情 報 保 護 學 會 誌
第 16 卷 第 4 號, 2006. 8

격자 이론을 이용한 공개키 암호의 분석 사례 고찰

한 대 완*, 염 용 진*

요 약

Lenstra 등에 의하여 LLL 알고리즘이 처음 개발된 이래 최근까지 격자 이론은 공개키 암호의 분석 및 안전성 증명에 광범위하게 이용되어지고 있다. 초창기 Knapsack 계열 암호의 분석에 부분적으로 활용되었던 격자 이론은 1990년대에 인수분해, Diffie-Hellman, 격자 기반 공개키 암호로 그 분석 적용 분야가 확대되었고, RSA-OAEP를 비롯한 여러 암호 시스템들의 안전성 증명 등에도 중요한 도구로 활용되었다. 본 논문에서는 암호학의 도구로 활용되는 격자 이론의 개요를 살펴보고, 공개키 암호 분야의 분석에 있어 격자 이론이 활용된 사례들을 각 분야별로 결과 위주로 소개한다.

Ⅰ. 서 론

격자 이론(lattice theory)이란 n차원 실공간에 있는 점들의 일정한 배열에 관한 연구로서 19세기부터 정수론과 결정학에서 나타나기 시작하여 수학과 물리학 등에서 오랜기간 동안 연구되어온 분야이다. 이러한 격자이론이 암호학에서 주목을 끌기 시작한 것은 Lenstra, Lenstra, Lovasz가 개발한 격자 축소 알고리즘(lattice reduction algorithm)인 LLL 알고리즘[1]이 등장한 20여 년 전부터이다. 1978년 Merkle과 Hellman에 의해서 개발된 배낭문제를 이용한 공개키 암호는 제안 초기 안전할 것으로 믿어졌으나, 1983년에 LLL 알고리즘을 이용한 공격에 의해서 그 취약성이 밝혀졌다. 그 이후, 격자 축소 알고리즘의 성능을 개선하기 위한 연구들이 많이 진행되었으며, 다시 이러한 알고리즘들은 RSA, DSA 등 대표적인 공개키 암호 및 서명 알고리즘들의 안전성 분석에 활용되었다.

한편, 1996년 Ajtai는 격자이론에서 오랫동안 미해결 문제로 남아있던 SVP가 randomized reduction 가정 하에서 NP-hard임을 증명하였고, Dwork과 함께 이러한 문제의 어려움에 기반한 공개키 암호를 제안하였다. 이후, GGH를 비롯하여 격자 기반 공개키 암호의 개발이 활발하였으나, 이러한 암호들은 대부분 다시 격자 축소 알고리즘을 이용한 분석 방법으로 안전하지 않음이 밝혀졌다. 현재까지는 NTRU만이 실용적이면서도 안전한 파라미터 설정이 가능한 암호로 알려져 있다.

격자 이론은 암호학 분야에서 아직까지는 개발보다는 분석의 도구로 많이 활용되고 있으며, 최근에도 이와 관련된 연구 결과들이 지속적으로 발표되고 있다. 본 논문에서는 암호학의 도구로 활용되는 격자 이론의 개요를 간략히 살펴보고, 공개키 암호 분석에 있어 격자 이론이 활용된 사례들을 Knapsack, 인수분해, Diffie-Hellman, 격자 이론 기반 공개키 암호 등의 각 분야별로 소개한다.

Ⅱ. 격자 이론의 개요

1. 관련 정의들

격자란 R^n의 이산 부분군(discrete subgroup)을 말한하며, 아래와 같이 R^n 상의 일차 독립인 벡터 $v_1, \cdots, v_d$들의 일차 선형 결합으로 나타나는 벡터들의 집합으로 정의되기도 한다.

$$L = \sum_{i=1}^{d} n_i v_i | n_i \in Z$$

이 때, 벡터 v_i들의 집합을 격자의 기저(basis)라고 하는데, 일반적으로 기저는 v_i를 행으로 갖는 행렬 V로 표현된다. 또한, 일차독립인 벡터의 개수 d를 격자

* ETRI부설 국가보안기술연구소({dwh;yjyeom}@etri.re.kr)

의 차원(dimension 또는 rank)이라고 하며 $\dim(L)$로 표기한다. $\dim(L) \geq 2$인 경우에는 동일한 격자 L에 대하여 무수히 많은 기저가 존재하며, 이러한 기저들 V, W 사이에는 행렬식이 ± 1인 정수 계수 행렬 U가 존재하여 $V = UW$가 성립한다. 따라서, 격자의 모든 기저들은 동일한 Gramian 행렬식 $\det_{1 \leq i,j \leq d} < b_i, b_j >$을 가지며, 이 Gramian 행렬식의 제곱근을 격자의 볼륨 $vol(M)$이라고 정의한다. 특별히, 격자의 차원이 n과 같은 경우의 볼륨은 기저들로 이루어진 행렬의 행렬식의 절대값과 같게 된다.

격자는 이산 집합이므로 격자 안에는 0이 아닌 가장 짧은 벡터가 존재한다. 이 벡터의 길이를 격자 L의 첫 번째 최소값(first minimum)이라고 정의하며, $\lambda_1(L)$로 표기한다. $\lambda_1(L)$의 개념을 확장하여 귀납적으로 연속된 최소값(succesive minima)을 다음과 같이 정의한다. 격자 L의 i-번째 최소값 $\lambda_i(L)$은 $(i-1)$-번째 최소값 $\lambda_{i-1}(L)$을 결정하는 $i-1$개의 벡터들에 대해서 일차독립이 되는 L의 벡터들 중에서 가장 짧은 벡터의 길이로 정의된다. $\lambda_2(L)/\lambda_1(L)$을 L의 격자 틈(lattice gap)이라고 정의하는데, 격자 틈은 격자 축소 알고리즘의 효율성과 밀접한 관련이 있다.

한편, Gaussian heuristic에 의하여 이상적인 경우의 격자 L에 있어 $\lambda_1(L)$은 다음과 같이 예상할 수 있다.

$$\lambda_1(L) \sim \sqrt{\frac{d}{2\pi e}} vol(L)^{\frac{1}{d}}$$

2. 격자 이론과 관련된 문제들

격자 이론과 관련하여 유명한 문제들로는 SVP, CVP, 및 SBP가 있다.

