A Comment on "Property of finite fields and its Cryptographic application"

S. Murphy and C.J. Mitchell

Information Security Group
Royal Holloway
University of London
Egham, Surrey TW20 0EX, U.K.

Email: s.murphy@rhul.ac.uk

Abstract: The "new" property of finite fields given by Wei Baodian *et al.* is a well-known fundamental result in finite field theory.

The recent letter of Wei Baodian *et al.* [5] states that the authors have "found a new property of finite fields that has not been discussed in the classical works on finite fields (e.g. [1, 2])". Unfortunately, this so-called "new property" is a well-known basic property of finite fields, and the main result of the paper (Theorem 4) is an imprecise statement of a standard finite field result.

Suppose θ is a primitive element of the finite field $F = GF(p^n)$, an extension of degree n over $K = GF(p)$. Any element $x \in F$ can be expressed as $x = \sum_{i=0}^{n-1} x_i \theta^i$. The problem considered by Wei Baodian *et al.* [5] is the determination of a polynomial $G^i : GF(p^n) \to GF(p)$ such that $G^i(x) = x_i$ $(i = 0, \ldots, n-1)$. The authors claim this problem has not previously been discussed, and give a solution to this problem in their Theorem 4, the crux of their paper.

Theorem 4: $G^i(x)$ contains and only contains items of the form x^{p^k}, $k = 0, 1, \ldots, n-1$, i.e. $G^i(x) = \sum_{i=0}^{n-1} c_{i,d} x^{p^k}$.

However, this is a well-known result concerning the *trace* function. The *trace* function $Tr : F \to K$ is the sum of conjugates, so $Tr(z) = z + z^p + \ldots + z^{p^{n-1}}$, and is the fundamental additive mapping of the finite field F. Theorem 4 is the basic property of the trace function and is well-known. For example, Lidl and Niederreiter [1] give the following (paraphrased) result.

Theorem 2.24: Let $F = GF(p^n)$ be a finite extension of the finite field $K = GF(p)$, both considered as vector spaces over K. Then the linear transformations from F into K are exactly the mappings $L_\beta(x) = Tr(\beta x)$.

The mapping of $x = (x_{n-1}, \ldots, x_0) \in F$ to $x_i \in K$ is certainly a linear transformation from F to K. Thus Theorem 2.24 in one of the "classical works on finite fields" tells us that it can be expressed as a trace function, and so immediately gives Theorem 4 of Wei Baodian *et al.* [5] :

$$x_i = G^i(x) = Tr(\beta x) = \sum_{i=0}^{n-1} \beta^{p^i} x^{p^i} \text{ for some } \beta.$$

Indeed, the use of such a trace representation of a "component" of a finite field element is a basic technique for the analysis of stream ciphers based on linear feedback shift registers [3].

The observations of Wei Baodian *et al.* [5] about the Rijndael S-Box thus add nothing to the discussions of Murphy and Robshaw [4] concerning the $GF(2)$-linear mapping of the S-Box and its *linearized* interpolation polynomial.

Conclusion. The claim by the authors of [5] to have found a new finite field property is unfounded.

References

[1] R. Lidl and H. Niederreiter. 'Finite Fields'. Cambridge University Press (Revised Edition), 1994.

[2] R. J. McEliece. 'Finite Fields for Computer Scientists and Engineers'. Kluwer Academic, 1987.

[3] R. A. Rueppel. ‘Analysis and Design of Stream Ciphers’. Springer-Verlag, 1986.

[4] S. Murphy and M. J. B. Robshaw. ‘Essential Algebraic Structure within the AES’. Advances in Cryptology — Proc. of CRYPTO ’02, LNCS 2442, 1–16, Springer Verlag, 2002.

[5] Wei Baodian, Liu Dongsu, Ma Wenping and Wang Ximmei. ‘Property of finite fields and its cryptography application’. *Electronics Letters*, Vol. 39, pp. 655-656, 2003.