Malaysian Journal of Mathematical Sciences 7(1): 111-123 (2013)

An Average Density of τ-adic Naf (τ-NAF) Representation: An Alternative Proof

Faridah Yunos and Kamel Ariffin Mohd Atan

Institute for Mathematical Research,
Universiti Putra Malaysia,
43400 Serdang, Selangor, Malaysia

E-mail: faridahy@putra.upm.edu.my and kamel@putra.upm.edu.my

ABSTRACT

In order to improve the efficiency of scalar multiplications on elliptic Koblitz curves, expansions of the scalar to a complex base associated with the Frobenius endomorphism are commonly used. One such expansion is the τ-adic Non Adjacent Form (τ-NAF), introduced by Solinas (1997). Some properties of this expansion, such as the average density, are well known. However in the literature there is no description on the same sequences occuring as length-l NAF's and length-l τ-NAF's to proof that the average density is approximately $\frac{1}{3}$. In this paper we provide an alternative proof of this fact.

Keywords: anomalous binary curves (Koblitz curves), scalar multiplication, τ-adic non-adjacent form, norm.

1. INTRODUCTION

In cryptographic protocols whose security relies on the hardness of the discrete logarithm problem on elliptic curves, the computationally most dominant part is the scalar multiplication nP, where P is a point on the curve and n is an integer, called the scalar. In order to increase the speed of this computation, special types of curves where large multiples of P could be computed quickly have been proposed very early in the history of elliptic curve cryptography (ECC). In this paper we will consider Koblitz curves.

The *Koblitz curves* are a special type of curves for which the Frobenius endomorphism can be used for improving the performance of computing a scalar multiplication (Koblitz (1987)). The Koblitz curves are defined over F_2 as follows

$$E_a: y^2 + xy = x^3 + ax^2 + 1$$

where $a \in \{0,1\}$ (Koblitz (1992)). The Frobenius map $\tau: E_a(F_{2^m}) \mapsto E_a(F_{2^m})$ for a point $P = (x, y)$ on $E_a(F_{2^m})$ is defined by

$$\tau(x, y) = (x^2, y^2) \ , \qquad \tau(O) = O$$

where O is the point at infinity. It stands that $(\tau^2 + 2)P = t\tau(P)$ for all $P \in E_a(F_{2^m})$, where the trace, $t = (-1)^{1-a}$. Thus, it follows that the Frobenius map can be considered as a multiplication with complex number $\tau = \frac{t+\sqrt{-7}}{2}$ (Solinas (2000)).

The τ-NAF proposed by Solinas, is one of the most efficient algorithms to compute scalar multiplications on Koblitz curves. Our paper is structured as follows.

2. τ- ADIC NON-ADJACENT FORM

In the ensuing discussion, the following definitions will be applied.

Definition 2.1. *A non-adjacent form (NAF) of a positive integer n is an expression $n = \sum_{i=0}^{l-1} n_i 2^i$ where $n_i \in \{-1,0,1\}$, $n_{l-1} \neq 0$, and no two consecutive digits n_i are nonzero. The length of the NAF is l.*

Definition 2.2. *A τ-adic Non-Adjacent Form of nonzero $\bar{n}$ an element of $Z(\tau)$ is defined as τ-NAF$(\bar{n}) = \sum_{i=0}^{l-1} c_i \tau^i$ where l is the length of an expansion of τ-NAF$(\bar{n})$, $c_{l-1} \neq 0$, $c_i \in \{-1,0,1\}$ and $c_i c_{i+1} = 0$.*

Definition 2.3. *We denote HW_l as hamming weight of nonzero element occurring among τ-NAF of all length-l element of $Z(\tau)$.*

Solinas proposed the following algorithm for computing the τ-NAF. It is completely analogous to the computation of the NAF for integers.

