김일성종합대학학보
(자연과학)
주체103(2014)년 제60권 제7호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 60 No. 7 JUCHE103(2014).

선형련립방정식에 기초한 한가지 검증가능한 비밀분배도식의 구성

김현정, 리철

위대한 령도자 **김정일**동지께서는 다음과 같이 지적하시였다.

《오늘 과학과 기술은 매우 빠른 속도로 발전하고있으며 사회발전에서 과학기술이 노는 역할은 더욱더 커지고있습니다. 현시대의 요구에 맞게 과학기술을 빨리 발전시켜야 우리의 자립적민족경제의 위력을 강화하고 사회주의건설을 더욱 다그칠수 있으며 사회주의의 우월성을 전면적으로 높이 발양시킬수 있습니다.》(《**김정일**선집》 제18권 증보판 441페지)

론문에서는 최근시기에 많이 연구되고있는 비밀분배리론에서 제기되는 한가지 새로운 비밀분배도식에 대하여 고찰하였다.

비밀분배문제는 콤퓨터망봉사체계의 보안을 비롯하여 여러가지 복잡하고 예민한 체계들의 보안을 위한 중요한 수단으로 리용되고있다.[1－4]

선행연구[1]에서는 비밀분배도식에서 접근구조가 론리턱값계층접근구조인 경우에 대수련립방정식을 리용하여 비밀분배를 실현하는 한가지 방법을 고찰하였으며 선행연구[2]에서는 론리턱값계층접근구조에 대한 검증가능한 비밀분배도식을 구성하였다.

비밀분배문제란 일반적으로 말하여 n명의 체계가입자들에게 체계의 비밀 d와 관련된 정보를 배포하되 가입자들의 허용된 부분모임은 그들이 가지고있는 정보를 종합하여 체계의 비밀 d를 회복할수 있도록 하는 문제를 말한다.

비밀분배도식의 중요한 요구조건은 정확성과 완전성을 보장하는것이다.

선행연구[2]에서는 접근구조를 $\Gamma=\{W\subset U:|W|\geq t\}$로 정의하고 그것에 기초하여 선형련립방정식에 기초한 비밀분배도식을 내놓았다. 여기서 $U=\{1, 2, \cdots, n\}$은 체계에서의 참가자들의 모임이고 t는 턱값이다.

관리자는 Z_n^t에서 벡토르 $x=(x_1, x_2, \cdots, x_t)$를 우연선택하되 $x_1=s$를 만족시키도록 한다. 그리고 n개의 t차원벡토르 $A_i=(a_{i1}, a_{i2}, \cdots, a_{it})\in Z_n^t$, $i=1, 2, \cdots, n$을 임의의 t개 벡토르들이 1차독립이 되도록 우연선택하고 $y_i=A_ix$, $i=1, 2, \cdots, n$을 참가자 i의 비밀분배몫으로 계산한다. 그리고 A_i는 공개하고 y_i는 비밀리에 보낸다.

U를 비밀을 회복하기 위하여 구성된 t명의 참가자들의 집단이라고 하자.

이제 A_U를 U에 속하는 참가자들이 가지고있는 A_i를 행으로 하는 t차행렬이라고 하고 Y_U는 U에 속하는 참가자들이 받은 비밀분배몫 y_i들로 이루어진 t차원렬벡토르라고 하면 이 집단은 선형련립방정식 $A_Ux=Y_U$를 풀어서 비밀 s를 계산할수 있다.

그런데 이 비밀분배도식에서는 참가자들의 허용된 부분모임에 속하는 매 참가자들이 다 정당하고 비밀분배단계에서 매 참가자가 비밀분배자로부터 받는 비밀분배몫 y_i가 정당하다는것을 전제로 하고있다.

그러나 일반적으로는 허용된 부분모임에 속하는 참가자라고 할지라도 정당치 못할수 있으며 비밀분배자가 배포한 비밀분배몫 y_i도 정당한것인지 아닌지 알수 없다고 가정한다.

