The Transactions of the Korea Information Processing Society
TKIPS Vol.13, No.2, pp.34~40

eISSN: 3022-7011
https://doi.org/10.3745/TKIPS.2024.13.2.34

A Multi-Compartment Secret Sharing Method

Cheolhoon Choi† · Minsoo Ryu††

ABSTRACT

Secret sharing is a cryptographic technique that involves dividing a secret or a piece of sensitive information into multiple shares or parts, which can significantly increase the confidentiality of a secret. There has been a lot of research on secret sharing for different contexts or situations. Tassa's conjunctive secret sharing method employs polynomial derivatives to facilitate hierarchical secret sharing. However, the use of derivatives introduces several limitations in hierarchical secret sharing. Firstly, only a single group of participants can be created at each level due to the shares being generated from a sole derivative. Secondly, the method can only reconstruct a secret through conjunction, thereby restricting the specification of arbitrary secret reconstruction conditions. Thirdly, Birkhoff interpolation is required, adding complexity compared to the more accessible Lagrange interpolation used in polynomial-based secret sharing. This paper introduces the multi-compartment secret sharing method as a generalization of the conjunctive hierarchical secret sharing. Our proposed method first encrypts a secret using external groups' shares and then generates internal shares for each group by embedding the encrypted secret value in a polynomial. While the polynomial can be reconstructed with the internal shares, the polynomial just provides the encrypted secret, requiring external shares for decryption. This approach enables the creation of multiple participant groups at a single level. It supports the implementation of arbitrary secret reconstruction conditions, as well as conjunction. Furthermore, the use of polynomials allows the application of Lagrange interpolation.

Keywords : Hierarchical Secret Sharing, Lagrange Interpolation, Polynomial

다중 컴파트먼트 비밀공유 기법

최 철 훈† · 유 민 수††

요 약

비밀공유 기법은 개인키와 같은 비밀을 복수의 지분으로 분할하여 분산 관리함으로써 비밀의 보안성을 높이는 기술이다. 그동안 다양한 상황에서 비밀공유를 적용하기 위한 많은 연구가 있어 왔으며, Tassa가 제안한 논리곱 기반의 비밀공유 방법은 도함수를 사용하여 계층적 비밀공유를 가능하게 하는 방법이다. 하지만 도함수를 사용하는 계층적 비밀공유는 몇 가지 한계를 가진다. 첫째, 각 레벨의 지분들이 하나의 도함수로부터 생성되기 때문에 하나의 레벨에 하나의 참여자 그룹만을 만들 수 있다. 둘째, 논리곱에 기반한 비밀 복원만 가능하여 임의의 비밀 복원 조건을 규정할 수 없다. 셋째, 도함수를 사용하기 때문에 버크호프 보간법을 필요로 하며, 이는 다항식 기반 비밀공유에 사용되는 라그랑주 보간법에 비해 구현이 복잡하고 어렵다. 본 논문에서는 논리곱 기반 계층적 비밀공유를 일반화시킨 다중 컴파트먼트 비밀공유 기법을 제안한다. 제안하는 기법은 비밀을 복원하는데 필요한 외부지분들을 이용하여 비밀을 암호화하고, 암호화된 비밀 값이 삽입된 다항식을 생성하여 내부지분들을 생성한다. 내부지분들로 다항식을 복원할 수는 있지만, 이 때 얻을 수 있는 값은 암호화된 비밀 값이며 복호화를 위해서는 외부지분들이 필요하다. 이 기법을 적용하면 하나의 계층에 복수의 참여자 그룹을 만들 수 있으며, 논리곱은 물론 임의의 비밀 복원 조건을 구현할 수 있다. 또한 다항식을 사용함에 따라 라그랑주 보간법을 적용하는 것도 가능해진다.

키워드 : 계층적 비밀 공유, 라그랑주 보간법, 다항식

1. 서 론

블록체인은 분산원장 시스템(distributed system)으로 지갑의 개인키(private key)를 안전하게 보관하는 것은 매우 중요한 문제이다. 개인키를 안전하게 보관하는 다양한 방법이 있을 수 있는데, 비밀공유(secret sharing)는 개인키를 복수의

※ 이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00590, 대규모 노드에서 블록단위의 효율적인 거래 확정을 위한 최종성 보장 기술개발).
† 준 회 원 : 한양대학교 컴퓨터소프트웨어학과 석사과정
†† 정 회 원 : 한양대학교 컴퓨터공학부 교수
Manuscript Received : November 20, 2023
Accepted : December 15, 2023
* Corresponding Author : Minsoo Ryu(msryu@hanyang.ac.kr)

지분(share)으로 분할하여 분산시킴으로써 개인키의 기밀성(confidentiality)을 향상시키는데 가장 효과적인 방법으로 알려져 있다.

대표적인 비밀공유 기법인 (t, n) 임계 비밀공유(TSS, threshold secret sharing)는 비밀(secret) S로부터 n개의 지분(share)을 만들어 n명의 참여자에게 배정하고, 임계값 t보다 같거나 많은 임의의 참여자들의 지분으로 비밀 S를 복원(reconstruct)하는 방법을 말한다. 참여자들을 복수의 레벨(level)로 분할(partition)하여 비밀공유 시스템을 구성할 수도 있는데, 이를 계층적 비밀공유(hierarchical secret sharing 또는 multilevel secret sharing)라 한다. 계층적 비밀공유에서는 상위 계층의 지분을 하위 계층의 지분보다 중요하게(more powerful) 취급하며, 이는 다양한 시나리오(scenario)에서 비밀에 대한 접근을 제어할 때 유용하다.

