(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년08월02일
(11) 등록번호 10-1292927
(24) 등록일자 2013년07월29일

(51) 국제특허분류(Int. Cl.)
G09C 1/00 (2006.01) *G06F 17/00* (2006.01)
(21) 출원번호 10-2008-7009948
(22) 출원일자(국제) 2006년10월16일
심사청구일자 2011년10월11일
(85) 번역문제출일자 2008년04월25일
(65) 공개번호 10-2008-0063785
(43) 공개일자 2008년07월07일
(86) 국제출원번호 PCT/US2006/040538
(87) 국제공개번호 WO 2007/053295
국제공개일자 2007년05월10일
(30) 우선권주장
11/263,701 2005년11월01일 미국(US)
(56) 선행기술조사문헌
US6104811 A
US6757686 B1
US20050175176 A1
전체 청구항 수 : 총 16 항

(73) 특허권자
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
로터, 크리스틴 이.
미국 98052-6399 워싱턴주 레드몬드 원 마이크로소프트 웨이
찰스, 데니스 엑스.
미국 98052-6399 워싱턴주 레드몬드 원 마이크로소프트 웨이
고렌, 이알 즈비
미국 98052-6399 워싱턴주 레드몬드 원 마이크로소프트 웨이
(74) 대리인
제일특허법인

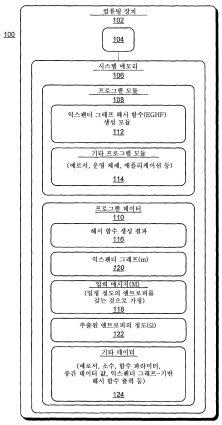
심사관 : 장상배

(54) 발명의 명칭 **익스팬더 그래프로부터의 해시 함수 생성**

(57) 요 약

익스팬더 그래프로부터의 해시 함수 생성이 기술된다. 일 양태로서, 익스팬더 그래프의 한 정점에서 다음 정점으로 진행하여 해시 함수를 계산한다. 익스팬더 그래프 상에서 입력 메시지의 각각의 부분집합들을 사용해 진행한다. 마지막으로 진행된 정점의 표지가 해시 함수의 출력이다.

대 표 도 - 도1



특허청구의 범위

청구항 1

해시 함수(hash function)에 대한 입력에 따라 익스팬더 그래프(expander graph)의 한 정점에서 다음 정점으로 진행(walking)하는 단계 - 상기 익스팬더 그래프 상에서 입력 메시지의 각각의 부분집합들을 사용해 진행하고, 상기 입력 메시지는 세그먼트(segment)로 분할되고, 상기 진행하는 단계에서 적어도 이들 세그먼트의 부분집합에 대하여, 부분집합의 특정 세그먼트의 특징에 기초하여 상기 익스팬더 그래프의 각각의 다음 정점(vertex)으로의 경로가 판정되고, 상기 익스팬더 그래프는 특성 p의 유한체(finite field)에 대한 초특이 타원 곡선의 그래프(graph of supersingular elliptic curves)를 포함함 - ;

마지막으로 진행된 정점의 표지(label)를 판정하는 단계; 및

상기 해시 함수의 결과로서 상기 표지를 출력하는 단계 - 상기 해시 함수는 충돌 회피성(collision resistant)임 - 를 포함하는

컴퓨터 구현 방법.

청구항 2

제1항에 있어서,

상기 익스팬더 그래프는 라마누잔 그래프(Ramanujan graph)를 더 포함하는 컴퓨터 구현 방법.

청구항 3

제1항에 있어서,

상기 익스팬더 그래프는 루보츠키-필립스-사르낙 익스팬더 그래프(Lubotzky-Phillips-Sarnak expander graph)를 더 포함하는 컴퓨터 구현 방법.

청구항 4

제1항에 있어서,

상기 결과는 암호화 해시(cryptographic hash)인 컴퓨터 구현 방법.

청구항 5

삭제

청구항 6

제1항에 있어서,

상기 입력 메시지는 일정 정도의 엔트로피(entropy)를 가지는 컴퓨터 구현 방법.

청구항 7

제1항에 있어서,

상기 익스팬더 그래프는 n개의 정점들을 포함하고, 상기 입력 메시지는 일정 정도의 엔트로피(a degree of entropy)를 가지며, 상기 방법은

상기 그래프의 정점들에 각각의 표지를 할당하는 단계; 및

상기 엔트로피의 정도를 판정하는 단계를 더 포함하고,

상기 진행하는 단계는 완전하게 랜덤인 정점 출력을 식별하기 위하여 상기 엔트로피의 정도를 사용해 상기 n개의 정점들을 진행하는 단계를 더 포함하며,

상기 출력은 상기 n개의 정점들 중에서 마지막으로 진행된 정점에 각각 할당된 표지이고, 이에 의해 상기 표지는 해시 함수의 결과인 컴퓨터 구현 방법.

청구항 8

제7항에 있어서,

상기 엔트로피의 정도(degree)를 판정하는 단계는 상기 입력 메시지와 연관된 랜덤니스(randomness)의 정도를 판정하기 위하여 추출 함수(extractor function)를 사용하는 단계를 더 포함하는 컴퓨터 구현 방법.

청구항 9

메시지를 세그먼트들로 분할하는 단계;

해시 함수에 대한 입력에 따라 익스팬더 그래프의 한 정점에서 다음 정점으로 진행하는 단계 - 상기 익스팬더 그래프 상에서 상기 익스팬더 그래프의 n개의 정점들 중 다음 정점으로의 경로를 판정하도록 상기 세그먼트들 중 하나를 각각 사용해 진행하고, 상기 익스팬더 그래프는 루보츠키-필립스-사르낙 익스팬더 그래프임 - ;

마지막으로 진행된 정점의 표지를 판정하는 단계; 및

상기 해시 함수의 결과로서 상기 표지를 출력하는 단계

를 위한 프로세서에 의해 실행될 수 있는 컴퓨터-프로그램 명령어(computer-programmed instructions)를 포함하는 컴퓨터 저장 매체.

청구항 10

제9항에 있어서,

상기 익스팬더 그래프는 라마누잔 그래프인 컴퓨터 저장 매체.

청구항 11

제9항에 있어서,

상기 결과는 암호화 해시인 컴퓨터 저장 매체.

청구항 12

제9항에 있어서,

상기 해시 함수는 충돌 회피성인, 컴퓨터 저장 매체.

청구항 13

제9항에 있어서,

상기 메시지로부터 추출된 엔트로피의 정도에 기초하여 상기 메시지가 상기 세그먼트로 분할되는 컴퓨터 저장 매체.

청구항 14

제9항에 있어서,

상기 익스팬더 그래프는 n개의 정점들을 포함하고, 상기 메시지는 일정 정도의 엔트로피를 가지며, 상기 컴퓨터-프로그램 명령어는

상기 그래프의 정점들에 각각의 표지를 할당하는 단계; 및

상기 엔트로피의 정도를 판정하는 단계를 위한 구조를 더 포함하고,

상기 진행하는 단계는 완전하게 랜덤인 정점 출력을 식별하기 위하여 상기 엔트로피의 정도를 사용해 상기 n개의 정점들을 따라 진행하는 단계를 포함하며,

상기 출력은 진행된 상기 n개의 정점들 중에서 마지막으로 진행된 정점에 각각 할당된 표지이고, 이에 의해 상기 표지는 해시 함수의 결과인 컴퓨터 저장 매체.

청구항 15

제14항에 있어서,

상기 엔트로피의 정도를 판정하는 단계를 위한 상기 컴퓨터 프로그램 명령어는 상기 메시지와 연관된 랜덤니스의 정도를 판정하기 위하여 추출 함수를 사용하는 단계를 위한 명령어를 더 포함하는 컴퓨터 저장 매체.