따라서 비밀분배자가 배포한 y_i와 허용된 부분모임에 속하는 참가자들의 정당성을 확인할수 있는 비밀분배도식이 요구된다.

이러한 비밀분배도식을 검증가능한 비밀분배도식이라고 부른다.

선행연구[2]에서는 선행연구[1]에서 제기한 방법이 비밀분배자나 혹은 참가자들이 속임수를 쓰려고 하는것과 같은 공격을 막을수 없다는것을 밝히고 그것을 해결할수 있는 한가지 방도로서 검증가능한 비밀분배도식을 구성하였다.

그런데 선행연구[2]에서 제기한 도식은 비밀분배단계에서의 검증을 위해 필요한 파라메터설정의 요구조건이 매우 강하기때문에 계산량적으로 해결하기 힘든 난점이 있다.

론문에서는 선행연구[2]에서 제기한 비밀분배도식보다 안전성은 떨어지지 않으면서도 요구조건이 훨씬 단순한 한가지 검증가능한 비밀분배도식을 제기하였다.

론문에서 제기한 도식은 다음과 같다.

비밀분배단계 n명으로 이루어진 집단에 비밀 $s \in Z_n^t$를 분배하기 위하여 비밀분배자는 다음과 같이 한다.

① Z_n^t에서 벡토르 $x=(x_1, x_2, \cdots, x_t)$를 우연선택하되 $x_1 = s$가 되도록 한다.

그리고 1차독립인 n개의 t차원벡토르 $A_i=(a_{i1}, a_{i2}, \cdots, a_{it}) \in Z_n^t$, $i=1, 2, \cdots, n$을 우연선택하고 비밀분배몫 $y_i = A_i x$, $i=1, 2, \cdots, n$을 계산한다.

② 비밀분배자는 검증식 $h_i = g^{x_i} \bmod n$, $i=1, 2, \cdots, t$를 계산한다.

비밀분배자는 매 참가자 $i=1, 2, \cdots, n$에게 g와 n, h_i, $i=1, 2, \cdots, t$ 그리고 A_i, $i=1, 2, \cdots, n$을 공개하고 y_i, $i=1, 2, \cdots, n$은 비밀로 전송한다. 여기서 g는 Z_n^t의 두제곱원소들로 이루어진 위수가 $L(n)/2$인 순환군 Q_n의 생성원소의 두제곱수이다.

③ 참가자 $i=1, 2, \cdots, n$은 $g^{y_i} \equiv \prod_{j=1}^{t} h_j^{a_{ij}} (\bmod n)$을 검사하여 비밀분배자로부터 받은 비밀분배몫이 정당한가 혹은 정당하지 않은가를 확인한다.

비밀회복단계 U를 비밀을 회복하기 위하여 선택된 t명으로 이루어진 참가자들의 부분모임이라고 하자.

① 매 참가자 $u \in U$는 U에 속하는 다른 모든 참가자들의 비밀분배몫의 정당성을 $g^{y_i} = \prod_{j=1}^{t} h_j^{a_{ij}} (\bmod n)$, $i \in U$를 계산하여 확인한다.

② 부분모임 U에 속하는 모든 참가자들의 비밀분배몫이 정당하면 U에 속하는 참가자들의 비밀분배몫 y_i들에 의하여 련립방정식 $A_U x = Y_U$를 풀어서 비밀 s를 구한다.

정리 1 론문에서 제기한 비밀분배도식은 완전비밀분배도식이다.

증명 우선 t명으로 이루어진 참가자들의 부분모임은 비밀을 회복할수 있다는것을 보기로 하자.

련립방정식 $A_U x = Y_U$를 풀어서 다시 쓰면 다음과 같다.

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1t}x_t = y_1$$
$$a_{21}x_1 + a_{22}x_2 + \cdots + a_{2t}x_t = y_2$$
$$\vdots$$
$$a_{t1}x_1 + a_{t2}x_2 + \cdots + a_{tt}x_t = y_t$$

따라서 결수행렬 A_U가 불퇴화행렬이므로 풀이는 항상 유일존재한다.

