ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
j.inst.Korean.electr.electron.eng.Vol.26,No.3,506~509,September 2022
https://doi.org/10.7471/ikeee.2022.26.3.506
논문번호 22-03-25
174

극소 부호의 새로운 확장 기법

A New Extension Method for Minimal Codes

정 진 호*★

Jin-Ho Chung*★

Abstract

In a secret sharing scheme, secret information must be distributed and stored to users, and confidentiality must be able to be reconstructed only from an authorized subset of users. To do this, secret information among different code words must not be subordinate to each other. The minimal code is a kind of linear block code to distribute these secret information not mutually dependent. In this paper, we present a novel extension technique for minimal codes. The product of an arbitrary vector and a minimal code produces a new minimal code with an extended length and Hamming weight. Accordingly, it is possible to provide minimal codes with parameters not known in the literature.

요 약

비밀 공유 기법에서는 비밀 정보가 사용자들에게 분산되어 저장되고, 특정 허가된 사용자의 부분 집합으로부터만 비밀이 재합성 될 수 있어야 한다. 이를 위해서는 서로 다른 부호어들 사이의 정보가 종속되지 않아야 한다. 극소 부호는 선형 블록 부호의 일종으로서 이러한 비밀 정보들이 상호 종속되지 않게 분산하는 역할을 한다. 본 논문에서는 극소 부호의 새로운 확장 기법을 제시한다. 임의의 벡터와 극소 부호의 곱을 통해 새로운 길이와 해밍 무게를 가지는 새로운 극소 부호가 생성된다. 이를 통해 기존에 알려지지 않은 파라미터를 가지는 극소 부호들을 제공할 수 있다.

Key words : Finite fields, interleaving, linear codes, minimal codes, secret sharing

Ⅰ. 서론

극소 부호(minmal code)는 선형 블록 부호(linear block code, [1])의 일종으로서, 비밀 공유 기법(secret-sharing scheme) 등에 사용되어 왔다. 비밀 공유 기법에서는 비밀 정보가 사용자들에게 분산되어 저장되고, 특정 허가된 사용자의 부분 집합으로부터만 비밀 정보가 재합성(reconstruction) 될 수 있어야 한다[2]. 이러한 비밀의 분산은 극소 부호에 의해 수학적으로 정의된다. 극소 부호의 가장 중요한 특성은 한 사용자의 부호어가 다른 사용자의 부호어에 종속되지 않아야 한다는 것이다. 수학적으로는 한 부호어의 서포트(support)가 다른 부호어의 서포트의 부분 집합이 되지 않는 것이다. 이러한 극소 부호는 정보의 분산이 요구되는 연합학습(federated learning), 블록체인(blockchain) 등의 분야에 적용될 수 있을 것으로 기대되고 있다. 새로운 극소 부호의 설계 기법은 부호 이론 분야에서 흥미로운 주제로 여겨지고 있다.

Aschikhmin과 Barg는 [3]에서 선형 블록 부호가 극

* Assistant Professor, Dept. of Electrical, Electronics, and Computer Engineering, University of Ulsan
★ Corresponding author
E-mail : jinho@ulsan.ac.kr, Tel : +82-52-259-1644
※ Acknowledgment
Manuscript received Aug. 9, 2022; revised Sep. 4, 2022; accepted Sep. 5, 2022.

소 부호가 될 충분 조건과 최소 거리 복호 방법을 제시하였다. Aschikhmin과 Barg의 충분 조건 하에 다양한 극소 부호들이 설계되었다[4-6]. Chang and Hyun은 처음으로 이러한 충분 조건에 종속되지 않는 극소 부호의 설계 방법을 발견하였다[7]. Ding, Heng, Zhou는 이진(binary) 부호가 극소 부호가 될 필요충분 조건을 제시함과 동시에, 무한한 이진 극소 부호의 부류를 설계하였다[8]. Heng, Ding, Zhou는 다양한 이진 및 삼진(ternary) 극소 부호를 발견하였다[9]. Bartoli와 Bonini는 비이진 극소 부호에 대한 일반화된 설계 방법과 귀납적인 확장 방법을 제안하였다[10]. Mesnager, Qi, Ru, Tan 등은 유한체에서 정의된 특성 함수를 통해 극소 부호를 설계하는 방법을 제시하였다[11]. 지금까지 알려진 극소 부호들은 대부분 유한체의 구조와 성질에 기반했기 때문에 길이가 유한체의 크기와 관련된 형태로 제한되어 왔다. 하지만, 다양한 정보어의 길이나 통신 환경에 따라 이에 맞는 새로운 파라미터를 가지는 극소 부호의 설계가 필요하다.

