情報保護學會論文誌
第16卷 第5號, 2006. 10

Domingo-Ferrer의 첫번째 privacy homomorphism에 대한 알려진 평문 공격*

이 문 성,† 한 상 근‡
한국과학기술원

Known-plaintext attack of the Domingo-Ferrer's first privacy homomorphism scheme*

Moon Sung Lee,† Sang Geun Hahn‡
Korea Advanced Institute of Science and Technology

요 약

우리는 Domingo-Ferrer의 첫번째 privacy homomorphism 스킴에 대하여 알려진 평문 공격을 한다. 그 결과, 법 n이 공개일 경우에는 두개의 평문-암호문 쌍이, 비밀일 경우에는 세개 또는 그 이상의 평문-암호문 쌍이 있으면 비밀키를 얻기에 충분하다는 것을 보인다.

ABSTRACT

We analyze Domingo-Ferrer's first privacy homomorphism scheme with known-plaintext attack. As a result, it is possible to get the secret key if we know two known plaintext-ciphertext pairs when modulus n is public, and three or more pairs are sufficient when modulus n is secret.

Keywords : *Domingo-Ferrer, privacy homomorphism, known-plaintext attack, homomorphic encryption*

Ⅰ. 서 론

Privacy homomorphism(이하 PH)의 개념은 Rivest 등에 의해서 1978년에 처음으로 소개되었다[1]. PH란 복호화 함수에 대해서 모르더라도 암호화된 자료만 가지고도 계산을 가능하게 하는, 즉 평문 x, y를 모르더라도 암호문 $E(x)$와 $E(y)$를 안다면 이를 이용하여 $E(x+y)$ 또는 $E(xy)$와 같은 것을 계산할 수 있는 암호화 방식이다. 우리가 잘 아는 RSA암호도 $E(xy)=E(x)E(y)$의 성질을 가지므로 PH의 일종이라 할 수 있다. [1]에서는 여러가지 방식의 PH들이 소개되었는데 그 중 두 가지는 알려진 평문 공격(Known Plaintext attack)에, 다른 두 가지는 암호문 단독 공격(Ciphertext Only attack)에 취약하다는 것이 Brickell 등에 의해서 밝혀졌다[2]. Brickell 등은 그 외에도 R-additive PH라는 개념을 제시한 후 암호문 단독 공격에 안전하다고 생각되는 R-additive PH를 제시하였다. R-additive PH란 암호문들만을 이용해서 대응하는 메세지들의 최대 R개까지의 합에 해당하는 암호문을 계산할 수 있는 암호화 방식이다. 일반적인 PH보다 조건을 강

접수일: 2006년 5월 25일; 채택일: 2006년 9월 22일
* 이 논문은 2004년도 한국학술진흥재단의 지원에 의하여 연구되었음(KRF-2004-041-C00060).
† 주저자, ms.lee@kaist.ac.kr
‡ 교신저자, sghahn@kaist.ac.kr

화시킴으로써 안전성을 얻으려 했던 방식인 것이다. 그 후 1996년에 Domingo -Ferrer에 의해서 덧셈, 뺄셈, 곱셈이 모두 가능한 대수적 PH가 제시되었고 (이하 PH_1)[3], 알려진 평문 공격에 안전하다고 주장되었다. 하지만 이 방식은 두 암호문의 곱셈을 하면 할수록 암호문의 분량이 급격히 커지는 단점이 있었다. 이런 단점을 보완한 새로운 방식이 2002년에 같은 저자에 의해서 제시되었고(이하 PH_2)[4], 저자들은 PH_2가 알려진 평문 공격에 안전하다고 주장하였다. 하지만 1년 후 PH_2가 알려진 평문 공격에 취약하다는 사실이 밝혀졌고[5,6], 그 후 PH_1 역시 알려진 평문 공격에 취약하다는 사실이 Cheon 등에 의해서 밝혀졌다[7].