Algorithm 2.1. (τ-NAF)

Input	:	Integers $r_o,\ r_1$
Output	:	τ-NAF$(r_0 + r_1\tau)$

Computation : Set $c_0 \leftarrow r_0,\ c_1 \leftarrow r_1$
Set $S \leftarrow \langle\rangle$
While $c_0 \neq 0\ \ or\ c_1 \neq 0$
If c_0 odd then
set $u \leftarrow 2 - (c_0 - 2c_1\ mod\ 4)$
set $c_0 \leftarrow c_0 - u$
else
set $u \leftarrow 0$
Prepend u to S
Set $(c_0, c_1) \leftarrow \left(c_1 + \frac{tc_0}{2}, -\frac{c_0}{2}\right)$
End While
Output S

In the following proposition Solinas mentions that the expected density (i.e. the ratio of non-zero bits to the total number of bits) of τ-NAF is $\frac{1}{3}$. Each $\bar{n} \in Z(\tau)$ admits a unique τ-NAF. The length of the τ-NAF of a randomly chosen scalar $\bar{n}$ is $\approx 2m$, whereas the bit length of $\bar{n}$ is $\approx m$.

Proposition 2.1. The average density among τ-NAF's of length l is given by

$$\frac{2^l(3l-4) - (-1)^l(6l-4)}{9(l-1)(2^l - (-1)^l)} \tag{1}$$

and is therefore asymptotically $\frac{1}{3}$.

Proof. The result follows from $\frac{2^l(3l-4)-(-1)^l(6l-4)}{9(l-1)(2^l-(-1)^l)}$ since the same sequences occur as length-l NAF's and length-l τ-NAF's. ■

With retrieval from the above proposition, he is able to estimate that the average Hamming weight among length-l τ-NAF's is roughly $\frac{l}{3}$.

Here, Solinas did not give evidence that the sequence of average density among τ-NAF's of length l was similar with NAF's. Researchers subsequent to Solinas such as Avanzi *et al.* (2005), Li *et al.* (2007), Brumley and Jarvinen (2007), Lin (2009), Hakuta *et al.* (2010), Roy *et al.* (2011) had accepted and use the above evidence without any modification. Next section will present an alternative proof that the average density of among τ-NAF's of length l is $\frac{1}{3}$.

3. RESULTS AND DISCUSSION

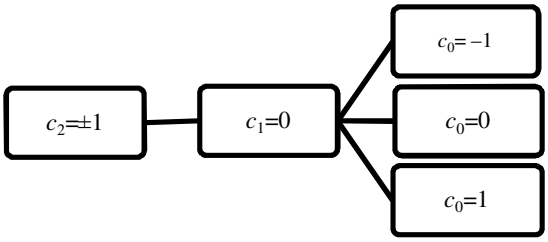
We will start by making short analysis on τ-NAF that have length-3 as in the following example.

Example 3.1. *Table 1 show us the all combination of* c_0, c_1 *and* c_2.

TABLE 1: Combinations of c_0, c_1, c_2 and t and their hamming weight

No.	c_2	c_1	c_0	t	HW
1	-1	0	-1	-1	2
2	-1	0	1	-1	2
3	-1	0	0	-1	1
4	-1	0	-1	1	2
5	-1	0	1	1	2
6	-1	0	0	1	1
7	1	0	-1	-1	2
8	1	0	1	-1	2
9	1	0	0	-1	1
10	1	0	-1	1	2
11	1	0	1	1	2
12	1	0	0	1	1
$4m_3 = 4(3) = 12$	$12m_3 = 12(3) = 36$				$HW_3 = 20$

There are 12 combinations of c_0, c_1, c_2 and t. The combinations are constructed based on the following tree diagram.



As such, we have 6 ways to arrange c_0, c_1 and c_2 also 2 ways as the total number of t. Thus we will have 12 combinations as described in above schedule. By using the similar method, we could get all outcomes of c_i.

From Table 1, we obtain the following results:

1. The number of arrangements of $c_2,\ c_1,\ c_0$ and t (or on the other hand, the number of all integers with τ-NAF of length l) is 12.
2. The total number of $-1,0$ and 1 is 36 (i.e. multiplication of l with the number of arrangements).
3. We define t_j the total number of -1 and 1 in column c_j for $j = 0,1,2$, thus we have $t_2 = 12,\ t_1 = 0$ and $t_0 = 8$.
4. The number of nonzero coefficients (i.e. the hamming weight of length 3, HW_3) is 20.
5. The average hamming weight (i.e. HW_3 divided by the number of arrangements of $c_2,\ c_1,\ c_0$ and t) is 2, and
6. The average density (i.e. average hamming weight divided by length) is 0.8.

