韓國通信情報保護學會誌
第1卷, 第1號, 1991. 4

소인수 분해와 암호학

임 종 인*·김 창 한**

1. 서 론

1976년 Diffie-Hellman[3]은 one-way 함수를 이용한 공개키(public key) 개념을 도입함으로써 암호학의 새로운 장을 열어놓은 것으로 평가받고 있다. 이 개념의 도입은 종래 암호에 있어서의 문제점이었던 key 교환문제를 해결하였을 뿐만 아니라 정보화 사회로 접어든 현대 사회에서 중요한 authentication digital signature, 사용자 확인(user-identification) 등의 실용을 가능하게 하였다. 공개키 개념을 이용한 암호법 중 가장 먼저 제안된 것은 1978년 Rivest-Shamir-Adleman에 의한 암호법이다. 이 암호법의 안전성은 소인수 분해의 어려움에 근거하고 있으며, key size는 512비트(10진수 155자리)이다. 한편, 발표후 10여년이 지난 오늘날에도 가장 널리 쓰이며 안전성을 인정받고 있는 공개키 암호법이나, 소인수 분해법의 눈부신 발전 및 하드웨어의 급속한 성능 향상으로 조만간 key size를 크게 해야 할 것으로 평가받고 있다. 그리고, 소인수 분해의 어려움에 안전성을 근거하여 그 안전성이 증명된 BBS generator는 1986년 Blum-Blum-Shub에 의해서 제안된 것으로 one time pad로 사용되는 psudo-random sequence의 생성 및 Blum-Goldwasser 공개키 scheme에 사용되고 있다. 본 논문의 목적은 효율적인 소인수분해법에 대한 간략한 소개 및 이의 응용 특히 RSA 암호법 및 BBS generator의 소개에 있다.

* 정회원, 고려대학교 자연과학대 수학과 부교수
** 정회원, 고려대학교 대학원 수학과 박사과정

2. 소인수 분해

가. 간략한 역사적 고찰 및 제안

1과 자기자신 이외에는 약수를 갖지 않는 양의 정수를 소수(prime number)라 하며 모든 정수는 소수들의 곱으로 유일하게 표시된다. 즉, 소인수 분해(prime-factorization)된다는 사실은 B.C 300년 전의 Euclid에게도 알려진 사실이지만 최초의 엄격한 증명은 1801년 Gauss가 저술한 Disquisitions Arithmeticae에 처음으로 나온다. 그러나 이 문제는 이전에도 Fermat(1601~1665), Euler(1707~1783) 등에 의해서 연구되었으며, 특히 Fermat가 제시했던 방법은 RSA키로 사용되는 형태의 합성수에 대한 인수분해에 특히 유용할 뿐 아니라 이들 형태의 합성수에 대한 기존의 인수분해법중 가장 효율적인 이차선별법(Quadratic Sieve Method, QS) 등에 기초가 되고 있다.

1978년 RSA가 개발됨으로서 갑자기 수학계 이

외의 타분야에서 주목받기 시작한 소인수분해 문제는 이전에는 정수론의 흥미있고도 어려운 문제 중의 하나로만 인식되어 발전속도가 느렸지만 1970년대에 개발된 Morrison-Brillhart의 연분수 이용 인수분해법과 Pollard의 인수분해법을 시발로 1980년대에는 큰 발전을 이루었다.

Eurocrypt'89에서 Pomerance가 제안한 이차선별법(QS)는 합성수의 인수사이즈에 관계없이 적용할 수 있기 때문에 주목받았으며 1987년 Silverman이 제안한 MPQS, 1990년 Lenstra 등이 제안한 NFS 등은 QS를 크게 개선시켰다. 특히 NFS는 몇가지 제한성에도 불구하고 MPQS로는 불가능하였던 138자리 십진수 인수분해에 적용 성공함으로서 현재 주목의 대상이 되고 있다. 또한 Pollard의 방법을 개선한 Lenstra의 타원 곡선법(ECM)은 1986년 발표된 것으로서 합성수 n의 비교적 작은 소인수를 가지고 있을 때 효율적이다. 이를 이용하여 1987년 말 일본의 Kenji-Koyama는 2^{713}-1의 23자리 소인수를 구하는 데 성공하였다.

합성수의 소인수의 모든 갯수는 추정할 수 있다. 예를 들면 RSA키 사이즈인 155자리 합성수는 평균 4개의 소인수를 가지고 있다. 따라서 목표 합성수 n이 주어지면 먼저 ECM을 적용하여 작은 인수를 구한 후 QS계열의 인수분해법을 적용하는 것이 바람직하다.

