(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년10월16일
(11) 등록번호 10-1451369
(24) 등록일자 2014년10월08일

(51) 국제특허분류(Int. Cl.)
G06F 12/14 (2006.01) *G06F 13/38* (2006.01)
(21) 출원번호 10-2013-7031170
(22) 출원일자(국제) 2012년04월20일
심사청구일자 2013년11월25일
(85) 번역문제출일자 2013년11월25일
(65) 공개번호 10-2013-0136008
(43) 공개일자 2013년12월11일
(86) 국제출원번호 PCT/US2012/034452
(87) 국제공개번호 WO 2012/148812
국제공개일자 2012년11월01일
(30) 우선권주장
61/480,518 2011년04월29일 미국(US)
(56) 선행기술조사문헌
US20110055664 A1
US07706538 B1
전체 청구항 수 : 총 10 항

(73) 특허권자
엘에스아이 코포레이션
미국 캘리포니아 95131, 새너제이, 라이더 파크 드라이브 1320
(72) 발명자
라암, 파보드 마이클
미국 95014 캘리포니아 쿠퍼티노 카스 피엘 10188
(74) 대리인
특허법인 남앤드남

심사관 : 이명진

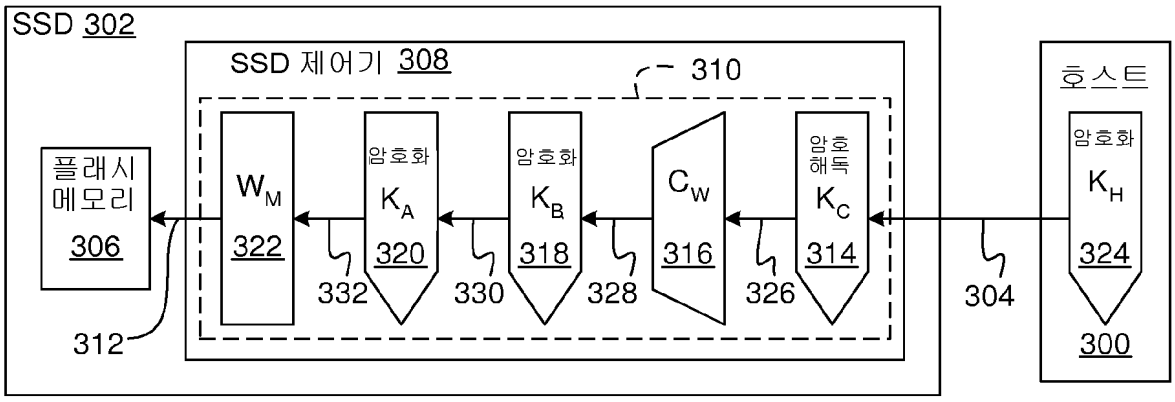
(54) 발명의 명칭 **암호화된 전송 고체 상태 디스크 제어기**

(57) 요 약

암호화된 전송 SSD 제어기는 플래시 메모리와 같은 비휘발성 메모리(NVM)에 압축된(및 옵션으로는 암호화된) 형태로 데이터의 저장을 위해 커맨드들 및 저장 어드레스들을 수신하고, 호스트와 데이터를 교환하는 인터페이스를 갖는다. 호스트로부터 수신된 암호화 데이터는 암호해독되어 플래시 메모리 기록 증폭을 유리하게 감소시키기

(뒷면에 계속)

대 표 도 - 도3a



위해 무손실 압축을 사용하여 압축된다. 압축된 데이터는 재암호화되어 플래시 메모리에 저장된다. 저장된 데이터는 호스트로 전달하기 전에 리트리브되고, 암호해독되고, 압축해제되며, 재암호화된다. 단일 집적 회로와 같은 보안 물리적 경계내에서 구현될 때, SSD 제어기는 호스트로의 전달을 포함하는, 플래시 메모리내의 저장을 통한 수신으로부터 암호화된 데이터를 보호한다. 특정한 실시예들에서, 제어기는 호스트와 세션 암호화/암호해독 키들을 교환하고 그리고/또는 암호화/암호해독 키들을 결정하기 위해 TCG Opal과 같은 보안 프로토콜을 사용한다.

특허청구의 범위

청구항 1

시스템으로서,

호스트로부터 암호화된 데이터 및 저장 어드레스를 수신하는 수단;

상기 수신하는 수단에서 수신된 상기 암호화된 데이터 중 적어도 일부를 암호해독하는 수단;

기록 증폭을 유리하게 감소시키기 위해 상기 암호해독하는 수단의 적어도 일부의 결과들을 압축하는 수단;

상기 압축하는 수단의 적어도 일부 결과들을 암호화하는 수단;

상기 암호화하는 수단의 적어도 일부 결과들을 포맷팅하는 수단;

상기 포맷팅하는 수단의 적어도 일부의 결과들을 상기 저장 어드레스에 따라 하나 또는 그 초과의 비휘발성 메모리(NVM)들에 저장하는 수단을 포함하고, 그리고

상기 수신하는 수단, 상기 암호해독하는 수단, 상기 압축하는 수단, 상기 암호화하는 수단, 및 상기 포맷팅하는 수단은 고체 상태 디스크(SSD)의 제어기에서 적어도 부분적으로 각각 구성되고, 상기 SSD는 상기 NVM들 및 상기 제어기를 포함하는, 시스템.

청구항 2

제 1 항에 있어서,

상기 호스트와 하나 또는 그 초과의 키들을 교환하는 수단을 더 포함하고, 그리고

상기 암호해독하는 수단은 암호화되어 수신된 데이터를 암호해독하기 위해 교환된 상기 키들 중 적어도 일부를 사용하는, 시스템.

청구항 3

제 2 항에 있어서,

상기 암호해독하는 수단, 상기 압축하는 수단, 및 상기 암호화하는 수단은 보안 물리적 경계내에 있는, 시스템.

청구항 4

제 3 항에 있어서,

상기 보안 물리적 경계는 단일 집적 회로를 포함하는, 시스템.

청구항 5

제 3 항에 있어서,

상기 보안 물리적 경계내에 교환된 상기 키들 중 적어도 일부를 세이빙하는 수단을 더 포함하는, 시스템.

청구항 6

제 1 항에 있어서,

상기 압축하는 수단은 무손실 압축을 구현하는, 시스템.

청구항 7

제 1 항에 있어서,

상기 암호화된 데이터는 보안 프로토콜에 따라 암호화되는, 시스템.

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

방법으로서,

호스트로부터 저장 어드레스를 수신하는 단계;

상기 저장 어드레스에 따라 하나 또는 그 초과의 비휘발성 메모리(NVM)들로부터 포맷되고, 암호화되고, 압축된 데이터를 받는(importing) 단계,

받은 데이터 중 적어도 일부를 포맷해제하는(unformatting) 단계;

포맷해제된 데이터 중 적어도 일부를 암호해독하는 단계;

암호해독된 데이터 중 적어도 일부를 압축해제하는 단계;

압축해제된 데이터 중 적어도 일부를 암호화하는 단계; 그리고

암호화된 데이터 중 적어도 일부를 상기 호스트로 보내는(exporting) 단계를 포함하고, 그리고

상기 받는 단계, 상기 포맷해제하는 단계, 상기 암호해독하는 단계, 상기 압축해제하는 단계, 상기 암호화하는 단계, 및 상기 보내는 단계는 각각 적어도 부분적으로 고체 상태 디스크(SSD)의 제어기를 통해 이루어지고, 상기 SSD는 상기 NVM들 및 상기 제어기를 포함하는, 방법.

청구항 14

제 13 항에 있어서,

상기 호스트와 하나 또는 그 초과의 키들을 교환하는 단계를 더 포함하고, 그리고

상기 암호화하는 단계는 상기 압축해제된 데이터를 암호화하기 위해 교환된 상기 키들 중 적어도 일부를 사용하는, 방법.

청구항 15

제 13 항에 있어서,

상기 암호해독하는 단계, 상기 압축해제하는 단계, 및 상기 암호화하는 단계를 보안 물리적 경계내에서 수행하는 단계를 더 포함하는, 방법.

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

명 세 서

기 술 분 야

[0001] 관련 출원들에 대한 상호 참조

[0002] 본 출원에 대한 우선권 이익 주장들은 (만약 있다면, 적절하게) 첨부하는 출원 데이터 시트, 요청서, 또는 송달물에서 이루어진다. 인스턴트 출원(instant application)의 타입에 의해 허용된 범위까지, 본 출원은 모두가 본 발명이 이루어질 때 인스턴트 출원과 일반적으로 소유되는 아래의 출원들을 모두 참조용으로 통합한다:

[0003] 2011년 4월 29일 출원되고, 제 1 발명자 이름이 Farbod Michael Raam이며, Encrypted - Transport Solid - State Disk Controller란 명칭의 미국 가출원 (대리인 사건 번호 SF - 10 - 08 및 출원 번호 61/480,518).

[0004] 분야: 비휘발성 저장 기술에서의 진보들은 사용의 성능, 효율성 및 유용성에서의 개선들을 제공하기 위해 요구된다.

[0005] 종래 기술: 공개적으로 또는 널리 공지된 바와 같이 명백하게 식별되지 않는 한, 컨텍스트, 정의들, 또는 비교 목적을 위해 포함하는 기법들 및 개념들의 여기에서의 언급은 이러한 기법들 및 개념들이 이전에 공개적으로 알려지거나 그렇지 않으면 종래 기술의 일부라는 것을 허용하는 것으로서 해석되어서는 안 된다. 특허들, 특허 출원들, 및 공개물들을 포함하는 (만약 있다면) 여기에 인용된 모든 참조들은 구체적으로 통합되든 또는 안되든 그들의 전부(entirety)들이 모두 인용에 의해 본원에 포함된다.

[0006] 개요

[0007] 본 발명은 예를 들어, 프로세스, 제조물, 장치, 시스템, 물질의 구성물, 및 컴퓨터 판독가능 저장 매체(예를 들어, 디스크와 같은 광 및/또는 자기 대량 저장 디바이스, 또는 플래시 저장부와 같은 비휘발성 저장부를 갖는 집적 회로에서의 매체들), 또는 프로그램 명령어들이 광 또는 전자 통신 링크들을 통해 전송되는 컴퓨터 네트워크와 같은 컴퓨터 판독가능 매체를 포함하는 다수의 방식들로 구현될 수도 있다. 본 명세서에서, 이들 구현들, 또는 본 발명이 택할 수도 있는 임의의 다른 형태가 기법들로서 불릴 수도 있다. 상세한 설명은 상기 식별된 분야에서의 사용의 성능, 효율성, 및 유용성에서의 개선들을 가능하게 하는 본 발명의 하나 또는 그 초과의 실시예들의 설명을 제공한다. 상세한 설명은 나머지 상세한 설명의 더 빠른 이해를 용이하게 하기 위한 도입부를 포함한다. 도입부는 여기에 설명한 개념들에 따른 시스템들, 방법들, 제조물들, 및 컴퓨터 판독가능한 매체들 중 하나 또는 그 초과의 예시적인 실시예들을 포함한다. 결론에서 더 상세히 논의하는 바와 같이, 본 발명은 등록 청구항들의 범위내의 모든 가능한 변경물(modification)들 및 변동물(variation)들을 포함한다.

도면의 간단한 설명

[0008] 도 1a는 비휘발성 메모리(NVM) 소자들(예를 들어, 플래시 메모리들)을 통해 구현되는 것과 같은 비휘발성 저장부를 관리하기 위해 암호화된 전송 기법들을 사용하는 고체 상태 디스크(SSD) 제어기를 포함하는 SSD의 실시예의 선택된 상세들을 예시한다.

도 1b는 도 1a의 SSD의 하나 또는 그 초과의 인스턴스들을 포함하는 시스템들의 다양한 실시예들의 선택된 상세들을 예시한다.

도 2는 도 1a에 예시된 바와 같은 비휘발성 저장부를 관리하기 위해 암호화된 전송 기법들을 사용하는 SSD의 특정한 애플리케이션의 일례를 예시한다.

도 3a는 암호화된 전송 SSD의 기록 데이터 경로 기능(functionality)의 실시예의 선택된 상세를 예시하고, 기록 데이터 경로 기능은 2-스테이지 사후 압축 암호화를 포함한다.

도 3b는 도 3a의 암호화된 전송 SSD의 판독 데이터 경로 기능의 실시예의 선택된 상세를 예시하고, 판독 데이터 경로 기능은 2-스테이지 사전 압축해제 암호해독을 포함한다.

도 4는 예를 들어, 암호화된 전송 SSD의 컨텍스트에서 암호화된 전송 데이터 전달을 수행하는 호스트와 SSD 제어기 사이의 보안 통신 링크의 생성, 사용, 및 폐기의 실시예를 예시하는 흐름도이다.

도 5는 암호화된 전송 SSD 제어기의 데이터 경로 제어 및/또는 동작의 실시예를 예시하는 흐름도이다.

도면들에서 참조 부호들의 리스트

참조 부호	소자 명칭
100	SSD 제어기
101	SSD
102	호스트
103	(옵션) 스위치/구조/중간 제어기
104	중간 인터페이스들
105	OS
106	펌웨어(FW)
107	드라이버
107D	점선 화살표(호스트 소프트웨어 ←→ I/O 디바이스 통신)
109	애플리케이션
109D	점선 화살표(애플리케이션 ←→ 드라이버를 통한 I/O 디바이스 통신)
109V	점선 화살표(애플리케이션 ←→ VF를 통한 I/O 디바이스 통신)
110	외부 인터페이스들
111	호스트 인터페이스들
112C	(옵션) 카드 메모리
113	태그 트랙킹
114	멀티-디바이스 관리 소프트웨어
115	호스트 소프트웨어
116	I/O 카드
117	I/O & 저장 디바이스들/자원들
118	서버들
119	LAN/WAN
121	데이터 프로세싱
123	엔진들
131	버퍼
133	DMA
135	ECC-X
137	메모리
141	맵
143	테이블
151	리사이클러
161	ECC
171	CPU
172	CPU 코어
173	커맨드 관리
175	버퍼 관리
177	트랜슬레이션 관리
179	코히어런시 관리
180	메모리 인터페이스
181	디바이스 관리
182	아이덴티티 관리
190	디바이스 인터페이스들
191	디바이스 인터페이스 로직
192	플래시 디바이스
193	스케줄링
194	플래시 다이
199	NVM
200	암호화된 전송 SSD
202	컴퓨터
204	원격 서버
206	VGA 디스플레이
208	VGA 비디오 신호들
210	VGA 제어기

212	보안 통신 링크(SSD - 원격 서버)
214	플래시 메모리
216	보안 물리적 경계(SSD 제어기)
218	보안 통신 링크(SSD - VGA 제어기)
220	보안 물리적 경계(VGA 제어기)
222	(원격 서버와 컴퓨터 사이의) 커플링
224	(컴퓨터와 SSD 제어기 사이의) 커플링
300	호스트
302	암호화된 전송 SSD
304	암호화된 데이터
306	플래시 메모리
308	SSD 제어기
310	기록 데이터 경로
312	포맷팅되어 암호화된 데이터
314	세션 암호해독 층
316	무손실 압축 층
318	내부 암호화 층
320	백 - 엔드 암호화 층
322	기록 포맷팅 층
326	암호해독된 데이터
328	압축된 데이터
330	압축되어 암호화된 데이터
332	백 - 엔드 암호화된 데이터
336	판독 디포맷팅 층
338	백 - 엔드 암호해독 층
340	내부 암호해독 층
342	판독 압축해제 층
344	세션 암호화 층
346	판독 데이터 경로
401	시작
402	오픈 채널 요청
403	호스트측 인증
404	호스트측 키 교환
405	호스트측 보안 트래픽 교환
405X	호스트측 TCG Ops/저장 액세스
406	클로즈 채널 요청
409	호스트 액션들
412	오픈 채널 수용
413	제어기측 인증
414	제어기측 키 교환
415	제어기측 보안 트래픽 교환
415X	제어기측 TCG Ops/저장 액세스
416	클로즈 채널 수용
417	키 파기
419	제어기 액션들
501	기록 데이터 수신
502	기록 데이터 암호해독
503	암호해독된 데이터 압축
504	압축된 데이터 암호화
505	암호화된 데이터 (재)암호화
506	(재)암호화된 데이터 변조
507	변조된 데이터 저장
508	제어기측으로의 호스트측 보안 트래픽
510	호스트측으로의 제어기측 보안 트래픽

511	암호화된 데이터 제공
512	압축해제된 데이터 암호화
513	(재)암호해독된 데이터 압축해제
514	암호해독된 데이터 암호해독
515	복조된 데이터 암호해독
516	판독된 데이터 복조
517	데이터 판독
522K	키=K_H
524K	키=K_B
525K	키=K_A

발명을 실시하기 위한 구체적인 내용

[0009] 본 발명의 하나 또는 그 초과의 실시예들의 상세한 설명이 본 발명의 선택된 상세들을 예시하는 첨부한 도면들과 함께 아래에 제공된다. 본 발명은 실시예들과 관련하여 설명된다. 여기에서의 실시예들은 단지 예시적인 것으로 이해되고, 본 발명은 여기에서의 실시예들 중 임의의 또는 모든 실시예들에 명백하게 제한되지 않거나 임의의 또는 모든 실시예들에 의해 제한되지 않으며, 본 발명은 다수의 대안물(alternative)들, 변경물들, 및 등가물(equivalent)들을 포함한다. 설명의 단조로움을 회피하기 위해, (제 1, 최종, 특정한, 다양한, 추가의, 다른, 특히, 선택, 일부, 및 현저한을 포함하지만 이에 제한되지 않는) 다양한 단어 라벨(word label)들이 실시예들의 개별 세트들에 적용될 수도 있고, 여기에서 사용되는 바와 같이, 이러한 라벨들은 품질, 또는 임의의 형

태의 우선순위 또는 편견을 전달하는 것으로 명백하게 의미되지 않고, 단지 개별 세트들 사이를 편리하게 구별하는 것으로 의미된다. 개시된 프로세스들의 일부 동작(operation)들의 순서는 본 발명의 범위내에서 변경(alter)가능하다. 다중의 실시예들이 프로세스, 방법 및/또는 프로그램 명령 특징들에서 변동(variation)들을 설명하는 역할을 하여도, 다른 실시예들은 사전결정되거나 동적으로 결정된 기준에 따라 복수의 다중의 실시예들에 각각 대응하는 동작의 복수의 모드들 중 하나의 정적 및/또는 동적 선택을 수행한다는 것이 예상된다. 다수의 특정한 상세들은 본 발명의 완전한 이해를 제공하기 위해 아래의 설명에 설명된다. 상세들은 예시를 위해 제공되고 본 발명은 상세들 중 일부 또는 모두 없이 청구항들에 따라 실시될 수도 있다. 명확화를 위해, 본 발명에 관련된 기술 분야에 공지된 기술적 자료는 본 발명을 불필요하게 모호하게 하지 않기 위해 상세히 설명하지 않는다.

