A Short Note on Irreducible Trinomials in Binary Fields

Mathieu Ciet*, Jean-Jacques Quisquater, and Francesco Sica*

Université catholique de Louvain, Crypto Group
Place du Levant, 3 1348 Louvain-la-Neuve, Belgium
{ciet, jjq, sica}@dice.ucl.ac.be – http://www.dice.ucl.ac.be/~crypto

1 Introduction

In this paper, we analyse the irreducibility of trinomials defined over $\mathbb{F}_2[X]$. For elliptic curve cryptography, prime extensions fields $\mathbb{F}_{2^p}$ are recommended to avoid current attacks like the Weil descent attack [3]. One often represents $\mathbb{F}_{2^p}$ as a quotient $\mathbb{F}_2[X]/(f(X))$, where f is an irreducible polynomial over $\mathbb{F}_2$ of degree p.

Performance reasons impose that irreducible polynomials have the shortest number of non zero terms. More precisely, the reduction polynomial plays a fundamental role in the basic field operations and particularly in modular reductions. This in turn is related to the number of carries in each modular reduction and this is where the structure of the polynomial plays a crucial role.

Recommended binary fields for elliptic curve cryptosystems, as in norms IEEEP1363, ANSI X9.62 or SEC1, are produced together with irreducible trinomials or pentanomials when no irreducible trinomials exist. However criteria for existence or non-existence of irreducible trinomials or pentanomials over given extensions are not clearly stated in the cryptographic literature (but cf. [4, § 4.5.2]).

The purpose of this short note is a first attempt to clarify some parts of this problem. We propose, following the work of [1, 6], to give a proof of the following theorem.

Main Theorem. *Let p be a prime, $p \equiv 13 \mod 24$ or $p \equiv 19 \mod 24$. Then there are no irreducible trinomials of degree p over $\mathbb{F}_2$. In particular, the quotient representation of 25% of all prime degree extensions of $\mathbb{F}_2$ has to use at least a pentanomial as a reduction polynomial.*

2 Proof of the Theorem

The proof relies on a theorem of Swan and Dalen [2, 6], originally due to Stickelberger [5]. We cite here a particular instance of the theorem.

* The work described in this paper has been supported by the European Commission through the IST Programme under Contract IST-1999-12324.

Theorem 1. *Let $f \in \mathbb{F}_q[X]$ be a squarefree polynomial over the finite field with q elements (q prime). Suppose f factors over $\mathbb{F}_q[X]$ into the product of r distinct irreducible factors. Let $F \in \mathbb{Z}[X]$ be a representative of f, that is $f = F \bmod q$. Then $\deg f - r$ is even if and only if $\operatorname{disc} F$ is a square $\bmod 4q$.*

By computing explicitly the value of the discriminant $\operatorname{disc} F$ in the case of trinomials, Swan was able to deduce the following theorem.

Theorem 2. *The polynomial $X^n + X^k + 1 \in \mathbb{F}_2[X]$ has an even number of irreducible factors if and only if*

1. *n is even, k is odd, $n \neq 2k$ and $nk/2 \equiv 0$ or $1 \mod 4$,*
2. *n is odd, k is even not dividing $2n$ and $n \equiv \pm 3 \mod 8$,*
3. *n is odd, k is even dividing $2n$ and $n \equiv \pm 1 \mod 8$,*
4. *one of the previous cases holds with k replaced by $n - k$.*

In particular if $n = p$ is a prime congruent to $\pm 3 \mod 8$, then $X^p + X^k + 1$ is irreducible implies that k or $n - k$ must be equal to 2. Since $X^p + X^k + 1$ and $X^p + X^{p-k} + 1$ both have the same number of factors, we see that we are reduced to examine the factorisation behaviour of $X^p + X^2 + 1$ (when $p \equiv \pm 3$ mod 8).

However, if $p \equiv 1 \mod 3$, it is immediate to see that $X^2 + X + 1$ divides $X^p + X^2 + 1$. Thus, for $p \equiv 13 \mod 24$ or $p \equiv 19 \mod 24$, polynomials of the form $X^p + X^k + 1$ are all reducible. The density of such p's is 1/4, by the prime number theorem for primes in arithmetic progressions. □

References

1. I.F. Blake, S. Gao, and R.L. Lambert. Construction and Distribution Problems for Irreducible Trinomials over Finite Fields. In D. Gollmann, editor, *Applications of Finite Fields*, Oxford-Clarendon Press, pages 19–32, 1996.
2. K. Dalen. On a theorem of Stickelberger. In *Math. Scand. 3*, pages 124–126, 1955.
3. P. Gaudry, F. Hess, and N.P. Smart. Constructive and Destructive Facets of Weil Descent on Elliptic Curves. *Journal of Cryptology*, 15(1):19–46, 2002.
4. A. J. Menezes, P. C. Van Oorshot, and S. C. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1997.
5. L. Stickelberger. Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper. In *Verh. 1 Internat. Math. Kongresses, Zürich 1897*, pages 182–193, Leipzig 1898.
6. R.G. Swan. Factorization of Polynomials over Finite Fields. In *Pac. J. Math.*, 19, pages 1099–1106, 1962.