예측 성공이 결정되는 경우, 상기 예측 추적 버퍼는: 상기 리오더 버퍼로부터 상기 제 1 예측 명령에 대한 확정 신호를 수신하는 경우, 상기 제 1 예측 명령의 유효 비트가 설정되어 있는지 결정하고; 그리고 상기 제 1 예측 명령의 유효 비트가 설정되어 있는 경우, 상기 제 1 예측 명령의 식별 정보를 상기 로드큐로 송신하고, 상기 로드큐는: 상기 제 1 예측 명령의 식별정보를 수신하는 경우, 상기 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값을 포함하는 확정 초인종 신호를 상기 L1 캐시 메모리로 송신할 수 있다.
- [0015] 대안적으로, 상기 로드큐는: 상기 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 예측 명령 로드 정보(SPL)가 설정되어 있는 경우에 상기 확정 초인종 신호를 송신할 수 있다.
- [0016] 대안적으로 상기 라이트 버퍼는: 상기 제 1 예측 명령의 상기 확정 초인종 신호를 수신하는 경우에, 추출 캐시블록 중에서 상기 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값에 대응하는 확정 캐시블록을 결정하고, 상기 L1 캐시 메모리는: 상기 확정 캐시블록의 교체 주소 정보에 대응하는 상기 태그 및 데이터 영역의 위치에 있는 갠 캐시블록의 예측 명령 갠 정보(SPI)를 해제할 수 있다.
- [0017] 대안적으로, 라이트 버퍼는: 상기 확정 캐시블록의 상태 데이터가 'clean'으로 설정된 경우에, 상기 확정 캐시

블록을 무효화하고, 또는 상기 확정 캐시블록의 상태 데이터가 'dirty'로 설정된 경우에, 상기 확정 캐시블록의 예측 명령 추출 정보(SPE)를 해제할 수 있다.

[0018] 대안적으로, 상기 라이트 버퍼는 라이트-백 버퍼(write-back buffer)일 수 있다.

발명의 효과

[0019] 본 개시는 활용률이 낮은 라이트-백 버퍼를 복구 버퍼로 활용하여 예측 명령에 의한 캐시 메모리의 변경된 상태를 구조적 복구함으로써 빠르고 적은 비용으로 일시적 실행 공격을 효과적으로 방어하는 프로세서를 제공할 수 있다.

도면의 간단한 설명

[0020] 도 1은 본 개시의 몇몇 실시예에 따른 프로세서의 개략적인 구조를 나타낸다.

도 2는 본 개시의 몇몇 실시예에 따른 프로세서의 코어의 개략적인 구조를 나타낸다.

도 3은 본 개시의 몇몇 실시예에 따른 프로세서의 L1 캐시 메모리의 개략적인 구조를 나타낸다.

도 4는 본 개시의 몇몇 실시예에 따라, 예측 명령에 의해 발생된 요청이 L1 캐시 메모리로 반환되는 경우에 L1 캐시 메모리의 동작을 설명하기 위한 도면이다.

도 5는 본 개시의 몇몇 실시예에 따라, 복구 초인종 신호에 따라 추출 캐시블록을 복구하는 L1 캐시 메모리의 동작을 설명하기 위한 도면이다.

도 6은 본 개시의 몇몇 실시예에 따라, 확정 초인종 신호에 따라 추출 캐시블록을 확정 처리하는 L1 캐시 메모리의 동작을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0021] 다양한 실시예들이 이제 도면을 참조하여 설명된다. 본 명세서에서, 다양한 설명들이 본 개시의 이해를 제공하기 위해서 제시된다. 그러나, 이러한 실시예들은 이러한 구체적인 설명 없이도 실행될 수 있음이 명백하다.

[0022] 용어 "또는"은 배타적 "또는"이 아니라 내포적 "또는"을 의미하는 것으로 의도된다. 즉, 달리 특정되지 않거나 문맥상 명확하지 않은 경우에, "X는 A 또는 B를 이용한다"는 자연적인 내포적 치환 중 하나를 의미하는 것으로 의도된다. 즉, X가 A를 이용하거나; X가 B를 이용하거나; 또는 X가 A 및 B 모두를 이용하는 경우, "X는 A 또는 B를 이용한다"가 이들 경우들 어느 것으로도 적용될 수 있다. 또한, 본 명세서에 사용된 "및/또는"이라는 용어는 열거된 관련 아이템들 중 하나 이상의 아이템의 가능한 모든 조합을 지칭하고 포함하는 것으로 이해되어야 한다.

[0023] 또한, "포함한다" 및/또는 "포함하는"이라는 용어는, 해당 특징 및/또는 구성요소가 존재함을 의미하는 것으로 이해되어야 한다. 다만, "포함한다" 및/또는 "포함하는"이라는 용어는, 하나 이상의 다른 특징, 구성요소 및/또는 이들의 그룹의 존재 또는 추가를 배제하지 않는 것으로 이해되어야 한다. 또한, 달리 특정되지 않거나 단수 형태를 지시하는 것으로 문맥상 명확하지 않은 경우에, 본 명세서와 청구범위에서 단수는 일반적으로 "하나 또는 그 이상"을 의미하는 것으로 해석되어야 한다.

[0024] 그리고, "A 또는 B 중 적어도 하나"이라는 용어는, "A만을 포함하는 경우", "B만을 포함하는 경우", "A와 B의 구성으로 조합된 경우"를 의미하는 것으로 해석되어야 한다.

[0025] 당업자들은 추가적으로 여기서 개시된 실시예들과 관련되어 설명된 다양한 예시적 논리적 블록들, 구성들, 모듈들, 회로들, 수단들, 로직들, 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 양쪽 모두의 조합들로 구현될 수 있음을 인식해야 한다. 하드웨어 및 소프트웨어의 상호교환성을 명백하게 예시하기 위해, 다양한 예시적 컴포넌트들, 블록들, 구성들, 수단들, 로직들, 모듈들, 회로들, 및 단계들은 그들의 기능성 측면에서 일반적으로 위에서 설명되었다. 그러한 기능성이 하드웨어로 또는 소프트웨어로서 구현되는지 여부는 전반적인 시스템에 부과된 특정 어플리케이션(application) 및 설계 제한들에 달려 있다. 숙련된 기술자들은 각각의 특정 어플리케이션들을 위해 다양한 방법들로 설명된 기능성을 구현할 수 있다. 다만, 그러한 구현의 결정들이 본 개시내용의 영역을 벗어나게 하는 것으로 해석되어서는 안 된다.

[0026] 제시된 실시예들에 대한 설명은 본 개시의 기술 분야에서 통상의 지식을 가진 자가 본 발명을 이용하거나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 개시의 기술 분야에서 통상의 지식을

가진 자에게 명백할 것이다. 여기에 정의된 일반적인 원리들은 본 개시의 범위를 벗어남이 없이 다른 실시예들에 적용될 수 있다. 그리하여, 본 발명은 여기에 제시된 실시예들로 한정되는 것이 아니다. 본 발명은 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위에서 해석되어야 할 것이다.