[0010] 도입

[0011] 이 도입부는 오직 상세한 설명의 더 빠른 이해를 용이하게 하기 위해 포함되고, 임의의 도입부의 단락들이 반드시 전체 주제의 축약된 관점이고 배타적이거나 제한적인 설명인 것으로 의미되지 않기 때문에 본 발명은 (만약 있다면, 명시적인 예들을 포함하는) 도입부에 제공되는 개념들에 제한되지 않는다. 예를 들어, 다음의 도입부는 오직 특정한 실시예들에 대해 공간 및 구성에 의해 제한된 개요 정보를 제공한다. 청구항들이 명세서의 나머지 전반적으로 궁극적으로 도시되고 논의되는 것들을 포함하는, 많은 다른 실시예들이 있다.

[0012] 약어들

[0013] 여기에 정의된 다양한 축약된 두문자어들(예를 들어, 약어들)의 적어도 일부가 여기에 사용된 특정한 소자들을 지칭한다.

약어	설명
AES	어드밴스드 암호화 표준
AHCI	어드밴스드 호스트 제어기 인터페이스
API	애플리케이션 프로그램 인터페이스
ASCII	정보 교환을 위한 미국 표준 코드
BCH	Bose Chaudhuri Hocquenghem
ATA	어드밴스드 기술 부착(AT 부착)
CD	콤팩트 디스크
CF	콤팩트 플래시
CMOS	상보적 금속 산화물 반도체
CPU	중앙 처리 장치
CRC	사이클릭 리던던시 체크
DAS	직접 부착 저장부
DDR	더블 데이터 레이트
DES	데이터 암호화 표준
DMA	직접 메모리 액세스
DNA	직접 NAND 액세스
DRAM	동적 랜덤 액세스 메모리
DVD	디지털 다기능/비디오 디스크
DVR	디지털 비디오 리코더
ECC	에러 정정 코드
eMMC	내장형 멀티미디어카드
eSATA	외부 직렬 어드밴스드 기술 부착
GPS	글로벌 포지셔닝 시스템
HDD	하드 디스크 드라이브
I/O	입/출력
IC	집적 회로
IDE	집적 드라이브 전자장치
JPEG	제이펙그(Joint Photographic Experts Group)
LAN	로컬 영역 네트워크
LB	논리 블록
LBA	논리 블록 어드레스
LDPC	저밀도 패리티 체크
LPN	논리 페이지 번호
LZ	Lempel - Ziv
MLC	멀티 레벨 셀
MMC	멀티미디어카드
MPEG	동영상 전문가 그룹
NAS	네트워크 부착 저장부
NCQ	네이티브 커맨드 큐잉
NVM	비휘발성 메모리
ONA	최적화된 NAND 액세스
ONFI	오픈 NAND 플래시 인터페이스
OS	운영 시스템
PC	개인 컴퓨터
PCIe	주변 컴포넌트 상호접속 익스프레스 (PCI 익스프레스)
PDA	휴대 정보 단말기
POS	판매 시점 정보 관리
RAID	저가/독립 디스크들의 리던던트 어레이
RS	리드 솔로몬
RSA	Rivest, Shamir & Adleman
SAN	저장부 부착 네트워크
SAS	직렬 부착 소형 컴퓨터 시스템 인터페이스 (직렬 SCSI)
SATA	직렬 어드밴스드 기술 부착 (직렬 ATA)

[0014]

SCSI	소형 컴퓨터 시스템 인터페이스
SD	보안 디지털
SDR	단일 데이터 레이트
SLC	단일 레벨 셀
SMART	셀프 모니터링 분석 및 리포팅 기술
SSD	고체 상태 디스크/드라이브
TCG	신뢰 컴퓨팅 그룹
UFS	단일화된 플래시 저장부
USB	범용 직렬 버스
VF	가상 함수
WAN	광역 네트워크

[0015]

[0016] 일부 저장 주변장치들은 호스트로부터 저장 주변장치에 송신된 데이터를 보호하기 위해 전송 암호화층을 사용하도록 인에이블된다. 호스트는 저장 매체(예를 들어, NVM)에 저장될 데이터를 저장 주변장치에 송신하기 전에 내부적으로 데이터를 암호화한다. 유사하게는, 저장 주변장치로부터 판독되고 호스트에 송신된 데이터는 그 데이터가 기록될 때와 동일한 암호화를 갖는 것으로 가정되고, 호스트는 사용을 위해 데이터를 암호해독한다. 호스트의 관점에서, 데이터는 저장 매체로 및 저장 매체로부터의 전체 경로상에서 암호화된다.

[0017] 일부 실시예들에서, SSD들과 같은 저장 주변장치들은 (NAND 플래시 칩들의 어레이와 같은) 저장 매체에 데이터를 저장하기 전에 소위 "백-엔드(back-end)" 암호화를 통해 데이터를 내부적으로 암호화하고, 저장 매체로부터 암호화된 데이터를 판독한 후에 데이터를 암호해독한다. SSD들에서, 백-엔드 암호화는 데이터를 보호하고, 일부 시나리오들에서는 NAND 플래시 칩들의 내구성을 개선시키는 스크램블링 특성을 제공하는 역할을 한다. 예를 들어, 백-엔드 암호화는 호스트 데이터에 대해 사용된 암호화의 임의의 다른 형태들과 독립적으로, 저장 매체에 저장되는 SSD의 펌웨어를 보호하기 위해 사용된다.

[0018] 일부 저장 주변장치들은 저장 보안 서브-시스템 클래스(예를 들어, TCG Opal)와 같은 보안 프로토콜에 따라 동작하고, 호스트로부터 수신되고 저장 매체에 기록될 데이터를 암호화하도록 인에이블되고, 저장 매체로부터 판독된 데이터를 암호해독하도록 더 인에이블된다. 일부 실시예들에서, 보안 프로토콜 암호화/암호해독은 암호화/암호해독 키를 부분적으로 결정하기 위해 저장 어드레스 범위와 같은 메타-데이터를 사용한다. 추가의 실시예들에서, 각각의 키와 각각 연관된 하나 또는 그 초과의 어드레스 범위들이 있다. 추가의 실시예들에서, 매칭되는 어드레스 범위들이 없다면 글로벌 "상기 중 어느 것도 아님(none of the above)" 키가 존재한다. 다양한 실시예들에 따르면, 보안 프로토콜 암호화/암호해독은 전송 암호화/암호해독과 동일한 것, 전송 암호화/암호해독과 상이한 것, 백-엔드 암호화/암호해독과 동일한 것, 및 백-엔드 암호화/암호해독과 상이한 것 중 하나 또는 그 초과이다.

[0019] 일부 실시예들에서, SSD들과 같은 저장 주변장치들은 (NAND 플래시 칩들의 어레이와 같은) 저장 매체에 데이터를 저장하기 전에 호스트로부터 수신된 데이터를 압축한다. 압축은 데이터 타입(예를 들어, JPEG 및/또는 MPEG 데이터)에 기초한 손실 있는 압축, 로컬화된 방식(예를 들어, LZ 압축)으로 수행된 무손실 압축, 데이터 중복제거, 및 압축된 데이터를 표현하기 위해 요구되는 저장부를 감소키는 임의의 가역 변환 중 하나 또는 그 초과를 포함한다. 저장 전에 데이터를 압축하는 것은 유리하게는 다양한 시나리오들에서 기록-증폭을 감소시키고 그리고/또는 표면상의(apparent) 저장 용량을 증가시킨다. 그러나, (예를 들어, 전송 암호화를 위해) 암호화된 데이터는 일부 시나리오들에서, 압축가능하지 않다.

[0020] 일부 실시예들에서, SSD와 같은 저장 주변장치는 전송 암호화 층에 대해 사용된 키(들)를 결정하기 위해 호스트와 키 교환을 수행하고, 옵션으로 및/또는 선택적으로 각 키가 어느 조건들하에서 사용되는지를 결정한다. 저장 주변장치가 호스트로부터 암호화된 전송 데이터를 수신할 때, 저장 주변장치는 전송 암호화에 따라 데이터를 암호해독하기 위해 키(들) 중 선택된 하나를 옵션으로 및/또는 선택적으로 사용한다. 이후, 암호해독된 데이터가 압축된다. TCG Opal과 같은 보안 프로토콜이 사용되는 추가의 실시예들에서, 압축된 데이터는 보안 프로토콜에 따라 옵션으로 및/또는 선택적으로 암호화된다. 보안 프로토콜과는 상이한 백-엔드 암호화가 있는 더 추가의 실시예들에서, 압축되고 옵션으로 및/또는 선택적으로 암호화된 데이터는 데이터가 저장 매체에 기록하기 위해 변조되기 전에 백-엔드 암호화에 의해 더 암호화된다.

[0021] 다른 실시예들에서, 전송 암호화는 TCG Opal보다는 재사용된다. 즉, 압축 후에, 압축된 데이터는 전송 암호화 키(들)/알고리즘을 사용하여 재암호화된다.

[0022] 데이터가 저장 매체로부터 역으로(back) 판독되고 호스트에 복귀(return)될 때, 데이터를 저장하는 상술한 동작

들은 원래의 암호화된 데이터가 호스트에 복귀되도록 유효하게 반전된다.

[0023] 암호화 알고리즘들의 예가 DES, 트리플(triple)-DES, AES-128, AES-256, RSA, 및 다른 공중 키 암호화 알고리즘들이다.

[0024] 일부 상황들에서, 기록 증폭(write amplification)은 특정한 사이즈의 호스트 저장 기록이 SSD의 플래시 메모리에 대해 (예를 들어, 다중의 특정한 사이즈의 사이즈를 각각 갖는) 복수의 기록들을 발생시킬 때 발생한다. 복수의 기록들은 예를 들어, 플래시 메모리의 일부의 기록(예를 들어, 프로그래밍) 전의 그 일부의 소거, 마모 레벨링, 가비지 회수(garbage collection), 및 시스템 데이터 기록들을 발생시키는 플래시 메모리 관리 동작들로부터 발생한다. 기록 증폭의 예시적인 계산이 호스트 기록들의 특정한 수집(collection)에 의해 기록된 데이터량에 의해 분할된, (예를 들어 호스트 기록들과 연관된 호스트 데이터의 기록을 완료하기 위한 시스템 기록들을 포함하는) 호스트 기록들의 특정한 수집 대신에 플래시 메모리에 기록된 데이터량이다. 일부 사용 시나리오들에서, 호스트 기록들의 특정한 수집에 의해 기록된 데이터의 압축은 호스트 기록들의 특정한 수집 대신에 플래시 메모리에 기록된 데이터량의 감소를 가능하게 한다. 호스트 기록들의 특정한 수집 대신에 플래시 메모리에 기록된 데이터량이 감소되기 때문에, 그에 따라 기록 증폭이 감소된다.

[0025] 일부 실시예들에서, NVM에서의 가변(varying) 사이즈 정량들의 압축된 데이터에 액세스하는 것은 일부 사용 시나리오들에서 개선된 저장 효율을 제공한다. 예를 들어, SSD 제어기는 (예를 들어, 디스크 기록 커맨드에 관하여) 컴퓨팅 호스트로부터 (압축되지 않은) 데이터를 수신하고, 데이터를 압축하며, 압축된 데이터를 플래시 메모리에 저장한다. (예를 들어, 디스크 판독 커맨드에 관한) 컴퓨팅 호스트로부터의 후속 요청에 응답하여, SSD 제어기는 플래시 메모리로부터의 압축된 데이터를 판독하고, 압축된 데이터를 압축해제하여, 압축해제된 데이터를 컴퓨팅 호스트에 제공한다. 압축된 데이터는 가변 사이즈 정량들에 따라 플래시 메모리에 저장되고, 정량 사이즈는 예를 들어, 압축 알고리즘, 동작 모드, 및 다양한 데이터에 대한 압축 유효성으로 인해 변한다. SSD 제어기는 헤더(들)가 플래시 메모리에서 어디에 저장되는지를 결정하기 위해 포함된 맵 테이블을 컨설팅함으로써 부분적으로 데이터를 압축해제한다. SSD 제어기는 적절한 (압축된) 데이터가 플래시 메모리에서 어디에 저장되는지를 결정하기 위해 플래시 메모리로부터 획득된 헤더(들)를 분석한다. SSD 제어기는 압축해제된 데이터를 생성하여 컴퓨팅 호스트에 제공하기 위해 플래시 메모리로부터의 적절한 데이터를 압축해제한다.

[0026] 다양한 실시예들에서, SSD 제어기는 컴퓨팅 호스트와 인터페이스하기 위한 호스트 인터페이스, 플래시 메모리와 같은 NVM와 인터페이스하기 위한 인터페이스, 및 인터페이스들을 제어하고 압축 및 압축해제를 수행(및/또는 그 수행의 다양한 양태들을 제어)하기 위한 회로뿐만 아니라 독립 실리콘 소자들을 갖는 하위 레벨 에러 정정, 상위 레벨 에러 정정, 및 동적 상위 레벨 리던던시 모드 관리를 포함한다.

[0027] 다양한 실시예들에 따르면, 일부 호스트 인터페이스들은 USB 인터페이스 표준, CF 인터페이스 표준, MMC 인터페이스 표준, eMMC 인터페이스 표준, 썬더볼트 인터페이스 표준, UFS 인터페이스 표준, SD 인터페이스 표준, 메모리 스틱 인터페이스 표준, xD-픽처 카드 인터페이스 표준, IDE 인터페이스 표준, SATA 인터페이스 표준, SCSI 인터페이스 표준, SAS 인터페이스 표준, 및 PCIe 인터페이스 표준 중 하나 또는 그 초과와 호환가능하다. 다양한 실시예들에 따르면, 컴퓨팅 호스트는 컴퓨터, 워크스테이션 컴퓨터, 서버 컴퓨터, 저장 서버, SAN, NAS 디바이스, DSA 디바이스, 저장 기구, PC, 랩탑 컴퓨터, 노트북 컴퓨터, 넷북 컴퓨터, 태블릿 디바이스 또는 컴퓨터, 울트라북 컴퓨터, (e-판독기와 같은) 전자 판독 디바이스, PDA, 네비게이션 시스템, (핸드헬드) GPS 디바이스, 자동 제어 시스템, 자동 미디어 제어 시스템 또는 컴퓨터, 프린터, 복사기 또는 팩스 머신 또는 일체형(all-in-one) 디바이스, POS 디바이스, 캐시-레지스터, 미디어 플레이어, 텔레비전, 미디어 리코더, DVR, 디지털 카메라, 셀룰러 핸드셋, 코드리스 전화 핸드셋, 및 전자 게임 중 모두 또는 임의의 부분들이다. 일부 실시예들에서, (SAS/SATA 브리지와 같은) 인터페이싱 호스트는 컴퓨팅 호스트 및/또는 컴퓨팅 호스트에 대한 브리지로서 동작한다.

[0028] 다양한 실시예들에서, SSD 제어기는 하나 또는 그 초과의 프로세서들을 포함한다. 프로세서들은 SSD 제어기의 동작을 제어 및/또는 수행하기 위해 펌웨어를 실행한다. SSD 제어기는 커맨드들 및/또는 상태뿐만 아니라 데이터를 전송 및 수신하기 위해 컴퓨팅 호스트와 통신한다. 컴퓨팅 호스트는 운영(operating) 시스템, 드라이버, 및 애플리케이션 중 하나 또는 그 초과를 실행한다. 컴퓨팅 호스트에 의한 SSD 제어기와의 통신은 옵션으로 및/또는 선택적으로 드라이버 및/또는 애플리케이션을 통한다. 제 1 예에서, SSD 제어기로의 모든 통신은 드라이버를 통하고, 애플리케이션은 드라이버가 SSD 제어기에 대한 특정한 커맨드들로 트랜슬레이션하는 상위 레벨 커맨드들을 드라이버에 제공한다. 제 2 예에서, 드라이버는 바이패스 모드를 구현하고, 애플리케이션은 드라이버를 통해 특정한 커맨드들을 SSD 제어기에 전송하도록 인에이블된다(enabled). 제 3 예에서, PCIe SSD 제어기는

하나 또는 그 초과의 가상 함수(VF)들을 지원하고, 일단 구성되면, 애플리케이션이 드라이버를 바이패스하여 SSD 제어기와 직접 통신하게 할 수 있다.

[0029] 다양한 실시예들에 따르면, 일부 SSD들은 HDD들, CD 드라이브들, 및 DVD 드라이브들과 같은 자기 및/또는 광 비휘발성 저장부에 의해 사용된 폼-팩터들, 전기적 인터페이스들, 및/또는 프로토콜들과 호환가능하다. 다양한 실시예들에서, SSD들은 제로 또는 그 초과의 패리티 코드들, 제로 또는 그 초과의 RS 코드들, 제로 또는 그 초과의 BCH 코드들, 제로 또는 그 초과의 비터비 또는 다른 트렐리스 코드들, 및 제로 또는 그 초과의 LDPC 코드들의 다양한 조합(combination)들을 사용한다.

[0030] 예시적인 실시예들

[0031] 결론에서, "EC"들(예시적인 조합들)로서 명시적으로 열거되는 적어도 일부를 포함하는 예시적인 실시예들의 집합이 따르는 상세한 설명에 대한 도입은 여기에 설명한 개념들에 따른 다양한 실시예 타입들의 부가의 설명을 제공하고, 이들 예들은 상호 배타적이고, 포괄적이거나, 제한적인 것으로 의미되지 않고, 본 발명은 이들 예시적인 실시예들에 제한되는 것이 아니라, 오히려 등록 청구항들의 범위내의 모든 가능한 변경물들 및 변동물들, 및 그들의 등가물들을 포함한다.

[0032] EC1) 방법으로서,

[0033] 하나 또는 그 초과의 비휘발성 메모리(NVM)들로부터 데이터를 수신하는 단계;

[0034] 수신된 데이터를 준비하는 단계;

[0035] 준비된 데이터를 동작들의 시퀀스에 따라 프로세싱하는 단계;

[0036] 프로세싱의 결과를 컴퓨팅 호스트에 제공하는 단계를 포함하고,

[0037] 동작들의 시퀀스는,

[0038] 준비된 데이터를 암호해독하는 것,

[0039] 암호해독된 데이터를 압축해제하는 것,

[0040] 압축해제된 데이터를 재암호화하는 것, 그리고

[0041] 재암호화된 데이터를 결과로서 제공하는 것을 포함하고, 그리고

[0042] 압축해제하는 것은 무손실 압축하는 것에 대해 대칭인, 방법.

[0043] EC2) EC1에 있어서, 암호해독은 제 1 암호해독이고, 준비하는 단계는 제 2 암호해독하는 것을 포함하는, 방법.

[0044] EC3) EC1에 있어서, 프로세싱하는 단계는 복수의 모드들 중 선택된 모드에 따라 선택적이고, 동작들의 시퀀스는 모드들 중 제 1 모드에 대응하는 동작들의 제 1 시퀀스인, 방법.

