KIPS Trans. Comp. and Comm. Sys.
Vol.13, No.1 pp.31~37
https://doi.org/10.3745/KTCCS.2024.13.1.31
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

A Share Hardening Method for Multi-Factor Secret Sharing

Sung Wook Chung† · Min Soo Ryu††

ABSTRACT

Conventional secret sharing techniques often derive shares from randomly generated polynomials or planes, resulting in lengthy and complex shares that are challenging to memorize and/or manage without the aid of a separate computer or specialized device. Modifying existing secret sharing methods to use a predetermined value, such as a memorizable password or bio-metric information, offers a solution. However, this approach raises concerns about security, especially when the predetermined value lacks randomness or has low entropy. In such cases, adversaries may deduce a secret S with just (t - 1) shares by guessing the predetermined value or employing brute force attacks. In this paper, we introduce a share hardening method designed to ensure the security of secret sharing while enabling the use of memorizable passwords or biometric information as predetermined shares.

Keywords : Security, Secret Sharing, Share, Hardening

다중-요소 비밀 공유를 위한 지분 강화 기법

정 성 욱† · 유 민 수††

요 약

기존의 비밀 공유방법들은 무작위적으로 생성된 다항식(polynomial) 또는 평면(plane)으로부터 지분을 유도하기 때문에 복잡하고 긴(complex and long) 형태의 지분을 생성한다. 그렇게 생성된 지분은 암기(not memorizable)가 불가능하고 관리가 어려우며, 이에 따라 지분을 보관하고 관리하기 위해 컴퓨터 시스템 또는 별도의 디지털 장치가 있어야 한다. 전통적인 비밀 공유방법을 변형하면 패스워드나 생체정보와 같이 사용자가 미리 선택한 값을 지분으로 설정하는 것이 가능할 수 있다. 그러나 이러한 방법은 사용자가 선택한 값의 무작위성(randomness) 또는 엔트로피(entropy)가 낮으면 완전 보안성을 보장하지 못할 수 있다. 즉, (t-1) 개 이하의 지분으로 비밀을 유추해내는 것이 가능해질 수 있다. 본 연구에서는 암기가 가능한 패스워드나 지문과 같은 생체정보와 같이 미리 지정된 값을 지분으로 사용하면서 비밀 공유의 보안성을 보장할 수 있는 지분 강화(share hardening) 방법을 제안한다.

키워드 : 보안, 비밀 공유, 지분, 강화

1. 서 론

1979년 Shamir는 비밀 보관의 보안성을 높이기 위해 임계 비밀 공유방법을 제안한 바 있다[1]. Shamir의 (t, n) 비밀 공유방법은 비밀 값으로 사용하는 상수항을 제외한 나머지 계수들을 랜덤하게 선택해서 $(t-1)$차 다항식을 결정하고, 이 다항식을 지나는 n개의 점으로부터 n개의 지분(share) $v_1, v_2, \ldots, v_n$을 결정한다. 지분을 정하는 구체적인 방법은 다양할 수 있다. 한 가지 방법은 n개의 점의 x 좌표를 0이 아닌 $1, 2, 3, \ldots, n$ 으로 정하고 해당 점들의 y 좌푯값을 지분으로 정하는 것이다. 만약 t개의 지분을 안다면 t개의 점을 알아낼 수 있으며, 이로부터 $(t-1)$차 다항식을 찾아내어 비밀 값에 해당하는 상수항을 알아낼 수 있다. t개의 점으로부터 $(t-1)$차 다항식을 구하는 것은 라그랑즈 보간법(Lagrange interpolation)을 이용하여 해결할 수 있다.

Shamir의 방법은 완전 보안성(perfect security)을 제공한다[2, 3]. 완전 보안성이란 $(t-1)$개 이하의 지분으로는 비밀 S에 대해 어떠한 정보도 알아낼 수 없다는 성질을 말한다. 다항식에 포함된 비밀은 점 $(0, S)$에 해당하는데, $S' \neq S$인 임의의 점$(0, S')$과 $(t-1)$개 지분으로 결정되는 $(t-1)$개의 점을 지나면서 원래의 다항식 $f(x)$와는 다른 $(t-1)$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.