청구항 16

컴퓨팅 장치로서,

프로세서에 결합된 메모리를 포함하고,

상기 메모리는,

익스팬더 그래프의 n개의 정점들 중 각 정점에 표지를 할당하는 단계;

메시지를 세그먼트들로 분할하는 단계;

해시 함수에 대한 입력으로서 상기 익스팬더 그래프의 한 정점에서 다음 정점으로 진행하는 단계 - 상기 익스팬더 그래프 상에서 상기 익스팬더 그래프의 n개의 정점들 중 다음 정점으로의 경로를 판정하도록 상기 세그먼트들 중 하나를 각각 사용해 진행하고, 진행 경로에서 다음 정점(vertex)으로의 경로를 판정하는 것은 현재의 정점으로부터 어떤 변(edge)이 횡단(traverse)될 것인가를 판정하기 위하여 다음 세그먼트로부터 비트(bit)를 판독함으로써 수행되고, 상기 익스팬더 그래프는 특성 p의 유한체에 대한 초특이 타원 곡선의 그래프, 라마누잔 그래프 및 루보츠키-필립스-사르낙 익스팬더 그래프로 구성된 그룹에서 선택됨 - ;

상기 정점들 중에서 마지막으로 진행된 정점의 표지를 판정하는 단계; 및

상기 해시 함수의 결과로서 상기 표지를 출력하는 단계

를 위한 상기 프로세서에 의해 실행될 수 있는 컴퓨터-프로그램 명령어를 포함하는 컴퓨팅 장치.

청구항 17

제16항에 있어서,

상기 결과는 암호화 해시인 컴퓨팅 장치.

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 일반적으로 해시 함수의 생성에 관한 것이며, 보다 구체적으로는 익스팬더 그래프로부터 해시 함수를 생성하는 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 해시 함수 생성은 다수의 알고리즘 및 암호 프로토콜에서 사용된다. 해시 함수란 그 상을 "균일하게" 분포시키는 함수 f: U→S로서, |U|≥|S|인 경우를 말한다. 즉, 대부분의 x∈U에 대하여, |{y∈U|f(x)=y}|는 $\frac{|U|}{|S|}$에 가깝다.

[0003] 해시 함수는 충돌 쌍(colliding pairs), 즉 f(x)=f(y)인 (x, y) 쌍의 개수를 최소화하므로 매우 유용하다. 해시 함수가 암호화에 적용되는 경우, 충돌 처리 문제가 어려운 것이 통상 바람직하다. 이는 f(x)=f(y)를 만족하는 별개의 요소들인 x와 y를 찾는 작업이 계산상 어려운 것을 의미한다. 주로, 주어진 x에 대하여 f(x)=f(y)를 만족하는 상이한 y를 찾는 것이 어렵다는 좀더 취약한 속성이 주목받고 있다.

발명의 상세한 설명

[0004] **요약**

[0005] 본 요약은 이하의 상세한 설명에서 더 설명되는 기술적 사상의 선택을 단순화된 형태로 소개하기 위하여 제공된다. 본 요약은 청구된 기술적 사상의 중요 특징 또는 본질적인 특징을 식별하는 것으로 의도된 것이 아니며, 청구된 기술적 사상의 범위를 판정하는데 도움이 되도록 사용되는 것으로 의도된 것도 아니다.

[0006] 이러한 관점에서, 익스팬더 그래프로부터의 해시 함수 생성이 기술된다. 본 발명의 일 양태에서, 해시 함수에 대한 입력으로서 익스팬더 그래프의 한 정점에서 다음 정점으로 진행(walking)한다. 익스팬더 그래프 상에서 입력 메시지의 각 부분집합을 사용해 진행한다. 해시 함수의 출력은 마지막으로 진행된 정점(vertex)의 표지(label)이다.

실 시 예

[0012] **개관**

[0013] 익스팬더 그래프로부터 해시 함수를 생성하기 위한 (예컨대, 시스템, 장치, 컴퓨터 판독가능 매체 등의) 시스템 및 방법이 도 1 내지 4를 참조하여 이하에 기술된다. 특정 익스팬더 그래프 상의 진행 경로(walk)를 취함으로써 해시 함수가 생성된다. 익스팬더 그래프 상의 랜덤 워크(random walk)는 매우 신속하게 혼합되므로, 입력 메시지가 균일하게 랜덤이면 해시 함수 출력도 통상 균일하다. 일 구현에서, 시스템 및 방법은 익스팬더 그래프와 함께 추출기(extractors)를 사용하여 해시 함수를 산출한다. 이러한 구현에서, 입력 메시지는 최소 엔트로피에 대한 일정한 하위 경계를 갖는다. 예컨대, (해싱에 의해 이루어지는) 메시지에 대한 암호 서명은 메시지에 "랜덤 패드(random pad)"를 부가한 후에 이루어진다(이러한 프로세스는 서명에 엔트로피를 주입한다). 입력 메시지가 어떤 소량의 엔트로피를 갖는다는 가정 아래, 추출기가 이러한 랜덤니스(randomness)를 이용해 추출을 행한 후, 추출기의 출력에 따라 진행 경로를 만든다.

[0014] 익스팬더 그래프로부터 해시 함수를 생성하기 위한 시스템 및 방법의 이러한 양태 및 기타 양태가 이하에 상세하게 기술된다.

[0015] **예시적인 시스템**

[0016] 익스팬더 그래프로부터 해시 함수를 생성하기 위한 시스템 및 방법은 퍼스널 컴퓨터와 같은 컴퓨팅 장치에 의하여 실행되는 컴퓨터 실행가능 명령어(프로그램 모듈)와 관련하여 기술되지만, 이에 제한되지는 않는다. 프로그램 모듈은 일반적으로 특정 작업을 수행하거나 특정 추상 데이터 유형을 구현하는 루틴, 프로그램, 객체, 컴포넌트, 데이터 구조 등을 포함한다. 시스템 및 방법은 전술한 것들과 관련하여 기술되지만, 이하에 기술되는 행동 및 동작은 하드웨어로도 구현될 수 있다.

[0017] 도 1은 본 발명의 일 실시예에 따라 익스팬더 그래프로부터 해시 함수를 생성하기 위한 예시적인 시스템(100)을 도시한다. 시스템(100)은 시스템 메모리(106)에 결합된 하나 이상의 처리 장치(104)를 포함하는 컴퓨팅 장치(102)를 포함한다. 프로세서(104)는 프로그램 모듈(108)로부터 컴퓨터 프로그램 명령어를 추출 및 실행하며, 시스템 메모리(106)의 프로그램 데이터(110) 부분으로부터 데이터를 추출하거나, 그 부분에 데이터를 저장한다. 프로그램 모듈(108)은, 예컨대, 익스팬더 그래프 해시 함수 생성 모듈("EGHF 생성 모듈")(112) 및 기타 프로그램 모듈(114)을 포함한다. 기타 프로그램 모듈(114)은, 예컨대, 모듈(112)이 생성한 익스팬더 그래프-기반 해시 함수 생성 결과(116)를 이용하는 하나 이상의 애플리케이션 및 운영 체제를 포함한다. 이러한 해시 함수 생성 결과(116)가 유용하게 쓰이는 다수의 애플리케이션이 존재한다. 예컨대, 이러한 생성 결과는 암호 작성(crytography), 해시 테이블, 오류 정정, 오디오 식별, 래빈-카프 스트링 검색 알고리즘(Rabin-Karp string search algorithms) 등을 구현하는 하나 이상의 애플리케이션에서 이용될 수 있다.

[0018] EGHF 생성 모듈(112)은 입력 메시지(118) 및 정점을 n개 갖는 익스팬더 그래프(120)로부터 해시 함수 생성 결과를 생성한다. 익스팬더 그래프(118)는 정점 또는 변 익스팬션(vertex or edge expansion)이 높은 스파스 그래프(sparse graph)인데, 이는 고도로(highly) 연결되어 있다는 의미이다. 일 구현에서, 익스팬더 그래프(118)는 라마누잔 그래프(Ramanujan graph)이다. 일 구현에서, 입력 메시지는 (엔트로피 또는) 랜덤니스의 정도이다.

