특집 05

컴퓨팅 보안을 위한 극소 부호의 연구 동향 및 전망

조동식 · 정진호 (울산대학교)

목 차

1. 서 론

극소 부호(minimal code)는 한 사용자의 부호어 정보(codeword information)들이 다른 사용자의 부호어 정보에 종속되지 않는 부호로서 기밀 공유 기법(secret-sharing scheme) 등에 사용될 수 있는 수학적 구조의 하나로 꾸준히 연구되고 있다[1][2]. 특히, 2010년대 중반부터 블록체인(blockchain)[3], 연합학습(federated learning)[4] 등과 같이 보안성을 포함하는 기술들이 주목 받으면서 활발하게 연구되어 오기 시작했다[5-9].

극소 부호는 전통적인 대수적 오류정정부호(error-correcting codes)와 마찬가지로 유한체(finite field) 상의 구조를 이용해서 설계되어 왔다. 특히, 이진(binary) 극소 부호에 대해서는 다양한 경우에 대한 설계 기법이 제시되어 왔다[5-7]. 또한, 최근에는 비이진 극소 부호에 대한 연구도 진행되고 있다[8][9]. 극소 부호에서는 각 사용자의 부호어들이 다른 부호어를 완벽하게 포함할 수 없기 때문에 기밀 정보들이 종속되지 않고, 서로에게 분산되는 형태를 가진다. 이를 통해 분산된 형태의 보안을 구현할 수 있고, 각 사용자들에 분산된 정보들을 합성해서 원래의 정보를 얻을 수 있다.

현재까지의 극소 부호에 대한 연구는 주로 부호어의 무게와 길이에 있어서 한정적인 경우에 대한 결과들을 제시해왔다. 이는 대부분 유한체의 알려진 특성들을 이용한 설계 방법들이 주류를 이루어 왔기 때문인데, 정보의 길이와 기밀 공유 정도에 따른 새로운 공유 부호들을 설계하는 것은 앞으로 기밀 공유 기법의 연구에 있어서 매우 중요한 문제가 될 것이다.

본 논문에서는 극소 부호의 수학적 정의와 개념을 설명하고, 현재까지의 극소 부호의 설계 방법들을 비교한다. 또한, 현재까지 알려진 극소 부호들의 한계와 향후 적용 분야 및 연구 주제들을 제시한다.

〈표 1〉 대표적인 이진과 비이진 극소 부호

문헌	알파벳 크기	길이와 해밍 무게	제약 조건
[5]	2	2^m-1, 3 different weights	$\frac{w_{\min}}{w_{\max}} > \frac{1}{2}$
[6]	2	2^m-1, 3 different weights	$\frac{w_{\min}}{w_{\max}} > \frac{1}{2}$
[7]	2	2^m-1, 5~6 different weights	$\frac{w_{\min}}{w_{\max}} \leq \frac{1}{2}$
[8]	p	p^m-1, 3 different weights	p는 홀수인 소수, $\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}$
[9]	p	p^m-1, 3~4 different weights	p는 홀수인 소수, $\frac{w_{\min}}{w_{\max}} \leq \frac{p-1}{p}$

2. 극소 부호의 수학적 서술

유한체는 유한한 개수의 원소를 가지고 덧셈, 곱셈은 물론 이들의 역연산을 자유롭게 할 수 있는 체(field)이다. 유한체는 통신, 보안을 위한 오류정정부호, 의사불규칙 수열의 설계 등 다양한 영역에 적용되어 왔다. 극소 부호는 오류정정 능력을 갖지는 않지만, 기존의 오류정정부호와 마찬가지로 유한체 위의 행렬(matrix)과 벡터(vector)에 기반해서 설계될 수 있다. 본 장에서는 유한체와 극소 부호의 수학적 정의를 다룬다.