※ 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 컴퓨터공학부 박사과정
†† 비 회 원 : 한양대학교 컴퓨터공학부 교수
Manuscript Received : November 20, 2023
Accepted : January 3, 2024
* Corresponding Author : Min Soo Ryu(msryu@hanyang.ac.kr)

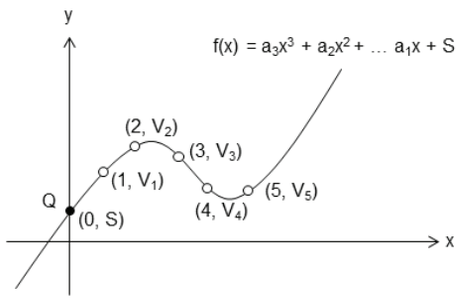

Fig. 1. Example of (4, 5) Threshold Secret Sharing Using Cubic Polynomials

기존의 비밀 공유방법은 다항식(polynomial)을 먼저 결정한 후 이로부터 지분을 유도하기 때문에 복잡하고 긴(complex and long) 형태의 지분을 생성한다[6]. 사용자 관점에서 그러한 지분은 암기(not memorizable)가 불가능하고 관리가 어려우며, 따라서 지분을 보관하고 관리하기 위해 별도의 컴퓨터 시스템 또는 디지털 장치를 사용해야 한다[7]. 전통적인 비밀 공유방법을 약간 변형하면 패스워드나 생체정보와 같이 사용자가 미리 선택한 값을 지분으로 설정하는 것이 가능할 수 있다. 그러나 이러한 방법은 사용자가 선택한 값의 무작위성(randomness) 또는 엔트로피(entropy)가 낮으면 완전 보안성을 보장하지 못할 수 있다. 즉, $(t-1)$개 이하의 지분으로 비밀을 유추해내는 것이 가능해질 수 있다.

본 논문에서는 비밀 공유방법의 사용 편의성(usability)을 개선하면서 다중-요소 인증(multi-facto authentication)을 가능하게 하는 지분 강화(share hardening) 기법을 제안한다. 제안하는 기법은 패스워드나 생체정보와 같이 사용자가 미리 선택한 값을 지정 지분(predetermined share)으로 사용하며, 추가로 강화지분(hardening share)의 개념을 도입하여 지정 지분의 보안성(security)을 보완한다. 지정지분과 강화지분이 결합할 때만 비밀 복원(secret reconstruction)에 사용될 수 있는 온전한 지분(full share)을 얻을 수 있다. 따라서 지정 지분의 보안성이 낮더라도 보안성이 높은 강화지분을 사용하면 나머지 $(t-1)$개의 지분으로는 비밀을 유추해내는 것이 불가능해진다. 이는 패스워드와 같은 사용자의 지식(knowledge), 생체정보와 같은 사용자의 고유성(inherence) 등을 지분으로 사용하는 다중-요소 비밀 공유(Multi-Factor Secret Sharing)를 가능하게 한다.

제안하는 지분 강화 기법은 기하학적 점(point)의 좌푯값(coordinates)을 지정지분과 강화지분으로 사용하기 때문에 기하학적 성질에 기반한 대부분의 비밀 공유방법에 적용할 수 있다. 예를 들면, 다항식을 사용하는 Shamir의 방법은 물론 Blakely의 비밀 공유방법에도[8] 적용할 수 있다.

2. 지정지분과 강화지분

Shamir 방법에서는 다항식을 먼저 랜덤하게(random) 결정하고 지분을 생성하는데, 이와 달리 미리 지정된 값을 지분으로 먼저 정하고 이로부터 다항식을 결정할 수 있다. 예를 들면, 미리 지정된 값을 p라 하면 y축 좌푯값이 p인 점 (k,p)를 먼저 정하고, 이 점을 지나도록 다항식의 계수(coefficient)를 정하는 것이다. 하지만 이러한 방법은 p가 무작위적이지 않거나 엔트로피가 낮으면 문제가 될 수 있다. 공격자가 $(t-1)$개 지분만으로도 p에 대한 추측(guessing) 또는 무차별 대입 공격(brute force attack) 등을 통해 비밀 S를 유추해내는(deduce) 것이 가능할 수 있기 때문이다.

Table 1. Terms Related to Share

Full share	Complete share for secret key computation or recovery.
Partial share	Complete when combined with other partial shares.
Aggregate share	A collection of partial shares that, when combined, function as a single complete share.
Predetermined share	User-specified arbitrary strings such as passcodes or biometric features.
Hardening share	A partial share can be combined with a predetermined share to create an aggregate share, compensating for any randomness in the predetermined share.

이러한 문제를 해결하기 위해 본 연구에서는 미리 선택된 지정 지분에 무작위성과 충분한 엔트로피를 가지는 하나 이상의 강화지분을 결합(bind)하는 방법을 제안한다.

