김일성종합대학학보 JOURNAL OF **KIM IL SUNG** UNIVERSITY
(자연과학) (NATURAL SCIENCE)
주체103(2014)년 제60권 제12호 Vol. 60 No. 12 JUCHE103(2014).

계층접근구조우에서의 검증가능한 비밀분배도식

김현정, 리철

론문에서는 정보보안분야에서 최근시기 연구되고있는 비밀분배리론에서 제기되는 한가지 새로운 비밀분배방법에 대하여 론의하였다.

비밀분배문제는 콤퓨터망봉사체계의 보안을 비롯하여 여러가지 복잡하고 예민한 체계들의 보안을 위한 중요한 수단으로 리용되고있다.[1－6]

선행연구[1]에서는 분리턱값접근구조인 경우에 대수련립방정식을 리용하여 비밀분배를 실현하는 한가지 방법을 제기하였고 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. 또한 선행연구[3]에서는 체계에 변질된 참가자가 t 명일 때 변질된 참가자들을 확증할수 있는 비밀분배도식을 구성하였다.

선행연구[4, 5]에서는 접근구조가 계층접근구조인 경우에 검증가능한 비밀분배도식을 제기하였다.

여기서는 접근구조가 계층구조인 경우에 한가지 검증가능한 비밀분배방법에 대하여 연구하였다.

비밀분배문제란 일반적으로 말하여 n 명의 체계가입자들에게 체계의 비밀 d 와 관련된 정보를 배포하되 가입자들의 허용된 부분모임은 그들이 가지고있는 정보를 종합하여 체계의 비밀 d 를 회복할수 있도록 하는 문제를 말한다.

U 를 참가자전부의 모임이라고 할 때 m 개의 부분모임 L_i, $1 \le i \le m$ 이 주어져서 $L_i \subset L_j$, $i < j$ 이고 $L_m = U$ 를 만족시키는 i 를 계층의 급이라고 하자.

이때 계층접근구조를 다음과 같이 정의한다.

$$\Gamma = \{W \subset U : |W \cap L_i| \ge t_i,\ \exists i,\ 1 \le i \le m\}$$

여기서 $0 < t_1 < t_2 < \cdots < t_{m-1} < t_m$ 은 급들의 턱값이다.

알고리듬은 다음과 같다.

비밀분배단계

① 비밀분배자는 $t_m - 1$ 차다항식 $f(x)$ 를 우연적으로 택한다.

이때 $f(0)$ 이 비밀이 되도록 한다.

$f(x)$ 의 결수들을 a_i, $0 \le i \le t_m - 1$ 로 표시하자.

② 비밀분배자는 매 계층급 i 에 대하여 $t_i - 1$ 차다항식을 $f_i(x) = \sum_{j=0}^{t_i - 1} a_j x^j$ 으로 선택한다.

그리고 임의의 참가자 $u \in L_i$ 에 대하여 x_u 를 선택하여 $y_u = f_i(x_u)$ 를 계산한다.

$g \in Z_p$를 Z_p의 생성원소라고 하자.

$h_j = g^{a_j} \bmod p$, $0 \le j \le t_m - 1$을 계산한다.

x_u, g, h_j, $1 \le j \le t_m - 1$들을 공개하고 y_u를 u의 비밀분배몫으로 하여 u에게 비밀로 보낸다.

③ 매 참가자 u는 검증식 $g^{y_u} \equiv \left(\prod_{j=0}^{t_i - 1} h_j^{x_u^j} \right) \bmod p$를 계산하여 비밀분배자로부터 받은 비밀분배몫 y_u가 정당한가하는것을 확인한다.

비밀결합단계

Q를 비밀을 회복하기 위하여 선택된 t_i명으로 이루어진 경기자들의 부분모임이라고 하자.

① 매 참가자 u는 U에 속하는 다른 모든 참가자들의 비밀분배몫의 정당성을 $g^{y_u} \equiv \left(\prod_{j=0}^{t_i - 1} h_j^{x_u^j} \right) \bmod p$, $u \in U$로 계산하여 확인한다.

② 부분모임 U에 속하는 모든 참가자들의 비밀분배몫이 정당하면 라그랑쥬보간법을 리용하여 다항식 $f(x)$를 계산하고 비밀 $f(0)$을 찾는다.

정의 1 다음과 같은 조건을 만족시키는 비밀분배도식을 완전비밀분배도식이라고 부른다.

i) 참가자들의 허용되지 않는 부분모임으로는 비밀에 대한 아무런 정보도 얻을수 없다.

ii) 참가자들의 허용된 부분모임으로는 비밀을 회복할수 있다.

정의 2 주어진 비밀분배도식에 대하여 비밀분배자와 참가자들이 다 정당하면 참가자들의 허용된 부분모임이 언제나 정확한 비밀을 회복할 때 그 비밀분배도식은 정확한 비밀분배도식이라고 부른다.

정리 1 론문에서 제기한 비밀분배도식은 완전비밀분배도식이다.

증명 우선 임의의 계층급 i, $1 \le i \le m$에 대하여 급이 i인 t_i명의 참가자들의 모임 Q는 비밀을 회복할수 있다는것을 보기로 하자.

그러면 i째 급에 대응되는 $t_i - 1$차다항식은 $f_i(x) = \sum_{j=0}^{t_i - 1} a_j x^j$이고 매 참가자 $u \in Q$에게는 비밀분배몫 $y_u = f_i(x_u)$가 배정되여있고 x_u는 공개한다.

따라서 Q로부터 t_i개의 표본 $(x_u,\ y_u)$가 얻어지며 라그랑쥬보간법에 의하여 다항식 $f_i(x) = \sum_{j=0}^{t_i - 1} a_j x^j$을 정확히 결정할수 있다는것은 이미 알려져있다.

