# On addition-subtraction chains of numbers with low Hamming weight

**Dustin Moody**[1], **Amadou Tall**[2]

[1] Computer Security Division, National Institute of Standards and Technology
Gaithersburg, Maryland, 20899, USA
e-mail: dustin.moody@nist.gov

[2] Departement de Mathematiques et Informatique, Université Cheikh Anta Diop de Dakar
Dakar, Senegal
e-mail: amadou7.tall@ucad.edu.sn

**Abstract:** An addition chain is a sequence of integers such that every element in the sequence is the sum of two previous elements. They have been much studied, and generalized to addition-subtraction chains, Lucas chains, and Lucas addition-subtraction chains. These various chains have been useful in finding efficient exponentiation algorithms in groups. As a consequence, finding chains of minimal length is critical. The main objective of this paper is to extend results known for addition chains to addition-subtraction chains with Lucas addition-subtraction as a tool to construct such minimal chains. Specifically, if we let $\ell^-(n)$ stand for the minimal length of all the Lucas addition-subtraction chains for $n$, we prove $|\ell^-(2n) - \ell^-(n)| \leq 1$ for all integers $n$ of Hamming weight $\leq 4$. Thus, to find a minimal addition-subtraction chain for low Hamming weight integers, it suffices to only consider odd integers.
**Keywords:** Addition chains, subtraction chains, addition-subtraction chains, Lucas chains.
**2010 Mathematics Subject Classification:** 11Y55, 11Y16.

# 1 Introduction

Addition chains are an important tool to perform fast exponentiation in groups [4, 5, 7, 10, 11, 12, 16]. In particular, in groups where computing $-P$ is as easy as computing $P$ (where $P$ is an element of the group), then addition-subtraction chains become more interesting than the general addition chains [1, 3, 7, 8, 10, 11, 12]. We begin by defining the various types of addition chains and their generalizations. Let $n$ be an integer.

## 1.1 Definitions

**Definition 1.** *[6] A sequence of positive integers $C = \{1 = a_0, a_1, \cdots, a_l = n\}$ is called an addition chain for $n$ if and only if for every $a_i \in C$ (with $i > 0$), there exists $a_j, a_k \in C$ with $j, k < i$ such that*

$$a_i = a_j + a_k.$$

As an example, the following is an addition chain for 42:

$$\{1, 2, 4, 5, 10, 11, 21, 42\}.$$

**Definition 2.** *[14] A sequence of positive integers $C = \{1 = a_0,\ a_1,\ \ldots,\ a_l = n\}$ is called an addition-subtraction chain for $n$ if and only if for every $a_i \in C$ , there exists $a_j, a_k \in C$ with $j, k < i$ such that*

$$a_i = a_j + a_k \text{ or } a_i = a_j - a_k.$$

We now give an addition-subtraction chain for 42:

$$\{1, 2, 3, 4, 8, 11, 22, 44, 42\}.$$

**Definition 3.** *[9] A sequence of positive integers $C = \{1 = a_0,\ a_1,\ \ldots,\ a_l = n\}$ is called a Lucas addition chain if and only if for every $a_i \in C$ ( with $i > 0$), there exists $a_j, a_k \in C$ with $j, k < i$ such that*

$$a_i = a_j + a_k \text{ where either } a_j = a_k \text{ or } |a_j - a_k| \in C.$$

The addition chain we gave above for 42 is not a Lucas addition chain, since $5 = 4 + 1$, but $4 - 1$ is not in the chain. An example of a Lucas addition chain for 42 is

$$\{1, 2, 3, 4, 7, 14, 28, 42\}.$$

**Definition 4.** *[13] A sequence of positive integers $C = \{1 = a_0,\ a_1,\ \ldots,\ a_l = n\}$ is called a Lucas addition-subtraction chain if and only if for any $a_i \in C$ (with $i > 0$), there exists $a_j, a_k \in C$ with $j, k < i$ such that*

$$a_i = \begin{cases} a_j + a_k & \text{and } |a_j - a_k| \in C \cup \{0\}, \\ & \text{or} \\ a_j + 1, & \\ & \text{or} \\ a_j - a_k. & \end{cases}$$

