근사최대공약수문제에 기초한 한가지 공개열쇠암호체계

곽위성, 김철은

우리는 량자콤퓨터로도 풀수 없는 첨단암호로서 안전성이 근사최대공약수문제의 계산복잡성에 기초한 한가지 공개열쇠암호체계를 연구하였다.

씨인수분해문제나 리산로그문제의 곤난성에 의거하고있는 RSA암호나 타원곡선암호들을 비롯한 공개열쇠암호들이 량자콤퓨터에 의한 단축공격법으로 쉽게 풀린다는데로부터 최근 안전성이 담보되는 새 세대 암호를 개발하기 위한 연구가 본격적으로 진행되고있다.[4]

현재 널리 연구되고있는 새 세대 암호들중 실용화의 측면에서 주목을 끌고있는것은 암복호화알고리듬이 단순한 옹근수모듈연산들로 정의되고 암호문들에서의 문자렬검색을 비롯한 다양한 연산을 안전하게 보장하는 공개열쇠암호체계이다.

이런 암호체계의 안전성은 근사최대공약수(AGCD)문제의 계산복잡성에 의거하고있다.

AGCD문제는 어떤 씨수 혹은 몇개의 씨수들의 적의 근사공배수가 여러개 주어졌을때 그것들의 공약수를 계산하는 문제로서 현재 오유동반학습(LWE)문제보다 더 어려운 문제로 알려져있다.

선행연구[1]에서 처음으로 제기된 AGCD문제에 의거하면서 옹근수연산으로 정의되는 공개열쇠암호체계는 1bit단위로 암, 복호화가 진행된다는 결함을 가지고있다.

선행연구[2, 3]에서는 AGCD변종문제(주어진 근사공배수들중에 근사값이 0인 수가 1개 끼워있는 경우의 AGCD문제)에 기초하여 한번에 여러bit들을 처리할수 있는 다중비트공개열쇠암호체계를 제기하였지만 안전성의 기초로 되는 AGCD변종문제의 계산복잡성이 AGCD문제보다 떨어지므로 량자콤퓨터에 의하여 비공개열쇠의 일부를 쉽게 알아낼수 있다는 약점을 가지고있다.

론문에서는 AGCD문제에 안전성의 기초를 두고있으면서 옹근수연산으로 정의되는 공개열쇠암호체계에 대한 선행연구들에서 나타난 결함들을 극복할수 있는 새로운 다중비트공개열쇠암호체계를 제기하였다.

우선 몇가지 기호들을 약속하자.

$a \leftarrow \varphi$ 는 분포 φ 에 따르는 우연량의 표본값을 선택한다는것을, $a \leftarrow A$ 는 모임 A 에서 원소 a 를 평등우연적으로 선택한다는것을, $[x]$ 는 x 에 가장 가까운 옹근수로서 만일 그런 옹근수가 2개 있다면 큰수를 선택한다는것을 의미한다.

$\mathrm{CRT}_{p_1,\cdots,p_k}(a_1,\ \cdots,\ a_k),\ a_i \in \left[-\dfrac{p_i}{2},\ \dfrac{p_i}{2}\right)$ 는 반열린구간 $\left[0,\ \prod_{i=1}^{k} p_i\right)$ 의 수로서 씨수 $p_1,\ \cdots,\ p_k$ 로 나눈 나머지가 각각 $a_1,\ \cdots, a_k$ 로 되는것을 의미한다. 중국나머지정리에 의하면 이런 수는 항상 유일존재한다. 즉

$$\mathrm{CRT}_{p_1,\ \cdots,\ p_k}(a_1, \cdots, a_k) = \left(\sum_{i=1}^{k} a_i \hat{p}_i (\hat{p}_i^{-1} \bmod p_i)\right) \bmod T,\ \ T := \prod_{i=1}^{k} p_i,\ \ \hat{p}_i := \frac{T}{p_i} = \prod_{j=1}^{k} p_j \Big/ p_i$$

η −비트씨수 $p_1, \cdots, p_k$ 들에 대하여 다음과 같은 분포를 정의하자.

$$\Phi_\rho(p_1, \cdots, p_k) := \{\mathrm{CRT}_{p_1, \cdots, p_k}(r_1, \cdots, r_k) \mid r_i \leftarrow \boldsymbol{Z} \cap (-2^\rho, 2^\rho)\}$$

$$D_{\gamma, \rho}(p_1, \cdots, p_k) := \left\{x = q\prod p_i + r \,\middle|\, q \leftarrow \boldsymbol{Z} \cap \left[0, 2^\gamma / \prod p_i\right), \ r \leftarrow \Phi_\rho(p_1, \cdots, p_k)\right\}$$

$$D_{\gamma, \rho, j}(p_1, \cdots, p_k) :=$$

$$= \left\{y = \mathrm{CRT}_{p_1, \cdots, p_k}(0, \cdots, [p_j/2], \cdots, 0) + q\prod p_i + r \,\middle|\, q \leftarrow \boldsymbol{Z} \cap \left[0, 2^\gamma / \prod p_i\right), \ r \leftarrow \Phi_\rho(p_1, \cdots, p_k)\right\}$$