[0019] 예컨대, 일 구현에서, 익스팬더 그래프(120)는 다음과 같이 결정된다. p가 소수이고, ℓ($\neq$p)이 또 다른 소수라고 가정한다. $q=p^2$일 때, 유한체(finite field) F_q에 대한 초특이 j-불변량(supersingular j-invariant)의 집합이 익스팬더 그래프 G(p,ℓ)의 정점 집합 V가 된다. j-불변량이 j_1 및 j_2인 초특이 타원 곡선들 사이에 ℓ차 아이소지니(isogeny)가 존재하는 경우, 정점 j_1 및 j_2 사이에 변이 존재한다. 그래프 G(p,ℓ)은 ℓ+1 정규 라마누잔 그래프(Ramanujan graph)로 알려져 있다. G(p,ℓ)의 정점 개수는 대략 p/12인 사원 대수(quarternion algebra) $B_{p,\infty}$ 의 분류 번호(class number)와 같다. G(p,ℓ)이 익스팬더 그래프(120)이다.

[0020] 다른 구현에서, 이하의 "다른 실시예"이란 제목의 절에 기술되는 것처럼, 익스팬더 그래프(120)가 루보츠키-필립스-사르낙 익스팬더 그래프(Lubotzky-Phillips-Sarnak graph)이다.

[0021] 해시 함수(116)를 생성하기 위하여, 익스팬더 그래프 해시 함수 생성 모듈(112)이 메시지(118)를 식별한다. 일 구현에서, 메시지는 엔트로피를 갖는다. EGHF 생성 모듈(112)은 익스팬더 그래프(120)를 구성하는 n개의 정점들 중의 각 정점에 각각의 이름 또는 표지를 할당한다. 입력 메시지가 그것과 연관된 엔트로피를 가지는 경우, EGHF 생성 모듈(112)은 추출 함수를 이용해 그 랜덤니스의 정도를 추출(판정)한다. 이러한 메시지로부터 랜덤니스를 추출하는 예시적인 추출 함수 및 기술은 이하의 "입력으로부터의 랜덤니스 추출"이란 제목의 절에서 상세하게 기술된다.

[0022] 랜덤하게 진행되는(방문되는) 익스팬더 그래프(120)의 정점들을 식별하기 위한 설정가능한 정점 변 규약(vertex edge convention)을 고려하여, 생성 모듈(112)이 추출된 엔트로피의 정도(존재시) 또는 (이하 기술되는) 기타 객관적인 기준에 기초해 입력 메시지(118)의 k-길이 비트 세그먼트를 식별한다. 익스팬더 그래프(120)를 진행하는 예시적인 동작은 이하의 "예시적인 절차"라는 제목의 절에서 상세히 기술된다. 정점들 중에서 마지막으로 진행된 정점과 연관된 각 이름/표지는 해시 함수 생성 결과(114)의 출력을 나타낸다.

[0023] 입력으로부터의 랜덤니스 추출

[0024] 최소-엔트로피: X가 $\{0,1\}^n$에서 값을 취하는 확률 변수라고 가정한다. X의 최소 엔트로피의 양은 $\min_{x\in\{0,1\}^n}\left(-\log\left(\Pr[X=x]\right)\right)$의 양으로 정의된다.

[0025] 분포의 근접성(closeness): X 및 Y가 $\{0,1\}^d$에 대한 2개의 분포라고 가정한다. 아래와 같은 조건을 만족하는 경우, X 및 Y는 ε-근접하다고 말한다(ε는 실수).

[0026] $$\max_{x\in\{0,1\}^d}\left|\Pr[X=x]-\Pr[Y=x]\right|\le\varepsilon$$

[0027] 추출기: X가 적어도 k의 최소 엔트로피를 갖는 $\{0,1\}^n$ 상의 임의의 확률 변수이며 U_d가 $\{0,1\}^d$ 상의 균일 분포인 경우, 분포 $Ext(X,U_d)$가 U_m에 ε-근접하면, 함수 $Ext:\{0,1\}^n\times\{0,1\}^d\rightarrow\{0,1\}^m$를 (k,$\varepsilon$)-추출기로 지칭한다.

[0028] 정리(Proposition): $Ext:\{0,1\}^n\times\{0,1\}^d\rightarrow\{0,1\}^m$가 (k,$\varepsilon$)-추출기인 경우, 랜덤 시드(random seed) $\sigma\in\{0,1\}^d$의 대부분의 선택에 있어서, 분포 $Ext(X,\sigma)$는 U_m에 ε-근접하다.

[0029] 증명: 분포 $Ext(X,U_d)$는 $X_d=Ext(X,\sigma)$로 정의된 $\sigma\in\{0,1\}^d$에 의해 색인되는 X_d 족 분포들 사이에서 랜덤으로 균일하게 분포를 선택하는 것으로 설명될 수 있다. Ext가 추출기라는 사실로부터 이들 분포 중의 다수가 U_m에 ε-근접하다는 것이 도출된다(증명 끝).

[0030] d는 $\log^2 n$ 이상이고 $m=k^{1-\alpha}$이며 α는 임의의 실수인 경우, 모든 $k>n^r$ (γ<1) 및 ε>0에 대한 다항 시간 추출기의 생성 결과가 알려져 있다.

[0031] 해시 함수의 생성

[0032] n이 G(p, ℓ)의 정점 개수이고 β>0일 때, 해시 함수 생성 결과(116)에 대한 입력을 나타내는 확률 변수 M(즉, 입력 메시지(118))은 적어도 $\log^{1+\beta} n$의 최소-엔트로피를 가진다. $\{0,1\}^N$이 입력 공간이라 가정한다. M의 엔트로피의 정도(122)를 판정하기 위하여, 생성 모듈(112)은 추출 함수 *Ext*를 구현하고 함수 $Ext:\{0,1\}^N\times\{0,1\}^d\rightarrow\{0,1\}^m$을 $k=\log^{1+\beta} n$, 매우 작은 ε 및 $m=\Theta(\log^{1+\alpha} n)$이란 파라미터들을 이용해 수정한다. 예시적인 설명을 위해, 이러한 파라미터들은 "기타 데이터"(124)의 각 부분으로 도시된다. 시스템(100)은 $N=k^{O(1)}$임을 가정한다. 생성 모듈(112)은 $\{0,1\}^d$로부터 랜덤으로 균일하게 a를 선택한다. 입력이 $x\in\{0,1\}^N$으로 주어진 경우, 생성 모듈(112)은 ω=*Ext*(x,a), 즉, 엔트로피의 정도(122)를 계산한다. 이러한 생성의 결과는 크기 m의 스트링이다. 생성 모듈(122)은 어떤 고정된 정점 v_0에서 시작되어 ω에 의하여 주어진 방향으로 이어지는 m 상의 진행 경로를 만들고, 마지막으로 진행된 정점의 표지가 해시 함수의 출력(116)이 된다.

[0033] 익스팬더 그래프의 결절점(nodes)이 초특이 타원 곡선 modulo 소수 p이고, 변이 원형 곡선들 사이의 ℓ차 아이소지니인 경우, 그 그래프에 대한 진행 경로는 다음과 같이 진행될 수 있다.

[0034] 타원 곡선 E에 대응하는 결절점에서 시작하여, $E[\ell]$의 ℓ-토션(ℓ-torsion)의 생성원 P 및 Q를 먼저 찾아야 한다. 이를 위해:

[0035] 1. n이 $F_q(E[\ell])\subseteq F_{q^n}$ 을 만족한다고 가정한다.

[0036] 2. E에 대한 유리 점(rational point) F_{q^n} 의 개수가 $S=\#E(F_{q^n})$ 라고 가정한다.(Original)

[0037] 3. ℓ^k가 S를 나누는 가장 큰 ℓ의 거듭 제곱일 때, $s=S/\ell^k$로 설정한다.