한편 비밀분배단계에서 매 참가자들에게 x_u, g, h_j, $1 \le j \le t_m - 1$들을 공개하고 y_u는 u의 비밀분배몫으로 하여 u에게 비밀로 보낸다.

참가자 u는 검증식 $g^{y_u} \equiv \left(\prod_{j=0}^{t_i - 1} h_j^{x_u^j} \right) \bmod p$를 계산할수 있다.

한편 $\prod_{j=0}^{t_i-1} h_j^{x_u^j} = \prod_{j=0}^{t_i-1} (g^{a_j})^{x_u^j} = \prod_{j=0}^{t_i-1} g^{a_j x_u^j} = g^{y_u}$ 이므로 비밀분배자와 참가자들이 다 정당하면 검증식은 항상 성립되며 따라서 비밀은 정확히 회복된다.

다음으로 Q를 t_i보다 엄격히 작은 수의 참가자들로 이루어진 모임이라고 하자.

그러면 t_i보다 작은 개수의 보간마디점 (x_u, y_u)가 얻어지게 되며 이 경우에 라그랑쥬보간법에 의하여 주어진 t_i-1차다항식 $f_i(x)$를 일의적으로 결정하는것은 불가능한 문제로 된다는것이 알려져있다.(증명끝)

새로운 비밀분배도식의 정확성은 정리 1의 증명과정에 의하여 쉽게 알수 있다.

정리 2 론문에서 제기한 비밀분배도식의 안전성은 리산로그문제풀이의 곤난성에 귀착된다.

증명 비밀분배단계에서 매 참가자들은 자기의 비밀분배몫 y_u를 비밀분배자로부터 비밀통로를 통하여 전달받는다.

따라서 공격자는 보간마디점 (x_u, y_u)들에 대한 정보를 전혀 알수 없고 주어진 t_i-1차다항식 $f_i(x)$를 결정하는데 라그랑쥬보간법을 리용할수 없다.

한편 공격자는 $h_j = g^{a_j} \bmod p$, $0 \le j \le t_m - 1$들을 풀어서 t_i-1차다항식 $f_i(x)$의 결수 a_j, $0 \le j \le t_m - 1$들을 결정하려고 할수 있는데 그것은 h_j, p, g를 알고 a_j, $0 \le j \le t_m - 1$들을 구하여야 하므로 리산로그문제의 풀이에 귀착된다.(증명끝)

정의 3 비밀분배자에 의하여 배포된 비밀분배몫들에 대하여 적어도 t_i $(\forall i \in \{1, m\})$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 하자.

정리 3 비밀분배도식에서 비밀분배몫들이 모순된 비밀분배몫이라면 비밀분배단계의 검증식은 적어도 하나의 참가자 u에 대하여 성립되지 않는다.

증명 변질된 비밀분배자는 비밀분배단계에서 참가자들에게 검증식 $g^{y_u} \equiv \left(\prod_{j=0}^{t_i-1} h_j^{x_u^j}\right) \bmod p$가 만족되도록 속임수를 써야 한다.

한편 x_u, g, h_j, $1 \le j \le t_m - 1$들이 참가자전부에게 공개되므로 변질된 비밀분배자는 y_u를 변경시키는 방법으로 속임수를 써야 한다.

이제 비밀분배자가 y_u를 y'_u로 변경시켰다고 하자.

그러면 $f(x_u) = y_u$가 $f(x'_u) = y'_u$로 되여야 하는데 x_u는 공개되므로 $x_u = x'_u$가 성립되여야 한다.

따라서 변경된 y'_u에 대하여 검증식 $g^{y_u} \equiv \left(\prod_{j=0}^{t_i-1} h_j^{x_u^j}\right) \bmod p$가 성립되지 않는다.

결국 제기한 비밀분배도식에서 비밀분배자는 발견되지 않으면서 참가자들을 속이는것이 불가능하다.(증명끝)

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

정리 4 비밀분배도식의 비밀결합단계에서 주어진 비밀분배묶들이 모순된 비밀분배묶이라면 검증식이 성립하지 않는다.

증명 제기한 도식의 비밀결합단계에서 허용된 참가자들의 부분모임에 속하는 참가자 u가 자기의 정당성을 그 부분모임에 속한 다른 참가자들에게 확인시킬 때

$$y'_u \neq y_u = f_i(x_u)$$

인 y'_u를 보낸다면 분명히 검증식 $g^{y_u} \equiv \left(\prod_{j=0}^{t_i-1} h_j^{x_u^j}\right) \bmod p$는 $\left(\prod_{j=0}^{t_i-1} h_j^{x_u^j}\right) \bmod p = g^{y_u} \bmod p$이기때문에 절대로 성립되지 않는다.(증명끝)

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

참 고 문 헌

[1] A. A. Selcut et al.; Cryptology ePrint Archive: Report 2010/403.
[2] A. A. Selcut et al.; Cryptology ePrint Archive: Report 2010/96.
[3] Yun Zhang et al.; Cryptology ePrint Archive: Report 2011/392.
[4] A. Choudhury; Cryptology ePrint Archive: Report 2011/330.
[5] T. Tassa; Journal of Cryptology, 20, 2, 237, 2007.
[6] E. F. Brickell; LNCS, 434, 468, 1990.

주체103(2014)년 8월 5일 원고접수

Verifiable Secret Sharing Scheme over Hierarchical Access Structure

Kim Hyon Jong, Ri Chol

We investigate a verifiable secret sharing scheme over hierarchical access structure.

Firstly we propose a verifiable secret sharing scheme over threshold hierarchical access structure and then show its completeness, security and verifiability.

Key word: hierarchical access structure