지정지분 p에 결합하는 m개의 강화지분을 $h_1, h_2, \ldots, h_m$으로 나타내고, 기존의 비밀 공유에서 생성되는 지분(share)과 구분하기 위해 지정지분과 강화지분을 부분 지분(partial share)이라 하자. 기존의 방법으로 생성되는 지분은 완전 지분이라 부르고, 지정지분 p와 m개의 강화지분을 모두 취합하여 얻을 수 있는 정보를 취합 지분(aggregate share)이라 부르자. 본 논문에서는 지정 지분의 개수에 제한을 두지 않지만, 설명의 편의상 하나의 지정 지분에 m개의 강화지분이 결합하는 경우만 고려한다. 이를 $(t,(m),n)$ 비밀 공유방법이라 하자. 만약 하나의 지정 지분을 사용하되 강화지분은 하나도 사용하지 않는다면 이를 특별히 $(t,(0),n)$ 비밀 공유로 표현하여 기존의 (t,n) 비밀 공유와 구분하도록 하자.

$(t,(m),n)$ 비밀 공유방법에 사용되는 부분 지분은 다음과 같은 두 가지 조건을 만족하도록 정의된다. 첫째, 지정지분과 m개의 강화지분이 모두 취합되면 완전 지분과 동등한 정보(equivalent information)를 얻을 수 있어야 한다. 이는 비밀의 복원(reconstruction)에 필요한 성질이며, 지정지분과 강화지분이 모두 취합되면 다른 $(t-1)$개의 완전 지분과 함께 비밀 S를 알아낼 수 있음을 의미한다. 둘째, $(m-1)$개의 강화지분으로는 취합 지분에 대해 어떠한 정보도 알아낼 수 없어야 한다. 이는 취합 지분의 기밀성(secrecy)을 유지하는데 필

요한 성질이다. 이론적으로는, $(m-1)$개의 강화지분을 알고 취합 지분을 알아낼 확률과 강화지분을 하나도 모르고 취합 지분을 알아낼 확률이 같을 때 두 번째 조건을 만족한다고 볼 수 있다.

위의 두 번째 조건을 만족하는 강화지분을 완전 보안성(perfect security)을 제공하는 (t,n) 비밀 공유방법에 적용한다면 $(t-1)$개의 완전 지분과 $(m-1)$개의 강화지분으로는 비밀 S에 대해 어떠한 정보도 알아낼 수 없다. 완전 보안성에 의해 $(m-1)$개의 강화지분은 취합 지분을 알아내는 데 어떠한 도움이 되지 않으며, 따라서 비밀을 알아내는 데 사용될 수 있는 정보는 $(t-1)$개의 완전 지분에 불과하다. 이는 두 번째 조건을 만족하는 강화지분이 비밀 공유의 완전 보안성을 보존할 수 있다는 의미이다.

3. 강화지분 생성

본 논문에서는 두 가지 강화지분 생성 기법을 제안한다. 첫 번째 기법은 비밀 공유에 사용될 다항식을 먼저 결정하고, 이에 기반하여 부분 지분을 생성하는 제약적 점 선택 기법(Constrained Point Selection)이다. 두 번째 기법은 부분 지분을 먼저 생성한 후 비밀 공유에 사용될 다항식을 결정하는 기법(Unconstrained Point Generation)이다.

3.1 제약적 점 선택 기법

비밀 공유에 사용될 다항식을 먼저 결정하고, 이에 기반하여 부분 지분을 생성한다. 생성하는 강화지분의 개수에 따라 강화지분을 생성하는 방법이 약간 다르다.

A. 단수의 강화지분을 생성하는 절차$(m=1)$.

(1) 랜덤한 계수 a_i를 가지는 $(t-1)$차 다항식 $f(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+...S$를 생성한다.

(2) $f(x)$가 지나는 점 중에서 x축 좌표값이 p인 점 R을 선택한다.

(3) 점 R의 y축 좌표값을 계산하여 강화지분 h로 정한다. 즉, $h=f(p)$이며, 취합 지분은 점 $R(p,f(p))$이 된다.

(4) $(n-2)$개의 완전 지분을 생성한다.

B. 복수의 강화지분을 생성하는 절차$(m>1)$.

(1) 랜덤한 계수 a_i를 가지는 $(t-1)$차 다항식 $f(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+...S$를 생성한다.

(2) 랜덤한 방법으로 $(m-1)$개의 강화지분 $h_1,h_2,...,h_{m-1}$을 생성한다.

(3) 입력 파라미터의 엔트로피를 보존하는 함수 $g()$를 이용하여 x축 좌표값이 $g(p,h_1,h_2,...,h_{m-1})$인 점 R을 선택한다.

(4) 점 R의 y축 좌표값을 마지막 강화지분 h_m으로 정한다. 즉, $h_m=f(g(p,h_1,h_2,...,h_{m-1}))$이며, 취합 지분은 점 $R(g(p,h_1,h_2,...,h_{m-1}),h_m)$이 된다.

(5) $(n-m-1)$개의 완전 지분을 생성한다.