정의 분포 $D_{\gamma, \rho}(p_1, \cdots, p_k)$ 와 평등분포 $U(\boldsymbol{Z} \cap [0, 2^\gamma))$ 을 구별하는 문제를 $(\rho, \eta, \gamma) - k -$ AGCD판정문제, 분포 $D_{\gamma, \rho, j}(p_1, \cdots, p_k)$ 와 평등분포 $U(\boldsymbol{Z} \cap [0, 2^\gamma))$ 을 구별하는 문제를 $(\rho, \eta, \gamma, j) - k -$ AGCD판정문제라고 부른다.

$(\rho, \eta, \gamma) - k -$ AGCD판정문제와 $(\rho, \eta, \gamma, j) - k -$ AGCD판정문제는 동등한 판정문제라는것을 쉽게 알수 있다. 즉 $(\rho, \eta, \gamma) - k -$ AGCD판정문제의 다항식시간판정기가 존재하면 $(\rho, \eta, \gamma, j) - k -$ AGCD문제의 다항식시간판정기도 존재하며 그 거꿀도 성립된다.

따라서 LWE문제의 AGCD문제에로의 귀착관계를 고려하면 $(\rho, \eta, \gamma) - k -$ AGCD판정문제는 량자콤퓨터로도 풀기 어렵다는것을 알수 있다.

이제부터 λ 는 보안파라메터, ρ 는 오유항의 길이, η 는 비공개열쇠(씨수)의 길이, γ 는 암호문의 길이, τ 는 공개열쇠로 주어지는 근사공배수의 개수, k 는 비밀열쇠개수(통보문공간의 차원수)로 약속한다.

이 파라메터들사이에는 다음과 같은 관계가 성립된다고 가정한다.[2]

$$\rho \geq \lambda, \ \gamma \geq \Omega(\lambda(\eta - \rho)^2 / \log\lambda), \ \gamma \geq \eta^2, \ \tau \geq \gamma + 2\lambda + 2$$

먼저 입력값이 $\lambda, \rho, \eta, \gamma, \tau, k$ 이고 출력값이 비공개열쇠 sk 와 공개열쇠 pk 인 열쇠생성알고리듬 KeyGen($\lambda, \rho, \eta, \gamma, \tau, k$) 에 대하여 보자.

걸음 1 η −비트홀씨수 $p_1, \cdots, p_k$ 를 선택하고 $sk := \{p_1, \cdots, p_k\}$ 로 놓는다.

걸음 2 $x_i \leftarrow D_{\gamma, \rho}(p_1, \cdots, p_k)$ $(i = 0, \cdots, \tau)$들을 선택하고 필요하면 번호를 다시 매겨 x_0 이 $\max\{x_0, x_1, \cdots, x_\tau\}$ 가 되도록 한다.

걸음 3 $\forall j = 1, \cdots, k$ 에 대하여 $\{1, \cdots, \tau\}$ 의 부분모임 S_j 를 우연선택한다.

$$y_j := \left(\mathrm{CRT}_{p_1, \cdots, p_k}(0, \cdots, \underset{j}{[p_j/2]}, \cdots, 0) + \sum_{i \in S_j} x_i\right) \bmod x_0$$

걸음 4 $X := \{x_0, \cdots, x_\tau\}$, $Y := \{y_1, \cdots, y_k\}$, $pk := \{X, Y\}$

입력값이 공개열쇠 pk, k 차원평문벡토르 $\boldsymbol{m} = (m_1, \cdots, m_k)$ $(m_i \in \{0, 1\})$이고 출력값이 $\boldsymbol{m}$ 의 암호문 c 인 암호화알고리듬 Enc(pk, $\boldsymbol{m}$) 에 대하여 보자.

걸음 1 모임 $\{1, \cdots, \tau\}$ 의 부분모임 S 를 우연선택한다.

걸음 2 $c := \left(\sum_{j \in S} x_j + \sum_{i=1}^{k} m_i y_i\right) \bmod x_0$

다음으로 입력값이 비공개열쇠 sk, 암호문 c 이고 출력값이 k 차원평문벡토르 $\boldsymbol{m} = (m_1, \cdots, m_k)$ $(m_i \in \{0, 1\})$인 복호화알고리듬 Dec(sk, c) 에 대하여 보자.

