A Note on Square Roots in Binary Fields

Roberto Maria Avanzi

Faculty of Mathematics and Horst Görtz Institute for IT-Security
Ruhr University Bochum, Germany
Roberto.Avanzi@ruhr-uni-bochum.de

Abstract. In this note we discuss a family of irreducible polynomials that can be used to speed up square root extraction in fields of characteristic two. This generalizes a family of trinomials discussed by Fong et al. and the results are not limited to trinomials. In fact, we show for the first time pentanomials (polynomials with five nonzero terms) and eptanomials (polynomials with seven nonzero terms) allowing fast square root computation. We call such polynomials *square root friendly*.
The obvious application is to point halving methods for elliptic curves and divisor halving methods for hyperelliptic curves.
We also note the existence of square root friendly trinomials of a given degree when we already know that an irreducible trinomial of the same degree exists, and formulate a conjecture on the degrees of the terms of square root friendly polynomials.

Keywords: *Binary fields, Polynomial basis, Square root extraction, Point and divisor halving.*

1 Introduction

The topic of this paper is square root extraction in binary fields. The seminal work [14] shows how to extract square roots very efficiently when the odd degree field extension of $\mathbb{F}_2$ is defined by a suitable irreducible trinomial.

If $p(X)$ is an irreducible polynomial of degree d used to define the extension field $\mathbb{F}_{2^d}/\mathbb{F}_2$, we consider the polynomial in X representing the square root of the image of X in $\mathbb{F}_{2^d}$. If this polynomial has low weight and/or degree, then general square roots can be extracted in $\mathbb{F}_{2^d}$ efficiently. We call such a polynomial $p(X)$ *square root friendly*. (The definition is not very precise because concrete bounds on weight and degree are not given.) In this paper we show sufficient conditions for an irreducible polynomial of odd degree d to yield a low weight $\sqrt{X}$. In particular, we give examples of pentanomials and eptanomials, but in at least one case, that of $\mathbb{F}_{2^{233}}$, that can be defined by trinomials, we show how one can perform square root computations even faster than in [14].

As the motivation comes from elliptic curve cryptography, in particular from point halving based methods for scalar multiplication, we begin in Section 2 by recalling point and divisor halving and how square root computations come into play. Then, in Section 3 our sufficient conditions are introduced. Square root friendly polynomials for several useful (and used in practice) binary fields are given in Section 4, together with a result about the existence of square root friendly trinomials, and a conjecture about the degrees of the non-leading terms of square root friendly polynomials.

2 Halving and Square Roots

2.1 Point and Divisor Halving

Let E be an elliptic curve defined over $\mathbb{F}_{2^d}$ by a *Weierstrass equation*

$$E \ : \ y^2 + xy = x^3 + ax^2 + b$$

with $a, b \in \mathbb{F}_{2^d}$ and having a subgroup $G \leq E(\mathbb{F}_{2^d})$ of large prime order.

Since computing the double of any given point P is the most common operation in a scalar multiplication performed by double-and-add methods, an important direction of research consists in optimizing doubling formulæ (for surveys on scalar multiplication methods and elliptic curve operations see, for example [6, Chs. 9 and 13] or [15, Ch. 3]).

Point halving [16, 21], on the other hand, consists in computing a point R whose double is P, i.e. such that $2R = P$. Being the inverse operation of the doubling, it is an automorphism of G. Therefore, given a point $P \in G$, there is a unique $R \in G$ such that $2R = P$.

In order to perform this operation one needs to solve a quadratic equation of the form $\lambda^2 + \lambda + c = 0$ for λ, extract a square root, perform two multiplications and some additions. We refer the reader to [16, 20, 21, 14] for details, including the usage of halving in place of doubling in scalar multiplication algorithms. Furthermore, there are two points R_1 and R_2 on the curve with $2R_1 = 2R_2 = P$, such that $R_1 - R_2$ is the unique point of order 2 of the curve. To determine which one is in G, an additional check involving a trace computation is required. Knudsen [16] and Schroeppel [20, 21] show how to perform all these operations. According to the analysis in [14], halving is about two times faster than doubling.