[0038] 4. $E[\ell]$로부터 랜덤으로 2개의 점 U, V를 선택한다:

[0039] (a) $E(F_{q^n})$ 에서 랜덤으로 2개의 점 U, V를 선택한다.

[0040] (b) $P'=sU$ 및 $Q'=sV$로 놓고, P' 또는 Q'이 O와 동일한 경우 (i)단계를 반복한다.

[0041] (c) $\ell^{i_1}P'\neq O$ 이고 $\ell^{i_2}Q'\neq O$ 이지만, $\ell^{i_1+1}P'=O$ 이고 $\ell^{i_2+1}Q'=O$ 인 최소의 i_1, i_2를 찾는다.

[0042] (d) $P=\ell^{i_1}P'$ 및 $Q=\ell^{i_2}Q'$ 로 설정한다.

[0043] 5. 주지된 샹크스의 베이비-스텝-자이언트-스텝 알고리즘(Shanks's Baby-steps-Giant-steps algorithm)을 이용해, Q가 P에 의해 생성된 군에 속하는지 여부를 판정한다. 속하는 경우, (d)단계가 반복된다.

[0044] E에 대해 동형인(isogenous) ℓ+1 타원 곡선의 F_{p^2} 에서의 j-불변량은 j_1, …, $j_{\ell+1}$이다. 이것들을 찾기 위하여:

[0045] (a) $1\leq i\leq\ell$인 경우 $G_1=<Q>$ 및 $G_{1+i}=<P+(i-1)*Q>$ 라고 가정한다.

[0046] (b) $1\leq i\leq\ell+1$인 각각의 i에 대하여, 벨루의 공식(Velu's formula)을 이용해 타원 곡선 E/G_i의 j-불변량을 계산한다.

[0047] 2-아이소지니들을 갖는 초특이 원형 곡선들의 그래프를 사용하는 경우, 예컨대, 다음의 명시적인 방식으로 랜덤 워크를 수행할 수 있다: 각 스텝마다, E 상의 의미 있는 2-비틀림 점(non-trivial 2-torsion point)을 3개 찾은 후, 그것들을 사전-지정된 방식으로 x축에 관하여 배열한다. 나아가, 진행 경로의 다음 결절점을 얻음으로써 어떤 점이 타원 곡선의 계수로 선택되는지를 판정하기 위하여 해시 함수에 대한 입력 비트를 사용한다.

[0048] 해시 함수의 출력은 거의 균일하다는 것에 대한 증명

[0049] 익스팬더 그래프 해시 함수 생성 모듈(112)에 의하여 구현되는 추출 함수의 출력은 거의 균일하다는 정리에 따르면, 본 예시적인 시스템에 의해 익스팬더 그래프 상에서 수행되는 진행 경로는 랜덤 워크에 매우 근접하다. (진행 경로가 랜덤이라는 것은, 그래프 상의 어떤 정점 v으로 진행되는 경우, 다음 스텝에서 어떤 정점으로 진행될 확률이 인접 정점 모두에 대해 동일하다는 것을 의미한다.) 이제, 그래프 G(p, ℓ)는 n개의 정점을 가지며 $m=\Omega(\log^{1+\alpha} n)$이므로, 진행 경로는 신속하게 혼합되어 출력 정점이 균일한 경우에 매우 근접하다. 이 문장의 의미는 이하에 명확하게 나타난다. 정점을 n개 갖는 d-정규 그래프 G 상의 스텝이 O(log n) 개인 랜덤 진행 경로가 신속하게 혼합됨을 나타내는 하나의 방식은

[0050] $$\left\| \left(\frac{1}{d}A\right)^{O(\log n)} \cdot v - \frac{1}{n}\vec{1} \right\| \le \varepsilon$$

[0051] 라고 표현하는 것이며, 여기에서 ε은 작고, A는 G의 인접 행렬(adjacency matrix)이며, v는 표준 단위 벡터들 중에서 임의의 것으로 선택될 수 있고, $\vec{1}$는 벡터 (1, 1, …, 1)이다. 행렬 $\frac{1}{d}A$는 그래프(120) 상의 균일하게 랜덤인 마코브 체인(Marcov chain)의 천이 행렬(transition matrix)을 의미할 수 있다. 이 구현에서, 시스템(100)은 그래프(120) 상의 거의 랜덤인 진행 경로를 구현한다. 이것은

[0052] $$\left\| \frac{1}{d}A - B \right\| \le \delta$$

[0053] 이고, δ가 작은 실수가 되도록, 천이 행렬로서 행렬 B를 사용하는 것을 의미할 수 있다(기호 ‖ ‖는 행렬 놈(matrix norm)을 의미함). 즉, 생성 모듈(112)은 랜덤 워크를 다소 교란한다. 이하의 정리는 δ가 충분히 작게 선택될 수 있다면, 이러한 새로운 랜덤 워크가 신속하게 혼합됨을 보일 것이다.

[0054] 정리: A 및 B가 2개의 하위-확률 행렬(sub-stochastic matrix)이라 가정하면, $\| A^k - B^k \| \le k \| A - B \|$이다.

[0055] 증명: 차 $A^k - B^k$는 $\sum_{0 \le i \le k-1} A^{k-i-1}(A-B)B^i$ 로 표현될 수 있다. 양 변의 놈을 구하고, (A 및 B가 하위-확률 행렬이므로) ‖ A ‖ = ‖ B ‖ = 1이라는 사실을 이용함으로써, 결과를 얻을 수 있다.(증명 끝)

[0056] 본 예시적인 시스템에 의해 수행되는 랜덤 워크의 길이는 O(log n)이다. 따라서, 파라미터 δ가 $O\left(\frac{1}{\log^2 n}\right)$이 되도록 구성될 수 있는 경우에는, 산출되는 유사 랜덤 워크가 신속하게 혼합될 것이다. 이것은 추출기의 파라미터 ε를 $O\left(\frac{1}{\log^2 n}\right)$과 같도록 설정함으로써 구성될 수 있다.

[0057] 충돌 회피성

[0058] 이러한 해시 함수(116) 하의 충돌을 직접적으로 찾아내는 것은 동일한 ℓ-거듭제곱 차의 초특이 타원 곡선 쌍 사이의 2개의 아이소지니를 찾아내는 것과 동등하다. 곡선들 사이의 높은 차수의 아이소지니들을 생성하는 것

은 계산이 어려운 문제라고 잘 알려진 것처럼, 그래프 $G(p,\ell)$가 작은 주기를 갖지 않는 한, 이러한 문제는 매우 어려운 것이다.

[0059] **다른 실시예**

[0060] 상기 기술된 그래프 $G(p,\ell)$를 사용하는 것에 대한 대안으로서, 시스템(100)은 루보츠키-필립스-사르낙 익스팬더 그래프(120)를 이용한다. ℓ 및 p는 2개의 별개의 소수이며, ℓ은 작은 소수이고, p는 상대적으로 크다고 가정한다. 또한, p 및 ℓ은 1 mod 4이라고, ℓ은 평방 잉여(quadratic residue) mod p라고 가정한다(이는 $\ell^{(p-1)/2}\equiv 1 \bmod p$인 경우이다). 파라미터 ℓ 및 p를 갖는 LPS 그래프는 $X_{\ell,p}$로 표시된다. 다음으로, 그래프 $X_{\ell,p}$를 구성하는 정점 및 변이 정의된다. $X_{\ell,p}$의 정점은 $PSL(2,F_p)$의 행렬, 즉 임의의 행렬 A에 대하여 $A=-A$의 등가 관계가 성립하고 행렬식이 1인 F_p의 성분(entry)을 갖는 가역적인 2x2 행렬이다. 행렬식이 1인 2x2 행렬 A에 대해, 집합 $\{0, \cdots, p-1\}^4$의 통상의 배열에서 사전편찬법적으로(lexicographically) 어느 쪽이 더 작은 지에 따라 그 정점을 위한 이름이 A의 성분들의 4-튜플 또는 $-A$의 성분들의 4-튜플이 될 것이다. 다음으로, 그래프를 구성하는 변이 설명된다. g_i가 이하에 명시적으로 정의된 행렬일 때, 행렬 A는 행렬 g_iA로 연결된다. i를 $i^2\equiv -1 \bmod p$를 만족시키는 정수라고 가정한다. 방정식 $g_0^2+g_1^2+g_2^2+g_3^2=\ell$에 대해, $8(\ell+1)$개의 해 $g=(g_0, g_1, g_2, g_3)$가 존재한다. 이러한 해들 중에서, $g_0>0$이고 g_0이 홀수이며, j=1, 2, 3일 때 g_j가 짝수인 것은 정확히 $\ell+1$개가 존재한다. 이러한 g 각각에 대해, 이하의 행렬을 연관시킨다.

