(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0032928
(43) 공개일자 2015년03월31일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/30* (2006.01)
(21) 출원번호 10-2014-7027625
(22) 출원일자(국제) 2013년04월11일
심사청구일자 없음
(85) 번역문제출일자 2014년09월30일
(86) 국제출원번호 PCT/CN2013/074053
(87) 국제공개번호 WO 2013/152725
국제공개일자 2013년10월17일
(30) 우선권주장
61/623,272 2012년04월12일 미국(US)

(71) 출원인
딩, 진타이
중국, 안후이 230026, 헤페이 시티, 바오헤 디스트릭트, 유니버시티 오브 사이언스 앤 테크놀러지 오브 차이나, 노던 캠퍼스, 아파트먼트 28-203
(72) 발명자
딩, 진타이
중국, 안후이 230026, 헤페이 시티, 바오헤 디스트릭트, 유니버시티 오브 사이언스 앤 테크놀러지 오브 차이나, 노던 캠퍼스, 아파트먼트 28-203
(74) 대리인
박경재

전체 청구항 수 : 총 19 항

(54) 발명의 명칭 **오류를 갖는 페어링을 이용한 새로운 암호 시스템들**

(57) 요 약

LWE 문제의 개념 확장으로 볼 수 있는 오류를 갖는 페어링의 수학적 원리를 사용함으로, 이 발명은 새로운 키 교환 시스템, 새로운 키 분배 시스템과 새로운 ID 기반 암호화 시스템의 구조를 준다. 이 새로운 시스템은 효과적이고 증명 가능한 안전성과 양자 컴퓨터 공격에 저항하는 아주 강력한 보안 특성을 가진다.

특허청구의 범위

청구항 1

첫 번째 집단 a와 두 번째 집단 B 사이에서 열린 채널을 통하여 키 교환을 수립하는 방법에 있어서,

(1) 집단 A와 집단 B가 함께 다음을 공개적으로 선택하는 단계 - 매개변수 n, 홀수인 소수 q, 그리고 작은 수 t(t << n), F_q위에서 n×n 행렬들의 분포가 되는 오류 분포 K_{n^2} 그리고 F_q에서 n×n 행렬 M을 무작위적이지만 규칙성 있게 선택한다. q는 n^3처럼 n으로 표현되는 다항식의 크기일 때, F_q의 원소들은 범위 [-(q-1)/2,q-1/2]에 속한 정수에 의해 표현됨 - ;

(2) 각 집단 개인별로 오류 분산 K_{n^2}에 따라 선택된 n×n 행렬인 비밀 행렬 S_i, (i=A,B)와 오류 분산 K_{n^2}을 따르는 n×n 행렬인 오류 행렬 e_i, (i=A,B)를 선택하는 단계 - 집단 A는 다음을 계산하고,

$$M_A = MS_A + te_A$$

집단 B는 다음을 계산하고,

$$M_B = M^t S_B + te_B$$

여기서 t (t <<n)는 작은 정수임 - ;

(3) 두 집단은 열린 통신 채널에서 M_i를 교환하는 단계 ;

(4) 집단 A : $K_A = S^t{}_A \times M_B = S^t{}_A M^t S_B + t S^t{}_A e_B$ 에 의해 계산하는 단계와,

집단 B : $K_B = M^t{}_A \times S_B = S^t{}_A M^t S_B + t e^t{}_A S_B$ 에 의해 계산하는 단계 ;

(5) 집단 A와 집단 B에 의해 공유된 키를 얻기 위해 라운딩 기법을 실시하는 단계 - 상기 라운딩 기법을 실시하는 단계는 다음의 (a)와 (b)를 포함하고,

(a) 집단 B에서 K_B의 항들의 모든 위치들의 목록 T_1을 만들고, 이 성분들은 범위 [-(q-1)/4,q-1/4]안에 있으며, 이 영역에 들어 있지 않은 성분들의 모든 위치들의 목록 T_2를 만들면 집단B는 목록 T_1을 집단 A에게 보내고,

(b) 각 집단들이 T_1의 모든 성분들을 t로 나눌 때의 나머지를 계산하고, T_1에 들어있지 않은 성분들, 즉, T_2의 모든 항들에 대해서 각 항에 (q-1)/2를 더하고 [-(q-1)/4,q-1/4]에 있으면 t로 나눈 후, 그 나머지를 t로 나누고, t로 나눈 후의 나머지는 두 집단 사이에 공유된 키를 부여함 - 를 포함하는, 방법.

청구항 2

중앙 서버에서 키 분배(KD) 시스템을 만드는 방법에 있어서,

(1) 중앙서버에서 선택된 매개변수 n, 홀수인 소수 q와 작은 수 t,(t<<n)를 선택하는 단계와 - q는 n^3처럼 n으로 표현되는 다항식의 크기이고 F_q의 원소들은 범위 [-(q-1)/2,q-1/2]에 속한 정수에 의해 표현되고, 오류 분포 K_{n^2}는 F_q위에서 n×n 행렬들의 분포임 -, 중앙 서버는 F_q위에서 무작위적으로 선택된 n×n 대칭 행렬을 마스터 키로써 선택하는 단계;

(2) 중앙 서버는 i로 색인된 각 사용자에게 ID로 오류 분산 K_{n^2} 를 따르는 작은 성분들로 이루어진 일반적인 행렬 A_i 부여하는 단계 - 각 사용자의 ID 행렬은 공개적이고 중앙 서버는 사용자를 식별할 수 있는 정보와 ID를 생성하도록 선택할 수 있음 - ;

(3) 중앙서버는 각 사용자에게 안전한 비밀을 배분하는 단계 -

$$E_i = A_i S + te_i$$

,

여기서 e_i는 오류 분산 K_{n^2} 에 따라 선택된 행렬이고 이것은 각 사용자에게 비밀로 유지함 - ;와,

사용자 i와 사용자 j간에 공유된 비밀키를 얻는 단계를 포함하고, 상기 공유된 비밀키를 얻는 단계는,

사용자 i가 다음을 계산하는 단계:

$$K_i = E_i \times A_j^t = A_i S A_j^t + te_i A_j^t$$

그리고 사용자 j가 다음을 계산하는 단계:

$K_j = A_i \times (E_j)^t = A_i S^t A_j^t + tA_i e_j^t = A_i S A_j^t + tA_i e_j^t$ 를 포함하고,

두 사용자는 다음의 간단한 라운딩 기법을 사용하여 두 사용자 간의 공유된 키를 도출하는 - 상기 간단한 라운딩 기법은 다음을 포함한다

● 사용자 j는 사용자 i와 공유한 키를 수립하길 원한다고 가정하자. 사용자 j는 K_j의 (행렬에서 그들의 위치를 포함하여) 범위 (-(q-1)/4,(q-1)/4)에 속한 모든 성분을 수집하고, 즉, 그 성분들은 (q-1)/2보다 0에 가깝고, 사용자 j는 사용자 i에게 행렬의 항목 값이 아닌 항목의 위치 목록을 보내고, 그 항목들은 0으로 꼬리표가 붙여진 컬렉션에서 무작위로 선택되었고, 항목의 목록은 0으로 태그 된 목록에 속하지 않으며, 사용자 i가 자기 자신의 행렬의 같은 항목, $E_i \times A_j$를 선택하고, 이후 이것은 공통된 항목 위치의 공유된 목록을 주고, 그러므로 행렬의 항목에 대응하며, 각 사용자들은 이러한 항목들을 1로 태그 된 t로 나누는 것을 계산하고, 그리고 (q-1)/2에서 0로 태그 된 각 항목들의 합의 나머지를 구하고, 이것은 값의 새로운 동일한 순서 목록, 즉, 공유된 비밀키를 구축함 -, 방법.

청구항 3

중앙 서버를 위해 ID 기반 암호화 시스템을 구축하는 방법에 있어서,

(1) 중앙서버에서 선택된 매개변수 n, 홀수인 소수 q와 작은 수 t,(t<<n)를 선택하는 단계 - q는 n^3처럼 n으로 표현되는 다항식의 크기이고 F_q의 원소들은 범위 [-(q-1)/2,q-1/2]에 속한 정수에 의해 표현되고, 오류 분포 K_{n^2} 는 F_q위에서 n×n 행렬들의 분포이고, 중앙서버에서 비밀 마스터키로 비밀 n×n 행렬 S를 선택한다. S는 특정한 오류 분포 K_{n^2} 에 따르는 작은 원소로써 선택됨. -,

(2) 중앙 서버는 균등 분포를 따르는 무작위적인 원소 M을 선택하지만 M은 역수를 가지는 것을 보장하는 단계 - 만약 중앙 서버가 처음에 찾지 못하면 찾을 때까지 시도하고, 이후 중앙 서버는

$M_1 = MS + te$

를 계산하고, e는 특정한 오류 분포 K_{n^2} 를 따르는 작은 수임 -,

(3) 중앙서버는 M과 M_1을 마스터 공개키로써 공표하는 단계 -,

(4) 중앙서버는 i로 색인된 각 사용자에게 공공 ID, A_i를 할당하는 단계 - A_i는 특정한 오류 분포 K_{n^2}를 따르는 작은 수이고, 중앙서버는 사용자 i를 식별할 수 있는 정보를 생성할 수 있는 결정권을 가짐 -

(5) 중앙 서버는 각 사용자 i에게 비밀키를 부여하는 단계 -

$$S_i = SA_i + tM^{-1}e_i$$

e_i는 항목들은 오류 분포 κ 를 따르는 작은 수임 -,

(6) A_i의 ID와 마스터 공유키를 사용하는 누군가는 ID A_i 사용자를 위해 새로운 공개키를 만드는 단계 - 이 키는

$A_i = M$

이고

$$B_i = M_1 A_i = MSA_i + teA_i$$

인 순서쌍 (A_i, B_i)로 주어짐 - 와, 그리고 앞부분에서 설명된 MLWE 암호화 시스템을 사용하기 위해 어떤 메시지를 암호화하는데 공개키를 사용하는 단계를 포함하는, 방법.

청구항 4

제 1 항에 있어서, q는 차수가 2 이상인 다항함수이거나 비슷함 함수이고, K_{n^2}은 각 구성요소들이 서로 독립적이고 구성요소는 이산 오류 분포 κ_σ처럼 특정한 오류 분포를 따르고, 즉, F_q위에서 이산 정규 분포는 대략 $\sqrt{n}$인 표준편차에서 0 중심이거나 비슷한 분산으로 전개되는, 방법.

청구항 5

제 2 항에 있어서, q는 차수가 2 이상인 다항함수이거나 비슷함 함수이고, K_{n^2}은 각 구성요소들이 서로 독립적이고 구성요소는 이산 오류 분포 κ_σ처럼 특정한 오류 분포를 따르고, 즉, F_q위에서 이산 정규 분포는 대략 $\sqrt{n}$ 인 표준편차에서 0 중심이거나 비슷한 분산으로 전개되는, 방법.