Tassa가 제안한 논리곱 기반 계층적 비밀공유(conjunctive hierarchical secret sharing)[1]에서는 하위 계층에서 비밀을 복원하기 위해 반드시 상위 계층의 지분을 필요로 한다. 예를 들면, 부사장 2명의 지분으로 비밀을 복원할 수 있지만, 직원 3명의 지분으로는 비밀을 복원할 수 없다. 그러나, 만약 직원 3명의 지분에 부사장 1명의 지분이 추가된다면 비밀을 복원하는 것이 가능해진다. 이러한 논리곱 기반 계층적 비밀공유를 위해 Tassa는 다항식의 도함수(derivatives)를 사용하는데, 이는 몇 가지 제약(limitation)을 가진다. 첫째, 각 레벨의 지분들이 하나의 도함수로부터 생성되기 때문에 하나의 레벨에 하나의 참여자 그룹(compartment)만을 만들 수 있다. 둘째, 논리곱에 기반한 비밀 복원만 가능하여 임의의(arbitrary) 비밀 복원 조건을 규정(specify)할 수 없다. 셋째, 도함수를 사용하기 때문에 버크호프 보간법(birkhoff interpolation)을 필요로 하며, 이는 다항식 기반 비밀공유에 사용되는 라그랑주 보간법(lagrange interpolation)에 비해 구현이 복잡하고 어렵다[2, 3].

본 논문에서는 논리곱 기반 계층적 비밀공유를 일반화(generalize)시킨 새로운 비밀공유 방법을 제안한다. 기본적인 아이디어는 임의의 컴파트먼트에서 비밀을 복원하는데 필요한 외부 컴파트먼트들의 지분(external share)들을 이용하여 비밀을 암호화(encrypt)하고, 암호화된 비밀값이 삽입(encode)된 다항식을 생성하여 내부 컴파트먼트 지분(internal share)들을 생성하는 것이다. 즉, 내부지분들로 다항식을 복원할 수는 있지만, 이 때 얻을 수 있는 것은 암호화된 비밀(encrypted secret)이며 이를 복호화(decrypt)하려면 암호화에 사용되었던 외부지분들이 필요하다. 제안하는 방법을 적용하면 하나의 레벨에 복수의 컴파트먼트를 만들 수 있으며, 논리곱은 물론 임의의(arbitrary) 비밀 복원 조건을 구현할 수 있다. 또한 다항식을 사용함에 따라 라그랑주 보간법을 적용할 수 있다.

2. 관련 연구

Shamir[4]와 Blakley[5]는 임계 비밀공유(threshold secret sharing) 방법을 제안한 바 있다. Shamir's Secret Sharing은 비밀값으로 사용하는 상수항을 제외한 나머지 계수들을 랜덤하게 선택해서 (t-1)차 다항식을 결정하고, 이 다항식을 지나는 n개의 점들로부터 n개의 지분 V_1, V_2, ..., V_n을 결정한다. 지분을 정하는 구체적인 방법은 다양할 수 있다. 한 가지 방법은 n개의 점들의 x 좌표를 0이 아닌 1, 2, 3, ... n으로 정하고 지분을 해당 점의 y 좌표값으로 정하는 것이다. 만약 t개의 지분이 주어진다면 t개의 점들이 모두 결정되며, 이로부터 (t-1)차 다항식을 찾아내어 비밀값에 해당하는 상수항을 알아낼 수 있다. 이 때 t개의 점으로부터 (t-1)차 다항식을 구하는 것은 라그랑주 보간법을 이용하여 해결할 수 있다.

Shamir의 방법은 완전보안성(perfect security)을 제공한다. 완전보안성이란 (t-1)개 이하의 지분으로는 비밀 S에 대해 어떠한 정보도 알아낼 수 없다는 성질을 말한다. 다항식에 포함된 비밀은 점 (0, S)에 해당하는데, S' ≠ S인 임의의 점 (0, S')과 (t-1)개 지분으로 결정되는 (t-1)개의 점을 지나면서 원래의 다항식 f(x)와는 상이한 (t-1)차 다항식이 항상 존재한다. 즉, (t-1)개의 지분을 알고 비밀 S를 추측하는 것이나 하나의 지분도 모르고 비밀 S를 추측하는 것은 확률적으로 차이가 없으며, 이는 (t-1)개의 지분으로는 비밀 S에 대해 어떠한 정보도 유추해낼 수 없음을 의미한다.

Simmons는 기하학적 객체(geometrical objects)를 사용하는 컴파트먼티드 비밀공유(compartmented secret sharing) 방법과 논리합 기반 계층적 비밀공유(disjunctive hierarchical secret sharing) 방법을 발표란 바 있다[6].

컴파트먼티드 비밀공유는 참여자들을(participant) 복수의 컴파트먼트로 나누고, 비밀을 복원하기 위해서는 컴파트먼트별로 정해진 숫자 이상의 참여자 지분(share)이 필요한 방법이다. 예를 들어, 두 개의 부서 A와 B의 직원들이 비밀공유에 참여한다고 해보면 다음과 같다. 비밀을 복원하기 위해 A 부서에서는 2명 이상의 지분과 B 부서에서는 3명 이상의 지분이 반드시 필요하다면, 이는 A와 B를 컴파트먼트로 하는 비밀