Birkner [10] has devised a divisor halving formula for genus two curves based on the doubling formulae by Lange and Stevens [18]. Birkner and Thériault [11] have dealt with genus three divisors. The performance of all

known halving formulæ depends (to a variable degree) on the performance of square root extraction. Further uses of point halving to speed up scalar multiplication on the special class of elliptic Koblitz Curves [17] are found in [5, 7] and [8].

2.2 Square Root Extraction

In what follows will be exclusively concerned with square root extraction for binary fields represented via a polynomial basis: Let $p(X)$ be an irreducible polynomial of *odd* degree d, and the field $\mathbb{F}_{2^d}$ be constructed as the quotient ring $\mathbb{F}_2[X]/(p(X))$. We identify X with its own image in $\mathbb{F}_{2^d}$.

The reason behind this is that in software applications it is customary to use a polynomial basis representation for the field extension $\mathbb{F}_{2^d}/\mathbb{F}_2$ instead of a normal basis [3], because in the latter representation the cost of a software multiplication is much higher than with a polynomial basis.

But, whereas with a normal basis a square root computation is just a shift of the bits internal representation of the field element by one position, matters are more complicated with polynomial bases.

In fact, even the cost of a squaring is no longer negligible. If $\alpha = \sum_{i=0}^{d-1} a_i X^i$ then $\alpha^2 = \sum_{i=0}^{d-1} a_i X^{2i}$ which, as a polynomial in X, has degree no longer necessarily bounded by d, and modular reduction modulo $p(X)$ is necessary. Its cost is very low, but cannot be completely ignored.

Things are even more complicated for square roots. Whereas squaring just consists in "spacing" the bits of the original element with zeros, the bits of a generic field element cannot be just "squeezed".

The classic method for computing $\sqrt{\alpha}$ is based on Fermat's little theorem $\alpha^{2^d} = \alpha$, hence $\sqrt{\alpha} = \alpha^{2^{d-1}}$. This requires $d-1$ squarings. In general, the cost of this operation is that of several field multiplications.

A more efficient method stems from the observation that $\sqrt{\alpha}$ can be expressed in terms of $\zeta := \sqrt{X}$. If

$$\alpha = \sum_{i=0}^{d-1} a_i X^i$$

we separate the even exponents from the odd exponents

$$\alpha = \sum_{i=0}^{\frac{d-1}{2}} a_{2i} X^{2i} + \sum_{i=0}^{\frac{d-3}{2}} a_{2i+1} X^{2i+1} = \sum_{i=0}^{\frac{d-1}{2}} a_{2i} X^{2i} + X \cdot \sum_{i=0}^{\frac{d-3}{2}} a_{2i+1} X^{2i}$$

and, since square root extraction in fields of even characteristic is a linear operation:

$$\sqrt{\alpha} = \sum_{i=0}^{\frac{d-1}{2}} a_{2i} X^i + \zeta \cdot \sum_{i=0}^{\frac{d-3}{2}} a_{2i+1} X^i \ . \tag{1}$$

Therefore, once ζ has been computed on a per-field basis, the computation of a generic square root is reduced to "bits extraction and packing", a "rectangular" multiplication of a degree $\leq d-1$ polynomial ζ with a polynomial $\sum_{i=0}^{(d-3)/2} a_{2i+1} X^i$ of degree $\leq (d-1)/2$, and a modular reduction. Intuitively, the cost should approach a half of the cost of a field multiplication, and this is confirmed by the analysis in [14, 16].

3 Some Square-Root Friendly Polynomials

As we have just seen, efficient square root computation depends on the efficiency of the multiplication of a generic degree $\leq (d-1)/2$ polynomial by $\zeta = \sqrt{X}$. If ζ is a very sparse element, for example of weight two or four (i.e. it has just two or four nonzero terms), then this product can be computed by a few shift and XOR operations. In [14] two types of trinomials have been shown that allow this. The kind that interests us is

$$p(X) = X^d + X^m + 1$$

with m odd. Then $X = X^{d+1} + X^{m+1}$ with $d+1$ and $m+1$ even, and

$$\zeta = X^{(d+1)/2} + X^{(m+1)/2} \ ,$$

and $p(X)$ is square root friendly. In fact, this idea is much more general.