청구항 6

제 3 항에 있어서, q는 차수가 2 이상인 다항함수이거나 비슷함 함수이고, K_{n^2}은 각 구성요소들이 서로 독립적이고 구성요소는 이산 오류 분포 κ_σ처럼 특정한 오류 분포를 따르고, 즉, F_q위에서 이산 정규 분포는 대략 $\sqrt{n}$ 인 표준편차에서 0 중심이거나 비슷한 분산으로 전개되는, 방법.

청구항 7

제 1 항에 있어서, 행렬의 곱셈이 정의되는 한 행렬들은 사각형이 될 수 있고 매개변수들은 그에 따라 조절되는, 방법.

청구항 8

제 2 항에 있어서, 행렬의 곱셈이 정의되는 한 행렬들은 사각형이 될 수 있고 매개변수들은 그에 따라 조절되는, 방법.

청구항 9

제 1 항에 있어서, $f(x)=x^n+1$일때, 행렬들은 환 $R_q=F_q[x]/f(x)$의 원소로 대체되고 이에 따라 변수들은 조절되는, 방법.

청구항 10

제 2 항에 있어서, $f(x)=x^n+1$일때, 행렬들은 환 $R_q = F_q[x]/f(x)$의 원소로 대체되고 이에 따라 변수들은 조절되는, 방법.

청구항 11

제 3 항에 있어서, $f(x)=x^n+1$일때, 행렬들은 환 $R_q = F_q[x]/f(x)$의 원소로 대체되고 이에 따라 변수들은 조절되는, 방법.

청구항 12

제 2 항에 있어서, 공유된 키를 두 사용자 i와 j에게 얻기 위한 절차는 i와 j의 역할을 바꾸는 것으로 한정되어 있는, 방법.

청구항 13

제 2 항에 있어서, 여러 중앙 서버는 분산된 KD 시스템을 만들기 위해서 함께 작동하는, 방법.

청구항 14

제 3 항에 있어서, 여러 중앙 서버는 분산된 IBE 시스템을 만들기 위해서 함께 작동하는, 방법.

청구항 15

제 3 항에 있어서, 과정은 계층(위계) IBE 시스템을 만들기 위해 더 연장되고 각 사용자들은 낮은 수준의 중앙 서버로 작동하는, 방법.

청구항 16

제 1 항에 있어서, 라운딩 기법은 비슷한 기법으로 대체되는, 방법.

청구항 17

제 1 항에 있어서, $f(x)=x^n+1$일때, 행렬들은 환 $R_q=F_q[x]/f(x)$의 원소로 대체되고 이에 따라 변수들은 조절되며, 각 f_i, $g(x)$는 영이 아닌 항이 적은 희소행렬이고 다항원소들은 $f(x)=\prod f_i(x) + g(x)$의 형태에서 선택되고 사용되는, 방법.

청구항 18

제 2 항에 있어서, $f(x)=x^n+1$일때, 행렬들은 환 $R_q=F_q[x]/f(x)$의 원소로 대체되고 이에 따라 변수들은 조절되며, 각 f_i, $g(x)$는 영이 아닌 항이 적은 희소행렬이고 사용된 다항원소들은 $f(x)=\prod f_i(x)+ g(x)$의 형태에서 선택되고 사용되는, 방법.

청구항 19

제 3 항에 있어서, $f(x)=x^n+1$일때, 행렬들은 환 $R_q=F_q[x]/f(x)$의 원소로 대체되고 이에 따라 변수들은 조절되며, 각 f_i, $g(x)$는 영이 아닌 항이 적은 희소행렬이고 다항원소들은 $f(x)=\prod f_i(x)+ g(x)$의 형태에서 선택되는,

방법.

명 세 서

기 술 분 야

[0001] 참고문헌들의 전체와 목적들을 포함하고 있는 “보안 통신과 안전한 정보 시스템들을 위한 새로운 방법들(New methods for secure communications and secure information systems)”이라는 제목의 2012년 4월 12일 제출된 Ser. No. 61623272를 토대로, 최근에 밝혀진 사실은 미국 임시 특허 출원을 우선적으로 주장한다. 이는 참고문헌들의 전체와 목적들을 포함하고 있다.

[0002] 이 발명은 특히 근본적으로 동일한 수학적 원칙인 오류를 갖는 페어링(pairing with errors)에 근거한 키 교환(key exchange, KE) 시스템, 키 분배(key distribution, KD) 시스템 그리고 신원 기반 암호(identity-based encryption,IBE) 시스템과 같은 암호 시스템들의 구성과 관련이 있다.

배 경 기 술

[0003] 인터넷, 핸드폰 등과 같은 현대적인 통신망에서 정보의 비밀을 보호하기 위해 우리는 메시지를 암호화 할 필요가 있다. 이를 위해서는 두 가지 방법이 있다. 첫 번째의 경우, 메시지를 암호화 하기 위해 발신자가 메시지를 암호화 할 때 사용하는 키와 수신자가 메시지를 해독할 때 사용하는 키가 같은 대칭 암호화 방식(symmetric cryptosystem)을 사용한다. 대칭 암호화 방식은 발신자와 수신자가 비밀을 유지한 채 위와 같이 공유되는 키를 교환하는 방법을 갖기를 요구한다. 이것은 무선 통신과 같이 어떠한 중앙 기관이 없는 열린 통신 채널(open communication channel)에서 두 사람간의 키 교환(KE)과 같은 일을 수행하기 위한 방법을 요구한다. 이것은 휴대폰 회사내의 휴대폰 시스템과 같이 중앙 서버를 갖는 시스템에서 어떤 두 이용자들이 중앙 서버에 의하여 설정된 키 분배(KD) 시스템을 통하여 공유된 키를 얻을 수 있는 것과 같은 효율적이고 확장 가능한 키 분배(KD) 시스템을 요구한다. 그러므로 안전하고 효율적인 KE 시스템과 KD 시스템을 갖는 것은 중요하며 가치가 있다. 처음 KE 시스템은 이산 로그 문제들(discrete logarithm problems)이 증명하기 어렵다는 사실을 기반으로 Diffie and Hellman [DiHe]에 의하여 제안되었다. 이 시스템은 Shor [SHO]의 업적에서 볼 수 있듯이 미래 양자 컴퓨터에 의해 보안성을 깨질 수 있다. 2차 방정식 [BSHKVY]을 통한 페어링을 이용한 시스템과 Boneh과 Boyen이 미국에서 7,590,236 특허 받은 타원곡선들을 통한 쌍일차(bilinear) 페어링에 기반으로 둔 시스템을 포함하여 많은 키 분배 시스템들이 있다. 그러나 존재하는 시스템들은 계산 효율성 또는 확장 가능성의 문제를 갖고 있다. 예를 들어, 타원 곡선들을 통한 쌍일차 페어링은 계산적으로 매우 많은 주의를 기울여야 한다.

[0004] 두 번째의 경우 암호화를 위해 수신자가 여러 개의 공개키와 개인 키를 갖고 있고 발신자가 오직 한 개의 공개키만 갖고 있는 비대칭 시스템(asymmetric system), 즉, 공개키 암호화 시스템을 이용한다. 발신자는 메시지를 암호화하기 위하여 공개키를 이용하고, 수신자는 메시지를 해독하기 위하여 개인 키를 이용하며, 오직 개인 키를 갖고 있는 사람만이 메시지를 해독할 수 있다. 보통의 공개키 시스템에서 우리는 공개키가 진짜임을 확인할 필요가 있고 각각의 공개키는 믿을 만한 중앙 기관에 의해 제공된 전자서명을 갖고 있어야 한다. 전자서명은 메시지의 수신자인 타당한 이용자가 공개키를 소유하고 있다는 것을 증명하는데 사용된다. 공개키가 암호화 시스템을 잘 작동시키기 위하여 우리는 공개키 사회 기반 시설(public key infrastructure, PKI) 시스템과 같은 시스템을 이용해야 한다.

[0005] 1984년, Shamir는 또 다른 공개키 암호화 시스템 [SHA]을 제안했다. 이 새로운 시스템에서는 개인 또는 기관의 신원을 확인할 수 있는 고유의 정보들로부터 개인 또는 기관의 공개키가 생성된다. 예를 들어 개인에 대한 정보는 이름, 거주지 주소, 생일, 지문 정보, 이 메일 주소, 사회 보장 번호(social security number) 등을 이야기할 것이다. 공개키는 신원을 확인할 수 있는 공적인 정보에 의해 결정되기 때문에 공개키 암호화 시스템의 종류는 신원 기반 암호(IBE) 시스템이라 부른다.

[0006] 신원 기반 암호(IBE) 의 공개키 암호화 시스템은 몇 가지 있고, 실질적으로 사용되는 (가장 좋은) 것은 Boneh과 Franklin에 의해 고안된 (미국, 특허: 7,113,594) 타원 곡선들을 통한 쌍일차(bilinear) 페어링을 기반으로 하는 IBE 시스템이다. IBE 시스템에서 발신자는 수신자의 신원을 기반으로 수신자의 공개키를 사용하여 주어진 수신자를 위해 메시지를 암호화한다. 수신자는 수신자의 개인 키를 이용해서 메시지를 해독한다. 안전하게 사용자를 위한 IBE 개인 키를 만들고 배부하는 시스템을 갖은 중앙 서버로부터 수신자는 개인 키를 얻는다. IBE 시스템은 발신자가 수신자의 공개키를 찾는 것을 요구하지 않지만, 예를 들어 이 메일 주소, ID number 등의 수신자의 신원을 얻을 수 있는 정보의 알고리즘을 이용해서 일치하는 공개키를 얻는다. 타원곡선들에 대한 쌍일차

페어링이 매우 많은 계산을 요구하기 때문에 최근 IBE 시스템들은 매우 복잡하고 계산적인 측면에서 효율적이지 않다. 또한, 타원곡선들에 대한 페어링을 기반으로 하고 있는 이 시스템들은 Shor [SHO]의 업적에서 볼 수 있듯이 양자 컴퓨터를 갖고 있다면 보안성이 깨질 수 있다. 격자(lattice)들을 기반으로 하는 구성들이 있지만 적용하는데 있어서 이것들은 복잡한 시스템이다 [ABB] [ABVVW] [BKPW]. 그러므로 우리가 안전하고 효율적인 IBE 시스템을 갖는다는 것은 중요하고 가치가 있는 일이다.

[0007] 명백하게도 실용적인 활용을 위해 더 효율적이고 안전한 KE, KD, 그리고 IBE 시스템에 대한 필요가 여전히 존재한다.

