

1056-13-1539

Jintai Ding (jintai.ding@uc.edu), Department of Mathematical Sciences, University of Cincinnati, Cincinnati, OH 45221, **Timothy J Hodges*** (timothy.hodges@uc.edu), Department of Mathematical Sciences, University of Cincinnati, Cincinnati, OH 45221, and **Victoria Kruglov** (kruglov@email.uc.edu), Department of Mathematical Sciences, University of Cincinnati, Cincinnati, OH 45221. *Growth of the ideal generated by a quadratic Boolean function.* Preliminary report.

We give exact formulas for the growth of the ideal $A\lambda$ for λ a quadratic element of the algebra of Boolean functions $A = \mathbb{F}_2[x_1, \dots, x_n]/(x_1^2 + x_1, \dots, x_n^2 + x_n)$ over the Galois field \mathbb{F}_2 . That is, we calculate $\dim A_k\lambda$ where A_k is the subspace of elements of degree less than or equal to k . For instance, if $\lambda = x_1x_2 + \dots + x_{n-1}x_n$, then

$$\dim A_k\lambda = \begin{cases} \delta(n, k), & \text{if } 0 \leq k < n/2 \\ \delta(n, k) - (\epsilon(k - n/2) + 1)2^{\frac{n}{2}-1}, & \text{if } n/2 \leq k \leq n \end{cases}$$

where $\delta(n, k) = \sum_{i=0}^{\lfloor k/4 \rfloor} \binom{n}{k-4i} + \sum_{i=0}^{\lfloor (k-1)/4 \rfloor} \binom{n}{k-1-4i}$ and $\epsilon(k) = \cos\left(\frac{k\pi}{2}\right) + \sin\left(\frac{k\pi}{2}\right)$. These results clarify some of the assertions made in a recent article of Yang and Chen concerning the efficiency of the XL algorithm in cryptography. (Received September 22, 2009)