Assume we have an irreducible polynomial $p(X)$ defining $\mathbb{F}_{2^d}$ over $\mathbb{F}_2$ of form

$$p(X) = X \cdot \mathcal{U}(X)^2 + 1 \tag{2}$$

where $\mathcal{U}$ is a polynomial of degree $(d-1)/2$ and even weight. Then, ζ has a very simple form in $\mathbb{F}_{2^d}$: from

$$X^2 \cdot \mathcal{U}(X)^2 + X = 0$$

we obtain

$$\zeta = X \cdot \mathcal{U}(X) \ ,$$

and ζ is represented by a polynomial of degree $1 + \frac{d-1}{2} = \frac{d+1}{2}$ in X.

Note at this point that the *polynomial* product

$$\zeta \cdot \sum_{i=0}^{\frac{d-3}{2}} a_{2i+1} X^i$$

has degree bounded by $\frac{d+1}{2} + \frac{d-3}{2} = d-1$, therefore *no polynomial reduction is required.*

Hence, irreducible polynomials of form (2) are square root friendly.

Definition. *An irreducible polynomial of form* (2) *is called a* special square root friendly polynomial.

We do not know whether there are irreducible polynomials which are not trinomials, not of form (2), and for which $\sqrt{X}$ has small weight. For trinomials $X^d + X^m + 1$ with even m one has to check on a case by case basis [14].

However, examples of special square root friendly polynomials abound. For example $X^{163} + X^{65} + X^{35} + X^{33} + 1$ is irreducible, and under this representation ζ has weight 4. On the other hand, the standard NIST polynomial [19] $X^{163} + X^7 + X^6 + X^3 + 1$ defines a ζ of weight 79. Changing polynomial is in fact easy without introducing incompatibilities in the practical use: we just change the base used for representation of the field elements before and after the whole scalar multiplication. The cost is comparable to a polynomial basis multiplication, and the conversion routines require each a matrix that occupies $O(d^2)$ bits of storage (see for instance [13], where the particular base change is to and from a normal basis representation, but the results are the same). Therefore this overhead is essentially negligible with respect to the full cost of the scalar multiplication that is in the order of magnitude of hundreds to thousands of field multiplications (see for example § 5.3 of [4]). The bulk of the computation is then performed in the "easy" representation, the inputs and outputs are given in the "standard" representation.

The cost of a square root extraction implemented by using the sparse version of ζ offered by the above polynomials can be roughly estimated using, for example, already published results. For example in [14], Example 3.12, the NIST-recommended trinomial

$$p(X) = X^{233} + X^{74} + 1$$

for the finite field $\mathbb{F}_{2^{233}}$ is used. Even though the term X^{74} does not have an even exponent, ζ has a sparse representation

$$\zeta = (X^{32} + X^{117} + X^{191})(X^{37} + 1) \ .$$

By means of this representation, finding a root via equation (1) requires roughly 1/8 of the time of a field multiplication. As we shall show in the next section we can choose

$$p(X) = X^{233} + X^{159} + 1$$

and in this case

$$\zeta = X^{117} + X^{80} \ .$$

In this case it is clear that much smaller amount of shift operations and XOR operations are required to multiply by ζ. Furthermore, as already remarked, there is no need to perform a reduction modulo $p(X)$ while with the standard polynomial this is in many cases (such as the one depicted above for $\mathbb{F}_{2^{233}}$) necessary. First implementation results show the cost of a square root to be about 8% of that of a multiplication.

Similar formulæ for cube root computations are found in [1] – their results are easily partially generalised to any odd characteristic.

4 Existence and other Properties

Square root friendly polynomials are easy to find. For example, for extension degree $d = 163$, a simple computer program immediately yields several examples.

In Table 1 we list *special* square root friendly polynomials of several degrees. The degrees have been taken from the NIST list of recommended binary curves and from the extension degrees used in [9]. All these extension degrees are interesting because they are either used in standards for elliptic curve cryptography or they represent good choices for extension degrees for defining hyperelliptic curve for cryptographic applications.

When no trinomial is available, a pentanomial is used. We always report the polynomial with least degree sediment (the sediment of an univariate polynomial is the polynomial itself with the leading term removed). In particular, observe that also efficient trinomials are available. Only in a handful of cases is the special square root friendly polynomial with least degree sediment the same as the standard one, i.e. the irreducible polynomial with least degree sediment but without the restriction on being square root friendly.

