通信情報保護學會誌
第2卷 第3號, 1992. 9

RSA 암호법과 EL Gamal 암호법의 비교

임종인* · 서광석**

1. 서 론

1970년대 중반 '공개키 암호법'이라는 개념이 Diffie-Hellman[3]에 의해 도입된 이후 여러가지 공개키 암호법이 제의되어 왔으며 이에 대한 활발한 이론 및 실제적 연구가 이루어져 왔다. 본 논문은 현재 대표적인 공개키 암호법으로 인정되고 있는 RSA 암호법과 El Gamal 암호법[4]을 비교하려는 것을 목적으로 하고 있다.

수학을 암호학에 응용하는데 있어서 중요한 것은 관련된 수학적 문제의 계산적 어려움이다. RSA 암호법과 El Gamal 암호법은 각각 소인수분해의 어려움과 이산로그 문제의 어려움에 안전도를 근거하고 있으며 일반적으로 거의 같은 안전도를 가지고 있는 것으로 인정되고 있다. 과거에도 수학적으로 중요한 문제였지만 이들 암호법이 탄생한 이후 소인수분해 문제와 이산로그 문제는 수학자들외에 응용분야에 종사하고 있는 많은 학자들의 관심을 끌어 지난 10여년간 큰 진전을 보아왔다. 필자는 ETRI와의 연구용역을 통해[16] 이들 문제를 접하고 컴퓨터 실행을 통한 연구를 계속하여왔다. 따라서 이러한 경험에 근거한 두 공개키 암호법의 비교에 자연스런 관심을 갖게 되었다. 최근 이러한 종류의 논문을[13] 접한 후 이 논문과 필자의 경험을 결합하여 본 논문을 쓰게 되었다.

본 논문에서는 주로 계산량에 근거한 두 공개 키 암호법의 난도 비교를 시도하려 한다. 이외에 message expansion기억 용량문제, 구현효율성 문제와 같은 중요한 실제적 문제가 있으나 이들은 필자의 전공이 아니므로 간략히 취급하려 한다. RSA 암호법과 El Gamal 암호법은 앞에서 언급한 바와 같이 소인수분해의 어려움과 이산로그 문제의 어려움에 안전도를 근거하고 있기에 이들 문제에 대한 최신 동향을 알아보는 것은 중요한 것이 될 것이다. 이것은 2절에서 다루었다.

소인수분해 문제는 1987년 MPQS법이 Silverman[12]에 의해 도입된 이후, 여러가지 부분적인 개선이 이루어져 왔지만 현재 일반적 소인수분해법으로는 MPQS가 가장 효율적인 것으로 인정되고 있다.[14] 1987년 Lenstra등[6]에 의해서 제의되고 1990년 512-bit 수인 $F_9=2^{512}+1=P7\times P49\times P99$의 소인수분해에 적용된 NFS가 있지만, 현재까지는 실용화되지 못했다. 최근 Coppersmith[2]가 NFS의 general-purpose 알고리즘화에 성공하였다고 보고하였으며 필자의 연구팀도 현재 연구용역을 통해 이 문제를 연구하고 있다. 따라서 본 논문에서는 MPQS를 이용한 소인수분해 문제의 난도 측정을 하고 있으므로 NFS의 실용화시에는 약간의 변화가

* 고려대학교 자연과학대 수학과 부교수
** 서남대학교 수학과 조교수

있을 것으로 생각된다.

갈로아체 $GF(2^n)$에서의 이산로그 계산문제는 소인수분해 문제에 비해 상대적으로 주목을 덜 받아왔다. 현재 가장 효율적인 이산로그 계산법도 1984년 Coppersmith[1]가 제시한 방법의 수정된 것으로써 Coppersmith 알고리즘은 여러가지 부분적인 개선이 이루어졌지만 현재 이를 대처할 것은 없는 것으로 평가되고 있다. 다만 El Gamal 암호법의 안전도를 확실하게 하기 위해서는 $n>1000$이 되어야 하는데 이 경우 수반되는 구현의 효율성, Message-expansion, 커다란 기억용량 문제가 선결과제가 되어 왔다. 이중 구현의 효율성에 대해서는 최근 최적 정규기저를[10] 통한 큰 진전이 이루어졌다. Coppersmith 알고리즘의 컴퓨터 실행경험은 현재 $GF(2^{127})$에 머물고 있으나,[1,16] 최근 이 분야에의 관심으로 보아 가까운 시일내에 큰 진전이 이루어질 것으로 예상된다. 이 논문에서 마지막으로 타원곡선에 관해 약간의 서술을 하였다.