- [0027] 스펙터(Spectre)와 멜트다운(Meltdown)과 같은 일시적 실행 공격(transient execution attack)은 최근에 발견된 프로세서의 구조적 취약점을 이용한 보안 공격 방식이다. 구체적으로, 일시적 실행 공격(transient execution attack)은 현재 많이 사용되고 있는 비순차(out-of-order, OoO) 프로세서의 예측 실행(speculative execution)과 캐시 메모리의 타이밍 부채널을 사용하여 비밀 데이터를 탈취하는 공격 방법이다.
- [0028] 본 개시는 일시적 실행 공격(transient execution attack)을 막기 위한 효율적이고 경량화된 방어 기법을 제안하는 데 있다. 본 개시에서 제안하고 있는 프로세서 및 메모리 상태 복구 방법은 활용률이 낮은 라이트 버퍼(특히, 라이트-백 버퍼)를 개량하여 예측 실행 도중 축출된 캐시 블록을 임시로 보관할 수 있다. 만약 예측 실행이 실패하는 경우, 라이트-백 버퍼에 임시로 저장되어 있던 데이터는 주캐시(예를 들어, L1 캐시 메모리)로 복구될 수 있다. 라이트-백 버퍼를 복구 버퍼로 사용함으로써 두 가지 이점이 획득될 수 있다. 첫 번째는 라이트-백 버퍼가 L1 캐시와 가까이 위치함으로 복구 시에 발생하는 성능저하를 줄일 수 있다. 두 번째는 복구를 위해 추가적인 메모리 버퍼를 사용하지 않기 때문에 구현하기 위해 추가적인 메모리 영역이 필요하지 않다.
- [0029] 도 1은 본 개시의 몇몇 실시예에 따른 프로세서(1000)의 개략적인 구조를 나타낸다.
- [0030] 본 개시의 몇몇 실시예에 따라, 비순차 실행(Out-of-order execution)을 위한 예측 실행(Speculative Execution)을 수행하는 프로세서(1000)는 도 1에 도시되는 바와 같은 다양한 컴포넌트들을 포함할 수 있다. 예를 들어, 본 개시의 몇몇 실시예에 따라, 프로세서(1000)는 코어(100), L1 캐시 메모리(200, 300), L2 캐시 메모리(400)를 포함할 수 있다. 도 1에 도시된 프로세서(1000) 및 프로세서(1000)에 포함되는 컴포넌트들의 구성은 간략화 하여 나타낸 예시일 뿐이다. 프로세서(1000)는 본 개시의 몇몇 실시예에 따라 일시적 실행 공격(transient execution attack)을 방어하기 위한 다양한 컴포넌트들을 포함할 수 있고, 개시된 컴포넌트들 중 일부만이 프로세서(100) 및 프로세서(100)에 포함되는 컴포넌트들을 구성할 수도 있다.
- [0031] 비순차 실행(Out-of-order execution: OoOE 또는 비순차적 명령어 처리라고도 함)은 중앙처리장치가 특정한 종류의 지연으로 인해 낭비될 수 있는 명령 사이클을 이용하고자 하는 패러다임일 수 있다. 비순차 실행은 명령 실행 효율을 높이기 위해 명령을 순서에 따라 처리하지 않는 기법일 수 있다.
- [0032] 비순차 실행을 위한 코어(100)의 구조는 비순차적으로 실행되는 명령어들이 코어의 구조적 상태(architectural state)를 원래의 프로그램 순서에 따라 올바르게 업데이트할 수 있도록 하기 위하여 다양한 컴포넌트들을 포함할 수 있다. 상술한 바와 같이, 코어(100)는 도 1에 도시되는 컴포넌트들 이외에 다양한 컴포넌트로 구성될 수 있다.
- [0033] 예측 실행(speculative execution)은 비순차 실행에 있어서 예측에 기반하여 더 나은 성능을 가져오는 방향으로 명령어를 처리하는 다양한 기법을 의미할 수 있다. 예를 들어, 예측 실행(speculative execution)은 예측에 기반하여 확정되지 않은 명령을 미리 수행하고, 결과 값이 예측 값과 다르다면 이미 처리한 명령어를 무효화하는 기법일 수 있다.
- [0034] 본 개시의 몇몇 실시예에 따라, 도 1을 참조하면, 코어(100)는 통합 예약 스테이션(Reservation station), 명령어 큐(InstQue), 분기 예측기(Branch Predictor), 평선 유닛(FU), 로드큐(LoadQueue, LQ), 예측 추적 버퍼(speculative track buffer, STB)를 포함할 수 있다. 상술한 바와 같이, 도 1에서 도시되는 코어(100)의 구조는 단지 예시에 불과하며, 코어(100)는 비순차 실행을 위한 예측 실행을 구현하기 위해 다양한 메커니즘을 가질 수 있다.
- [0035] L1 캐시 메모리(200)는 명령어에 대한 L1 I-캐시 및 데이터에 대한 L1 D-캐시를 포함할 수 있다. 본 개시의 명세서 및 청구범위에 걸쳐 사용되는 용어 “L1 캐시 메모리”는 통상적으로 L-1 D-캐시를 지칭하기 위해 사용된다. 다만, 용어 “L1 캐시 메모리”는 L1 I-캐시를 지칭하거나 또는 L1 I-캐시 및 L1 D-캐시를 포함하는 캐시 메모리, 및 그 외의 다양한 구조의 L1 캐시 메모리를 지칭할 수 있다.
- [0036] L1 캐시 메모리(200)는 라이트-백 버퍼(write-back buffer)(210), MSHR(Miss Status Holding Register)(220), 캐시블록들과 캐시블록의 태그들이 저장되는 태그 및 데이터 영역(230)을 포함할 수 있다. 상술한 바와 같이, 도 1에서 도시되는 L1 캐시 메모리(200)의 구조는 단지 예시에 불과하며, L1 캐시 메모리(100)는 비순차 실행을 위한 예측 실행을 구현하기 위해 다양한 메커니즘을 가질 수 있다.

- [0037] 여기서, 라이트 버퍼(210)는 라이트-백 버퍼(write-back buffer)일 수 있다. 다만 이에 한정되지 않고, 라이트 버퍼는 다양한 유형의 버퍼를 포함할 수 있다. 예를 들어, 라이트 버퍼는 라이트-스루 버퍼(Write-Through buffer)일 수 있다. 본 개시의 명세서 및 청구범에 걸쳐 사용되는 용어 “라이트 버퍼”는 통상적으로 라이트-백 버퍼인 라이트 버퍼(210)를 지칭하기 위해 사용된다. 다만 이에 한정되지 않고, “라이트 버퍼”는 다양한 유형의 버퍼 및 그들의 조합을 포함할 수 있다.
- [0038] 도 1을 참고하여 종래의 프로세서의 구조에 비해 변형된 컴포넌트들에 대하여 설명하면, 변형된 컴포넌트는 점 무늬를 가지도록 표시되었다. 또한, 점선과 일점 쇄선은 캐시 메모리 상태 복구를 위한 데이터 경로와 신호 경로를 표시한다. 예를 들어, 라이트 버퍼(210)는 복구 버퍼로 사용되기 때문에, 라이트 버퍼(210)로부터 L1 캐시 메모리(200)의 태그 및 데이터 영역으로 복구되는 데이터의 경로가 추가될 수 있다. 복구/확정 초인종 신호는 라이트 버퍼(210) 상에 저장된 캐시블록을 복구할 것인지 추출할 것인지 확인하는데 사용될 수 있다. 적절한 복구/확정 초인종 신호를 생성하기 위해, 프로세서(1000)는 예측 명령을 추적하기 위한 예측 추적 버퍼(speculative track buffer, STB)를 포함할 수 있다.
- [0039] 본 개시의 몇몇 실시예에 따라, 비순차 실행을 위한 예측 실행을 수행하는 프로세서(1000)는 예측 실행이 실패하는 경우 예측 실행이 된 이후 명령어들은 모두 취소할 수 있다. 이 경우 프로세서(1000)는 취소되는 예측 명령에 의해 갱신된 캐시 메모리의 상태 변경을 복구할 수 있다. 이를 위해, 이하에서 설명되는 바와 같이, 프로세서(1000)는 이하에서 설명되는 컴포넌트들을 포함하고, 그리고 프로세서(1000)의 컴포넌트는 다음과 같은 동작을 수행할 수 있다.
- [0040] 본 개시의 몇몇 실시예에 따라, 상기 코어(100)는 예측 명령이 리오더 버퍼(reorder buffer, ROB)(130)에 할당되는 경우, 예측 명령을 추적하기 위해 예측 추적 정보를 저장하는 예측 추적 버퍼(speculative track buffer, STB)(100)를 포함할 수 있다. 또한, 코어(100)는 예측 명령에 포함되는 제 1 예측 명령의 예측 성공 또는 예측 실패가 결정되는 경우, 제 1 예측 명령의 제 1 예측 추적 정보에 기초하여 제 1 예측 명령이 속하는 제 1 예측 블록에 대한 확정 초인종 신호(Commit Doorbell) 또는 복구 초인종 신호(restore doorbell)를 L1 캐시 메모리(200)로 송신하는 로드큐(LoadQueue, LQ)(120)를 포함할 수 있다.
- [0041] 예측 추적 버퍼(110)는 예측 명령이 리오더 버퍼(130)에 할당되는 경우에, 리오더 버퍼(130)에 할당된 예측 명령을 추적하기 위해 예측 추적 정보를 저장할 수 있다. 리오더 버퍼(210)는 디코딩(decoding)된 명령어를 프로그램 순서에 따라 저장하고 있는 구조체로서 연산을 완료한 명령어를 원래의 순서대로 커밋(commit)할 수 있다. 이를 위해 각 명령어는 비순차 실행이 수행되기 이전 디스패치(dispatch) 단계에서 원래의 순서대로 리오더 버퍼(210)의 엔트리에 할당될 수 있다. 실행되는 모든 명령은 연산을 완료하고 파이프라인에서 커밋되기 전까지 리오더 버퍼(210)의 엔트리를 할당되어 있을 수 있다.
- [0042] 어느 한 예측 명령에 대한 예측 실행에 대하여 예측 성공이 결정되는 경우, 코어(100)는 예측 성공한 예측 명령을 커밋하고 예측 성공한 예측 명령에 대한 확정 동작을 수행할 수 있다. 편의상, 예측 성공 또는 예측 실패가 결정되는 어느 한 예측 명령은 제 1 예측 명령으로 지칭될 수 있다. 이 경우에, 코어(100)는 예측 성공한 제 1 예측 명령을 비예측 명령으로 확정적으로 처리할 수 있다. 코어(100)는 예측 성공 이전에 제 1 예측 명령에 의해 캐시 메모리 상에서 발생한 변경 상태를 확정하도록 로드큐(120)를 통해 캐시 메모리(예를 들어, L1 캐시 메모리(200))로 확정 초인종 신호를 송신할 수 있다. 구체적으로 설명하면, 로드큐(120)는 예측 추적 버퍼에 저장되어 있는 제 1 예측 명령의 예측 추적 정보를 이용하여 예측 성공한 예측 명령이 속하는 예측 블록을 결정할 수 있다. 예측 블록은 어느 한 예측 명령을 근원으로 하는 하나 이상의 예측 명령의 집합일 수 있다. 환언하면, 예측 블록은 어느 한 예측 명령에 따라 예측 실행되는 하나 이상의 명령들을 지칭할 수 있다. 편의상, 제 1 예측 명령이 속하는 예측 블록은 제 1 예측 블록으로 지칭될 수 있다. 이 경우에, 제 1 예측 블록은 제 1 예측 명령을 근원으로 하는 하나 이상의 예측 명령의 집합일 수 있다.
- [0043] 프로세서(1000)는 제 1 예측 명령에 대한 예측 실행의 결과가 결정되는 경우, 제 1 예측 명령이 속하는 제 1 예측 블록에 대한 확정 신호를 생성할 수 있다. 이로 인해, 본 개시의 프로세서(1000)는 특정 로드 명령이 리오더 버퍼(230)에서 확정될 때 기다리지 않고 예측 명령을 처리할 수 있는 장점을 가질 수 있다.
- [0044] 로드큐(120)는 제 1 예측 명령을 근원으로 하는 예측 블록에 의한 L1 캐시 메모리(200)의 상태 변경을 확정하도록 확정 초인종 신호를 L1 캐시 메모리(200)로 송신할 수 있다. 이 경우에, 이하에서 설명되는 바와 같이, L1 캐시 메모리(200)의 라이트 버퍼(210)는 예측 성공한 예측 명령에 의해 추출된 캐시블록을 안전하게 확정 처리할 수 있다.