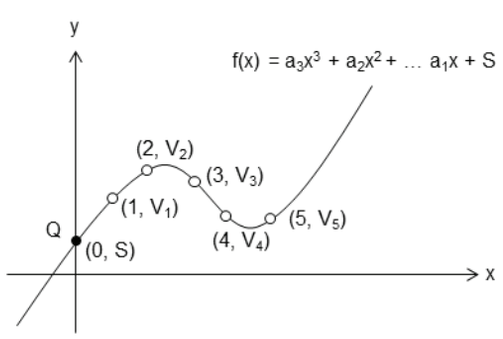

Fig. 1. Example of (4, 5) Secret Sharing Using 3-degree Polynomial

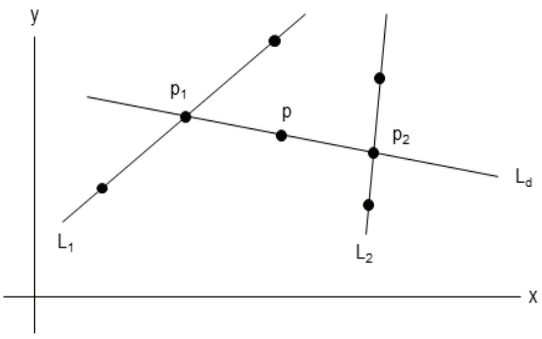

Fig. 2. Example of a Compartmented Secret Sharing Using Two Lines

공유로 볼 수 있다. Simmons는 기하학적 객체를 사용하여 컴파트먼티드 비밀공유 방법을 제안하였는데, Fig.2는 두 개의 직선을 사용하는 간단한 예를 보여준다. 비밀이 점 p에 존재한다고 하면 다음과 같다. 컴파트먼트 A에서는 2개의 점으로 직선 L_1을 결정하여 미리 알려진 직선 L_d와의 교점 p_1을 찾을 수 있다. 컴파트먼트 B에서도 2개의 점으로 직선 L_2를 결정하여 미리 알려진 직선 L_d와의 교점 p_2를 찾을 수 있다. 두 컴파트먼트에서 p_1과 p_2가 결정되면 p_1과 p_2의 중간점으로 정의되는 비밀을 나타내는 p를 찾을 수 있다.

논리합 기반 계층적 비밀공유는 참여자들을 복수의 레벨로 나눈다. 각 레벨별로 비밀을 복원하는 것이 가능한데, 상위 레벨의 지분으로 하위 레벨의 지분을 대신 사용하여 비밀을 복원하는 것도 가능하다. 예를 들어, 부사장 2명 또는 직원 3명의 지분으로 비밀을 복원할 수 있지만, 부사장의 지분이 직원의 지분을 대체하는 것도 가능하다. 즉, 직원 2명과 부사장 1명의 지분으로도 비밀을 복원할 수 있다. Fig.3은 하나의 직선과 하나의 평면을 이용하는 예를 보여준다. 비밀이 점 p에 존재한다고 해보면 다음과 같다. 컴파트먼트 A에서는 2개의 점으로 직선 L_1을 결정하여 미리 알려진 직선 L_d와의 교점 p를 찾을 수 있다. 컴파트먼트 B에서도 3개의 점으로 평면 P_2를 결정하여 미리 알려진 직선 L_d와의 교점 p를 찾을 수 있다. 만약, 컴파트먼트 A에 배정되는 점들이 평면 P_2에 존재한다면 이들은 컴파트먼트 B의 점 대신 평면 P_2를 찾는데 사용될 수 있다.

Tassa는 논리곱(conjunctive) 기반 계층적 비밀공유 방법을 발표하였다[1]. Tassa의 방법도 참여자들을 복수의 레벨로 나눈다는 점에서 논리합 기반 계층적 비밀공유[6]와 유사하나, 하위 레벨에서 비밀을 복원하려면 반드시 상위 레벨의 지분이 필요하다는 점에서 다르다. 예를 들면, 부사장 2명의 지분으로 비밀을 복원할 수 있지만, 직원 3명의 지분으로는 비밀을 복원할 수 없다. 그러나 직원 3명의 지분과 부사장 1명의 지분으로는 비밀을 복원할 수 있다. Tassa는 하위 레벨의 지분을 생성하기 위해 다항식의 도함수를 사용한다. 임의의 다항식에 대해 도함수의 계(order)가 증가할수록 다항식에 대한 정보가 줄어든다는 점을 이용한 것이다. 즉, 하위 레벨에서 지분들을 이용하여 도함수를 찾아낼 수 있지만, 이것으로는 비밀을 담고있는 상위 레벨의 다항식을 알아낼 수 없다. 따라서 상위레벨의 지분이 반드시 필요하다.

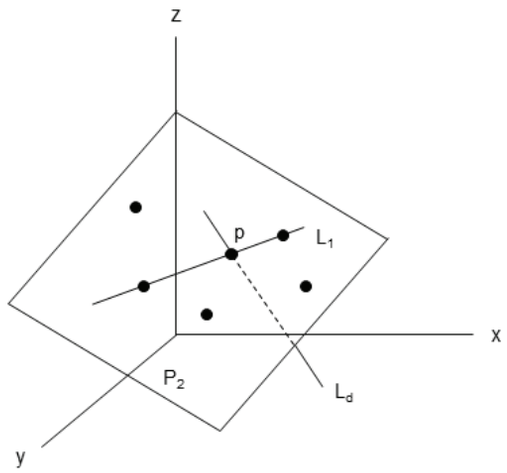

Fig. 3. Example of a Disjunctive Secret Sharing Using One Line and One Plane

최근에도 여러 방법을 사용한 계층적 비밀공유 기법 [8-12]은 꾸준히 연구되고 있다. [8]은 타원곡선(elliptic curve)으로 계층적 비밀공유 기법을 구현하였지만 타원곡선 공간상에서만 가능하다는 제약이 있다. [9]에서 제안한 CRT(Chinese Remainder Theorem)를 사용한 계층적 비밀공유 기법은 실용적인 특정 상황에서는 적용할 수 없다는 문제점[10]이 있다.