발명의 내용

과제의 해결 수단

[0008] 첫 번째로 본 발명은 두 집단 A와 B가 열린 통신 채널을 통해 안전한 KE를 수행할 수 있는 새로운 방법을 포함하고 있다. 이 방법은 두 가지 다른 방법이지만 각기 다른 약간의 오류들 안에서 동일한 쌍일차 형태의 페어링의 계산을 기초로 하고 있다. KE 과정에서 각각의 사용자는 비밀리에 특정한 오류 분포를 따르면서 성분(entry)이 작은 비밀 행렬을 각각 S_A와 S_B로 선택하고 무작위로 공개 행렬 M을 선택한다. 그 후에, 각 사용자들은 그들의 비밀 행렬과 공개적으로 작은 오류를 갖는 선택된 행렬을 곱하고, 새로운 행렬을 교환한 뒤, 각기 다른 작은 오류를 가진 두 가지 다른 방법으로 M을 기초로 한 서로 같은 쌍일차 형태를 통 S_A와 S_B의 페어링을 계산한다. 이와 같은 수학적 계산방법을 오류를 갖는 페어링(pairing with errors) 이라고 부른다. 공유된 키는 라운딩 기법(Rounding technique)을 한 페어링으로부터 얻는다. 이 방법은 2005년 Regev에 의해 발견된 learning with errors(LWE) 문제의 개념을 확장한 것으로 볼 수 있다 [Reg]. 이 시스템의 보안성은 수학적으로 증명되기 어려운 특정 격자문제가 얼마나 증명되기 어려운가에 달려있다 [DiLi]. 이 시스템은 오직 행렬의 곱셈을 사용하기에 매우 효율적이다. 이러한 시스템은 미래의 양자 컴퓨터의 공격에 저항할 수 있다.

[0009] 이 발명은 두 번째로 중앙 서버 또는 기관이 KD시스템을 구축할 수 있는 새로운 방법을 포함하고 있다. 이 시스템에서는 중앙 서버 또는 기관이 각 사용자 i에게 성분이 작은 A_i 행렬과 같은 공공의 ID를 할당하거나 또는, 각 사용자를 고유하게 식별할 수 있는 정보를 갖는 특정 오류 분포를 따르는 성분이 작은 A_i행렬과 같은 ID를 만든 후, 안전한 방법으로 각각의 사용자에게 중앙 서버 또는 기관의 약간의 오류가 있지만 다른 행렬인 비밀 마스터 키 M과 ID 행렬의 특정한 곱셈을 기반으로 한 개인의 키를 제공한다. 그러면, 이 시스템에서 임의의 두 사용자가 특정 라운딩 기법을 이용하여 그들 간에 공유된 키를 유도하기 위해 서로 다른 약간의 오류를 갖는 두 가지 다른 방법에서 마스터키 M 행렬을 기반으로 동일한 쌍일차 형태와 두 사용자 ID 행렬의 페어링을 계산할 것이다. 이 방법은 2005년 등록된 Regev에 의해 발견된 learning with errors(LWE) 문제에 대한 개념의 확장으로 볼 수 있다 [Reg]. 이 시스템의 보안은 오류를 갖는 페어링과 관련된 문제들이 얼마나 수학적으로 증명되기 어려운지에 달렸다. 이 시스템은 오직 행렬의 곱셈을 포함하고 있기 때문에 매우 효율적이다.

[0010] 이 발명은 세 번째로 중앙 서버 또는 기간을 통해 IBE 시스템을 구축할 수 있는 새로운 방법을 포함하고 있다. 이 시스템에서는 중앙 서버 또는 기관은 각 사용자 i에게 특정 오류 분포를 따르면서 성분이 작은 행렬처럼 공공의 ID A_i를 할당하거나 또는, 각 사용자를 고유하게 식별할 수 있는 정보를 갖는 특정 오류 분포를 따르면서 성분이 작은 행렬처럼 사용자 각각의 ID를 만든다. 중앙 서버 또는 기관으로부터 각 사용자들은 중앙 서버 또는, 다른 행렬인 마스터 공개키 M의 일부와 관련이 있는 오류를 갖는 또 다른 행렬인 기관의 마스터 개인키 S와 ID행렬의 특정 곱셈을 기반으로 한 개인키 S_i를 부여받는다. 중앙 서버 또는 기관은 약간의 오류를 가진 M과 S의 곱셈으로 마스터 키의 다른 절반을 확립할 것이다. 우리는 이것을 M_1이라 한다. 그러면 이 시스템에서 사용자 i에게 메시지를 이 시스템에서 보내길 원하는 임의의 사용자가 마스터 비밀 키인 행렬 S에 기초한 쌍일차 형태의 M 및 A_i의 페어링과 M으로 구성된 공개키 I를 계산할 것이다. 그리고, MLWE 문제에 기반한 암호화 시스템을 이용하여 메시지를 암호화하고, 사용자 i는 메시지를 해독하기 위해 비밀 키 S_i를 사용할 것이다. 이 방법은 2005년에 등록된 Regev에 의해 발견된 learning with errors(LWE)문제에 대한 개념의 확장으로 볼 수 있다. 이 시스템의 보안은 수학적으로 증명되기 어려운 특정 격자문제가 얼마나 증명하기 어려운지에 달렸다. 이 시스템은 오직 행렬의 곱셈을 포함하고 있기 때문에 매우 효율적이다.

[0011] 우리의 구조에서 ideal lattice의 원소들에 의하여 행렬을 대체할 수 있으며, 우리는 또한 라운딩 기법의 다른 유형을 사용할 수 있다. 또한, 우리는 여러 서버가 KD 및 IBE 시스템을 구축하기 위해 함께 작업할 수 있는 분

산된 방식에서 시스템을 구축할 수 있다.

[0012] 즉, 우리는 안전하고 보다 효율적인 KE, KD 및 IBE 시스템을 구축하기 위해 LWE의 문제에 대한 개념의 연장선으로 볼 수 있는 오류를 갖는 페어링의 동일한 수학적 원리를 사용한다.

[0013] 본 발명은 특정한 예시로 설명하였지만, 많은 다양성, 대안들, 수정은 암호화의 기술 부분의 숙련자들에게 명백해 질 것이 분명하다. 그러므로 본 문서에 제시한 발명의 실시 예들은 예시를 위한 것이지, 제한하려는 것이 아니다. 다양한 변경은 청구에 규정 본 발명의 사상 및 범위를 벗어나지 않으면 본 문서에 기재하고 청구에 규정이 이루어질 수 있다. 본 발명의 청구는 "보안 통신과 안전한 정보 시스템을 위한 새로운 방법들"(2012년 4월 12일 보관, 단지 기술적인 세부 사항이 추가되었다) 이라는 제목의 Ser. No. 61623272와 함께 미국 임시 특허 출원을 기반으로 한다.

발명을 실시하기 위한 구체적인 내용

[0014] 1.1 오류를 갖는 페어링의 기본 개념

[0015] 2005년 Regev에 의해 도입된 learning with errors(LWE) 문제[Reg], 그리고 그것의 확장인, ring learning with errors, RLWE 문제[LPR]는 증명이 가능한 안전성 속성(provable secure properties)을 가진 암호화 구조에 폭넓은 응용프로그램이 있다. 주요한 주장은 그들이 어떠한 최악의 경우 어떤 격자 문제, 더 나아가 관련 암호화 구조만큼 견고하다는 것이다.

[0016] LWE 문제는 다음과 같이 설명할 수 있다. 첫 번째, 우리는 매개변수 n, 법(modulus) (소수) q, 그리고 q개의 원소를 갖는 유한한 환(체) F_q에 대한 오류 확률 분포 κ 를 갖고 있다. 설명을 단순화하기 위해, 우리는 q가 홀수인 소수가 되도록 뽑을 것이다. 다만, 약간의 수정을 해야 하는 경우를 제외하고, 모든 정수에서 사용할 수 있다.

[0017] F_q에서는 각각의 원소는 집합 {-(q - 1)/2,…,0,…,(q - 1)/2}로 표현된다. 이 "오류" 분포에 의한 설명에서는 원소 값이 작은 것을 선택하는 확률이 매우 높은 것과 같은 분포를 의미한다. 많은 선택이 있으며, 이러한 선택은 직접적으로 시스템의 보안에 영향이 있다. 시스템이 원활히 그리고 안전하게 작동되기 위해, 좋은 오류 분포를 선택해야 한다.

[0018] F_q^n에서 무작위이며 균일하게 원소 A를 선택하고, κ 에 따라 $e \in F_q$를 선택한 뒤, $(A, < A, S+e >)$(여기서 + 는 F_q에서의 덧셈이다)를 출력하여 얻게 되는 F_q에서의 $\Pi_{S,\kappa}$ 을 확률 분포라고 한다. $\Pi_{S,\kappa}$ 로부터 독립적 샘플들의 임의의 숫자를 갖은 F_q^n에서의 어떤 S에 대해 알고리즘이 S를 높은 확률로 출력한다면, 알고리즘은 법 q와 오류 분포 κ 를 갖은 LWE 문제를 해결한다.

[0019] LWE 문제에 기초한 관련 암호화 구조의 증명 가능한 안전성(provable security)을 달성하기 위해, n의 특정한 다항식 함수가 되도록 q, 즉, q(n)으로 나타나는 n의 다항식 함수에 의해 대체되는 q를 선택하고, κ 는 표준편차는 $\sigma = \alpha q \geq \sqrt{n}$ 이고 0을 주변에서 중심으로 한 정규 분포의 특정 이산 버전으로 선택한 후, 또한, F_q의 원소들은 [-(q - 1)/2,(q - 1)/2)] 범위 내의 정수로 표시한다. 그리고 이 분포를 κ_σ로 나타낸다.

[0020] LWE 문제에 기초하는 원래의 암호화 시스템에서는 시간당 1 비트(bit)를 암호화할 수 있으므로, 시스템은 다소 비효율적이고 사이즈가 큰 키를 갖는다. LWE 문제에 기반을 두는 암호체계의 효율성을 증대시키기 위해서 새로운 문제, 다항식환 F_q [x] [LPR]의 잉여환을 기반으로 하는 LWE 문제가 제안되었다. 이것을 환 LWE(RLWE) 문제라고 부른다. RLWE 문제에 기초하는 암호화 체계에서는 그들의 보안이 일반적인 격자를 대신하여 Ideal lattice 모임(class)의 부분모임(subclass)에서 어려운 문제들을 줄인다.

[0021] 후에, LWE의 새로운 형태가 [ACPS]에서 제안되었다. 이 LWE 문제의 새로운 형태는 LWE 문제에 기반을 두고 있다. 우리는 A×S의 행렬 곱셈을 수행할 수 있도록 벡터 A를 m×n 크기의 행렬 A로 대체하고, S 또한 n×1 크기의 행렬로 대체한다. 우리는 또한 e를 m×1 크기의 행렬로 대체한다. 우리는 q원소들을 갖은 같은 유한체에서 계산을 할 것이다.

[0022] 설명을 간단히 하기 위해 구체적으로 A가 n×n크기의 행렬이고 S와 e가 n×1크기의 행렬인 경우에 대해서만 제

시할 것이다.