- [0045] 본 개시의 몇몇 실시예에 따라, 라이트 버퍼(210)는 예측 명령에 의해 발생한 요청이 상기 L1 캐시 메모리로 반환됨에 따라 L1 캐시 메모리(200)의 태그 및 데이터 영역(230)으로부터 추출되는 추출 캐시블록을 저장할 수 있다. 또한, 라이트 버퍼(210)는 제 1 예측 블록에 대한 확정 초인종 신호 또는 복구 초인종 신호를 수신하는 경우에, 제 1 예측 블록에 대응하는 추출 캐시블록에 대한 확정 동작 또는 복구 동작을 수행할 수 있다.
- [0046] 구체적으로 설명하면, 예측 명령에 의해 발생한 요청은 예측 명령을 수행하기 위해 코어(100)가 참조하고자 하는 데이터가 캐시 메모리 상에 저장되어 있는지 확인하는 요청일 수 있다. L1 캐시 메모리(200)의 캐시 히트(cache hit)는 예측 명령에 의해 발생한 요청에 따라 코어(100)가 참조하고자 하는 데이터가 L1 캐시 메모리(200) 상에 존재하는 경우를 의미할 수 있다. 또한, L1 캐시 메모리(200)의 캐시 미스(cache miss)는 예측 명령에 의해 발생한 요청에 따라 코어(100)가 참조하고자 하는 데이터가 L1 캐시 메모리(200) 상에 존재하지 않는 경우를 의미할 수 있다. 캐시 미스가 발생하는 경우, L1 캐시 메모리(200)는 저레벨 캐시(예를 들어, L2 캐시 메모리(300)), 메모리, 또는 디스크에 대하여 해당 데이터를 요청할 수 있다. L1 캐시 메모리(200)의 캐시 미스가 발생함에 따라, L1 캐시 메모리(200)는 저레벨 캐시, 메모리, 또는 디스크로 예측 명령에 의해 발생한 요청을 송신하고, 이에 따라 예측 명령에 의해 발생한 요청이 저레벨 캐시, 메모리 또는 디스크로부터 다시 반환될 수 있다. 예측 명령에 의해 발생한 요청이 반환됨에 따라, 저레벨 캐시, 메모리 또는 디스크로부터 수신한 데이터는 L1 캐시 메모리(200) 상의 데이터 영역 상에 저장될 수 있다. 이러한 데이터는 편의상 갱신 캐시블록으로 지칭될 수 있다. 일반적으로 L-1 캐시 메모리(200)는 비교적 적은 용량을 가지므로, 이전에 데이터 영역 상에 저장된 일부 데이터가 갱신 캐시블록을 저장하기 위해서 추출될 수 있다. 추출되는 데이터는 편의상 추출 캐시블록으로 지칭될 수 있다. 추출 캐시블록은 복구 버퍼로 역할하는 라이트 버퍼(210) 상에 저장될 수 있다.
- [0047] 로드큐(120)에 의해 송신된 제 1 예측 블록에 대한 확정 초인종 신호(Commit Doorbell)를 수신하는 경우, 라이트 버퍼(210)는 제 1 예측 블록에 대응하는 추출 캐시블록에 대한 확정 동작을 수행할 수 있다. 여기서 확정 동작은 제 1 예측 블록에 대응하는 추출 캐시블록을 캐시블록의 상태에 따라 저레벨 캐시에 갱신하거나 또는 삭제(무효화)하는 동작을 포함할 수 있다. 제 1 예측 블록에 대응하는 추출 캐시블록에 대한 복구 동작은 이하에서 설명되는 예측 실행에 대하여 예측 실패가 결정되는 경우와 관련하여 설명된다.
- [0048] 어느 한 예측 명령에 대한 예측 실행에 대하여 예측 실패가 결정되는 경우, 코어(100)는 예측 실패한 예측 명령을 스쿼시(squash)하고, 예측 실패한 예측 명령에 대한 복구 동작을 수행할 수 있다. 예를 들어, 리오더 버퍼(130)는 엔트리에서 예측 실패한 예측 명령을 제거할 수 있다. 이 경우에, 코어(100)는 예측 명령에 의해 캐시 메모리 상에서 발생한 변경 상태를 복구하도록 로드큐(120)를 통해 캐시 메모리(예를 들어, L1 캐시 메모리(200))로 복구 초인종 신호를 송신할 수 있다. 구체적으로 설명하면, 예측 성공한 경우와 마찬가지로, 로드큐(120)는 예측 추적 버퍼에 저장되어 있는 예측 추적 정보를 이용하여 예측 실패한 예측 명령이 속하는 예측 블록을 결정할 수 있다. 편의상, 예측 성공한 경우와 관련하여 설명한 예와 마찬가지로, 예측 실패가 결정되는 예측 명령은 제 1 예측 명령으로 지칭되고, 그리고 제 1 예측 명령이 속하는 예측 블록은 제 1 예측 블록으로 지칭될 수 있다.
- [0049] 로드큐(120)는 제 1 예측 명령을 근원으로 하는 예측 블록에 의한 L1 캐시 메모리(200)의 상태 변경을 복구하도록 복구 초인종 신호를 L1 캐시 메모리(200)로 송신할 수 있다. 이 경우에, L1 캐시 메모리(200)는 예측 실패한 제 1 예측 명령에 의해 L1 캐시 메모리(200)의 데이터 영역 상에 갱신된 캐시블록을 무효화할 수 있다. 그리고, 라이트 버퍼(210)는 제 1 예측 블록에 대응하는 추출 캐시블록에 대한 복구 동작을 수행할 수 있다. 예를 들어, 예측 실패한 제 1 예측 명령에 의해 추출됨으로써 라이트 버퍼(210) 상에 저장된 추출 캐시블록은 다시 캐시 메모리의 데이터 영역 상에 원래 위치로 복구될 수 있다. 따라서, 라이트 버퍼(210)는 추출된 캐시블록을 일시적으로 보관하는 복구 버퍼로 사용될 수 있다. 상술한 바와 같이, 라이트-백 버퍼와 같은 라이트 버퍼(210)를 복구 버퍼로 사용함으로써 두 가지 이점이 획득될 수 있다. 첫 번째는 라이트 버퍼(210)가 L1 캐시 메모리(200)의 데이터 영역과 가까이에 위치함으로 복구 시에 발생하는 성능저하를 줄일 수 있다. 두 번째는 복구를 위해 추가적인 메모리 버퍼를 사용하지 않기 때문에 구현하기 위해 추가적인 메모리 영역이 필요하지 않다.
- [0050] 도 2는 본 개시의 몇몇 실시예에 따른 코어(100)의 구조 및 그 동작을 설명하기 위한 도면이다.
- [0051] 이하에서, 도 2를 참조하여, 본 개시의 몇몇 실시예에 따라 개선된 프로세서(1000)의 코어(100)의 구조와 그들의 동작에 대하여 자세히 설명한다. 또한, 도 2를 참조하여, 코어(100) 상에서 예측 추적 버퍼(110), 로드큐(120), 리오더 버퍼(130)를 활용하여 복구/확정 초인종을 생성하는 예시가 상세하게 설명된다.
- [0052] 상술한 바와 같이, 코어(100)는 L1 캐시 메모리 상에 복구 동작 또는 확정 동작을 시작하기 위한 복구/확정 초인종 신호(10/20)를 로드큐(120)를 통해 L1 캐시 메모리(200)로 송신할 수 있다. 상술한 바와 같이, 코어(100)

는 예측 실행의 결과에 따라 적절한 시점에 복구/확정 초인종 신호(10/20)를 송신하기 위해 예측 명령을 추적하는 예측 추적 버퍼(110)를 포함할 수 있다.

[0053] 예측 추적 버퍼(110)는 예측 명령이 리오더 버퍼(reorder buffer, ROB)(130)에 할당되는 경우, 예측 명령을 추적하기 위해 예측 추적 정보를 저장할 수 있다. 예측 추적 버퍼(110)는 예를 들어 분기 명령과 같은 예측 명령을 추적하는 순환 버퍼일 수 있다. 도 2를 참조하여 구체적인 동작에 대하여 설명하면, 'BNE' 명령이 리오더 버퍼 상에 할당되는 경우, 'BNE' 명령에 대한 예측 추적 정보가 예측 추적 버퍼(110)의 엔트리에 저장될 수 있다. 예측 추적 정보는 예측 명령을 추적하기 위한 다양한 정보를 포함할 수 있다. 예를 들어, 도 2에서 도시되는 바와 같이, 예측 추적 정보는 예측 명령이 유효한지를 나타내는 유효 비트(111)와 예측 명령의 리오더 버퍼(130) 상의 엔트리 넘버(112)를 포함할 수 있다. 도 2에서 설명한 실시예와 마찬가지로, 제 1 예측 명령이 속하는 예측 블록은 제 1 예측 블록으로 지칭될 수 있다. 도 2를 참조하여 설명하면, 예측 블록에 속하는 예측 명령을 동일한 무늬를 가지도록 표시되었다. 예를 들어, 제 1 예측 명령이 'BNE'인 경우, 'BNE'를 근원으로 하는 제 1 예측 블록은 연한 점무늬로 표시되어 있다. 다른 예로, 제 1 예측 명령이 'BEQ'인 경우, 'BEQ'를 근원으로 하는 제 1 예측 블록은 같은 방향의 사선 무늬를 가지도록 표시되어 있다. 예측 추적 정보는 제 1 예측 명령의 리오더 버퍼 상의 엔트리 넘버(112)를 포함하므로, 제 1 예측 명령의 예측 실행의 결과가 결정되는 경우, 로드큐(120)는 제 1 예측 명령의 리오더 버퍼 상의 엔트리 넘버(112)를 제 1 예측 명령의 식별정보로 사용하여 로드큐(120) 상에 할당되어 있는 제 1 예측 블록을 식별할 수 있다.