복수의 강화지분을 생성할 때 입력 파라미터의 엔트로피를 보존하는 함수 $g()$를 사용하는 것은 비밀의 기밀성(secrecy)을 보장하기 위한 것이다. 함수 $g()$가 엔트로피를 보존한다면 강화지분 $h_1,h_2,...,h_{m-1}$ 중 하나라도 모르면 점 R을 알아낼 수 없다. 강화지분 $h_1,h_2,...,h_{m-1}$이 랜덤하게 생성되었고, $g(p,h_1,h_2,...,h_{m-1})$가 엔트로피를 보존하기 때문이다. 다양한 방법들을 함수 $g()$로 사용할 수 있는데, 엔트로피를 보존할 수 있는 암호화 알고리즘(encryption algorithm), 일방향 함수(one way function), 의사랜덤 생성기(pseudorandom generator), 의사랜덤 함수(pseudorandom function) 등이 가능하다. 한 가지 방법은 XOR 암호화를 사용하는 것이며, XOR 연산자를 $\oplus$로 나타내면 아래와 같이 나타낼 수 있다[9, 10].

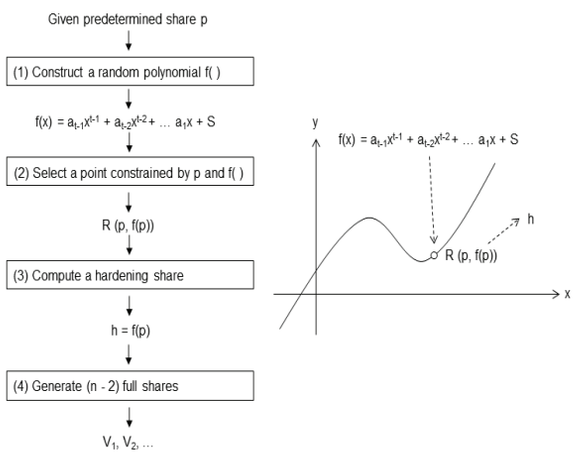

Fig. 2. Constrained Point Selection Technique to Generate Singular Reinforcing Shares

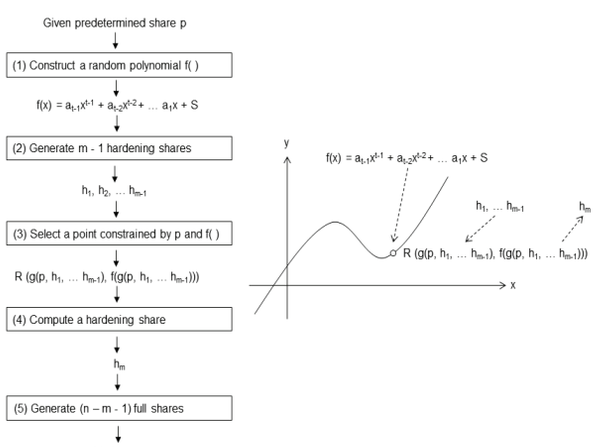

Fig. 3. Constrained Point Selection Techniques to Generate Multiple Reinforcing Stakes

$$g(p, h_1, h_2, \ldots, h_{m-1}) = p \oplus h_1 \oplus h_2 \oplus \ldots \oplus h_{m-1}$$

3.2 비 제약적 점 생성 기법

부분 지분을 먼저 생성한 후 비밀 공유에 사용될 다항식을 결정하는 기법이다. 이 기법 또한 생성하는 강화지분의 개수에 따라 강화지분을 생성하는 방법이 약간 다르다.

C. 단수의 강화지분을 생성하는 절차$(m = 1)$.

(1) 랜덤한 방법으로 강화지분 h를 생성한다.

(2) x축 좌푯값이 p이고 y축 좌푯값이 h인 점 R을 선택한다. $h = f(p)$이며, 취합 지분은 점 $R(p,f(p))$가 된다.

(3) 하나의 계수 a_i를 제외한 나머지 계수들을 랜덤하게 생성하여 $(t-1)$차 다항식 $f()$를 생성한 후, 다항식 $f()$가 점 R을 지나도록 계수 a_i를 정한다.

$$f(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \ldots S$$

(4) (n - 2) 개의 완전 지분을 생성한다.

D. 복수의 강화지분을 생성하는 절차$(m > 1)$.

(1) 랜덤한 방법으로 m개의 강화지분 $h_1, h_2, \ldots, h_m$을 생성한다.

