Extended Double-Base Number System with applications to Elliptic Curve Cryptography

Christophe Doche[1] and Laurent Imbert[2]

[1] Department of Computing
Macquarie University, Australia
doche@ics.mq.edu.au
[2] LIRMM, CNRS, Université Montpellier 2, UMR 5506, France
& ATIPS, CISaC, University of Calgary, Canada
Laurent.Imbert@lirmm.fr

Abstract. We investigate the impact of larger digit sets on the length of Double-Base Number system (DBNS) expansions. We present a new representation system called *extended DBNS* whose expansions can be extremely sparse. When compared with double-base chains, the average length of extended DBNS expansions of integers of size in the range 200–500 bits is approximately reduced by 20% using one precomputed point, 30% using two, and 38% using four. We also discuss a new approach to approximate an integer n by $d2^a3^b$ where d belongs to a given digit set. This method, which requires some precomputations as well, leads to realistic DBNS implementations. Finally, a left-to-right scalar multiplication relying on extended DBNS is given. On an elliptic curve where operations are performed in Jacobian coordinates, improvements of up to 13% overall can be expected with this approach when compared to window NAF methods using the same number of precomputed points. In this context, it is therefore the fastest method known to date to compute a scalar multiplication on a generic elliptic curve.

Keywords. Double-base number system, Elliptic curve cryptography.

1 Introduction

Curve-based cryptography, especially elliptic curve cryptography, has attracted more and more attention since its introduction about twenty years ago [1–3], as reflected by the abundant literature on the subject [4–7]. In curve-based cryptosystems, the core operation that needs to be optimized as much as possible is a scalar multiplication. The standard method, based on ideas well known already more than two thousand years ago, to efficiently compute such a multiplication is the double-and-add method, whose complexity is linear in terms of the size of the input. Several ideas have been introduced to improve this method; see [8] for an overview. In the remainder, we will mainly focus on two approaches:

- Use a representation such that the expansion of the scalar multiple is sparse. For instance, the non-adjacent form (NAF) [9] has a non-zero digit density of

1/3 whereas the average density of a binary expansion is 1/2. This improvement is mainly obtained by adding -1 to the set $\{0, 1\}$ of possible coefficients used in binary notation. Another example is the double-base number system (DBNS) [10], in which an integer is represented as a sum of products of powers of 2 and 3. Such expansions can be extremely sparse, *cf.* Section 2.
- Introduce precomputations to enlarge the set of possible coefficients in the expansion and reduce its density. The k-ary and sliding window methods as well as window NAF methods [11, 12] fall under this category.

In the present work, we mix these two ideas. Namely, we investigate how precomputations can be used with the DBNS and we evaluate their impact on the overall complexity of a scalar multiplication.

Also, computing a sparse DBNS expansion can be very time-consuming although it is often neglected when compared with other representations. We introduce several improvements that considerably speed up the computation of a DBNS expansion, *cf.* Section 4.

The plan of the paper is as follows. In Section 2, we recall the definition and basic properties of the DBNS. In Section 3, we describe how precomputations can be efficiently used with the DBNS. Section 4 is devoted to implementation aspects and explains how to quickly compute DBNS expansions. In Section 5, we present a series of tests and comparisons with existing methods before concluding in Section 6.

2 Overview of the DBNS

In the *Double-Base Number System*, first considered by Dimitrov *et al.* in a cryptographic context in [13], any positive integer n is represented as

$$n = \sum_{i=1}^{\ell} d_i 2^{a_i} 3^{b_i}, \text{ with } d_i \in \{-1, 1\}. \tag{1}$$

This representation is obviously not unique and is in fact highly redundant. Given an integer n, it is straightforward to find a DBNS expansion using a greedy-type approach. Indeed, starting with $t = n$, the main task at each step is to find the $\{2, 3\}$-integer z that is the closest to t (i.e. the integer z of the form $2^a 3^b$ such that $|t - z|$ is minimal) and then set $t = t - z$. This is repeated until t becomes 0. See Example 2 for an illustration.

Remark 1. *Finding the best $\{2, 3\}$-approximation of an integer t in the most efficient way is an interesting problem on its own. One option is to scan all the points with integer coordinates near the line $y = -x \log_3 2 + \log_3 t$ and keep only the best approximation. A much more sophisticated method involves continued fractions and Ostrowski's number system, cf. [14]. It is to be noted that these methods are quite time-consuming. See Section 4 for a more efficient approach.*

Example 2. *Take the integer $n = 841232$. We have the sequence of approximations*

$$\begin{aligned} 841232 &= 2^7 3^8 + 1424, \\ 1424 &= 2^1 3^6 - 34, \\ 34 &= 2^2 3^2 - 2. \end{aligned}$$

As a consequence, $841232 = 2^7 3^8 + 2^1 3^6 - 2^2 3^2 + 2^1$.

It has been shown that every positive integer n can be represented as the sum of at most $O\big(\frac{\log n}{\log \log n}\big)$ signed $\{2, 3\}$-integers. For instance, see [13] for a proof. Note that the greedy approach above-mentioned is suitable to find such short expansions.