[0054] 본 개시의 몇몇 실시예에 따라, 로드큐(120)의 엔트리는 종전의 프로세서 구조에 비해 예측 추적 버퍼와 연계하기 위한 예측 명령 로드 정보(SPL)(121) 및 예측 명령 추적 식별 정보(STB ID)(122)를 저장하는 영역을 더 포함할 수 있다. 예측 명령 로드 정보(SPL)는 예측 명령이 예측 실행의 결과에 따라 비예측 명령이 되었는지 여부를 나타내는 값일 수 있다. 예를 들어, 예측 명령이 로드큐(120)에 할당되는 경우 아직 예측 실행의 결과가 결정되지 않았음을 표시하기 위해 예측 명령 로드 정보(SPL)가 설정될 수 있다(예를 들어, 예측 명령 로드 정보(SPL)는 '1'의 1 비트 값을 가짐). 이후에 예측 명령의 결과가 예측 성공으로 결정되는 경우, 예측 명령을 비예측 명령으로 확정 처리하기 위해 예측 명령 로드 정보(SPL)가 해제될 수 있다(예를 들어, 예측 명령 로드 정보(SPL)는 '0'의 1비트 값을 가짐).

[0055] 예측 명령 추적 식별 정보(STB ID)(122)는 로드큐(120)에 의해 예측 블록을 결정하는데 사용될 수 있다. 예를 들어, 동일한 예측 명령 식별 정보(122)를 가지는 로드큐(120)의 엔트리는 동일한 예측 블록에 속할 수 있다. 도 2를 참조하면, 동일한 방향의 사선 무늬를 가지는 로드큐(120)의 첫번째 및 두번째 엔트리는 동일한 예측 블록에 속할 수 있다. 이 경우에, 로드큐(120)의 첫번째 및 두번째 엔트리는 동일한 예측 명령 추적 식별 정보(STB ID)를 가질 수 있다. 다른 예로, 동일한 점무늬를 가지는 로드큐(120)의 세번째 및 네번째 엔트리는 동일한 예측 블록에 속할 수 있다. 이 경우에, 로드큐(120)의 세번째 및 네번째 엔트리는 동일한 예측 명령 추적 식별 정보(STB)를 가질 수 있다.

[0056] 이하에서, 제 1 예측 명령의 예측 성공 또는 예측 실패가 결정됨에 따라 복구 초인종 신호(10) 및 확정 초인종 신호(20)를 발생시키는 구체적인 동작들이 설명된다.

[0057] 본 개시의 몇몇 실시예에 따라, 제 1 예측 명령의 예측 실패가 결정되는 경우, 로드큐(120)는 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값을 포함하는 복구 초인종 신호(10)를 L1 캐시 메모리(200)로 송신할 수 있다.

[0058] 구체적으로 설명하면, 제 1 예측 명령의 예측 실패가 결정되는 경우, 리오더 버퍼(130) 상에서 제 1 예측 명령 이후에 디스패치(dispatch)된 명령들(즉, 제 1 예측 블록)이 추출될 수 있다. 이 경우에, 리오더 버퍼(130)에 추출되는 명령들은 예측 추적 버퍼(110) 및 로드큐(120)에서도 같이 추출될 수 있다. 예를 들어, 도 2를 참조하면, 'BNE'인 제 1 예측 명령의 예측 실패가 결정되는 경우, 'BNE' 이후에 실행된 명령들이 예측 추적 버퍼(110) 및 로드큐(120)에서 추출(또는 무효화)될 수 있다. 로드큐(120)는 무효화되는 제 1 예측 블록에 의해 L1 캐시 메모리(200) 상에서 발생한 변경 상태를 복구하기 위해 제 1 예측 블록에 대한 복구 초인종 신호(10)를 L1 캐시 메모리(200)로 송신할 수 있다. 제 1 예측 블록에 대한 복구 초인종 신호(10)는 제 1 예측 블록에 속하는 하나 이상의 예측 명령의 주소값(124)을 포함할 수 있다. 이 경우에, 이하에서 설명되는 바와 같이, L1 캐시 메모리(200)는 복구 초인종 신호(10)에 포함된 예측 명령의 주소값(124)을 이용하여 라이트 버퍼(210)로부터 L1 캐시 메모리(200)의 데이터 영역으로 복구될 복구 캐시블록을 결정할 수 있다. 이하에서, 제 1 예측 명령의 예측 성공이 결정되는 경우에 대하여 설명한다.

[0059] 본 개시의 몇몇 실시예에 따라, 상기 제 1 예측 명령의 예측 성공이 결정되는 경우, 예측 추적 버퍼(110)는 리

오더 버퍼(130)로부터 제 1 예측 명령에 대한 확정 신호를 수신하는 경우, 제 1 예측 명령의 유효 비트가 설정되어 있는지 결정하고, 그리고 제 1 예측 명령의 유효 비트가 설정되어 있는 경우, 상기 제 1 예측 명령의 식별 정보를 상기 로드큐(120)로 송신할 수 있다. 로드큐(120)는 제 1 예측 명령의 식별정보를 수신하는 경우, 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값을 포함하는 확정 초인종 신호를 상기 L1 캐시 메모리(200)로 송신할 수 있다.

[0060] 구체적으로 설명하면, 제 1 예측 명령의 예측 성공이 결정되는 경우, 코어(100)는 제 1 예측 명령이 속하는 제 1 예측 블록에 포함되는 예측 명령을 비예측 명령으로 확정 처리할 수 있다. 이 경우에, 예측 추적 버퍼(110)는 리오더 버퍼(130)로부터 제 1 예측 명령에 대한 확정 신호를 수신할 수 있다. 제 1 예측 명령에 대한 확정 신호는 예를 들어 제 1 예측 명령의 인덱스 번호를 포함할 수 있다. 이 경우에, 예측 추적 버퍼(110)는 제 1 예측 명령의 인덱스 번호를 예측 추적 정보에 포함되어 있는 예측 명령들의 리오더 버퍼(130) 상의 엔트리 넘버(112)와 비교함으로써 제 1 예측 명령에 대한 예측 추적 정보를 탐색할 수 있다. 제 1 예측 명령에 대한 예측 추적 정보가 탐색되는 경우, 예측 추적 버퍼(110)는 제 1 예측 명령에 대한 예측 추적 정보의 유효 비트(111)가 설정(예를 들어, '1'의 1비트 값을 가짐)되어 있는지 확인할 수 있다. 유효 비트가 설정되어 있는 경우, 예측 추적 버퍼(110)는 제 1 예측 명령의 식별 정보를 로드큐(120)로 송신할 수 있다. 여기서 예측 명령의 식별 정보는 제 1 예측 명령의 리오더 버퍼(130) 상의 엔트리 넘버(112)를 포함할 수 있다. 반대로, 유효 비트가 설정되어 있지 않은 경우(예를 들어, '0'의 1비트 값을 가짐), 예측 추적 버퍼(110)는 제 1 예측 명령의 식별 정보를 로드큐(120)로 송신하지 않을 수 있다.

[0061] 로드큐(120)는 제 1 예측 명령의 식별 정보를 수신하는 경우, 제 1 예측 명령의 식별 정보를 이용하여 로드큐(120) 상에 저장되어 있는 제 1 예측 블록을 결정할 수 있다. 그리고, 로드큐(120)는 제 1 예측 블록에 포함되는 예측 명령에 대한 확정 초인종 신호(20)를 L1 캐시 메모리(200)로 송신할 수 있다. 이 경우에, L1 캐시 메모리(200)는 이하에서 설명되는 바와 같이 제 1 예측 블록에 의한 캐시 메모리의 변경 상태를 확정 처리할 수 있다. 여기서, 확정 초인종 신호는 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값(124)을 포함할 수 있다. 예측 명령의 주소값(124)은 라이트 버퍼(210) 상에 저장되어 있는 추출 캐시블록 중에서 확정 처리될 확정 캐시블록을 결정하는데 사용될 수 있다.

[0062] 본 개시의 몇몇 실시예에 따라, 로드큐(120)는 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 예측 명령 로드 정보(SPL)가 설정되어 있는 경우에 확정 초인종 신호(20)를 송신할 수 있다.