2.1 유한체

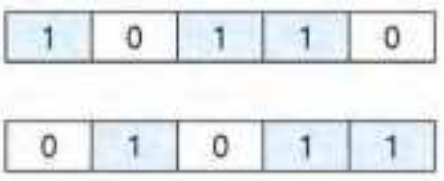
유한체는 덧셈에 대한 항등원인 0과 원시원소(primitive elements) α의 거듭제곱들로 이루어지는 집합이며, 덧셈과 곱셈의 연산이 정의될 수 있다. 또한, 유한체는 항상 소수(prime number)의 거듭제곱 개수의 원소를 가진다. 이러한 소수를 유한체의 표수(characteristic number)라 부른다. 원소의 개수가 $q = p^n$ (p는 소수, n은 자연수)이고, 원시원소 α를 갖는 유한체 GF(p^n)은 다음과 같이 구성된다:

$$GF(p^n) = \{0,\ \alpha,\ \alpha^2,\ \cdots,\ \alpha^{q-2}\}.$$

유한체는 덧셈에 대해서 아벨리안 군(Abelian group)이며, 0을 제외한 나머지 원소들은 곱셈에 대해서 순환 군(cyclic group)이다. 여기서 α는 n차의 원시 다항식(primitive polynomial)의 근이며, 유한체의 원소들은 α에 대한 n 차원 상의 벡터로 나타내거나 α의 거듭제곱으로 나타낼 수 있다. 정수환(integer ring)과 달리 유한체는 덧셈, 곱셈과 이들의 역연산(inverse operation)이 자유롭기 때문에 암호와 부호 등의 설계에 많이 사용되어 왔다.

2.2 극소 부호의 정의

n차원 좌표계 상의 벡터 v의 서포트(support)는 0이 아닌 좌표의 위치로 정의된다. 어떤 n차원 벡터들의 집합 C에서 임의의 독립인 두 벡터들의 서포트가 서로 포함 관계에 있지 않고 전체 집합이 벡터 공간을 이루면 C는 극소 부호라고 불린다.



(그림 1) 서포트가 종속되지 않는 두 벡터

그림 1은 서포트가 서로 포함되지 않는 두 개의 5차원 이진 벡터의 한 예를 나타낸다. 정보의 위치가 서로 종속되지 않기 때문에 기밀이 한 사용자에게 집중되지 않고, 분산 및 공유되는 시스템에 적용될 수 있다.

3. 극소 부호의 연구 동향

기밀 공유 시스템에서는 기밀이 여러 사용자에게 나누어서 전달되고, 이러한 사용자들로부터 전달된 기밀들이 정해진 방법에 의해 합성되어서 원래의 정보를 다시 생산한다. 여기서 각각의 사용자들은 서로에게 종속되지 않아야 하며, 이를 구현하기 위해서는 극소 부호가 사용될 수 있다. 현재까지의 극소 부호는 실용적인 측면보다는 이론적인 부분에서 연구가 이루어져 왔다고 볼 수 있다.

3.1 이진 극소 부호의 설계에 대한 연구 동향

이진 극소 부호는 1979년에 Hwang에 의해 제안되었으나[1], 기밀 공유의 관점에서 해석 되기 시작한 것은 Massey의 연구에 의해서이다[2]. 유한체를 기반으로 한 체계적인 설계 방법은 1998년 Ashikhmin과 Barg에 의해 시작되었다[5]. 또한, Carlet 등은 완전 비선형 사상에 의한 극소 부호의 설계 방법을 제시하였다[6]. 이 논문에서는 극소 부호의 무게 분포(weight distribution)에 대한 분석도 제시되었다. 다음 정리는 극소 부호의 설계에 있어서 매우 중요한 성질의 하나이다.

정리 1 [5]. 유한체 F_q 위의 어떤 선형 부호 C가 다음을 만족하면 극소 부호이다:

$$\frac{w_{\min}}{w_{\max}} > \frac{q-1}{q}.$$

여기서, $w_{\min}(w_{\max})$는 C의 부호어의 해밍 무게 중에서 가장 작은(큰) 값이다.