(2) 부분 지분 $p, h_1, h_2, \ldots, h_m$으로 결정되는 점 R을 선택한다. 이때, 점 R은 부분 지분들의 조합에 따라 다양하게 결정할 수 있다. 한 가지 방법은 하나의 부분 지분을 점 R의 x축 또는 y축 좌푯값으로 사용하고 나머지 부분 지분들에 엔트로피를 보존하는 함수 $g()$를 이용하여 점 R의 나머지 좌푯값으로 사용하는 것이다. 이 경우 취합 지분의 형태는 $(p, g(h_1, h_2, \ldots, h_m))$, $(h_i, g(h_1, h_2, \ldots, p, \ldots, h_m))$, $(g(h_1, h_2, \ldots, h_m), p)$, $(g(h_1, h_2, \ldots, p, \ldots, h_m), h_i)$ 등이 될 수 있다. 다른 방법은 x축 좌푯값과 y축 좌푯값에 엔트로피를 보존하는 함수 $g_1()$과 $g_2()$를 각각 적용하는 것이다. 이 경우 취합 지분의 형태는 $(g_1(p, h_1, h_2, \ldots), g_2(h_i, \ldots, h_m))$가 된다. 이때 각 부분 지분은 적어도 한번은 사용되어야 한다.

(3) 하나의 계수 a_i를 제외한 나머지 계수들을 랜덤하게 생성하여 $(t-1)$ 차 다항식 $f()$를 생성한 후, 다항식 $f()$가 점 R을 지나도록 계수 a_i를 정한다.

$$f(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \ldots S$$

(4) $(n-m-1)$ 개의 완전 지분을 생성한다.

4. 적용 예시와 보안성 비교

4.1 제약적 점 선택 기법의 적용 예시

유한체(finite field) F_q상에서의 Shamir 비밀 공유에 적용하는 적용 예시를 설명한다. 유한체 F_q는 q로 나눈 나머지 값으로 정의되는데, 계산의 편의상 q의 값으로 소수(prime) 13을 가정한다. 이에 따라 비밀 공유에 사용되는 비밀 S, 계수 a_i, 좌푯값, 지분들은 모두 F_{13}에서 정의된다.

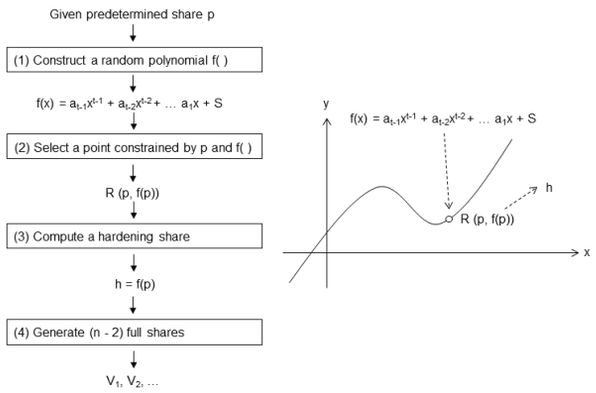

Fig. 4. Unconstrained Point Generation Technique to Generate Singular Reinforcing Shares

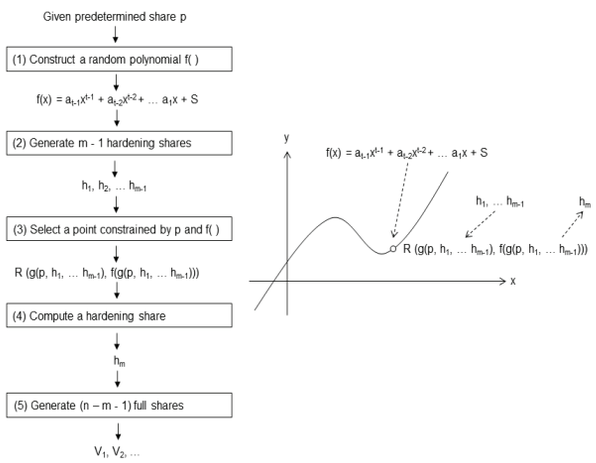

Fig. 5. Unconstrained Point Generation Technique to Generate Multiple Reinforcing Stakes

비밀 값 $S = 3$이고 지정 지분을 $p = 5$로 정하고 m개의 강화지분을 생성해보자. 랜덤하게 생성된 2차 다항식 $f(x) = x^2 + 9x + 3$이 주어져 있고, $f(x)$가 지나는 3개의 점 $(1, f(1)), (2, f(2)), (3, f(3))$으로부터 3개의 지분 $V_1 = 0, V_2 = 12, V_3 = 0$이 이미 정해져 있다고 하자.

단수의 강화지분을 생성하는 경우$(m = 1)$, $f(x)$에 존재하는 점 중에서 x축 좌푯값이 $p = 5\,(= 0101)$인 점 R을 선택하자. 점 R의 y축 좌푯값이 강화지분이 h가 되며, 즉 $h = f(p) = f(5) = 8$ 이다. 이때 점 R의 좌표는 $(5,8)$이다.