[0063] 구체적으로 설명하면, 예측 명령 로드 정보(SPL)가 해제되어 있는 경우 예측 명령은 이미 비예측 명령으로 확정 처리된 경우이므로, 로드큐(120)는 제 1 예측 블록 중에서 예측 명령 로드 정보(SPL)가 해제된 명령에 대하여 확정 초인종 신호를 송신할 필요가 없다. 따라서, 로드큐(120)는 제 1 예측 블록의 예측 명령 로드 정보(SPL)를 확인한 후에, 예측 명령 로드 정보(SPL)가 설정되어 있는 명령에 대하여 확정 초인종 신호(20)를 송신할 수 있다.

[0064] 도 3은 본 개시의 몇몇 실시예에 따른 프로세서(1000)의 L1 캐시 메모리(200)의 개략적인 구조를 나타낸다.

[0065] 이하에서, 도 3을 참조하여, 본 개시의 몇몇 실시예에 따라 개선된 프로세서(1000)의 L1 캐시 메모리(200)의 구조와 그들의 동작에 대하여 자세히 설명한다.

[0066] 본 개시의 몇몇 실시예에 따라, 도 3을 참조하면, L1 캐시 메모리(200)의 컴포넌트 중에서 종전의 프로세서 구조에 비해 추가된 구성은 볼드체로 표시되어 있다. 구체적으로 설명하면, MSHR(220)은 예측 명령 로드 정보(SPL) 및 스쿼시 정보(SQ)를 저장하는 영역을 엔트리 상에 더 포함할 수 있다. MSHR(220)의 예측 명령 로드 정보(SPL)는 캐시 미스에 따라 예측 명령에 의해 발생한 요청을 저레벨 캐시, 메모리, 또는 디스크로 송신하는 경우에, 예측 명령에 의해 발생한 요청이 비확정 명령으로 확정 처리되었는지를 나타내는 정보일 수 있다. 스쿼시 정보(SQ)는 예측 명령에 의해 발생한 요청이 L1 캐시 메모리(200)로 반환되기 전에 복구 초인종 신호를 수신한 경우, 이중 처리를 방지하기 위해 이후에 반환되는 요청을 무시하는데 사용될 수 있다.

[0067] 본 개시의 몇몇 실시예에 따라, 라이트 버퍼(210)는 추출 캐시블록을 저장하는 경우에, 상기 추출 캐시블록의 예측 명령 추출 정보(SPE)(211), 상태 데이터(212), 교체 주소 정보(213)를 설정할 수 있다.

[0068] 상술한 바와 같이, 라이트 버퍼(210)는 캐시 미스가 발생하는 경우에 갱신 캐시블록을 저장하기 위해 데이터 영역 상에 저장된 일부 데이터를 추출할 수 있다. 추출되는 데이터는 편의상 추출 캐시블록으로 지칭될 수 있다. 상술한 바와 같이 추출 캐시블록은 복구 버퍼로 역할하는 라이트 버퍼(210) 상에 저장될 수 있다. 본 개시에 몇몇 실시예에 따라, 라이트 버퍼(210)는 추출 캐시블록의 복구 동작을 지원하기 위해 변형되었다. 구체적으로 설

명하면, 라이트 버퍼(210)는 예측 명령 추출 정보(SPE), 상태 데이터, 교체 주소 정보(213)를 설정하는 영역을 엔트리 상에 더 포함할 수 있다. 예측 명령 추출 정보(SPE)는 추출 캐시블록이 확정 동작에 의해 확정 처리되지 않았음을 나타낼 수 있다. 예를 들어, 예측 명령 추출 정보(Speculative evicted, SPE)는 추출 캐시블록이 라이트 버퍼(210)에 저장되는 경우에 설정될 수 있다. 또한, 예측 명령 추출 정보(SPE)는 비예측 명령으로 확정처리하기 위해 추출 캐시블록에 대하여 확정 초인종 신호를 수신한 경우에 해제될 수 있다. 상태 데이터(212), 교체 주소 정보(213)는 이하에 설명되는 바와 같이 추출 캐시블록의 복구 동작 또는 확정 동작에 사용될 수 있다. 상태 데이터(212), 교체 주소 정보(213)는 추출 캐시블록이 라이트 버퍼(210)에 저장되는 경우에 태그 및 데이터 영역(230)으로부터 복제될 수 있다. 태그 및 데이터 영역(230)은 갱신 캐시블록에 대하여 예측 명령 갱신 정보(SPI)(231)를 설정하기 위한 영역을 더 포함할 수 있다. 예측 명령 갱신 정보(SPI)(231)는 갱신 캐시블록을 저장하기 위해 추출되는 캐시블록이 라이트 버퍼(210) 상에 저장됨을 나타내는 정보일 수 있다. 예측 명령 갱신 정보(SPI)(231)는 이하에서 설명되는 바와 같이 메모리 상태 변경을 확정 처리하는 경우에 해제될 수 있다.

[0069] 이하에서, 도 4 내지 도 6을 참조하여, L1 캐시 메모리 상에 추출 캐시블록의 확정 동작 및 복구 동작이 설명된다.

[0070] 도 4는 본 개시의 몇몇 실시예에 따라, 예측 명령에 의해 발생된 요청이 L1 캐시 메모리(200)로 반환되는 경우에 L1 캐시 메모리(200)의 동작을 설명하기 위한 도면이다.

[0071] 본 개시의 몇몇 실시예에 따라, L1 캐시 메모리(200)는 예측 명령에 의해 발생한 요청에 따라 L1 캐시 메모리(200)로 반환된 갱신 캐시블록을 L1 캐시 메모리(200)의 태그 및 데이터 영역(230)에서 추출되는 캐시블록의 위치에 저장하고, 그리고 갱신 캐시블록에 대하여 예측 명령 갱신 정보(SPI)(231)를 설정할 수 있다.

[0072] 구체적으로 설명하면, 상술한 바와 같이, 라이트 버퍼(210)는 예측 명령에 의해 발생한 요청이 상기 L1 캐시 메모리(200)로 반환됨에 따라 L1 캐시 메모리(200)의 태그 및 데이터 영역(230)으로부터 추출되는 캐시블록의 위치에 반환된 요청에 따라 수신된 데이터를 저장할 수 있다. 구체적으로 설명하면, L1 캐시 메모리(200)에서 캐시 미스가 발생하는 경우, L1 캐시 메모리(200)는 저레벨 캐시, 메모리, 또는 디스크에 대하여 해당 데이터를 요청할 수 있다. 이러한 요청에 대한 정보는 MSHR(220) 상에 저장될 수 있다. 이 경우에, MSHR(220)은 예측 명령에 의해 발생한 요청이 예측 명령에 의한 요청임을 나타내도록 예측 명령 로드 정보(SPL)를 설정할 수 있다. 예측 명령에 의해 발생한 요청이 L1 캐시 메모리(200)로 반환되는 경우(도 4에서 원문자 1번 참조), MGHR(220)은 해당 요청에 대한 예측 명령 로드 정보(SPL)가 설정되어 있는지 확인할 수 있다. 해당 요청에 대한 예측 명령 로드 정보(SPL)가 설정되어 있는 경우, 예측 실행의 결과가 아직 결정되지 않았으므로 해당 요청에 의해 추출되는 캐시블록(즉, 추출 캐시블록)은 라이트 버퍼(210) 상에 저장될 수 있다(도 4에서 원문자 2번 참조). 이 경우에, 태그 및 데이터 영역(230) 상에 저장되어 있는 상태 데이터(232), 태그(233), 데이터(234) 등이 복제되고, 그리고 라이트 버퍼(210) 상에 저장될 수 있다(도 3의 212, 214, 215 참조). 또한, 해당 요청에 의해 사용된 태그 및 데이터 영역(230)의 주소값은 라이트 버퍼(210) 상에 추출 캐시블록의 교체 주소 정보(213)로 저장될 수 있다. 교체 주소 정보(213)는 이하에 설명되는 바와 같이, 추출 캐시블록을 다시 태그 및 데이터 영역(230) 상에 복구하는데 사용될 수 있다. 그리고, 반환된 요청에 의해 수신된 데이터는 추출 캐시블록이 위치하던 태그 및 데이터 영역(230) 상에 갱신 캐시블록으로 저장될 수 있다(도 4에서 원문자 3번). 이러한 갱신 캐시블록은 예측 명령에 의해 발생한 요청에 따라 저장되었으므로, 갱신 캐시블록에 대하여 예측 명령 갱신 정보(SPI)가 설정될 수 있다.

[0073] 도 5는 본 개시의 몇몇 실시예에 따라, 복구 초인종 신호(10)에 따라 추출 캐시블록을 복구하는 L1 캐시 메모리(200)의 동작을 설명하기 위한 도면이다.

[0074] 본 개시의 몇몇 실시예에 따라, 라이트 버퍼(210)는 제 1 예측 명령의 복구 초인종 신호(10)를 수신하는 경우에, 추출 캐시블록 중에서 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값에 대응하는 복구 캐시블록을 결정하고, 그리고 복구 캐시블록을 복구 캐시블록의 교체 주소 정보(213)에 기초하여 태그 및 데이터 영역(230)에 복구할 수 있다.

[0075] 여기서 설명되는 L1 캐시 메모리(200)의 복구 동작은 로드큐(120)로부터 복구 초인종 신호(Restore Doorbell)(10)를 수신하는 경우(도 5에서 원문자 1번 참조)에 수행될 수 있다. 복구 초인종 신호(10)를 수신하는 경우, 라이트 버퍼(210)는 복구 초인종 신호에 포함되어 있는 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값을 이용하여 태그 및 데이터 영역(230) 상에 복구될 추출 캐시블록을 결정할 수 있다. 편의상 복구될 추출 캐시블록은 복구 캐시블록으로 지칭될 수 있다. 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값은 추출 캐시블록에 저장된 예측 명령의 주소값이므로 복구 캐시블록을 결정하는데 사용될 수 있다. 복구

캐시블록이 결정되는 경우, L1 캐시 메모리(200)는 복구 캐시블록의 교체 주소 정보(213)를 이용하여 복구 캐시블록이 추출 전에 태그 및 데이터 영역(230) 상에 저장되어 있던 위치를 식별할 수 있다.