[0045] EC4) EC3에 있어서,

[0046] 동작들의 제 2 시퀀스가 모드들 중 제 2 모드에 대응하고, 그리고

[0047] 동작들의 제 2 시퀀스는,

[0048] 압축해제된 데이터를 결과로서 제공하는 것을 포함하는, 방법.

[0049] EC5) 방법으로서,

[0050] 컴퓨팅 호스트로부터 데이터를 수신하는 단계;

[0051] 수신된 데이터를 동작들의 시퀀스에 따라 프로세싱하는 단계;

[0052] 하나 또는 그 초과의 비휘발성 메모리(NVM)들에서의 저장을 가능하게 하기 위해 프로세싱의 결과를 준비하는 단계를 포함하고,

[0053] 동작들의 시퀀스는,

[0054] 수신된 데이터를 암호해독하는 것,

[0055] 암호해독된 데이터를 압축하는 것,

[0056] 압축된 데이터를 재암호화하는 것, 그리고

[0057] 재암호화된 데이터를 결과로서 제공하는 것을 포함하고, 그리고

[0058] 압축은 무손실인, 방법.

[0059] EC6) EC5에 있어서, 준비하는 단계는 암호화하는 단계를 포함하는, 방법.

[0060] EC7) EC5에 있어서, 프로세싱하는 단계는 복수의 모드들 중 선택된 모드에 따라 선택적이고, 동작들의 시퀀스는 모드들 중 제 1 모드에 대응하는 동작들의 제 1 시퀀스인, 방법.

[0061] EC8) EC7에 있어서,

[0062] 동작들의 제 2 시퀀스가 모드들 중 제 2 모드에 대응하고, 그리고

[0063] 동작들의 제 2 시퀀스는,

[0064] 압축된 데이터를 결과로서 제공하는 것을 포함하는, 방법.

[0065] EC9) 방법으로서,

[0066] 하나 또는 그 초과의 비휘발성 메모리(NVM)들로부터 데이터를 수신하는 단계;

[0067] 수신된 데이터를 준비하는 단계;

[0068] 준비된 데이터를 복수의 모드들 중 선택된 모드에 따라 프로세싱하는 단계;

[0069] 프로세싱의 결과를 컴퓨팅 호스트에 제공하는 단계를 포함하고,

[0070] 모드들 중 제 1 모드가,

[0071] 준비된 데이터를 암호화하는 것,

[0072] 암호해독된 데이터를 제 1 압축해제된 데이터로서 압축해제하는 것,

[0073] 제 1 압축해제된 데이터를 제 1 재암호화된 데이터로서 재암호화하는 것, 그리고

[0074] 제 1 재암호화된 데이터를 결과로서 제공하는 것을 포함하고, 그리고

[0075] 모드들 중 제 2 모드가,

[0076] 준비된 데이터를 제 2 압축해제된 데이터로서 압축해제하는 것,

[0077] 제 2 압축해제된 데이터를 제 2 재암호화된 데이터로서 재암호화하는 것, 그리고

[0078] 제 2 재암호화된 데이터를 결과로서 제공하는 것을 포함하는, 방법.

[0079] EC10) EC9에 있어서, 준비하는 단계는 암호해독하는 단계를 포함하는, 방법.

[0080] EC11) EC9에 있어서, 압축해제하는 것은 무손실 압축하는 것에 대해 대칭인, 방법.

[0081] EC12) EC9에 있어서,

[0082] 모드들 중 제 3 모드가,

[0083] 제 1 압축해제된 데이터를 결과로서 제공하는 것을 포함하는, 방법.

[0084] EC13) 방법으로서,

[0085] 컴퓨팅 호스트로부터 데이터를 수신하는 단계;

[0086] 수신된 데이터를 복수의 모드들 중 선택된 모드에 따라 프로세싱하는 단계;

[0087] 하나 또는 그 초과의 비휘발성 메모리(NVM)들에서의 저장을 가능하게 하기 위해 프로세싱의 결과를 준비하는 단계를 포함하고,

[0088] 모드들 중 제 1 모드가,

[0089] 수신된 데이터를 암호해독하는 것,

[0090] 암호해독된 데이터를 압축하는 것,

[0091] 암호해독되어 압축된 데이터를 재암호화하는 것, 그리고

[0092] 재암호화된 데이터를 결과로서 제공하는 것을 포함하고, 그리고

[0093] 모드들 중 제 2 모드가,

[0094] 암호해독되어 압축된 데이터를 결과로서 제공하는 것을 포함하는, 방법.

[0095] EC14) EC13에 있어서, 준비하는 단계는 암호화하는 단계를 포함하는, 방법.

[0096] EC15) EC13에 있어서, 재암호화하는 것은 암호해독하는 것에 대해 대칭인, 방법.

[0097] EC16) EC13에 있어서, 재암호화하는 것은 보안 프로토콜에 따르고, 암호해독하는 것은 전송 프로토콜에 따르는, 방법.

[0098] EC17) EC13에 있어서, 컴퓨팅 호스트와 전송 세션 암호화 키들을 안전하게 교환하고, 암호해독하는데 있어서 전송 세션 암호화 키들 중 적어도 일부를 사용하는 단계를 더 포함하는, 방법.

[0099] EC18) EC17에 있어서, 전송 세션 암호화 키들을 안전하게 교환하는 단계는,

[0100] 비대칭 키 교환을 사용하여 컴퓨팅 호스트와 고체 상태 디스크(SSD) 사이에 보안 링크를 확립하는 단계, 그리고

[0101] 보안 링크내에서 전송 세션 암호화 키들을 교환하는 단계를 포함하는, 방법.

[0102] EC19) EC13에 있어서,

[0103] 모드들 중 제 3 모드가,

[0104] 수신된 데이터를 압축하는 것,

[0105] 압축된 데이터를 암호화하는 것, 그리고

[0106] 압축되어 암호화된 데이터를 결과로서 제공하는 것을 포함하는, 방법.

[0107] EC20) EC19에 있어서, 암호화하는 것은 보안 프로토콜에 따르는, 방법.

[0108] EC21) EC19에 있어서,

[0109] 모드들 중 제 4 모드가,

[0110] 압축된 데이터를 결과로서 제공하는 것을 포함하는, 방법.

[0111] EC22) EC13에 있어서, 준비하는 단계는 결과를 스크램블링하고 그리고/또는 변조하는 단계를 포함하는, 방법.

[0112] EC23) EC13에 있어서, 준비하는 단계는 암호화하는 단계를 포함하는, 방법.

[0113] EC24) EC13에 있어서, 저장하는 단계를 더 포함하는, 방법.

[0114] EC25) EC24에 있어서, 저장하는 단계는 플래시 메모리 인터페이스를 통하는, 방법.

[0115] EC26) EC13에 있어서, 수신하는 단계는 저장 인터페이스 표준과 호환가능한 저장 인터페이스를 통하는, 방법.

[0116] EC27) EC13에 있어서, 컴퓨팅 호스트를 통해 암호화된 데이터로서 데이터를 제공하는 단계를 더 포함하는, 방법.

[0117] EC28) EC13에 있어서, 암호해독하는 것, 압축하는 것, 및 재암호화하는 것은 고체 상태 디스크(SSD)의 제어기를 통해 적어도 부분적으로 구현되는, 방법.

[0118] EC29) 시스템으로서,

[0119] 컴퓨팅 호스트로부터 데이터를 수신하는 수단;

[0120] 수신된 데이터를 암호해독하는 수단,

[0121] 암호해독된 데이터를 압축하는 수단,

[0122] 암호해독되어 압축된 데이터를 재암호화하는 수단, 그리고

[0123] 재암호화된 데이터를 암호화된 모드 기록 데이터로서 제공하는 수단

[0124] 을 통해 적어도 부분적으로 구현된 동작의 암호화된 모드, 그리고

[0125] 수신된 데이터를 압축하는 수단, 그리고

[0126] 수신되어 압축된 데이터를 비암호화된 모드 기록 데이터로서 제공하는 수단

[0127] 을 통해 적어도 부분적으로 구현된 동작의 비암호화된 모드

[0128] 를 포함하는 동작의 복수의 모드들 중 하나를 선택적으로 인에이블하는 수단;

[0129] 인에이블된 모드 기록 데이터를 선택하는 수단;

[0130] 선택된 모드 기록 데이터를 암호화하는 수단; 그리고

[0131] 하나 또는 그 초과의 비휘발성 메모리(NVM)들에 저장을 위해 선택되어 암호화된 모드 기록 데이터를 포맷팅하는 수단을 포함하는, 시스템.

[0132] EC30) EC29에 있어서, 전송 세션 암호화 키들을 안전하게 교환하고, 수신된 데이터를 암호화되어 수신된 데이터로서 암호해독하기 위해 전송 세션 암호화 키들 중 적어도 일부를 사용하는 수단을 더 포함하는, 시스템.

[0133] EC31) EC29에 있어서, 압축하는 수단 중 하나 또는 그 초과는 기록 증폭을 유리하게 감소시키기 위해 무손실 압축을 수행하도록 인에이블되는, 시스템.

[0134] EC32) EC29에 있어서, 암호해독된 데이터를 압축하는 수단 및 수신된 데이터를 압축하는 수단은 적어도 일부를 공통으로 갖는, 시스템.

[0135] EC33) EC29에 있어서, 수단들은 고체 상태 디스크(SSD)의 제어기를 통하고, NVM들은 SSD에서 구성된 플래시 메모리들인, 시스템.

[0136] EC34) EC33에 있어서, 제어기를 컴퓨팅 호스트와 인터페이싱하는 수단을 더 포함하는, 시스템.

[0137] EC35) EC34에 있어서, 인터페이싱하는 수단은 저장 인터페이스 표준과 호환가능한, 시스템.

[0138] EC36) EC34에 있어서, 컴퓨팅 호스트의 모두 또는 임의의 부분들을 더 포함하는, 시스템.

[0139] EC37) EC29에 있어서, NVM들과 인터페이싱하는 수단을 더 포함하는, 시스템.

[0140] EC38) EC37에 있어서, 인터페이싱하는 수단은 플래시 메모리 인터페이스를 포함하는, 시스템.

[0141] EC39) EC29에 있어서, NVM들 중 적어도 하나를 더 포함하는, 시스템.

[0142] EC40) EC29에 있어서,

[0143] 컴퓨팅 호스트로부터의 요청들과 인터페이싱하는 수단으로서, 이 요청들은 NVM들에 저장된 정보에 관련되는, 컴퓨팅 호스트로부터의 요청들과 인터페이싱하는 수단; 그리고

[0144] NVM들에 인터페이싱하는 수단을 더 포함하는, 시스템.

[0145] EC41) EC40에 있어서, 수단들은 단일 집적 회로(IC)에서 일괄적으로 구현되는, 시스템.

[0146] EC42) EC40에 있어서, 수단들은 고체 상태 디스크(SSD)에서 구성되는, 시스템.

[0147] EC43) EC30에 있어서, 전송 세션 암호화 키들을 안전하게 교환하는 수단은,

[0148] 비대칭 키 교환을 사용하여 호스트와 고체 상태 디스크(SSD) 사이에 보안 링크를 확립하는 수단, 그리고

[0149] 보안 링크내에서 전송 세션 암호화 키들을 교환하는 수단을 포함하는, 시스템.

[0150] EC44) 저장 디바이스의 프로세싱 소자에 의해 실행될 때, 프로세싱 소자로 하여금, 하기의 동작들을 수행 및/또는 제어하게 하는 명령어들의 세트가 저장된 유형의 컴퓨터 판독가능 매체로서, 상기 동작들은,

[0151] 컴퓨팅 호스트로부터 데이터를 수신하고;

[0152] 수신된 데이터를 암호해독하며,

[0153] 암호해독된 데이터를 압축하고,

[0154] 암호해독되어 압축된 데이터를 재암호화하며, 그리고

[0155] 재암호화된 데이터를 암호화된 모드 기록 데이터로서 제공하는 것

[0156] 을 통해 적어도 부분적으로 구현된 동작의 암호화된 모드, 그리고

[0157] 수신된 데이터를 압축하고, 그리고

[0158] 수신되어 압축된 데이터를 비암호화된 모드 기록 데이터로서 제공하는 것

[0159] 을 통해 적어도 부분적으로 구현된 동작의 비암호화된 모드

[0160] 를 포함하는 동작의 복수의 모드들 중 하나를 선택적으로 인에이블하고;

[0161] 인에이블된 모드 기록 데이터를 선택하며;

[0162] 선택된 모드 기록 데이터를 암호화하고; 그리고

[0163] 하나 또는 그 초과의 비휘발성 메모리(NVM)들에 저장을 위해 선택되어 암호화된 모드 기록 데이터를 포맷팅하는 것을 포함하는, 유형의 컴퓨터 판독가능 매체.

[0164] EC45) EC44에 있어서, 유형의 컴퓨터 판독가능 매체 및 프로세싱 소자는 고체 상태 디스크(SSD)에서 구성되는, 유형의 컴퓨터 판독가능 매체.

[0165] EC46) EC45에 있어서, NVM들 중 적어도 하나는 SSD에서 구성되는, 유형의 컴퓨터 판독가능 매체.

[0166] EC47) 암호해독 및 재암호화를 갖거나 참조하는 임의의 상술한 EC들로서, 암호해독 및 재암호화 중 어느 하나 또는 그 초과는 보안 물리적 경계내에서 수행되는, EC들.

[0167] EC48) 암호해독, 재암호화, 압축, 및 압축해제를 갖거나 참조하는 임의의 상술한 EC들로서, 암호해독, 재암호화, 압축, 및 압축해제 중 어느 하나 또는 그 초과는 보안 물리적 경계내에서 수행되는, EC들.

[0168] EC49) 보안 물리적 경계를 갖거나 참조하는 임의의 상술한 EC들로서, 보안 물리적 경계는 단일 집적 회로(IC)를 통해 구현되는, EC들.

[0169] EC50) 전송 세션 암호화 키들을 갖거나 참조하는 임의의 상술한 EC들로서, 전송 세션 암호화 키들은 대칭 키 암호화/암호해독과 호환가능한, EC들.

[0170] EC51) 대칭 키 암호화/암호해독을 갖거나 참조하는 임의의 상술한 EC들로서, 대칭 키 암호화/암호해독은,

[0171] AES 128,

[0172] AES 192, 그리고

[0173] AES 256 중 하나 또는 그 초과와 호환가능한, EC들.

[0174] EC52) 무손실 압축을 갖거나 참조하는 임의의 상술한 EC들로서, 무손실 압축은 렘펠-지프(Lempel-Ziv: LZ) 압축을 포함하는, EC들.

[0175] EC53) 무손실 압축을 갖거나 참조하는 임의의 상술한 EC들로서, 무손실 압축은 사전 코더(dictionary coder) LZ77 압축을 포함하는, EC들.

[0176] EC54) SSD 제어기를 갖거나 참조하는 임의의 상술한 EC들로서, SSD 제어기는 단일 집적 회로(IC)에서 구현되는, EC들.

[0177] EC55) SSD 제어기 및 NVM들을 갖거나 참조하는 임의의 상술한 EC들로서, SSD 제어기 및 NVM들은 SSD에서 구성되는, EC들.

[0178] EC56) NVM들을 갖거나 참조하는 임의의 상술한 EC들로서, NVM들 중 적어도 하나는 하나 또는 그 초과의 플래시 메모리들을 포함하는, EC들.

[0179] EC57) 저장 인터페이스 표준을 갖거나 참조하는 임의의 상술한 EC들로서, 저장 인터페이스 표준은,

[0180] 범용 직렬 버스(USB) 인터페이스 표준,

[0181] 콤팩트 플래시(CF) 인터페이스 표준,

[0182] 멀티미디어카드(MMC) 인터페이스 표준,

[0183] 내장형 MMC(eMMC) 인터페이스 표준,

[0184] 썬더볼트 인터페이스 표준,

[0185] UFS 인터페이스 표준,

[0186] 보안 디지털(SD) 인터페이스 표준,

[0187] 메모리 스틱 인터페이스 표준,

[0188] xD-픽처 카드 인터페이스 표준,

[0189] 집적 드라이브 전자장치(IDE) 인터페이스 표준,

[0190] 직렬 어드밴스드 기술 부착(SATA) 인터페이스 표준,

[0191] 외부 SATA(eSATA) 인터페이스 표준,

[0192] 소형 컴퓨터 시스템 인터페이스(SCSI) 인터페이스 표준,

[0193] 직렬 부착 소형 컴퓨터 시스템 인터페이스(SAS) 인터페이스 표준,

[0194] 섬유 채널 인터페이스 표준,

[0195] 이더넷 인터페이스 표준, 그리고

[0196] 주변 컴포넌트 상호접속 익스프레스(PCIe) 인터페이스 표준 중 하나 또는 그 초과를 포함하는, EC들.

[0197] EC58) 플래시 메모리 인터페이스를 갖거나 참조하는 임의의 상술한 EC들로서, 플래시 메모리 인터페이스는,

[0198] 오픈 NAND 플래시 인터페이스(ONFI),

[0199] 토글 모드 인터페이스,

[0200] 더블 데이터 레이트(DDR) 동기 인터페이스,

[0201] DDR2 동기 인터페이스,

[0202] 동기 인터페이스, 그리고

[0203] 비동기 인터페이스 중 하나 또는 그 초과와 호환가능한, EC들.

[0204] EC59) 컴퓨팅 호스트를 갖거나 참조하는 임의의 상술한 EC들로서, 컴퓨팅 호스트는,

[0205] 컴퓨터,

[0206] 워크스테이션 컴퓨터,

[0207] 서버 컴퓨터,

[0208] 저장 서버,

[0209] 저장 부착 네트워크(SAN),

[0210] 네트워크 부착 저장(NAS) 디바이스,

[0211] 직접 부착 저장(DAS) 디바이스,

[0212] 저장 기구,

[0213] 개인 컴퓨터(PC),

[0214] 랩탑 컴퓨터,

[0215] 노트북 컴퓨터,

[0216] 넷북 컴퓨터,

[0217] 태블릿 디바이스 또는 컴퓨터,

[0218] 울트라북 컴퓨터,

[0219] 전자 판독 디바이스(e-리더),

[0220] 휴대 보조 단말기(PDA),

[0221] 네비게이션 시스템,

[0222] (핸드헬드) 글로벌 포지셔닝 시스템(GPS) 디바이스,

[0223] 자동 제어 시스템,

[0224] 자동 미디어 제어 시스템 또는 컴퓨터,

[0225] 프린터, 복사기 또는 팩스 머신 또는 일체형 디바이스,

[0226] 판매 시점 정보 관리(POS) 디바이스,

[0227] 캐시-레지스터,

[0228] 미디어 플레이어,

[0229] 텔레비전,

[0230] 미디어 리코더,

[0231] 디지털 비디오 리코더(DVR),

[0232] 디지털 카메라,

[0233] 셀룰러 핸드셋,

[0234] 코드리스 전화 핸드셋, 그리고

[0235] 전자 게임 중 하나 또는 그 초과를 포함하는, EC들.