By using similar method of constructing Table 1, we will see that the number of arrangements c_i for $l = 1, \dots, 15$ follow like the following sequence

$$4,4,12,20,44,84,172,340,684,1364,2732,5460,10924,43692.$$

It can be written as

$$4,4(1),4(3),4(5),4(11),4(43),\dots,4(10923).$$

By making an analysis on the above sequence, we obtain the number of arrangements c_i and t is $4m_l$ where $m_l = 1,1,3,5,\dots,10923$ come from the following theorems.

Theorem 3.2. *If* $m_1 = 1$ *and* $b_l = \begin{cases} 0 & if\ l\ is\ even \\ 1 & if\ l\ is\ odd \end{cases}$ *then*

$$m_l = b_l + \sum_{k=1}^{l-1} m_k \tag{2}$$

for $l > 1$.

Proof. If $l = 2$ then

$$\begin{aligned} m_2 &= b_2 + \sum_{k=1}^{1} m_k \\ &= 0 + 1 \\ &= 1. \end{aligned}$$

Assume that $m_{l'} = b_{l'} + \sum_{k=1}^{l'-1} m_k$ for $l' > 1$ is true for $l = l'$.

Now, for $l = l' + 1$

$$\begin{aligned} m_{l'+1} &= b_{l'+1} + m_1 + m_2 + \cdots + m_{l'} \\ &= b_{l'+1} + \textstyle\sum_{k=1}^{l'} m_k \\ &= b_{l'+1} + \textstyle\sum_{k=1}^{l'+1-1} m_k. \end{aligned}$$

.

Thus, (2) is still true for $l = l' + 1$, therefore it is true for all $l > 1$.

The above expression can be simplified as follows.

$$\begin{aligned} m_{l'+1} &= b_{l'+1} + \sum_{k=1}^{l'+1-1} m_k \\ &= b_{l'+1} + m_1 + \cdots + m_{l'-1} + m_{l'} \\ &= b_{l'-1} + m_1 + \cdots + m_{l'-1} + m_{l'} \\ &= \left(b_{l'-1} + m_1 + \cdots + m_{l'-2}\right) + m_{l'-1} + m_{l'} \\ &= m_{l'-1} + m_{l'-1} + m_{l'} \\ &= 2m_{l'-1} + m_{l'}. \quad \blacksquare \end{aligned}$$

Theorem 3.3. *If $m_l = b_l + \sum_{k=1}^{l-1} m_k$ (as given by Theorem 3.2) then*

$$m_l = \frac{(-1)^l\left((-2)^l - 1\right)}{3} \tag{3}$$

for $l \geq 1$.

Proof.

$$\begin{aligned} m_l &= b_l + \sum_{k=1}^{l-1} m_k \quad \text{where } b_l = \begin{cases} 0 & if\ l\ is\ even \\ 1 & if\ l\ is\ odd \end{cases} \\ &= e_l + 2m_{l-1} \text{ where } e_l = \begin{cases} -1 & if\ l\ is\ even \\ 1 & if\ l\ is\ odd \end{cases} \\ &= (-1)^{l-1} + 2m_{l-1} \\ &= \sum_{i=1}^{l} (-1)^{i-1} 2^{l-i}. \end{aligned}$$

This is a geometric series where the first term is 2^{l-1}, the common ratio is $-\frac{1}{2}$ and the number of terms is l, therefore

$$m_l = \frac{(-1)^l((-2)^l-1))}{3}. \qquad \blacksquare$$

Thus, the number of all integers with τ-NAF is $4\frac{(-1)^l((-2)^l-1)}{3}$ for any element of $Z(\tau)$ with length-l. This is four times of the number of positive integers with NAF of length-l (Ratsimihah and Prodinger (2005)).

Now, we construct the following table in order to find the hamming weights occurring among τ-NAF of all length-l elements of $Z(\tau)$. We define t_{l-j} as the total number of -1 and 1 for c_{l-j} where $j = 1,2,3,\dots,13$.