본 논문에서는 PH_1에 대해서 Cheon 등의 알려진 평문 공격보다 더 적은 수의 알려진 평문-암호문 쌍으로 공격할 수 있음을 보인다. Cheon 등의 알려진 평문 공격은 암호화에 쓰이는 랜덤한 다항식의 차수가 d 라 할 때, $d+1$개 이상의 알려진 평문-암호문 쌍을 필요로 하는 반면 제안하는 방식은 2개 정도의 알려진 평문-암호문 쌍만으로 공격할 수 있다.

Ⅱ. Domingo-Ferrer의 스킴

여기서는 1996년에 발표된 Domingo-Ferrer의 스킴 PH_1을 살펴본다.

⊙ 공개된 값 : n과 d (n은 안전성을 높이기 위해 비밀이 될 수도 있다. 그럴 경우에는 효율성이 떨어진다.)

⊙ 비밀키 : $pq=n$을 만족하는 큰 소수 p와 q, $Z_p-\{0\}$에서 큰 부분군을 생성하는 수 $r_p \in Z_p$와 Z_q에 대해서 비슷한 성질을 만족하는 $r_q \in Z_q$.

⊙ 암호화 : 메세지를 $a \in Z_n$라 하자. 다음 조건을 만족하는 d차 이하의 랜덤한 다항식 $f(X) \in Z_n[X]$, $f(0)=0$, $f(1) \bmod n = a$ 를 선택한다. 암호문은 다음과 같다.

$$E(a) = (f(r_p X) \bmod p, f(r_q X) \bmod q) \quad (1)$$
$$= (g_p(X), g_q(X))$$

암호문은 다항식의 계수로서만 표현되고, r_p와 r_q의 값은 암호문에서 드러나지 않는다.

⊙ 복호화 : 암호문을 $(g_p(X), g_q(X))$라 하자: r_p와 r_q를 이용하여 $f_p(X) = g_p(r_p^{-1}X) \bmod p$와 $f_q(X) = g_q(r_q^{-1}X) \bmod q$를 계산한 후, $a_p = f_p(1) \equiv a \pmod p$와 $a_q = f_q(1) \equiv a \pmod q$를 계산하고, 중국인의 나머지 정리를 이용, 메세지 a를 계산한다.

암호화된 메세지에 대한 덧셈, 뺄셈, 곱셈의 계산은 다항식의 덧셈, 뺄셈, 곱셈을 그대로 이용하면 된다. n이 공개되어 있을 경우에는 다항식의 계수들을 법 n으로 계산하고, n이 비밀일 경우에는 계수를 정수로서 계산하면 된다. 곱셈 횟수가 증가하면 다항식의 차수가 커지기 때문에 효율성이 감소하며, n이 비밀인 경우에는 계수의 크기가 급격히 증가해서 비효율적이다.

Ⅲ. 알려진 평문 공격

여기서 우리는 Domingo-Ferrer의 PH_1에 대한 새로운 알려진 평문 공격을 제안한다. Cheon 등의 공격법은 행렬식을 이용하였는데, 우리는 다항식의 종결식(Resultant)을 이용하여 더 좋은 결과를 얻을 수 있음을 보인다. 종결식을 이용한 공격은 Wagner가 Domingo-Ferrer의 PH_2를 분석할 때 사용하였던 방법이다[5]. 우선 종결식의 정의와 성질을 알아보자. 자세한 내용은 [8]을 참조하기 바란다.

종결식은 Sylvester행렬의 행렬식으로 정의된다. 즉, 주어진 두개의 다항식

$$f(X) = v_0 X^n + \cdots + v_n = v_0 (X-\alpha_1)\cdots(X-\alpha_n),$$

$$g(X) = w_0 X^m + \cdots + w_m = w_0 (X-\beta_1)\cdots(X-\beta_m)$$

에 대하여 종결식은 다음과 같이 정의된다[8].

$$Res(f,g) = \begin{vmatrix} v_0 & v_1 & \cdots & v_n & & \\ & v_0 & v_1 & \cdots & v_n & \\ & & \cdots & \cdots & \cdots & \\ & & & v_0 & v_1 & \cdots & v_n \\ w_0 & w_1 & \cdots & w_m & & \\ & w_0 & w_1 & \cdots & w_m & \\ & & \cdots & \cdots & \cdots & \\ & & & w_0 & w_1 & \cdots & w_m \end{vmatrix} \quad (2)$$

따라서, 주어진 두개의 다항식 $f(X)$와 $g(X)$에 대하여 종결식 $\mathrm{Res}(f,g)$를 f와 g의 계수를 이용하여 쉽게 구할 수 있음을 알 수 있다.