[0236] EC60) 적어도 하나의 플래시 메모리를 갖거나 참조하는 임의의 상술한 EC들로서, 적어도 하나의 플래시 메모리의 적어도 일부는,

[0237] NAND 플래시 기술 저장 셀들, 그리고

[0238] NOR 플래시 기술 저장 셀들 중 하나 또는 그 초과를 포함하는, EC들.

[0239] EC61) 적어도 하나의 플래시 메모리를 갖거나 참조하는 임의의 상술한 EC들로서, 적어도 하나의 플래시 메모리의 적어도 일부는,

[0240] 단일 레벨 셀(SLC) 플래시 기술 저장 셀들, 그리고

[0241] 멀티 레벨 셀(MLC) 플래시 기술 저장 셀들 중 하나 또는 그 초과를 포함하는, EC들.

[0242] EC62) 적어도 하나의 플래시 메모리를 갖거나 참조하는 임의의 상술한 EC들로서, 적어도 하나의 플래시 메모리의 적어도 일부는,

[0243] 폴리실리콘 기술 기반 전하 저장 셀들, 그리고

[0244] 실리콘 질화물 기술 기반 전하 저장 셀들 중 하나 또는 그 초과를 포함하는, EC들.

[0245] EC63) 적어도 하나의 플래시 메모리를 갖거나 참조하는 임의의 상술한 EC들로서, 적어도 하나의 플래시 메모리의 적어도 일부는,

[0246] 2차원 기술 기반 플래시 메모리 기술, 그리고

[0247] 3차원 기술 기반 플래시 메모리 기술 중 하나 또는 그 초과를 포함하는, EC들.

[0248] 시스템

[0249] 도 1a는 NVM 소자들(예를 들어, 플래시 메모리들)을 통해 구현되는 것과 같은 비휘발성 저장부를 관리하기 위해 전송 암호화 층을 사용하는 SSD 제어기를 포함하는 SSD(101)의 실시예의 선택된 상세들을 예시한다. SSD 제어기는 NVM 소자들(예를 들어, 플래시 메모리들)을 통해 구현된 것과 같은 비휘발성 저장부를 관리하기 위한 것이

다. SSD 제어기(100)는 하나 또는 그 초과의 외부 인터페이스(110)를 통해 호스트(미도시)에 통신가능하게 커플링된다. 다양한 실시예들에 따르면, 외부 인터페이스들(110)은 SATA 인터페이스, SAS 인터페이스, PCIe 인터페이스, 섬유 채널 인터페이스, (10 기가바이트 이더넷과 같은) 이더넷 인터페이스, 임의의 선행 인터페이스들의 비표준 버전, 커스텀 인터페이스, 또는 저장부 및/또는 통신 및/또는 컴퓨팅 디바이스들을 상호접속하기 위해 사용된 임의의 다른 타입의 인터페이스 중 하나 또는 그 초과이다. 예를 들어, 일부 실시예들에서, SSD 제어기(100)는 SATA 인터페이스 및 PCIe 인터페이스를 포함한다.

[0250] SSD 제어기(100)는 플래시 디바이스(192)의 하나 또는 그 초과와 같은 하나 또는 그 초과의 저장 디바이스들을 포함하는 NVM(199)에 하나 또는 그 초과의 디바이스 인터페이스들(190)을 통해 통신가능하게 더 커플링된다. 다양한 실시예들에 따르면, 디바이스 인터페이스들(190)은 비동기 인터페이스, 동기 인터페이스, 단일 데이터 레이트(SDR) 인터페이스, 더블 데이터 레이트(DDR) 인터페이스, DRAM-호환가능 DDR 또는 DDR2 동기 인터페이스, ONFI 2.2 또는 ONFI 3.0 호환가능 인터페이스와 같은 ONFI 호환가능 인터페이스, 토글 모드 호환가능 플래시 인터페이스, 임의의 선행 인터페이스들의 비표준 버전, 커스텀 인터페이스, 또는 저장 디바이스들에 접속하기 위해 사용된 임의의 다른 타입의 인터페이스 중 하나 또는 그 초과이다.

[0251] 각 플래시 디바이스(192)는 일부 실시예들에서, 하나 또는 그 초과의 개별 플래시 다이(194)를 갖는다. 플래시 디바이스(192)의 특정한 하나의 타입에 따르면, 특정한 플래시 디바이스(192)에서의 복수의 플래시 다이(194)는 옵션으로 및/또는 선택적으로 병렬로 액세스가능하다. 플래시 디바이스(192)는 SSD 제어기(100)에 통신가능하게 커플링하도록 인에이블된 저장 디바이스의 하나의 타입을 단지 나타낸다. 다양한 실시예들에서, SLC NAND 플래시 메모리, MLC NAND 플래시 메모리, NOR 플래시 메모리, 폴리실리콘 또는 실리콘 질화물 기술 기반 전하 저장 셀들을 사용하는 플래시 메모리, 2차원 또는 3차원 기술 기반 플래시 메모리, 판독 전용 메모리, 정적 랜덤 액세스 메모리, 동적 랜덤 액세스 메모리, 강자성 메모리, 위상 변화 메모리, 레이스트랙(racetrack) 메모리, 또는 임의의 다른 타입의 메모리 디바이스 또는 저장 매체와 같은 임의의 타입의 저장 디바이스가 사용가능하다.

[0252] 다양한 실시예들에 따르면, 디바이스 인터페이스들(190)은 버스 당 하나 또는 그 초과의 플래시 디바이스(192)를 갖는 하나 또는 그 초과의 버스들, 버스 당 하나 또는 그 초과의 플래시 디바이스(192)를 갖는 버스들의 하나 또는 그 초과의 그룹들 - 그룹에서의 버스들은 일반적으로 병렬로 액세스됨 -, 또는 디바이스 인터페이스들(190)상의 하나 또는 그 초과의 플래시 디바이스(192)의 임의의 다른 구성으로서 구성된다.

[0253] 도 1a에 계속하여, SSD 제어기(100)는 호스트 인터페이스들(111), 데이터 프로세싱(121), 버퍼(131), 맵(141), 리사이클러(151), ECC(161), 디바이스 인터페이스 로직(191), 및 CPU(171)와 같은 하나 또는 그 초과의 모듈들을 갖는다. 도 1a에 예시된 특정한 모듈들 및 상호접속들은 단지 하나의 실시예를 나타내며, 예시되지 않은 부가의 모듈들뿐만 아니라 모듈들 중 일부 또는 모두의 많은 배열들 및 상호접속들이 구상된다. 제 1 예에서, 일부 실시예들에서, 이중-포팅(dual-porting)을 제공하기 위해 2개 또는 그 초과의 호스트 인터페이스들(111)이 존재한다. 제 2 예에서, 일부 실시예들에서, 데이터 프로세싱(121) 및/또는 ECC(161)는 버퍼(131)와 조합된다. 제 3 예에서, 일부 실시예들에서, 호스트 인터페이스들(111)은 버퍼(131)에 직접 커플링되고, 데이터 프로세싱(121)은 버퍼(131)에 저장된 데이터에 대해 옵션으로 및/또는 선택적으로 동작한다. 제 4 예에서, 일부 실시예들에서, 디바이스 인터페이스 로직(191)은 버퍼(131)에 직접 커플링되고, ECC(161)는 버퍼(131)에 저장된 데이터에 대해 옵션으로 및/또는 선택적으로 동작한다.

[0254] 호스트 인터페이스들(111)은 외부 인터페이스들(110)을 통해 커맨드들 및/또는 데이터를 전송 및 수신하고, 일부 실시예들에서는, 태그 트랙킹(113)을 통해 개별 커맨드들의 진행을 트랙킹한다. 예를 들어, 커맨드들은 판독하기 위해 (LBA와 같은) 어드레스 및 (다수의 LBA 정량, 예를 들어, 섹터들과 같은) 데이터량을 특정하는 판독 커맨드를 포함하고, 이에 응답하여, SSD는 판독 상태 및/또는 판독 데이터를 제공한다. 다른 예에 있어서, 커맨드들은 기록하기 위해 (LBA와 같은) 어드레스 및 (다수의 LBA 정량, 예를 들어, 섹터들과 같은) 데이터량을 특정하는 기록 커맨드를 포함하고, 이에 응답하여, SSD는 기록 상태를 제공하고 그리고/또는 기록 데이터를 요청하며 옵션으로 후속하여 기록 상태를 제공한다. 또 다른 예에 있어서, 커맨드들은 더 이상 할당될 필요가 없는 (하나 또는 그 초과의 LBA들과 같은) 하나 또는 그 초과의 어드레스들을 특정하는 할당해제(de-allocation) 커맨드(예를 들어, 트림 커맨드)를 포함하고, 이에 응답하여, SSD는 맵을 그에 따라 변경하고 옵션으로 할당해제 상태를 제공한다. 일부 컨텍스트들에서, ATA 호환가능 TRIM 커맨드는 예시적인 할당해제 커맨드이다. 또 다른 예에 있어서, 커맨드들은 수퍼 커패시터 테스트 커맨드 또는 데이터 경화 성공 문의를 포함하고, 이에 응답하여 SSD는 적절한 상태를 제공한다. 일부 실시예들에서, 호스트 인터페이스들(111)은 SATA 프로토콜과 호환가능하고, NCQ 커맨드들을 사용하여, 0 내지 31의 번호로서 표현된 고유 태그를 각각 갖는 32개까지의 펜딩 커

맨드들을 갖도록 인에이블된다. 일부 실시예들에서, 태그 트랙킹(113)은 외부 인터페이스들(110)을 통해 수신된 커맨드에 대한 외부 태그를 SSD 제어기(100)에 의한 프로세싱 동안 커맨드를 트랙킹하기 위해 사용된 내부 태그와 연관시키도록 인에이블된다.

[0255] 다양한 실시예들에 따르면, 하나 또는 그 초과의 데이터 프로세싱(121)은 버퍼(131)와 외부 인터페이스들(110) 사이에서 전송된 데이터 중 일부 또는 모두를 옵션으로 및/또는 선택적으로 프로세싱하고, 데이터 프로세싱(121)은 버퍼(131)에 저장된 데이터를 옵션으로 및/또는 선택적으로 프로세싱한다. 일부 실시예들에서, 데이터 프로세싱(121)은 포맷팅, 리포맷팅, 트랜스코딩, 및 임의의 다른 데이터 프로세싱 및/또는 조작 작업 중 하나 또는 그 초과를 수행하기 위해 하나 또는 그 초과의 엔진들(123)을 사용한다.

[0256] 버퍼(131)는 디바이스 인터페이스들(190)로부터 외부 인터페이스들(110)로/외부 인터페이스들(110)로부터 디바이스 인터페이스들(190)로 전송된 데이터를 저장한다. 일부 실시예들에서, 버퍼(131)는 하나 또는 그 초과의 플래시 디바이스(192)를 관리하기 위해 SSD 제어기(100)에 의해 사용된 맵 테이블들 중 일부 또는 모두와 같은 시스템 데이터를 부가적으로 저장한다. 다양한 실시예들에서, 버퍼(131)는 데이터의 임시 저장을 위해 사용된 메모리(137), 버퍼(131)로 및/또는 버퍼(131)로부터의 데이터의 이동(movement)을 제어하기 위해 사용된 DMA(133), 상위 레벨 에러 정정 및/또는 리던던시 기능(function)들을 제공하기 위해 사용된 ECC-X(135), 및 다른 데이터 이동 및/또는 조작 기능들 중 하나 또는 그 초과를 갖는다. 상위 레벨 리던던시 기능의 일례가 RAID형 능력이고, 여기서, 리던던시는 디스크 레벨 대신 플래시 디바이스(예를 들어, 플래시 디바이스(192)의 다중의 플래시 디바이스들) 레벨 및/또는 플래시 다이(예를 들어, 플래시 다이(194)) 레벨에 있다.

[0257] 다양한 실시예들에 따르면, 하나 또는 그 초과의 ECC(161)는 버퍼(131)와 디바이스 인터페이스들(190) 사이에서 전송된 데이터 중 일부 또는 모두를 옵션으로 및/또는 선택적으로 프로세싱하고, ECC(161)는 버퍼(131)에 저장된 데이터를 옵션으로 및/또는 선택적으로 프로세싱한다. 일부 실시예들에서, ECC(161)는 예를 들어, 하나 또는 그 초과의 ECC 기법들에 따라, 하위 레벨 에러 정정 및/또는 리던던시 기능들을 제공하기 위해 사용된다. 일부 실시예들에서, ECC(161)는 CRC 코드, 해밍 코드, RS 코드, BCH 코드, LDPC 코드, 비터비 코드, 트렐리스 코드, 하드 판정 코드, 소프트 판정 코드, 소거 기반 코드, 임의의 에러 검출 및/또는 정정 코드, 및 이들의 임의의 조합 중 하나 또는 그 초과를 구현한다. 일부 실시예들에서, ECC(161)는 (LDPC 디코더들과 같은) 하나 또는 그 초과의 디코더들을 포함한다.

[0258] 디바이스 인터페이스 로직(191)은 디바이스 인터페이스들(190)을 통해 플래시 디바이스(192)의 인스턴스들을 제어한다. 디바이스 인터페이스 로직(191)은 플래시 디바이스(192)의 프로토콜에 따라 플래시 디바이스(192)의 인스턴스들로/인스턴스들로부터 데이터를 전송하도록 인에이블된다. 디바이스 인터페이스 로직(191)은 디바이스 인터페이스들(190)을 통해 플래시 디바이스(192)의 인스턴스들의 제어를 선택적으로 시퀀싱하기 위한 스케줄링(193)을 포함한다. 예를 들어, 일부 실시예들에서, 스케줄링(193)은 플래시 디바이스(192)의 인스턴스들에 대한 동작들을 큐잉(queue)하고, 플래시 디바이스(192)(또는 플래시 다이(194))의 인스턴스들 중 개별 인스턴스들이 이용가능할 때 플래시 디바이스(192)(또는 플래시 다이(194))의 인스턴스들 중 개별 인스턴스들에 동작들을 선택적으로 전송하도록 인에이블된다.

[0259] 맵(141)은 외부 데이터 어드레스들을 NVM(199)에서의 위치들에 매핑하기 위해 테이블(143)을 사용하여, 외부 인터페이스들(110)상에서 사용된 데이터 어드레싱과 디바이스 인터페이스들(190)상에서 사용된 데이터 어드레싱 사이에서 변환한다. 예를 들어, 일부 실시예들에서, 맵(141)은 테이블(143)에 의해 제공된 매핑을 통해 하나 또는 그 초과의 플래시 다이(194)를 타겟으로 하는 블록 및/또는 페이지 어드레스들로 외부 인터페이스들(110)상에서 사용된 LBA들을 변환한다. 드라이브 제조 또는 할당해제 이후 기록된 적이 없는 LBA들에 대해, 맵은 LBA들이 판독된 경우 복귀하기 위해 디폴트값으로 포인팅한다. 예를 들어, 할당해제 커맨드를 프로세싱할 때, 맵은 할당해제된 LBA들에 대응하는 엔트리(entry)들이 디폴트값들 중 하나에 포인팅하도록 변경된다. 다양한 실시예들에서, 각각 대응하는 포인터를 갖는 다양한 디폴트값들이 존재한다. 복수의 디폴트값들은 (제 1 범위에서와 같은) 일부 할당해제된 LBA들을 하나의 디폴트값으로서 판독하는 것을 가능하게 하면서, (제 2 범위에서와 같은) 다른 할당해제된 LBA들을 다른 디폴트값으로서 판독하는 것을 가능하게 한다. 다양한 실시예들에서, 디폴트값들은 플래시 메모리, 하드웨어, 펌웨어, 커맨드 및/또는 원시 독립변수들 및/또는 파라미터들, 프로그램가능한 레지스터들, 또는 이들의 다양한 조합들에 의해 정의된다.

[0260] 일부 실시예들에서, 맵(141)은 외부 인터페이스들(110)상에서 사용된 어드레스들과 디바이스 인터페이스들(190)상에서 사용된 데이터 어드레싱 사이에서 트랜슬레이션들을 수행하고 그리고/또는 룩업하기 위해 테이블(143)을 사용한다. 다양한 실시예들에 따르면, 테이블(143)은 1-레벨 맵, 2-레벨 맵, 멀티-레벨 맵, 맵 캐시,

압축된 맵, 하나의 어드레스 공간으로부터 다른 어드레스 공간으로의 임의의 타입의 매핑, 및 이들의 임의의 조합 중 하나 또는 그 초과이다. 다양한 실시예들에 따르면, 테이블(143)은 정적 랜덤 액세스 메모리, 동적 랜덤 액세스 메모리, (플래시 메모리와 같은) NVM, 캐시 메모리, 온-칩 메모리, 오프-칩 메모리, 및 이들의 임의의 조합 중 하나 또는 그 초과이다.

[0261] 일부 실시예들에서, 리사이클러(151)는 가비지 회수를 수행한다. 예를 들어, 일부 실시예들에서, 플래시 디바이스(192)의 인스턴스들은 블록들이 재기록가능하기 전에 소거되어야 하는 블록을 포함한다. 리사이클러(151)는 예를 들어, 맵(141)에 의해 유지된 맵을 스캔함으로써 플래시 디바이스(192)의 인스턴스들 중 어느 부분들이 액티브하게 사용중인지 (예를 들어, 할당해제 대신에 할당되는지)를 결정하고, 플래시 디바이스(192)의 인스턴스들 중 미사용(예를 들어, 할당해제된) 부분들을 이들을 소거함으로써 기록하는데 이용가능하게 하도록 인에이블된다. 추가의 실시예들에서, 리사이클러(151)는 플래시 디바이스(192)의 인스턴스들 중 더 큰 인접 부분들을 기록하는데 이용가능하게 하기 위해 플래시 디바이스(192)의 인스턴스들내에 저장된 데이터를 이동시키도록 인에이블된다.

[0262] 일부 실시예들에서, 플래시 디바이스(192)의 인스턴스들은 상이한 타입들 및/또는 특성들의 데이터를 저장하기 위한 하나 또는 그 초과의 대역들을 갖도록 선택적으로 및/또는 동적으로 구성되고, 관리되고 그리고/또는 사용된다. 대역들의 수, 배열, 사이즈, 및 타입은 동적으로 변경(change)가능하다. 예를 들어, 컴퓨팅 호스트로부터의 데이터는 핫(hot)(액티브한) 대역에 기록되지만, 리사이클러(151)로부터의 데이터는 콜드(cold)(덜 액티브한) 대역에 기록된다. 일부 사용 시나리오들에서, 컴퓨팅 호스트가 긴 순차적 스트림을 기록하면, 이후 핫 대역의 사이즈가 증가하는 반면에, 컴퓨팅 호스트가 랜덤하게 기록하거나 거의 기록하지 않으면, 이후 콜드 대역의 사이즈가 증가한다.