The addition-subtraction chain we gave above is not a Lucas addition-subtraction chain for 42, because $11 = 3 + 8$, but $8 - 3$ is not in the chain. An example of a Lucas addition-subtraction chain is given by

$$\{1, 2, 3, 6, 12, 24, 48, 42\}.$$

In this work, we will focus on Lucas addition-subtraction chains [13]. These chains have a weaker restriction than Lucas addition chains. This allows these chains to have shorter chains than Lucas addition chains for infinitely many integers. Lucas addition-subtraction chains are one of the simpler known methods for computing addition-subtraction chains [15, 13]. It is therefore important to see what properties of addition chains (and Lucas addition chains and addition-subtraction chains) are true for the Lucas addition-subtraction chains.

Formally, the length of a chain is the number of elements in the chain, except we do not count $a_0 = 1$. That is, the length of the chain $\{a_0 = 1, a_1, ..., a_l\}$ is $l$. We are usually interested in chains with as few elements as possible. Let $\ell(n)$ and $\ell^-(n)$ denote the minimal lengths of an addition chain and addition-subtraction chain for $n$ respectively. Similarly, we define $\ell_L(n)$ and $\ell_L^-(n)$ for the Lucas version of the same type of chains.

Recall that the Hamming weight $h(n)$ of a positive integer $n$ is the number of 1s in the binary expansion of $n$. Concretely, if $n = \sum e_i 2^i$, with $e_i \in \{0, 1\}$, then the Hamming weight of $n$ is $h(n) = \sum e_i$. We also recall the definition of the non-adjacent form of any integer $n$, which gives a signed representation of $n$ with minimal weight. The non-adjacent form of $n$ is the unique signed-digit representation $n = \sum k_i 2^i$, with $k_i \in \{-1, 0, 1\}$ and $k_i k_{i+1} = 0$. We define $\bar{s}_2(n) = \sum |k_i|$ as the weight of the non-adjacent form of $n$.

## 1.2 Motivation

We note that because an addition chain is also an addition-subtraction chain, then $\ell^-(n) \leq \ell(n)$ for any $n$. We similarly have that

$$\ell^-(n) \leq \ell_L^-(n) \leq \ell_L(n), \quad \ell(n) \leq \ell_L(n),$$

for any $n$. However, the relationship between the values of $\ell(n)$ and $\ell_L^-(n)$ is not so simple. For example, there are infinitely many integers such that $\ell_L^-(n) \leq \ell(n)$ but at the same time, we have infinitely many integers such that $\ell_L^-(n) \geq \ell(n)$ (see [13, 14]).

This paper investigates the minimal length of Lucas addition-subtraction chains for integers with low Hamming weight $h(n)$. Our main result will be to prove that if $h(n) \leq 4$, then

$$\ell_L^-(n) + 1 = \ell_L^-(2n). \tag{1}$$

Equation (1) is known to hold for addition chains [6], as well as for addition-subtraction chains (when $h(n) \leq 4$) [14]. We thus show that in order to find the minimal length of a Lucas addition-subtraction chain, it suffices to only consider odd integers (at least for integers with $h(n) \leq 4$). As a consequence, we establish that Lucas addition-subtraction chains give minimal addition-subtraction chains for integers $n$, with $h(n) \leq 4$. Our proof will also be constructive, providing a method to construct these minimal Lucas addition-subtraction chains (and addition-subtraction chains), for all integers of Hamming weight $\leq 4$.

For several of our proofs, we will need an important theorem due to Volger [14]. For integers of low Hamming weight, Volger's results give the length of a minimal addition-subtraction chain.