$GF(2^m)$ 위에서의 타원곡선을 이용한 El Gamal 암호법을 이용할때는 $GF(2^{4n})$에서의 El Gamal 암호법과 같은 안전도를 유지하는 것으로 평가되고 있으나 최근 타원곡선 이론에 대한 급속한 발전속도로 보아 안심할 수는 없다하겠다.

2. 소인수 분해법과 이산로그 계산법의 현황

본 절에서는 현재 소개된 소인수 분해법과 이산로그 계산법 중 효율적인 것들에 대해 알아보려 한다.

2.1 소인수 분해법

소인수 분해 문제는 Euclid이래로 정수론에서 가장 흔히 있는 문제의 하나가 되어 왔지만 1978년 RSA 암호법이 도입된 이후 이론적 연구와 병행한 컴퓨터 실행을 통하여 급속한 발전을 이루어왔다. 이 절에서는 MPQS, ECM 그리고 NFS를 소개하려 한다. MPQS는 1987년 Silverman[12]이 여러개의 다항식(Multiple Polynomials)을 이용하여 QS를 개선한 것으로서 현재 실용화된 소인수 분해법 중 가장 효율적인 것으로 평가되고 있다. 합성수 n을 MPQS를 이용하여 소인수 분해하려 할 때, 실행시간은

$$L_{\log n}(1/2,\ 1)=\exp((1+0(1))\ (\log n\ \log\log n)^{1/2})$$

으로 추정되고 있으며, 1990년 Lenstra와 Manasse[6,8]등은 일반적인 100자리 합성수를 MPQS를 사용하여 인수분해 할 수 있음을 보였으며 two-large prime variation이라는 개선법을 통해 116자리 합성수의 인수분해에도 성공하였다. 이 경우 실제 컴퓨터 실행시간은 Super Computer 사용시 한 달 이상으로 추정된다.

국내에서도 본 연구팀이 91년 large-prime variation을 이용한 개선된 MPQS의 알고리즘 완성에 성공하였으나 여건의 미비로 40자리 정도의 수에만 적용할 수 있었다.[16] 위에서 소개한 116자리 합성수의 인수분해시 MPQS를 적용하면 일차 방정식을 푸는 문제가 발생하는데 이 경우 방정식의 갯수는 100,000개 이상이 되므로 막대한 계산량을 처리해야 할 뿐 아니라 기억용량의 문제가 현실적으로 더욱 큰 문제가 될 수 있다.

NFS는 1989년 Lenstra등이 제시한 최선의 소인수 분해법으로서 합성수 n에 적용시 실행시간은

$$L_{\log n}(1/3,\ 1.526)=\exp((1.526+0(1))\ (\log^n)^{1/3}\ (\log\log n)^{1/3})$$

로 추정되고 있다.

NFS는 100자리 이상의 합성수에 적용시 MPQS보다 효율적인 것으로 평가되었으나 Lenstra등이 제시한 것은 $r^e \pm s$ 형태의 특수한 수에만 적용될 수 있는 것이었다.

1990년 6월 Lenstra등은[7] NFS를 이용하여 155자리 합성수인 $2^{512}+1$의 인수분해에 성공함으로서 NFS의 효율성을 보였다. 이들은 수백대의 workstation을 E-mail로 연결함으로서 막대한 계산량을 처리하였고 200,000개 이상의 일차방정식으로 구성된 일차방정식 계를 풀었다. 최근 Coppersmith[2] 등은 NFS 를 확장하여 일반적인 합성수에 적용가능하도록 하는데 성공하였으나, 아직 실용화 여부는 지켜보아야 할 것이다. 확장된 NFS의 실행시간은 $L_{\log n}(1/3,\ 1.902)$로 추정되고 있다.

이것이 실용화 된다면 125자리 이상의 합성수 인수분해에는 NFS가 MPQS 보다 효율적인 것으로 판단되고 있으나 현재 이 정도 크기의 일반합성수 인수분해 경험이 없기에 속단하기에는 이르다고 하겠다. 이와같은 사유로 본 논문에서는 MPQS를 사용한 소인수 분해 시행 시간을 채택하였다.