[0263] CPU(171)는 SSD 제어기(100)의 다양한 부분들을 제어한다. CPU(171)는 CPU 코어(172)를 포함한다. 다양한 실시예들에 따라, CPU 코어(172)는 하나 또는 그 초과의 단일-코어 또는 멀티-코어 프로세서들이다. 일부 실시예들에서, CPU 코어(172)에서의 개별 프로세서들 코어들은 멀티-쓰레드된다(multi-threaded). CPU 코어(172)는 명령어 및/또는 데이터 캐시들 및/또는 메모리들을 포함한다. 예를 들어, 명령 메모리는 CPU 코어(172)로 하여금 SSD 제어기(100)를 제어하기 위해 프로그램들(예를 들어, 때때로 펌웨어로 칭하는 소프트웨어)을 실행할 수 있게 하기 위한 명령어들을 포함한다. 일부 실시예들에서, CPU 코어(172)에 의해 실행된 펌웨어 중 일부 또는 모두는 (예를 들어, 도 1b에서 NVM(199)의 펌웨어(106)로서 예시된 바와 같이) 플래시 디바이스(192)의 인스턴스들상에 저장된다.

[0264] 다양한 실시예들에서, CPU(171)는 커맨드들이 진행중인 동안 외부 인터페이스들(110)을 통해 수신된 커맨드들을 트랙킹 및 제어하기 위한 커맨드 관리(173), 버퍼(131)의 할당 및 사용을 제어하기 위한 버퍼 관리(175), 맵(141)을 제어하기 위한 트랜슬레이션 관리(177), 데이터 어드레싱의 일치성을 제어하고 예를 들어, 외부 데이터 액세스들과 리사이클 데이터 액세스들 사이의 충돌들을 회피하기 위한 코히어런시 관리(179), 디바이스 인터페이스 로직(191)을 제어하기 위한 디바이스 관리(181), 식별 정보의 변경(modification) 및 통신을 제어하기 위한 아이덴티티 관리(182), 및 옵션으로 다른 관리 유닛들을 더 포함한다. 다양한 실시예들에 따르면, CPU(171)에 의해 수행된 관리 기능들 중 어느 것도, 임의의 것 또는 모두는 하드웨어, (외부 인터페이스들(110)을 통해 접속된 CPU 코어(172) 또는 호스트상에서 실행하는 펌웨어와 같은) 소프트웨어, 또는 이들의 임의의 조합에 의해 제어 및/또는 관리된다.

[0265] 일부 실시예들에서, CPU(171)는 성능 통계의 수집 및/또는 리포팅, SMART의 구현, 전력 시퀀싱의 제어, 전력 소모의 제어 및/또는 모니터링 및/또는 조정, 정전에 대한 응답, 클록 레이트들의 제어 및/또는 모니터링 및/또는 조정, 및 다른 관리 작업들 중 하나 또는 그 초과와 같은 다른 관리 작업들을 수행하도록 인에이블된다.

[0266] 다양한 실시예들은 SSD 제어기(100)와 유사하고 예를 들어, 호스트 인터페이스들(111) 및/또는 외부 인터페이스들(110)의 적용을 통해 다양한 컴퓨팅 호스트들과의 동작과 호환가능한 컴퓨팅 호스트 플래시 메모리 제어기를 포함한다. 다양한 컴퓨팅 호스트들은 컴퓨터, 워크스테이션 컴퓨터, 서버 컴퓨터, 저장 서버, SAN, NAS 디바이스, DAS 디바이스, 저장 기구, PC, 랩탑 컴퓨터, 노트북 컴퓨터, 넷북 컴퓨터, 태블릿 디바이스 또는 컴퓨터, 울트라북 컴퓨터, (e-판독기와 같은) 전자 판독 디바이스, PDA, 네비게이션 시스템, (핸드헬드) GPS 디바이스, 자동 제어 시스템, 자동 미디어 제어 시스템 또는 컴퓨터, 프린터, 복사기 또는 팩스 머신 또는 일체형 디바이스, POS 디바이스, 캐시-레지스터, 미디어 플레이어, 텔레비전, 미디어 리코더, DVR, 디지털 카메라, 셀룰러 핸드셋, 코드리스 전화 핸드셋, 및 전자 게임 중 하나 또는 임의의 조합을 포함한다.

[0267] 다양한 실시예들에서, SSD 제어기(또는 컴퓨팅 호스트 플래시 메모리 제어기) 중 모두 또는 임의의 부분들은 단

일 IC, 멀티-다이 IC의 단일 다이, 멀티-다이 IC의 복수의 다이들, 또는 복수의 IC들상에서 구현된다. 예를 들어, 버퍼(131)는 SSD 제어기(100)의 다른 소자들과 동일한 다이상에서 구현된다. 다른 예에 있어서, 버퍼(131)는 SSD 제어기(100)의 다른 소자들과는 상이한 다이상에서 구현된다.

[0268] 도 1b는 도 1a의 SSD의 하나 또는 그 초과의 인스턴스들을 포함하는 시스템들의 다양한 실시예들의 선택된 상세들을 예시한다. SSD(101)는 디바이스 인터페이스들(190)을 통해 NVM(199)에 커플링된 SSD 제어기(100)를 포함한다. 도면은 다양한 클래스들의 실시예들: 호스트에 직접 커플링된 단일 SSD, 각각의 외부 인터페이스들을 통해 호스트에 직접적으로 각각 커플링되는 복수의 SSD들, 및 다양한 상호접속 소자들을 통해 호스트에 간접적으로 커플링된 하나 또는 그 초과의 SSD들을 예시한다.

[0269] 호스트에 직접적으로 커플링된 단일 SSD의 예시적인 실시예로서, SSD(101)의 하나의 인스턴스는 외부 인터페이스들(110)을 통해 호스트(102)에 직접적으로 커플링된다(예를 들어, 스위치/구조/중간 제어기(103)가 생략되고, 바이패스되거나, 통과된다). 각각의 외부 인터페이스들을 통해 호스트에 직접적으로 각각 커플링된 복수의 SSD들의 예시적인 실시예로서, SSD(101)의 복수의 인스턴스들 각각은 외부 인터페이스들(110)의 각각의 인스턴스를 통해 호스트(102)에 직접적으로 각각 커플링된다(예를 들어, 스위치/구조/중간 제어기(103)가 생략되고, 바이패스되거나, 통과된다). 다양한 상호접속 소자들을 통해 호스트에 간접적으로 커플링된 하나 또는 그 초과의 SSD들의 예시적인 실시예로서, SSD(101)의 하나 또는 그 초과의 인스턴스들 각각은 호스트(102)에 간접적으로 각각 커플링된다. 각각의 간접 커플링은 호스트(102)에 커플링하는 중간 인터페이스들(104) 및 스위치/구조/중간 제어기(103)에 커플링된 외부 인터페이스들(110)의 각각의 인스턴스를 통한다.

[0270] 스위치/구조/중간 제어기(103)를 포함하는 실시예들 중 일부는 메모리 인터페이스(180)를 통해 커플링되고 SSD들에 의해 액세스가능한 카드 메모리(112C)를 또한 포함한다. 다양한 실시예들에서, SSD들, 스위치/구조/중간 제어기, 및/또는 카드 메모리 중 하나 또는 그 초과는 물리적으로 식별가능한 모듈, 카드, 또는 플러그가능한 소자(예를 들어, I/O 카드(116))상에 포함된다. 일부 실시예들에서, SSD(101)(또는 그것의 변동물들)는 호스트(102)로서 동작하는 개시자에 커플링되는 SAS 드라이브 또는 SATA 드라이브에 대응한다.

[0271] 호스트(102)는 OS(105), 드라이버(107), 애플리케이션(109), 및 멀티-디바이스 관리 소프트웨어(114)의 다양한 조합들과 같은 호스트 소프트웨어(115)의 다양한 소자들을 실행하도록 인에이블된다. 점선 화살표(107D)는 호스트 소프트웨어 ←→ I/O 디바이스 통신, 예를 들어, 드라이버(107), 드라이버(107), 및 애플리케이션(109)을 통해, 드라이버(107)를 통하거나 VF로서 직접적으로 중 어느 하나에 의해, SSD(101)의 인스턴스들 중 하나 또는 그 초과로/그로부터 전송/수신되고, OS(105)의 임의의 하나 또는 그 초과로부터/그로 수신/전송된 데이터를 나타낸다.

[0272] OS(105)는 SSD와의 인터페이싱을 위해 (드라이버(107)에 의해 개념적으로 예시된) 드라이버들을 포함하고 그리고/또는 그 드라이버들과 동작하도록 인에이블된다. 다양한 버전들의 윈도우들(예를 들어, 95, 98, ME, NT, XP, 2000, 서버, 비스타, 및 7), 다양한 버전들의 리눅스(예를 들어, Red Hat, Debian, 및 Ubuntu), 및 다양한 버전들의 MacOS(예를 들어, 8, 9 및 X)가 OS(105)의 예들이다. 다양한 실시예들에서, 드라이버들은 표준 인터페이스 및/또는 SATA, AHCI, 또는 NVM 익스프레스와 같은 프로토콜과 동작가능한 표준 및/또는 일반 드라이버들(때때로, "수축 포장(shrink-wrapped)" 또는 "사전 설치(pre-installed)"로 칭함)이거나, 옵션으로는 SSD(101)에 특정한 커맨드들의 사용을 가능하게 하도록 커스터마이징되고 그리고/또는 판매자 특정된다. 일부 드라이브들 및/또는 드라이버들은 애플리케이션(109)과 같은 애플리케이션 레벨 프로그램들이 최적화된 NAND 액세스(때때로 ONA로 칭함) 또는 직접 NAND 액세스(때때로, DNA로 칭함) 기법들을 통해 SSD(101)에 직접적으로 커맨드들을 통신할 수 있게 하기 위한 통과(pass-through) 모드들을 갖고, 이것은 커스터마이징된 애플리케이션이 일반 드라이버를 갖더라도 SSD(101)에 특정된 커맨드들을 사용할 수 있게 한다. ONA 기법들은 비표준 변경자들(힌트들)의 사용, 판매자 특정 커맨드들의 사용, 압축성(compressibility)에 따른 실제 NVM 사용과 같은 비표준 통계의 통신, 및 다른 기법들 중 하나 또는 그 초과를 포함한다. DNA 기법들은 NVM에 매핑되지 않은 판독, 기록, 및/또는 소거 액세스를 제공하는 비표준 커맨드들 또는 판매자 특정 커맨드들의 사용, 예를 들어, I/O 디바이스가 그렇지 않으면 행할 데이터의 포맷팅을 바이패스함으로써 NVM에 더 직접적인 액세스를 제공하는 비표준 또는 벤더 특정 커맨드들의 사용, 및 다른 기법들 중 하나 또는 그 초과를 포함한다. 드라이버의 예들은 ONA 또는 DNA 지원이 없는 드라이버, ONA-인에이블된 드라이버, DNA-인에이블된 드라이버, 및 ONA/DNA-인에이블된 드라이버이다. 드라이버의 다른 예들은 판매자-제공, 판매자-개발, 및/또는 판매자-강화 드라이버, 및 클라이언트-제공, 클라이언트-개발, 및/또는 클라이언트-강화 드라이버이다.

[0273] 애플리케이션-레벨 프로그램들의 예들은 ONA 또는 DNA 지원이 없는 애플리케이션, ONA-인에이블된 애플리케이

션, DNA - 인에이블된 애플리케이션, 및 ONA/DNA - 인에이블된 애플리케이션이다. 점선 화살표(109D)는 애플리케이션←→ I/O 디바이스 통신(예를 들어, 드라이버를 통한 바이패스 또는 애플리케이션에 대해 VF를 통한 바이패스), 예를 들어, 중개자로서 OS를 사용하는 애플리케이션 없이 SSD와 통신하는 ONA - 인에이블된 애플리케이션 및 ONA - 인에이블된 드라이버를 나타낸다. 점선 화살표(109V)는 애플리케이션 ←→ I/O 디바이스 통신(예를 들어, 애플리케이션에 대해 VF를 통한 바이패스), 예를 들어, 중개자들로서 OS 또는 드라이버를 사용하는 애플리케이션 없이 SSD와 통신하는 DNA - 인에이블된 애플리케이션 및 DNA - 인에이블된 드라이버를 나타낸다.

[0274] 일부 실시예들에서, NVM(199)의 하나 또는 그 초과의 부분들은 펌웨어 저장부, 예를 들어, 펌웨어(106)에 대해 사용된다. 펌웨어 저장부는 하나 또는 그 초과의 펌웨어 이미지들(또는 그것의 부분들)을 포함한다. 예를 들어, 펌웨어 이미지는 예를 들어, SSD 제어기(100)의 CPU 코어(172)에 의해 실행된 펌웨어의 하나 또는 그 초과의 이미지들을 갖는다. 다른 예에 있어서, 펌웨어 이미지는 예를 들어, 펌웨어 실행 동안 CPU 코어에 의해 참조되는 상수들, 파라미터 값들, 및 NVM 디바이스 정보의 하나 또는 그 초과의 이미지들을 갖는다. 펌웨어의 이미지들은 예를 들어, 현재의 펌웨어 이미지 및 (펌웨어 업데이트들에 관한) 제로 또는 그 초과의 이전의 펌웨어 이미지들에 대응한다. 다양한 실시예들에서, 펌웨어는 일반, 표준, ONA 및/또는 DNA 동작 모드들을 제공한다. 일부 실시예들에서, 펌웨어 동작 모드들 중 하나 또는 그 초과는 드라이버에 의해 옵션으로 통신되고 그리고/또는 제공되는 키들 또는 다양한 소프트웨어 기법들을 통해 인에이블된다(예를 들어, 하나 또는 그 초과의 API들이 "언락(unlock)"된다).

[0275] 스위치/구조/중간 제어기가 부족한 일부 실시예들에서, SSD는 외부 인터페이스들(110)을 통해 직접적으로 호스트에 커플링된다. 다양한 실시예들에서, SSD 제어기(100)는 RAID 제어기와 같은 다른 제어기들의 하나 또는 그 초과의 중간 레벨들을 통해 호스트에 커플링된다. 일부 실시예들에서, SSD(101)(또는 그것의 변동물들)는 SAS 드라이브 또는 SATA 드라이브에 대응하고, 스위치/구조/중간 제어기(103)는 개시자에 차례로 커플링되는 확장자에 대응하거나, 대안적으로는, 스위치/구조/중간 제어기(103)는 확장자를 통해 개시자에 간접적으로 커플링되는 브리지에 대응한다. 일부 실시예들에서, 스위치/구조/중간 제어기(103)는 하나 또는 그 초과의 PCIe 스위치들 및/또는 구조들을 포함한다.

[0276] 호스트(102)가 컴퓨팅 호스트(예를 들어, 컴퓨터, 워크스테이션 컴퓨터, 서버 컴퓨터, 저장 서버, SAN, NAS 디바이스, DAS 디바이스, 저장 기구, PC, 랩탑 컴퓨터, 노트북 컴퓨터, 및/또는 넷북 컴퓨터)인 실시예들 중 일부와 같은 다양한 실시예들에서, 컴퓨팅 호스트는 하나 또는 그 초과의 로컬 및/또는 원격 서버들(예를 들어, 옵션의 서버들(118))과 (예를 들어, 옵션 I/O & 저장 디바이스들/자원들(117) 및 옵션 LAN/WAN(119)을 통해) 통신하도록 옵션으로 인에이블된다. 예를 들어, 통신은 SSD(101) 소자들 중 임의의 하나 또는 그 초과의 로컬 및/또는 원격 액세스, 관리, 및/또는 사용을 가능하게 한다. 일부 실시예들에서, 통신은 전체적으로 또는 부분적으로 이더넷을 통한다. 일부 실시예들에서, 통신은 전체적으로 또는 부분적으로 섬유 채널을 통한다. 다양한 실시예들에서, LAN/WAN(119)은 서버 팜에서의 네트워크, 서버 팜들을 커플링하는 네트워크, 메트로 - 영역 네트워크, 및 인터넷 중 임의의 하나 또는 그 초과와 같은 하나 또는 그 초과의 로컬 및/또는 광역 네트워크들을 나타낸다.

[0277] 다양한 실시예들에서, 하나 또는 그 초과의 NVM들과 결합하여 SSD 제어기 및/또는 컴퓨팅 호스트 플래시 메모리 제어기는 USB 저장 컴포넌트, CF 저장 컴포넌트, MMC 저장 컴포넌트, eMMC 저장 컴포넌트, 썬더볼트 저장 컴포넌트, UFS 저장 컴포넌트, SD 저장 컴포넌트, 메모리 스틱 저장 컴포넌트, 및 xD - 픽처 카드 저장 컴포넌트와 같은 비휘발성 저장 컴포넌트로서 구현된다.

[0278] 다양한 실시예들에서, SSD 제어기(또는 컴퓨팅 호스트 플래시 메모리 제어기) 중 모두 또는 임의의 부분들, 또는 그것의 기능들은 제어기가 커플링될 호스트(예를 들어, 도 1b의 호스트(102))에서 구현된다. 다양한 실시예들에서, SSD 제어기(또는 컴퓨팅 호스트 플래시 메모리 제어기) 중 모두 또는 임의의 부분들, 또는 그것의 기능들은 하드웨어(예를 들어, 로직 회로), 소프트웨어 및/또는 펌웨어(예를 들어, 드라이버 소프트웨어 또는 SSD 제어 펌웨어), 또는 이들의 임의의 조합을 통해 구현된다. 예를 들어, (예를 들어, 도 1a의 ECC(161) 및/또는 ECC - X(135)와 유사한) ECC 유닛의 기능 또는 그와 연관된 기능은 호스트상의 소프트웨어를 통해 부분적으로 및 SSD 제어기에서 펌웨어와 하드웨어의 조합을 통해 부분적으로 구현된다. 다른 예에 있어서, (예를 들어, 도 1a의 리사이클러(151)와 유사한) 리사이클러 유닛의 기능 또는 그와 연관된 기능은 호스트상의 소프트웨어를 통해 부분적으로 및 컴퓨팅 호스트 플래시 메모리 제어기에서 하드웨어를 통해 부분적으로 구현된다.

[0279] 전송 암호화 사용 및 동작의 예

[0280] 도 2는 도 1a에 예시된 바와 같은 비휘발성 저장부를 관리하기 위해 암호화된 전송 기법들을 사용하는 암호화된

전송 SSD(200)의 특정한 애플리케이션의 일례를 예시한다. 컴퓨터(202)가, 이후 원격 서버(204)로부터 인터넷으로 통해 다운로딩되고, 암호화된 전송 SSD(200)상에 일시적으로 저장되며, 시청을 위해 VGA 디스플레이(206)로 전달되는 유료 영화를 선택하고 그것의 대여료를 지불하기 위해 사용된다. 따라서, 영화는 VGA 디스플레이를 제어하는 VGA 비디오 신호들(208)로서 컴퓨터로부터 발생할 때까지 서버로부터 이동(transit)하는 동안 (예를 들어, 도난으로부터) 보호된다.