For the extension degrees for which there are no trinomials we have computed also the special square root friendly eptanomials with smallest

Degree	Irreducible tri/pentanomial	$\zeta = \sqrt{X}$	Standard?
47	$X^{47} + X^5 + 1$	$X^{24} + X^3$	Yes
53	$X^{53} + X^{19} + X^{17} + X^{15} + 1$	$X^{27} + X^{10} + X^9 + X^8$	No
59	$X^{59} + X^{21} + X^{17} + X^{15} + 1$	$X^{30} + X^{11} + X^9 + X^8$	No
67	$X^{67} + X^{25} + X^{17} + X^5 + 1$	$X^{34} + X^{13} + X^9 + X^3$	No
71	$X^{71} + X^9 + 1$	$X^{36} + X^5$	No
73	$X^{73} + X^{25} + 1$	$X^{37} + X^{13}$	Yes
79	$X^{79} + X^9 + 1$	$X^{40} + X^5$	Yes
83	$X^{83} + X^{29} + X^{25} + X^3 + 1$	$X^{42} + X^{15} + X^{13} + X^2$	No
89	$X^{89} + X^{51} + 1$	$X^{45} + X^{26}$	No
97	$X^{97} + X^{33} + 1$	$X^{49} + X^{17}$	No
101	$X^{101} + X^{35} + X^{31} + X^3 + 1$	$X^{51} + X^{18} + X^{16} + X^2$	No
107	$X^{107} + X^{37} + X^{33} + X^{23} + 1$	$X^{54} + X^{19} + X^{17} + X^{12}$	No
109	$X^{109} + X^{43} + X^{41} + X^{23} + 1$	$X^{55} + X^{22} + X^{21} + X^{12}$	No
127	$X^{127} + X + 1$	$X^{64} + X$	Yes
131	$X^{131} + X^{45} + X^{41} + X^9 + 1$	$X^{66} + X^{23} + X^{21} + X^5$	No
137	$X^{137} + X^{21} + 1$	$X^{69} + X^{11}$	Yes
139	$X^{139} + X^{53} + X^{33} + X^{25} + 1$	$X^{70} + X^{27} + X^{17} + X^{13}$	No
149	$X^{149} + X^{51} + X^{47} + X^9 + 1$	$X^{75} + X^{26} + X^{24} + X^5$	No
157	$X^{157} + X^{55} + X^{47} + X^{11} + 1$	$X^{79} + X^{28} + X^{24} + X^6$	No
163	$X^{163} + X^{57} + X^{49} + X^{29} + 1$	$X^{82} + X^{29} + X^{25} + X^{15}$	No
179	$X^{179} + X^{61} + X^{57} + X^{41} + 1$	$X^{90} + X^{31} + X^{29} + X^{21}$	No
199	$X^{199} + X^{67} + 1$	$X^{100} + X^{34}$	No
211	$X^{211} + X^{73} + X^{69} + X^{35} + 1$	$X^{106} + X^{37} + X^{35} + X^{18}$	No
233	$X^{233} + X^{159} + 1$	$X^{117} + X^{80}$	No
239	$X^{239} + X^{81} + 1$	$X^{120} + X^{41}$	No
251	$X^{251} + X^{89} + X^{81} + X^3 + 1$	$X^{126} + X^{45} + X^{41} + X^2$	No
269	$X^{269} + X^{91} + X^{87} + X^{61} + 1$	$X^{135} + X^{46} + X^{44} + X^{31}$	No
283	$X^{283} + X^{97} + X^{89} + X^{87} + 1$	$X^{142} + X^{49} + X^{45} + X^{44}$	No
409	$X^{409} + X^{87} + 1$	$X^{205} + X^{44}$	Yes
571	$X^{571} + X^{193} + X^{185} + X^5 + 1$	$X^{286} + X^{97} + X^{93} + X^3$	No

Table 1. Some special square root friendly trinomials and pentanomials.

degree sediment – the idea was, that perhaps one can find good eptanomials with a sediment of significantly lower degree than the best pentanomials, to improve modular reduction. These eptanomials are given in Table 2. The interesting observation here seems to be that sediment degree differences are very limited, so the eptanomials do not bring advantages.