TABLE 2: All hamming weight of element in $Z(\tau)$ with $l = \{1,2,3,\dots,13\}$

l	t_{l-1}	t_{l-2}	t_{l-3}	t_{l-4}	t_{l-5}	t_{l-6}	t_{l-7}	t_{l-8}	t_{l-9}	t_{l-10}	t_{l-11}	t_{l-12}	t_{l-13}	HW_l
1	4													4
2	4													4
3	12	0	8											20
4	20	0	8	8										36
5	44	0	24	8	24									100
6	84	0	40	24	24	40								212
7	172	0	88	40	72	40	88							500
8	340	0	168	88	120	120	88	168						1092
9	684	0	344	168	264	200	264	168	344					2436
10	1364	0	680	344	504	440	440	504	344	680				5300
11	2732	0	1368	680	1032	840	968	840	1032	680	1368			11540
12	5460	0	2728	1368	2040	1720	1848	1848	1720	2040	1368	2728		24868
13	10924	0	5464	2728	4104	3400	3784	3528	3784	3400	4104	2728	5464	53412

The hamming weight for $l = 1,2,3,\dots,13$ is

$$4,4,20,36,100,212,500,1092,2436,5300,11540,24868,53412.$$

It can be written as

$$4,4,4(3+2(1\cdot 1)),4(5+2(1\cdot 1+1\cdot 1)),4(11+2(1\cdot 3+1\cdot 1+3\cdot 1)),$$
$$\dots,4(2731+2(1\cdot 683+1\cdot 341+3\cdot 171+5\cdot 85+11\cdot 43+21\cdot 21+$$
$$43\cdot 11+85\cdot 5+171\cdot 3+341\cdot 1+683\cdot 1)).$$

As a result, we obtain the following theorems.

Theorem 3.4. *If* $HW_1 = HW_2 = 4$ *then*

$$HW_l = 4\left(m_l + 2\sum_{k=1}^{l-2} m_k\, m_{l-k-1}\right) \tag{4}$$

for $l > 2$.

Proof. If $l = 3$ then

$$\begin{aligned} HW_3 &= 4\left(m_3 + 2\sum_{k=1}^{1} m_k\, m_{2-k}\right) \\ &= 4(m_3 + 2(m_1 m_1)) \\ &= 4(3 + 2(1 \cdot 1)) \\ &= 20. \end{aligned}$$

Assume that $HW_{l'} = 4\left(m_{l'} + 2\sum_{k=1}^{l'-2} m_k m_{l'-k-1}\right)$ is true for $l = l'$.
Hence, if $l = l' + 1$, then

$$\begin{aligned} HW_{l'+1} &= 4\left(m_{l'+1} + 2\sum_{k=1}^{l'-1} m_k m_{l'-k}\right) \\ &= 4\left(m_{l'+1} + 2m_{l'-1} + 2\sum_{k=1}^{l'-2} m_k m_{l'-k}\right) \\ &= 4\left((2\,m_{l'-1} + m_{l'}) + 2m_{l'-1} + 2\sum_{k=1}^{l'-2} m_k \left(b_{l'-k} + \sum_{k'=1}^{l'-k-1} m_{k'}\right)\right) \\ &= 4\left(m_{l'} + 4m_{l'-1} + 2\sum_{k=1}^{l'-2} m_k \left(b_{l'-k} + m_{l'-k-1} + \sum_{k'=1}^{l'-k-2} m_{k'}\right)\right) \\ &= 4\left(m_{l'} + 4m_{l'-1} + 2\sum_{k=1}^{l'-2} m_k m_{l'-k-1} + 2\sum_{k=1}^{l'-2} m_k \left(b_{l'-k} + \sum_{k'=1}^{l'-k-2} m_{k'}\right)\right) \\ &= 16m_{l'-1} + HW_{l'} + 8\sum_{k=1}^{l'-2} m_k \left(b_{l'-k} + \sum_{k'=1}^{l'-k-2} m_{k'}\right) \end{aligned}$$

Since $b_{l'-k} = b_{l'-k-2}$ then

$$\begin{aligned} HW_{l'+1} &= 16m_{l'-1} + HW_{l'} + 8\sum_{k=1}^{l'-2} m_k \left(m_{l'-k-2} + b_{l'-k-2} + \sum_{k'=1}^{l'-k-3} m_{k'}\right) \\ &= 16m_{l'-1} + HW_{l'} + 8\sum_{k=1}^{l'-2} m_k \left(m_{l'-k-2} + m_{l'-k-2}\right) \\ &= 16m_{l'-1} + HW_{l'} + 16\sum_{k=1}^{l'-2} m_k m_{l'-k-2}\,. \end{aligned}$$

Thus, (4) is true for $l = l' + 1$, therefore it is true for all $l > 2$. ■

Theorem 3.5. *If* $HW_l = 4\left(m_l + 2\sum_{k=1}^{l-2} m_k m_{l-k-1}\right)$ *(as given by Theorem 3.4) then* $HW_l = -\frac{(-1)^l 4\left((3l+5)\left(1-(-2)^l\right)+3l\right)}{27}$ *for* $l > 2$.