3. 비밀 공유와 액세스 구조

(t, n) 임계 비밀공유는 비밀 S로부터 n개의 지분을 만들어 n명의 참여자 $U_1, U_2, \ldots U_n$에게 배정하고, 임계값 t보다 같거나 많은 임의의 참여자들의 지분으로 비밀 S를 복원하는 방법을 말한다. 임계 비밀공유를 사용하면 지분들이 참여자들에게 분산되기 때문에 비밀 S의 기밀성(secrecy)이 높아진다. 공격자(adversary)는 t명에게 분산된 지분들을 탈취해야만 비밀을 알아낼 수 있기 때문이다. 또한 임계 비밀공유를 사용하면 비밀을 분실할 위험도 낮아진다. n개의 참여자 지분 중 일부를 유실하더라도 최소 t명의 지분만 확보할 수 있다면 비밀 S를 복원하는 것이 가능하기 때문이다. 일반적으로 (t, n) 비밀공유 방법은 2단계로 실행된다.

- 1단계(공유 단계, Sharing Phase): 총 n개의 지분을 생성하여 참여자(participant)들에게 배정(allocate)한다.
- 2단계(복원 단계, Reconstruction Phase): 임의의 t명의 지분을 취합하여 비밀 S를 복원(reconstruct)한다.

비밀공유에 참여하는 참여자들을 집합 $U = \{U_1, U_2, \ldots U_n\}$라 하고, 참여자 집합 U의 멱집합(power set) 2^U에서 비밀을

복원할 수 있는 부분집합들의 집합(collection)을 액세스 구조(access structure)로 정의한다. 이 정의에 따르면 (t, n) 비밀공유에서는 참여자들의 수가 t 이상인 부분집합들이 액세스 구조 A를 구성한다. 참여자들의 집합 U를 복수의 레벨로 분할하여 액세스 구조를 정의하면 계층적 비밀공유가 된다. 일반적으로 계층적 비밀공유에서는 상위 계층의 지분을 하위 계층의 지분보다 중요하게 취급하며, 이는 다양한 시나리오에서 비밀에 대한 접근을 제어할 때 유용하다.

Tassa가 제안한 논리곱 기반 계층적 비밀공유[1]에서는 하위 계층에서 비밀을 복원하기 위해 반드시 상위 계층의 지분을 필요로 한다. 예를 들면, 부사장 2명의 지분으로 비밀을 복원할 수 있지만, 직원 3명의 지분으로는 비밀을 복원할 수 없다. 그러나, 만약 직원 3명의 지분에 부사장 1명의 지분이 추가된다면 비밀을 복원하는 것이 가능해진다. 이러한 논리곱 기반 계층적 비밀공유를 위해 Tassa는 다항식의 도함수를 사용하여 하위 레벨의 지분을 생성한다. 도함수의 계가 증가할 때마다 정보가 손실된다는 점을 이용한 것이다. 즉, 하위 레벨에서 해당하는 도함수를 알아낼 수는 있지만, 상위 레벨의 도함수 또는 다항식은 알아낼 수 없다. 도함수를 이용하는 Tassa의 비밀공유 방법은 몇 가지 제약을 가진다. 첫째, 각 레벨의 지분들이 하나의 도함수로부터 생성되기 때문에 하나의 레벨에 하나의 참여자 그룹만을 만들 수 있다. 둘째, 논리곱에 기반한 액세스 구조만 가능하여 임의의 비밀 복원 조건을 규정할 수 없다. 셋째, 도함수를 사용하기 때문에 버크호프 보간법을 필요로 하며, 이는 다항식 기반 비밀공유에 사용되는 라그랑주 보간법에 비해 구현이 복잡하고 어렵다.

4. 다중 컴파트먼트 비밀공유

본 논문에서는 논리곱 기반 계층적 비밀공유를 일반화시킨 새로운 비밀공유 방법을 제안한다. 제안하는 방법을 적용하면 하나의 레벨에 복수의 컴파트먼트를 만들 수 있으며, 논리곱을 포함하여 임의의 액세스 구조를 구현할 수 있다. 또한 다항식을 사용하여 라그랑주 보간법을 적용하는 것도 가능해진다.

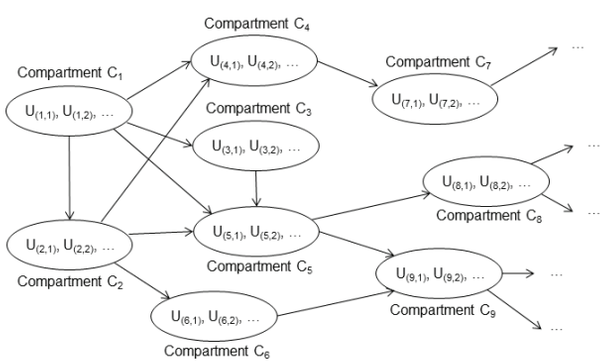

Fig. 4. Example of a Secret Sharing System Consisting of Multiple Compartments Represented by a Directed Graph

임의의 액세스 구조를 구현할 수 있는 제안하는 비밀공유 시스템은 Fig.4와 같이 유향 그래프(directed graph)로 표현될 수 있다. Fig.4에서 노드는 참여자들로 구성되는 컴파트먼트 C를 나타내며, 화살표는 컴파트먼트에서 비밀을 복원하는데 외부 컴파트먼트의 지분이 필요하다는 조건을 나타낸다. 예를 들면, Fig.4에서 컴파트먼트 C_4에서 비밀을 복원하기 위해서는 컴파트먼트 C_1과 C_2의 지분의 일부가 필요하다.

