

**Mesnager, Sihem; Kim, Kwang Ho; Choe, Jong Hyok; Lee, Dok Nam; Go, Dae Song**  
**Solving  $x + x^{2^l} + \dots + x^{2^{ml}} = a$  over  $\mathbb{F}_{2^n}$ .** (English) Zbl 1446.11207  
Cryptogr. Commun. 12, No. 4, 809-817 (2020).

Summary: This paper presents an explicit representation for the solutions of the equation  $\sum_{i=0}^{k-1} x^{2^{li}} = a \in \mathbb{F}_{2^n}$  for any given positive integers  $k, l$  with  $l \mid k$  and  $n$ , in the closed field  $\overline{\mathbb{F}_2}$  and in the finite field  $\mathbb{F}_{2^n}$ . As a by-product of our study, we are able to completely characterize the  $a$ 's for which this equation has solutions in  $\mathbb{F}_{2^n}$ .

**MSC:**

**11T06** Polynomials over finite fields  
**12E05** Polynomials in general fields (irreducibility, etc.)

Cited in **1** Review  
Cited in **3** Documents

**Keywords:**

linear equation; binary finite field; zeros of polynomials; linearized polynomial

**Full Text:** [DOI](#)

**References:**

- [1] Blake, I.; Seroussi, G.; Smart, N., Elliptic curves in cryptography. Number 265 in London mathematical society lecture note series (1999), Cambridge: Cambridge University Press, Cambridge
- [2] Carlet, C.: Boolean functions for cryptography and error correcting codes. Chapter of the monography. In: Crama, Y., Hammer, P. (eds.) Boolean models and methods in mathematics, computer science, and engineering, pp 257-397. Cambridge University Press, Cambridge (2010) · [Zbl 1209.94035](#)
- [3] Carlet, C.: Vectorial Boolean functions for cryptography. Chapter of the monography. In: Crama, Y., Hammer, P. (eds.) Boolean models and methods in mathematics, computer science, and engineering, pp 398-469. Cambridge University Press, Cambridge (2010) · [Zbl 1209.94036](#)
- [4] Mullen, GL; Panario, D., Handbook of finite fields. Discrete mathematics and its applications (2013), Boca Raton: CRC Press, Boca Raton

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.