**Theorem 1.1** (Volger)**.** *Let $\ell^-(n)$ be the minimal length of all addition-subtraction chains for $n$, then:*

1. $\ell^-(2^a) = a$,
2. $\ell^-(2^a + 2^b) = a + 1$, *for all* $a > b$,
3. $\ell^-(2^a - 2^b) = a + 1$, *for all* $b \leq a - 3$,

4. $\ell^-(2^a + 2^b + 2^c) = a + 2$, *for all* $a,\ b,\ c$ *such that* $c < b \leq a - 2$,

5. $\ell^-(2^a + 2^{a-1} + 2^b) = a + 2$, *for all* $b \leq a - 4$,

6. $\ell^-(n) \geq \lfloor \log(n) \rfloor + 2$, *if* $\bar{s}_2(n) \geq 3$.

We note there are two cases for integers of Hamming weight 3 not covered by Volger. The first is when $n = 2^a + 2^{a-1} + 2^{a-2}$. However, in this case we observe $n = 2^{a+1} - 2^{a-2}$, and so by Volger's third result, $\ell^-(n) = a + 2$. The remaining case is when $n = 2^a + 2^{a-1} + 2^{a-3}$. The non-adjacent form is $n = 2^{a+1} - 2^{a-1} + 2^{a-3}$, and so by part 6 of Volger's results we know $\ell^-(n) \geq a+2$ and since it is easy to construct an addition-subtraction chain for $n$ of length $a+2$, then $\ell^-(n) = a+2$. Combining these two cases with 4) and 5) above, we've shown $\ell^-(n) = a+2$, for any $n = 2^a + 2^b + 2^c$, where $a > b > c$.

# 2 Minimal lengths for low Hamming weight numbers

We will start by quantifying $\ell_L^-(n)$ for all integers of Hamming weight less than four. Similar results are known for addition chains and addition-subtraction chains [6, 14]. The minimal lengths we prove for Lucas addition-subtraction chains are equal to the minimal lengths for addition-subtraction chains (for integers with $h(n) \leq 4$).

**Theorem 2.1.** *Let $n$ be a positive integer. Depending on the Hamming weight of $n$, we have the following:*

- *For h(n)=1, $n = 2^a$, we have $\ell_L^-(n) = a$.*
- *For h(n)=2, $n = 2^a + 2^b$, we have $\ell_L^-(n) = a + 1$.*
- *For h(n)=3, $n = 2^a + 2^b + 2^c$, we have $\ell_L^-(n) = a + 2$.*
- *For h(n)=4, $n = 2^a + 2^b + 2^c + 2^d$, we have $\ell_L^-(n) = a + 2$ or $a + 3$.*

The proof will be given by the next three propositions. The first covers integers which are either a power of 2, or a sum or difference of powers of 2.

**Proposition 2.1.1.** *Let $n$ be a positive integer.*

1. *If $n = 2^a$, then $\ell_L^-(n) = a$.*
2. *If $n = 2^a - 2^{a-1}$, then $\ell_L^-(n) = a - 1$.*
3. *If $n = 2^a - 2^{a-2}$, then $\ell_L^-(n) = a$.*
4. *If $n = 2^a - 2^b$ with $b \leq a - 3$, then $\ell_L^-(n) = a + 1$.*
5. *If $n = 2^a + 2^b$ with $b < a$, then $\ell_L^-(n) = a + 1$.*

*Proof.* 1. If $n = 2^a$, then an obvious chain is given by $\{1, 2, 4, ..., 2^{a-1}, 2^a\}$. Any chain of length $a - 1$ can have no element greater than $2^{a-1}$, hence the given chain is minimal.

2. If $n = 2^a - 2^{a-1}$, then $n = 2^{a-1}$, and so $\ell_L^-(n) = a - 1$ by the first case.

3. If instead $n = 2^a - 2^{a-2}$, then we can write $n = 2^{a-1} + 2^{a-2}$ and the result now follows from the proof for integers of the form $2^a + 2^b$, which we give in case 5.