본 논문에서는 극소 부호의 새로운 확장 기법을 제시한다. 임의의 벡터와 극소 부호의 곱(product)을 통해 새로운 길이(length)와 해밍 무게(Hamming weight)를 가지는 새로운 극소 부호가 생성된다. 이를 통해 기존에 알려지지 않은 파라미터(parameter)를 가지는 극소 부호들을 제공할 수 있다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 선형 부호와 극소 부호에 대한 배경 지식들을 설명한다. Ⅲ장에서는 새로운 극소 부호의 설계 방법을 제시하고, 새로운 극소 부호들의 무게 특성과 최소 거리 등의 성질에 대해 살펴 본다. 마지막으로 Ⅳ장에서는 결론을 맺는다.

Ⅱ. 배경

어떤 소수의 거듭제곱 q에 대해 유한체 F_q 상에서 정의된 길이가 N인 선형 블록 부호 C는 N차원 벡터 공간(vector space)의 K차원 부분 공간(subspace)로 정의된다. (N,K) 선형 블록 부호 C는 다음과 같은 벡터들의 집합으로 나타낼 수 있다:

$$C=\{\underline{x}_0,\underline{x}_1,\cdots,\underline{x}_{M-1}\}. \quad (1)$$

여기서 각각의 벡터 $\underline{x}_i$, $0\le i\le M-1$는 부호어(codeword)라 불린다. 또한, M은 서로 다른 부호어의 개수로서 사용자 수를 의미한다. K는 정보를 가지는 부분의 길이를 의미하는데, N개의 벡터 성분 중에서 독립적인 성분의 개수와 같다. 벡터의 각 원소는 다음과 같이 나타낼 수 있다:

$$\underline{x}_i=(x_i[0],x_i[1],\cdots,x_i[N-1]). \quad (2)$$

선형 부호의 성질에 따라 두 부호어의 합 $\underline{x}_i+\underline{x}_j$는 C에 속하는 어떤 부호어 $\underline{x}_k$가 된다. 또한 F_q의 임의의 원소 $a\in F_q$에 대해서도 $a\underline{x}_i$는 C의 어떤 부호어 $\underline{x}_{k'}$이 된다. 부호어 $\underline{x}_i$의 서포트는 다음 집합으로 정의된다:

$$\mathrm{supp}(\underline{x}_i)=\{0\le n\le N-1 : x_i[n]\neq 0\}. \quad (3)$$

즉, 부호어에서 0이 아닌 값에 해당하는 위치들의 집합이다. 또한, $\underline{x}_i$의 해밍 무게는 $\underline{x}_i$의 서포트의 집합 크기로 정의된다. (N,K) 선형 블록 부호 C의 임의의 부호어 $\underline{x}_i$의 서포트가 다른 부호어 $\underline{x}_j$의 서포트의 부분 집합이 되지 않는 성질을 만족한다면 C는 (N,K) 극소 부호라고 불린다. 이러한 경우에 $\underline{x}_i$가 0이 아니면서 $\underline{x}_j$가 0인 위치가 반드시 존재하고, 그 반대의 경우도 마찬가지이다.

Ⅲ. 본론

1. 새로운 극소 부호의 확장 방법

본 절에서는 기존의 극소 부호와 임의의 길이의 벡터의 곱을 통해 새로운 극소 부호를 설계한다. $C=\{\underline{x}_0,\underline{x}_1,\cdots,\underline{x}_{M-1}\}$는 F_q 상의 (N,K) 극소 부호라 하자. 그리고, $0\le a\le N-1$에 대해서 F_q 상의 길이가 l, $l\ge 2$인 영벡터(zero vector)가 아닌 임의의 벡터 $\underline{s}_a=(s_a(0),s_a(1),\cdots,s_a(l-1))$를 정의하자. 정리 1에서는 새로운 길이 ln의 극소 부호가 제시된다.

정리 1. 길이가 ln인 부호어 $\underline{y}_i$를 다음과 같이 정의하자:

$$y_i[a,b]:=y_i[al+b]=s_a[b]\cdot x_i[a]. \quad (4)$$

여기서, $0\le a\le N-1$이고 $0\le b\le l-1$이다. 새로운 부호 $E=\{\underline{y}_0,\underline{y}_1,\cdots,\underline{y}_{M-1}\}$은 (lN,K) 극소 부호이다.