나. 효율적 소인수분해법의 소개

합성수 n이 주어졌을 때,

$$x^2 \equiv y^2 \bmod n \qquad (*)$$

를 만족하는 정수쌍 x, y를 구할 수 있으면 n이 합성수이므로 최대공약수 $d=(x-y, n)$는 확률(1/2) 이상으로 $d \neq 1$이고 $d \mid n$이므로 우리는 n의 한 인수를 얻게 된다. 따라서 (*)를 만족하는 정수쌍 x, y를 구하는 것은 의미가 크다 하겠다. 이차선별법(QS)는 여기에 착안한 인수분해법으로서 (*)를 만족하는 x, y를 구하기 위해서 2단계를 거치고 있다.

먼저 relation collecting 단계로서 $f(x)=(x+[\sqrt{n}])^2-n$이라는 정계수 다항식을 이용하고 있다. $f(x)$는 x가 정수일 경우에는 $(x+[\sqrt{n}])^2 \equiv f(x) \bmod n$을 만족한다.

특별히 $f(x)$가 적당한 bound B이하의 솟수들의 곱으로만 표시될 때 이들 관계식 만을 모으는 과정을 relation collecting 단계라 한다. 충분히 많은 관계식이 모아지면 계수행렬에 Gauss소기법 등을 적용하여 $f(x_1)\cdots f(x_k)=y^2$과 같이 되는 $x_1, \cdots, x_k$를 구할 수 있게 된다. 이 단계를 Elimination(소거) 단계라 한다. QS를 시행하면 대부분의 시행시간은 이들 단계에서 소모되고 있다. Pomerance의 QS 적용시 $n \approx 10^{100}$일 경우 $f(x)$는 10^{50}에서 10^{60}정도가 될 것이고 이들 값이 최초의 10^5개의 소수들의 곱으로만 인수분해될 확률은 10^{-9}정도이다. 즉, $10^{10}<X<2\times10^{10}$에 대해서 10개 정도만이 바람직한 $f(x)$를 가져다 줄 것이다. 따라서, 충분히 많은 (10^5개 이상) $f(x)$를 얻기 위해서는, $n \approx 10^{100}$일 경우에는 한번의 $f(x)$처리당 10번의 bit 연산만 가정해도 10^{15}이상의 bit 연산이 필요하여 거의 불가능한 큰 계산이 되고만다. 이와 같이 relation collecting 단계에서 걸리는 시행시간이 너무 크기 때문에 이의 해결방법으로써 MPQS에서는 $f_{a,b}(x)=ax^2+2bx+c$ ($b^2-ac=n$, $0 \leq b < a$) 형태의 다항식을 a, b를 변형시켜 복수로 사용함으로써 MPQS는 QS로써는 불가능하였던 $2^{353}+1$ 같은 100자리가 넘는 수의 인수분해에 성공하였다[8]. 시행시간은 26일 정도가 소모되었다(elapsed time).

그러나, MPQS를 사용하여 155자리 RSA키 사이즈의 합성수를 인수분해하는 것은 100자리 수의 40000배 정도가 걸릴 것으로 생각되기에 역시 개선이 필요하였다. 1990년 Lenstra 등에 의해서 발표된 수체선별법(Number field sieve Method, NFS)은[5] 현재까지는 $r^e \pm s$ 형태의 수에만 적용가능한 미완성 형태의 방법이지만 MPQS로써는 불가능하였던 $2^{457}+1$이라는 138자리 합성수의 인수분해에 적용함으로써 주목받고 있다[5]. 시행시간은 9주이며 collecting 단계에서 7주, elimination 단계에서 2주가 걸렸다. NFS는 대수적 정수론을 비롯한 고도의 수학지식이 요구되고 적용가능 수에 대한 제약이 있으나 현재 Pomerance 등에 의해서 개선이

시도되고 있다. NFS를 사용한다 하더라도 현재로써는 155자리 수에 대한 인수분해는 불가능하다.

그러나 그래프이론 등을 이용한 행렬연산이론의 발달은 elimination 단계에의 시행시간을 줄여줄 것이고 하드웨어에서의 지난 10여년간의 발전을 생각해 볼때 가까운 장래에 RSA키 사이즈를 바꾸어야 할 지도 모른다. 참고로 1977년에는 78자리(256bit) 합성수의 인수분해에는 10^4일(약 27년)이 걸렸지만 현재는 같은 알고리즘으로 하루정도면 충분하다.