[0023] F_q에서 $\Pi_{S,\kappa n}$ 은 각각의 성분을 F_q에서 독립적이고 균일하게 선발한 n×n행렬 A를 선택하고, e는 예를 들어, 각각의 성분은 오류 분포 κ 를 독립적으로 따르는 것과 같은 특정 오류 분포 κ_n으로부터 선택된 성분을 갖는 F_q에서의 n×1벡터로 선택하며, (A,A×S+e)(+는 F_q^n에서 사용하는 덧셈)를 출력하여 얻어진 확률분포로 한다. $\Pi_{S,\kappa n}$ 으로부터 독립적 샘플들의 임의의 숫자를 갖은 F_q^n에서의 어떤 벡터 S에 대해 알고리즘이 S를 높은 확률로 출력한다면, 알고리즘은 법 q와 오류 분포 κ_n을 갖은 LWE를 해결한다.

[0024] 작은 S, 즉, 오류 분포 κ_n을에 따라 독립적으로 성분이 선택되는 경우, 우리는 이 문제를 small LWE(SLWE)라고 부른다. 만약 A를 대칭적인 조건으로 부과하는 경우에 우리는 이것을 small symmetric LWE(SSLWE) 문제라고 부른다. 만약 작은 양의 정수로 고정되어 있는 z에 대해 (-z,…,0,1,…,z)의 집합에서 무작위이며 독립적으로 비밀키S를 뽑는다면, 우리는 이것을 uniformly small LWE (USLWE)문제라고 일컫는다.

[0025] 실질적인 활용을 위해 우리는 오류 분포의 서로 다른 종류를 갖는 S와 e를 선택할 수 있다.

[0026] [ACPS]의 결과 때문에 만약 비밀 S의 좌표와 오류 e의 성분이 LWE 오류 분포 κ_σ로부터 독립적으로 샘플링하면, 해당 LWE 문제가 균일하게 무작위의 비밀 S를 가진 LWE만큼 증명되기 어렵다. 원소 S가 작은, 즉, 작은 비밀(small secret)을 갖은 환 LWE 문제를 해결하면 균일한 비밀(uniform secret)을 가지면서 ring LWE 문제를 해결할 수 있는 RLWE문제의 경우와 동일하다.

[0027] 우리는 이 문제를 전체 행렬 형태로 좀 더 확장한다.

[0028] F_q 에서 Π_{S,κ_n^2}은 각각의 성분을 F_q에서 독립적이고 균일하게 선발한 n×n행렬 A를 선택하고, e는 예를 들어, 오류 분포 κ 를 독립적으로 따르면서 선택된 분포 같은 특정 오류 분포인 K_{n^2}를 따르는 F_q에서 성분을 갖는 n×n 행렬로 선택하며, (A,A×S+e)(+는 $F_q^{n^2}$에서 사용하는 덧셈)를 출력하여 얻어진 확률분포로 한다. Π_{S,κ_n^2} 로부터 독립적 샘플(들)의 임의의 숫자를 갖은 F_q^n에서의 어떤 n×n 행렬 S에 대해 알고리즘이 S를 (높은 확률로) 출력한다면, 알고리즘은 법 q와 오류 분포 κ_n^2를 갖은 LWE를 해결한다.

[0029] 우리는 이 문제를 matrix LWE(MLWE) 문제라고 부른다. 오류 분포 K_{n^2}를 따르는 성분이 작은 S를 선택하는 경우 우리는 이 문제를 small MLWE(SMLWE)라고 부른다. 만약 A를 대칭적인 조건으로 부과하는 경우에 우리는 이것을 small symmetric MLWE(SSMLWE) 문제라고 부른다. 만약 작은 양의 정수로 고정되어 있는 z에 대해 -z,…,0,1,…,z의 집합에서 무작위이며 독립적으로 비밀(secret) S를 뽑는 다면, 우리는 이것을 uniformly small MLWE(USMLWE)문제라고 일컫는다. MLWE 문제는 오직 n을 LWE 문제와 같이 두고 동일한 행렬을 공유한다는 것은 분명하다. 그래서 이것은 LWE문제에 부합할 만큼 증명하기 어렵다.

[0030] 우리는 S와 e에 대한 다른 오류 분포를 사용할 수 있다.

[0031] 구조 뒤의 수학적 원리는 행렬 A,B 그리고 C의 곱셈의 결합성의 사실에 비롯한다.

[0032] $A \times B \times C = (A \times B) \times C = A \times (B \times C)$.

[0033] 위와 같은 곱셈은 수학적으로 C의 열벡터와 A의 행벡터의 쌍일차 페어링 계산처럼 보여질 수 있다.

[0034] 특정 오류 분포, 예를 들어, 오류 분포를 따르는 성분을 갖는 오류 분포를 따르면서 성분이 작은 A와 B 행렬에 대해, 직접적으로 계산을 하는 것 대신 첫 번째로 우리는

[0035] $AB+E_a$

[0036] 를 계산하고, 그 후에

[0037] $(AB+E_A)C$ 또는 $(AB+ E_A)C+E_{AC}$

[0038] 또는 다음을 계산한다.

[0039] $BC+E_C$.

[0040] 그 다음에 E_A,E_B,E_{AC},E_{BC}가 같은(혹은 다른) 오류 분포를 따르는 성분이 작은 행렬일 때,

[0041] $A(BC+E_C)$ 또는 $(AB+E_A)C+E_{BC}$

[0042] 를 계산한다. 그 다음 이 두 행렬들 간의 작은 오류 또는 차이가 있는 ABC를 계산하는 방법이 두 가지 있다. 위와 같은 계산을 오류를 갖는 페어링이라고 말한다. 모든 구조는 이와 같은 오류를 갖는 페어링과, A와 C의 값이 작은 경우 두 가지 다른 페어링이 서로 가깝다는 사실에 달렸다.

[0043] 우리는 동일한 매개변수를 갖는 LWE 문제에 부합하게 MLWE 문제가 증명되기 어렵다는 이론을 수학적으로 증명할 수 있다. 이것은 구조에 대해 증명 가능한 안전성의 기초를 제공한다.

[0044] 1.2 오류를 갖는 페어링을 기반으로 한 새로운 KE 시스템 구조

[0045] 두 집단 Alice와 Bob은 열린 채널에서 키 교환(KE)를 실행하기로 했다. 열린 채널에서의 키 교환은 Alice와Bob의 통신은 악의가 있는 공격자를 포함한 누구에게나 열려있다는 것을 말한다. 쉽게 설명하기 위해서 여기서 말하는 모든 행렬은 n×n 행렬을 포함한다고 가정하자. 하지만 행렬이 n×n 행렬과 같을 필요는 없으며, 행렬 곱셈이 잘 정의될 수 있도록 호환 가능한 크기를 선택하는 것을 제외한 모든 사이즈의 행렬이 될 수 있다.

[0046] 키 변경 프로토콜은 다음과 같은 단계로 실행한다.

[0047] (1) Alice와 Bob은 먼저 공개적으로 F_q, n과 F_q 에서 균일하게 무작위로 n×n 행렬 M을 선택한다. 여기서 q는 n 차 다항식의 크기이다. 예를 들어 $q \approx n^3$ 로 나타낸다. 또한 오류 분포 K_{n^2}가 F_q에서 n×n 행렬의 분포가 되도록 선택한다. 예를 들어, 분포의 각각의 구성요소는 독립적이며 LWE 경우와 같은 이산 오류 분포 κ_σ와 같은 어떤 오류 분포를 따른다. 즉, F_q에서의 이산 정규 분포는 0 주위에 표준편차가 대략 $\sqrt{n}$이다. 위의 모든 정보는 공개된다. 그들은 함께 공개적으로 작은 (소수인) 정수 t (t<<n)를 선택한다.

[0048] (2) 그리고 각자의 집단은 오류 분포 K_{n^2}을 따르는 n×n 행렬로 그들만의 비밀 S_i (i=A,B)를 선택한다. 또한 오류 분포를 따르는 n×n 행렬을 e_i로 택한다. 작은 정수 t (t<<n)에 대하여 Alice는 다음을 계산한다

[0049] $M_A = MS_A + te_A$,

[0050] Bob은 다음을 계산한다

[0051] $M_B = M^t S_B + te_B$.

[0052] (3) 두 집단은 열린 통신 채널에서 M_i를 교환한다. M_i (i = A,B)는 공개되어 있으나 S_i와 e_i (i = A,B)는 비밀 상태를 유지한다.

[0053] (4) Alice는 다음을 계산한다:

[0054] $$K_A = S_A^t \times M_B = S_A^t M^t S_B + tS_A^t e_B .$$

[0055] Bob은 다음을 계산한다:

[0056] $$K_B = M_A^t \times S_B = S_A^t M^t S_B + te_A^t S_B$$.

[0057] (5) 두 집단은 공유키를 얻기 위하여 다음과 같이 라운딩 기법을 실행한다:

[0058] (a) Bob는 K_B의 성분 중 [-(q -1)/4,(q -1)/4] 범위에 있는 성분들의 위치를 리스트 T_1으로 만들고 범위에 있지 않는 성분들의 위치를 리스트 T_2으로 만든다. 그리고 Bob는 Alice에게 T_1을 보낸다.

[0059] (b) 그러고 나서 각 집단들은 T_1 에서 성분의 t로 나눈 나머지 계산한다. 그리고 T_1에 있지 않은 성분, 즉, T_2에 있는 성분에 대하여 (q -1)/2을 각 성분에 더한 후, q로 나눈 나머지를 ([-(q -1)/4,(q -1)/4] 범위 안에 오도록) 계산한 뒤 t로 나눈 나머지를 계산한다. 두 집단은 이 과정을 통하여 공유키를 얻을 수 있다.

[0060] Alice와 Bob가 위의 경우처럼 어떤 라운딩 기법을 통하여 교환한 키가 공유된 비밀이 되도록 K_A와 K_B부터 유도하는 이유는 e_i와 S_i 가 작기 때문이다. 그러므로 K_A와 K_B는 비슷하다. 우리는 이 시스템을 SMLWE 키 교환 프로토콜이라고 부른다. 우리는 이 효과적인 시스템의 증명 가능한 안전성을 입증할 수 있다 [Dili].

[0061] 통신과 계산의 효율성, 이 두 가지 측면에 있어서 새로운 시스템은 아주 좋은 시스템이다. 두 집단은 F_q에서 n^2 개의 성분을 교환하고 t=2일 때, n^2 비트를 얻기 위해서 각각 $2n^{2.8}$번의 (Strassen fast matrix multiplication[STR]을 이용한) 계산을 실행하여야 한다.

[0062] S_i와 e_i는 서로 다른 종류의 오류 분포를 따를 수 있다.

[0063] 같은 시스템 매개변수 n, q를 고르면 정리를 증명할 수 있다. 즉, 오류 분포를 적절하게 선택하면 SLWE 행렬 키 교환 프로토콜은 증명 가능한 안전성이다 [DiLi]. 증명은 오류를 갖는 페어링 문제를 따르는 수학적 어려움에 기댄다.