증명 : 먼저 E가 선형 부호임을 증명한다. 0과 $M-1$ 사이의 두 정수 i와 j에 대해서

$$\begin{aligned} y_i[a,b]+y_j[a,b] &= s_a[b]x_i[a]+s_a[b]x_j[a] \\ &= s_a[b]\{x_i[a]+x_j[a]\} \\ &= s_a[b]x_k[a] \\ &= y_k[a,b]. \end{aligned} \tag{5}$$

이 성립한다. 또한,

$$\begin{aligned} ay_i[a,b]+y_j[a,b] &= as_a[b]x_i[a] \\ &= s_a[b](ax_i[a]) \\ &= s_a[b]x_{k'}[a] \\ &= y_{k'}[a,b]. \end{aligned} \tag{6}$$

이다. 따라서, E는 선형 부호이다. 다음으로는 극소성(minimality)를 증명해야 한다. 서로 다른 임의의 i와 j에 대해 원래 부호 C의 극소성에 의해 어떤 $0 \le a \le N-1$에 대해 $x_i[a] \neq 0$이고 $x_j[a]=0$이 성립한다. $\underline{s}_a$는 영벡터가 아니기 때문에 이러한 a에 대해

$$y_i[a] = s_a[b]x_i[a] \neq 0 \tag{7}$$

이고,

$$y_j[a] = s_a[b]x_j[a] = 0 \tag{8}$$

인 $0 \le b \le l-1$이 존재한다. 따라서 부호어 $\underline{y}_i$의 서포트는 $\underline{y}_j$의 서포트에 부분 집합이 되지 않는다. 같은 방법으로 $\underline{y}_j$의 서포트도 $\underline{y}_i$의 서포트의 부분 집합이 아님을 보일 수 있다. 그러므로 새롭게 설계된 부호 E는 극소 부호이다.

정리 1에서 각각의 부호어 $\underline{y}_i$는 원래 부호의 부호어 $\underline{x}_i$의 원소들의 값 만큼 $\underline{s}_a$에 상수배한 벡터들을 연접(concatenation)한 것과 같다. 그림 1은 이러한 극소 부호의 확장 방법을 나타내고 있다.

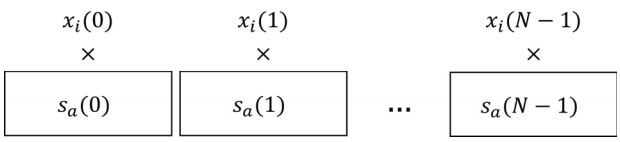

Fig. 1. Extension method for minimal codes.
그림 1. 극소 부호의 확장 방법

2. 새로운 극소 부호의 무게 성질

선형 블록 부호 C의 부호어들의 해밍 무게 중에서 최소값을 $w_{\min}$, 최대값을 $w_{\max}$라 하자. 극소 부호의 무게 분포에 대해서 Aschikhmin과 Barg는 다음 정리를 제시하였다.

정리 2 [3]. F_q 상의 선형 부호 C의 $w_{\min}$과 $w_{\max}$가 다음을 만족하면 C는 극소 부호가 된다:

$$\frac{w_{\min}}{w_{\max}} \ge \frac{q-1}{q}. \tag{9}$$

정리 2의 경계는 극소 부호의 설계에 대한 충분조건으로서 새로운 극소 부호를 만드는데 중요한 가이드라인이 되어 왔다. 하지만, (9)의 경계에 한정되는 무게를 가지는 부호들은 부호어들 사이의 해밍 무게가 너무 좁은 범위로 한정된다. 이에 따라, 최근에 (9)의 범위를 벗어나는 새로운 극소 부호에 대한 연구들이 활발하게 진행되어 왔다[7-11].

새로운 부호 E의 무게 분포는 $\underline{s}_a$들의 무게 분포와 원래 부호 C의 무게 분포에 의해 결정된다. 가장 자명한 경우로 $\underline{s}_a$들의 해밍 무게가 1로 고정되면, 새로운 부호 E의 무게 분포는 C의 무게 분포와 일치하게 된다. 또한, $\underline{s}_a$들의 해밍 무게의 최대치는 길이와 같은 l이다. 모든 $\underline{s}_a$들의 무게가 l로 고정되었을 때는 기존의 무게 분포에서 각각의 값들이 l배가 된다. 각각의 $\underline{s}_a$들의 해밍 무게는 1에서 l 사이의 값을 임의로 선택할 수 있기 때문에 a에 따른 $\underline{s}_a$의 해밍 무게 변화에 따라 다양한 무게 분포가 생길 수 있다. 또한, 정리 2의 범위 밖에 있는 부호를 확장시켰을 경우에 역시 정리 2에 한정되지 않는 부호를 얻을 수 있음을 알 수 있다.