유향 그래프로 표현되는 제안하는 비밀공유 시스템에서 액세스 구조를 컴파트먼트별로 정의하자. 우선 컴파트먼트 C_i에 속하는 n_i명의 참여자 집합을 $U_i = \{U_{(i,\ 1)}, U_{(i,\ 2)}, \ldots, U_{(i,\ ni)}\}$라 하자. 컴파트먼트 C_i에서는 U_i에 속하는 t_i명의 내부지분 소유자(internal share holder)들과 다른 컴파트먼트에 속하는 외부지분 소유자(external share holder)들의 지분을 사용하여 비밀 S를 복원할 수 있다. 컴파트먼트 C_i에서 비밀을 복원하는데 필요로 하는 외부지분 소유자들의 집합을 $r_{i(\cdot)}$로 나타내고, 그러한 집합들이 m_i개 있다면 $R_i = \{r_{i(1)}, r_{i(2)}, \ldots r_{i(mi)}\}$로 나타내자. 즉, R_i의 원소 중 하나만 있으면 컴파트먼트 C_i의 t_i명의 내부지분 소유자들과 함께 비밀을 복원할 수 있다. 컴파트먼트 C_i에서 비밀을 복원할 수 있는 내부지분 소유자들과 외부지분 소유자들의 집합을 액세스 집합(access set)이라 하고, 액세스 집합들의 모음(collection)을 컴파트먼트 C_i의 액세스 구조 A_i라 하자. 컴파트먼트 C_i의 액세스 구조 A_i는 내부지분 소유자 집합 U_i의 멱집합(power set) 2^{Ui}와 외부지분 소유자들로 정의되는 R_i로 정의되며, $A_i = \{\alpha\colon \alpha = u \cup r, u \in 2^{Ui}, r \in R_i, |\alpha \cap U_i| \geq t_i\}$로 나타낼 수 있다.

제안하는 방법에서는 임의의 외부지분 소유자 집합을 액세스 구조에 포함시킬 수 있다. 논리곱은 물론 다양한 비밀 복원의 조건을 규정할 수 있다. 그러나 액세스 구조에서 외부지분으로 내부지분을 대신할 수는 없다. 이는 상위 계층의 지분으로 하위 계층의 지분을 대신할 수 있는 Simmons의 논리합 기반 계층적 비밀공유[6]와 다른 점이다.

본 논문의 기본적인 아이디어는 R_i의 외부지분들을 이용하여 비밀을 암호화하고, 암호화된 비밀값이 삽입된 다항식을 생성하여 내부지분들을 생성하는 것이다. 내부지분들로 다항식을 복원할 수는 있지만, 이 때 얻을 수 있는 것은 암호화된 비밀이며 이를 복호화하려면 암호화에 사용되었던 외부지분들이 필요하다.

제안하는 비밀공유 기법에서 사용될 수 있는 암호화 방법은 다양한데, 충분한 엔트로피(entropy)[7]를 보존하면서 COA(Ciphertext-Only Attack)에 저항적(resistant)인 암호화 방법을 사용하면 비밀에 대한 보안성을 보장할 수 있다. 일반적으로 다항식을 사용하는 비밀공유 방법에서는 랜덤하게 생성된 다항식을 사용하여 비밀에 대한 보안성을 보장한다. 반면에 본 논문에서는 암호화된 비밀값들로부터 다항식을 유도하기 때문에 암호화된 비밀값들이 충분한 엔트로피를 가지지 못한다면 비밀에 대한 보안성을 보장할 수 없다. 또한, 내부지분들로 다항식을 복원한 후에는 암호화된 비밀값들을 구할

수 있기 때문에 암호화 알고리즘이 COA에 저항적이어야 한다. 그렇지 않다면 내부지분들만으로도 비밀을 알아낼 가능성이 생긴다.

컴파트먼트 C_i의 외부지분 소유자 집합들의 모음 $R_i = \{r_{i(1)}, r_{i(2)}, \ldots r_{i(mi)}\}$로부터 얻을 수 있는 암호화 키(encryption key)들의 집합을 $K_i = \{K_{i(1)}, K_{i(2)}, \ldots K_{i(mi)}\}$로 나타내자. 각 $r_{i(k)}$의 외부지분들로부터 암호화 키 $K_{i(k)}$를 구하는 방법은 미리 알려져 있다고 가정한다. 이제 컴파트먼트 C_i를 위한 비밀공유 기법을 설명하도록 한다. 아래의 설명에서 컴파트먼트 C_i에 속하는 참여자 $U_{(i,\ j)}$에게 배정될 지분을 $V_{(i,\ j)}$라 하고, 그러한 지분들의 집합을 $V_i = \{V_{(i,\ 1)}, V_{(i,\ 2)}, \ldots, V_{(i,\ ni)}\}$로 나타내도록 한다.

4.1 공유 단계

비밀 S와 R_i가 주어지면, R_i로부터 K_i를 먼저 구한 후 (t_i, n_i) 비밀공유를 위한 n_i개의 내부지분들을 생성한다. 설명의 편의상 t_i, n_i, m_i의 아래 첨자(subscript)는 생략하여 단지 t, n, m으로 나타내도록 한다.