걸음 $\boldsymbol{m} = (m_1, \cdots, m_k) = ([2c/p_1] \bmod 2, \cdots, [2c/p_k] \bmod 2)$

복호화알고리듬 $\mathrm{Dec}(sk,\ c)$의 정확성에 대하여 론의하자.

보조정리 1 k차원평문벡토르 $\boldsymbol{m}=(m_1,\cdots,\ m_k)$ $(m_i\in\{0,\ 1\})$의 암호문을 c로 표시하면 임의의 $i=1,\cdots,\ k$에 대하여 어떤 옹근수 Q_i와 조건 $|R_i|\le 2\tau(k+1)(2^{\rho}-1)$을 만족시키는 옹근수 R_i가 존재하여 $c=p_iQ_i+R_i+m_i[p_i/2]$가 성립된다.

증명 $c=\left(\sum_{j\in S}x_j+\sum_{i=1}^{k}m_iy_i\right)\bmod x_0=$

$$=\left(\sum_{i=1}^{k}m_i\left(\mathrm{CRT}_{p_1,\cdots,\ p_k}\left(0,\cdots,\ \left[\frac{p_i}{2}\right],\cdots,0\right)\right)+\sum_{i=1}^{k}m_i\left(\sum_{t\in S_i}x_t\right)+\sum_{j\in S}x_j\right)\bmod x_0$$

이때 적당한 옹근수 F와 $G\le k\tau+\tau=\tau(k+1)$이 존재하여 웃식은 다음의 식과 같다.

$$\mathrm{CRT}_{p_1,\cdots,\ p_k}\left(m_1\left[\frac{p_1}{2}\right],\cdots,\ m_i\left[\frac{p_i}{2}\right],\cdots,\ m_k\left[\frac{p_k}{2}\right]\right)+F\prod p_i+\sum_{i=1}^{k}m_i\left(\sum_{t\in S_i}x_t\right)+\sum_{j\in S}x_j-Gx_0$$

$x_j\leftarrow D_{\gamma,\ \rho}(p_1,\cdots,\ p_k)$이므로 어떤 q_{ji}와 $r_{ji}\in(-2^{\rho},\ 2^{\rho})$이 존재하여 $x_j=p_iq_{ji}+r_{ji}$가 성립되며 따라서 $c\equiv\left(m_i\left[\frac{p_i}{2}\right]+\sum_{i=1}^{k}m_i\left(\sum_{t\in S_i}r_{ti}\right)+\sum_{j\in S}r_{ji}-Gr_{0i}\right)\bmod p_i$이다.

$R_i:=\sum_{i=1}^{k}m_i\left(\sum_{t\in S_i}r_t\right)+\sum_{j\in S}r_j-Gr_0$으로 놓으면 $c\equiv\left(R_i+m_i\left[\frac{p_i}{2}\right]\right)\bmod p_i$이므로 어떤 옹근수 Q_i가 있어서 $c=p_iQ_i+R_i+m_i[p_i/2]$가 성립된다. R_i의 웃한계를 구해보면

$$|R_i|=\left|\sum_{i=1}^{k}m_i\left(\sum_{t\in S_i}r_t\right)+\sum_{j\in S}r_j-Gr_0\right|\le\left|\sum_{i=1}^{k}m_i\left(\sum_{t\in S_i}r_t\right)+\sum_{j\in S}r_j\right|+|Gr_0|\le 2\tau(k+1)(2^{\rho}-1)$$

이므로 보조정리가 증명된다.(증명끝)

보조정리 2 비공개열쇠 $sk=\{p_1,\cdots,\ p_k\}$에 대하여 k차원2진벡토르 $(m_1,\cdots,\ m_k)$와 옹근수 $c:=p_iQ_i+R_i+m_i[p_i/2]$를 줄 때 임의의 $i=1,\ \cdots,\ k$에 대하여 $|R_i|<p_i/4-1/2$이면 $\mathrm{Dec}(sk,\ c)=(m_1,\cdots,\ m_k)$가 성립된다.

정리 1 $\eta-\rho>\log(\tau(k+1))+4$일 때 평문 $\boldsymbol{m}:=(m_1,\cdots,m_k)$, $m_i\in\{0,\ 1\}$의 암호문 $c:=\mathrm{Enc}(pk,\ \boldsymbol{m})$은 평문 $\boldsymbol{m}$으로 복호화된다.