[0281] 영화는 암호화된 포맷으로 서버로부터 전송되고, 암호화된 포맷으로 SSD내에 저장되며, 암호화된 포맷으로 VGA 제어기(210)로 전달된다. 일부 상황들에서, VGA 비디오 신호들(208)은 고품질 비디오 레코딩에 적합하지 않으며, 따라서 영화가 VGA 비디오 신호들로서 도난될 가능성을 감소시킨다.

[0282] 컴퓨터는 원격 서버와 암호화된 전송 SSD(200) 사이에 (파선(212)에 의해 개념적으로 예시된) 보안 통신 링크를 확립함으로써 영화의 암호화된 전송을 시작한다. 일단 보안 통신 링크가 확립되면, 호스트로서 작용하는 원격 서버는 암호화 키들을 SSD와 교환한다. 원격 서버는 교환된 키들에 따라 영화를 암호화하고, 암호화된 영화를 보안 통신 링크를 통해 시청을 대기하는 임시 저장부에 대한 암호화된 전송 SSD(200)로 전송한다.

[0283] 암호화된 전송 SSD(200)는 플래시 메모리(214)에 저장을 위해 다운로딩된 영화를 압축한다. 일부 실시예들 및/또는 사용 시나리오들에서, 압축은 예를 들어, 플래시 메모리 기록 증폭의 최소화 및/또는 표면상의 저장 용량의 증가를 가능하게 한다. 그러나, 일부 상황들에서, 암호화된 영화는 효율적으로 압축되지 않는다. 따라서, (예를 들어, 단일 집적 회로로서 구현된) 보안 물리적 경계(SSD 제어기)(216)내에서, SSD는 다운로딩된 영화를 암호해독하기 위해 교환된 암호화 키를 사용한다. 암호해독된 영화는 저장을 위해 보안 물리적 경계(SSD 제어기)(216)로부터 플래시 메모리(214)로 보내기 전에 압축되고, 이후 재암호화된다. 다운로딩이 완료될 때, 원격 서버는 보안 통신 링크를 접속해제한다.

[0284] 영화 시청을 시작하기 위해, 컴퓨터는 VGA 제어기(210)와 암호화된 전송 SSD(200) 사이에 (파선(218)에 의해 개념적으로 예시된) 보안 통신 링크를 확립하여, 다운로딩된 영화의 저장 어드레스를 제공한다. 호스트로서 작용하는 VGA 제어기와 암호화된 전송 SSD(200) 사이에 암호화 키 교환이 있다. 암호화된 전송 SSD(200)는 플래시 메모리(214)로부터 저장된 영화를 리트리브(retrieve)하고, 보안 물리적 경계(SSD 제어기)(216)내에서 리트리브된 영화를 암호해독하고, 그 결과를 압축해제하고, 교환된 암호화 키를 사용하여 재암호화하며, 이후 재암호화된 영화를 VGA 제어기(210)로 보낸다. VGA 제어기는 암호화된 영화를 수신하고, VGA 제어기(210)의 보안 물리적 경계(VGA 제어기)(220)내에서, 교환된 암호화 키를 사용하여 영화를 암호해독하며, VGA 제어 신호들(208)을 제공하여, VGA 디스플레이(206)를 통한 영화 시청을 가능하게 한다. 부당변경(tampering) 또는 도난에 영향을 받는 비암호화된 형태에서 이용가능한 영화가 보안 물리적 경계(SSD 제어기)(216) 및 보안 물리적 경계(VGA 제어기)(220) 외부에 어디에도 없다.

[0285] 일부 실시예들에서, 원격 서버와 SSD 사이의 보안 통신 링크는 여러 소자들: 원격 서버와 컴퓨터 사이의 커플링(222), 컴퓨터를 통한 전송, 및 컴퓨터와 SSD 사이의 커플링(224)을 사용한다. 원격 서버와 컴퓨터 사이의 커플링(222)은 예를 들어, 원격 서버(204) 및 인터넷에 대한 커플링(미도시), 인터넷을 통한 전송, 및 컴퓨터(202)의 네트워킹 인터페이스를 통한 인터넷에 대한 다른 커플링을 통한다. 컴퓨터와 SSD 사이의 커플링(224)은 예를 들어, 컴퓨터(202)의 저장 인터페이스(미도시) 및 암호화된 전송 SSD(200)의 외부 인터페이스를 통한다. 일부 실시예들에서, VGA 제어기와 SSD 사이의 보안 통신 링크는 여러 소자들: 컴퓨터를 통한 전송, 컴퓨터와 SSD 사이의 커플링(224)을 사용한다.

[0286] 다양한 실시예들에서, 암호화된 전송 SSD(200)는 도 1a에 예시된 하나 또는 그 초과의 소자들에 따라 구현된다. 예를 들어, 플래시 메모리(214)는 도 1a의 NVM(199)에 대응하고 그리고/또는 SSD와 컴퓨터 사이의 커플링(224)은 도 1a의 하나 또는 그 초과의 외부 인터페이스(110)들에 대응한다. 다양한 컨텍스트들에서, 도 2에 예시된 특정한 애플리케이션은 도 1b에 예시된 하나 또는 그 초과의 소자들에 따라 구현된다. 예를 들어, 암호화된 전송 SSD(200)는 도 1b에서의 SSD(101)의 인스턴스에 대응하고, 컴퓨터(202)는 도 1b의 호스트(102)에 대응한다.

[0287] 전송 암호화 층 실시예들

[0288] 상기 예에서, 원격 서버(204)는 유로 영화의 다운로딩 및 저장 동안 호스트였다. 이후, 시청 동안에는, VGA 제어기(210)가 호스트로서 수행되었다. 도 2, 도 3a, 도 3b, 도 4, 및 도 5에 관하여 용어가 사용될 때, "호스트"의 예는 암호화된 전송 SSD의 특정한 실시예들로 데이터의 암호화된 전송 동안 암호화 키 교환 및 데이터 암호화/암호해독을 수행하는 시스템 플랫폼이다.

[0289] 도 3a, 도 3b, 도 4, 및 도 5는 암호화된 전송 SSD의 기능의 특정한 실시예들의 상세들을 예시한다. 도 3a는 2

-스테이지 사후 압축 데이터 암호화를 포함하는 기록 데이터 경로 기능을 예시한다. 도 3b는 도 3a의 기록 데이터 경로 기능의 "반대(reversing)"와 호환가능한 2-스테이지 사전 압축해제 암호해독을 포함하는 판독 데이터 경로 기능을 예시한다. 도 4는 암호화/암호해독 키들의 교환 및 호스트와 암호화된 전송 SSD 사이의 데이터 전송을 위해 보안 통신 링크를 확립하도록 사용된 핸드-쉐이킹(hand-shaking)을 예시한다. 도 5는 도 3a 및 도 3b에 예시된 바와 같은 데이터 경로들을 포함하는 호스트와 암호화된 전송 SSD 사이의 기록 및 판독 데이터 전송 동작들을 예시한다.

[0290] 도 3a의 블록도는 암호화 키들을 교환하고 플래시 메모리(306)에 저장을 위해 암호화된 데이터(304)를 전송하는 암호화된 전송 SSD(302)와 통신가능하게 커플링된 호스트(300)를 예시한다. 암호화된 전송 SSD(302)는 플래시 메모리(306) 및 SSD 제어기(308)를 포함한다. 다양한 실시예들 및/또는 사용 시나리오들에서, 암호화된 전송 SSD(302), SSD 제어기(308), 및 플래시 메모리(306)는 도 1a의 SSD(101), SSD 제어기(100), 및 NVM(199)에 각각 대응한다.

[0291] 특정한 실시예에서, SSD 제어기(308)는 호스트(300)와 플래시 메모리(306) 사이의 암호화된 데이터의 전송을 프로세싱하는 기록 데이터 경로(310)를 포함한다. 기록 데이터 경로(310)는 세션 암호해독 층(314), 무손실 압축 층(316), 내부 암호화 층(318), 백-엔드 암호화 층(320), 및 기록 포맷팅 층(322)을 포함한다. 기록 데이터 경로(310)는 암호화된 데이터(304)를 수신하고, 플래시 메모리(306)에 저장을 위해 포맷팅되어 암호화된 데이터(312)를 보낸다.

[0292] 일부 실시예들에서, 기록 데이터 경로(310)의 하나 또는 그 초과의 동작들 중 임의의 부분들은 도 1a의 SSD(101)의 하나 또는 그 초과의 소자들 중 부분들에 의해 수행된다. 예를 들어, 버퍼(131), ECC(161), 디바이스 인터페이스 로직(191), 및 디바이스 인터페이스들(190)의 부분들과 협력하여 데이터 프로세싱(121) 중 부분들은 기록 데이터 경로(310)의 동작들을 수행한다. 다른 실시예들에서, 상기 언급한 층들 중 하나 또는 그 초과는 하나 또는 그 초과의 전용 하드웨어 로직 회로 블록들 및/또는 하나 또는 그 초과의 내장된 프로세서들 및 연관된 펌웨어에서 구현된다. SSD 제어기(308)가 단일 집적 회로내에서 구현될 때, 단일 집적 회로는 암호해독된 데이터(326) 및 압축된 데이터(328)에서의 암호해독된 정보뿐만 아니라 임의의 교환된 키들이 (예를 들어, 부당변경 또는 도난으로부터) 안전하다는 것을 보장하는 보안 물리적 경계(미도시)를 제공한다.

[0293] 일부 실시예들에서, 암호화된 데이터가 플래시 메모리(306)에 기록되기 전에, 호스트(300) 및 암호화된 전송 SSD(302)는 보안 접속을 확립하고, 세션 암호화/암호해독 키들을 교환한다. 일부 시나리오들에서, 호스트는 기록 커맨드 및 저장 어드레스를 발행(issue)하고, 이후 (도 3a에 K_H로 예시된) 세션 암호화 키를 사용하여 데이터 암호화를 시작하고 결과(304)를 보낸다.

[0294] SSD 제어기(308)는 암호화된 데이터(304)를 수신하고, (도 3a에 K_C로 예시된) 세션 암호해독 키를 사용하여 세션 암호해독 층(314)에서 수신된 데이터를 암호해독하여, 암호해독된 데이터(326)를 생성한다. 암호해독된 데이터(326)는 무손실 압축 층(316)에 의해 압축되어, 압축된 데이터(328)를 생성한다. 일부 실시예들 및/또는 사용 시나리오들에서, 무손실 압축은 유리하게는, 저장되어야 하는 데이터량을 감소시킴으로써 플래시 메모리에 기록된 데이터의 표면상의 저장 용량을 증가시키고 그리고/또는 기록 증폭율을 감소시킨다. 특정한 실시예에서, 압축 기법은 LZ 무손실 압축(예를 들어, LZ77과 같은 s 사전 코더이다.

[0295] 압축된 데이터(328)는 내부 암호화 층(318)에 의해 암호화되어, 압축되어 암호화된 데이터(330)를 생성한다. 특정한 실시예에서, 내부 암호화 층(318)은 호스트(300)에 의해 사용된 세션 암호화 기법을 사용하여 암호화된 데이터(304)를 생성한다(예를 들어, K_B=K_H를 갖는 동일한 암호 알고리즘). 다른 실시예에서, 내부 암호화 층(318)의 암호화 기법은 예를 들어, TCG Opal과 같은 보안 프로토콜에 의해 결정된다. 이러한 보안 프로토콜의 특정한 실시예에서, 내부 암호화 층(318)에 의해 사용된 암호화 키(K_B)는 저장 어드레스 범위와 같은 메타-데이터에 의해 적어도 부분적으로 결정된다. 다른 실시예에서, 각각의 암호화 키와 각각 연관된 복수의 어드레스 범위들이 존재한다. 추가의 실시예들에서, 매칭되는 어드레스 범위들이 없다면 글로벌 "상기 중 어느 것도 아님(none of the above)" 키가 존재한다.

[0296] 일부 실시예들에서, 압축되어 암호화된 데이터(330)는 암호화 키(K_A)를 사용하는 백-엔드 암호화 층(320)에서 다시 암호화되어, 백-엔드 암호화된 데이터(332)를 생성한다. 다른 특정한 실시예에서, 백-엔드 암호화 층(320)은 내부 암호화 층(318)에 의해 사용된 것과는 상이한 암호화 기법 및/또는 키(들)(예를 들어, K_A!=K_B)를 사용한다. 또 다른 실시예들에서, 스크램블러가 암호화 대신에 사용된다.

[0297] 백-엔드 암호화된 데이터(332)는 저장 어드레스 매핑, 에러 정정을 위한 인코딩, 및 변조와 같은 기법들을 통해 기록 포맷팅 층(322)에 의해 프로세싱되어, 플래시 메모리(306)로 보내지는 포맷팅되어 암호화된 데이터(312)를 생성한다.

[0298] 기록 데이터 경로(310)의 다른 실시예(미도시)에서, 내부 암호화 층(318)은 존재하지 않고, 이는 백-엔드 암호화 층(320)으로의 압축된 데이터(328)의 직접 입력을 가능하게 한다. 다양한 실시예들에서, 단일-스테이지, 사후 압축 암호화 기록 데이터 경로는 (a) 백-엔드 암호화, (b) 호스트(300)에 의해 사용되는 바와 같은 전송 세션 암호화, 및 (c) 보안 프로토콜에 의해 결정된 암호화 중 하나를 이용한다.

[0299] 기록 데이터 경로(310)의 다른 실시예(미도시)에서, 호스트에 의해 송신된 데이터는 암호화되지 않지만 평문(clear-text)으로서 송신된다. 세션 암호해독 층(314)이 존재하지 않고, 이는 호스트로부터 무손실 압축 층(316)으로의 데이터의 직접 입력을 가능하게 한다. 내부 암호화 키(K_B)에 대한 값은 보안 프로토콜에 의해 결정된다. 백-엔드 암호화 층(320)은 백-엔드 암호화를 수행하기 위해 키(K_A)를 사용한다.

[0300] 기록 데이터 경로(310)의 다른 실시예(미도시)에서, 세션 암호해독 층(314) 및 내부 암호화 층(318) 모두가 존재하지 않는다. 호스트로부터 입력된 평문 데이터는 무손실 압축 층(316)에 직접 적용되고, 압축된 데이터(328)는 백-엔드 암호화 층(320)에 직접 적용된다. 백-엔드 암호화 키(K_A)에 대한 값은 (a) 백-엔드 암호화 키값 및 (b) 보안 프로토콜에 의해 결정된 값 중 하나이다.

[0301] 도 3b에 도시된 블록도는 암호화 키들을 교환하고 암호화된 전송 SSD(302)에서의 저장부로부터 호스트(300)로 암호화된 데이터(304)를 전송하는 암호화된 전송 SSD(302)와 통신가능하게 커플링된 호스트(300)를 예시한다. 도면은 도 3a에 예시된 암호화된 전송 SSD의 기록 데이터 경로 기능과 호환가능한 판독 데이터 경로 기능의 실시예의 선택된 상세들을 예시하고, 판독 데이터 경로 기능은 2-스테이지 사전 압축해제 암호해독을 포함한다.

[0302] 특정한 실시예에서, SSD 제어기(308)는 플래시 메모리(306)와 호스트(300) 사이의 암호화된 데이터의 전송을 프로세싱하는 판독 데이터 경로(346)를 포함한다. 판독 데이터 경로(346)는 판독 디포맷팅 층(336), 백-엔드 암호해독 층(338), 내부 암호해독 층(340), 판독 압축해제 층(342), 및 세션 암호화 층(344)을 포함한다. 판독 데이터 경로(346)는 플래시 메모리(306)에서의 저장부로부터 포맷팅되어 암호화된 데이터(312)를 받아서 암호화된 데이터(304)를 호스트(300)에 출력한다.

[0303] 일부 실시예들에서, 판독 데이터 경로(346)의 하나 또는 그 초과의 동작들 중 임의의 부분들은 도 1a의 SSD(101)의 하나 또는 그 초과의 소자들 중 부분들에 의해 수행된다. 예를 들어, 버퍼(131), ECC(161), 디바이스 인터페이스 로직(191), 및 디바이스 인터페이스들(190)의 부분들과 협력하여 데이터 프로세싱(121) 중 부분들은 판독 데이터 경로(346)의 동작들을 수행한다. 다른 실시예들에서, 상기 언급한 층들 중 하나 또는 그 초과는 하나 또는 그 초과의 전용 하드웨어 로직 회로 블록들 및/또는 하나 또는 그 초과의 내장된 프로세서들 및 연관된 펌웨어에서 구현된다. SSD 제어기(308)가 단일 집적 회로내에서 구현될 때, 단일 집적 회로는 암호해독된 데이터(326) 및 압축된 데이터(328)에서의 암호해독된 정보뿐만 아니라 임의의 교환된 키들이 (예를 들어, 부당변경 또는 도난으로부터) 안전하다는 것을 보장하는 보안 물리적 경계(미도시)를 제공한다.

[0304] 일부 실시예들에서, 포맷팅되어 암호화된 데이터(312)가 플래시 메모리(306)로부터 판독되기 전에, 호스트(300) 및 암호화된 전송 SSD(302)는 보안 접속을 확립하고, 세션 암호화/암호해독 키들을 교환한다. 일부 시나리오들에서, 호스트는 판독 커맨드 및 리트리브 어드레스를 발행하고, 이후, 암호화된 전송 SSD(302)에 의한 암호화된 데이터(304)의 전달을 대기한다. 호스트(300)는 수신된 데이터를 암호해독하기 위해 (도 3b에서 K_H로 예시된) 세션 암호해독 키를 사용한다.

[0305] SSD 제어기(308)는 플래시 메모리(306)로부터 포맷팅되어 암호화된 데이터(312)를 받는다. SSD 제어기(308)는 받은 데이터를 판독 디포맷팅 층(336)에서 디포맷팅하여, 저장 어드레스 매핑, 에러 정정을 위한 디코딩, 및 복조와 같은 기법들을 통해 백-엔드 암호화된 데이터(332)를 생성한다. 백-엔드 암호화된 데이터(332)는 백-엔드 암호해독 층(338)에서 암호해독되어, 압축되어 암호화된 데이터(330)를 생성한다. 압축되어 암호화된 데이터(330)는 내부 암호해독 층(340)에 의해 암호해독되어, 압축된 데이터(328)를 생성한다. 압축된 데이터(328)는 판독 압축해제 층(342)에서 압축해제되어, 암호해독된 데이터(326)를 생성한다. 암호해독된 데이터(326)는 세션 암호화 키(K_C)를 사용하여 세션 암호화 층(344)에 의해 암호화되어, 암호화된 데이터(304)를 생성한다. 판독 동작은 기록 동작의 반대와 유사하다. 판독 디포맷팅 층(336), 암호해독 층들(338 및 340), 판독 압축해제 층(342), 및 세션 암호화 층(344)은 데이터를 플래시 메모리(306)에 저장되게 하는 기록 동작들의 효

과들 반전시킨다.

