Brickell, E. F.; **Moore, J. H.**

Some remarks on the Herlestam-Johannesson algorithm for computing logarithms over $GF(2^P)$. (English) Zbl 0554.12012

Advances in cryptology, Proc. Workshop, Santa Barbara/Calif. 1982, 15-19 (1983).

[For the entire collection see Zbl 0511.00040.]

Let t be a primitive element in $GF(2^p)$ and let α be expressed as $\sum_{i=0}^{n-1} a_i t^i$, where a_i is 0 or 1. Define the Hamming weight, HWT(α), as the number of non-zero a_i, and define MINHJ(α) as min HWT(β), where β belongs to the set $t^{-2^r}\alpha^{2^s}$ $(0 \leq r, s \leq p-1)$. *T. Herlestam* and *R. Johannesson* [BIT 21, 326-334 (1981; Zbl 0493.12023)], with a view to cryptanalysis of the Pohlig-Hellman algorithm [cf. *S. C. Pohling* and *M. E. Hellman*, IEEE Trans. Inf. Theory IT-24, 106-110 (1978; Zbl 0375.68023)], proposed an heuristic method of finding logarithms over $GF(2^p)$ that took fewer steps in practice than one would expect if HWT(α) and MINHJ(α) were independent.

In the present paper, to test this hypothesis of independence, the authors compute the probability that $MINHJ(\alpha) = 1$, given that $HWT(\alpha) = i$, for various polynomials that implement $GF(2^{31})$. Only for some polynomials does the assumption of independence appear to be supported. They report also that the assumption that the probability that $MINJ(\alpha) = j$ depends only on HWT(α) is somewhat suspect.

Reviewer: H.J.Godwin

MSC:

11T06 Polynomials over finite fields
94B35 Decoding
68Q25 Analysis of algorithms and problem complexity

Keywords:

cryptosystem; logarithms over finite fields; Hamming weight; cryptanalysis; Pohlig-Hellman algorithm