- SVP(Shortest Vector Problem): 격자 L의 임의의 기저가 주어졌을 때, L의 가장 짧은 벡터 u를 찾는 문제, 즉, $\|u\| = \lambda_1(L)$인 u를 찾는 문제.
- CVP(Closest Vector Problem): 격자 L의 임의의 기저와 L에 속하지 않는 임의의 벡터 $v \in R^n$가 주어졌을 때 v와 가장 거리가 가까운 L의 벡터 u를 찾는 문제. 즉, $\|u-v\| \leq \|w-v\|$ for all $w \in L$인 u를 찾는 문제
- SBP(Shortest Basis Problem): 격자 L의 임의의 기저가 주어졌을 때, 사전에 정의된 "짧은" 기저를 찾는 문제. 일반적으로 "짧은" 기저는 각 기저 벡터들의 길이가 짧고 벡터들 사이의 각이 수직에 가까운 기저를 의미한다.

SVP와 CVP를 바로 푸는 것이 매우 어렵기 때문에 다음과 같이 찾고자 하는 벡터의 조건을 완화시킨 근사 버전의 문제들도 많이 연구되고 있다.

- ASVP(Approximate SVP): SVP와 동일한 조건 하에서, d에 대한 근사 함수 f가 존재하여 $\|u\| \leq f(d)\lambda_1(L)$인 u를 찾는 문제.
- ACVP(Approximate CVP): CVP와 동일한 조건 하에서, d에 대한 근사 함수 f가 존재하여 $\|u-v\| \leq f(d)\|w-v\|$ for all $w \in L$인 u를 찾는 문제.

이 문제들의 계산 복잡도를 증명하기 위한 연구들이 계산 이론에서 많이 진행되었으며, 주요 결과는 다음과 같다.

- SVP는 randomized reduction 하에서 NP-hard이다.
- ASVP with $f(d) \leq \sqrt{2}$는 randomized reduction 하에서 NP-hard이다.
- CVP는 NP-hard이다.
- ACVP with $f(d) = 2^{\log^{1-\varepsilon} d}$는 NP-hard이다.

그 밖에 $\|\cdot\|_\infty$ 노름 하에서의 위 문제들의 복잡도 등 격자 이론과 관련된 문제들의 계산 복잡도와 관련한 자세한 내용은 참고문헌 [2]를 참조하기 바란다.

3. CVP와 SVP의 근사 해결 알고리즘들

d에 대한 다항식 근사 함수 $f(d)$를 가지는 ACVP와 ASVP를 해결하는 다항식 시간 알고리즘은 아직까지 알려지지 않고 있다. 단, $f(d)$가 d에 대한 준지수(subexponential) 함수인 경우에는 다항식 시간 알고리즘들이 존재하며, 이 중 LLL과 같은 격자 축소 알고리즘들을 이용한 알고리즘들이 가장 많이 사용된다. LLL은 임의의 주어진 기저를 특정한 성질을 만족하는 기저로 변환해 주는 알고리즘으로, 이 때 LLL의 출력으로 나오는 기저에 포함된 벡터들이 ASVP의 해가 될 수 있다. 즉, 격자 L의 임의의 기저가 주어졌을 때 LLL 알고리즘은 $O(d^6)$ 시간 안에 다음 조건을 만

족하는 기저 $(b_1,\cdots,b_d)$를 출력한다.

$$\|b_1\| \le 2^{(d-1)/4} vol(L)^{1/d},$$
$$\|b_i\| \le 2^{(d-1)/2} \lambda_i(L).$$

따라서, LLL은 SVP를 $2^{(d-1)/2}$의 근사량으로 해결할 수 있는 다항식 시간 알고리즘이 된다.

ACVP를 푸는 알고리즘으로는 Babai의 nearest plane 알고리즘과 embedding 방법이 있는데, 실제 암호 분석에서는 embedding 방법이 많이 사용된다. 이 방법은 R^n상의 d차원 CVP를 R^{n+1}상의 $(d+1)$차원 SVP로 변환하여 푸는 방식으로, 먼저 CVP의 입력 기저 $(b_1,\cdots,b_d)$와 벡터 v에 대하여, $(b_i,0)\in R^{n+1}$들과 $(v,1)\in R^{n+1}$에 의해 생성되는 $(d+1)$차원 격자를 생각한다. 만일 u가 원래 CVP의 해였다면, $(v-u,1)$은 새로 생성된 격자의 SVP의 해가 될 확률이 높게 된다. 따라서, 새로운 격자의 SVP를 LLL 등의 알고리즘을 이용하여 풂으로써 원래 CVP의 해를 풀 수 있게 된다.

결국, CVP나 SVP의 해결에는 격자 축소 알고리즘이 요긴하게 사용되며, 따라서 격자 축소 알고리즘의 성능을 높이기 위한 연구들도 많이 진행되었다. 이와 관련하여, Schnorr는 LLL을 변형하여 BKZ라고 불리는 일련의 격자 축소 알고리즘들을 제안하였다 [3]. BKZ는 블록 크기라고 불리는 파라미터 k를 조정함에 따라 각각 다른 성능을 보이는 알고리즘으로, k가 고정되면 $O(d^4k^{k/2})$시간 안에 $O(k^{d/k})\lambda_1(L)$보다 작은 벡터를 출력해 준다. 따라서, k가 증가함에 따라 출력 벡터의 길이는 짧아지지만 상대적으로 수행 시간이 길어지게 된다. BKZ는 현재까지 제안된 격자 축소 알고리즘들 가운에 수행 속도와 근사 정확성 면에서 가장 효율적인 격자 축소 알고리즘으로, 실제 성능은 이론적인 수치보다 훨씬 좋게 나타난다.

Ⅲ. Knapsack 계열 공개키 암호의 분석

1. Knapsack 문제

격자 이론이 암호학과 관련을 맺게 된 것은 격자 축소 알고리즘이 knapsack 문제 기반 공개키 암호의 분석에 효과적으로 사용되면서부터이다.