[0061] $$\begin{pmatrix} g_0+ig_1 & g_2+ig_3 \\ -g_2+ig_3 & g_0-ig_1 \end{pmatrix}$$

[0062] 이에 따라, $PSL(2,F_p)$의 $\ell+1$개 행렬의 집합 S를 얻게 된다. $\mathbf{g}_i$는 이러한 집합 S에 속하는 행렬을 나타낸다. $\mathbf{g}$가 S에 속하면, $\mathbf{g}^{-1}$도 그러함은 자명하다. 나아가, ℓ이 작으므로, 행렬들의 집합 S를 철저한 검색에 의해 매우 신속하게 찾아낼 수 있다.

[0063] **예시적인 절차**

[0064] 도 2는 본 발명의 일 실시예에 따라 익스팬더 그래프로부터 해시 함수를 생성하기 위한 예시적인 절차를 도시한다. 예시적인 설명을 위해, 절차(200)의 동작들은 도 1의 시스템(100)의 컴포넌트를 참조하여 설명된다. 컴포넌트 참조 번호의 첫째 자리 숫자는 그 컴포넌트가 최초로 나타난 특정 도면을 식별한다.

[0065] 블록(202)에서, EGHF 생성 모듈(112)(도 1)이 입력 메시지(118)를 세그먼트로 분할한다. 예컨대, 입력 메시지는 길이 N을 가진다. k-정규 익스팬더 그래프(120)에 정점이 n개 존재하는 경우(각 정점은 이름/표지를 가짐), 하나의 임의의 정점으로부터 나오는 각 변의 이름은 log k개의 비트를 가질 것이다. 입력 메시지(118)는 log k 길이의 청크들(chunks)로 쪼개어진다. 블록(204)에서, EGHF 생성 모듈(112)은 해시 함수에 대한 입력으로서 익스팬더 그래프(120) 상을 진행한다. 진행 경로는 다음과 같이 판정된다. 어떤 정점 v에서, 정점 v로부터 횡단할 변을 판정하기 위하여, 입력으로부터 다음 청크의 log k개의 비트를 판독함으로써 이러한 변의 다른 끝점인 진행 경로의 다음 정점을 판정한다. 예컨대, EGHF 생성 모듈(112)은 입력 메시지(118)의 첫 번째 k개의 비트(세그먼트/청크)에 의해 특정된 첫 번째 정점으로부터 익스팬더 그래프(120)의 변에 대한 랜덤 워크를 시작한다. 익스팬더 그래프(120)에서 다음으로 진행되는 정점은 다음 log k 개의 비트 청크에 의해 특정된다. 이러한 동작들이 익스팬더 그래프(120)에서 변의 이름이 정점들에 대응하는 방식을 특정하는 규약을 고려하여 반복하여 수행된다. 이러한 규약 중의 일례는 각 정점 v에 대하여 함수 $f_v:\{1, \cdots, k\}\rightarrow E$가 존재한다는 것이다. 즉, $f_v(1)$은 v로부터의 첫 번째 변, $f_v(2)$는 v로부터의 두 번째 변 등임을 의미한다.

[0066] 블록(206)에서, EGHF 생성 모듈(112)은 마지막으로 진행된 정점의 표지를 판정한다. 블록(208)에서, EGHF 생성 모듈(112)는 그 표지를 해시 함수의 결과로서 출력한다.

[0067] 도 3은 본 발명의 일 실시예에 따라 익스팬더 그래프로부터 해시 함수를 생성하기 위한 예시적인 절차를 도시한다. 예시적인 설명을 위해, 절차(300)의 동작들은 도 1의 시스템(100)의 컴포넌트를 참조하여 설명된다. 블록

(302)에서, 익스팬더 그래프 해시 함수 생성 모듈("EGHF 생성 모듈")(112)(도 1)이 엔트로피를 갖는 메시지(118)를 식별한다. 블록(304)에서, EGHF 생성 모듈(112)이 익스팬더 그래프(120)의 각 정점에 각각의 표지를 할당한다. 블록(306)에서, EGHF 생성 모듈(112)이 추출 함수를 이용하여 입력 메시지(118)의 엔트로피의 정도를 판정한다. 이렇게 판정된 정도가 추출된 엔트로피의 정도(122)로서 도시되어 있다. 블록(308)에서, EGHF 생성 모듈(112)은 추출된 엔트로피의 정도(122)에 기초하여 익스팬더 그래프(120)를 진행한다. 블록(310)에서, EGHF 생성 모듈(112)이 익스팬더 그래프(120) 및 마지막으로 진행된 정점과 연관된 표지를 해시 함수 생성의 결과(116)로서 출력한다. 즉, 블록(302) 내지 블록(310)의 동작들은 해시 함수 생성 결과(116)를 위한 동작들에 해당한다.

[0068] **예시적인 운영 환경**

[0069] 도 4는 익스팬더 그래프로부터의 해시 함수 생성이 전체적으로 또는 부분적으로 구현될 수 있는 적합한 컴퓨팅 시스템 환경의 예를 도시한다. 예시적인 컴퓨팅 환경(400)은 도 1의 예시적인 시스템 및 도 2와 도 3의 예시적인 동작들에 대해 적합한 컴퓨팅 환경의 일례에 불과하며, 본 명세서에 기술된 시스템 및 방법의 용도 또는 기능성의 범위에 대한 어떤 제한을 제안하는 것으로 의도된 것이 아니다. 또한, 컴퓨팅 환경(400)이 컴퓨팅 환경(400)에 도시된 컴포넌트들 중 임의의 하나 또는 그 컴포넌트들의 임의의 조합과 관련하여 어떤 의존성이나 요구사항을 갖는 것으로 해석되어서도 안된다.

[0070] 본 명세서에 기술된 방법 및 시스템은 많은 기타 범용 또는 특수 목적의 컴퓨팅 시스템, 환경 또는 구성을 이용해 동작할 수 있다. 사용하는데 적합할 수 있는 잘 알려진 컴퓨팅 시스템, 환경 및/또는 구성의 예로서, 퍼스널 컴퓨터, 서버 컴퓨터, 멀티프로세서 시스템, 마이크로프로세서-기반 시스템, 네트워크 PC, 미니컴퓨터, 메인프레임 컴퓨터, 상기 시스템들이나 장치들 중 임의의 것을 포함하는 분산 컴퓨팅 환경, 기타 등등이 있지만 이에 제한되는 것은 아니다. 또한, 소형 버전 또는 부분집합 버전의 프레임워크가 핸드헬드 컴퓨터 또는 기타 컴퓨팅 장치와 같은 자원이 제한된 클라이언트에 구현될 수 있다. 본 발명은 통신 네트워크를 통해 연결된 원격 처리 장치에 의해 작업이 수행되는 분산 컴퓨팅 환경에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 로컬 및 원격 메모리 저장 장치 모두에 위치할 수 있다.