마지막으로 소개할 ECM을 1986년 Lenstra[9]가 타원곡선을 이용하여 Pollard의 p−1법[5]을 개선한 것으로서 합성수 n이 p라는 소인수를 가지고 있을때 p를 발견하는데 걸리는 실행시간은 $L_{logp}(1/2, 1)\sqrt{2}$으로 추정되고 있으므로 $p \approx \sqrt{n}$ 이라는 최악의 경우에도 MPQS와 실행시간이 같아지게 되어 일견 MPQS 보다 효율적인 것으로 보인다.

그러나 대부분 덧셈연산에 수반되는 MPQS의 경우와 달리 ECM의 경우는 커다란 사이즈 정수의 곱셈과 나눗셈이 수반되므로 실제 실행시간이 훨씬 더 걸린다. 현재 ECM의 실행기록은 38자리 소인수의 발견으로 보고되고 있다. 이와같은 특징 때문에 ECM은 두 개의 커다란 솟수의 곱으로 되어 있는 RSA 암호법의 합성수에는 적용될 수 없고 일반적인 수의 인수분해시 MPQS에 앞서 적용하여 작은 사이즈의 소인수를 먼저 발견하는데 사용하면 효율적일 것이다.

2.2 이산로그 계산법

갈로아체 $GF(2^n)$이 주어졌을 때 우리는 위수가 2^n-1인 원시원 g를 발견할 수 있다. 그러면 $GF(2^n)$의 임의의 원소 x는 적당한 정수 $r(0 \le r \le 2^n-2)$에 대해서 $x=g^r$의 꼴로 표시될 수 있다. 이때 r을 g를 basis로 하는 x의 이산로그라 하고 $r=\log_g x$로 표시하는 것은 잘 알려진 사실이다. 19세기 초 Galois에 의해서 Galois체가 도입된 이후 이산로그 문제는 중요한 수학적 문제의 하나가 되어왔지만 Diffie-Hellman의 키 교환법[3]과 이를 변형한 El Gamal의 공개키 암호법이 1989년 제시된 이후 본격적인 관심을 끌어왔다 하겠다. 이산로그 문제는 일반적인 갈로아체 GF(q)에서도 정의될 수 있지만 하드웨어 구현시의 편리함 때문에 $GF(2^n)$이 주로 사용되고 있다. $GF(2^n)$에서의 이산로그 계산법 중 가장 효율적인 것으로는 Coppersmith의 방법을 들 수 있다. Coppersmith의 방법은 1984년 제시된 것으로서 이후 여러가지 테크닉을 이용한 개선이 꾸준히 이루어져 왔으며, 최근에는 소인수 분해법의 large prime variation과 비견되는 large irreducible factor method를 이용한 개선된 Coppersmith 알고리즘이 제시되었다. Coppersmith 알고리즘의 실행기록은 소인수 분해법의 경우와 달리 $GF(2^{127})$에 머물고 있다. 이유는 여러가지로 설명될 수 있겠지만 Cunningham table의 완성과 같은 동기가 없었고 Coppersmith 이산로그 계산 알고리즘을 수행할 때 발생하는 일차방정식이 MPQS의 경우와 달리 binary linear equation system이 아니고 2^n-1을 법(modulus)으로 하는 linear equation system이기 때문에 실제 시행시 부딪히는 벽은 계산속도 보다도 기억용량이 되기 때문이다.

또한 RSA 경우 보다 El Gamal의 경우에는 3절에서 설명되듯이 bit length가 훨씬 커지기 때문에 연산처리시의 계산속도가 늦어지는 것도 큰 문제가 되어왔다.

이 문제는 1982년 Massey와 Omura[15]가 $GF(2^n)$에서의 정규기저를 이용한 고속연산법을 제시한 이후 급속한 발전을 이루어 왔으며 최근에는 Varistone[10] 등이 제시한 최적정규기저(Optimal normal basis)를 사용하여 $GF(2^n)$에서의 곱셈 및 멱승(exponentiation) 연산시 연산 횟수를 획기적으로 줄일 수 있게 되었다.

본 연구팀은 현재 이 분야에 대해 연구하고 있으며 내년경에는 결과가 나올 예정이다.

3. RSA 암호법과 El Gamal 암호법의 비교

3절에서는 먼저 정수의 소인수 분해 실행시간과 갈로아체 $GF(2^n)$에서의 이산로그 계산 실행시간을 비교하려 한다. 이에 근거하여 계산량의 관점에서 RSA와 El Gamal 암호법을 비교하려 하며 이후 멱승처리량(exponentiation through root)을 비롯한 다른 면에서 두가지 암호법을 비교하려 한다.