[0076] 본 개시의 몇몇 실시예에 따라, L1 캐시 메모리(200)는 복구 캐시블록을 태그 및 데이터 영역(230)에 복구하기 위해, 복구 캐시블록의 교체 주소 정보(213)에 대응하는 갱신 캐시블록을 복구 캐시블록으로 교체하고, 그리고 복구 캐시블록의 예측 명령 갱신 정보(SPI)를 해제할 수 있다.

[0077] 태그 및 데이터 영역(230) 상에 복구 위치가 식별되면, 복구 캐시블록은 복구 위치 상에 있던 갱신 캐시블록과 교체됨으로써 복구될 수 있다(도 5의 원문자 2번 참조). 이에 따라 태그 및 데이터 영역(230) 상에 저장된 복구 캐시블록은 예측 명령에 의해 갱신된 캐시블록이 아니므로, L1 캐시 메모리(200)는 복구 캐시블록에 대한 예측 명령 갱신 정보(SPI)(231)를 해제할 수 있다.

[0078] 본 개시의 몇몇 실시예에 따라, L1 캐시 메모리(200)는 제 1 예측 명령의 복구 초인종 신호(10)를 수신하는 시점에 제 1 예측 명령에 의해 발생한 요청이 L1 캐시 메모리로 반환되지 않은 경우, 제 1 예측 명령에 대한 스쿼시 정보(SQ)(222)를 설정하는 MSHR(Miss Status Holding Register)를 포함할 수 있다. 그리고, MSHR(220)은 제 1 예측 명령에 대한 스쿼시 정보(SQ)가 설정되어 있는 경우, 제 1 예측 명령에 의해 반환된 요청을 무시할 수 있다.

[0079] 상술한 바와 같이, 본 개시에 따른 MSHR(220)은 스쿼시 정보(SQ)(222)를 저장하는 영역을 엔트리 상에 더 포함할 수 있다. 스쿼시 정보(SQ)(222)는 예측 명령에 의해 발생한 요청이 L1 캐시 메모리(200)로 반환되기 전에 복구 초인종 신호(10)를 수신한 경우, 이중 처리를 방지하기 위해 이후에 반환된 요청을 무시하는데 사용될 수 있다.

[0080] 구체적으로 설명하면, L1 캐시 메모리(200)에서 캐시 미스가 발생함에 따라, 예측 명령에 의해 발생한 요청이 저레벨 캐시, 메모리, 또는 디스크로 송신된 이후에, L1 캐시 메모리(200)가 예측 명령이 속하는 예측 블록에 대한 복구 초인종 신호를 해당 요청이 반환되기 전에 먼저 수신할 수 있다. 이 경우에, 라이트 버퍼(210) 상에 예측 명령에 의해 발생한 요청에 의해 추출된 추측 캐시블록이 검색되지 않으므로, MSHR(210)은 해당 요청에 관련된 예측 명령이 저장되어 있는지 검색하게 된다. 해당 요청이 반환되기 전이므로, MSHR(210) 상에 해당 요청에 관련된 제 1 예측 명령이 저장되어 있을 수 있다. 이 경우에 MSHR(210)은 이중 처리를 방지하기 위해 제 1 예측 명령에 대하여 추출 정보(squashed, SQ)(222)를 설정할 수 있다. 추출 정보(squashed, SQ)(222)가 설정되어 있는 경우 제 1 예측 명령에 의해 반환된 요청에 따라 수신된 데이터는 무효화되어야 하므로, MSHR(210)은 이중 처리를 방지하기 위해 제 1 예측 명령에 의해 반환된 요청을 무시할 수 있다.

[0081] 도 6은 본 개시의 몇몇 실시예에 따라, 확정 초인종 신호(20)에 따라 추출 캐시블록을 확정하는 L1 캐시 메모리(200)의 동작을 설명하기 위한 도면이다.

[0082] 본 개시의 몇몇 실시예에 따라, 라이트 버퍼(210)는 제 1 예측 명령의 확정 초인종 신호(20)를 수신하는 경우에, 추출 캐시블록 중에서 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값에 대응하는 확정 캐시블록을 결정할 수 있다. 또한, L1 캐시 메모리(200)는 확정 캐시블록의 교체 주소 정보(213)에 대응하는 태그 및 데이터 영역(230)의 위치에 있는 갱신 캐시블록의 예측 명령 갱신 정보(SPI)(231)를 해제할 수 있다.

[0083] 여기서 설명되는 L1 캐시 메모리(200)의 확정 처리 동작은 로드큐(120)로부터 확정 초인종 신호(Commit Doorbell)(20)를 수신하는 경우(도 6에서 원문자 1번 참조)에 수행될 수 있다. 확정 초인종 신호(20)를 수신하는 경우, 라이트 버퍼(210)는 확정 초인종 신호(20)에 포함되어 있는 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값을 이용하여 확정 처리될 추출 캐시블록을 결정할 수 있다. 편의상 확정 처리될 추출 캐시블록은 확정 캐시블록으로 지칭될 수 있다. 제 1 예측 블록에 포함되는 하나 이상의 예측 명령의 주소값은 추출 캐시블록에 저장된 예측 명령의 주소값이므로, 예측 명령의 주소값은 확정 캐시블록을 결정하는데 사용될 수 있다. 확정 캐시블록이 결정되는 과정은 도 5에서 설명된 복구 캐시블록이 결정되는 과정과 동일할 수 있다. 확정 캐시블록이 결정되는 경우, 확정 캐시블록이 추출됨에 따라 태그 및 데이터 영역(230) 상에 저장된 갱신 캐시블록에 대한 확정 처리를 위해, L1 캐시 메모리(200)는 교체 주소 정보(213)를 이용하여 태그 및 데이터 영역(230) 상에 확정 처리될 갱신 캐시블록을 결정할 수 있다. 자세히 설명하면, 확정 캐시블록의 교체 주소 정보는 태그 및 데이터 영역(230) 상에 확정 캐시블록이 추출됨에 따라 저장된 갱신 캐시블록의 위치를 나타낼 수 있다. 따라서, 확정 캐시블록의 교체 주소 정보는 확정 처리될 갱신 캐시블록을 식별하는데 사용될 수 있다. 확정 처리될 갱신 캐시블록이 결정되는 경우, L1 캐시 메모리(200)는 확정 캐시블록의 교체 주소 정보에 대응하는 갱신 캐시블록의 예측 명령 갱신 정보(SPI)(231)를 해제할 수 있다. 확정 초인종 신호를 수신함에 따라 확정 캐시블록이 결정되는 경우, L1 캐시 메모리(200)는 확정 캐시블록의 교체 주소 정보에 대응하는 갱신 캐시블록의 예측 명령 갱신 정보(SPI)(231)를 해제할 수 있다.

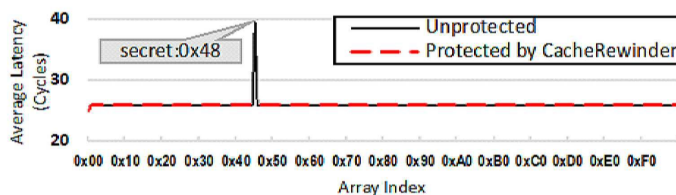
시블록들이 태그 및 데이터 영역(220) 상에 복구될 수 없으므로, 갱신 캐시블록의 예측 명령 갱신 정보(SPI)(231)는 확정 처리를 위해 해제(도 6의 원문자 2번 참조)될 수 있다.

[0084] 본 개시의 몇몇 실시예에 따라, 라이트 버퍼(210)는 확정 캐시블록의 상태 데이터(212)가 'clean'으로 설정된 경우에, 상기 확정 캐시블록의 예측 명령 추출 정보(SPE)(211)를 해제하고, 확정 캐시블록의 상태 데이터(212)가 'dirty'로 설정된 경우에, 상기 확정 캐시블록을 무효화할 수 있다.

[0085] 상술한 바와 같이, 확정 캐시블록들은 다시 태그 및 데이터 영역(220) 상에 복구되지 않아야 한다. 이 경우에, 확정 캐시블록은 상태 데이터에 따라 처리될 수 있다(도 6의 원문자 번호 3 참조). 구체적으로 설명하면, 확정 캐시블록의 상태 데이터가 'dirty'로 설정된 경우에, 확정 캐시블록은 라이트 버퍼(210)에 그대로 남을 수 있다. 그리고 라이트 버퍼(210)는 확정 캐시블록의 예측 명령 추출 정보(SPE)(211)를 해제할 수 있다. 이 경우에, 확정 캐시블록은 더 이상 예측 명령에 의해 추출된 캐시블록이 아니므로, 기존의 라이트 버퍼(210)의 동작에 따라 처리될 수 있다. 예를 들어, 확정 캐시블록은 저레벨 캐시로 갱신될 수 있다. 또한, 라이트 버퍼(210)는 확정 캐시블록의 상태 데이터가 'clean'으로 설정된 경우에, 확정 캐시블록은 라이트 버퍼(210) 상에서 제거될 수 있다. 확정 캐시블록이 제거된 공간은 다른 캐시블록을 위한 공간으로 할당될 수 있다.