[0306] 기록 동안 내부 암호화 층(318)에 의해 사용된 암호화 키(K_B)가 저장 어드레스 범위와 같은 메타-데이터에 의해 적어도 부분적으로 결정될 때 또는 각각의 암호화 키들이 복수의 어드레스 범위들에 의해 결정되는 경우 또는 어드레스 범위들 중 어느 것도 매칭되지 않기 때문에 "상기 어느 것도 아님" 키가 사용되는 경우에, 대응하는 암호해독 키들이 압축된 데이터(328)를 생성하기 위해 내부 암호해독 층(340)에 의해 사용된다.

[0307] 판독 데이터 경로(346)의 다른 실시예(미도시)에서, 내부 암호해독 층(340)은 존재하지 않고, 이는 판독 압축해제 층(342)으로의 백-엔드 암호해독 데이터의 직접 입력을 가능하게 한다. 다양한 실시예들에서, 단일-스테이지, 사전 압축해제 암호해독 판독 데이터 경로는 (a) 백-엔드 암호해독, (b) 호스트(300)에 의해 사용되는 바와 같은 전송 세션 암호해독, 및 (c) 보안 프로토콜에 의해 결정된 암호해독 중 하나를 이용한다.

[0308] 판독 데이터 경로(346)의 다른 실시예(미도시)에서, 호스트에 의해 수신된 데이터는 암호화되지 않지만 평문으로서 송신된다. 세션 암호화 층(344)이 존재하지 않고, 이는 판독 압축해제 층(342)이 데이터를 호스트에 직접 제공할 수 있게 한다. 내부 암호해독 키(K_B)에 대한 값은 보안 프로토콜에 의해 결정된다. 백-엔드 암호해독 층(338)은 키(K_A)를 사용하여, 플래시 메모리에 데이터를 기록하는 동안 사용된 백-엔드 암호화를 역으로(reverse) 한다.

[0309] 판독 데이터 경로(346)의 다른 실시예(미도시)에서, 내부 암호해독 층(340) 및 세션 암호화 층(344) 모두가 존재하지 않고, 이는 판독 압축해제 층(342)으로의 백-엔드 암호해독 데이터의 직접 입력을 가능하게 하며, 판독 압축해제 층(342)이 데이터를 평문으로서 호스트에 직접 제공할 수 있게 한다. 백-엔드 암호해독 층(338)은 (a) 백-엔드 암호화 키값 및 (b) 보안 프로토콜에 의해 결정된 값 중 하나를 사용하여, 플래시 메모리에 데이터를 기록하는 동안 사용된 백-엔드 암호화를 역으로 한다.

[0310] 또 다른 실시예들(미도시)에서, 호스트와 암호화된 전송 SSD 사이에서 송신된 데이터는 선택적으로 암호화되어 통신되며, 그렇지 않으면 평문으로서 통신된다. 예를 들어, 호스트 데이터의 하나 또는 그 초과의 어드레스 범위들은 (예를 들어, TCG-Opal에서와 같이 각각의 키들에 따르는 것과 같이) 암호화된 형태로 통신되는 데 반해, 다른 어드레스 범위들은 평문 형태로 통신된다. 다른 예에 있어서, 호스트로부터의 커맨드의 타입은 (판독 또는 기록 암호화된 커맨드들뿐만 아니라 판독 또는 기록 평문 커맨드들과 같이) 데이터가 암호화되어 통신되거나 평문으로서 통신되는지를 특정한다.

[0311] 다양한 실시예들에서, 충분한 자원들이 (기록 데이터 경로(310)와 같은) 호스트-플래시 기록 데이터 경로 및 (판독 데이터 경로(346)와 같은) 플래시-호스트 판독 데이터 경로의 동시 및 비간섭 동작을 가능하게 하기 위해 SSD 제어기에서 구현되어, 호스트와 암호화된 전송 SSD 사이의 동시 및 비간섭 양방향 기록 및 판독 동작들을 가능하게 한다. 다른 실시예들에서, 기록 및 판독 데이터 경로들 중 임의의 또는 모든 부분들은 공유되어서, 호스트와 암호화된 전송 SSD 사이의 동시 및/또는 비간섭 기록 및 판독 동작들을 방지하지만, 하드웨어의 감소(예를 들어, 일부 상황들에서는, 유리하게는 비용 감소)를 가능하게 한다.

[0312] 도 4는 도 2, 도 3a, 및 도 3b에 관하여 예시되어 설명한 바와 같이, 예를 들어, 암호화된 전송 SSD의 컨텍스트에서 암호화된 전송 데이터 전달을 수행하는 호스트와 SSD 제어기 사이의 보안 통신 링크의 생성, 사용, 및 폐기의 실시예를 예시하는 흐름도이다. 호스트 액션들(409)이 우측에 예시되어 있고, 제어기 액션들(419)이 좌측에 예시되어 있다.

[0313] 요약하면, 보안 통신 링크가 확립되고, 호스트 및 제어기는 상대방의 아이덴티티를 각각 인증하고, 대칭 암호화/암호해독 키들이 교환되고, 암호화된 데이터 전송이 발생하며, 완료될 때, 통신 링크는 접속해제되고 제어기가 대칭 암호화/암호해독 키의 자신의 카피를 파기한다.

[0314] 시작(401)에서, 호스트는 제어기로 하여금 오픈 채널 수용(412)으로 진행하게 하는 오픈 채널 요청(402)을 한다. 오픈 채널 수용(412)을 호스트가 보고, 호스트측 인증(403)으로 진행한다. 제어기는 제어기측 인증(413)으로 진행한다. 일부 시나리오들에서, 일단 양측이 상대측의 아이덴티티를 인증하면, 각 측은 공중 암호화 키를 다른 측에 송신하여, 보안 통신 링크의 생성을 완료한다.

[0315] 보안 통신 링크를 사용하여, 2개의 측들은 대칭 암호화/암호해독 키들을 교환한다(제어기측 키 교환(414) 및 호스트측 키 교환(404)). 일부 실시예들에서, AES128, AES192, 및 AES256과 같은 AES 암호화 기법이 사용된다. 이러한 실시예에서, 단일 키가 양측에 의해 암호화 및 암호해독을 위해 사용된다(K_C=K_H).

[0316] 보안 트래픽 교환이 발생하고(제어기측 보안 트래픽 교환(415) 및 호스트측 보안 트래픽 교환(405)), 그동안, 예를 들어, 도 3a에 대해 설명한 바와 같은 암호화된 데이터 기록 동작, 도 3b에 대해 설명한 바와 같은 암호화된 데이터 판독 동작, 또는 양자가 발생한다. 예를 들어, 대칭 암호화/암호해독 키들의 교환에 의해 결정된 바와 같은 키(K_C)는 도 3a의 세션 암호해독 층(314) 및 도 3b의 세션 암호화 층(344)의 키(K_C)에 대응한다. 호스트로부터 제어기로 송신된 데이터는 참조 부호 "508"(제어기측으로의 호스트측 보안 트래픽(508))로 표시되는데 반해, 제어기로부터 호스트로 송신된 데이터는 참조 부호 "510"(호스트측으로의 제어기측 보안 트래픽(510))으로 표시된다.

[0317] 일부 실시예들에서, 보안 트래픽 교환 "아래"에서 개념적으로 동작하는 보안 프로토콜이 옵션으로 이용된다. 제어기는 내부 암호화/암호해독 키들을 결정하기 위해 사용된 정보 및/또는 제어기측 TCG Ops/저장 액세스(415X)에 의해 예시된 제어기측 보안 프로토콜 기반 액세스들을 가능하게 하기 위한 프로토콜 정보를 수신하고 저장한다. 호스트는 내부 암호화/암호해독 키들을 결정하기 위해 사용된 대응하는 정보 및/또는 호스트측 TCG Ops/저장 액세스(405X)에 의해 예시된 호스트측 보안 프로토콜 기반 액세스들을 가능하게 하기 위한 프로토콜 정보를 결정 및/또는 수신하고, 이후 저장한다. 옵션의 보안 프로토콜과의 보안 트래픽 교환은 내부 암호화 층(318)(도 3a에 예시된 바와 같은 호스트 기록들) 및 내부 암호해독 층(340)(도 3b에 예시된 바와 같은 호스트 판독들)에 키 정보를 제공하기 위해 제어기측 TCG Ops/저장 액세스 (415X)와 연관된 내부 암호화/암호해독 키들 및/또는 프로토콜 정보를 사용한다. 일부 실시예들, 예를 들어, 보안 프로토콜과 같은 TCG Opal에 기초한 일부 실시예들에서, 내부 암호화/암호해독 층들에 대한 키 정보는 호스트 요청과 연관된 하나 또는 그 초과의 어드레스 범위들에 의존한다.

[0318] 보안 트래픽 교환이 완료될 때, 호스트측은 클로즈(close) 채널 요청(406)으로 진행하고, 제어기측은 클로즈 채널 수용(416)으로 진행한다. 보안 통신 링크는 폐기되고 제어기는 대칭 암호화/암호해독 키(K_C)의 자신의 카피를 파기한다(키 파기(417)).

[0319] 도 5는 (도 2, 도 3a, 도 3b, 및 도 4에 관하여 예시하고 설명한 바와 같이) 암호화된 전송 SSD 제어기의 데이터 경로 제어 및/또는 동작의 실시예를 예시하는 흐름도이다. 도 5에서, 기록 데이터 경로 제어 동작들(501 내지 507)은 좌측에 있고, 판독 데이터 경로 제어 동작들(517 내지 511)은 우측에 있다. 데이터 경로 제어 및/또는 동작들은 도 3a 및 도 3b에 예시된 바와 같은 2-스테이지 사후 압축 암호화 데이터 경로에 적용되고, 도 4의 제어기측 보안 트래픽 교환(415) 동안 발생하는 이벤트들에 대응한다. 도 5에 적용가능한 예시적인 동작 컨텍스트가 도 1b이고, 여기서, 개념적으로, 호스트(102)는 SSD 제어기(100)를 통해 암호화된 데이터를 NVM(199)에 기록하고, SSD 제어기를 통해 NVM(199)으로부터 암호화된 데이터를 판독한다.

[0320] 기록 동작 동안, SSD 제어기는 (예를 들어, 호스트로부터) 암호화된 기록 데이터를 수신하고(기록 데이터 수신(501)), (예를 들어, 도 3a의 314를 통해) 교환된 암호화/암호해독 키(K_H)(K_C=K_H)(키=K_H(522K))를 사용하여 암호화된 기록 데이터를 암호해독한다(기록 데이터 암호해독(502)). 암호해독된 데이터는 (예를 들어, 도 3a의 316을 통해) 압축된다(암호해독된 데이터 압축(503)). 압축된 데이터는 (예를 들어, 도 3a의 318을 통해) 내부 암호화 층에 의해 내부 암호화 키(K_B)를 사용하여 암호화된다(압축된 데이터 암호화(504)). 압축되어 암호화된 데이터는 (예를 들어, 도 3a의 320을 통해) 백-엔드 암호화 층에 의해 백-엔드 암호화 키(K_A)(키=K_A(525K))를 사용하여 (재)암호화된다(암호화된 데이터 (재)암호화(505)). 백-엔드 암호화된 데이터는 (예를 들어, 도 3a의 322를 통해) 변조되고((재)암호화된 데이터 변조(506)) NVM(199)에 저장된다(변조된 데이터 저장(507)). 일부 실시예들에서, 내부 암호화 키(K_B)는 기록 데이터를 수신하기 위해 사용된 키와 별개이다(K_B!=K_C)(키=K_B(524K)). 다른 실시예들에서, K_B에 대한 값은 보안 프로토콜에 의해 결정되고, 특정한 실시예에서, K_B=K_H이다. 참조 부호 "508"(제어기측으로의 호스트측 보안 트래픽(508))은 호스트로부터 SSD 제어기로 전송된 데이터를 나타내고, 참조 부호 "510"(호스트측으로의 제어기측 보안 트래픽(510))은 SSD 제어기로부터 호스트로 전송된 데이터를 나타낸다.

[0321] 판독 동작 동안, SSD 제어기는 NVM(199)으로부터 포맷팅되어 암호화된 데이터를 받고(데이터 판독(517)), (예를 들어, 도 3b의 336을 통해) 판독된 데이터를 복조한다(판독된 데이터 복조(516)). 복조된 데이터는 (예를 들어, 도 3b의 338을 통해) 암호해독되고(복조된 데이터 암호해독(515)), 결과가 (예를 들어, 도 3b의 340을 통해) 다시 암호해독된다(암호해독된 데이터 암호해독(514)). 결과가 (예를 들어, 도 3b의 342를 통해) 압축해제되고((재)암호해독된 데이터 압축해제(513)), 이후, (예를 들어, 도 3b의 344를 통해) 암호화되고(압축해제된

데이터 암호화(512), 결과적인 암호화된 데이터가 호스트(102)에 제공된다(암호화된 데이터 제공(511)).

[0322] 예시적인 구현 기법들

[0323] 일부 실시예들에서, 예를 들어, 플래시 메모리들, 컴퓨팅 호스트 플래시 메모리 제어기, 및/또는 (도 1a의 SSD 제어기(100)와 같은) SSD 제어기, 및 프로세서, 마이크로프로세서, 시스템-온-칩, 응용 주문형 집적 회로, 하드웨어 가속기, 또는 상기 언급한 동작들 중 모두 또는 부분들을 제공하는 다른 회로의 부분들로 암호화된 전송 SSD 제어기에 의해 수행된 동작들 중 모두 또는 부분들의 다양한 조합들이 컴퓨터 시스템에 의한 프로세싱과 호환가능한 사양에 의해 특정된다. 이 사양은 하드웨어 서술 언어들, 회로 기술들(descriptions), 넷리스트 기술들, 마스크 기술들, 또는 레이아웃 기술들과 같은 다양한 기술들에 따른다. 예시적인 기술들은 Verilog, VHDL, SPICE, PSpice와 같은 SPICE 변형들, IBIS, LEF, DEF, GDS-II, OASIS, 또는 다른 기술들을 포함한다. 다양한 실시예들에서, 프로세싱은 하나 또는 그 초과의 집적 회로들상에 포함을 위해 적합한 로직 및/또는 회로를 생성하고, 검증하거나, 특정하기 위해 해석(interpretation), 편집(compilation), 시뮬레이션, 및 합성의 임의의 조합을 포함한다. 다양한 실시예들에 따른 각 집적 회로는 다양한 기법들에 따라 설계가능하고 그리고/또는 제조가능하다. 기법들은 (필드 또는 마스크 프로그램가능한 게이트 어레이 집적 회로와 같은) 프로그램가능한 기법, (전체적 또는 부분적 셀-기반 집적 회로와 같은) 반특별 주문형(semi-custom) 기법, 및 (실질적으로 특수화된 집적 회로와 같은) 특별 주문형 기법, 이들의 임의의 조합, 또는 집적 회로들의 설계 및/또는 제조와 호환가능한 임의의 다른 기법을 포함한다.

[0324] 일부 실시예들에서, 명령어들의 세트가 저장된 컴퓨터 판독가능한 매체에 의해 설명된 바와 같은 동작들 중 모두 또는 부분들의 다양한 조합들은 하나 또는 그 초과의 프로그램 명령들의 실행 및/또는 해석에 의해, 하나 또는 그 초과의 소스 및/또는 스크립 언어 스테이트먼트(statement)들의 해석 및/또는 컴파일링에 의해, 또는 프로그래밍 및/또는 스크립팅 언어 스테이트먼트들로 표현된 정보의 컴파일링, 트랜슬레팅(translating), 및/또는 해석에 의해 생성된 2진 명령들의 실행에 의해 수행된다. 스테이트먼트들은 (C, C++, Fortran, Pascal, Ada, Java, VBscript, 및 Shell과 같은) 임의의 표준 프로그래밍 또는 스크립팅 언어와 호환가능하다. 프로그램 명령어들, 언어 스테이트먼트들, 또는 이진 명령어들 중 하나 또는 그 초과는 하나 또는 그 초과의 컴퓨터 판독가능한 저장 매체 소자들상에 옵션으로 저장된다. 다양한 실시예들에서, 프로그램 명령어들 중 일부, 모두, 또는 다양한 부분들은 하나 또는 그 초과의 함수(function)들, 루틴들, 서브-루틴들, 인-라인 루틴들, 절차들, 매크로들, 또는 이들의 부분들로서 실현된다.

[0325] 결론

[0326] 텍스트 및 도면들을 준비하는데 있어서 단지 편의를 위해 특정한 선택들이 설명에서 이루어졌고, 반대의 표시가 있지 않은 한, 이 선택들은 설명한 실시예들의 구조 또는 동작에 관한 부가의 정보를 전달하는 것으로서 자체적으로 해석되어서는 안 된다. 선택들의 예들은 도면 넘버링을 위해 사용된 지정들의 특정한 구성 또는 배치(assignment) 및 실시예들의 특징들 및 소자들을 식별하고 참조하기 위해 사용된 소자 식별자들(예를 들어, 콜아웃(callout)들 또는 수치적 지시자들)의 특정한 구성 또는 배치를 포함한다.

[0327] 단어들 "포함한다" 또는 "포함하는"은 개방형 범위의 논리 세트들을 설명하는 추론들로 해석되도록 구체적으로 의도되고, 단어 "내(within)"가 명시적으로 후속하지 않는 한, 물리적 한정을 전달하는 것으로 의미되지 않는다.

[0328] 상술한 실시예들이 설명 및 이해의 명확화를 위해 일부 상세히 설명되었지만, 본 발명은 제공된 상세들에 제한되지 않는다. 본 발명의 많은 실시예들이 존재한다. 개시된 실시예들은 예시적인 것이고 제한적인 것이 아니다.

[0329] 설명과 일치하는 구조, 배열, 및 사용에서의 많은 변동물들이 가능하고, 등록 특허의 청구항들의 범위내에 있다는 것이 이해될 것이다. 예를 들어, 사용된 상호접속 및 기능-유닛 비트-폭들, 클록 속도들, 및 기술의 타입은 각 컴포넌트 블록에서 다양한 실시예들에 따라 변경가능하다. 상호접속 및 로직에 주어진 명칭들은 단지 예시적인 것이고, 설명된 개념들을 제한하는 것으로 해석되어서는 안 된다. 플로우차트 및 흐름도 프로세스, 액션, 및 기능 소자들의 순서 및 배열은 다양한 실시예들에 따라 변경가능하다. 또한, 반대가 구체적으로 언급되지 않는 한, 특정된 값 범위들, 사용된 최대 및 최소값들, 또는 (플래시 메모리 기술 타입들, 및 레지스터들 및 버퍼들에서의 엔트리들 또는 스테이지들의 수와 같은) 다른 특정한 사양들은 단지 설명된 실시예들의 것들이고, 구현 기술에서 개선들 및 변경들을 트랙(track)하는 것으로 기대되고, 제한들로서 해석되어서는 안 된다.