[0071] 도 4와 관련하여, 익스팬더 그래프로부터 해시 함수를 생성하기 위한 예시적인 시스템은, 예컨대, 도 1의 시스템(100)을 구현하는 컴퓨터(410)의 형태로 범용 컴퓨팅 장치를 포함한다. 이하에 기술되는 컴퓨터(410)의 양태는 도 1의 컴퓨팅 장치(102)의 예시적인 구현이다. 컴퓨터(410)의 컴포넌트들은 처리 장치(420), 시스템 메모리(430), 및 시스템 메모리를 비롯한 각종 시스템 컴포넌트들을 처리 장치(420)에 연결시키는 시스템 버스(421)를 포함할 수 있지만 이에 제한되는 것은 아니다. 시스템 버스(421)는 메모리 버스 또는 메모리 컨트롤러, 주변 장치 버스 및 각종 버스 아키텍처 중 임의의 것을 이용하는 로컬 버스를 비롯한 몇몇 유형의 버스 구조 중 어느 것이라도 될 수 있다. 예로서, 이러한 아키텍처는 ISA(Industry Standard Architecture) 버스, MCA(Micro Channel Architecture) 버스, EISA(Enhanced ISA) 버스, VESA(Video Electronics Standard Association) 로컬 버스, 그리고 메자닌 버스(mezzanine bus)로도 알려진 PCI(Peripheral Component Interconnect) 버스 등을 포함하지만 이에 제한되는 것은 아니다.

[0072] 컴퓨터(410)는 통상적으로 각종 컴퓨터 판독가능 매체를 포함한다. 컴퓨터(410)에 의해 액세스 가능한 매체는 그 어떤 것이든지 컴퓨터 판독가능 매체가 될 수 있고, 이러한 컴퓨터 판독가능 매체는 휘발성 및 비휘발성 매체, 이동식 및 비이동식 매체를 포함한다. 예로서, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 포함하지만 이에 제한되는 것은 아니다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보를 저장하는 임의의 방법 또는 기술로 구현되는 휘발성 및 비휘발성, 이동식 및 비이동식 매체를 포함한다. 컴퓨터 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 기타 메모리 기술, CD-ROM, DVD(digital versatile disk) 또는 기타 광 디스크 저장 장치, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 또는 기타 자기 저장 장치, 또는 컴퓨터(410)에 의해 액세스되고 원하는 정보를 저장하는데 사용될 수 있는 임의의 기타 매체를 포함하지만 이에 제한되는 것은 아니다.

[0073] 통신 매체는 통상적으로 반송파(carrier wave) 또는 기타 전송 메커니즘(transport mechanism)과 같은 피변조 데이터 신호(modulated data signal)에 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터 등을 구현하고 모든 정보 전달 매체를 포함한다. "피변조 데이터 신호"라는 용어는, 신호 내에 정보를 인코딩하도록 그 신호의 특성들 중 하나 이상을 설정 또는 변경시킨 신호를 의미한다. 예로서, 통신 매체는 유선 네트워크 또는 직접 배선 접속(direct-wired connection)과 같은 유선 매체, 그리고 음향, RF, 적외선, 기타 무선

매체와 같은 무선 매체를 포함하지만, 이에 제한되는 것은 아니다. 상술된 매체들의 모든 조합이 또한 컴퓨터 판독가능 매체의 범위 내에 포함되는 것으로 한다.

[0074] 시스템 메모리(430)는 판독 전용 메모리(ROM)(431) 및 랜덤 액세스 메모리(RAM)(432)와 같은 휘발성 및/또는 비휘발성 메모리 형태의 컴퓨터 저장 매체를 포함한다. 시동 중과 같은 때에, 컴퓨터(410) 내의 구성요소들 사이의 정보 전송을 돕는 기본 루틴을 포함하는 기본 입/출력 시스템(BIOS)(433)은 통상적으로 ROM(431)에 저장되어 있다. RAM(432)은 통상적으로 처리 장치(420)가 즉시 액세스 할 수 있고 및/또는 현재 동작시키고 있는 데이터 및/또는 프로그램 모듈을 포함한다. 예로서, 도 4는 운영 체제(434), 애플리케이션 프로그램(435), 기타 프로그램 모듈(436) 및 프로그램 데이터(437)를 도시하고 있지만 이에 제한되는 것은 아니다.

[0075] 컴퓨터(410)는 또한 기타 이동식/비이동식, 휘발성/비휘발성 컴퓨터 저장 매체를 포함한다. 단지 예로서, 도 4는 비이동식·비휘발성 자기 매체에 기록을 하거나 그로부터 판독을 하는 하드 디스크 드라이브(441), 이동식·비휘발성 자기 디스크(432)에 기록을 하거나 그로부터 판독을 하는 자기 디스크 드라이브(431), CD-ROM 또는 기타 광 매체 등의 이동식·비휘발성 광 디스크(436)에 기록을 하거나 그로부터 판독을 하는 광 디스크 드라이브(433)를 포함한다. 예시적인 운영 환경에서 사용될 수 있는 기타 이동식/비이동식, 휘발성/비휘발성 컴퓨터 저장 매체로는 자기 테이프 카세트, 플래시 메모리 카드, DVD, 디지털 비디오 테이프, 고상(solid state) RAM, 고상 ROM 등이 있지만 이에 제한되는 것은 아니다. 하드 디스크 드라이브(441)는 통상적으로 인터페이스(440)와 같은 비이동식 메모리 인터페이스를 통해 시스템 버스(421)에 접속되고, 자기 디스크 드라이브(431) 및 광 디스크 드라이브(433)는 통상적으로 인터페이스(430)와 같은 이동식 메모리 인터페이스에 의해 시스템 버스(421)에 접속된다.

[0076] 위에서 설명되고 도 4에 도시된 드라이브들 및 이들과 관련된 컴퓨터 저장 매체는, 컴퓨터(110)에 대한 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 및 기타 데이터를 저장한다. 도 4에서, 예를 들어, 하드 디스크 드라이브(441)는 운영 체제(444), 애플리케이션 프로그램(443), 기타 프로그램 모듈(446), 및 프로그램 데이터(447)를 저장하는 것으로 도시되어 있다. 이들 컴포넌트가 운영 체제(434), 애플리케이션 프로그램(433), 기타 프로그램 모듈(436), 및 프로그램 데이터(437)와 동일하거나 그와 다를 수 있다는 것을 유의하여야 한다. 애플리케이션 프로그램(433)은, 예컨대, 도 1의 컴퓨팅 장치(102)의 프로그램 모듈(108)을 포함한다. 프로그램 데이터(437)은, 예컨대, 도 1의 컴퓨팅 장치(102)의 프로그램(110)을 포함한다. 운영 체제(444), 애플리케이션 프로그램(443), 기타 프로그램 모듈(446) 및 프로그램 데이터(447)에 다른 번호가 부여되어 있다는 것은 적어도 이들이 다른 사본(copy)이라는 것을 나타내기 위한 것이다.

[0077] 사용자는 일반적으로 마우스, 트랙볼(trackball) 또는 터치 패드로 지칭되는 포인팅 장치(461) 및 키보드(462) 등의 입력 장치를 통해 명령 및 정보를 컴퓨터(410)에 입력할 수 있다. 기타 입력 장치(도시 생략)에는 마이크로폰, 조이스틱, 게임 패드, 위성 접시, 스캐너 등이 포함될 수 있다. 이들 및 기타 입력 장치는 주로 시스템 버스에 결합된 사용자 입력 인터페이스(460)를 통해 처리 장치(420)에 접속되지만, 병렬 포트, 게임 포트 또는 USB(universal serial bus) 등의 다른 인터페이스 및 버스 구조에 의해 접속될 수도 있다.