4. If $n = 2^a - 2^b$ and $b \leq a - 3$, then a Lucas addition-subtraction chain with length $a + 1$ for $n$ is
$$\{1, 2, 2^2, ..., 2^{a-b}, 2^{a-b} - 1, 2^{a-b+1} - 2^1, ..., 2^a - 2^b\}.$$
From Volger's results, we know any chain for $n$ must have length at least $a + 1$, and so the given chain is minimal.

5. If $n = 2^a + 2^b$, Volger's results give us that $\ell^-(n) = a + 1$. So we need only note that there is a Lucas addition-subtraction chain of length $a + 1$ for $n$:
$$\{1, 2, 2^2, ..., 2^{a-b}, 2^{a-b} + 1, 2^{a-b+1} + 2^1, ..., 2^a + 2^b\}.$$
That is, the chain consists of $a - b$ doublings, followed by a +1 step, and then $b$ doublings.

□

For integers with Hamming weight 3, we can also determine their minimal length exactly.

**Proposition 2.1.2.** *If $n = 2^a + 2^b + 2^c$, then $\ell_L^-(n) = a + 2$.*

*Proof.* As noted previously, it follows from Volger's results that $\ell^-(n) = a + 2$ and so $\ell_L^-(n) \geq a + 2$. We can easily construct a chain of length $a + 2$ for $n$. We first do $a - b$ doublings, followed by a +1 step. Then we do $b - c$ more doublings, followed by a $+1$ step and then $c$ doublings:

$$\{1, 2, 2^2, ..., 2^{a-b}, 2^{a-b} + 1, 2^{a-b+1} + 2^1, ..., \\ 2^{b-c}(2^{a-b} + 1) = 2^{a-c} + 2^{b-c}, 2^{a-c} + 2^{b-c} + 1, ..., 2^a + 2^b + 2^c\}.$$

This proves the desired result. □

**Proposition 2.1.3.** *If $n = 2^a + 2^b + 2^c + 2^d$, then $\ell_L^-(n) = a + 2$ or $a + 3$.*

*Proof.* If $\bar{s}_2(n) < 3$ then $n$ is of the form $2^a$ or $2^a \pm 2^b$, and $\ell_L^-(n) = a + 2$ by Proposition 2.1.1. For the rest of the proof, we can therefore assume $\bar{s}_2(n) \geq 3$ and so we have $\ell_L^-(n) \geq a + 2$ by Volger's part 6). Just as we did in the proof of the previous proposition, we can easily create a chain of length $a + 3$ for $n$. We first do $a - b$ doublings, followed by a +1 step, then $b - c$ more doublings, followed by a $+1$ step and then $c - d$ doublings. Finally, we do one last +1 step, and $d$ doublings.

$$\{1, 2, 2^2, ..., 2^{a-b}, 2^{a-b} + 1, 2^{a-b+1} + 2^1, ..., 2^{b-c}(2^{a-b} + 1) = 2^{a-c} + 2^{b-c}, 2^{a-c} + 2^{b-c} + 1, ...,$$

$$2^{c-d}(2^{a-c}+2^{b-c}+1), 2^{c-d}(2^{a-c}+2^{b-c}+1) = 2^{a-d}+2^{b-d}+2^{c-d}, 2^{a-d}+2^{b-d}+2^{c-d}, ..., 2^a+2^b+2^c+2^d\}.$$

This shows that $\ell_L^-(n) \leq a + 3$. □

To show we can have both $\ell_L^-(n) = a+2$ and $a+3$ for an integer $n$ with $h(n) = 4$, we give some infinite families with these different minimal lengths.