[0086] 모든 라이트 버퍼(210)의 엔트리가 점유된 경우에, 더 많은 캐시미스가 발생하면 추출된 캐시블록을 저장할 수 있는 공간이 부족하기 때문에 본 개시의 몇몇 실시예에 따른 프로세서(1000)는 로드 명령어에 대한 수행을 일시 중단할 수 있다. 따라서, 라이트 버퍼(210)가 넘치는 상황이 발생하지 않기 때문에 본 개시에 따른 프로세서는 PRIME+PROBE 등의 방식을 개량한 캐시 부채널 공격에 취약하지 않을 수 있다. 그리고, 기존의 라이트 버퍼(210)의 버퍼 동작에 따라 여유 공간이 생기게 되는 경우, 프로세서(1000)는 로드 명령어에 대한 수행을 재개할 수 있다.

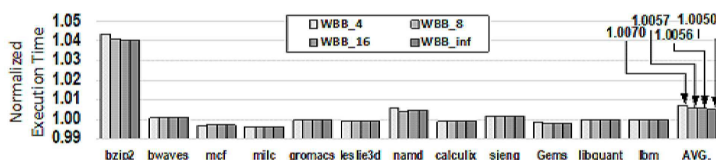
[0087] [표 1]



[0088]

[0089] 표 1을 참조하면, 본 개시의 프로세서(1000)가 일시적 실행 공격을 효과적으로 방어할 수 있음을 볼 수 있다. 기존의 프로세서는 일시적 실행 공격에 의하여 평균 레이턴시(Average latency)가 급격히 상승한 부분이 존재하며, 이 경우에 데이터가 탈취될 수 있다. 이와 달리, 본 개시에 따른 프로세서(1000)는 평균 레이턴시(Average latency)가 급격히 상승하는 부분이 없이 일정한 수치를 유지함을 볼 수 있다.

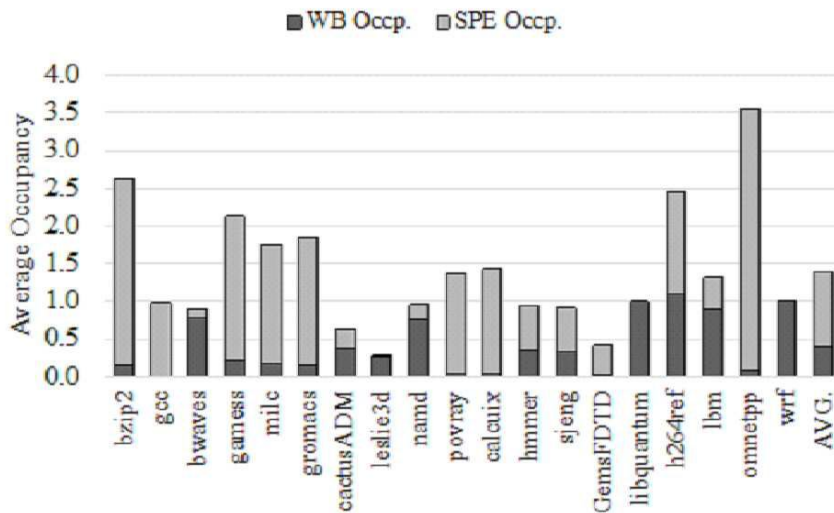
[0090] [표 2]



[0091]

[0092] 표 2를 참조하면, 본 개시의 프로세서(1000)에 의해 캐시 메모리의 상태 변경이 복구되는 경우 매우 낮은 오버헤드(약 0.5% 내지 0.7%)가 발생하였다. 또한, 표 2는 성능 평가에 있어서 라이트 버퍼의 크기가 작은 비율을 차지함을 나타내었다.

[0093] [표 3]



[0094]

[0095] 표 3을 참조하면, 본 개시의 프로세서(1000) 상에 평균적으로 약 0.98만큼 라이트 버퍼(210) 활용률이 높아짐을 알 수 있다.

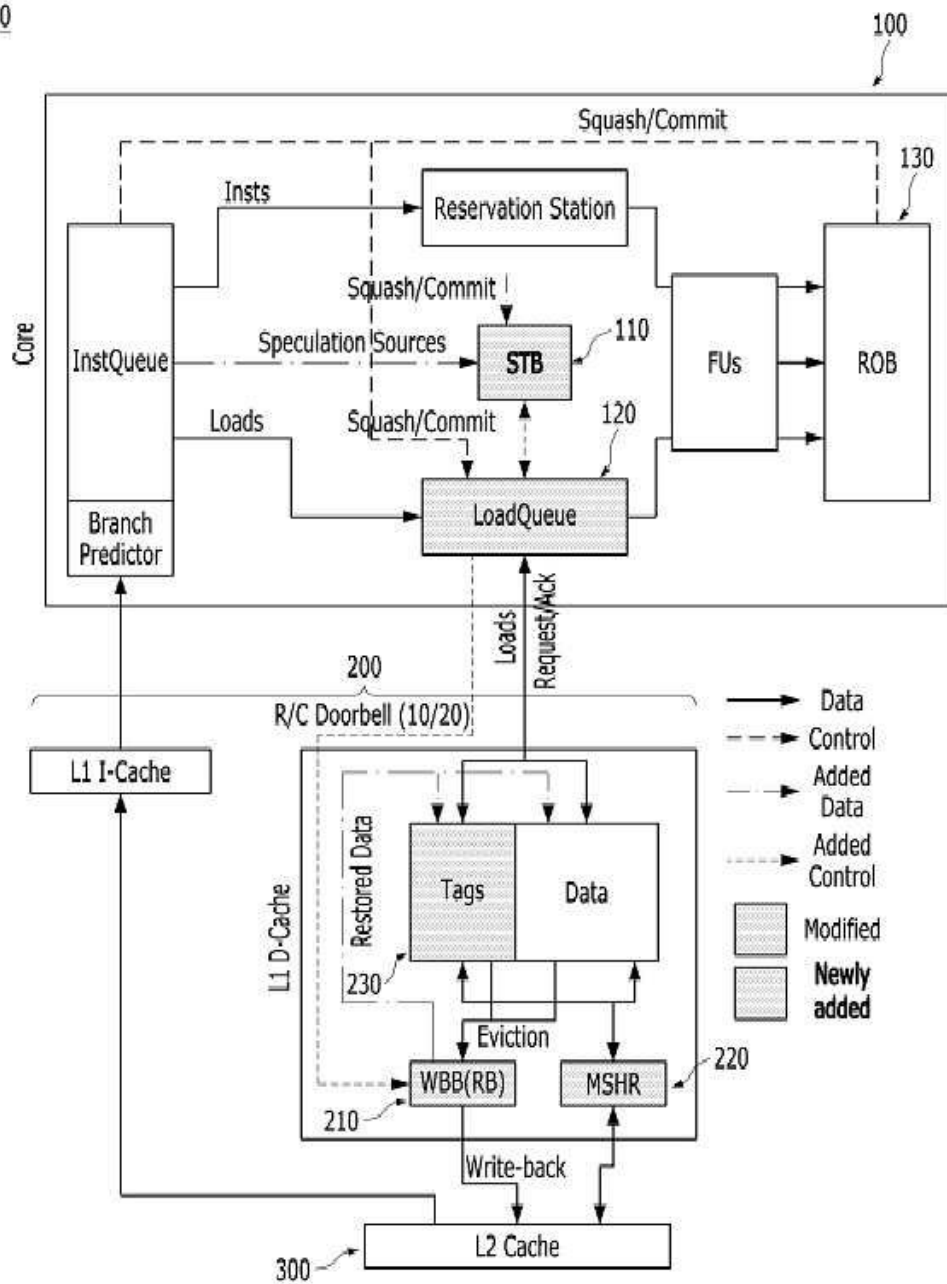
[0096] 결과적으로, 본 개시는 라이트-백 버퍼에서 활용되지 않고 남은 공간들을 예측 실행에 따른 캐시 메모리의 상태를 복구하기 위한 공간으로 활용하여 기존의 일시적 실행 공격을 방어하기 위한 구조적 해결 방법을 제시할 수 있다.

[0097] 제시된 실시예들에 대한 설명은 임의의 본 개시의 기술 분야에서 통상의 지식을 가진 자가 본 개시를 이용하거나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 명백할 것이며, 여기에 정의된 일반적인 원리들은 본 개시의 범위를 벗어남이 없이 다른 실시예들에 적용될 수 있다. 그리하여, 본 개시는 여기에 제시된 실시예들로 한정되는 것이 아니라, 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위에서 해석되어야 할 것이다.