Theorem. *Let d be an odd positive integer. If an irreducible trinomial $p(X)$ over $\mathbb{F}_2$ of degree d exists, then $p(X)$ can be chosen of form* (2)*, i.e. where all the non-vanishing exponents are odd.*

Proof. Let

$$X^d + X^m + 1$$

Degree	Irreducible eptanomial	$\zeta = \sqrt{X}$
53	$X^{53} + X^{19} + X^{15} + X^5 + X^3 + X + 1$	$X^{27} + X^{10} + X^8 + X^3 + X^2 + X$
59	$X^{59} + X^{21} + X^{17} + X^{13} + X^3 + X + 1$	$X^{30} + X^{11} + X^9 + X^7 + X^2 + X$
67	$X^{67} + X^{25} + X^{17} + X^7 + X^3 + X + 1$	$X^{34} + X^{13} + X^9 + X^4 + X^2 + X$
83	$X^{83} + X^{29} + X^{25} + X^7 + X^5 + X^3 + 1$	$X^{42} + X^{15} + X^{13} + X^4 + X^3 + X^2$
101	$X^{101} + X^{35} + X^{31} + X^9 + X^7 + X + 1$	$X^{51} + X^{18} + X^{16} + X^5 + X^4 + X$
107	$X^{107} + X^{37} + X^{33} + X^{15} + X^9 + X^7 + 1$	$X^{54} + X^{19} + X^{17} + X^8 + X^5 + X^4$
109	$X^{109} + X^{39} + X^{31} + X^9 + X^5 + X^3 + 1$	$X^{55} + X^{20} + X^{16} + X^5 + X^3 + X^2$
131	$X^{131} + X^{45} + X^{41} + X^{13} + X^9 + X + 1$	$X^{66} + X^{23} + X^{21} + X^7 + X^5 + X$
139	$X^{139} + X^{49} + X^{41} + X^7 + X^5 + X^3 + 1$	$X^{70} + X^{25} + X^{21} + X^4 + X^3 + X^2$
149	$X^{149} + X^{51} + X^{47} + X^9 + X^7 + X + 1$	$X^{75} + X^{26} + X^{24} + X^5 + X^4 + X$
157	$X^{157} + X^{55} + X^{47} + X^{15} + X^9 + X^3 + 1$	$X^{79} + X^{28} + X^{24} + X^8 + X^5 + X^2$
163	$X^{163} + X^{57} + X^{49} + X^{15} + X^9 + X + 1$	$X^{82} + X^{29} + X^{25} + X^8 + X^5 + X$
179	$X^{179} + X^{61} + X^{57} + X^{13} + X^9 + X^5 + 1$	$X^{90} + X^{31} + X^{29} + X^7 + X^5 + X^3$
211	$X^{211} + X^{73} + X^{65} + X^{13} + X^{11} + X^3 + 1$	$X^{106} + X^{37} + X^{33} + X^7 + X^6 + X^2$
251	$X^{251} + X^{85} + X^{81} + X^7 + X^5 + X^3 + 1$	$X^{126} + X^{43} + X^{41} + X^4 + X^3 + X^2$
269	$X^{269} + X^{91} + X^{87} + X^{15} + X^{13} + X^{11} + 1$	$X^{135} + X^{46} + X^{44} + X^8 + X^7 + X^6$
283	$X^{283} + X^{97} + X^{89} + X^{13} + X^9 + X + 1$	$X^{142} + X^{49} + X^{45} + X^7 + X^5 + X$
571	$X^{571} + X^{193} + X^{185} + X^{15} + X^{11} + X^3 + 1$	$X^{286} + X^{97} + X^{93} + X^8 + X^6 + X^2$

Table 2. Some special square root friendly eptanomials.

be an irreducible trinomial with $d > m > 0$ and m even. Then it is easy to prove that the polynomial

$$X^d + X^{d-m} + 1$$

is also irreducible – but $d - m$ is odd. In fact, let $q(X)$ be a monic polynomial over $\mathbb{F}_2$ with $q(X) = 1$, i.e. non-vanishing constant term. Define

$$\hat{q}(X) = X^{\deg q} q(X^{-1})$$

to be the *inversion* of $q(X)$. It ie easy to see that $\hat{q}(X)$ is a monic polynomial with non-vanishing constant term. Then, a factorization $q(X) = g(X)h(X)$ implies $\hat{q}(X) = \hat{g}(X)\hat{h}(X)$. Applying this result to $q(X) = X^d + X^{d-m} + 1$ proves that it must be irreducible, otherwise $p(X) = \hat{q}(X)$ would be reducible, too. □