[0078] 또한, 모니터(491) 또는 다른 유형의 디스플레이 장치가 비디오 인터페이스(490) 등의 인터페이스를 통해 시스템 버스(421)에 접속될 수 있다. 모니터 외에도, 컴퓨터는 프린터(496) 및 오디오 장치(497) 등의 기타 주변 출력 장치를 포함할 수 있고, 이들은 출력 주변장치 인터페이스(493)를 통해 접속될 수 있다.

[0079] 컴퓨터(410)는 원격 컴퓨터(480)와 같은 하나 이상의 원격 컴퓨터로의 논리적 접속을 사용하여 네트워크화된 환경에서 동작할 수 있다. 일 구현에서, 원격 컴퓨터(480)는 도 1의 컴퓨팅 장치(102) 또는 네트워크화된 컴퓨터(104)를 나타낸다. 원격 컴퓨터(480)는 퍼스널 컴퓨터, 서버, 라우터, 네트워크 PC, 피어 장치 또는 기타 통상의 네트워크 노드일 수 있고, 도 4에는 메모리 저장 장치(481)만이 도시되었지만, 그것의 특정 구현의 기능으로서, 컴퓨터(410)와 관련하여 상술된 구성요소들의 대부분 또는 그 전부를 포함할 수 있다. 도 4에 도시된 논리적 접속은 로컬 영역 네트워크(LAN)(471) 및 광대역 네트워크(WAN)(473)를 포함하지만, 기타 네트워크를 포함할 수도 있다. 이러한 네트워킹 환경은 사무실, 전사적 컴퓨터 네트워크(enterprise-wide computer network), 인트라넷 및 인터넷에서 일반적인 것이다.

[0080] LAN 네트워킹 환경에서 사용될 때, 컴퓨터(410)는 네트워크 인터페이스 또는 어댑터(470)를 통해 LAN(471)에 접속된다. WAN 네트워킹 환경에서 사용될 때, 컴퓨터(410)는 통상적으로 인터넷과 같은 WAN(473)을 통하여 통신을 설정하기 위한 모뎀(472) 또는 기타 수단을 포함한다. 내장형 또는 외장형일 수 있는 모뎀(472)은 사용자 입력 인터페이스(460) 또는 기타 적절한 메커니즘을 통해 시스템 버스(421)에 접속된다. 네트워크화된 환경에서, 컴퓨터(410) 또는 그의 일부와 관련하여 기술된 프로그램 모듈은 원격 메모리 저장 장치에 저장될 수 있다.

예로서, 도 4는 원격 애플리케이션 프로그램(483)이 메모리 장치(481)에 상주하는 것으로 도시하고 있지만 이에 제한되는 것은 아니다. 도시된 네트워크 접속은 예시적인 것이며 이 컴퓨터들 사이에 통신 링크를 설정하는 기타 수단이 사용될 수 있다.

[0081] **결론**

[0082] 익스팬더 그래프로부터 해시 함수를 생성하기 위한 시스템 및 방법이 구조적 특징 및/또는 방법론적 동작이나 행동에 특화된 언어로 기술되었지만, 이하의 청구항에 정의되는 본 발명의 기술적 사상이 기술된 특정 특징 또는 동작으로 제한될 필요가 없음을 이해하여야 한다. 오히려, 지금까지 기술된 시스템(100)의 특정 특징 및 동작은 청구된 기술적 사상을 구현하기 위한 예시적인 형태로서 개시된 것이다.

도면의 간단한 설명

[0007] 도면에서, 컴포넌트 참조 번호의 첫째 자리 숫자는 그 컴포넌트가 최초로 나타난 특정 도면을 식별한다.

[0008] 도 1은 본 발명의 일 실시예에 따라 익스팬더 그래프로부터 해시 함수를 생성하기 위한 예시적인 시스템을 도시한 도면.

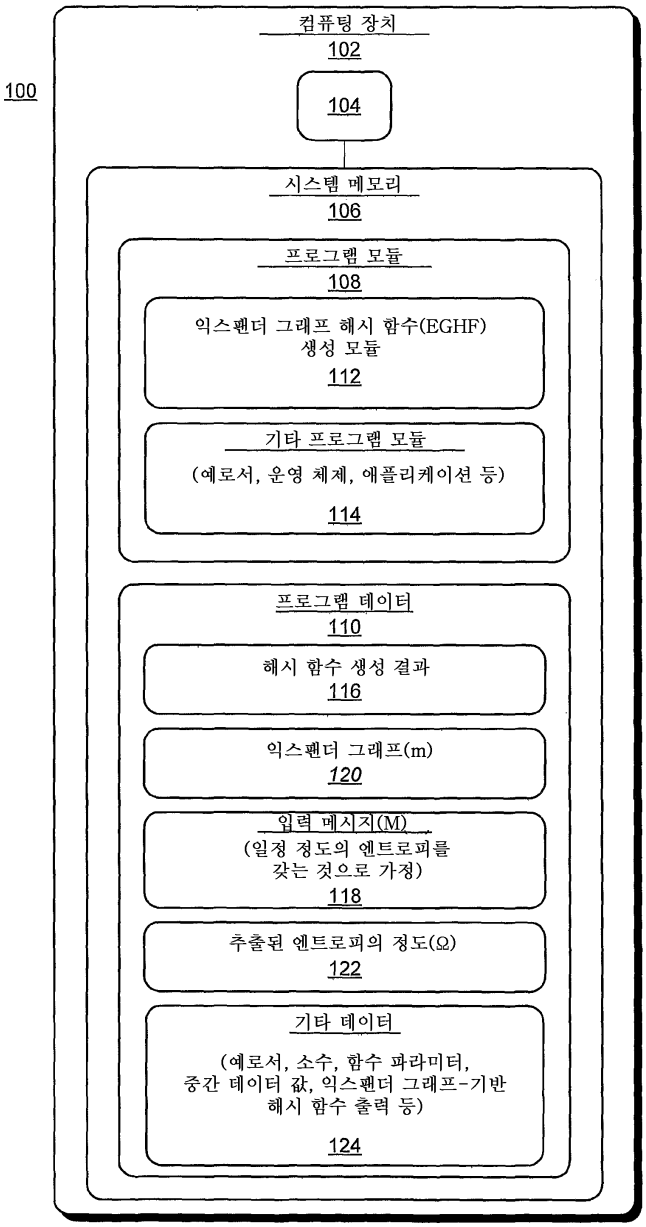
[0009] 도 2는 본 발명의 일 실시예에 따라 익스팬더 그래프로부터 해시 함수를 생성하기 위한 예시적인 절차를 도시한 도면.

[0010] 도 3은 본 발명의 일 실시예에 따라 익스팬더 그래프로부터 해시 함수를 생성하기 위한 예시적인 절차를 도시한 도면.

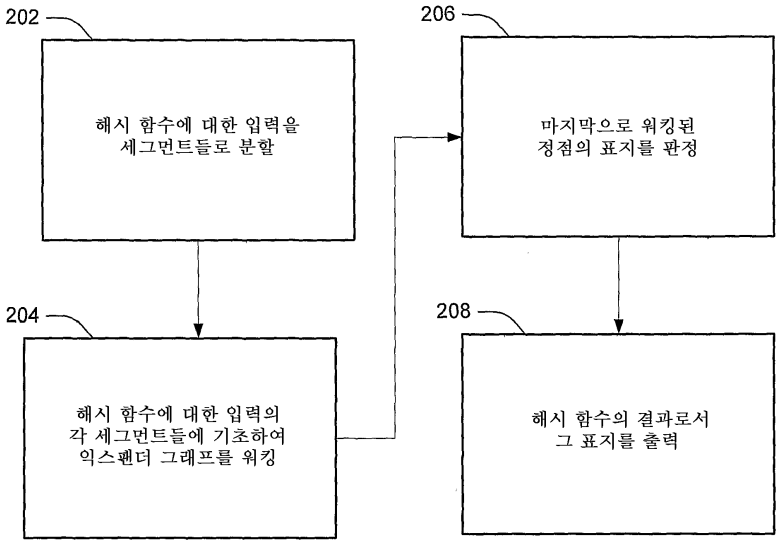
[0011] 도 4는 익스팬더 그래프로부터의 해시 함수 생성이 전체적으로 또는 부분적으로 구현될 수 있는 적합한 컴퓨팅 환경의 예를 도시한 도면.