Table 1. Examples of new parameters of minimal codes (N: length, K: information legnth, d :minimum distance).
표 1. 새로운 극소 부호의 예시 (N: 길이, K: 정보 길이, d :최소 거리)

	Original Codes	Extended Codes
N	255	$255 \cdot l$
K	9	$9 \cdot l$
d	60	$60 \sim 60 \cdot l$
Number of distinct weights	4	4 or more

선형 부호에서는 부호 간의 거리를 나타내는 최소 거리(minimum distance)도 오류 확률과 관련된 중요한 성능 지표 중에 하나이다. 선형성에 의해 최소 거리는 부호어들의 해밍 무게 중 최소값과 같다. 원래의 극소 부호 C의 최소 거리를 d로 가정하면, 새로운 극소 부호 E의

최소 거리는 $\underline{s}_a$의 선택에 따라 d에서 $l \cdot d$의 범위를 가지는 것을 알 수 있다. 따라서, 길이가 확장됨에 따라 길이와 최소 거리 사이의 비율도 유지됨을 알 수 있다. 표 1에서는 확장된 부호의 길이, 무게, 최소 거리에 대한 예시를 나타내었다.

Ⅳ. 결론

본 논문에서는 기존의 극소 부호를 임의의 배수 길이로 확장하고, 해밍 무게의 관점에서도 다양한 분포를 얻을 수 있는 확장 방법을 제시하였다. 또한, 선형 부호의 중요한 성질인 최소 거리도 커질 수 있음을 확인하였다. 이러한 극소 부호의 확장을 통해 연합학습, 블록체인 등의 다양한 애플리케이션에서 실제 상황에 맞는 다양한 파라미터들을 가지는 부호들을 적용할 수 있을 것이다.

References

[1] W. E. Ryan, S. Lin, *Channel Codes*, 2nd ed.; Cambridge University Press, UK, 2009.

[2] J. L. Massey, "Minimal codewords and ecret sharing," *Proc. 6th Joint Swedish-Russian Int. Workshop Inform. Theory*, pp.276-279, 1993.

[3] A. Ashikhmin and A. Barg, "Minimal vectors in linear codes," IEEE Trans. Inf. Theory, vol.44, no.5, pp.2010-2017, 1998. DOI: 10.1109/18.705584

[4] C. Carlet, C. Ding, and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," *IEEE Trans. Inf. Theory,* vol.51, no.6, pp.2089-2102, 2005.
DOI: 10.1109/TIT.2005.847722

[5] J. Yuan and C. Ding, "Secret sharing schemes from three classes of linear codes," *IEEE Trans. Inf. Theory*, vol.52, no.1, pp.206-212, 2006.
DOI: 10.1109/TIT.2005.860412

[6] K. Ding and C. Ding, "A class of two-weight and three-weight codes and their applications in secret sharing," *IEEE Trans. Inf. Theory*, vol.61, no.11, pp.5835-5842, 2015.
DOI: 10.1109/TIT.2015.2473861

[7] S. Chang and J. Y. Hyun, "Linear codes from simplicial complexes," *Des., Codes Cryptogr.,* vol.86, no.10, pp.2167-2181, 2018.
DOI: 10.1007/s10623-017-0442-5

[8] C. Ding, Z. Heng, and Z. Zhou, "Minimal binary linear codes," *IEEE Trans. Inf. Theory*, vol.64, no.10, pp.6536-6545, 2018.
DOI: 10.1109/TIT.2018.2819196

[9] Z. Heng, C. Ding, and Z. Zhou, "Minimal linear codes over finite fields," *Finite Fields Their Appl.,* vol.54, pp.176-196, 2018.
DOI: 10.1016/j.ffa.2018.08.010

[10] D. Bartoli and M. Bonini, "Minimal linear codes in odd characteristic," *IEEE Trans. Inf. Theory,* vol.65, no.7, pp.4152-4155, 2019.
DOI: 10.1109/TIT.2019.2891992

[11] S. Mesnager, Y. Qi, H. Ru, and C. Tang, "Minimal linear codes from characteristic functions," *IEEE Trans. Inf. Theory,* vol.66, no.9, pp.5404-5413, 2020. DOI: 10.1109/TIT.2020.2978387