한편 $t-1$명이하의 참가자들의 임의의 모임은 비밀을 회복할수 없다.

사실 참가자들의 인원수가 $t-h$라고 하면 우의 련립방정식에는 h개의 자유변수가 있게 되고 따라서 $x_i \in Z_n$이라는것을 고려하면 h개의 자유변수가 취할수 있는 값의 가능한 경우수는 C_n^h이다. 그만한 서로 다른 값들에 대응되는 풀이들중에서 $x_1 = s$인 풀이를 찾을 확률은 $1/C_n^h$을 넘지 않는다. 즉 $t-h$명의 참가자들이 비밀을 회복할 확률은 n이 큰 씨수인 경우 무시할수 있다.(증명끝)

론문에서 제기한 비밀분배도식의 정확성은 t명의 허용된 참가자들의 부분모임이 비밀을 회복하기 위하여 구성하는 련립방정식이 결수행렬이 불퇴화이기만 하면 유일한 풀이를 가진다는것을 고려하면 곧 나온다.

정리 2 비밀분배자와 참가자들이 정당하다면 비밀분배단계와 비밀회복단계에서 검증식들은 언제나 성립한다.

증명 비밀분배단계에서 분배자는 매 참가자 $i=1, 2, \cdots, n$에게 g와 n, h_i, $i=1, 2, \cdots, t$ 그리고 A_i, $i=1, 2, \cdots, n$을 공개하고 y_i, $i=1, 2, \cdots, n$은 비밀로 전송한다.

따라서 매 참가자 i는 $g^{y_i} \bmod n$을 계산할수 있다.

한편 $\prod_{j=1}^{t} h_j^{a_{ij}} \bmod n = \prod_{j=1}^{t} (g^{x_j})^{a_{ij}} \bmod n = \prod_{j=1}^{t} g^{a_{ij}x_j} \bmod n = g^{a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{it}x_t} \bmod n = g^{y_i} \bmod n$

이므로 비밀분배자와 참가자가 다 정당하면 검증식은 항상 성립되고 따라서 참가자 i는 자기의 비밀분배몫이 정당하다는것을 확인할수 있다.(증명끝)

정리 3 론문에서 제기한 비밀분배도식은 리산로그문제를 풀기 힘든 정도에서 안전하다.

증명 공격자는 단위시간동안에 $t-1$명이상의 참가자를 변질시킬수 없다고 가정한다.

그리고 공격자는 변질된 참가자들의 정보를 그대로 정확히 알수 있다고 가정한다.

이제 U를 $t-h$ $(h>0)$명의 참가자들로 이루어진 집단이라고 하자.

그리고 비밀분배자가 선택한 본래의 풀이를 x^*이라고 하자.

그러면 U에 속하는 참가자들에 의하여 구성되는 련립방정식

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1t}x_t = y_1$$
$$a_{21}x_1 + a_{22}x_2 + \cdots + a_{2t}x_t = y_2$$
$$\vdots$$
$$a_{t1}x_1 + a_{t2}x_2 + \cdots + a_{tt}x_t = y_{t-h}$$

을 리용하여 비밀을 알아내려고 할수 있다.

이 경우 성공할 확률은 정리 1에서 본바와 같이 $1/C_n^h$보다 클수 없고 따라서 n이 충분히 크면 무시할수 있다.

한편 공격자는 비밀분배단계의 둘째 단계에서 계산되여 공개되는 정보 $h_i = g^{x_i} \bmod n$, $i = 1, 2, \cdots, t$ 를 직접 리용하여 비밀을 알아내려고 할수 있다.

그런데 이것은 리산로그문제를 푸는것과 동등하다.