2절에서 살펴 본 바와 같이 MPQS를 사용하여 합성수 N을 인수분해 하는데 걸리는 실행시간과

갈로아체 $GF(2^n)$에서 Coppersmith 이산로그 계산법을 실행할때의 실행시간은 각각 $\exp[(1+o(1))(\exp N)^{1/2}(\log\log N)^{1/2}]$과 $\exp[(1.35+o(1))n^{1/3}(\log n)^{2/3}]$으로 추정된다. N이 512-bit 합성수 일때 위의 식은 인수분해를 위해서 6.69×10^{19} 'operations'라는 계산량을 필요로 하고 있음을 알 수 있으며, 이 계산량은 윗식에 의하여 $n \approx 850$ 정도가 되며 마찬가지로 N이 332 bit일 때는 2.34×10^{15} 'operations'의 계산량이 필요하고 이것은 $n \approx 475$에 대응된다.

실제로 Coppersmith 알고리즘을 실행하여 보면 나타나는 일차 방정식의 계수가 MPQS의 경우와 달리 이항 계수가 아니기 때문에 훨씬 복잡하고 실행시간이 추정 시간보다 많이 소요됨을 알 수 있다. 이러한 사유로 n의 크기를 보다 더 보수적으로 택할 필요가 있다. 따라서 N이 각각 332 bit와 512 bit일 때 n을 400^+와 700^+ 정도의 크기로 택하면 거의 같은 계산량을 요할 것으로 추정된다.

이제까지는 소인수 분해의 어려움과 이산로그 계산의 어려움이라는 RSA와 El Gamal 암호법이 안전도를 근거로 하는 정수론 문제의 난해성을 분석하여 두 암호법을 비교 분석하였다. 이제 두 암호법을 다른 면에서 비교하려 한다.

RSA와 El Gamal 암호법을 실행하기 위해서는 각각 modular 멱승과 갈로아체에서의 이산멱승(discrete exponentiation)을 요하고 있다. 이들 멱승은 선형적 기법인 'square and multiply' 멱승법에 의해서 시행되는 것이 보통이다. 그러나 El Gamal 암호법에서 쓰이는 이산멱승의 경우에는 Massey-Omura 방법을[15] 사용할 수 있다는 장점이 있다. 1982년 Massey와 Omura에 의해서 개발된 이 방법은 squaring을 원소계수벡터의 cyclic shifting으로 바꾸어 주며 채택하는 정규기저에 종속하는 곱셈함수를 이용하여 곱셈 과정을 자동화할 수 있다.

특히 Vanstone[10]등에 의해 최근 개발된 최적 정규기저 사용시 $GF(2^n)$에서 곱셈함수의 영이 아닌 성분이 $2n-1$로 대폭 줄어들기 때문에 곱셈에 소요되는 시간이 대폭 줄어든다. 따라서 사용하는 갈로아체 $GF(2^n)$을 잘 선택하여 최적 정규기저를 갖는 것으로 하면 이산멱승에 소요되는 시간은 특히 줄어들 수 있을 것이다. 최적 정규기저는 특히 관련 곱셈함수를 단순화 시키기 때문에 과거에는 거의 불가능하였던 $n > 1000$의 $GF(2^n)$에서의 Massey-Omura 고속연산 chip설계 및 하드웨어 구현을 가능하게 만들었다. 앞으로 이 부분에서의 연구가 진전된다면 구현상의 효율성 때문에 El Gamal 암호법이 좀 더 유리한 위치에 설 것으로 추정 된다. 마지막으로 타원곡선 위에서의 암호법을 언급하려 한다. 갈로아체 $GF(2^n)$ 위에서의 타원곡선은 덧셈하에서의 군을 이루고 이러한 사실을 이용하여 $GF(2^n)$에서와 같이 이산로그를 정의할 수 있다. 따라서 비슷한 방법으로 El Gamal 암호법을 정의할 수 있는데 이 경우 이산로그 계산에 소요되는 실행시간은 얼마나 될 것인가? 최근 Vanstone[9] 등은 $GF(2^n)$ 위에서 타원곡선을 잘 선택하면 Coppersmith 알고리즘 사용시 $GF(2^{4n})$ 위에서의 이산로그 계산하는 것과 같은 정도의 계산량을 갖게 된다는 것을 보였다. 예를들면 $GF(2^n)$ ($n \approx 175, 200$) 위에서의 타원곡선을 사용하여 El Gamal 암호법을 채택하면 현재로서는 $GF(2^m)$ ($n \approx 700, 800$) 위에서의 El Gamal 암호법을 채택한 것과 같은 안전도를 갖게 된다고 할 수 있다. 따라서 bit-length의 급속한 증가로 인한 message-expansion 문제가 어느 정도 해결된다고 볼 수 있다. 하지만 현재 타원곡선 분야에서 이루어지고 있는 활발한 연구로 볼 때 안심할 수 만은 없다.