[0064] 다음과 같이 주어져 있다고 가정하자..

[0065] (1) n×n 행렬 M, 소수 q, 작은 양수 t, 오류 분포 κ_n 그리고;

[0066] (2)

$$M'_A = MS'_A + te_A$$

[0067] 와

[0068]

$$M'_B = M^t S'_B + te_B ,$$

[0069] 여기서 e_i 는 n×1 벡터로써 오류 분포 κ_n를 따르고, n×1 벡터 S'_i의 성분 또한 같은 오류 분포를 따른다;

[0070] (3)

$$K'_B = M_A^t \times S'_B = (S'_A)^t M^t S'_B + t\langle e_A, S'_B \rangle$$

[0071] 는 [-(q -1)/4,(q -1)/4]범위에 있거나 없을 수 있다.

[0072] 하지만 여기서, K'_B가 [-(q -1)/4,(q -1)/4]범위에 있을 때,

[0073]

$$K'_A = (S'_A)^t \times M_B = (S'_A)^t M^t S'_B + t\langle S'_A, e_B \rangle$$

[0074] 의 t로 나눈 나머지를 구하고, 범위에 있지 않을 때에는 높은 확률로 K'_A+(q-1)/2의 q로 나눈 나머지를 다시 t로 나누어 나머지를 구하는 알고리즘을 구하는 것이 문제가 된다. 이러한 문제를 오류를 갖는 페어링 문제(pairing with error problem, PEP)라고 부른다.

[0075] 증명은 다음과 같은 사실을 따른다. 행렬 버전은 여러 SLWE 샘플을 조합하여 하나의 행렬 SLWE 샘플로 볼 수 있

기 때문에 SMLWE 문제는 SLWE 문제만큼 어렵다.

[0076] 여기서 행렬의 크기가 행렬 곱에 대하여 일치하는지 확인하여 구성할 직사각행렬을 선택해야 한다는 점에 유의하여야 한다. 하지만 매개변수들은 보안을 보장하기 위하여 적절히 선택되어야 한다.

[0077] 마찬가지로 오류를 갖는 ring learning with errors(RLWE) 문제에 기반한 키 교환 시스템을 구축할 수 있다 [LPR]. 그리고 [LNV]에 설명된 RLWE 문제의 변형을 원한다.

[0078] RLWE 문제에 대하여 환 R = Z[x]/f(x)과 R_q = R/qR,을 생각하자. 여기서 f(x)는 차수가 n인 Z[x]에서의 다항식이고 Z는 정수환이며 q는 홀수인 소수이다. 여기서 Z_q = F_q = Z/q에서의 원소들은 다음과 같은 원소들로 나타낼 수 있다: -(q -1)/2,...,0,...,(q - 1)/2. 이와 같은 원소들은 원소의 노름(norm)에 대하여 이야기 할 때 Z의 원소들처럼 생각한다. R_q의 모든 원소는 차수가 n-1인 다항식에 의해 나타낸다. 또한 그것의 성분처럼 대응되는 계수들로 이루어진 벡터로 볼 수 있다. 원소

[0079] $$a(x)=a_0+a_1x+\ldots+a_{n-1}(x)^{(n-1)}$$

[0080] 에 대하여

[0081] $$\|a\| = \max|a_i|$$.

[0082] 와 벡터

[0083] $(a_0,a_1,\ldots,a_{(n-1)})$의 노름(norm) l_∞을 정의하자. 그리고 이 벡터를 Z^n에서의 원소처럼 여기고 a_i는 Z의 원소이다. 또한 q 짝수인 정수로 선택 할 수 있고 변수들은 약간의 수정이 필요하다.

[0084] $RLWE_{f,q,\chi}$ 문제는 차수가 n인 다항식f(x), 소수 q, R_q에서의 오류 분포 χ에 대하여 매개화 되어있다. 이것은 다음과 같이 정의된다.

[0085] 비밀 s는 R_q의 원소이고, 균일하게 선택된 임의의 환 원소이다. 주어진 임의의

[0086] $$(a_i,b_i=a_i\times s+e_i)$$

[0087] 의 표본의 다항식수 s를 구하는 것이 문제이다. 여기서 a_i은 균일하게 무작위로 선택된 R_q의 원소이고, e_i은 다음과 같은 어떤 오류 분포 χ에서 선택 된다.

[0088] 이러한 문제가 난해한 이유는 b_i가 일정하게 R_q에서 계산상 구분할 수 없기 때문이다. $RLWE_{f,q,\chi}$ 문제를 해결하는 것이 관련된 변수들에 대한 ideal lattice에서 쇼트 벡터 문제를 해결하는 양자 알고리즘을 얻을 수 있다고 알려져 있다는 것을 [LPR]에 보일 수 있다. 다음의 문제는 기하급수적으로 훨씬 더 어렵다.

[0089] 여기서 다시 [ACPS], [LPR]에서 $RLWE_{f,q,\chi}$ 문제는 변형과 동등(equivalent)하고 여기서 비밀 s는 오히려 R_q에서 균일한 것 보다 오류 분포 χ에서 표본화 되는 것이고 오류 원소 e_i는 어떤 작은 정수 t의 배수라는 사실을 이용하자.

[0090] 증명 가능한 안전성을 유도하기 위해서 구체적으로 매개변수를 선택하여 RLWE 문제를 생각해 볼 필요가 있다.

[0091] ● f(x)가 $n=2^u$ 에 대하여 원분 다항식 x^n+1가 되도록 선택하자.

[0092] ● 오류 분포 χ는 $n\gg\sigma>\omega(\sqrt{\log n})>1$ 에 대한 이산 가우스 분포 $D_{Z^n,\sigma}$이다.

[0093] ● q=1 (mod 2n)이고 q는 n의 다항식이며 . $q \approx n^5$ 이다;

[0094] ● t는 $t \ll n \ll q$인 작은 소수이다.

[0095] 또한 응용을 위해서 다른 매개변수를 사용할 수 있다.

[0096] 위와 같이 정의된 $RLWE_{f,q,\chi}$ 에서 두 가지 중요한 사실이 있다. 이것은 키 교환 시스템을 위해 필요하다.

[0097] (1) 표준편차 σ를 갖는 이산 가우스에서 도출된 벡터의 길이는 σn를 유계로 한다. 즉, χ 따라 선택되는 X에 대하여

[0098] $$Pr(\|X\| > \sigma n) \leq 2^{-n+1}$$

[0099] 이다.

[0100] (2) 환 R_q 에서의 곱셈은 적당한 규모의 구성원소의 노름(norm)으로부터 증가한다. 즉, $X,Y \in R_q$와 위에서 정의한 l_∞ 노름에 대하여

[0101] $$\|X \times Y \pmod{f(x)}\| \leq n\|X\|\|Y\|$$

[0102] 이다.

[0103] 위에서 설정한 $RLWE_{f,q,\chi}$ 으로 부터 두 집단 Alice와 Bob이 열린 채널에서 키를 교환할 준비가 되었다. 키 교환은 다음과 같은 단계를 따른다.

[0104] (1) Alice 와 Bob은 먼저 $q(\approx n^3$ 또는 유사한 n의 다항함수), n, f(x)와 χ 을 포함한 $RLWE_{f,q,\chi}$ 에 대한 모든 매개변수를 공개적으로 선택한다. 또한 균일하게 R_q에서 임의의 원소 M 을 선택한다. 위의 모든 정보들은 공개된다.

[0105] (2) 그러면 각각의 집단은 오류 분포 χ를 따르는 R_q 에서의 원소 s_i를 그들의 비밀로 선택하고, 오류 분포 χ를 따르는 원소인 e_i를 독립적으로 선택한다. 다만 작은 소수 $t(t \ll n)$를 공통적으로 선택한다.

[0106] 작은 정수 $t(t \ll n)$에 대하여 Alice는 다음을 계산한다

[0107] $$M_A = Ms_A + te_A,$$

[0108] Bob은 다음을 계산한다.

[0109] $$M_B = Ms_B + te_B.$$

[0110] (3) 두 집단은 M_i를 교환한다. 다시 말하자면 M_i는 공개되어 있지만 반드시 s_i와 e_i는 비밀을 유지해야 한다.

[0111] (4) Alice는 다음을 계산한다:

[0112] $$K_A = s_A \times M_B = s_A M s_B + te_B s_A.$$

[0113] Bob은 다음을 계산한다:

[0114] $$K_B = M_A \times s_B = S_A M s_B + te_A s_B.$$

[0115] (5) 두 집단은 모두 공유키를 도출하기 위해서 라운딩 기법을 다음과 같이 실행한다.

[0116] (a) Bob은 크기가 n인 리스트를 만든다. K_B의 x^i 계수가 [-(q - 1)/4,(q - 1)/4]범위에 있다면 이 리스트는 i=0,…,n-1이고 j=1인 (i,j) 의 형태의 순서쌍으로 이루어져있다. 만약 범위 안에 있지 않는다면 j=0이

다.

[0117] (b) Bob은 Alice에게 이 리스트를 보낸다. 그러면 서로는 다음과 같은 방법으로 대응되는 성분의 t로 나눈 나머지를 계산한다. :

[0118] 리스트 (i,j)의 원소에 대하여

[0119] 1) j=1일 때, 각 집단은 K_A와 K_B 의 i번째 성분의 t로 나눈 나머지를 구한다.

[0120] 2) j=0일 때, 각 집단은 K_A와 K_B 의 i번째 성분에 (q - 1)/2를 더한 후 q로 나눈 나머지가 [-(q - 1)/4,(q - 1)/4] 범위에 포함될 수 있도록 한다. 그런 다음 다시 t로 나눈 나머지를 구한다.

[0121] s_i와 e_i에 대하여 서로 다른 분포를 사용할 수 있다.

[0122] 그것은 두 사용자 사이에 공유키를 준다. 우리는 이러한 시스템을 RLWE 키 교환 시스템이라고 부른다. 우리는 이 키 교환 시스템의 실패 확률이 아주 낮다는 것을 추측할 수 있다. 환 R_q의 가환성과 결합성이 RLWE 키 교환 시스템의 구성에서 중요한 역할을 한다는 것에 주목한다.

[0123] 보안 해석적 측면에서, 환 R_q에서 비슷한 PEP을 이용한 $RLWE_{f,q,\chi}$ 문제의 어려움을 따르는 시스템의 증명 가능한 안전성을 보일 수 있다 [DILI].

[0124] 다음과 같이 주어졌다고 가정하자.

[0125] ● R_q의 임의의 원소 M, 소수 t,q와 위의 $RLWE_{f,q,\chi}$ 에서 선택된 매개변수를 갖는 오류 분포 χ;

[0126] ● 오류 분포 χ를 따르는 e_i와 s_i에 대하여 $M_A=Ms_A+te_A$와 $M_B=Ms_B+te_B$.