또한 종결식은 다음과 같은 식으로도 표현된다[8].

$$Res(f,g)=v_0^m u_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j) \quad (3)$$

따라서, f와 g가 공통근이 있을 경우에 이 종결식의 값이 0이 됨을 알 수 있다. 만약 f와 g가 법 p로 공통근이 있을 경우에는 종결식 Res(f,g)은 법 p로 0이 된다. 즉, p의 배수가 된다.

우리는 이와 같은 종결식의 성질을 이용하여 다음과 같은 방법으로 비밀키를 구한다. 우선 두개의 큰 소수의 곱인 n이 공개된 경우를 살펴보고, 그 후 비밀일 경우를 살펴본다.

1. n이 공개된 경우

두 개의 평문-암호문 쌍 $(a,(g_p(X),g_q(X)))$, $(a',(g_p'(X),g_q'(X)))$을 가지고 있다고 가정하자. $h_p(X)=g_p(X)-a$, $h_p'(X)=g_p'(X)-a'$ 이라 하면, h_p와 h_p'은 주어진 평문-암호문 쌍으로부터 쉽게 계산될 수 있으며, 법 p로 공통근 r_p^{-1}를 가짐을 알 수 있다. 따라서 h_p와 h_p'의 종결식 Res(h_p,h_p')은 p의 배수가 되어, gcd$(n,$Res$(h_p,h_p'))$은 n 또는 p가 된다. Res(h_p,h_p')는 q와 독립적인 값이므로 이 값이 0이 되지 않는 한 q의 배수가 될 확률은 거의 없으므로 gcd$(n,$Res$(h_p,h_p'))$는 매우 높은 확률로 p가 된다. p를 구하면, $pq=n$을 이용, q도 쉽게 구할 수 있다.

일단 p를 알게 되면, 다항식 $h_p(X)$와 $h_p'(X)$의 법 p에서의 gcd(h_p,h_p')를 쉽게 찾아서 법 p로 인수분해하면 공통근들을 찾으며 그 공통근 중 하나가 r_p^{-1}가 되고, 법 p로 역원을 구하면 r_p가 된다. 같은 방식으로 $h_q(X)=g_q(X)-a$와 $h_q'(X)=g_q'(X)-a'$을 이용하여 r_q도 구할 수 있으므로 비밀키를 모두 구할 수 있다. 다항식을 소수인 법으로 인수분해하는 것이 쉬운 문제라는 것은 주지의 사실이다.

2. n이 비밀인 경우

이 경우에는 위의 경우보다 약간 더 많은 알려진 평문-암호문 쌍이 필요하다. 최소 세개 이상의 평문-암호문 쌍

$$\begin{aligned}&(a,(g_p(X),g_q(X))),\\&(a',(g_p'(X),g_q'(X))),\\&(a'',(g_p''(X),g_q''(X)))\end{aligned} \quad (4)$$

이 주어져 있다고 가정하자. 위에서와 같은 방식으로 다음과 같은 다항식들을 정의한다.

$$\begin{aligned}&h_p(X)=g_p(X)-a,\\&h_p'(X)=g_p'(X)-a',\\&h_p''(X)=g_p''(X)-a''\end{aligned} \quad (5)$$

앞에서와 같은 이유로 (5)의 다항식들 h_p, h_p', h_p''들은 법 p에서의 공통근으로 r_p^{-1}를 가질 것이다. 따라서 이들 세 다항식 중 임의의 두 다항식의 종결식은 p의 배수가 될 것이며, 그 종결식들의 최대공약수 역시 p의 배수가 될 것이다. 즉,

$$G=\gcd(Res(h_p,h_p'),Res(h_p,h_p''),Res(h_p',h_p'')) \quad (6)$$

라 하면, $p|G$ 임을 알 수 있다.