This initial class of DBNS is therefore very sparse. When one endomorphism is virtually free, like for instance triplings on supersingular curves defined over $\mathbb{F}_3$, the DBNS can be used to efficiently compute $[n]P$ with $\max a_i$ doublings, a very low number of additions, and the necessary number of triplings [15]. Note that this idea has recently been extended to Koblitz curves [16]. Nevertheless, it is not really suitable to compute scalar multiplications in general. For generic curves where both doublings and triplings are expensive, it is essential to minimize the number of applications of these two endomorphisms. Now, one needs at least $\max a_i$ doublings and $\max b_i$ triplings to compute $[n]P$ using (1). However, given the DBNS expansion of n returned by the greedy approach, it seems to be highly non-trivial, if not impossible, to attain these two lower bounds simultaneously.

So, for generic curves the DBNS needs to be adapted to compete with other methods. The concept of *double-base chain*, introduced in [17], is a special type of DBNS. The idea is still to represent n as in (1) but with the extra requirements $a_1 \geqslant a_2 \geqslant \cdots \geqslant a_\ell$ and $b_1 \geqslant b_2 \geqslant \cdots \geqslant b_\ell$. These properties allow to compute $[n]P$ from right-to-left very easily. It is also possible to use a Horner-like scheme that operates from left-to-right. These two methods are illustrated after Example 3.

Note that, it is easy to accommodate these requirements by restraining the search of the best exponents (a_{j+1}, b_{j+1}) to the interval $[0, a_j] \times [0, b_j]$.

Example 3. *A double-base chain of n can be derived from the following sequence of equalities:*

$$\begin{aligned} 841232 &= 2^7 3^8 + 1424, \\ 1424 &= 2^1 3^6 - 34, \\ 34 &= 3^3 + 7, \\ 7 &= 3^2 - 2, \\ 2 &= 3^1 - 1. \end{aligned}$$

As a consequence, $841232 = 2^7 3^8 + 2^1 3^6 - 3^3 - 3^2 + 3^1 - 1$.

In that particular case, the length of this double-base chain is strictly bigger than the one of the DBNS expansion in Example 2. This is true in general as well and the difference can be quite large. It is not known whether the bound $O\left(\frac{\log n}{\log \log n}\right)$ on the number of terms is still valid for double-base chains.

However, computing $[841232]P$ is now a trivial task. From right-to-left, we need two variables. The first one, T being initialized with P and the other one, S set to point at infinity. The successive values of T are then P, $[3]P$, $[3^2]P$, $[3^3]P$, $[2^1 3^6]P$, and $[2^7 3^8]P$, and at each step T is added to S. Doing that, we obtain $[n]P$ with 7 doublings, 8 triplings, and 5 additions. To proceed from left-to-right, we notice that the expansion that we found can be rewritten as

$$841232 = 3\big(3\big(3\big(2^1 3^3 (2^6 3^2 + 1) - 1\big) - 1\big) + 1\big) - 1,$$

which implies that

$$[841232]P = [3]\big([3]\big([3]\big([2^1 3^3]([2^6 3^2]P + P) - P\big) - P\big) + P\big) - P.$$

Again, 7 doublings, 8 triplings, and 5 additions are necessary to obtain $[n]P$.

More generally, one needs exactly a_1 doublings and b_1 triplings to compute $[n]P$ using double-base chains. The value of these two parameters can be optimized depending on the size of n and the respective complexities of a doubling and a tripling (see Figure 2).

To further reduce the complexity of a scalar multiplication, one option is to reduce the number of additions, that is to minimize the density of DBNS expansions. A standard approach to achieve this goal is to enlarge the set of possible coefficients, which ultimately means using precomputations.

3 Precomputations for DBNS scalar multiplication

We suggest to use precomputations in two ways. The first idea, which applies only to double-base chains, can be viewed as a two-dimensional window method.

3.1 Window method

Given integers w_1 and w_2, we represent n as in (1) but with coefficients d_i in the set $\{\pm 1, \pm 2^1, \pm 2^2, \dots, \pm 2^{w_1}, \pm 3^1, \pm 3^2, \dots, \pm 3^{w_2}\}$. This is an indirect way to relax the conditions $a_1 \geqslant a_2 \geqslant \cdots \geqslant a_\ell$ and $b_1 \geqslant b_2 \geqslant \cdots \geqslant b_\ell$ in order to find better approximations and hopefully sparser expansions. This method, called (w_1, w_2)-*double-base chain*, lies somewhere between normal DBNS and double-base chain methods.

Example 4. *The DBNS expansion of* $841232 = 2^7 3^8 + 2^1 3^6 - 2^2 3^2 + 2^1$, *can be rewritten as* $841232 = 2^7 3^8 + 2^1 3^6 - \mathbf{2} \times 2^1 3^2 + 2^1$, *which is a* $(1, 0)$*-window-base chain. The exponent* a_3 *that was bigger than* a_2 *in Example 2 has been replaced by* a_2 *and the coefficient* d_3 *has been multiplied by* 2 *accordingly. As a result, we now have two decreasing sequences of exponents and the expansion is only four terms long.*

It remains to see how to compute $[841232]P$ from this expansion. The right-to-left scalar multiplication does not provide any improvement, but this is not the case for the left-to-right approach. Namely, writing

$$841232 = 2\bigl(3^2\bigl(3^4(2^6 3^2 + 1) - 2\bigr) + 1\bigr),$$

we see that

$$[841232]P = [2]\bigl([3^2]\bigl([3^4]([2^6 3^2]P + P) - [2]P\bigr) + P\bigr).$$

If $[2]P$ is stored along the computation of $[2^6 3^2]P$ then 7 doublings, 8 triplings and only 3 additions are necessary to obtain $[841232]P$.