Knapsack 문제란, 양의 정수의 집합 $a_1,\cdots,a_n$과 양의 정수 $s=\sum_{i=1}^{n} x_i a_i$ $(x_i\in 0,1)$가 주어졌을 때, x_i를 구하는 문제를 말한다. 1978년에 Merkle과 Hellman은 knapsack 문제에 기반한 공개키 암호(MH)를 처음으로 제안하였다 [4]. Shamir는 1982년에 Lenstra의 integer programming 알고리즘을 이용하여 간단한 버전의 MH 스킴을 분석하였고, 같은 해 Adleman은 LLL을 이용하여 더욱 간단한 분석을 시도하였다 [5]. 그 후, Brickell은 보다 일반적인 중첩된 MH 스킴에 대한 분석을 시도하여, 현실적으로 사용 가능한 파라미터를 갖는 MH의 경우 안전하지 않음을 보였다 [6,7]. MH의 분석 이후에도 knapsack 문제를 이용한 공개키 암호의 개발이 계속 시도되었지만, 모두 격자 공격 내지는 저밀도 공격(low-density attack)에 의하여 분석되었고, 가장 최근까지 분석되지 않았던 knapsack 기반 암호인 Chor-Rivest 암호 시스템[8]의 경우도 대수적인 분석 방법으로 역시 안전하지 않음이 밝혀졌다.

2. Knapsack 공개키 암호에 대한 저밀도 공격

이번 절에서는 knapsack 기반 공개키 암호의 분석에 가장 유용하게 사용되는 저밀도 공격에 대하여 간단히 살펴본다.

$s=\sum_{i=1}^{n} x_i a_i$ $(x_i\in 0,1)$가 knapsack 문제의 입력이라고 하자. 확장된 GCD 알고리즘을 이용하면 $s=\sum_{i=1}^{n} y_i a_i$가 되는 정수 $y_1,\cdots,y_n$은 쉽게 구할 수 있다. 이제 다음과 같은 일차 방정식을 생각하자.

$$z_1 a_1 + \cdots + z_n a_n = 0.$$

이 방정식의 해 $(z_1,\cdots,z_n)\in R^n$들의 집합은 R^n상의 격자 L을 이루고, $X=(y_1-x_1,\cdots,y_n-x_n)$가 L에 속함은 쉽게 알 수 있다. 이제, 또 다른 R^n상의 벡터 $Y=(y_1-1/2,\cdots,y_n-1/2)$를 생각해 보자. 그러면, X와 Y의 거리는 정확히 $\sqrt{n/4}$이 되고, X가 L 안에 있는 벡터들 중 Y와의 거리가 가장 짧은 벡터가 됨을 쉽게 보일 수 있다. 따라서, knapsack 문제는 (L, Y)를 입력으로 갖는 CVP로 귀착되고, 격자 L이 특정한 성질을 만족할 경우 LLL 등을 이용하여 해당 CVP를 풂으로써 원래 knapsack 문제의 해를 구할 수 있게 된다. 여기서, L이 만족해야 하는 성질은 a_i들의 조건과 관련이 있는데, 이와 관련된 개념이 다음과 같이 정의되는 격자 밀도(density) d이다.

$$d=\frac{n}{\max_{1\le i\le n}\log_2 a_i}.$$

2장에서 언급하였듯이 CVP는 주로 embedding

방법에 의하여 풀게 된다. 그런데, embedding 방법은 $\|X-Y\|$가 $\lambda_1(L)$보다 작은 경우에 원하는 해를 찾을 수 있다. $\lambda_1(L)$은 $\sqrt{\frac{n}{2\pi e}}vol(L)^{\frac{1}{n}}$로 근사할 수 있고, a_i들이 높은 확률로 서로 소일 것이므로, $vol(L)$은 다음과 같이 근사할 수 있다.

$$vol(L)=(\sum_{i=1}^{n}a_i^2)^{1/2}\sim 2^{n/d}\sqrt{n}.$$

따라서, knapsack의 해를 구하기 위한 조건은,

$$\sqrt{\frac{n}{4}}\le 2^{1/d}\sqrt{\frac{n}{2\pi e}}$$

가 되고, 이는 다시 아래와 같이 근사할 수 있다.

$$d\le\frac{1}{\log_2\sqrt{\pi e/2}}\sim 0.955....$$

d가 1보다 큰 경우는 하나의 암호문에 대응하는 평문이 다수가 되기 때문에 암호학적으로 의미가 없게 된다. 따라서 $d<1$인 경우의 knapsack만이 공개키 암호의 설계에 활용될 수 있다. 그런데, $d\le 0.955$인 경우는 위 방법에 의하여 해를 구할 수 있기 때문에, 결과적으로 대부분의 knapsack 기반 암호는 안전하지 않게 된다.

현실적인 관점에서 보면, LLL 등의 격자 축소 알고리즘이 정확한 SVP 오라클은 아니기 때문에 격자의 차원이 커지면 위 분석 결과가 틀리게 된다. 그러나, 실험적으로 n이 100-200인 경우에는 위 방법으로 대부분의 knapsack 기반 암호는 분석되었다. 그보다 큰 차원의 경우에는 공격이 안 될 수도 있지만, 그러한 경우에는 키 크기 등이 너무 커지기 때문에 비현실적인 암호 알고리즘이 된다. 결론적으로, 현실적으로 사용 가능한 파라미터를 갖는 knapsack 기반 암호는 격자 이론 기반 공격에 의하여 모두 분석되었다고 볼 수 있다.

Ⅳ. 인수분해 기반 공개키 암호에의 적용

격자 이론이 공개키 암호 연구에 있어 더욱 각광을 받게 된 것은 1990년대 중반 인수분해 기반 공개키암호의 분석 및 안전성 증명에 요긴하게 사용되면서부터이다. 이를 가능하게 한 것이 다음 절에서 소개할 Coppersmith의 정리들이다. 최근 10여 년 동안 발표된 RSA의 안전성 분석 결과들은 모두 Coppersmith의 정리로부터 시작된다고 해도 과언이 아니다. 재미있는 사실은, 이 정리들이 특별한 조건을 만족하는 RSA 암호 및 서명 알고리즘의 공격에 활용되기도 했지만, 한편으로는 RSA-OAEP와 같은 패딩 방식의 안전성을 증명하는데도 동시에 활용되었다는 점이다.