[0127] ● $(K_B)_i$, 즉, $K_B=M_A\times s_B=s_AMs_B+te_As_B$의 계수 x^i는 범위 [-(q - 1)/4,(q - 1)/4]에 있거나 없을 수 있다.

[0128] 문제는 K_B(또는 K_A) t로 나눈 나머지 또는 높은 확률로 K_B+(q-1)/2 (또는 K_A+(q-1)/2) ([-(q - 1)/4,(q - 1)/4]범위 안에 있도록) q로 나눈 나머지를 계산한 후, t로 나눈 나머지를 도출하는 알고리즘을 찾는 것이다. 우리는 이러한 문제를 환 위에서 오류를 갖는 페어링 문제(pairing with error problem over ring, RPE)라고 부른다.

[0129] RLWE키 교환 시스템은 거의 SLWE키 교환 시스템에 관한 증명 가능한 안전성 증명의 평행한 확장이다. RLWE 키 교환 시스템은 $RLWE_{f,q,\chi}$ 문제의 어려움을 기반으로 증명 가능한 안전성이다.

[0130] 같은 매개변수 q와 n에 대하여, 이 시스템은 알고리즘의 FFT타입을 이용한 환 R_q에서 빠르게 곱셈을 할 수 있는 확률 때문에 아주 효율적이다.

[0131] 1.3 오류를 갖는 페어링을 기반으로 한 새로운 KD 시스템의 구조

[0132] 대형 네트워크에서 합법적인 사용자 간에 키 분배는 중요한 문제이다. 키 분배 시스템에서 종종 어려운 문제는 효율적이고 측정 가능한 시스템을 어떻게 구성하느냐이다. 예를 들면, [BSHKVY] 구성의 경우 시스템은 중앙서버의 마스터 키가 n×n대칭 행렬 M이고 각각의 사용자의 ID가 크기가 n인 행벡터 H_i로 보여지도록 기본적으로 이해되었다. 중앙서버는 각각의 사용자에게 비밀 $H_i\times M$을 부여한다. 그러면 두 사용자는 $H_i\times M\times H_j^t$를 공유키로 얻을 수 있다. M의 대칭성은

[0133] $$H_i \times M \times H_j^t = H_j^t \times M \times H_i$$

[0134] 이도록 한다. 그러나 많은 사용자들은 마스터 키를 얻기 위하여 공동으로 작업하여야 한다. 만약 누군가 비밀키 $H_i \times M$을 충분히 모으면 이것은 마스터키 M을 알아내기 위해서 사용될 수 있다. 그렇게 된다면 시스템을 파괴할 수 있다.

[0135] 우리는 믿을 수 있는 중앙서버에서 오류를 갖는 페어링을 이용하는 정확히 측정 가능한 키 분배 시스템을 구축할 것이다. 이것은 위의 아이디어와 LWE의 아이디어를 결합한 것으로 볼 수 있다.

[0136] 다시 $-(q-1)/2,\ldots,0,\ldots,(q-1)/2$로 나타내는 원소를 갖는 유한 체 F_q에서 계산하자. 우리는 $q \approx n^3$이나 이와는 다른 비슷한 n의 다항함수를 고른다. 또한 κ_n^2을 $n \times n$행렬 공간에서의 오류 분포가 되도록 고른다. 예를 들면, 각각의 성분은 독립적이고 각각의 성분은 오류 분포 κ_σ을 따르는 분포이다. LWE의 경우처럼 이산 분포 κ_σ는 F_q 에서 0주위에 표준편차가 대략 $\sqrt{n}$인 이산 정규 분포이다. 이와 같은 매개변수를 선택하는 것은 수정될 수 있다.

[0137] 키 분배 시스템은 다음과 같은 단계로 설정되어있다.

[0138] (1) 우리는 중앙서버를 갖고 있다. 중앙서버는 대칭적인 임의로 고른 $n \times n$ 행렬 S를 마스터키로 고른다. 행렬 S의 성분은 F_q의 원소이다:

[0139] $S=S^t$

[0140] (2) i로 색인된 각각의 사용자에 대하여, 중앙서버는 오류 분포 κ_n^2을 따르는 작은 성분으로 이루어진 (일반적으로 대칭적이지 않은) 행렬 A_i를 (ID로) 부여한다. 사용자 각각의 ID 행렬은 공개적이고 이메일 주소와 이름 등으로 사용자를 확인할 수 있는 정보들로 생성될 수 있다.

[0141] (3) 사용자 각각에 대하여 중앙서버는 안전하게 비밀을 나누어 준다:

[0142] $$E_i = A_i S + te_i,$$

[0143] 여기서 e_i는 κ_n^2와 같은 어떤 오류 분포에 의해 선택되는 (대칭이 아닌) 행렬이다. 이것은 사용자들의 개인정보를 지킨다.

[0144] 사용자 i와 j는 서로 간의 공유된 비밀키를 각자 다음의 식을 통해 얻을 수 있다.

[0145] $$K_i = E_i \times A_j^t = A_i S A_j^t + te_i A_j^t;$$

[0146] $$K_j = A_i \times (E_j)^t = A_i S^t A_j^t + tA_i e_j^t = A_i S A_j^t + tA_i e_j^t.$$

[0147] 이는 ID들이 공개되어 있기 때문에 가능하다. 그 다음에, 사용자 i와 j는 공유키를 유도하기 위해 아래와 같은 간단한 라운딩 기법을 사용할 수 있다.

[0148] ● 사용자 j가 i와 함께 공유키를 설정하길 원할 때, j는 $(-(q-1)/4,(q-1)/4)$의 범위 내에 존재하는 K_j내부의 성분들(행렬 내부에서 성분들이 갖는 위치를 포함하여)을 모두 선택한다. 즉, 이러한 성분들은 $(q-1)/2$보다 0에 가깝다. 그 후 사용자 j는 사용자 i에게 목록 두 개를 보낸다. 하나는 무작위로 고른 성분들의 위치에 대한 목록이다. 이때 목록에는 오직 성분들의 위치만 포함될 뿐, 하나하나의 값은 포함되지 않는다. 이 목록은 0으로 태그 된다. 다른 하나는 0으로 태그 된 목록에 들어 있지 않은 성분들의 목록이다. 그런 다음, 사용자 i는 자신이 가진 행렬 $E_i \times A_j$내부에서 같은 성분들을 선택한다. 이제 두 사용자는 서로 간의 공통된 성분들의 위치가 포

함된 목록을 공유하게 되었으며, 그에 따른 행렬의 성분 역시 공유하게 된다. 그러면 각각의 사용자는 1로 태그된 이러한 성분들을 t로 나눈 나머지를 구하고 (q-1)/2에서 0로 태그 된 각 성분들의 합의 나머지를 구한다. 이것은 값의 새로운 동일한 순서 목록, 즉, 공유된 비밀 키를 구축한다.

[0149] S는 대칭성이 있으므로

[0150] $$A_iSA_j^t=A_iS^tA_j^t$$

[0151] 이다. 그러므로 사용자 j는

[0152] $$A_iSA_j^t+tA_ie_j^t$$

[0153] 을 유도할 수 있다. 두 사용자가 계산한 결과의 차이는 다음과 같다.

[0154] $$E_i\times A_j^t-A_i\times E_j^t$$

[0155] $$=A_iSA_j^t+te_iA_j^t-(A_iSA_j^t+tA_ie_j^t)$$

[0156] $$=te_iA_j^t-tA_ie_j^t$$

[0157] 이때 t의 값이 작고, $e_iA_j^t$ 와 $A_ie_j^t$ 의 값도 작기 때문에, 위 차이도 작다. 이는 e_i, e_j, A_i 와 A_j 가 모두 작다는 사실에서 비롯된 것이다. 그러므로 어떠한 라운딩 기법으로부터 i와 j는 공통의 키를 가지게 되고, 그러므로 하나의 키 분배 시스템을 만들게 된다.

[0158] 두 행렬 te_iA_j 와 $te_i^tA_i$ 에 대한 오류 항들이 작기 때문에, A_iS A_i 내에서 1로 태그 된 항목들(오류 항들은 제외하고)은 필수적으로 [-(q-1)/4,(q-1)/4]범위 내에 있거나 또는 범위에 매우 가까울 것이다. 그러므로 오류 항은 (-(q-1)/2,(q-1)/2) 를 넘으며 A_iSA_i에서 선택된 항이 될 수 없다. 0으로 태그 된 항목들에 대해서도 같은 사실이 적용되며, 이와 같은 과정을 통해 두 사용자 사이의 공유키가 형성된다.

[0159] 행렬 K_i와 K_j를 구성하는 방법으로부터, 우리는 두 행렬의 각 항목들이 균등 분포를 따른다는 것을 알 수 있다. 그러므로 사용자 j가 행렬 K_j에서 뽑은 첫 번째 목록의 크기는 매번 n^2에 가까워야 함을 예상할 수 있다. 그러므로 적절한 n을 고르면 우리는 공유되는 비밀을 충분한 비트만큼 얻을 수 있다.

[0160] 또한 우리는 비대칭(non symmetric)행렬을 통해 이 시스템의 다른 버전을 만들 수 있다. 이때, 중앙 서브는 A_iS+e 나 $A_i^tS+e^t$ 와 같은 더 많은 행렬들을 계산할 필요가 있다. 그런 다음 우리는 키 분배와 같은 작업을 수행할 수 있다. 따라서 이 시스템은 별로 효율적이지 않다.

[0161] 다시 말해, RLWE 문제는 matrix-based LWE의 특별한 가환 버전으로 볼 수 있다. 환에서 하나의 원소가 그 환과 준동형(homomorphism)이라고 보여질 수 있기 때문이다. 동시에 우리는 키 분배를 위해 RLWE를 사용할 수 있다.

[0162] 이제 왜 이러한 키 분배가 측정 가능한지 알아보자. 분명히 각 사용자는 A_i 와 $E_i = A_iS + te_i$ 로 구성된 한 쌍을 가지고 있다. 그리고 여러 사용자들이 함께 여러 쌍을 가질 수도 있다. 그리고 비밀 마스터 키 S를 찾으려면 그에 상응하는 MLWE 문제를 풀어야 한다. 이를 제외하고는, 우리는 비밀 S에 대칭성(symmetric)의 조건을 부여한다. 이 문제가 LWE 문제만큼 어렵다는 것을 입증하는 건 어렵지 않다. 왜냐하면 우리는 주어진 LWE 문제를 비밀인 대칭 행렬을 통해 MLWE 문제로 전환시킬 수 있기 때문이다. 그러므로 이 문제가 확장 가능함을 보이는 건 쉽다.

[0163] 시스템의 증명 가능한 안전성에 대해, 상황은 논문 [DiLi]에서 한 것과 흡사하다. 즉, 역시 같은 방식으로 증명 가능한 안전성을 논할 수 있다.

[0164] 이전에 이야기 했듯이, RLWE는 MLWE의 특별한 경우로 볼 수 있기 때문에, 매우 간단한 키 분배 시스템을 설립하기 위해 RLWE을 사용할 수 있다.