복수의 강화지분을 생성하는 경우$(m > 1)$, $m = 3$이라고 하자. 랜덤한 방법으로 2개의 강화지분 h_1과 h_2를 먼저 생성하며, 얻어진 값이 각각 $h_1 = 6\,(= 0110)$, $h_2 = 8\,(= 1000)$이라 하자. XOR 암호화를 함수 $g()$로 사용하여 x축 좌푯값이 $p \oplus h_1 \oplus h_2$인 점 R을 선택하자. $p \oplus h_1 \oplus h_2$는 아래와 같이 계산할 수 있다.

$$p \oplus h_1 \oplus h_2 = 0101 \oplus 0110 \oplus 1000 = 1011\,(=11)$$

따라서 점 R의 x축 좌푯값은 11이고, 점 R의 y축 좌푯값이 강화지분 h_3가 된다. 즉, $h_3 = f(p \oplus h_1 \oplus h_2)$이며, 이를 계산하면 $h_3 = f(11) = 223 \pmod{13} = 1$이 된다. 이때 점 R의 좌표는 (11, 1)이다.

4.2 비 제약적 점 선택 기법의 적용 예시

비밀 값 $S = 3$이고 지정 지분을 $p = 5$로 정하고 m개의 강화지분을 생성해보자.

단수의 강화지분을 생성하는 경우$(m = 1)$, 랜덤한 방법으로 강화지분 h를 먼저 생성하며, 얻어진 값은 $h = 8$이라고 하자. 이때 취합 지분이 될 점 $R(p,h)$는 $(5,8)$이 된다. 하나의 계수 a_2를 제외한 나머지 계수들을 랜덤하게 생성하여 2차 다항식 $f(x) = a_2x^2 + a_1x + a_0 = a_2x^2 + 9x + 3$을 생성했다고 하자. 다항식 $f(x)$가 점 $R(5,8)$을 지나도록 계수 a_2를 정하면 $f(x)$는 아래와 같이 구해질 수 있다.

$$f(5) = 25a_2 + 45 + 3 = 8 \pmod{13}$$
$$25a_2 = -40 = 12 \pmod{13}$$

F_{13}에서 25의 곱셈 역원(multiplicative inverse)이 12임을 이용하면,

$$25a_2 \cdot 12 = 12 \cdot 12 \pmod{13}$$
$$a_2 = 144 = 1 \pmod{13}$$

2차 다항식은 $f(x) = x^2 + 9x + 3$이 된다.

복수의 강화지분을 생성하는 경우$(m > 1)$, $m = 3$이라고 하자. 랜덤한 방법으로 3개의 강화지분 h_1, h_2, h_3을 먼저 생성하며, 얻어진 값이 각각 $h_1 = 6(= 0110)$, $h_2 = 8(= 1000)$, $h_3 = 2(= 0010)$라고 하자. 이미 설명한 바와 같이 취합 지분이 될 점 R을 정하는 방법은 다양하며, $(p, g(h_1, h_2, \ldots, h_m))$ 형태를 사용해보자. XOR 암호화를 $g()$로 사용하면 점 R의 좌표는 $(p, h_1 \oplus h_2 \oplus h_3))$이 되며, $h_1 \oplus h_2 \oplus h_3$는 아래와 같이 계산할 수 있다.

$$h_1 \oplus h_2 \oplus h_3 = 0110 \oplus 1000 \oplus 0010 = 1100 (= 12)$$

따라서 점 R의 좌표는 $(5, 12)$이 된다. 하나의 계수 a_2를 제외한 나머지 계수들을 랜덤하게 생성하여 2차 다항식 $f(x) = a_2x^2 + a_1x + a_0 = a_2x^2 + 9x + 3$을 생성했다고 하자. 이 다항식 $f(x)$가 점 $R(5, 12)$을 지나도록 계수 a_2를 정해보자.

$$f(5) = 25a_2 + 45 + 3 = 12 \pmod{13}$$
$$25a_2 = -36 = 3 \pmod{13}$$

F_{13}에서 25의 곱셈 역원이 12임을 이용하면,

$$25a_2 \cdot 12 = 3 \cdot 12 \pmod{13}$$
$$a_2 = 36 = 10 \pmod{13}$$

따라서 2차 다항식은 $f(x) = 10x^2 + 9x + 3$이 된다.

4.3 보안성 비교

제안하는 방법을 사용하면 미리 지정된 값을 지분으로 사용하는 것을 허용하면서 비밀 공유의 보안성을 강화할 수 있다. 제안하는 $(t, (m), n)$ 비밀 공유방법의 보안성은 $(t, (0), n)$ 비밀 공유방법 및 (t, n) 비밀 공유방법과의 비교를 통해 보일 수 있다. 이해를 돕기 위해 구체적인 예를 통해 설명하도록 한다.