Coppermsith의 정리들과 인수분해 기반 공개키 암호들의 분석 관련 내용을 상세히 설명하는 것은 본 논문의 성격에 맞지 않으므로 본 장에서는 결과 위주로 간단히 소개하고자 한다.

1. Coppersmith의 정리들

일반적으로 일변수 모듈러 고차방정식의 해를 구하는 문제나 정수 계수 다변수 방정식의 해를 구하는 문제는 어려운 것으로 알려져 있다. Coppermsith는 1996년 Eurocypt에 발표된 두 편의 논문[9,10]을 통해 위 두 방정식의 작은 근을 찾는 방법과 관련하여 다음 정리들을 증명하였는데, 이 정리들이 향후 인수분해 기반 공개키 암호들의 분석에 큰 영향을 끼치게 되었다.

정리1. P를 차수가 δ이고 인수분해를 모르는 N에 대한 모듈러 일변수 모닉 다항식이라고 하자. 그러면, $P(x_0)\equiv 0 \pmod N$이고 $|x_0|\le N^{1/\delta}$를 만족하는 모든 x_0를 $(\log N,\delta)$에 관한 다항식 시간 안에 구할 수 있다.

Coppersmith는 LLL 알고리즘을 이용하여 정리 1을 증명하였다. RSA의 암호문 $c=m^e \pmod N$으로부터 평문 m을 구하는 것은 $x^e-c\equiv 0 \pmod N$의 해를 구하는 것과 같다는 점에서 위 정리가 RSA의 분석에 활용될 수 있다는 점은 쉽게 알 수 있다.

정리 1이 일변수 모듈러 다항식의 작은 해를 구하는 문제라면, 아래의 정리 2는 정수 계수 이변수 다항식의 작은 해를 구하는 문제와 연관된다.

정리2. 이변수 다항식 $P(x,y)$의 각 변수별 최고 차수가 δ 이하이고, 계수들이 서로 소이고, X,Y가 구하고 싶은 해 x_0,y_0의 절대값의 상한이라고 하자. 또한, $\hat{P}(x,y)=P(Xx,Yy)$로 정의하고, D를 $\hat{P}$의 계수들의 최대값의 절대치라고 하자. 만약 $XY<D^{2/(3\delta)}$이면, $P(x_0,y_0)=0, |x_0|<X, |y_0|<Y$를 만족하는 (x_0,y_0)를 $(\log D,\delta)$에 관한 다항식 시간 안에 구할 수 있다.

위 정리는 2보다 큰 다변수 방정식으로도 확장이 가능하며, 다항식의 형태에 따라서 상한 값들도 향상시킬 수 있다. 정리 2는 특정한 조건을 만족하는 경우의 RSA 모듈러스의 인수분해 및 인수분해 기반 공개키 암호들의 공격에 활용되었는데, 이와 관련된 내용들은 다음 절들에서 살펴보기로 한다.

2. RSA에 대한 분석

격자 이론을 이용한 RSA 분석은 앞 절에서 소개한 Coppersmith의 정리들을 직접 적용하거나 그 정리들의 변형 및 개선된 정리들을 적용함으로써 얻어지며, 크게 암호화 지수 e가 작은 경우와 복호화 지수 d가 작은 경우로 나뉘어 시도되었다.

- e가 작은 경우[11]: 평문의 일부 정보를 아는 경우 암호문으로부터 평문 전체를 복구하는 공격이다. 예를 들어, 암호화를 할 때 평문의 고정된 위치에 패딩을 사용하는 경우 패딩의 랜덤성이 떨어진다면 안전성에 문제가 될 수 있다. 그러나, 이 공격은 e가 3 정도로 매우 작을 경우에만 적용 가능하며, 65537 정도만 돼도 적용되지 않는다.
- d가 작은 경우: d가 N에 비하여 매우 작은 경우 암호문으로부터 d 전체를 복구하는 공격이다. 격자 이론이 도입되기 전에도 $d \le N^{0.25}$인 경우의 공격이 Wiener에 의하여 제안되어 있었다. Boneh와 Durfee는 Coppersmith의 기법을 이용하여 $d \le N^{0.292}$인 경우로 공격을 확장하였다 [12]. Boneh 등의 공격은 p와 q의 크기가 서로 비슷한 경우(balanced)만 적용되었지만, 후에 Durfee와 Nguyen은 unbalanced RSA의 경우로 공격을 확장하였다 [13].

격자 이론을 이용한 RSA의 분석은 May와 Bloomer 등을 중심으로 최근까지도 기존의 결과들보다 향상된 결과들이 발표되고 있다 [14-18].

3. RSA 함수의 안전성 증명

격자 이론은 RSA의 공격 뿐 아니라, 반대로 RSA의 안전성을 증명하는 도구로도 유용하게 활용되었다. RSA가 능동적 선택 암호문 공격(ACCA)에 안전하려면 적절한 패딩 스킴을 적용한 후 암호화해야 한다. 이러한 패딩 스킴으로는 Bellare와 Rogaway가 제안한 RSA-OAEP가 있는데, 이 패딩 스킴의 안전성을 증명하는데 격자 이론이 유용하게 사용되었다.

Shoup은 e가 3인 경우의 RSA-OAEP의 안전성을 정리 1을 이용하여 증명하였고 [19], Fujisaki 등은 임의의 e에 대한 안전성을 또 다른 격자 문제의 해결을 통하여 증명하였다 [20]. 또한, Boneh는 RSA와 Rabin 함수에 대한 간결화된 OAEP를 제안하였는데 [21], 이 패딩 스킴의 안전성을 증명하는 데에도 역시 Coppersmith의 정리(Rabin)와 선형 방정식의 작은 해를 찾는 문제(RSA)를 통한 격자 이론이 사용되었다.