1) $n \geq t \geq m$을 만족하는 t와 n을 선택한 후, 암호화 알고리즘 $E(key, plaintext)$를 이용하여 비밀 S를 암호화한 값을 좌표로 가지는 m개의 점 $(n+1, E(K_{i(1)}, S))$, $(n+2, E(K_{i(2)}, S))$, ... $(n+m, E(K_{i(m)}, S))$을 생성한다.
2) 생성된 m개의 점들을 지나면서 랜덤하게 선택된 계수 $a_{t-1}, a_{t-2}, \ldots, a_m$을 가지는 (t-1)차 다항식 $f_i(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \ldots a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \ldots a_0$를 생성한다.
3) 다항식 $f_i(x)$를 지나는 점 $(1, f_i(1))$, $(2, f_i(2))$, ... $(n, f_i(n))$으로부터 n개의 내부지분 $V_{(i,\ 1)} = f_i(1)$, $V_{(i,\ 2)} = f_i(2)$, ... $V_{(i,\ n)} = f_i(n)$을 생성하여 C_i의 참여자들 $U_{(i,\ 1)}, U_{(i,\ 2)}, \ldots, U_{(i,\ ni)}$에게 배정한다.

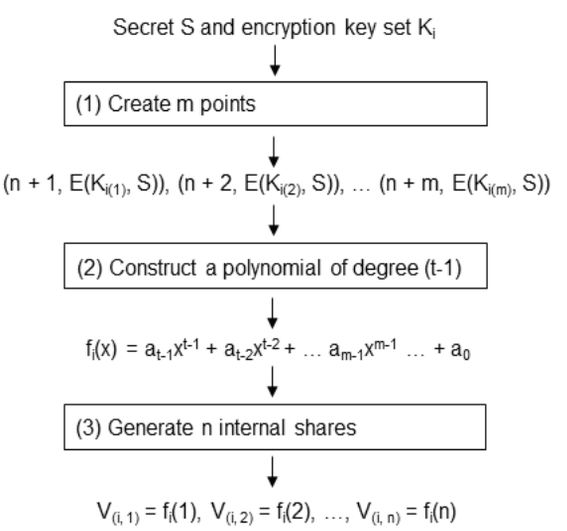

Fig. 5. Sharing Phase for Multi-compartment Secret Sharing

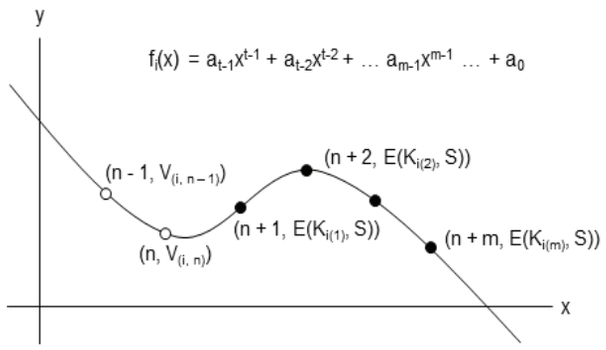

Fig. 6. Points and Coordinates in the Sharing Phase for Multi-compartment Secret Sharing

4.2 복원 단계

외부지분 소유자 집합 $r_{i(k)}$를 포함하는 액세스 집합 $\alpha \in A_i$를 이용하여 아래의 순서에 따라 비밀을 복원한다.

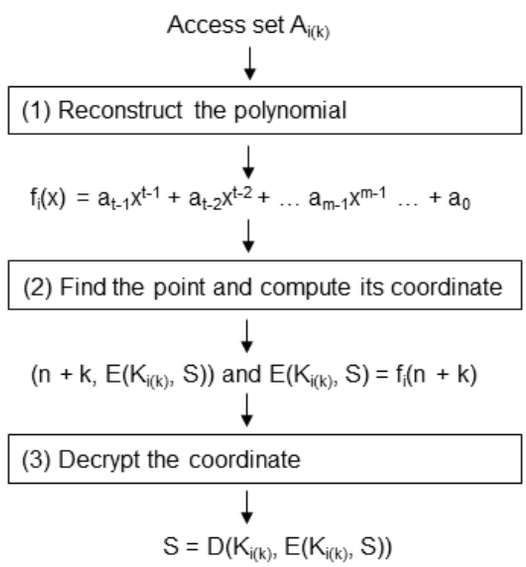

Fig. 7. Reconstruction Phase for Multi-compartment Secret Sharing

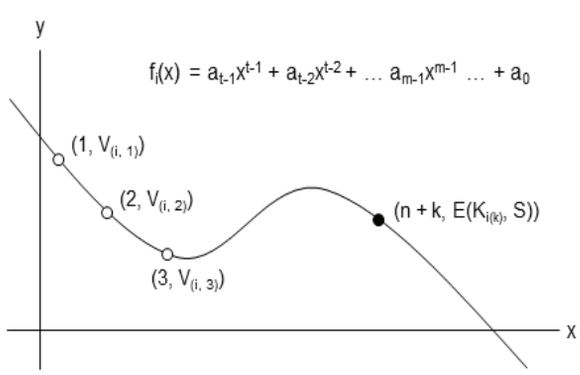

Fig. 8. Points and Coordinates in the Reconstruction Phase for Multi-compartment Secret Sharing

1) 액세스 집합 α에 속하는 t개의 내부지분으로 (t-1)차 다항식 $f_i(x)$를 복원한다.
2) 복원된 다항식 $f_i(x)$가 지나는 점 중에서 x축 좌표값이 n + k인 점의 y축 좌표값을 계산하여 암호화된 비밀값 $E(K_{i(k)}, S)$를 알아낸다. $E(K_{i(k)}, S) = f_i(n + k)$이므로 $f_i(n + k)$를 계산하면 된다.
3) $r_{i(k)}$로부터 복호화에 필요한 키 $K_{i(k)}$를 구하고, 복호화 알고리즘 D(*key*, *ciphertext*)를 이용하여 비밀 S를 복원한다. 즉, $S = D(K_{i(k)}, E(K_{i(k)}, S))$로 구할 수 있다.