정리 1은 이진 부호뿐만 아니라 비이진 부호에도 적용되고, 기밀 공유 기법에서 각 사용자들이 어떤 종류의 정보량을 가질 수 있는지 알려주는 중요한 내용을 포함하고 있다. 하지만, 이는 극소 부호가 존재할 충분 조건이기 때문에, 정리 1의 경우에 포함되지 않는 이진 극소 부호에 대한 연구도 진행되었다. Ding 등은 가장 작은 해밍 무게와 가장 큰 무게 사이의 비율이 1/2을 넘지 않는 경우에 대해서 최초로 극소 부호의 설계법을 제시하였다 [7]. 이 설계법에 의하면 임의의 m에 대해 무한하게 큰 길이의 부호에 대해 2^m-1의 길이를 가지는 극소 부호를 생성할 수 있다. 또한, 정리 1의 조건에서 벗어나기 때문에 기밀 공유 기법에 있어서 다양한 환경에 적용이 가능한 방법을 제시했다고 볼 수 있다. 하지만, 새로운 설계 방법으로도 길이에 대한 다양성은 확보하지 못했기 때문에 향후 중요한 문제라고 할 수 있다.

3.2 비이진 극소 부호의 설계

홀수인 소수 p의 알파벳 크기를 가진 부호에 대한 연구도 최근 들어 진행되고 있다. Ding 등은 2~3 종류의 해밍 무게를 갖는 극소 부호에 대한 설계 방법을 제시하였다[8]. 하지만 해밍 무게가

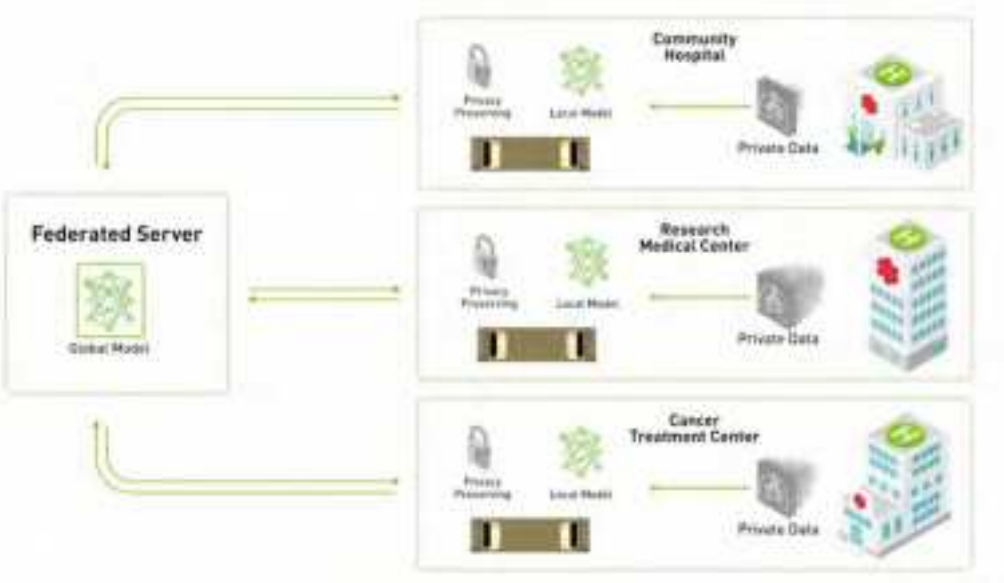
부호의 길이에 비해서 작은 값을 가지고 무게의 종류가 적기 때문에 한 사용자에게 많은 정보량을 할당할 수 없고, 정보량의 다양화를 구현하기 힘들다는 단점을 가지고 있었다. Xu 등은 최근에 [9]에서 정리 1의 경우에서 벗어나면서 4 종류의 해밍 무게를 가지면서 큰 해밍 무게를 가질 수 있는 비이진 극소 부호에 대한 설계 방법을 제시하였다. 하지만, 비이진 극소 부호는 이진 극소 부호에 비해 다양한 설계 방법이 제시되지는 못하였다.