한편, RSA의 안전성은 인수분해의 어려움과 긴밀한 관계가 있다. 일반적으로 RSA 암호화 함수의 역을 구하는 것은 인수분해보다는 쉬울 것이라고 예상되고 있다. 이와 관련된 또 하나의 문제는 RSA의 공개키로부터 비밀키를 복원하는 문제와 인수분해와의 관계인데, 이 문제 또한 Coppersmith의 정리를 이용하여 두 문제의 어려움이 다항식 시간으로 동등하다는 사실이 May에 의해 비교적 최근에 밝혀졌다 [22].

V. DH 기반 공개키 암호의 분석

1. Diffie-Hellman 문제의 비트 안전성 증명

격자 이론이 기반 문제의 안전성을 증명하는데 활용된 또 하나의 예로, 유한 소수체(finite prime field) 상의 Diffie-Hellman (DH) 문제의 비트 안전성 증명 문제가 있다.

유한 소수체 상의 DH 문제란, 소수 q, 순환 군 $G=Z_q^*$, G의 생성원 g, 및 G의 원소 g^a와 g^b가 주어졌을 때, g^{ab}를 G에서 계산하는 것이 어렵다는 문제이다. Boneh와 Venkatesan은 [23]에서 동일한 가정 하에, g^{ab}의 최상위 ℓ비트만을 알아내는 것이 g^{ab} 전부를 알아내는 것과 동치라는 사실을 보였다. 이를 보다 엄밀히 기술하면 다음 정리와 같다.

정리3. q를 n비트 소수, g를 Z_q^*의 생성원이라고 하자. ϵ을 고정하고, $\ell=\ell(n)=\lceil \epsilon\sqrt{n} \rceil$로 놓자. 주어진 q,g,g^a,g^b로부터 g^{ab}의 최상위 ℓ비트를 출력하는 다항식 시간 알고리즘이 존재한다고 가정하자. 그러면, q,g,g^a,g^b와 $q-1$의 인수분해가 주어졌을 때, g^{ab}를 출력하는 다항식 시간 알고리즘 또한 존재한다.

위 정리의 증명에는 hidden number problem (HNP)이라고 불리우는 다음 문제의 해를 구하는 과정이 핵심적으로 사용되었다.

정의(HNP). Z_q^*에서 서로 독립적으로 랜덤하고 균일하게 선택된 $t_1,\cdots,t_d$와 모든 i에 대한 $MSB_\ell(\alpha t_i)$ 값이 주어졌을 때, $\alpha \in Z_q$를 구하는 문제.

Boneh 등은 HNP를 특정 격자 상의 CVP 문제로 변환하여 해결함으로써 정리 3을 증명하였다. 즉, 아래 행렬의 행벡터에 의해 생성되는 $(d+1)$차원 격자 L을 생각해 보자.

$$\begin{pmatrix} q & 0 & \cdots & 0 & 0 \\ 0 & q & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & q & 0 \\ t_1 & t_2 & \cdots & t_d & 1/2^{\ell+1} \end{pmatrix}$$

이제, $a_i = MSB_\ell(\alpha t_i \bmod q)$라고 하자. 그러면, 벡터 $T=(a_1,\cdots,a_n,\alpha/2^{\ell+1})$는 L에 포함됨을 알 수 있고, $A=(a_1,\cdots,a_n,0)$는 T와의 거리가 매우 가까우므로, L에 매우 가까운 벡터이다. 따라서, (L,T)를 입력으로 하는 CVP를 풂으로써 α를 구할 수 있게 된다.

Boneh 등의 증명에서는 t_i들이 균일하게 분포해야 된다는 강한 조건이 있었으나, 그 후 이같은 조건을 완화시켜 보다 일반적인 환경에서의 DH 비트 안전성 증명도 발표되었고 [24], 유한 소수체가 아닌 보다 일반적인 수학적 대상 위에서의 HNP의 해결에 대한 결과들도 발표되었다 [25,26].

2. DH 기반 전자서명의 분석

HNP의 격자 분석법을 통한 해결이 한편으론 DH 프로토콜의 안전성을 증명하는데 기여하였으나, 역으로 DH 기반으로 설계된 DSA 전자 서명의 취약성을 밝히는데도 활용되었다.

DSA의 파라미터는 512비트 이상의 소수 p, $p-1$을 나누는 160비트 소수 q, 위수가 q인 Z_p의 원소 g로 구성된다. 사용자의 비밀키 α는 Z_q^*의 임의의 원소, 공개키 β는 $g^\alpha \bmod p$로 선택된다. 평문 m에 대한 서명값은 Z_q^*의 임의의 원소 k를 선택한 후, SHA-1 해쉬함수 h를 이용하여 아래와 같이 계산한 (r,s)가 된다.

$$r=(g^k \bmod p) \bmod q$$
$$s=k^{-1}(h(m)+\alpha r) \bmod q$$

Howgrave-Graham과 Smart는 [27]에서 충분히 많은 d개의 서명값들과 서명값 계산에 필요한 k의 충분히 많은 ℓ비트들을 알면, α를 복원할 수 있음을 보였다. 저자들이 제시한 가정은 특정한 형태의 HNP 문제로 귀결됨은 쉽게 알 수 있고, 해당되는 HNP를 격자 축소 알고리즘을 통하여 풀면 α를 구할 수 있게 된다. Nguyen 등은 160비트 q의 경우, $\ell=3$, $d=100$ 정도면 해당되는 HNP가 풀림을 실험적으로 보였다 [28].

한편, 이러한 격자 이론을 이용한 공격은 후에 ECDSA, Nyberg-Rueppel, RDSA, ESIGN 등 여러 가지 DH 문제에 기반한 서명 알고리즘에도 비슷하게 적용되었다 [29-32].