결국 론문에서 제기한 비밀분배도식은 리산로그문제를 푸는것이 곤난하다면 안전하다.(증명끝)

정의 비밀분배자에 의하여 배포된 비밀분배몫들에 대하여 적어도 t 명으로 이루어진 서로 다른 허용된 참가자들의 부분모임들이 서로 다른 비밀값을 회복한다면 그 비밀분배몫들은 모순된 비밀분배몫이라고 부른다.

이제 이 비밀분배도식에서 비밀분배자 혹은 참가자가 절대로 속임수를 쓸수 없다는것을 보기로 한다.

정리 4 비밀분배도식에서 비밀분배몫들이 모순된 비밀분배몫이라면 비밀분배단계의 검증식이 적어도 하나의 참가자 i 에 대하여 성립하지 않는다.

증명 변질된 비밀분배자는 비밀분배단계에서 식 $g^{y_i} \equiv \prod_{j=1}^{t} h_j^{a_{ij}} (\bmod n)$, $i = 1, 2, \cdots, n$ 이 만족되도록 속임수를 써야 한다.

한편 g, n 과 h_i, a_{ij}, $i, j = 1, 2, \cdots, t$ 들이 참가자전부에게 공개되므로 정당하지 못한 비밀분배자는 y_i, $i = 1, 2, \cdots, n$ 를 변경시키는 방법으로 속임수를 써야 한다.

비밀분배자가 y_i 를 y_i' 로 변경시켰다고 하면 련립방정식 $A_U x = Y_U$ 에서 i 째 방정식 $a_{i1}x_1' + a_{i2}x_2' + \cdots + a_{it}x_t' = y_i'$ 가 $a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{it}x_t \neq y_i'$ 로 되여 검증식이 만족되지 않는다.

또한 $x' = (x_1', x_2', \cdots, x_t') \in Z_n^t$ 를 적당히 택하여 $a_{i1}x_1' + a_{i2}x_2' + \cdots + a_{it}x_t' = y_i'$ 가 성립되도록 하고 y_i' 를 참가자 i 에게 보낼수도 있으나 h_i, $i = 1, 2, \cdots, n$ 들을 수정할수 없으므로 불가능하다.

따라서 제기한 비밀분배도식에서 관리자는 발견되지 않으면서 참가자들을 속이는것이 불가능하다.(증명끝)

이 정리는 비밀분배도식에서 비밀분배자가 변질되는 경우 발견되지 않고 절대로 속임수를 쓸수 없다는것을 보여준다.

정리 5 비밀분배도식의 비밀회복단계에서 주어진 비밀분배몫들이 모순된 비밀분배몫이라면 검증식이 성립되지 않는다.

증명 제기한 도식의 비밀회복단계에서 허용된 참가자들의 부분모임에 속하는 참가자 i 가 자기의 정당성을 그 부분모임에 속한 다른 참가자들에게 확인할 때 $y_i' \neq y_i = A_i x$ 인 y_i' 를 보낸다면 분명히 $g^{y_i} \equiv \prod_{j=1}^{t} h_j^{a_{ij}} (\bmod n)$ 은 $\prod_{j=1}^{t} h_j^{a_{ij}} \bmod n = g^{y_i} \bmod n$ 이기때문에 절대로 성립하지 않는다.(증명끝)

이 정리는 비밀분배도식에서 참가자가 변질되는 경우에도 발견되지 않고 절대로 참가자들을 속일수 없다는것을 보여준다.

참 고 문 헌

[1] A. A. Selcuk et al.; Cryptology ePrint Archive: Report 2010/403.
[2] Kamer Kaya et al.; Cryptology ePrint Archive: Report 2010/96.
[3] Yun Zhang et al.; Cryptology ePrint Archive: Report 2011/392.
[4] Ashish Choudhury; Cryptology ePrint Archive: Report 2011/330.

주체103(2014)년 3월 5일 원고접수

On the Construction of a Verifiable Secret Sharing Scheme based on System of Linear Equations

Kim Hyon Jong, Ri Chol

We suggest a new verifiable secret sharing scheme based on a system of linear equations and prove its completeness, verifiability and security.

Key word: secret sharing scheme