Fig. 7의 $(3, (0), 8)$ 비밀 공유방법에서는 공격자(adversary)가 3개의 지분을 획득하면 비밀 S를 알아낼 수 있으며, 심지어 2개의 지분을 획득한 예도 지정지분 p_7의 취약성을 이용하여 비밀 S에 대한 정보를 유추해내는 것이 가능할 수 있다. 그러나 Fig. 7의 $(3, (1), 8)$ 비밀 공유방법에서는 지정 지분이 포함된 임의의 3개의 지분으로는 비밀 S를 알아낼 수 없다. 나아가 2개 이하의 지분으로는 비밀 S를 알아낼 수 없으며 S에 대한 어떠한 정보도 유추해낼 수 없다.

한편, 정상적인 상황(normal case)에서 비밀을 복원할 경우 $(3, (1), 8)$ 비밀 공유방법은 $(3, (0), 8)$ 비밀 공유방법에 비해 보관 및 사용 측면에서 추가적인 오버헤드를 초래할 수 있다. 비밀을 복원할 때 $(3, (1), 8)$ 비밀 공유방법은 4개의 지분이 필요하지만 $(3, (0), 8)$ 비밀 공유방법은 3개의 지분이 필요하기 때문이다. 다행히 지정지분 p_7로 패스워드나 생체정보를 사용한다면 지정지분 p_7을 별도로 보관하는 오버헤드를 피할 수 있다. 그러나 패스워드나 생체정보를 입력받는데 필요한 추가적인 사용자 인터페이스(user interface)와 처리

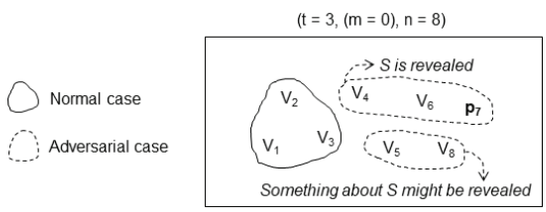

Fig. 6. $(3, (0, 8))$ Secret Sharing Method

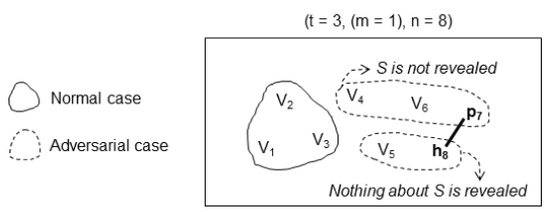

Fig. 7. $(3, (1), 8)$ Secret Sharing Method

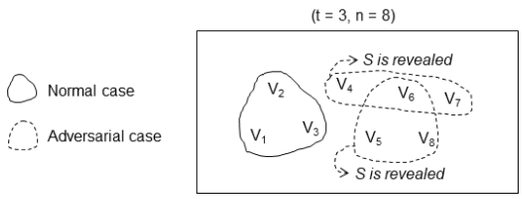

Fig. 8. $(3,8)$ Secret Sharing Method

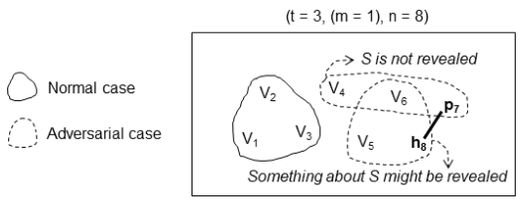

Fig. 9. $(3,1,8)$ Secret Sharing Method

(processing)는 불가피하다. 이는 보안성과 사용성의 교환 거래관계(trade-off)로 볼 수 있으며, 사용성이 일부 희생되더라도 높은 보안성이 요구되는 상황에서는 $(3,(1),8)$ 비밀 공유 방법이 좋은 대안이 될 수 있다.

지정 지분을 사용하지 않는 $(3,8)$ 비밀 공유와 지정지분과 강화지분을 모두 사용하는 $(3,(1),8)$ 비밀 공유를 비교해보자. $(3,8)$ 비밀 공유방법에서는 공격자가 임의의 3개의 지분을 획득하면 비밀 S를 알아낼 수 있다. $(3,(1),8)$ 비밀 공유 방법에서는 공격자가 획득한 3개의 지분에 강화지분과 지정지분이 포함되지 않으면 $(3,8)$ 비밀 공유방법과 마찬가지로 비밀 S를 알아낼 수 있다. 그러나 공격자가 획득한 3개의 지분에 지정지분 p_7이 포함되면 비밀 S를 알아낼 수 없다. 또한 공격자가 획득한 3개의 지분에 강화지분 h_8이 포함되면 지정지분 p_7이 필요하므로 p_7을 알아내기 위한 추가적인 노력이 필요하다. 따라서 $(3,(1),8)$ 비밀 공유방법이 $(3,8)$ 비밀 공유방법에 비해 우수한 보안성을 가진다.