Proof. From Theorem 3.4, we have $HW_l = 4\left(m_l + 2\sum_{k=1}^{l-2} m_k m_{l-k-1}\right)$.

By using (3), we obtain

$$HW_l = 4\left(\frac{(-1)^l\left((-2)^l - 1\right)}{3} + 2\sum_{k=1}^{l-2} \frac{(-1)^k\left((-2)^k - 1\right)}{3} \cdot \frac{(-1)^{l-k-1}\left((-2)^{l-k-1} - 1\right)}{3}\right)$$

$$= 4\left(\frac{(-1)^l\left((-2)^l - 1\right)}{3} - \frac{2(-1)^l\sum_{k=1}^{l-2}\left((-2)^k - 1\right)\left((-2)^{l-k-1} - 1\right)}{9}\right)$$

$$= -\frac{4(-1)^l}{3}\left(1 - (-2)^l + \frac{2}{3}\left(\sum_{k=1}^{l-2} 1 - \sum_{k=1}^{l-2}(-2)^{l-k-1} - \sum_{k=1}^{l-2}(-2)^k + \sum_{k=1}^{l-2}(-2)^{l-1}\right)\right)$$

$$= -\frac{4(-1)^l}{3}\left(1 - (-2)^l + \frac{2}{3}\left(l - 2 + \frac{2}{3}\left(1 - (2)^{l-2}\right) + \frac{2}{3}(1 - (2)^{l-2}) + (l-2)(-2)^{l-1}\right)\right)$$

$$= -\frac{4(-1)^l}{3}\left(\frac{2}{3}\left(l - 2 + \frac{4}{3}(1 - (-2)^{l-2}) + (-2)^{l-1}(l-2)\right) + 1 - (-2)^l\right)$$

$$= -\frac{4(-1)^l}{27}\left((3l+5)(1-(-2)^l) + 3l\right). \quad ■$$

Theorem 3.6. *Suppose that the average hamming weight of* τ*-NAF of all length-*l *elements of* $Z(\tau)$ *is denoted as* $AVGHW_l$*, then we have*

$$AVGHW_l = \frac{1}{3}\left(\frac{3l+5}{3} + \frac{l}{1-(-2)^l}\right). \tag{5}$$

Proof.

$$AVGHW_l = \frac{HW_l}{4m_l}$$
$$= \frac{-\frac{4(-1)^l}{27}\left((3l+5)(1-(-2)^l)+3l\right)}{4\frac{(-1)^l((-2)^l-1)}{3}}$$
$$= \frac{1}{3}\left(\frac{3l+5}{3} + \frac{l}{1-(-2)^l}\right). \quad \blacksquare$$

Theorem 3.7. *Suppose that the average density of nonzero coefficient c_i for every length l denoted as $AVGDensity_l$, then we have*

$$AVGDensity_l = \frac{1}{3}\left(1 + \frac{5}{3l} + \frac{1}{1-(-2)^l}\right). \tag{6}$$

Proof.

$$AVGDensity_l = \frac{AVGHW_l}{l}$$

By using equation (5), we get

$$AVGDensity_l = \frac{\frac{1}{3}\left(\frac{3l+5}{3} + \frac{l}{1-(-2)^l}\right)}{l}$$
$$= \frac{1}{3}\left(1 + \frac{5}{3l} + \frac{1}{1-(-2)^l}\right). \quad \blacksquare$$

Example 3.8. *The average hamming weight and density occurring among τ-NAF of an integer of element in $Z(\tau)$ with length, $l = 83$ are $28.22222222 \approx 29$ and $0.340026774 \approx \frac{1}{3}$ respectively.*

Example 3.9. *The average hamming weight and the average density occurring among τ-NAF of an integer of element in $Z(\tau)$ with length, $l = 163$ are $54.88888889 \approx 55$ and $0.33674165 \approx \frac{1}{3}$ respectively.*

This means that we have proved that the sequence of average density among τ-NAF's of length l is similar with NAF's. This is because our formula (6) is equal to Proposition 3.6 (see page 16 Ratsimihah and Prodinger (2005)) with their analysis on NAF's. Also surprisingly that fomula (6) is not equal to formula (1). We showed that formula (6) is more accurate compared to formula (1) that have been applied by previous researchers.