[0165] 우리는 환 R_q 로 $F_q[x]/x^n+1$ 을 선택한다. 증명 가능한 안전성을 입증하기 위해 적당한 매개변수로서 n과 q를 뽑는데, $n=2^k$이고 q=1 mod(2n) [LPR]이다. 우리는 증명 가능한 안전성 시스템에 대해, 이와 같은 매개변수와 오류 분포([LPR]의 χ와 같은)의 전통적인 관념을 따를 것이다.

[0166] 이 구조는 본질적으로 위의 시스템에 기초한다. 우리는 오류 분포 χ에 의해 환 R_q가 갖는 오류 문제를 적절하게 정의하고 있다. 그 문제는 다음과 같이 정의된다:

[0167] E = A×S + te'

[0168] 에 대해 우리는 한 쌍의 (A,E)를 갖고 있다. 여기서 A,S,e' 는 R의 원소이며, t는 작은 정수이고 e' 는 χ의 분포를 따르는 오류 원소이다. S는 고정된 원소이고 마지막으로 A는 임의로 선택되며 균등 분포를 따른다. 그리고 비밀 S를 찾는 것이 문제이다.

[0169] 우리는 중앙 서버를 이용하여 다음과 같은 방법을 통해 간단한 키 분배 시스템을 구축할 수 있다.

[0170] (1) 중앙 서버 역시 R_q에서 임의의 원소 M을 균등 분포에 따라 뽑을 수 있다.

[0171] (2) 중앙 서버는 각각의 사용자에게 A_i라는 공공 ID를 부여한다. 이때 A_i 는 R_q 에서 뽑은 작은 원소의 형태이므로 즉, χ와 같은 오류 분포를 따른다.

[0172] (3) 각각의 사용자는 중앙 서버에 의해 비밀키를 얻는다.

[0173] $$S_i=MA_i+te_i$$

[0174] 여기서 e_i 는 오류 분포 χ를 따른다.

[0175] (4) 만약 두 사용자 i와 j가 공유키를 성립하길 원하며, 이를 위해 사용자 i가

[0176] $$K_i=A_j\times S_i=A_jMA_i+tA_je_i$$

[0177] 를 계산하여 자신의 비밀키이자, j의 ID 행렬인 A_i 를 사용할 수 있고 사용자 j가

[0178] $$K_j=A_i\times S_j=A_jMA_i+tA_ie_j$$

[0179] 를 계산하여 자신의 비밀키를 사용할 수 있다면, 이제 다음과 같은 라운딩 기법을 이용해 공유키를 도출한다:

[0180] (a) 사용자 i는 크기가 n인 목록을 만들 것이다. 그 목록은 (a,b) 형태의 여러 쌍들로 구성된다. 이때 a= 0,…,n-1이다. 만약 K_i의 계수인 x^a가 [-(q-1)/4,(q-1)/4] 범위 안에 존재하면 b=1이고, 그렇지 않으면 b=0이다.

[0181] (b) i는 위 목록을 j에게 보낸다. 그런 다음에, 각자는 다음과 같은 방법으로 항목들을 t로 나눠 나머지를 계산한다.

[0182] 1) 만약 b=1이면, K_i와 K_j의 a번째 항목 각각을 t로 나눈다.

[0183] 2) 만약 b=0이면, (q-1)/2를 K_i와 K_j의 a번째 항에 더하고, [-(q-1)/4,(q-1)/4] 범위 안에 존재하도록 q로 나눈다. 그런 다음, t로 나누어 나머지를 구한다.

[0184] A_i와 e_i가 R_q의 작은 원소들이기 때문에, 우리는 $A_i\times e_i$역시 작다는 것을 알 수 있다. 이 점이 우리가 공유되는

비밀키를 실제로 갖게 되었음을 확실시하게 하며, 키 분배 역시 제공해 준다.

[0185] 여기서 우리는 RLWE 문제에서 곱셈에 대해 교환 법칙이 성립함을 적극적으로 사용한다. 우리의 구조에서 중요한 특성은 간단하고 쉽다는 점이다. 시스템의 증명 가능한 안전성 역시 간편하다.

[0186] 1.4 오류를 갖는 페어링에 기반한 새로운 시스템 IBM의 구조

[0187] 먼저 MLWE에 기반한 새로운 공개키 암호체계를 만든다. 암호 시스템을 구축하기 위해, 우리는 유사한 변수인 $q \approx n^3$, n^4 또는 n에 대한 유사한 다항 함수를 선택한다. 우리는 다시 오류 분포로서 K_{n^2}을 선택한다. 예를 들어 각각의 구성요소에서 오류 분포가 독립적이고 각각의 구성요소가 LWE의 경우에서처럼 일정한 이산 분포인 κ_σ을 따른다면 F_q에 대한 이산 정규 분포는 0 주변에서 표준 편차가 대략 $\sqrt{n}$이다. 더불어 분명히 우리는 높은 차원의 가우스 분포를 선택할 수 있다. 이 분포는 증명 가능한 안전성에 목적에 매우 편리해야 한다. 우리는 이 간단한 분포를 암호 시스템의 타당성에 관한 논쟁을 단순화하기 위해 선택한다. 물론 다른 매개변수를 선택할 수도 있다.

[0188] 이와 같은 배경을 바탕으로 우리는 다음과 같은 방법으로 MLWE의 문제에서와 같은 암호 시스템을 구축할 수 있다:

[0189] (1) 우리는 n×n 행렬 S를 선택한다. 행렬 S의 항목들은 작고 오류 분포를 따른다. 예를 들어, 각각의 항목들은 독립적으로 그리고 무차별적으로 오류 분포 κ_σ를 따른다.

[0190] (2) MLWE의 설정에서 우리는 한 쌍의 결과물 (A,E)를 얻을 것이다. 이때 E = A×S + e 또는 E = A×S + te이며 t는 t<<n로서 작다. 그리고 그것들이 우리의 암호 시스템에서 공개키로 형성된다. e는 어떤 오류 분포, 우리가 위에서 사용했던 것과 같은 분포를 따른다.

[0191] (3) S는 우리의 암호체계의 개인키이다.

[0192] (4) 메시지 m은 2진법 원소인 0과 1을 이용해 n×n행렬로 표현되거나, modular t에 대한 항목들, 즉, 0,1,…,t-1까지를 이용해 n×n행렬로 표현된다.

[0193] (5) 메시지를 보내는 사람은 S와 흡사한 n×n 형태의 작은 행렬 B를 고른다. 즉, B는 오류 분포 K_{n^2}를 따른다. 예를 들어, 각각의 항목들은 독립적으로 그리고 무차별적으로 분포 κ_σ를 따른다. 그런 다음 보낸 사람은 다음과 같이 암호화된 메시지를 계산한다.

[0194] $(D_1, D_2) = (B\times A + e_1, B\times E + e_2 + m(q/2))$,

[0195] 또는

[0196] $(D_1, D_2) = (B\times A + e_1, B\times E + te_2 + m)$

[0197] 여기서 e_1와 e_2는 e와 같은 오류 분포를 따르는, 독립적으로 선택된 오류 행렬이다.

[0198] (6) 해독하기 위해, 첫 번째 경우, 합법적인 사용자는 다음 식을 계산한다.

[0199] $$D_2-D_1\times S=(BE+e_2+m(q/2)-(BA+e_1)S)=eE+e_2-e_1S+m(q/2)$$

[0200] 여기서 모든 것은 F_q에서 이루어지고 우리는 행렬의 각 항목을 확인해 볼 수 있다. 즉, 만약 각 항목이 0 가까이 있으면 결과(output)는 0이고, (q-1)/2에 근접하면 결과는 1이다. 또는 실수 나눗셈과 같은 방법으로 각 항목들을 (q-1)/2로 나눈 후 0 또는 1로 바꾼다. 그러면 결과로서 m이 도출될 것이다. 두 번째의 경우, 합법적인 사용자가 다음 식을 t로 나누면 m이 유도된다.

[0201] $$D_2-D_1\times S=(BE+te_2+m-(BA+te_1)S)=teE+te_2-te_1S+m$$

[0202] A,B,e_i는 다른 오류 분포를 따를 수 있다.

[0203] 다소 큰 n을 이용하면 결과물을 통해 우리가 요구하는 만큼의 높은 확률을 가진 올바른 평문을 얻을 수 있다. 높은 확률로 해독할 수 있는 것은 다음과 같은 점 때문이다.

[0204] D_2-D1×S

[0205] =BE + e_2 + m(q/2)-(BA+e)S

[0206] =B×(A×S+e)+ e_2 + m(q/2) - (BA+e_1)×S

[0207] =B×e + e_2 - e_1×S + m(q/2)

[0208] B×e + e_2 - e_1×S 는 오류 항으로 보여질 수 있고, 이는 다음의 확률 변수에 대한 분포에 의해 결정된다. KE 또는 KD 시스템의 경우에서처럼 매개변수를 적절히 선택하면, 해독 과정은 n이 충분히 큰 수 일 때 분명히 올바른 답을 도출 할 것이다. 이는 두 번째 경우에서도 마찬가지이다.

[0209] 새로운 방법의 한 가지 핵심은, 계산 과정의 속도를 높이기 위해 우리는 행렬 곱셈 [CW]를 사용할 수 있기 때문에, 비트 당 속도에 대해 평균적으로 더 빠르게 암호화 할 수 있다는 점이다.

[0210] 여기서 우리는 행렬 곱셈에 대해 교환 법칙이 성립하지 않기 때문에, RLWE와 관계가 있는 시스템의 경우와는 달리, 두 개의 원소를 곱할 때 순서가 매우 중요함을 알고 있다.

[0211] 우리는 암호화하기 위해 같은 아이디어를 RLWE [LPR]에 적용할 수 있다. 이때 모든 원소는 환 R_q 안에 있고 E = A×S + te 이다. t는 작은 양의 정수이며, S의 원소들 역시 작고 오류 분포 K_{n^2}을 따른다. 다음과 같이 메시지를 암호화한다.

[0212] $$(D_1,D_2)=(BA+te_1,BE+te_2+m)$$

[0213] 그리고 다음을 계산하여 해독한다.

[0214] $$(BE+te_2+m-B(AS+te_1))(\mathrm{mod}\,t)$$

[0215] 이는 아래에 근거하여 유효하다.

$$D_2 - D_1 \times S$$
$$= BE + te_2 + m - (BA + t_1e_1)S$$
$$= B \times (A \times S + te) + te_2 + m - (BA + te_1) \times S$$
$$= tB \times e + te_2 - te_1 \times S + m$$

[0216]

[0217] t로 나누면 오류 항들이 작기 때문에 우리는 여지없이 본래의 평문으로 돌아가야 한다.

[0218] MLWE 문제를 위해 시스템의 증명 가능한 안전성을 얻는 것이 필요할 때, 분명 우리는 적절하게 분포를 선택해야 한다.