도면

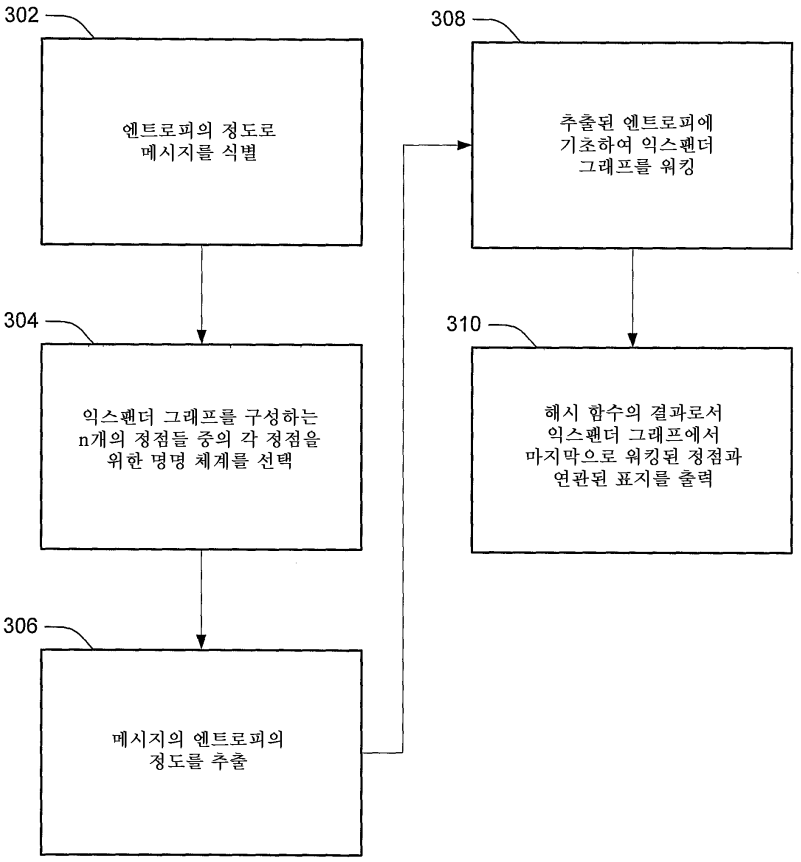
도면1


100
컴퓨팅 장치
102
104
시스템 메모리
106
프로그램 모듈
108
익스팬더 그래프 해시 함수(EGHF) 생성 모듈
112
기타 프로그램 모듈
(예로서, 운영 체제, 애플리케이션 등)
114
프로그램 데이터
110
해시 함수 생성 결과
116
익스팬더 그래프(m)
120
입력 메시지(M)
(일정 정도의 엔트로피를 갖는 것으로 가정)
118
추출된 엔트로피의 정도(Ω)
122
기타 데이터
(예로서, 소수, 함수 파라미터, 중간 데이터 값, 익스팬더 그래프-기반 해시 함수 출력 등)
124

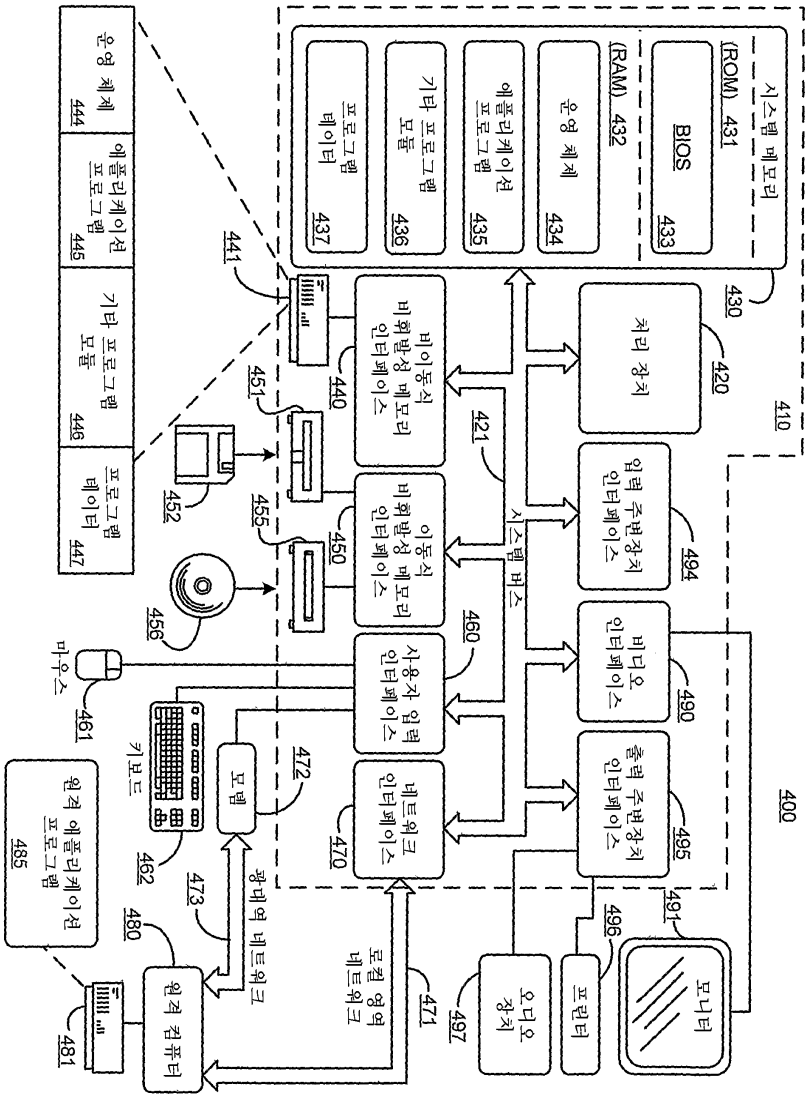
도면2


202
해시 함수에 대한 입력을
세그먼트들로 분할
204
해시 함수에 대한 입력의
각 세그먼트들에 기초하여
익스팬더 그래프를 워킹
206
마지막으로 워킹된
정점의 표지를 판정
208
해시 함수의 결과로서
그 표지를 출력

도면3


302
엔트로피의 정도로
메시지를 식별
304
익스팬더 그래프를 구성하는
n개의 정점들 중의 각 정점을
위한 명명 체계를 선택
306
메시지의 엔트로피의
정도를 추출
308
추출된 엔트로피에
기초하여 익스팬더
그래프를 워킹
310
해시 함수의 결과로서
익스팬더 그래프에서
마지막으로 워킹된 정점과
연관된 표지를 출력

도면4


시스템 메모리
(ROM) 431
BIOS 433
(RAM) 432
운영 체제 434
에플리케이션 프로그램 435
기타 프로그램 모듈 436
프로그램 데이터 437
430
410
400
처리 장치 420
입력 주변장치 인터페이스 494
비디오 인터페이스 490
출력 주변장치 인터페이스 495
시스템 버스 421
비휘발성 메모리 인터페이스 440
이동식 비휘발성 메모리 인터페이스 450
사용자 입력 인터페이스 460
네트워크 인터페이스 470
모니터 491
프린터 496
오디오 장치 497
로컬 영역 네트워크 471
광대역 네트워크 472
모뎀 473
원격 컴퓨터 480
원격 에플리케이션 프로그램 485
441
451
452
455
456
마우스 461
키보드 462
481
운영 체제 444
에플리케이션 프로그램 445
기타 프로그램 모듈 446
프로그램 데이터 447