Ⅵ. 격자 이론 기반 공개키 암호의 분석

1. Ajtai-Dwork 암호시스템과 그 분석

LLL 알고리즘이 Knapsack, RSA, DH 계열 공개키 암호 및 서명의 분석에 효율적으로 활용된 이래 격자 이론은 공개키 암호 분석 분야에 있어 매우 유용한 도구로 자리 잡았다. 반면, CVP나 SVP 등 계산 이론에서 충분히 어려움이 검증 받은 격자 이론의 난제들이 있었으나, 이 문제들을 이용한 공개키 암호의 개발은 시도되지 않았다. 이는 계산 이론에서 어려움이 증명된 다른 문제들의 경우도 마찬가지 상황이었는데, 그 이유는 다음과 같다. 어떤 난제가 일방향함수로 활용되려면 문제의 대상들이 평균적으로(average case) 풀기 어려워야 하는데, 계산 이론에서 다루는 난제들은 최악의 경우(worst case) 그 해결이 어려운 문제들이기 때문이다.

그런데, 1996년 Ajtai는 특정한 격자 상에서 SVP의 worst case 어려움이 average case 어려움과 동치라는 사실을 보였다 [33]. 이 결과는 격자 이론이 암호 알고리즘 개발 분야에 활용되게끔 유도한 획기적인 업적이었으며, 뒤이어 Ajtai는 Dwork과 더불어 자신의 이론에 기반한 공개키 암호(AD 시스템)를 제안하였다 [34].

AD 암호 시스템은 제안 당시부터 현실적으로 활용 가능한 암호라기보다는 격자 이론에 기반한 안전성이 증명되는 공개키 암호가 처음으로 제안되었다는데 의미가 있었던 암호였다. 그런데, 이마저도 적은 차원의 경우 안전하지 않음이 Nguyen과 Stern에 의하여 격자 축소 알고리즘을 이용한 heuristic한 분석을 통하

여 밝혀졌다 [35].

2. GGH 암호시스템과 그 분석

Ajtai의 논문에 영향을 받아 Goldreich 등은 현실적으로 사용 가능한 최초의 격자 기반 공개키 암호를 제안하였는데 [36], 이 암호는 저자들의 이름을 따 GGH라고 불리워진다. GGH는 기존에 잘 알려져 있던 코드 이론 기반 McEliece 암호를 격자 버전으로 변형한 암호이다.

GGH는 동일한 격자를 표현하는 다양한 기저들 중 기저 벡터의 길이가 작은 기저를 비밀키, 큰 기저를 공개키로 사용한다. 즉, GGH 키복구 공격에 대한 안전성은 SBP의 어려움에 기반한다. 한편, 암호문은 공개키인 기저 벡터들을 평문 정보에 따라 적당히 선형 결합한 후 길이가 작은 에러 벡터를 더해서 얻어진다. 즉, 평문 복구 공격에 대한 안전성은 CVP의 어려움에 기반한다.

GGH는 암·복호화 속도가 RSA 등에 비하여 빠르지만, 키의 크기가 크다는 단점이 있다. 제안자들은 격자의 차원이 적당히 작은 경우 효율성 상에 문제가 없을 뿐 아니라 충분한 안전성을 갖는다고 주장하며, 안전성을 공개적으로 검증받기 위하여 인터넷을 통하여 차원이 200, 250, 300, 350, 400인 파라미터에 대한 challenge를 실시하였다.

그런데, 그 후 얼마 되지 않아 Nguyen은 GGH에 대한 격자 공격을 제안하였다 [37]. 원래 GGH는 격자 공격에 대한 안전성을 높이기 위하여 격자 틈(2장의 정의 참조)이 작도록 설계되었다. 그런데, Nguyen은 원래 암호화 함수와 연관된 CVP를 약간의 조작을 통하여 격자 틈이 큰 새로운 CVP로 변환하여, 350차원 이하의 GGH 파라미터에 대하여서는 암호문에 대한 평문을 모두 복구하였고, 400차원 파라미터의 경우 암호문의 일부 정보를 찾아내었다.

결과적으로, GGH가 안전하기 위해서는 400차원 이상의 파라미터를 사용해야 하는데, 이 경우 공개키의 크기가 너무 커져 현실적으로 사용할 수 없는 알고리즘이 된다. 이러한 문제점으로 인하여 제안자들은 GGH가 완전히 깨졌음을 인정하였다.

3. NTRU 암호시스템과 그 분석

GGH와 거의 비슷한 시기에 Brown 대학교의 Hoffstein 교수 등은 특수한 다항식 링(truncated polynomial ring)의 연산을 사용하여 NTRU 공개키 암호 시스템을 제안하였다 [38]. NTRU의 키생성과 암·복호화에 사용되는 연산들은 다항식 연산과 정수 상의 모듈러 연산으로 격자와는 직접적인 관련이 없지만, 그 안전성은 특정한 형태의 격자 상의 CVP와 연관이 있게 된다. 즉, NTRU는 GGH의 특수한 형태로 볼 수 있다. 그런데, GGH가 격자를 표현하는 기저 행렬 전체를 공개키로 사용함으로써 격자의 차원이 커짐에 따라 키 크기가 많이 커지는 반면, NTRU는 하나의 벡터 정보만을 공개키로 이용하기 때문에 격자의 차원이 커져도 키 크기가 많이 증가하지 않는다. 이러한 장점으로 인하여 NTRU는 현재까지 제안된 공개키 암호들 중 이동 통신, 스마트 카드 등 경량 환경에 가장 적합한 공개키 암호로 간주되고 있다.

한편, NTRU가 제안된 후 곧바로 Coppersmith와 Shamir는 NTRU에 대한 격자 공격을 제안하였다 [39]. 저자들은 NTRU 키생성 식에 나타나는 공개키와 비밀키의 선형성을 이용하여, 공개키로부터 NTRU 격자라고 불리는 특수한 격자를 생성한 후, 이 격자의 가장 짧은 벡터가 비밀키 정보를 포함하고 있음을 보이고, 실험적으로 100차원 이하의 키를 수 분만에 찾아내었다. Coppersmith 등의 공격이 발표된 뒤로 격자 공격의 성능을 개선하기 위한 많은 연구들이 진행되었고 [40], 반대로 NTRU 측에서는 다년간의 분석과 실험을 통하여 격자 공격에 안전하기 위한 파라미터의 조건을 연구하고 있다 [41]. 그 결과, 현재 사용되고 있는 격자 축소 알고리즘의 성능으로는 NTRU 파라미터 다항식의 차원이 200 정도 이상이고 격자 틈이 일정 조건을 만족하면 현실적인 공격이 불가능하다는 사실이 받아들여지고 있다.