증명 $\eta-\rho>\log(\tau(k+1))+4$가 성립된다고 가정하면 다음의 식이 성립된다.

$$\eta-\rho>\log(\tau(k+1))+4\Leftrightarrow\ 2^{\eta-\rho}>2^{\log(\tau(k+1))+4}=16\tau(k+1)\ \Leftrightarrow\ 2^{\eta}/8>2^{\rho}2\tau(k+1)\ \Leftrightarrow$$

$$\Leftrightarrow\ 2^{\eta-1}/4>2^{\rho}2\tau(k+1)\Leftrightarrow\ 2^{\eta-1}/4-1/2>2\tau(k+1)2^{\rho}-1/2$$

한편 $2\tau(k+1)2^{\rho}-1/2>2\tau(k+1)(2^{\rho}-1)$이 성립되므로 우의 마지막부등식으로부터 부등식 $2^{\eta-1}/4-1/2>2\tau(k+1)(2^{\rho}-1)$이 나온다.

p_i가 η비트옹근수이고 $p_i>2^{\eta-1}$이므로 $2\tau(k+1)(2^{\rho}-1)<p_i/4-1/2$이 성립된다.

보조정리 1로부터 임의의 $i=1,\cdots,\ k$에 대하여 어떤 옹근수 Q_i와 조건 $|R_i|\le 2\tau(k+1)$ $|R_i|\le 2\tau(k+1)(2^{\rho}-1)$을 만족시키는 옹근수 R_i가 존재하여 $c=p_iQ_i+R_i+m_i[p_i/2]$이다.

$|R_i| \le 2\tau(k+1)(2^\rho - 1) < p_i/4 - 1/2$ 이므로 보조정리 2에 의하여 $\mathrm{Dec}(sk, c) = \boldsymbol{m}$ 이 성립된다.(증명끝)

보조정리 3[1] 분포 $\left\{ \left(x_1, \cdots, x_\tau, \left(\sum_{i=1}^{\tau} s_i x_i \right) \bmod x_0 \right) \middle| x'_1, \cdots, x'_\tau \leftarrow \boldsymbol{Z}_{x_0}, s_1, \cdots, s_\tau \leftarrow \{0, 1\} \right\}$

과 평등분포 $U(\boldsymbol{Z}_{x_0}^{\tau+1})$의 확률거리는 $\sqrt{x_0/2^\tau}/2$보다 작다.

정리 2(안전성정리) 론문의 공개열쇠암호체계는 $(\rho, \eta, \gamma) - k -$ AGCD판정문제를 풀기 힘들다는 가정밑에서 CPA 안전하다.

증명 $(\rho, \eta, \gamma) - k -$ AGCD판정문제를 풀기 힘들다는 기본가정으로부터 공개열쇠 pk와 $\boldsymbol{Z} \cap [0, 2^\gamma)$ 우에서 평등우연적으로 취하여 만든 거짓공개열쇠

$$pk' = \{\{x'_0, \cdots, x'_\tau\}, \{y'_1, \cdots, y'_k\}\}$$

는 계산구별불가능하다.

한편 가정 $\tau \ge \gamma + 2\lambda + 2$와 보조정리 3으로부터 분포

$$\left\{ \left(x'_1, \cdots, x'_\tau, \left(\sum_{i \in S} x'_i \right) \bmod x_0 \right) \middle| x'_1, \cdots, x'_\tau \leftarrow \boldsymbol{Z}_{x_0}, S \leftarrow 2^{\{1, \cdots, \tau\}} \right\}$$

와 평등분포 $U(\boldsymbol{Z}_{x_0}^{\tau+1})$사이의 확률거리는 $2^{-\lambda}$보다 작다.

따라서 분포 $\left\{ \left(\sum_{i \in S} x'_i \right) \bmod x_0 \middle| x'_1, \cdots, x'_\tau \leftarrow \boldsymbol{Z}_{x_0}, S \leftarrow 2^{\{1, \cdots, \tau\}} \right\}$와 평등분포 $U(\boldsymbol{Z} \cap [0, x_0))$의 확률거리도 $2^{-\lambda}$보다 작다. 이로부터 공격자가 실지 암호문과 평등우연적으로 선택된 우연수를 정확히 구별할 확률은 $2^{-\lambda}$보다 작다.(증명끝)

참 고 문 헌

[1] M. V. Dijk et al.; Fully Homomorphic Encryption over the Integers, Springer, 24～43, 2010.

[2] J. S. Coron et al.; Batch Fully Homomorphic Encryption over the Integers, Springer, 315～335, 2013.

[3] J. S. Coron et al.; Scale-Invariant Fully Homomorphic Encryption over the Integers, Springer, 311～328, 2014.

[4] D. J. Bernstein et al.; Post-Quantum Cryptography, Springer, 1～10, 2009.

주체107(2018)년 9월 8일 원고접수

A New Public-Key Cryptosystem Based on the AGCD Problem

Kwak Wi Song, Kim Chol Un

We present a new public-key cryptosystem over integers that its security is based on decisional AGCD problem. Our cryptosystem is tolerant of quantum attacks and has the advantage of existing cryptosystems that the length of cipher texts is short.

Key words: public-key cryptosystem, AGCD problem