Existence results for pentanomial-defined fields are still an open question. However, on the basis of the above table and further experimental results, we found further evidence for an observation of Ahmadi and Menezes: In [2] they list irreducible pentanomials $p(X)$ having only non-constant terms with odd exponent for which the sediment has lowest degree, and observe that if $d \equiv \pm 3 \pmod 8$, the degree of the sediment

is at least $d/3$, whereas if $d \equiv \pm 1 \pmod 8$, then the degree of the sediment is usually quite small. In fact, if a trinomial exists for degree d, then a special square-root friendly polynomial (even a pentanomial) with a rather low degree sediment usually exists. Furthermore a pattern in the distribution of degrees of the second term of the sediment can be observed.

Conjecture. *Let d be an odd natural integer, and c be the minimum of the degrees of the sediments of all special square root friendly polynomials of degree d. Further, let c' be the minimum of the degrees of the second highest degree terme of all the sediments of degree c of special square root friendly polynomials of degree d. Then*

$$3\,c - d = c - c' = \begin{cases} 8 & \text{if } d \equiv 1 \pmod 3 \\ 4 & \text{if } d \equiv 2 \pmod 3 \end{cases} .$$

A first result in this direction has already been proved by Bluher [12] using a result of Swan [22] (that in fact goes back to Stickelberger). Her result is: *The odd degree polynomial $f(X) = X^d + \sum_{i \in \mathcal{S}} X^i + 1$ in $\mathbb{F}_2[X]$, where $\mathcal{S} \subset \{i : i \text{ odd}, 0 < i < d/3\} \cup \{i : i \equiv d \pmod 4, 0 < i < d\}$ has no repeated roots; if $d = \pm 1 \pmod 8$, then f has an odd number of irreducible factors; and if $d = \pm 3 \pmod 8$, then f has an even number of irreducible factors.*

We also observe that these polynomials enjoy another very useful property. In [2] it is proved: *If $\mathbb{F}_{2^d}$ is defined by an irreducible polynomial $p(X)$ whose non constant terms all have odd exponents, then the trace of a field element α represented as $\sum_{i=0}^{d-1} a_i X^i$ with respect to the polynomial basis induced by $p(X)$ is its constant term a_0.* In other words, the only trace-one element in the polynomial basis defined by $p(X)$ is 1. This is very important in the applications: for instance, as remarked in § 2, a trace computation is necessary to correctly halve a point. It is especially fortunate that the same family of polynomials makes square roots and trace computations faster.

In Conjecture 6 of [2] the authors also speculate that if an irreducible pentanomial of degree d exists, then an irreducible pentanomial of the same degree defining a polynomial basis with only one trace-one element also exists. In the similar vein we could try to restrict our own conjecture to pentanomials, but we have the following example for degree 1987:

$$X^{1987} + X^{665} + X^{661} + X^{549} + 1 \ .$$

This polynomial has minimal degree sediment, and the sediment has minimal degree second term among all irreducible pentanomials. We have $d \equiv 1 \pmod 3$ and $3c - d = 8$, but the second term of the sediment has degree 661, not 657. On the other hand, with eptanomials we find following irreducible

$$X^{1987} + X^{665} + X^{657} + X^{25} + X^{21} + X^9 + 1 \ ,$$

and we know of no other irreducibles of the form

$$X^{1987} + X^c + X^{c'} + \ \textit{other lower odd degree terms} \ + 1$$

with c smaller than 665 or with $c = 665$ and c' smaller than 657.

Further open questions are: how to find polynomials like the above that are also efficient for almost-inverse computations; to balance the possibly increased modular reduction cost with the savings obtained in other parts of the computations. These will be the subject of future work.