[0219] LWE 문제들에 관련된 격자에 기반을 둔 신원 기반 암호 시스템에는 몇 가지 버전이 있다 [ABB], [ABVVW], [BKPW]. 그러나 그것들은 다소 복잡해 보인다. 우리는 신원 기반 암호 시스템을 구축하기 위해 MLWE을 이용할

수 있다.

[0220] 중앙 서버를 통해 우리는 간단한 신원 기반 암호 시스템을 아래와 같은 과정으로 구축할 수 있다.

[0221] (1) 먼저 중앙 서버는 비밀 마스터 키로써 비밀 n×n 행렬 S을 뽑는다. 이때 S는 KE 또는 KD 시스템에서처럼, 오류 분포 같은 오류 분포 K_{n^2} 을 따르는 작은 원소이다.

[0222] (2) 더불어 중앙 서버는 균등 분포 또는 유사한 분포를 따르는 임의의 원소 M을 뽑는다. 이때 M은 반드시 역을 가져야 한다. 만약 한번에 이와 같은 M을 찾을 수 없다면, 찾을 때까지 계속해야 한다. q가 크면 만족하는 M을 찾을 확률이 높다. 그 다음에, 중앙 서버는 다음을 계산한다.

[0223] $M_1 = MS + te$

[0224] 이때 e는 오류 분포 K_{n^2} 을 따르는 작은 수이다.

[0225] (3) 중앙 서버는 마스터 공개키로서 M과 M_1을 공개한다.

[0226] (4) 각각의 사용자에게 중앙 서버는 공개 ID로서 A_i를 부여한다. 이때 A_i 는 오류 분포 K_{n^2} 을 따르는 작은 수이며 사용자를 구별하는 정보로부터 만들어 질 수 있다.

[0227] (5) 각자는 다음의 비밀키를 갖는다.

[0228] $$S_i = SA_i + tM^{-1}e_i$$

[0229] 이때 e_i의 항목들은 오류 분포 κ를 따르고 작다. M이 공개되어 있기 때문에 위의 비밀키는 다음의 주어진 것과 같다.

[0230] $MS_i = MSA_i + te_i$

[0231] (6) ID로서 A_i를 가진 사용자에게 새로운 공개키를 제공하기 위해, 누구든지 ID, 즉, A_i와 마스터 공개키를 사용할 수 있다. 마스터 공개키는 한 쌍의 (A_i, B_i) 형태이며 이때

[0232] $A_i = M$

[0233] 이고

[0234] $B_i = M_iA_i = MSA_i + teA_i$

[0235] 이다. 또한 이것은 위의 MLWE 암호 시스템을 사용하여 어떤 메시지를 암호화하는데 공개키로써 사용된다.

[0236] 이것은 신원 기반 암호 시스템을 제공한다.

[0237] S, A_i, e_i, e는 다른 오류 분포를 따를 수 있다.

[0238] A_i 와 e는 작기 때문에 $A_i \times e$ 역시 작다. 그리고 우리는 아래와 같이 알고 있다.

$$MS_i - B_i = MS_i - B_i$$
$$= M(SA_i + tM^{-1}e_i) - MSA_i + teA_i$$
$$= MSA_i + tMM^{-1}e_i) - MSA_i + teA_i$$
$$= te_i - teA_i$$

[0239]

[0240] e,A_i 그리고 e_i가 작기 때문에 $e - A_ie_i$역시 작고 $te_i - tA_ie_i$도 작다. 그러므로 입력값이 (A_i, B_i)일 때 MLWE 문제의 정답은 S_i이다. 즉, S_i는 암호 해독에 사용될 수 있는 비밀키이며, 결과적으로 구조가 유효하다. 이제 안전성을 보장하기 위해 적절하게 매개변수를 뽑을 필요가 있다.

[0241] 이 구조의 핵심은 쉽고 간단하다는 것이다. 이 시스템의 증명 가능한 안정성 역시 쉽고 간단하다.

[0242] 이러한 구조는 RLWE 문제를 이용하여 확장될 수 있다. 우리는 환 R로 $F_q[x]/x^n+1$ 를 선택한다. 증명 가능한 안정선을 입증하기 위해 적당한 매개변수로서 n과 q를 선택하는데, $n=2^k$이고 $q=1 \bmod(2n)$이다 [LPR]. 그러나 안전한 응용을 위해 다른 매개변수를 선택할 수 있다.

[0243] 이 구조는 직접적으로 RLWE의 암호 시스템에 기초한다 [LPR]. 다시 말해, 우리는 환 R이 갖는 오류 문제를 적절하게 정의하고 있다. 그 문제는 다음과 같이 정의된다. 우리는 한 쌍의 (A,E)를 갖고 있다. 이때

[0244] $E = A \times S + te'$

[0245] 이며 A,S,e'는 R_q의 원소이다. 여기서 t는 작은 정수이고 e'는 오류 분포 χ를 따르는 오류 원소이며 S는 고정된 원소, A는 임의로 선택되며 균등 분포를 따른다. 그리고 비밀 S를 찾는 것이 문제이다. 우리는 RLWE 문제 을 이용해 공개키 암호 시스템을 구축할 수 있다는 것을 알고 있다 [LPR]. 여기서 A와 E는 공개키로써 역할을 하고, 비밀 S는 작아야 하며 개인키로써 역할을 한다. ring-LWE 문제에서 곱셈에 교환 법칙이 성립한다는 사실을 우리는 이용할 수 있다.

[0246] 중앙 서버에서 다음과 같이 간단하고 기반으로 독자적인 암호 시스템을 구축할 수 있다.

[0247] (1) 중앙 서버는 비밀 마스터키로 R의 비밀 S를 선택하고, 비밀 S는 일정한 오류 분포 χ를 따르는 선택된 작은 원소이다.

[0248] (2) 중앙 서버는 정규 분포인 R에서 무작위 원소 M을 선택하고, M은 역수를 갖는다. 보장한다. 맨 처음 원소 M을 찾을 수 없다면 찾을 때까지 반복할 것이다. q가 클 때, 이와 같은 M을 찾기 위한 성공 확률은 높다. e가 작고 오류 분포 χ를 따른다고 할 때, 중앙서버는

[0249] $M_1 = MS + te$

[0250] 을 계산할 것이다.

[0251] (3) 중앙서버는 마스터 공개키로써 M과 M_1을 공표할 것이다.

[0252] (4) 각각의 사용자에게 중앙 서버는 공개적인 ID, A_i를 할당하고, 여기에서 A_i는 R_q에서 작은 요소이고 오류 분포 χ를 따른다.

[0253] (5) 각각의 사용자는 다음과 같은 비밀키를 받는다:

[0254] $$S_i = SA_i + tM^{-1}e_i$$

[0255] 여기서 e_i는 R에서 작은 요소이고 오류 분포 χ를 따른다. 이것은 M이 공개되었기 때문에 다음과 같다.

[0256] $MS_i = SMA_i + te_i$

[0257] (6) 어떤 누구이든지 ID A_i 를 부여받은 사용자를 위한 새로운 공개키를 만들기 위해서 A_i인 ID와 마스터 공개키를 사용할 수 있다. A_i는 $A_i = M$, $B_i = A_iM_1 = A_iMS + tA_ie = MSA_i + tA_ie$인 순서쌍 (A_i, B_i),로 주어져있다. 그리고 새로운 공개키는 모든 메시지를 암호화 하는 공개키로서 사용된다.

[0258] S, A_i, e, e_i 처럼 작은 요소들은 서로 다른 오류 분포들을 따를 수 있다.

[0259] A_i 와 e는 R에서 작은 요소이기 때문에 $A_i \times e$ 역시 작은 요소이다. 가환환이기 때문에

[0260] $$S_iA_i - B_i = S_iM - B_i$$

[0261] $$= M(SA_i + tM^{-1}e_i) - MSA_i + A_ite$$

[0262] $$= MSA_i + tMM^{-1}e_i - MSA_i + A_ite$$

[0263] $$= te - tA_ie_i$$

[0264] 이다. e와 A_i는 작기 때문에 $e - A_ie_i$ 역시 작으므로 $te - tA_ie_i$는 작다. 그러므로 S_i는 문제의 입력으로 순서쌍 (A_i, B_i)를 갖는 ring LWE 문제에 대한 해결책이다. 그러므로 S_i는 복호화에 사용될 수 있는 비밀키이다.

[0265] 우리는 비슷한 과정을 이용하는 계층적 IBE 시스템(hierarchical IBE system)을 쉽게 구축할 수 있고 각각의 사용자는 중앙 서버처럼 될 수 있다.

[0266] 구성의 중요한 특징은 간단하고 복잡하지 않으며 효과적이다. 시스템의 증명 가능한 안전성 역시 복잡하지 않다.

[0267] 환에서 오류를 갖는 페어링을 이용하는 위의 모든 시스템에서

[0268] $$f(x) = \prod f_i(x) + g(x)$$

[0269] 형태의 다항식을 이용한다. 이때 각 f_i, g(x)는 0이 아닌 2, 3 개의 항을 갖는 것 같이 적은 조건을 지니고 있는 매우 드문 행렬이다. 이러한 종류의 다항식을 이용하는 것은 암호화와 복호화 계산에 속도를 낼 수 있다.

[0270] 참고문헌

[0271] [ABB] S. Agrawal, D. Boneh, X. Boyen: Efficient Lattice (H)IBE in the Standard Model.In proceedings of Eurocrypt 2010, Lecture Notes in Computer Science, Volume 6110, pp.553-572, 2010.

[0272] [ABVVW] S. Agrawal, X. Boyen, V. Vaikuntanathan, P. Voulgaris, H.Wee: Fuzzy Identity Based Encryption from Lattices. IACR Cryptology ePrint Archive 2011: 414 (2011).

[0273] [ACPS] B. Applebaum, D. Cash, C. Peikert, A. Sahai; Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems. Advances in Cryptology-CRYPTO 2009, Lecture Notes in Computer Science, Volume 5677 pp 595-618, 2009.

[0274] [BKPW] M. Bellare, E. Kiltz, C. Peikert, B. Waters: Identity-Based (Lossy) Trapdoor Functions and Applications. In Proceedings of EUROCRYPT 2012, Lecture Notes in ComputerScience, Volume 7237, pp 228-245 2012.

[0275] [BSHKVY] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung: Perfectly-Secure Key Distribution for Dynamic Conferences. in Advances in Cryptology?Crypto 92, Lecture Notes in Computer

Science, Volume 740, pp 471-486, 1993.

[0276] [BKW] A. Blum, A. Kalai, and H.Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. Journal of the ACM, 50(4), pp506-19, 2003.

[0277] [COP] D. Coppersmith, Shmuel Winograd, Matrix multiplication via arithmetic progressions, Journal of Symbolic Computation - Special issue on computational algebraic complexity archive 9 (3), pp 251-280, 1990.

[0278] [DiHe] W. Diffie, M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory 22 (6), pp 644-54, 1976.