It is straightforward to design an algorithm to produce (w_1, w_2)-double-base chains. We present a more general version in the following, *cf.* Algorithm 1. See Remark 6 (v) for specific improvements to (w_1, w_2)-double-base chains.

Also a left-to-right scalar multiplication algorithm can easily be derived from this method, *cf.* Algorithm 2.

The second idea to obtain sparser DBNS expansions is to generalize the window method such that any set of coefficients is allowed.

3.2 Extended DBNS

In a (w_1, w_2)-double-base chain expansion, the coefficients are signed powers of 2 or 3. Considering other sets $\mathcal{S}$ of coefficients, for instance odd integers coprime with 3, should further reduce the average length of DBNS expansions. We call this approach *extended DBNS* and denote it by $\mathcal{S}$-DBNS.

Example 5. *We have* $841232 = 2^7 3^8 + \mathbf{5} \times 2^5 3^2 - 2^4$. *The exponents form two decreasing sequences, but the expansion has only three terms. Assuming that* $[5]P$ *is precomputed, it is possible to obtain* $[841232]P$ *as*

$$[2^4]\bigl([2^1 3^2]([2^4 3^6]P + [5]P) - P\bigr)$$

with 7 *doublings,* 8 *triplings, and only* 2 *additions*

This strategy applies to any kind of DBNS expansion. In the following, we present a greedy-type algorithm to compute extended double-base chains.

Algorithm 1. Extended double-base chain greedy algorithm

INPUT: A positive integer n, a parameter a_0 such that $a_0 \leqslant \lceil \log_2 n \rceil$, and a set $\mathcal{S}$ containing 1.

OUTPUT: Three sequences $(d_i, a_i, b_i)_{1 \leqslant i \leqslant \ell}$ such that $n = \sum_{i=1}^{\ell} d_i 2^{a_i} 3^{b_i}$ with $|d_i| \in \mathcal{S}$, $a_1 \geqslant a_2 \geqslant \cdots \geqslant a_\ell$, and $b_1 \geqslant b_2 \geqslant \cdots \geqslant b_\ell$.

---

1. $b_0 \leftarrow \lceil (\log_2 n - a_0) \log_2 3 \rceil$ [See Remark 6 (ii)]
2. $i \leftarrow 1$ and $t \leftarrow n$
3. $s \leftarrow 1$ [to keep track of the sign]
4. **while** $t > 0$ **do**
5. find the best approximation $z = d_i 2^{a_i} 3^{b_i}$ of t with $d_i \in \mathcal{S}$, $0 \leqslant a_i \leqslant a_{i-1}$, and $0 \leqslant b_i \leqslant b_{i-1}$
6. $d_i \leftarrow s \times d_i$
7. **if** $t < z$ **then** $s \leftarrow -s$
8. $t \leftarrow |t - z|$
9. $i \leftarrow i + 1$
10. **return** (d_i, a_i, b_i)

Remarks 6.

(i) Algorithm 1 processes the bits of n from left-to-right. It terminates since the successive values of t form a strictly decreasing sequence.

(ii) The parameters a_0 and b_0 are respectively the biggest powers of 2 and 3 allowed in the expansion. Their values have a great influence on the density of the expansion, *cf.* Section 5 for details.

(iii) To compute normal DBNS sequences instead of double-base chains, replace the two conditions $0 \leqslant a_i \leqslant a_{i-1}$, $0 \leqslant b_i \leqslant b_{i-1}$ in Step 5 by $0 \leqslant a_i \leqslant a_0$ and $0 \leqslant b_i \leqslant b_0$.

(iv) In the following, we explain how to find the best approximation $d_i 2^{a_i} 3^{b_i}$ of t in a very efficient way. In addition, the proposed method has a time-complexity that is mainly independent of the size of $\mathcal{S}$ and not directly proportional to it as with a naïve search. See Section 4 for details.

(v) To obtain (w_1, w_2)-double-base chains, simply ensure that $\mathcal{S}$ contains only powers 2 and 3. However, there is a more efficient way. First, introduce two extra variables $a_{\max}$ and $b_{\max}$, initially set to a_0 and b_0 respectively. Then in Step 5, search for the best approximation z of t of the form $2^{a_i} 3^{b_i}$ with $(a_i, b_i) \in [0, a_{\max} + w_1] \times [0, b_{\max} + w_2] \setminus [a_{\max} + 1, a_{\max} + w_1] \times [b_{\max} + 1, b_{\max} + w_2]$. In other words, we allow one exponent to be slightly bigger than its current maximal bound, but the (exceptional) situation where $a_i > a_{\max}$ and $b_i > b_{\max}$ simultaneously is forbidden. Otherwise, we should be obliged to include in $\mathcal{S}$ products of powers of 2 and 3 and increase dramatically the number of precomputations. Once the best approximation has been found, if a_i is bigger than $a_{\max}$, then a_i is changed to $a_{\max}$ while d_i is set to $2^{a_i - a_{\max}}$. If b_i is bigger than $b_{\max}$, then b_i is changed to $b_{\max}$ while d_i is set to $3^{b_i - b_{\max}}$. Finally, do $a_{\max} \leftarrow \min(a_i, a_{\max})$ and $b_{\max} \leftarrow \min(b_i, b_{\max})$ and the rest of the Algorithm remains unchanged.