4. 결 론

본 논문에서는 대표적인 공개키 암호법인 RSA 암호법과 El Gamal 암호법을 주로 계산량적 관점과 구현 효율성 면에서 비교하여 보았다. $GF(2^n)$ 위에서의 El Gamal 암호법은 최적 정규기저를 사용하면 구현 효율성이 대폭 향상되고 타원곡선 사용시 현재로서는 RSA 암호법의 경우 보다 bit-length도 줄어들 수 있기 때문에 앞으로 발전의 여지가 많지 않은 RSA 암호법 보다 더욱 선호될 것으로 추정된다.

참 고 문 헌

1. D. Coppersmith, "Fast evaluation of logarithms in fields of characteristic two," IEEE Trans. Inform. Theory, Vol. IT-30, No. 4, pp. 587-594, July 1984.

2. D. Coppersmith, "Modifications to the number fields sieve," IBM Research Report #RC 16264(Nov. 1990 : updated Mar. 1991).

3. W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, Vol. IT-22, No. 6, pp. 644-654, Nov. 1976.

4. T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithm," IEEE Trans. Inform. Theory, Vol. IT-31, No. 4, pp. 469-472, July 1985.

5. A.K. Lenstra and H.W. Lenstra, Jr., "Algorithms in number theory," in Handbook of Theoretical Computer Science, A. Meyer, M. Nivat, M. Paterson, and D. Perrin, eds., North Holland, Amsterdam(in press).

6. A.K. Lenstra, H.W. Lenstra, Jr., M.S. Manasse, and J.M. Pollard, "The number field sieve," Proc, 22nd ACM Symp. Theory of Computing, pp. 464-572, 1990.

7. A.K. Lenstra and M.S. Manasse, "Factoring by electronic mail," in Lecture Notes in Computer Science 434 : Advances in Cryptology : Proc. Eurocrypt'89. J.J. Quisquater and J. Vandewalle, Eds., Houthalen, Belgium, April 10-23, 1989, pp. 335-371. Berlin : Springer-Verlag, 1990 : I. Damgard, Ed., pp. 72-82, Berlin : Springer-Verlag, 1991.

8. H.W., Lenstra, Jr., "Factoring with elliptic curves," Ann. Math, Vol. 126, pp. 649-673, 1987.

9. A. Menezes, T. Okamoto, and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite fields," (Unpublished manuscuipt, Sept, 1990).

10. R. Mullin, I. Onyszchuk, S. Vanstone, and R. Wilson, "Optimal normal basis in GF(p^n)". Discrete Applied Mathematics, Vol. 22, pp. 149-161, 1988/1989.

11. R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, Vol. 21. pp. 120-126, 1978.

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

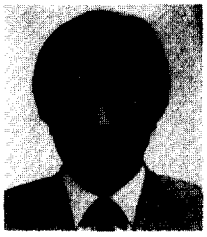
13. Paul C. Van Oorschot, "A Comparison of Practical Public Key Cryptosystems Based on Integer Factorization and Discrete Logarithms," IEEE Press 'Contemporaty Cryptology', pp. 289-322, 1992.

14. Pomerance "Factroing" in proceedings of symposium in applied Math. Vol. 42, AMS, 1990.

15. J.L. Massey and J.K. Omura, Patint Application of "Computational Method and Apparatus for Finite Field Arithmetic, "submitted in 1981.

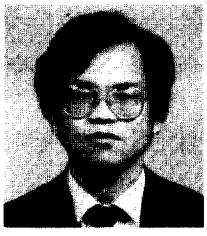
16. 조인호, 임종인, ETRI 연구보고서, 1987-1991.

□ 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)
현 재 高麗大學校 自然科學大學 副教授
關心分野 : 정수론 및 관련응용분야



서 광 석(正會員)

1982년 고려대학교 수학과 졸업
1989년 고려대학교 대학원 졸업(석사, 박사)
1989년 고려대학교 부설 산업개발 연구소 선임연구원
1991년 서남대학교 수학과 조교수
關心分野 : 정수론 및 관련응용분야