3.3 기존 극소 부호의 설계의 한계

기존에 알려진 모든 극소 부호는 캐릭터 합과 같은 유한체의 알려진 성질에 의존하여 설계되었기 때문에 소수 p에 대해 길이가 p^{m-1}인 경우에만 설계되었다. 따라서 다양한 시스템 환경에 적용될 수 없는 단점이 있었다. 또한, 부호의 부분만을 잘라서 사용할 때는 유한체의 특성이 파괴되어서 대부분의 장점들이 없어지는 특성을 가진다. 그렇기 때문에 합성수(composite number)의 길이를 가지면서 기존 유한체 기반 설계의 장점들을 그대로 가진 극소 부호의 설계가 필요하다. 또한, 정보량을 조절할 수 있는 각 부호어의 해밍 무게에 있어서도 가변적인 특성을 가질 수 있는 설계가 필요할 것이다. 앞으로 사용될 분산형 보안 시스템을 위한 복호화 및 부호화 방법에 대한 실용적인 접근도 중요할 것이다.

4. 극소 부호의 적용 및 전망

블록 체인 기술은 비트코인 등의 암호화폐 뿐만 아니라 분산형 데이터 시스템의 구현에 있어서 매우 중요한 부분으로 주목받고 있다 [3]. 연합학습에서는 중앙 서버에 연산이 집중되던 연산과 보안이 각각의 작은 서버들로 분산된다. 의료 분야에서는 이미 NVIDIA 등을 중심으로 개인정보의 보호와 효율성을 동시에 만족하는 인공지능 기술에 대한 연구가 활발하게 진행되고 있다[10].



(그림 2) 의료 데이터를 위한 연합학습 모델 (NVIDIA, [10])

4.1 극소 부호의 적용 분야

극소 부호는 수학적인 설계는 어렵지만, 한번 설계된 부호를 저장 및 사용하는데 있어서 복잡도는 매우 작다고 볼 수 있다[5]. 따라서, 기밀 공유 기법이 적용되는 블록체인에 적용될 수 있음은 물론, 효율성과 보안성을 동시에 만족시키는 연합학습을 위한 기밀 공유 및 분배 수단으로 매우 중요한 가치를 가질 수 있을 것이다. 현재 비이진법 반도체에 대한 연구가 활발히 진행되고 있고, 향후 상용화되어서 통신, 보안, 데이터 시스템 등에 적용될 수 있기 때문에 비이진 극소 부호의 설계도 매우 중요한 문제가 될 것이다.

4.2 극소 부호의 전망

현재까지의 극소 부호에 대한 연구는 매우 제한적인 그룹에서만 수행되어 왔고, 쓰인 수학적 도구들도 매우 제한적이다. 하지만, 기존의 오류정정부호나 수열의 설계에서도 새로운 수학적 구조의 발견을 통해 이러한 문제를 해결한 사례들이 있다[11]. 발전된 수학적 구조들을 적용할 뿐만 아니라 머신 러닝(machine learning)을 통한 부호 설계 기법[12] 등을 통해 다양한 형태의 극소 부호를 설계할 수 있을 것으로 전망된다.

5. 결 론

앞서 언급한 바와 같이 극소 부호는 연합 학습, 블록 체인 등과 같은 미래 애플리케이션에서 사용될 기밀 공유 기법들에 사용될 수 있다. 현재까지의 설계 기법은 제한적인 수학적 도구만을 사용해 왔기 때문에 다양한 환경에서의 적용에 한계가 있었다.