우선, G를 평문-암호문 쌍으로부터 구한다. 만약 G가 소수라면 $p=G$ 가 되는 것이고, 소수가 아니라면 소인수분해를 통해서 p를 알 수 있다. 일반적으로, 종결식 Res(h_p,h_p'), Res(h_p,h_p''), Res(h_p',h_p'')들은 소수 p의 배수 중 임의의 하나들이 되므로, 이들의 최대공약수가 p외에 큰 소수를 포함할 확률은 상당히 작다. 따라서 G는 소수이거나 소수 p에 작은 수들을 곱한 값이 될 것이고, 쉽게 소인수 분해가 될 것이다. 만약 소인수 분해가 잘 안된다면, 알려진 평문-암호문 쌍이 좀 더 필요하다. 새로운 평문-암호문 쌍을 가져와서 h_p'''을 계산한 후, h_p, h_p', h_p''과의 종결식을 구하고, 그 종결식들과 G의 최대공약수를 구해 보면 소수 p가 되거나, p에 작은 수들을 곱한 것이 될 것이므로 p를 구할 수 있다. $h_q(X)=g_q(X)-a$와 h_q', h_q''들을 이용하여 마찬가지 방식으로 q 역시 구할 수 있다.

일단 p와 q를 알게 되면 n이 공개일 경우와 같은 방식으로 r_p와 r_q를 구할 수 있고, 비밀키를 알게 되어 암호문을 해독할 수 있게 된다.

결과적으로 공격방법에 사용된 계산들, 즉 종결식을 구하는 것과 다항식들의 gcd를 구하는 것, 그리고 주어진 소수를 법으로 다항식을 인수분해하는 것은

모두 쉽기 때문에 충분히 빠른 시간에 매우 높은 확률로 공격이 가능하는 것을 알 수 있다.

3. 예 제

여기서는 예제를 통해서 우리의 방법으로 비밀키를 얻을 수 있음을 보여준다. 공개키와 비밀키가 다음과 같다고 하자.

$p = 17952915162207054683,$

$q = 14270821805301197639,$

$r_p = 5020707987769003944,$

$r_q = 6339887576334177325,$

$d = 6,$

$n = pq = 256202853165546923555007829714663493437.$

평문 두 개를 각각

$a = 112358132134558914423337761098715 97,$

$a' = 213471118294069109178287465744 1209$

라 하고, 두 개의 랜덤한 다항식 f와 f'은 각각

$$f(X) = 719830507249647877926098820546945363 22X^6 + 199244177743702249932336521299851922584X^5 + 163971366156093170412641544690852522398X^4 + 106610569353371162900887362456711670965X^3 + 105322804500067342116283298947189662344X^2 + 121487826831655513401707213470800037295X$$

$$f'(X) = 140135820941460871462157884224213899378X^6 + 516928345215621327566325016975878160 97X^5 + 121080006932440204186175202925204657145X^4 + 219475393356406073883637720635000142290X^3 + 248327280010544165144429885674262942681X^2 + 244102211610957187478089906577041957366X$$

라 하면 두 개의 메세지 a와 a'은 다음과 같이 암호화된다.

$$E(a) = (f(r_pX) \bmod p, f(r_qX) \bmod q) = (g_p(X), g_q(X)) = (225304732518459956 0X^6 + 167567779536580838 86X^5 + 164386595420690045 6X^4 + 607035164265981118 7X^3 + 985985534519491801 0X^2 + 141039387359904174 68X, 133715953726813927 36X^6 + 497250695172204530 6X^5 + 129448599093333433 48X^4 + 371623520749192724 2X^3 + 330681924846641742 5X^2 + 506791033535933139 9X)$$

$$E(a') = (f'(r_pX) \bmod p, f'(r_qX) \bmod q) = (g_p'(X), g_q'(X)) = (626558864996859821X^6 + 6490940938330104917X^5 + 406382220789766761 7X^4 + 664807818108444858 1X^3 + 150073774846337935 25X^2 + 111778832669622073 41X, 966305383514738790 4X^6 + 624461040513926083 6X^5 + 783912768563483326 1X^4 + 655946846527207030 2X^3 + 665822472605818493 1X^2 + 851673789336228994X)$$

우리는 위 두 개의 평문-암호문 쌍들을 이용해서 비밀키를 구한다. 다음 계산을 통해서 p와 q를 구할 수 있다.