4.3 적용 예시

제안하는 기법을 유한체(finite field) F_q상에서의 Shamir 비밀공유에 적용해보자. 유한체(finite field) F_q는 q로 나눈 나머지 값으로 정의되는데, 계산의 편의상 q의 값으로 소수(prime) 19를 가정한다. 이에 따라 비밀공유에 사용되는 비밀 S, 계수 a_i, 좌표값, 지분들은 모두 F_{19}에서 정의된다.

3개의 컴파트먼트로 구성되는 비밀공유 시스템을 예로 들면 유향 그래프를 Fig.9와 같이 나타낼 수 있다. 컴파트먼트 C_1에는 2개의 지분 $V_1 = \{V_{(1,\ 1)}, V_{(1,\ 2)}\}$, 컴파트먼트 C_2에는 4개의 지분 $V_2 = \{V_{(2,\ 1)}, V_{(2,\ 2)}, V_{(2,\ 3)}, V_{(2,\ 4)}\}$이 이미 배정되어 있고, 컴파트먼트 C_3에는 아직 지분이 배정되어 있지 않은 상태이다. 컴파트먼트 C_3에 대해 2개 이상의 내부지분과 외부지분 $\{V_{(1,\ 2)}, V_{(2,\ 4)}\}$으로 비밀 S를 복원할 수 있도록 3개의 내부지분을 만든다.

비밀 S = 8이라 하고, 비밀복원에 필요한 외부지분 집합 $\{V_{(1,\ 2)}, V_{(2,\ 4)}\}$으로 얻을 수 있는 키(key) $K_{3(1)}$로 비밀을 암호화하면 $E(K_{3(1)}, S) = E(K_{3(1)}, 8) = 7$을 얻을 수 있다고 가정한다. 제안하는 기법을 적용하는 예는 아래와 같다.

1) 공유 단계

a) $m_3 = 1$이고 $n_3 = 3$이므로 암호화 알고리즘 E( )를 이용하여 비밀 S를 암호화한 값을 좌표로 가지는 1개의 점 $(n_3+1, E(K_{3(1)}, S))$, 즉 (4, 7)을 먼저 생성한다.

b) $t_3 = 2$이므로 생성된 점 (4, 7)을 지나면서 랜덤하게 선택된 계수 $a_1 = 3$을 가지는 1차 다항식 $f_3(x) = a_1x + a_0 = 3x + 14$을 생성한다.

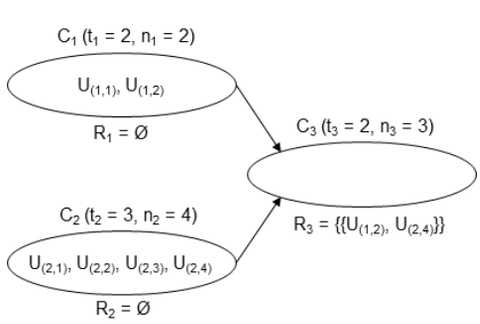

Fig. 9. Example of a Secret Sharing System with Three Compartments

c) $n_3 = 3$이므로 다항식 $f_3(x)$를 지나는 3개의 점 (1, $f_3(1)$), (2, $f_3(2)$), (3, $f_3(3)$)으로부터 3개의 내부지분 $V_{(3,\ 1)} = f_3(1) = 17$, $V_{(3,\ 2)} = f_3(2) = 1$, $V_{(3,\ 3)} = f_3(3) = 4$를 생성하여 C_3의 참여자들에게 배정한다.

2) 복원 단계

2개의 내부지분 $V_{(3,\ 2)}$, $V_{(3,\ 3)}$과 하나의 외부지분 집합 $\{V_{(1,\ 2)}, V_{(2,\ 4)}\}$를 가지고 비밀을 복원해보자.

a) 먼저 2개의 내부지분 $V_{(3,\ 2)} = 1$, $V_{(3,\ 3)} = 4$를 사용하여 라그랑주 보간법을 적용하면 $f_3(x) = 3x + 14$를 얻을 수 있다.

b) 암호화된 비밀은 점 $(n_3+1, E(K_{3(1)}, S))$의 y축 좌표값이고, $n_3 = 3$이므로 $E(K_{3(1)}, S) = f_3(4) = 7$을 얻을 수 있다.

c) $S = D(K_{3(1)}, E(K_{3(1)}, S))$이므로, 외부지분 집합 $\{V_{(1,\ 2)}, V_{(2,\ 4)}\}$으로부터 $K_{3(1)}$을 계산하여 $S = D(K_{3(1)}, 7) = 8$임을 알아낼 수 있다.

5. 결 론

본 논문에서 제안하는 다중 컴파트먼트 비밀공유 기법은 Tassa의 논리곱 기반 계층적 비밀공유 방법을 일반화한 것으로 세 가지 장점을 제공한다.