기존 비밀 공유 또는 강화지분을 사용하지 않는 $(t,(0),n)$ 비밀 공유방법에서 임곗값(threshold) t를 증가시키면 공격에 대한 보안성을 높일 수 있다. 예를 들면, $(t+1,n)$ 또는 $(t+1,(0),n)$ 비밀 공유방법을 사용하면 공격자는 $(t+1)$개의 지분을 획득해야 하므로 공격에 대한 보안성이 높아진다. 하지만, 그러한 방법을 $(t+1,(m),n)$ 비밀 공유방법과 비교한다면 위의 설명과 같은 방식으로 $(t+1,(m),n)$ 비밀 공유방법의 보안성이 상대적으로 우수함을 보일 수 있다.

5. 결 론

본 논문에서는 비밀 공유방법의 사용 편의성을 개선하기 위한 지분 강화 기법을 제안하였다. 제안하는 기법은 패스워드나 생체정보와 같이 사용자가 미리 선택한 값을 지정 지분으로 사용하며, 추가로 강화지분의 개념을 도입하여 지정 지분의 보안성을 보완한다.

제안하는 기법은 패스워드와 같은 사용자의 지식, 생체정보와 같은 사용자의 고유성 등을 지분으로 사용하는 다중-요소 비밀 공유를 가능하게 한다. 패스워드는 전자적 해킹이 불가능하며, 생체정보는 전자적 해킹이 어려운 동시에 복제의 위험 또한 낮다. 또한 패스워드나 생체정보는 보관을 위한 별도의 디지털 장치가 있어야 하지 않으며, 게다가 우수한 접근성(accessibility)으로 인해 비밀 공유 시스템의 사용성을 개선할 수 있다.

References

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

[2] M. Carpentieri, "A perfect threshold secret sharing scheme to identify cheaters," *Designs, Codes and Cryptography*, Vol.5, No.3, pp.183-187, 1995.

[3] R. Steinfeld, H. Wang, and J. Pieprzyk, “Lattice-based threshold-changeability for standard Shamir secret- sharing schemes,” *Advances in Cryptology-ASIACRYPT 2004: 10th International Conference on the Theory and Application of Cryptology and Information Security*, Jeju Island, Korea, December 5-9, 2004. Proceedings 10, Springer.

[4] E. Dawson and D. Donovan, “The breadth of Shamir's secret-sharing scheme,” *Computers & Security*, Vol.13, No.1, pp.69-78, 1994.

[5] Y. Tian, J. Ma, C. Peng, and Q. Jiang, “Fair (t, n) threshold secret sharing scheme,” *IET Information Security*, Vol.7, No.2, pp.106-112, 2013.

[6] A. Bogdanov, S. Guo, and I. Komargodski, “Threshold secret sharing requires a linear size alphabet,” *Theory of Cryptography: 14th International Conference*, TCC 2016-B, Beijing, China, October 31-November 3, 2016, Proceedings, Part II 14, Springer.

[7] I. Komargodski and A. Paskin-Cherniavsky, “Evolving secret sharing: dynamic thresholds and robustness,” *Theory of Cryptography: 15th International Conference*, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part II 15, Springer.

[8] G. R. Blakley, “Safeguarding cryptographic keys,” Managing Requirements Knowledge, International Workshop on, IEEE Computer Society, 1979.

[9] J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, “A new (k, n)-threshold secret sharing scheme and its extension,” *Information Security: 11th International Conference*, ISC 2008, Taipei, Taiwan, September 15-18, 2008. Proceedings 11, Springer.

[10] J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, "On a fast (k, n)-threshold secret sharing scheme," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol.91, No.9, pp.2365-2378, 2008.

정 성 욱

https://orcid.org/0009-0007-3990-5228
e-mail : swchung@hanyang.ac.kr
2016년 고려대학교 전자정보공학부(학사)
2018년 충남대학교 컴퓨터공학부(석사)
2018년 ~ 현 재 한양대학교 컴퓨터공학부 박사과정
관심분야 : Blockchain, Operating Systems

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(공학박사)
1999년 ~ 2001년 Inus Technology 연구원
2001년 ~ 2002년 자동화시스템연구소 연구원
2003년 ~ 현 재 한양대학교 컴퓨터공학부 교수
관심분야 : Operating Systems, Real-TIme SYstems, Blockchain