$h_p(X) = g_p(X) - a,\ h_p'(X) = g_p'(X) - a'$을 구한 후 종결식을 구해 보면,

$$g = Res(h_p(X), h_p'(X)) \bmod n = 151428641060129935088844470718697388855$$

가 되며, $p = \gcd(n, g) = 17952915162207054683$가 되어 p를 구할 수 있고, q 역시 다음처럼 쉽게 구할 수 있다.

$q = n/p = 14270821805301197639.$

이제 다음과 같은 과정으로 r_p를 구할 수 있고, 마찬가지로 r_q 역시 쉽게 구할 수 있다.

$$\gcd(h_p(X), h_p'(X)) \bmod p = X + 15929856129994795006$$

$$r_p = (-15929856129994795006)^{-1} \bmod p = 5020707987769003944$$

Ⅳ. 결 론

두가지 privacy homomorphism 스킴들이 Domingo-Ferrer에 의하여 1996년[3]과 2002년[4]에 제안되었다. 두번째 스킴은 Wagner[5]와 Bao[6]에 의해서 분석되었고, 첫번째 스킴은 Cheon 등[7]에 의해서 분석되었다. 우리는 종결식을 이용하는 것이 Cheon 등의 공격보다 더 효율적임을 보였다. 결론적으로, Domingo-Ferrer의 첫번째 스킴 PH_1은 법 n이 공개인 경우에는 두개의 알려진 평문-암호문 쌍이 있으면 해독이 가능하고, 법 n이 비밀인 경우에는 세개 또는 그 이상의 알려진 평문-암호문 쌍이 있으면 해독이 가능하다.

참 고 문 헌

[1] R. Rivest, L. Adleman, M. Dertouzos, On data banks and privacy homomorphisms, *Foundations of Secure Computation*, Academic Press, new York, pp. 169-179, 1978.

[2] E. Brickell, Y. Yacobi, On privacy homomorphisms, *Advances in Cryptology, Eurocrypt'87*, LNCS, vol. 304, Springer-Verlag, Berlin, pp. 117-125, 1988.

[3] J. Domingo-Ferrer, A new privacy homomorphism and applications, *Information Processing Letters*, vol. 60, pp. 277-282, 1996.

[4] J. Domingo-Ferrer, A provably secure additive and multiplicative privacy homomorphism, ISC2002, LNCS, vol. 2443, Springer-Verlag, Berlin, pp. 471-483, 2002.

[5] D. Wagner, Cryptanalysis of an algebraic privacy homomorphism, ISC2003, LNCS, vol. 2851, Springer-Verlag, Berlin, pp. 234-239, 2003.

[6] F. Bao, Cryptanalysis of a provable secure additive and multiplicative privacy homomorphism, International Workshop on Coding and Cryptography(WCC), pp. 43-50, 2003.

[7] J.-H. Cheon, W.-H. Kim, H.-S. Nam, Known-plaintext cryptanalysis of the Domingo-Ferrer algebraic privacy homomorphism scheme, *Information Processing Letters*, vol. 97, pp. 118-123, 2006.

[8] Serge Lang, *Algebra*, Addison-Wesley Publishing company, 3rd Edition, 1995.

〈著者紹介〉

이 문 성 (Moon Sung Lee) 학생회원

2001년 2월 : 한국과학기술원 물리학과 졸업
2003년 2월 : 한국과학기술원 수학과 석사 졸업
2003년 3월~현재 : 한국과학기술원 수학과 박사과정
〈관심분야〉 암호학, 정수론

한 상 근 (Sang Geun Hahn) 종신회원

1979년 : 서울대학교 수학과 졸업
1982년 : 뉴멕시코 주립대 석사 졸업
1987년 : 오하이오 주립대 박사 졸업
1987년 ~ 현재 : 한국과학기술원 수학과 교수
〈관심분야〉 암호학, 타원곡선, 정수론