(vi) Examples of sets $\mathcal{S}$ used in Section 5 are all subset of $\{1, 5, 7, 11, 13, 17, 19, 23, 25\}$.

We now give an algorithm to compute a scalar multiplication from the expansion returned by Algorithm 1.

Algorithm 2. Extended double-base chain scalar multiplication

INPUT: A point P on an elliptic curve E, a positive integer n represented by the sequence $(d_i, a_i, b_i)_{1 \leqslant i \leqslant \ell}$ as returned by Algorithm 1, and the points $[k]P$ for each $k \in \mathcal{S}$.

OUTPUT: The point $[n]P$ on E.

1. $T \leftarrow O_E$ [O_E is the point at infinity on E]
2. set $a_{\ell+1} \leftarrow 0$ and $b_{\ell+1} \leftarrow 0$
3. **for** $i = 1$ **to** ℓ **do**
4. $T \leftarrow T \oplus [d_i]P$
5. $T \leftarrow [2^{a_i - a_{i+1}} 3^{b_i - b_{i+1}}]T$
6. **return** T

Example 7. *For $n = 841232$, the sequence returned by Algorithm 2 with $a_0 = 8$, $b_0 = 8$, and $\mathcal{S} = \{1, 5\}$ is $(1, 7, 8), (5, 5, 2), (-1, 4, 0)$. In the next Table, we shows the intermediate values taken by T in Algorithm 2 when applied to the above-mentioned sequence. The computation is the same as in Example 5.*

i	d_i	$a_i - a_{i+1}$	$b_i - b_{i+1}$	T
1	1	2	6	$[2^2 3^6]P$
2	5	1	2	$[2^1 3^2]([2^2 3^6]P + [5]P)$
3	-1	4	0	$[2^4]\big([2^1 3^2]([2^2 3^6]P + [5]P) - P\big)$

Remark 8. *The length of the chain returned by Algorithm 1 greatly determines the performance of Algorithm 2. However, no precise bound is known so far, even in the case of simple double-base chains. So, at this stage our knowledge is only empirical, cf. Figure 2. More work is therefore necessary to establish the complexity of Algorithm 2.*

4 Implementation aspects

This part describes how to efficiently compute the best approximation of any integer n in terms of $d_1 2^{a_1} 3^{b_1}$ for some $d_1 \in \mathcal{S}$, $a_1 \leqslant a_0$, and $b_1 \leqslant b_0$. The method works on the binary representation of n denoted by $(n)_2$. It operates on the most significant bits of n and uses the fact that a multiplication by 2 is a simple shift.

To make things clear, let us explain the algorithm when $\mathcal{S} = \{1\}$. First, take a suitable bound B and form a two-dimensional array of size $(B + 1) \times 2$. For each $b \in [0, B]$, the corresponding row vector contains $[(3^b)_2, b]$. Then sort this array with respect to the first component using lexicographic order denoted by $\preccurlyeq$ and store the result.

To compute an approximation of n in terms of $2^{a_1}3^{b_1}$ with $a_1 \leqslant a_0$ and $b_1 \leqslant b_0$, find the two vectors v_1 and v_2 such that $v_1[1] \preccurlyeq (n)_2 \preccurlyeq v_2[1]$. This can be done with a binary search in $O(\log B)$ operations.

The next step is to find the first vector v_1' that is before v_1 in the sorted array and that is suitable for the approximation. More precisely, we require that:

- the difference δ_1 between the binary length of n and the length of $v_1'[1]$ satisfies $0 \leqslant \delta_1 \leqslant a_0$,
- the corresponding power of 3, *i.e.* $v_1'[2]$, is less than b_0.

This operation is repeated to find the first vector v_2' that is after v_2 and fulfills the same conditions as above. The last step is to decide which approximation, $2^{\delta_1}3^{v_1'[2]}$ or $2^{\delta_2}3^{v_2'[2]}$, is closer to n.

In case $|\mathcal{S}| > 1$, the only difference is that the array is of size $\big(|\mathcal{S}|(B+1)\big) \times 3$. Each row vector is of the form $[(d3^b)_2, b, d]$ for $d \in \mathcal{S}$ and $b \in [0, B]$. Again the array is sorted with respect to the first component using lexicographic order. Note that multiplying the size of the table by $|\mathcal{S}|$ has only a negligible impact on the time complexity of the binary search. See [18, Appendix A] for a concrete example and some improvements to this approach.