4. 새로운 격자 문제의 해결을 통한 분석

앞서 살펴보았던 공개키 암호들에 대한 격자 공격은 구체적인 적용 방식은 다르지만 대부분 동일한 원리로 이루어졌다. 즉, 공개된 정보로부터 격자를 구성하고, 해당 격자의 CVP나 SVP를 풂으로써 비밀 정보를 구하는 방법을 사용하였다.

그런데, 최근 격자 기반 공개키 암호, 특히 서명 알고리즘의 분석에는 단순 CVP나 SVP가 아닌 새로운 격자 문제의 해결을 통한 분석이 시도되고 있다. Szydlo는 [42]에서 격자를 표현하는 Gramian 행렬들이 서로 같은 격자를 표현하는지 여부를 가리는 문제를 해결하면 GGH와 NTRU 서명 알고리즘을 분석

할 수 있음을 보였다. 또, Nguyen과 Regev는 [43]에서 R^n상의 격자 L의 고정된 한 기저는 모르지만, 이 기저 벡터들이 생성하는 다면체(parallelepiped)를 P라 할 때, R^n상의 충분히 많은 벡터 V들의 $V \pmod{L} \in P$ 값이 주어지면 L의 기저를 복원할 수 있다는 사실을 보였고, 이를 GGH와 NTRU 서명의 분석에 활용하였다. 한편, Gama 등은 NTRU 격자가 일반적인 격자에 비하여 특별한 성질(Sympletic)을 가지고 있는 점에 주목하여 이러한 격자들에 특화된 격자 축소 알고리즘을 제안하고, 이 알고리즘이 기존의 알고리즘보다 NTRU 분석에 효율적임을 주장하였다 [44].

Ⅷ. 결 론

본 논문에서는 격자 이론의 개요와 공개키 암호 분석에 있어 격자 이론이 활용된 사례들을 결과 위주로 살펴보았다. 2000년 이전까지의 공개키 암호에 대한 격자 공격의 결과들을 본 논문보다 자세히 살피고자 한다면 [45]를 참조하기 바란다.

LLL 알고리즘이 발표된 이후 약 20 여년간 격자 이론은 여러 공개키 암호의 분석과 증명에 가장 강력하고 주요한 도구로 사용되어지고 있다. 최근에는 이러한 용도를 넘어 격자 이론상의 난제를 기반으로 하는 새로운 알고리즘의 개발에 관한 연구와, 격자 축소 알고리즘 자체의 성능을 향상시키기 위한 연구들도 활발하게 진행되고 있다.

격자 이론 분야는 아직까지 미해결된 문제들이 많이 남아 있고, 암호학에 있어서의 활용도도 앞으로 더욱 높아질 것으로 전망된다. 따라서, 학문적으로나 실용적인 면에서 관련 분야에 대한 더욱 많은 관심을 가져야 할 것으로 판단된다.

참 고 문 헌

[1] A. K. Lenstra, H. W. Lenstra, L. Lovasz, Facto-ring polynomials with rational coefficients, Mat-hematische Ann. 261:513-534, 1982.

[2] D. Micciancio, S. Goldwasser, Complexity of lattice problems: A Cryptographic perspective, Kluwer Academic Publishers, 2002.

[3] C.P. Schnorr, A hierarchy of polynomial lattice basis reduction algorithms, Theoretical Computer Science, 53:201-224, 1987.

[4] R. Merkle, M. Hellman, Hiding information and signatures in trapdoor knapsacks, IEEE Tran. inform. theory, IT-24:525-530, September 1978.

[5] L. M. Adleman, On breaking generalized knapsack public key cryptosystems, 15th STOC, 402-412, ACM, 1983.

[6] E. F. Brickell, Solving low density knapsacks, Crypto'83, 25-37, Plenum Press, 1984.

[7] E. F. Brickell, Breaking iterated knapsacks, Crypto '84, LNCS 196, 342-358, Springer-Verlag, 1985.

[8] B. Chor, R. L. Rivest, A knapsack-type public key cryptosystem based on arithmetic in finite fields, IEEE Trans. Inform. Theory, 34, 1988.

[9] D. Coppersmith, Finding a small root of a univariate modular equation, Eurocypt'96, LNCS 1070, 155-165, Springer-Verlag, 1996.

[10] D. Coppersmith, Finding a small root of a bivariate integer equation: Factoring with high bits known, Eurocypt '96, LNCS 1070, 178-189, Springer-Verlag, 1996.

[11] D. Coppersmith, Low-exponent RSA with related messages, Eurocypt'96, LNCS 1070, 1-10, Springer-Verlag, 1996.

[12] D. Boneh, G. Durfee, Cryptanalysis of RSA with private key d less than $N^{0.292}$, Eurocrypt'99, LNCS 1592, 1-11, Springer-Verlag, 1999.

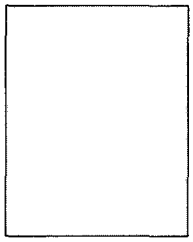
[13] G. Durfee, P. Q. Nguyen, Cryptanalysis of the RSA schemes with short secret exponent from Asiacrypt'99, Asiacrypt 2000, LNCS 1976, 2000.