This study is particular about the accuracy of formula of average density and improving the proof made by Solinas (2000). It was built not for the purpose to speed up communication or denying the formula (1) which is suitable for $l > 2$ but the formula (6) is more accurate option in order to calculate the number of elliptic operations. The main purpose of our research is to prove that average density among τ-NAF's of length l is asymptotically $\frac{1}{3}$ as l increases will be easily accessible by the following Theorem.

Theorem 3.10. $\lim_{l\to\infty} AVGDensity_l = \frac{1}{3}$.

Proof. By using equation (6),

$$\begin{aligned}\lim_{l\to\infty} AVGDensity_l &= \frac{1}{3}\lim_{l\to\infty}\frac{1}{3}\left(1+\frac{5}{3l}+\frac{1}{1-(-2)^l}\right)\\ &= \frac{1}{3}.\end{aligned}$$

■

4. CONCLUSION

As we know the advantage of τ-adic method is it can eliminate the elliptic doublings in scalar multiplication method, and double the number of elliptic additions. This is a scalar expression that is equivalent to τ-NAF developed by some researchers for example Solinas (2000) and Joye and Tymen (2001). Since the hamming weight of a scalar representation is the product of its length and its density, our alternative formula (6) will help us to estimate the hamming weight of scalar based on τ-NAF's method. Therefore we can observe the effectiveness of that method in scalar multiplication compared to the ordinary τ-NAF.

REFERENCES

Avanzi, R. M., Heuberger, C. and Prodinger, H. 2005. *Minimality of the Hamming Weight of the τ-NAF for Koblitz Curves and Improved Combination with Point Halving*. http://eprint.iacr.org/2005/225.pdf

Brumley, B.B. and Jarvinen, K. 2007. Koblitz Curves and Integer Equivalents of Frobenius Expansions. *Lecturer Notes in Computer Science*. **4876**: 126-137. Springer.

Joye, M. and Tymen, C. 2001. Protection against Differential Analysis for Elliptic Curve Cryptography: An Algebraic Approach, in *Cryptography Hardware and Embedded Systems-CHES'***01**, *Lecturer Notes in Computer Science.* **2162**:377-390. Springer-Verlag.

Hakuta, K., Sato, H. and Takagi, T. 2010. Explicit Lower bound for the Length of Minimal Weight τ-adic Expansions on Koblitz Curves. *Journal of Math-for-Industry.* **2** (2010A-7): 75-83.

Ratsimihah, J.R. and Prodinger, H. 2005. *Redundant Representation of Numbers*. *http://resources.aims.ac.za/archive/2005/joel.ps*

Koblitz, N. 1987. Elliptic curve cryptosystem. *Mathematics Computation.* **48** (177): 203-209.

Koblitz, N. 1992. CM curves with good cryptographic properties. *Proc. Crypto'***91**: 279-287. Springer-Verlag.

Li, M., Qin, B., Kong, F. and Li, D. 2007**.** Wide-W-NAF Method for Scalar Multiplication on Koblitz Curves. *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/ Distributed Computing*:143-148.

Lin, T. C. 2009. Algorithm on Elliptic Curves over fields of Characteristic Two with Non-Adjacent Forms. *International Journal of Network Security.* **9**(2): 117-120.

Roy, S. S., Robeiro, C., Mukhopadhyay, D., Takahashi, J. and Fukunaga, T. 2011. *Scalar Multiplication on Koblitz Curves Using* τ^2 *-NAF*. http://eprint.iacr.org/2011/318.pdf

Solinas, J. A. 1997. An Improved Algorithm for Arithmetic on a Family of Elliptic Curve*s,* in B. Kaliski, editor, *Advance in Cryptology-CRYPTO'***97**. *Lecture Notes in Computer Science*. **1294**: 357-371. Springer-Verlag.

Solinas, J. A. 2000. Efficient Arithmetic on Koblitz Curves, in Kluwer Academic Publishers, Boston, Manufactured in the Netherlands, *Design, Codes, and Cryptography.* **19**:195-249.