3. 암호에의 응용

가. RSA 암호법

1978년 Rivest-Shamir-Adleman은 오늘날 RSA 또는 MIT 암호법이라 불리는 암호법을 제안하였다[7]. 이것은 1976년 Diffie-Hellman의 공개키 개념 도입이래 최초로 제안된 공개키의 암호법으로써 소인수분해의 어려움에 안전성을 근거하고 있다. 키를 생성하기 위해서는 먼저 2개의 비슷한 사이즈(보통 256bit)의 두 소수 p, q를 택하여 $n=pq$를 만든다. e가 $\Phi(n)=(p-1)(q-1)$과 서로소인 정수라 할때 $ed\equiv 1 \pmod{\Phi(n)}$인 d가 Euclid Algorithm을 이용하여 구해진다. 이때 (e, n)이 공개키가 되고 (d, n)은 비밀키가 된다. Euler의 정리로부터 모든 정수 m에 대해 $m^{ed}\equiv m \bmod n$이므로 $0\leq m < n$이면 $m^{ed} \bmod n = m$이 된다.

예)

$p=19$, $q=23$, $n=pq=437$ $\phi(n)=(p-1)(q-1)=396$ $e=13$이라 하자

$13\times 61=793=2\phi(n)+1$이므로 $d=61$이다. $m=123$이라 하면

$123^{13} \bmod 437=386$이고 $386^{61} \bmod 437 = 123$이 된다.

위의 예에서 보듯이 $C=m^e \bmod n$이라 하면 $C^d \bmod n = m$이 되므로 송신자 A가 수신자 B에게 메시지 m을 보내고자 할 때 A는 public directory에서 B의 공개키(e_B, n_B)를 찾는다. 이를 이용하여 A는 $C=m^{e_B} \bmod n_B$라는 암호문(ciphertext)을 만들고 이를 B에게 전송한다. B는 비밀키 d_B를 사용하여 메시지 $m=C^{d_B} \bmod n_B$을 얻게 된다. 혹 송신자 A에 대한 Authentication(인증)이 필요할 경우 A는 암호문 C를 바로 전송하지 않고 자신의 비밀키를 사용하여 만든 $C'=C^{d_A} \bmod n_A$를 B에게 전송하면 된다. 이 경우 B는 A의 공개키(e_A, n_A)를 이용하여 $C=(C')^{e_A} \bmod n_A$을 구한 후 자신의 비밀키 d_A는 A만이 알고 있으므로 C'는 송신자가 A라는 것의 Authentication이 될 수 있을 것이다.

RSA 암호법은 대표적인 비밀키 암호법인 DES에 비해 암호화 속도가 훨씬 느리고 몇가지 형태의 chosen ciphertext attack에 취약할 수 있다는 것이 밝혀져 있다[2]. 또한 연분수 등을 이용한 비밀키 공략법[10] 때문에 이의 선택에도 신중해야 한다는 점이 있다. 또한 RSA의 안전도가 소인수분해의 어려움과 동치(equivalent)라는 것은 나.의 BBS generator의 경우와는 달리 증명되지 않고 있다. 그러나 RSA는 현재 공개키 암호법중 가장 널리 쓰이고 있으며 Authentication의 경우에서와 같이 공개키 암호법을 이용한 정보화 사회에서의 암호의 역할증대를 통한 응용 때문에 중요성이 커지고 있다. 더불어서 RSA의 분석을 위한 소인수분해 이론 등의 이론적 분야에서의 계속적인 연구지원이 필수적이라 하겠다.

나. BBS generator

수열이 pseudo-random하다는 것은 이 수열이 pseudo-random generator라 불리는 eterministic process를 통해서 만들어졌지만 외견상 patternless이고 random일 때를 말한다. pseudo-random generator는 seed라 불리는 starting sequence로부터 훨씬 더 긴 pseudo-random sequence를 만들어 내게 된다. 안전도가 보장된 비밀키 암호법인 one-time pad 암호법에 있어서 사용되는 pad는 random일 뿐만 아니라 암호화시킬 메시지만큼 길어야 하고 한번만 사용되어야 한다는 조건을 만족해야 한다. Output Feedback mode를 이용하면 같은 seed를 여러번 사용할 수 있지만 randomness를

보장할 수 없다는 취약점이 있다. 1986년 Blum-Blum-Shub[1]에 의해서 제안된 pseudo-random generator인 BBS generator는 4k+3 형태인 두 솟수의 곱으로 이루어진 Blum integer n을 이용하고 있으며 이것은 소인수분해의 어려움에 근거하여 Cryptographically strong 즉, randomness를 보장할 수 있다는 것이 증명되었다[11].

n을 Blum integer라 하자. Quadratic residue x^2 mod n이 주어졌을 때 square root중 역시 quadratic residue가 되는 것 즉, Principal square root는 하나만 존재하고, 이것을 구하는 것은 n을 소인수분해하는 것과 동치라는 것이 Rabin에 의해서 증명되었다[6]. 또한 대부분의 quadratic residue x에 대해서 x^2 mod n을 보고 x의 least significant bit를 추정하는 것은 동전던지기를 하여 추정하는 것과 같다는 것이 밝혀져 있다[9].