Acknowledgement. *The author is grateful to Darrel Hankerson and Alfred Menezes for fruitful conversations on the matter in the month of March, 2005, to Nicolas Thériault and Peter Birkner for further discussions on the matter during a stay at the Fields Institute, Toronto, in September, 2006, and to Toni Bluher for very informative email exchanges during the Spring of 2007.*

References

1. O. Ahmadi, D. Hankerson, and A. Menezes. *Formulas for cube roots in $\mathbb{F}_{3^m}$.* Discrete Applied Math. **155** (3), 260–270, 2007.
2. O. Ahmadi, and A. Menezes. *On the number of trace-one elements in polynomial bases for $\mathbb{F}_{2^n}$.* Designs, Codes and Cryptography, **37**, 493-507, 2005.
3. D. W. Ash, I. F. Blake and S. Vanstone. *Low complexity normal bases.* Discrete Applied Math. **25** 191–210, 1989.
4. R. M. Avanzi. *Delaying and Merging Operations in Scalar Multiplication: Applications to Curve-Based Cryptosystems.* To appear in proceedings of SAC 2006.
5. R. M. Avanzi, M. Ciet, and F. Sica. *Faster Scalar Multiplication on Koblitz Curves combining Point Halving with the Frobenius Endomorphism.* Proceedings of PKC 2004, LNCS **2947**, 28–40. Springer–Verlag, 2004.
6. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. *The Handbook of Elliptic and Hyperelliptic Curve Cryptography.* CRC Press, 2005.
7. R. M. Avanzi, C. Heuberger, and H. Prodinger. *Scalar Multiplication on Koblitz Curves Using the Frobenius Endomorphism and its Combination with Point Halving: Extensions and Mathematical Analysis.* Algorithmica **46** (2006), 249–270
8. R. M. Avanzi, C. Heuberger, and H. Prodinger. *On Redundant τ-adic Expansions and Non-Adjacent Digit Sets.* To appear in proceedings of SAC 2006.
9. R. M. Avanzi, N. Thériault, and Z. Wang. *Rethinking Low Genus Hyperelliptic Jacobian Arithmetic over Binary Fields: Interplay of Field Arithmetic and Explicit Formulæ.* CACR Technical Report 2006-07.

10. P. Birkner. *Efficient Divisor Class Halving on Genus Two Curves.* To appear in: Proceedings of Selected Areas in Cryptography – SAC 2006. Springer Verlag LNCS.
11. P. Birkner, and N. Thériault. *Efficient Divisor Class Doubling and Halving on Genus Three Curves.* In preparation.
12. A.W. Bluher. *A Swan-like Theorem.* Finite Fields and Their Applications **12**, 128–138, 2006.
13. J.-S. Coron, D. M'Raïhi, and C. Tymen. *Fast generation of pairs* $(k, [k]P)$ *for Koblitz elliptic curves.* In: *Proceedings of SAC 2001*, LNCS **2259**, 151–164. Springer, 2001.
14. K. Fong, D, Hankerson, J, López, A, Menezes:. *Field Inversion and Point Halving Revisited.* IEEE Trans. Computers 53(8), 1047–1059, 2004.
15. D. Hankerson, A. J. Menezes, and S. A. Vanstone. *Guide to elliptic curve cryptography.* Springer–Verlag, 2003.
16. E. W. Knudsen. *Elliptic Scalar Multiplication Using Point Halving.* Proocedings of ASIACRYPT 1999, LNCS **1716**, 135–149. Springer, 1999.
17. N. Koblitz. *CM-curves with good cryptographic properties.* In: *Proceedings of CRYPTO 1991*, LNCS **576**, 279–287. Springer, 1991.
18. T. Lange and M. Stevens. *Efficient doubling for genus two curves over binary fields.* In: *Selected Areas in Cryptography – SAC 2004.* LNCS **3357**, 170–181, Springer-Verlag, 2005.
19. National Institute of Standards and Technology. *Recommended Elliptic Curves for Federal Government Use.* NIST Special Publication, July 1999.
Available from: `http://csrc.nist.gov/csrc/fedstandards.html`
20. R. Schroeppel. *Point halving wins big.* Talks at: (i) Midwest Arithmetical Geometry in Cryptography Workshop, November 17–19, 2000, University of Illinois at Urbana-Champaign; and (ii) ECC 2001 Workshop, October 29–31, 2001, University of Waterloo, Ontario, Canada.
21. R. Schroeppel. *Elliptic curve point ambiguity resolution apparatus and method.* International Application Number PCT/US00/31014, filed 9 November 2000.
22. R.G. Swan. *Factorization of Polynomials over Finite Fields.* In Pac. J. Math. **19**, 1099–1106, 1962.