[14] A. May, Cryptanalysis of unbalanced RSA with small CRT-exponent, Crypto

2002, LNCS 2442, 242-256, Springer-Verlag, 2002.
[15] J. Blomer, A. May, New partial key exposure attacks on RSA, Crypto 2003, LNCS 2729, 27-43, Springer-Verlag, 2003.
[16] J. S. Coron, Finding small roots of bivariate integer polynomial equations revisited, Eurocrypt 2004, LNCS 3027, 492-505, Springer-Verlag, 2004.
[17] M. Ernst, Partial key exposure attacks on RSA up to full size exponents, Eurocrypt 2005, LNCS 3494, 371-386, Springer-Verlag, 2005.
[18] J. Blomer, A. May, A tool kit for finding small roots of bivariate polynomials over the integers, Eurocrypt 2005, LNCS 3494, 251-267, Springer-Verlag, 2005.
[19] V. Shoup, OAEP reconsidered, Crypto 2001, LNCS 2139, 239-259, Springer-Verlag, 2001.
[20] E. Fujisaki, T. Okamoto, D. Poincheval, J. Stern, RSA-OAEP is secure under the RSA assumption, Crypto 2001, LNCS 2139, Springer-Verlag, 2001.
[21] D. Boneh; Simplified OAEP for the RSA and Rabin functions, Crpyto 2001, LNCS 2139, 275-291, Springer-Verlag, 2001.
[22] A. May, Computing the RSA secret key is deterministic polynomial time equivalent to factoring, Crypto 2004, LNCS 3152, 213-219, Springer-Verlag, 2004.
[23] D. Boneh, R. Venkaesan, Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes, Crypto'96, LNCS 1109, 129-142, Springer-Verlag, 1996.
[24] P.Q. Nguyen, I. E. Shparlinski, The insecurity of the Digital Signature Algorithm with partially known nonces, J. of Cryptology, Vol 15(3), 151-176, 2002.
[25] I.E. Shparlinski, On the generalized hidden number problem and bit security of XTR, 14th Symp. on Appl. algebra, Algebraic Algorithms, and Error-Correcting Codes, LNCS 2227, 268-277, Springer-Verlag, 2001.
[26] D. Boneh, I. E. Shparlinski, On the unpredictability of bits of the elliptic curve Diffie-Hellman scheme, Crypto 2001, LNCS 2139, 201-212, Springer-Verlag, 2001.
[27] N. Howgrave-Graham, N. P. Smart, Lattice attacks on digital signature schemes, Designs, Codes and Cryptography, Vol 23, 283-290, 2001.
[28] P.Q. Nguyen, The dark side of the hidden number problem: Lattice attacks on DSA, CCNT'99, Birkhauser, 2000.
[29] P.Q. Nguyen, I. E. Shparlinski, The insecurity of the elliptic curve Digital Signature Algorithm with partially known nonces, Design, Codes, and Cryptography, vol 30(2), 201-217, 2003.
[30] E. El Mahassni, P. Q. Nguyen, I. E. Sparlinski, The insecurity of Nyuberg-Rueppel and other DSA-like signature schemes with partially known nonces, CaLC 2001, LNCS 2146, 97-109, Springer-Verlag, 2001.
[31] P. Fouque, G. Poupard, On the security of RDSA, Eurocrypt 2003, LNCS 2656, 462-476, Springer-Verlag, 2003.
[32] P. Fouque, N. Howgrave-Graham, G. Marinet, G. Poupard, Insecurity of ESIGN in practical implementations, Asiacrypt 2003, LNCS 2894, 492-506, Springer-Verlag, 2003.
[33] M. Ajtai, Generating hard instance of lattice problems, 28th STOC, 99-108, ACM, 1996.
[34] M. Ajtai, C. Dwork, A public-key cryptosystem with worst-case/average-

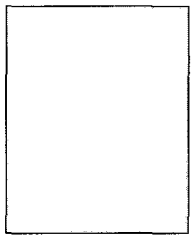
case equivalence, 29th STOC, 284-293, ACM, 1997.
[35] P. Q. Nguyen, J. Stern, Cryptanalysis of the Ajtai-Dwork cryptosystem, Crypto'98, LNCS 1462, 223-242, Springer-Verlag, 1998.
[36] O. Goldreich, S. Goldwsser, S. Halevi, Public-key cryptosystems from lattice reduction problems, Crypto'97, LNCS 1294, 112-131, Springer-Verlag, 1997.
[37] P.Q. Nguyen, Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from Crypto '97, Crypto'99, LNCS 1666, 288-304, Springer-Verlag, 1999.
[38] J. Hoffstein, J. Pipher, J.H. Silverman, NTRU: a ring based public key cryptosystem, ANTS III, LNCS 1423, 267-288, Springer-Verlag, 1998.
[39] D. Coppersmith, A. Shamir, Lattice attacks on NTRU, Eurocrypt'97, 52-61, Springer-Verlag, 1997.
[40] A. May, J.H. Silverman, Dimension reduction methods for convolution modular lattices, CaLC 2001, LNCS 2146, 110-125, 2001.
[41] J. Hoffstein, J.H. Silverman, W. Whyte, Estimated breaking times for NTRU lattices, Technical Reports #12, version 2, NTRU Cryptosystems, 2003.
[42] M. Szydlo, Hypercubic lattice reduction and analysis of GGH and NTRU signatures, Eurocrpyt 2003, LNCS 2656, 433-448, Springer-Verlag, 2003.
[43] P.Q. Nguyen, O. Regev, Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures, Eurocrypt 2006, LNCS 4004, 271-288, Springer-Verlag, 2006.
[44] N. Gama, N. Howgrave-Graham, P.Q. Nguyen, Symplectic lattice reduction and NTRU, Eurocrypt 2006, LNCS 4004, 233-253, Springer-Verlag, 2006.
[45] P.Q. Nguyen, J. Stern, The two faces of lattices in cryptology, CaLC 2001, LNCS 2146, 146-180, Springer-Verlag, 1998.

〈著 者 紹 介〉



한 대 완(Daewan Han)
정회원

1995. 2 : 서울대학교 수학과 (학사)
1997. 2 : 서울대학교 수학과 (석사)
2001. 3 ~ 현재 : 국가보안기술연구소 선임연구원
〈관심분야〉 암호 이론, 정보보호



염 용 진(Yongjin Yeom)
정회원

1991. 2 : 서울대학교 수학과 (학사)
1994. 2 : 서울대학교 수학과 (석사)
1999. 2 : 서울대학교 수학과 (박사)
2000. 4 ~ 현재 : 국가보안기술연구소 팀장
〈관심분야〉 암호 이론, 정보보호