[0330] 당업계에 공지된 기능적으로 등가인 기법들이 다양한 컴포넌트들, 서브-시스템들, 동작들, 함수들, 루틴들, 서

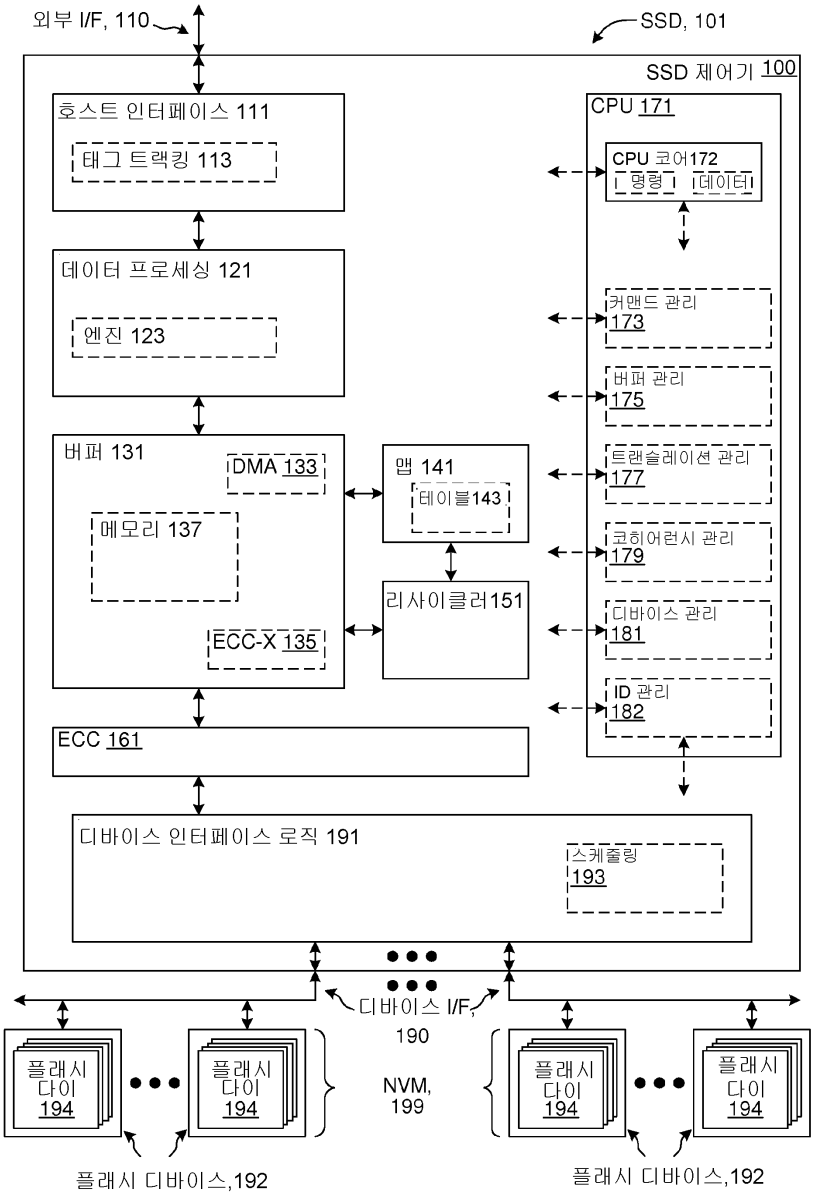
브-루틴들, 인-라인 루틴들, 절차들, 매크로들, 또는 이들의 부분들을 구현하기 위해 설명한 것들 대신에 이용가능하다. 실시예의 기능이 (하드웨어에서의 이전의 기능들의 소프트웨어로의 이동을 용이하게 하는) 더 빠른 프로세싱 및 (소프트웨어에서의 이전의 기능들의 하드웨어로의 이동을 용이하게 하는) 더 높은 집적 밀도의 설계 제약들 및 기술 트렌드들에 의존하기 때문에, 실시예들의 많은 기능적 양태들이 하드웨어(예를 들어, 일반적으로 전용 회로) 또는 소프트웨어(예를 들어, 프로그램된 제어기 또는 프로세서의 일부 방식을 통해) 중 어느 하나에서 선택적으로 실현가능하다는 것이 또한 이해된다. 다양한 실시예들에서의 특정한 변동물들은 파티셔닝하는데 있어서의 차이들, 상이한 폼 팩터들 및 구성들, 상이한 운영 시스템들 및 다른 시스템 소프트웨어의 사용, 상이한 인터페이스 표준들, 네트워크 프로토콜들, 또는 통신 링크들의 사용, 및 특정한 애플리케이션의 고유 엔지니어링 및 비즈니스 제약들에 따라 여기에 설명한 개념들을 구현할 때 기대되는 다른 변동물들을 포함하지만 이에 제한되지 않는다.

[0331] 실시예들은 설명한 실시예들의 많은 양태들의 최소의 구현을 위해 요구되는 바를 훨씬 넘어선 상세 및 환경적 컨텍스트로 설명되었다. 당업자는 일부 실시예들이 나머지 소자들 중에서 기본적인 협력을 변경하지 않고 개시된 컴포넌트들 또는 특징들을 생략한다는 것을 인식할 것이다. 따라서, 개시된 많은 상세들이 설명한 실시예들의 다양한 양태들을 구현하기 위해 요구되지 않는다는 것이 이해된다. 나머지 소자들이 종래 기술로부터 구별가능한 범위까지, 생략되는 컴포넌트들 및 특징들은 여기에 설명한 개념들을 제한하지 않는다.

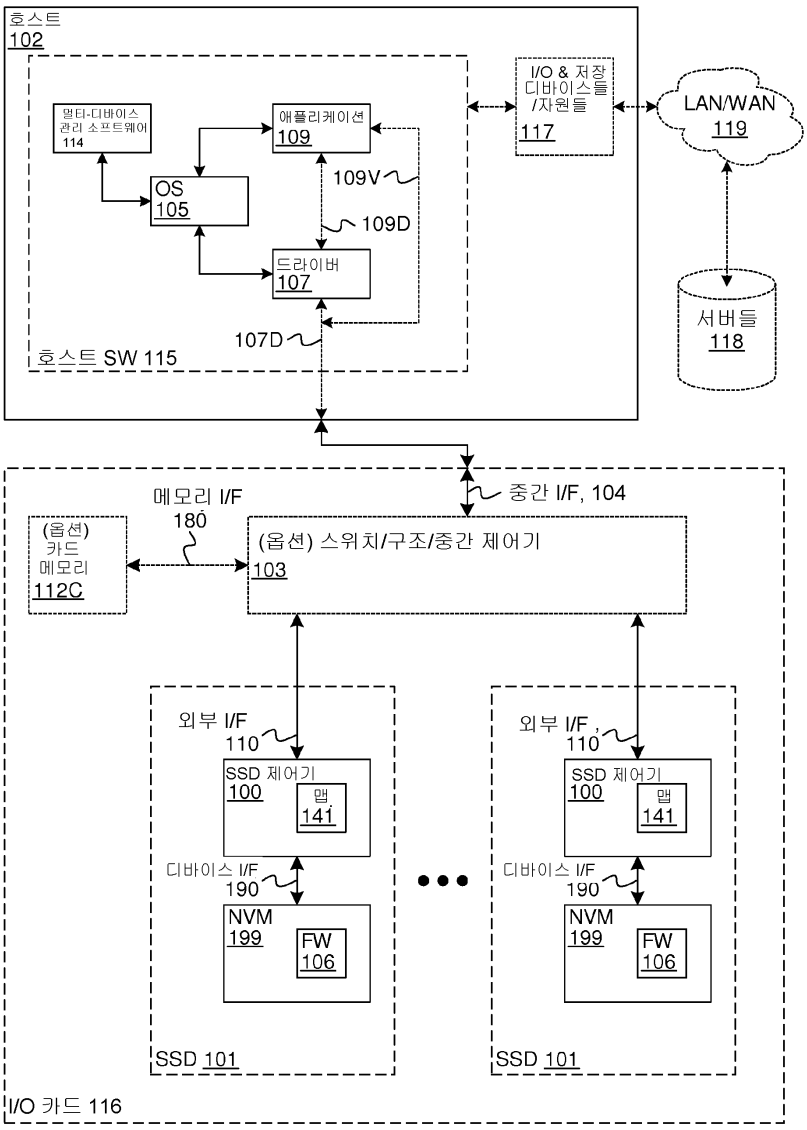
[0332] 설계에서의 모든 이러한 변동물들은 설명한 실시예들에 의해 전달된 교시들을 넘는 비현실적인 변경들이다. 여기에 설명한 실시예들이 다른 컴퓨팅 및 네트워킹 애플리케이션들에 대한 넓은 적용가능성을 가지며, 설명한 실시예들의 특정한 애플리케이션 또는 산업에 제한되지 않는다는 것이 또한 이해된다. 따라서, 본 발명은 등록특허의 청구항들의 범위내에 포함되는 모든 가능한 변경물들 및 변동물들을 포함하는 것으로 해석되어야 한다.

도면

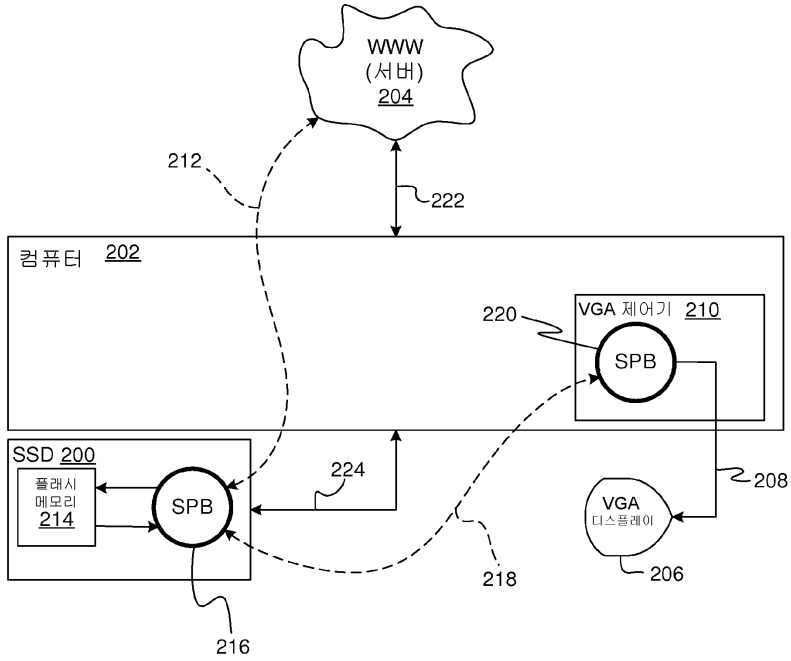
도면1a


외부 I/F, 110
SSD, 101
SSD 제어기 100
호스트 인터페이스 111
태그 트랙킹 113
데이터 프로세싱 121
엔진 123
버퍼 131
DMA 133
메모리 137
ECC-X 135
맵 141
테이블143
리사이클러151
ECC 161
디바이스 인터페이스 로직 191
스케줄링 193
CPU 171
CPU 코어172
명령
데이터
커맨드 관리 173
버퍼 관리 175
트랜슬레이션 관리 177
코히어런시 관리 179
디바이스 관리 181
ID 관리 182
디바이스 I/F, 190
NVM, 199
플래시 다이 194
플래시 디바이스,192
플래시 디바이스,192

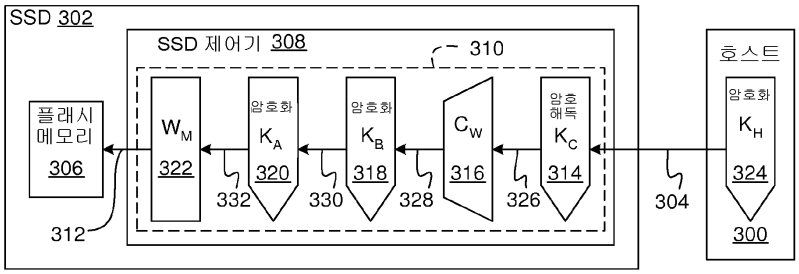
도면1b


호스트
102
멀티-디바이스
관리 소프트웨어
114
애플리케이션
109
OS
105
109V
109D
드라이버
107
107D
호스트 SW 115
I/O & 저장
디바이스들
/자원들
117
LAN/WAN
119
서버들
118
메모리 I/F
180
(옵션)
카드
메모리
112C
중간 I/F, 104
(옵션) 스위치/구조/중간 제어기
103
외부 I/F
110
SSD 제어기
100
맵
141
디바이스 I/F
190
NVM
199
FW
106
SSD 101
I/O 카드 116

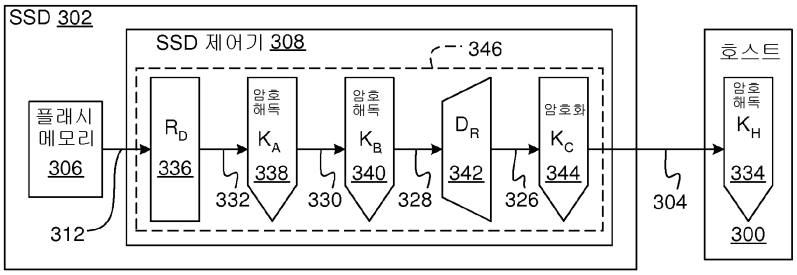
도면2



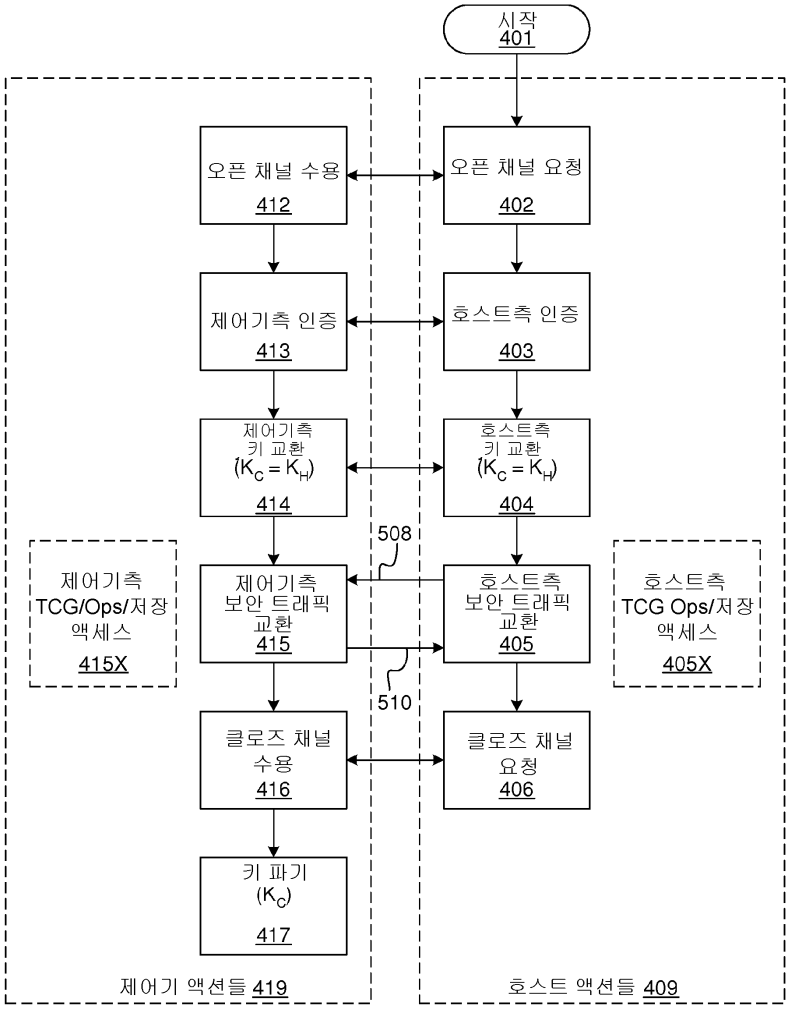
도면3a



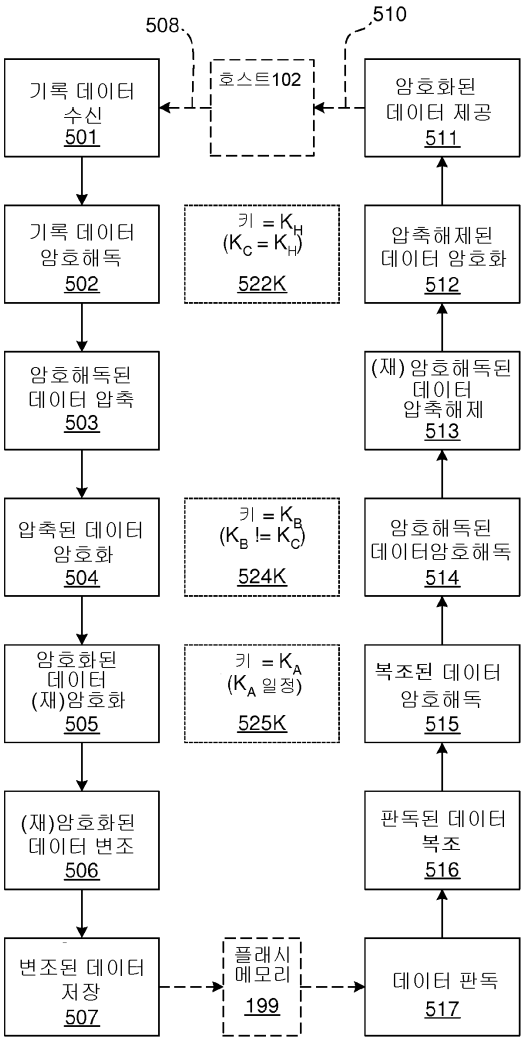
도면3b



도면4


시작
401
오픈 채널 수용
412
오픈 채널 요청
402
제어기측 인증
413
호스트측 인증
403
제어기측
키 교환
(Kc = KH)
414
호스트측
키 교환
(Kc = KH)
404
508
제어기측
TCG/Ops/저장
액세스
415X
제어기측
보안 트래픽
교환
415
호스트측
보안 트래픽
교환
405
호스트측
TCG Ops/저장
액세스
405X
510
클로즈 채널
수용
416
클로즈 채널
요청
406
키 파기
(Kc)
417
제어기 액션들 419
호스트 액션들 409

도면5


508
510
기록 데이터 수신 501
호스트102
암호화된 데이터 제공 511
기록 데이터 암호해독 502
키 = K_H ($K_C = K_H$) 522K
압축해제된 데이터 암호화 512
암호해독된 데이터 압축 503
(재) 암호해독된 데이터 압축해제 513
압축된 데이터 암호화 504
키 = K_B (K_B != K_C) 524K
암호해독된 데이터암호해독 514
암호화된 데이터 (재)암호화 505
키 = K_A (K_A 일정) 525K
복조된 데이터 암호해독 515
(재)암호화된 데이터 변조 506
판독된 데이터 복조 516
변조된 데이터 저장 507
플래시 메모리 199
데이터 판독 517