This approximation method ultimately relies on the facts that lexicographic and natural orders are the same for binary sequences of the same length and also that it is easy to adjust the length of a sequence by multiplying it by some power of 2. The efficiency comes from the sorting operation (done once at the beginning) that allows to retrieve which precomputed binary expansions are close to n, by looking only at the most significant bits.

For environments with constrained memory, it may be difficult or even impossible to store the full table. In this case, we suggest to precompute only the first byte or the first two bytes of the binary expansions of $d3^b$ together with their binary length. This information is sufficient to find two approximations A_1, A_2 in the table such that $A_1 \leqslant n \leqslant A_2$, since the algorithm operates only on the most significant bits. However, this technique is more time-consuming since it is necessary to actually *compute* at least one approximation and sometimes more, if the first bits are not enough to decide which approximation is the closest to n.

In Table 1, we give the precise amount of memory (in bytes) that is required to store the vectors used for the approximation for different values of B. Three situations are investigated, *i.e.* when the first byte, the first two bytes, and the full binary expansions $d3^b$, for $d \in \mathcal{S}$ and $b \leqslant B$ are precomputed and stored.

See [19] for a in PARI/GP implementation of Algorithm 1 using the techniques described in this section.

5 Tests and results

In this section, we present some tests to help evaluating the relevance of extended double-base chains for scalar multiplications on generic elliptic curves defined over $\mathbb{F}_p$, for p of size between 200 and 500 bits. Comparisons with the best

Bound B	25	50	75	100	125	150	175	200
$\mathcal{S} = \{1\}$								
First byte	33	65	96	127	158	190	221	251
First two bytes	54	111	167	223	279	336	392	446
Full expansion	85	293	626	1,084	1,663	2,367	3,195	4,108
$\mathcal{S} = \{1, 5, 7\}$								
First byte	111	214	317	420	523	627	730	829
First two bytes	178	356	534	712	890	1,069	1,247	1,418
Full expansion	286	939	1,962	3,357	5,122	7,261	9,769	12,527
$\mathcal{S} = \{1, 5, 7, 11, 13\}$								
First byte	185	357	529	701	873	1,045	1,216	1,381
First two bytes	300	597	894	1,191	1,488	1,785	2,081	2,366
Full expansion	491	1,589	3,305	5,642	8,598	12,173	16,364	20,972
$\mathcal{S} = \{1, 5, 7, 11, 13, 17, 19, 23, 25\}$								
First byte	334	643	952	1,262	1,571	1,881	2,190	2,487
First two bytes	545	1,079	1,613	2,148	2,682	3,217	3,751	4,264
Full expansion	906	2,909	6,026	10,255	15,596	22,056	29,630	37,947

Table 1. Precomputations size (in bytes) for various bounds B and sets $\mathcal{S}$

systems known so far, including ℓ-NAF$_w$ and normal double-base chains are given.

In the following, we assume that we have three basic operations on a curve E to perform scalar multiplications, namely addition/subtraction, doubling, and tripling. In turn, each one of these elliptic curve operations can be seen as a sequence of inversions I, multiplications M, and squarings S in the underlying field $\mathbb{F}_p$.

There exist different systems of coordinates with different complexities. For many platforms, projective-like coordinates are quite efficient since they do not require any field inversion for addition and doubling, *cf.* [20] for a comparison. Thus, our tests will not involve any inversion. Also, to ease comparisons between different scalar multiplication methods, we will make the standard assumption that S is equivalent to 0.8M. Thus, the complexity of a scalar multiplication will be expressed in terms of a number of field multiplications only and will be denoted by N_{M}.

Given any curve $E/\mathbb{F}_p$ in Weierstraß form, it is possible to directly obtain $[3]P$ more efficiently than computing a doubling followed by an addition. Until now, all these direct formulas involved at least one inversion, *cf.* [21], but recently, an inversion-free tripling formula has been devised for Jacobian projective coordinates [17]. Our comparisons will be made using this system. In Jacobian coordinates, a point represented by $(X_1 : Y_1 : Z_1)$ corresponds to the affine point

$(X_1/Z_1^2, Y_1/Z_1^3)$, if $Z_1 \neq 0$, and to the point at infinity O_E otherwise. A doubling can be done with $4\mathrm{M}+6\mathrm{S}$, a tripling with $10\mathrm{M}+6\mathrm{S}$ and a mixed addition, *i.e.* an addition between a point in Jacobian coordinates and an affine point, using $8\mathrm{M}+3\mathrm{S}$.

With these settings, we display in Figure 1, the number of multiplications N_{M} required to compute a scalar multiplication on a 200-bit curve with Algorithm 2, for different choices of a_0 and various DBNS methods. Namely, we investigate double-base chains as in [17], window double-base chains with 2 and 8 precomputations, and extended double-base chains with $\mathcal{S}_2 = \{1, 5, 7\}$ and $\mathcal{S}_8 = \{1, 5, 7, 11, 13, 17, 19, 23, 25\}$, as explained in Section 3.2. Comparisons are done on $1,000$ random 200-bit scalar multiples. Note that the costs of the precomputations are not included in the results.