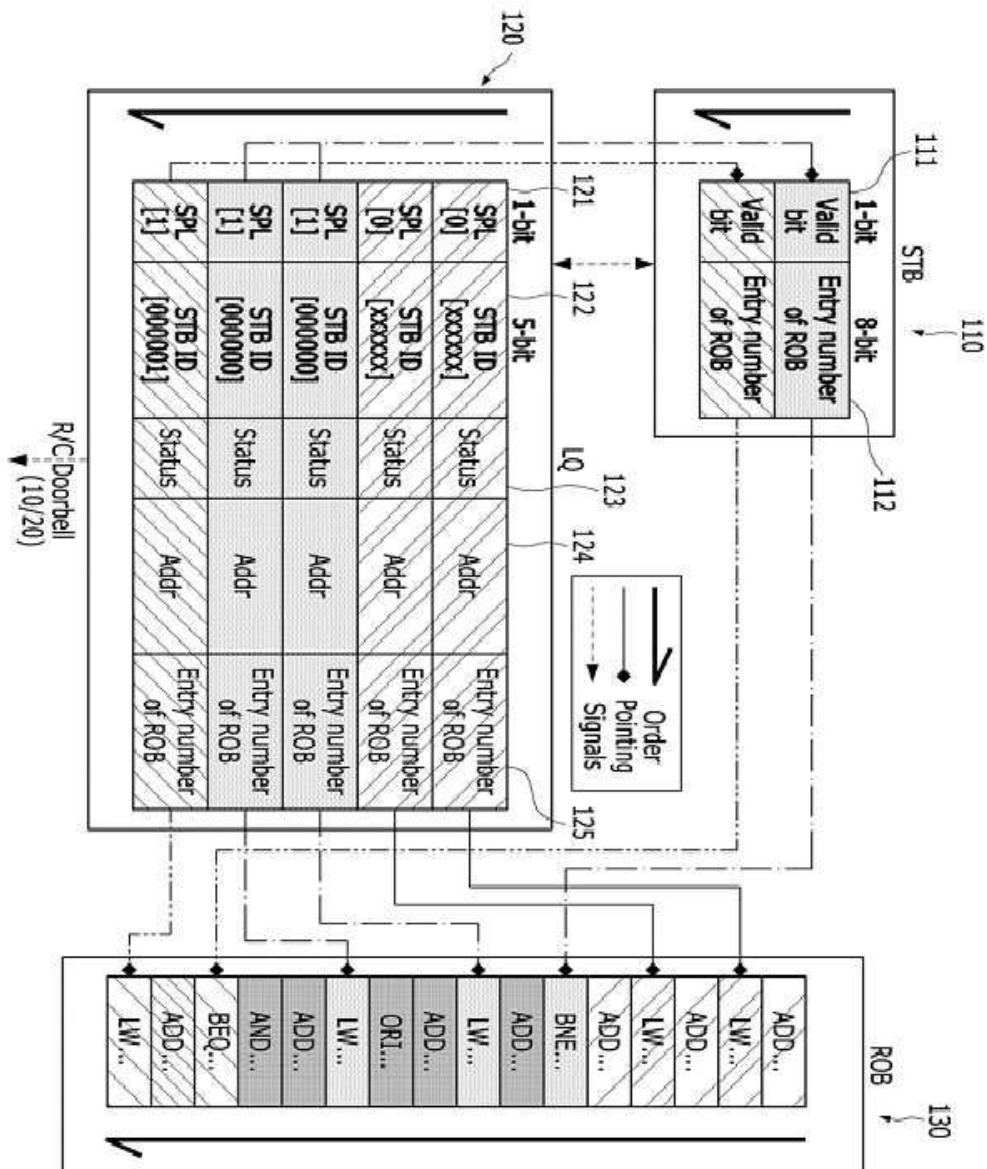
도면

도면1

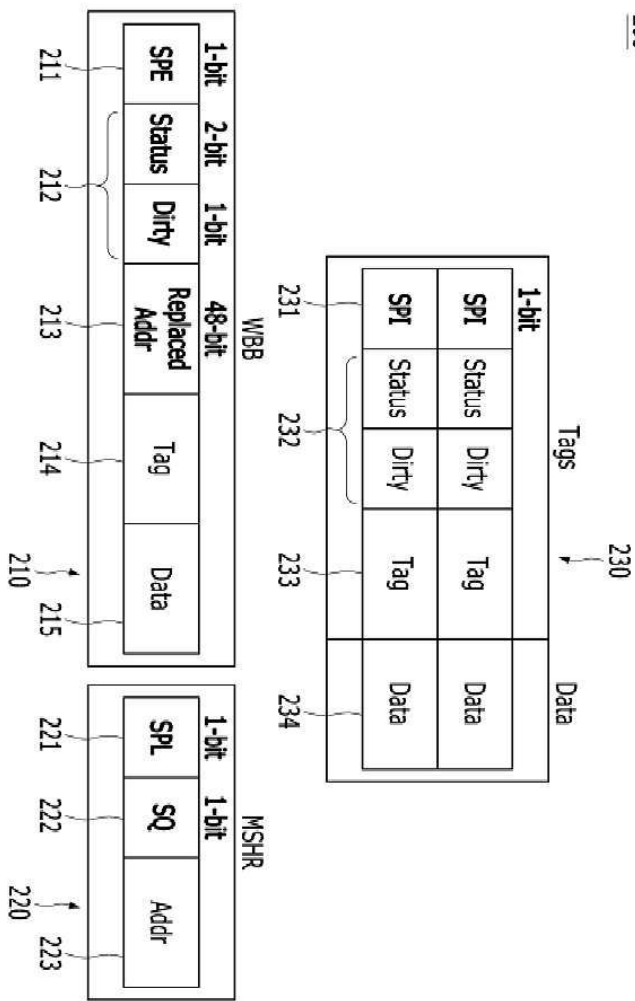
1000



도면2

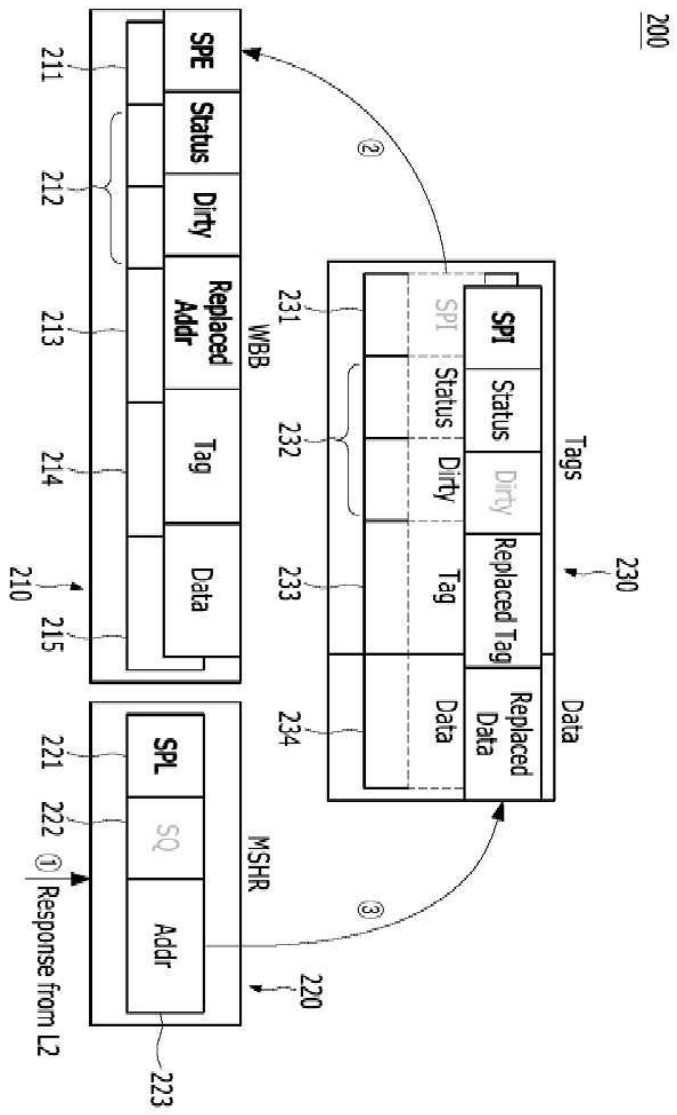


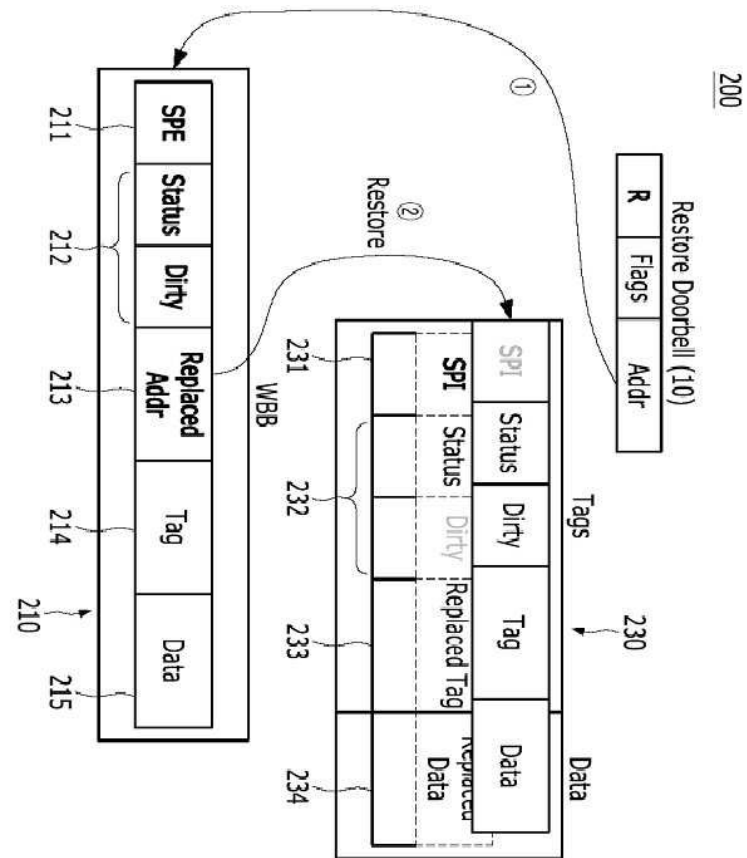
200



도면3

도면4





도면5