첫째, 다양한 계층적 비밀공유 시스템을 구성할 수 있다. 특히, 하나의 레벨에 복수의 컴파트먼트를 만드는 것이 가능해진다. 유향 비순환 그래프(directed acyclic graph)로 표현된 Fig.4의 비밀공유 시스템을 위상정렬(topological sorting)을 이용하여 다시 그리면 Fig.10의 계층적 구조가 된다. Fig.10에서 볼 수 있듯이, 하나의 레벨에 여러 개의 컴파트먼트가 존재할 수 있으며, 또한 레벨의 개수에도 제한이 없다. 참고로, 도함수를 사용하는 Tassa의 방법에서는 하나의 레벨에 하나의 컴파트먼트만 존재하며, 최초 다항식의 차수(degree)에 의해 레벨의 개수도 제한된다.

둘째, 임의의 액세스 구조를 정의할 수 있다. 각 컴파트먼트에서 비밀을 복원할 수 있는 조건으로 논리곱(conjunction)은 물론 임의의 외부지분들을 이용하여 액세스 구조를 지정할 수 있다.

셋째, 다항식에 기반하고 있어 라그랑주 보간법을 사용할 수 있다. 라그랑주 보간법은 도함수를 사용할 때 필요한 버크호프 보간법에 비해 덜 복잡하고 구현이 용이하다.

본 논문에서 제안하는 기법을 사용하면 기존의 계층적 비밀공유 시스템보다 더 다양한 시나리오에 적용할 수 있을 것으로 기대된다. 특히, 블록체인 지갑을 사용하는 개인 또는 기업에서는 다양한 조직 구성에 맞게 키를 안전하게 분산저장 및 복원할 수 있게 된다. 블록체인에서의 개인키 보관 및 복원은 물론 그 외의 다양한 분야에서도 활용될 수 있을 것으로 기대된다.

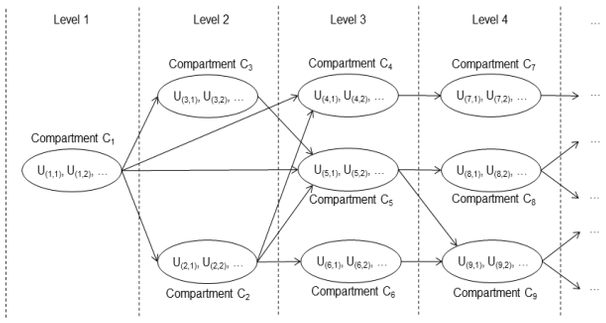

Fig. 10. Example of a Secret Sharing System that Transforms a Directed Graph Structure into a Hierarchical Structure

References

[1] T. Tassa, "Hierarchical threshold secret sharing," *Theory of Cryptography Conference*, Springer, 2004.

[2] H. Ghodosi, J. Pieprzyk, and R. Safavi-Naini, "Secret sharing in multilevel and compartmented groups," *Information Security and Privacy: Third Australasian Conference*, ACISP'98 Brisbane, Australia, July 13-15, 1998 Proceedings 3, Springer, 1998.

[3] T. Tassa and N. Dyn, "Multipartite secret sharing by bivariate interpolation," *Journal of Cryptology*, Vol.22, pp.227-258, 2009.

[4] A. Shamir, "How to share a secret," *Communications of the ACM*, Vol.22, No.11, pp.612-613, 1979.

[5] G. R. Blakley, "Safeguarding cryptographic keys," *Managing Requirements Knowledge, International Workshop on*, IEEE Computer Society, 1979.

[6] G. J. Simmons, "How to (really) share a secret," *Conference on the Theory and Application of Cryptography*, Springer, 1988.

[7] C. Cachin, "Entropy measures and unconditional security in cryptography," ETH Zurich, 1997.

[8] M. Chintamani, P. Paul, and L. Sa, "Conjunctive hierarchical multi-secret sharing scheme using elliptic curves," *Indian Journal of Pure and Applied Mathematics*, pp.1-9, 2023.

[9] L. Harn and M. Fuyou, "Multilevel threshold secret sharing based on the Chinese Remainder Theorem," *Information Processing Letters*, Vol.114, No.9, pp.504-509, 2014.

[10] O. Ersoy, K. A. Y. A. Kamer, and K. Kaskaloglu, "Multilevel threshold secret sharing based on the Chinese remainder theorem," International Journal of Information Security Science, Vol.8, No.2, pp.17-29, 2019.

[11] A. N. Tentu, P. Paul, and C. V. Vadlamudi, "Conjunctive hierarchical secret sharing scheme based on MDS codes," *Combinatorial Algorithms: 24th International Workshop*, IWOCA 2013, Rouen, France, July 10-12, 2013, Revised Selected Papers 24, Springer, 2013.

[12] J, Yuan, J. Yang, C. Wang, X. Jia, F. W. Fu and G. Xu, "A new efficient hierarchical multi-secret sharing scheme based on linear homogeneous recurrence relations," *Information Sciences*, Vol.592, pp.36-49, 2022.

최 철 훈

https://orcid.org/0009-0004-5551-8306
e-mail : chchoi726@hanyang.ac.kr
2023년 한양대학교 컴퓨터소프트웨어학부 (학사)
2023년~현 재 한양대학교 컴퓨터소프트웨어학과 석사과정
관심분야 : Operating Systems, Blockchain

유 민 수

https://orcid.org/0000-0002-4137-3052
e-mail : msryu@hanyang.ac.kr
1995년 서울대학교 제어계측공학과(학사)
1997년 서울대학교 전기공학부(석사)
2002년 서울대학교 전기공학부(박사)
1999년 ~ 2001년 Inus Technology 연구원
2001년 ~ 2002년 서울대학교 자동화시스템연구소 연구원
2003년 ~ 현 재 한양대학교 컴퓨터공학부 교수
관심분야 : Operating Systems, Real-Time Systems, Software Engineering, Blockchain