Figure 1 indicates that $a_0 = 120$ is close to the optimal choice for every method. This implies that the value of b_0 should be set to 51. Similar computations have been done for sizes between 250 and 500. It appears that a simple and good heuristic to minimize N_{M} is to set $a_0 = \lceil 120 \times \mathrm{size}/200 \rceil$ and b_0 accordingly. These values of a_0 and b_0 are used in the remainder for sizes in $[200, 500]$.

In Figure 2, we display the average length of different extended DBNS expansions in function of the size of the scalar multiple n. Results show that the length of a classic double-base chain is reduced by more than 25% with only 2 precomputations and by 43% with 8 precomputations.

In Table 2, we give the average expansion length ℓ, as well as the maximal power a_1 (resp. b_1) of 2 (resp. 3) in the expansion for different methods and different sizes. The symbol $\#\mathcal{P}$ is equal to the number of precomputed points for a given method and the set $\mathcal{S}_m$ contains the first $m+1$ elements of $\{1, 5, 7, 11, 13, 17, 19, 23, 25\}$. Again, $1,000$ random integers have been considered in each case.

In Table 3, we give the corresponding complexities in terms of the number of multiplications and the gain that we can expect with respect to a window NAF method involving the same number of precomputations.

See [18] for a full version including a similar study for some special curves.

6 Conclusion

In this work, we have introduced a new family of DBNS, called extended DBNS, where the coefficients in the expansion belong to a given set $\mathcal{S}$. A scalar multiplication algorithm relying on this representation and involving precomputations was presented. Also, we have desribed a new method to quickly find the best approximation of an integer by a number of the form $d2^a3^b$ with $d \in \mathcal{S}$. This approach greatly improves the practicality of the DBNS. Extended DBNS sequences give rise to the fastest scalar multiplications known to date for generic elliptic curves. In particular, given a fixed number of precomputations, the extended DBNS is more efficient than any corresponding window NAF method. Gains are especially important for a small number of precomputations, typically up to three points. Improvements larger than 10% over already extremely optimized methods can be expected. Also, this system is more flexible, since it can be used with any given set of coefficients, unlike window NAF methods.

Further research will include an extension of these ideas to Koblitz curves, for which DBNS-based scalar multiplication techniques without precomputations exist already, see [16, 22, 23]. This will most likely lead to appreciable performance improvements.

Acknowledgements

This work was partly supported by the Canadian NSERC strategic grant #73-2048, *Novel Implementation of Cryptographic Algorithms on Custom Hardware Platforms* and by a French-Australian collaborative research program from the *Direction des Relations Européennes et Internationales du CNRS*, France.

References

1. Miller, V.S.: Use of elliptic curves in cryptography. In: Advances in Cryptology – Crypto 1985. Volume 218 of Lecture Notes in Comput. Sci. Springer-Verlag, Berlin (1986) 417–426
2. Koblitz, N.: Elliptic curve cryptosystems. Math. Comp. **48** (1987) 203–209
3. Koblitz, N.: Hyperelliptic cryptosystems. J. Cryptology **1** (1989) 139–150
4. Blake, I.F., Seroussi, G., Smart, N.P.: Elliptic curves in cryptography. Volume 265 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge (1999)
5. Hankerson, D., Menezes, A.J., Vanstone, S.A.: Guide to elliptic curve cryptography. Springer-Verlag, Berlin (2003)
6. Avanzi, R.M., Cohen, H., Doche, C., Frey, G., Nguyen, K., Lange, T., Vercauteren, F.: Handbook of Elliptic and Hyperelliptic Curve Cryptography. Discrete Mathematics and its Applications (Boca Raton). CRC Press, Inc. (2005)
7. Blake, I.F., Seroussi, G., Smart, N.P.: Advances in Elliptic Curve Cryptography. Volume 317 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge (2005)
8. Doche, C.: Exponentiation. In: [6]. (2005) 145–168
9. Morain, F., Olivos, J.: Speeding up the Computations on an Elliptic Curve using Addition-Subtraction Chains. Inform. Theor. Appl. **24** (1990) 531–543
10. Dimitrov, V.S., Jullien, G.A., Miller, W.C.: Theory and applications of the double-base number system. IEEE Trans. on Computers **48** (1999) 1098–1106
11. Miyaji, A., Ono, T., Cohen, H.: Efficient Elliptic Curve Exponentiation. In: Information and Communication – ICICS'97. Volume 1334 of Lecture Notes in Comput. Sci., Springer (1997) 282–291
12. Takagi, T., Yen, S.M., Wu, B.C.: Radix-r non-adjacent form. In: Information Security Conference – ISC 2004. Volume 3225 of Lecture Notes in Comput. Sci. Springer-Verlag, Berlin (2004) 99–110
13. Dimitrov, V.S., Jullien, G.A., Miller, W.C.: An algorithm for modular exponentiation. Information Processing Letters **66** (1998) 155–159