이제 BBS generator를 서술해 보자. n과 서로소인 random integer x를 택해 $x_0 \equiv x^2 \bmod n$로 하여 seed를 만든다. $c \geq 0$에 대해서 $x_{i+1} \equiv x_i^2 \bmod n$으로 하여 b_i를 x_i의 least significant bit로 하였을 때 $BBS_{n,t}(x_0) = b_0 b_1 \cdots b_{t-1}$과 같이 하여 BBS generator를 만들 수 있다. BBS generator는 Cryptographically strong하다는 것이 증명될 뿐 아니라 $x_i \equiv x_0^{2^i} \bmod n$이므로 $x^{\Phi(n)} \equiv 1 \bmod n$이라는 Euler의 정리를 이용하면,

$$x_i \equiv x_0^{2^i \bmod \Phi(n)} \bmod n$$

을 통해서 seed x_0로부터 신속하고 direct하게 각 bit를 얻을 수 있다는 것이 또 하나의 장점이다. n=pq일 때 p, q를 비밀로 하고 n을 공개키로 사용할 수도 있다. m이 t-bit의 메시지라면 x_0를 seed로 하여 $BBS_{n,t}(x_0)$와 x_t를 위와 같이 말할 수 있다. 송신자는 $\langle x_t, m \oplus BBS_{n,t}(x_0) \rangle$를 n을 공개키로 하는 수신자에게 보내면 수신자는 x_t를 이용하여 n=pq를 만들어 X_0를 구할 수 있다. 이로부터 $BBS_{n,t}(X_0)$를 만들어 m을 복원할 수 있게 된다. 이 암호법은 Blum-Goldwasser Scheme으로서 RSA보다 빠르고 정보가 조금도 새지 않는 다는 것이 증명되지만 chosen ciphertext attack에는 매우 취약하다.

참 고 문 헌

1. Blum, L., Blum, M, and Shub. M., "A simple unpredictable pseudo-random number generator." Siam Journal on computing, Vol. 15, 1986, pp. 364－383.

2. Chor, B.-Z.. Goldreich, O., Hastad, J., Freidmann, J., Rudich, S. and Smolensky, R., "The bit extraction problem or t-resilient functions." Proceedings of the 26th IEEE Symposium on Foundations of Computer Science, 1985. pp. 396－407.

3. Diffie, W. and Hellman, M. E., "New directions in cryptography," IEEE Transactions on Information Theory, Vol. IT-22, 1976, pp. 644－654.

4. A. K. Lenstra, M. S., Manasse, "Factoring by electronic mail," Proceedings Eurocrypst'89.

5. A. K. Lenstra, H. W. Renstra, Jr., M. S. Manasse, J. M. Pollard, "The number field" Sieve, ACM, 1990, pp. 564－572.

6. Rabin, M. O., "Digitalized Signatures and Public Key Functions as Intractable as factorization," MIT Laboratory for Computer Science, Jaunary, 1979, TR 212.

7. Rivest, R. L., Shamir, A. and Adleman, LM. "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, Vol. 21. 1978, pp. 210－126.

8. R. D. Silverman, "The multiple polynomial quadratic sieve," Math. Comp. Vol. 48, 1987, 329－339.

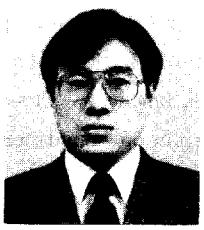
9. Vazirani, U. V. and Vazirani, V. V., "Trapdoor pseudo-random number generators with applications to protocol design," Proceedings of the 24th IEEE Symposium on Foundations of Computer Science, 1983, pp. 23－30.

10. M. J. Wiener, "Cryptanalysis of short RSA secret exponents," Eurocrypt'89, 1989 Houthalen, Belgium.

11. YAO, A. C－C, "Theory and Applications of trapdoor functions," Proceed of the 23rd IEEE Sym-

posium on Foundations of Computer Science, 1982,
pp. 80－91.

□ 著者紹介



임 종 인(正會員)

1980年2月 高麗大學校 數學科 卒業(學士)
1986年2月 高麗大學校 大學院 卒業(理學博士)
現 高麗大學校 自然科學大學 副教授
關心分野： 정수론 및 관련응용분야

김 창 한(正會員)

1985年 2月 高麗大學校 數學科 卒業(學士)
1987年 8月 高麗大學校 大學院 卒業(碩士)
現 高麗大學校 大學院 在學(博士過程)
關心分野： 정수론 및 응용분야