향후 극소 부호는 데이터의 형태에 따라 비이진 알파벳을 가지고, 가변적인 길이 및 무게를 갖는 형태로 발전해야 할 것이다. 이를 위해서는 정수환, 가우스 수(Gaussian number) 등의 수학적 이론을 이용할 뿐만 아니라 기계 학습 기반의 설계까지 고려되어야 할 것이다. 뿐만 아니라 극소 부호의 보안성을 비교할 수 있는 엄밀한 수학적인 척도가 정의되고, 이에 따른 설계 기법도 제시되어야 할 것이다.

참 고 문 헌

[1] J. Massey, “Minimal codewords and secret sharing,” in Proc. 6th Joint Swedish-Russian Workshop on Information Theory, Sweden, 1993, pp. 246-249.

[2] T.-Y. Hwang, “Decoding linear block codes for minimizing word error rate,” IEEE Trans. Inform. Theory, vol. IT-25, pp. 733-737, Nov. 1979.

[3] “Blockchains: The great chain of being sure about things,” The Economist, Oct. 31, 2015.

[4] Konečný, Jakub; McMahan, Brendan; Ramage, Daniel (2015). "Federated Optimization: Distributed Optimization Beyond the Datacenter," arXiv:1511.03575

[5] A. Ashikhmin and A. Barg, "Minimal Vectors in Linear Codes," IEEE Trans. Inform. Theory, vol. 44, no. 5, pp. 2010-2017, Sept. 1998.

[6] C. Carlet, C. Ding, and J. Yuan, “Linear codes from perfect nonlinear mappings and their secret sharing schemes,” IEEE Trans. Inform. Theory, vol. 51, no. 6, pp. 2089-2102, Jun. 2005.

[7] C. Ding, Z. Heng and Z. Zhou, "Minimal binary linear codes," IEEE Trans. Inform.

Theory, vol. 64, no. 10, pp. 6536-6545, Oct. 2018.
[8] K. Ding and C. Ding, "A class of two-weight and three-weight codes and their Applications in secret sharing," IEEE Trans. Inform. Theory, vol. 61, no. 11, pp. 5835-5842, Nov. 2015.
[9] G. Xu and L. Qu, "Three classes of minimal linear codes over the finite fields of odd characteristic," IEEE Trans. Inform. Theory, vol. 65, no. 11, pp. 7067-7078, Nov. 2019.
[10] https://resources.nvidia.com/en-us-federated-learning/what-is-it?%5D
[11] J.-H. Chung and K. Yang, “k-fold cyclotomy and its application to frequency-hopping sequences,” IEEE Trans. Inform. Theory, vol. 57, no. 4, pp. 2306-2317, Apr. 2011.
[12] L. Huang, H. Zhang, R. Li, Y. Ge, and J. Wang, “AI Coding: Learning to Construct Error Correction Codes,” IEEE Trans. Commun., vol. 68, no. 1, Jan. 2020.

저 자 약 력

조 동 식

이메일 : dongsikjo@ulsan.ac.kr

- 2017년 고려대학교 컴퓨터학 (박사)
- 2004년~2018년 전자통신연구원(ETRI) 선임연구원
- 2018년~2020년 원광대학교 디지털콘텐츠공학과 교수
- 2018년 가상현실 증강현실의 미래 저자
- 2021년 MDPI Electronics Guest Editors (LifeXR)
- 2021년~현재 울산대학교 IT융합전공 교수
- 관심분야 : 홀로그램, VR/AR/MR, 컴퓨터그래픽스, HCI

정 진 호

이메일 : jinho@ulsan.ac.kr

- 2005년 포항공과대학교 전자공학과 및 수학과 (학사)
- 2007년 포항공과대학교 정보통신학과 (석사)
- 2011년 포항공과대학교 전자공학과 (박사)
- 2013년~2020년 울산과학기술원 / 조교수
- 2013년 워털루대학교 / 방문 조교수
- 2021년~현재 울산대학교 AI융합전공 조교수
- 관심분야 : 정보이론, 인공지능 보안, 무선통신