14. Berthé, V., Imbert, L.: On converting numbers to the double-base number system. In: In F. T. Luk, editor, Advanced Signal Processing Algorithms, Architecture and Implementations XIV, volume 5559 of Proceedings of SPIE. (2004) 70–78
15. Ciet, M., Sica, F.: An Analysis of Double Base Number Systems and a Sublinear Scalar Multiplication Algorithm. In: Progress in Cryptology – Mycrypt 2005. Volume 3715 of Lecture Notes in Comput. Sci., Springer (2005) 171–182
16. Avanzi, R.M., Sica, F.: Scalar Multiplication on Koblitz Curves using Double Bases. In: proceedings of Vietcrypt 2006. Lecture Notes in Comput. Sci. (2006) See also Cryptology ePrint Archive, Report 2006/067, `http://eprint.iacr.org/`.
17. Dimitrov, V.S., Imbert, L., Mishra, P.K.: Efficient and secure elliptic curve point multiplication using double-base chains. In: Advances in Cryptology – Asiacrypt 2005. Volume 3788 of Lecture Notes in Comput. Sci., Springer (2005) 59–78
18. Doche, C., Imbert, L.: Extended double-base number system with applications to elliptic curve cryptography (2006) full version of the present paper, see Cryptology ePrint Archive, `http://eprint.iacr.org/`.
19. Doche, C.: A set of GP-PARI functions to compute DBNS expansions (2006) `http://www.ics.mq.edu.au/~doche/dbns_basis.gp`.
20. Doche, C., Lange, T.: Arithmetic of Elliptic Curves. In: [6]. (2005) 267–302
21. Ciet, M., Joye, M., Lauter, K., Montgomery, P.L.: Trading inversions for multiplications in elliptic curve cryptography. Des. Codes Cryptogr. **39** (2006) 189–206
22. Dimitrov, V.S., Jarvine, K., Jr, M.J.J., Chan, W.F., Huang, Z.: FPGA Implementation of Point Multiplication on Koblitz Curves Using Kleinian Integers. In: proceedings of CHES 2006. Lecture Notes in Comput. Sci. (2006)
23. Avanzi, R.M., Dimitrov, V.S., Doche, C., Sica, F.: Extending Scalar Multiplication using Double Bases. In: proceedings of Asiacrypt 2006. Lecture Notes in Comput. Sci., Springer (2006)

Appendix: Graphs and tables

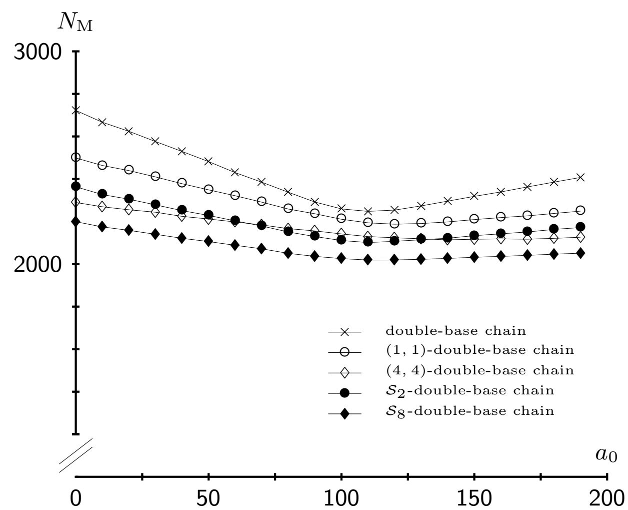

Fig. 1. Average number of multiplications to perform a random scalar multiplication on a generic 200-bit curve with various DBNS methods parameterized by a_0

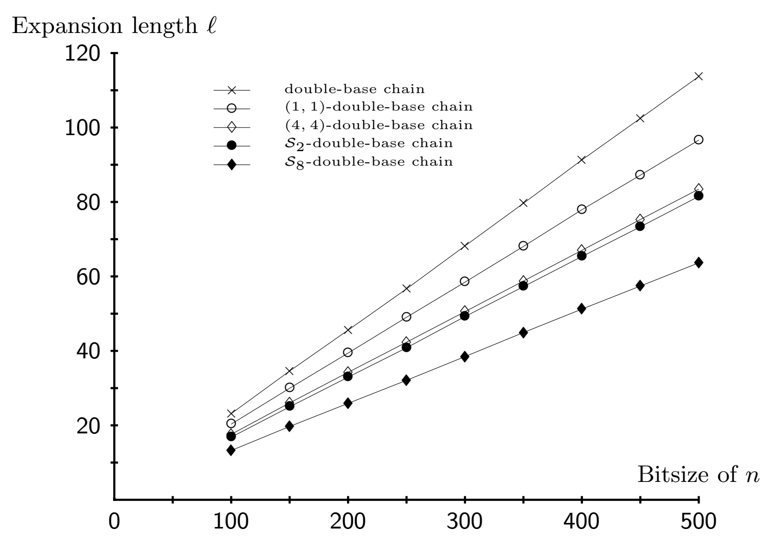

Fig. 2. Average expansion length ℓ of random scalar integers n with various DBNS

Size		200 bits			300 bits			400 bits			500 bits		
	$\#\mathcal{P}$	ℓ	a_1	b_1	ℓ	a_1	b_1	ℓ	a_1	b_1	ℓ	a_1	b_1
2NAF_2	0	66.7	200	0	100	300	0	133.3	400	0	166.7	500	0
Binary/ternary	0	46.1	90.7	68.1	69.2	136.4	102.2	91.9	182.6	136.3	114.4	228.0	170.7
DB-chain	0	45.6	118.7	50.4	68.2	178.7	75.5	91.3	239.0	100.6	113.7	298.6	126.2
3NAF_2	1	50	200	0	75	300	0	100	400	0	125	500	0
$(1, 0)$-DB-chain	1	46.8	118.9	50.2	70.5	179.1	75.1	94.5	239.3	100.3	117.7	298.8	125.9
$(0, 1)$-DB-chain	1	42.9	118.7	50.4	63.8	178.7	75.5	85.4	239.0	100.6	106.4	298.6	126.2
$\mathcal{S}_1$-DB chain	1	36.8	118.1	49.9	55.0	178.0	75.0	72.9	238.2	100.1	91.0	297.8	125.7
2NAF_3	2	50.4	0	126	75.6	0	189	100.8	0	252	126	0	315
$(1, 1)$-DB-chain	2	39.4	118.9	50.2	58.5	179.1	75.1	77.9	239.3	100.3	96.6	298.8	125.9
$\mathcal{S}_2$-DB chain	2	32.9	117.8	49.8	49.2	177.8	74.9	65.3	238	100.0	81.5	297.7	125.6
4NAF_2	3	40	200	0	60	300	0	80	400	0	100	500	0
$\mathcal{S}_3$-DB chain	3	30.7	117.5	49.7	45.7	177.5	74.8	60.6	237.8	99.8	75.6	297.3	125.4
$(2, 2)$-DB-chain	4	36.8	119.2	49.8	54.7	179.3	74.8	72.6	239.4	100.1	90.5	299.0	125.7
$\mathcal{S}_4$-DB chain	4	28.9	117.3	49.6	43.2	177.3	74.7	57.6	237.6	99.8	71.5	297.1	125.4
$(3, 3)$-DB-chain	6	35.3	119.3	49.5	52.2	179.4	74.6	69.2	239.5	99.6	86.1	299.2	125.2
$\mathcal{S}_6$-DB chain	6	27.3	117.4	49.4	40.6	177.3	74.5	54.0	237.6	99.6	67.1	297	125.3
3NAF_3	8	36	0	126	54	0	189	72	0	252	90	0	315
$(4, 4)$-DB-chain	8	34.2	119.3	49.3	50.5	179.5	74.2	67.0	239.6	99.3	83.5	299.3	125
$\mathcal{S}_8$-DB chain	8	25.9	117.2	49.3	38.5	177.1	74.4	51.2	237.4	99.5	63.6	296.9	125.2

Table 2. Parameters for various scalar multiplication methods on generic curves

Size		200 bits		300 bits		400 bits		500 bits	
	$\#\mathcal{P}$	N_{M}	Gain	N_{M}	Gain	N_{M}	Gain	N_{M}	Gain
2NAF_2	0	2442.9	—	3669.6	—	4896.3	—	6122.9	—
Binary/ternary	0	2275.0	6.87%	3422.4	6.74%	4569.0	6.68%	5712.5	6.70%
DB-chain	0	2253.8	7.74%	3388.5	7.66%	4531.8	7.44%	5666.5	7.45%
3NAF_2	1	2269.6	—	3409.6	—	4549.6	—	5689.6	—
$(1, 0)$-DB-chain	1	2265.8	0.17%	3410.3	−1.98%	4562.3	−1.72%	5707.4	−1.69%
$(0, 1)$-D B-chain	1	2226.5	1.90%	3343.2	1.95%	4471.0	1.73%	5590.4	1.74%
$\mathcal{S}_1$-DB chain	1	2150.4	5.25%	3238.1	5.03%	4326.3	4.91%	5418.1	4.77%
2NAF_3	2	2384.8	—	3579.3	—	4773.8	—	5968.2	—
$(1, 1)$-DB-chain	2	2188.6	8.23%	3285.5	8.21%	4390.0	8.04%	5487.7	8.05%
$\mathcal{S}_2$-DB chain	2	2106.5	11.67%	3174.1	11.32%	4243.6	11.11%	5314.8	10.95%
4NAF_2	3	2165.6	—	3253.6	—	4341.6	—	5429.6	—
$\mathcal{S}_3$- DB chain	3	2078.1	4.04%	3132.8	3.71%	4189.8	3.50%	5248.5	3.34%
$(2, 2)$-DB-chain	4	2158.2	—	3242.6	—	4333.1	—	5421.6	—
$\mathcal{S}_4$-DB chain	4	2056.7	—	3105.0	—	4156.1	—	5204.0	—
$(3, 3)$-DB-chain	6	2139.4	—	3215.0	—	4291.7	—	5371.9	—
$\mathcal{S}_6$-DB chain	6	2036.3	—	3074.3	—	4115.4	—	5155.1	—
3NAF_3	8	2236.2	—	3355.8	—	4475.4	—	5595.0	—
$(4, 4)$-DB-chain	8	2125.4	4.95%	3192.2	4.88%	4264.1	4.72%	5340.5	4.55%
$\mathcal{S}_8$-DB chain	8	2019.3	9.70%	3049.8	9.12%	4084.3	8.74%	5116.8	8.55%

Table 3. Complexity of various extended DBNS methods for generic curves and gain with respect to window NAF methods having the same number of precomputations