**Proposition 2.1.4.** *If $n = 2^a + 2^b + 2^c + 2^d$, with $a - b = c - d = j$ (meaning that $n = 2^a + 2^{a-j} + 2^c + 2^{c-j}$), then $\ell_L^-(n) = a + 2$.*

*Proof.* Note that we can write $n$ as

$$n = 2^{c-j}(2^{a-c} + 1)(2^j + 1).$$

From Proposition 2.1.1, we know $\ell_L^-(2^{a-c}+1) = a-c+1$ and $\ell_L^-(2^j+1) = j+1$. By the factor method (Corollary 11 of [13]), we have

$$\ell_L^-((2^{a-c} + 1)(2^j + 1)) \leq \ell_L^-((2^{a-c} + 1) + \ell_L^-((2^j + 1) = a - c + j + 2.$$

That is, we can construct a Lucas addition-subtraction chain for $(2^{a-c} + 1)(2^j + 1)$ of length $a - c + j + 2$. If we augment that chain by $c - j$ doublings, then we will get a chain for $n$ of length $a - c + j + 2 + c - j = a + 2$.

□

**Proposition 2.1.5.** *If $n = 2^a + 2^{a-1} + 2^{a-2} + 2^b$ with $0 < b < a - 3$, then $\ell_L^-(n) = a + 3$.*

*Proof.* We know that

$$n = 2^a + 2^{a-1} + 2^{a-2} + 2^b = 2^{a+1} - 2^{a-2} + 2^b$$

and from Volger's results

$$\ell^-(2^{a+1} - 2^{a-2} + 2^b) \geq a + 3,$$

so likewise $\ell_L^-(n) \geq a+3$. However, from Proposition 9 we see that $a+3$ is also an upper bound, and hence we have equality. □

We conclude this section with two results we will need in the proof of our main theorem. The first gives another infinite family with $h(n) = 4$, and $\ell^-(n) = a + 2$. The second shows that any minimal chain for integers of Hamming weight 2 contains only elements of a certain form.

**Proposition 2.1.6.** *If $n = 2^a + 7 \cdot 2^d$ with $a \geq d + 3$, then $\ell_L^-(n) = a + 2$.*

*Proof.* The proof will be done in two cases. We first investigate the case where $d = 0$ or $1$, and then after treat the case $d > 1$.

If $d \leq 1$, then

$$n = 2^a + 7 \cdot 2^d = 2^a + (2^3 - 1) \cdot 2^d = 2^a + 2^{d+3} - 2^d = 2^{d+3}(2^{a-d-3} + 1) - 2^d$$

and a chain can be constructed easily as follows:

$$c = \{1,\ \cdots,\ 2^{a-d-3},\ 2^{a-d-3} + 1,\ 2 \cdot (2^{a-d-3} + 1),\ \cdots,$$

$$2^{d+3} \cdot (2^{a-d-3} + 1),\ 2^{d+3}(2^{a-d-3} + 1) - 2^d\}.$$

If instead $d > 1$ then we prove $\ell_L^-(n) = a + 2$ by induction on $(a,\ d)$. When $(a, d) = (5, 2)$, then $n = 2^5 + 7 \cdot 2^2 = 60$, and a corresponding minimal chain is $\{1, 2, 4, 8, 7, 15, 30, 60\}$ and $\ell^-(n) = a+2$. Let us now suppose now that the result holds for $(k, d)$ (with $2 \leq d \leq k-3$), and we will prove that it also holds for all $(k + 1, d)$ with $2 \leq d \leq k - 2$. We have

$$n = 2^{k+1} + 7 \cdot 2^d = 2(2^k + 7 \cdot 2^{d-1}).$$

We know that $\ell_L^-(2^k + 7 \cdot 2^{d-1}) = k + 2$ by the induction hypothesis (as well as the case where $d - 1 \leq 1$ which we treated previously). We simply add one doubling step to the chain for $2^k + 7 \cdot 2^{d-1}$ to get a chain for $n = 2^{k+1} + 7 \cdot 2^d$ of length $k + 3$, and the theorem holds. □

We conclude this section with an important lemma we will need in the proof of our main result.

**Lemma 2.2.** *The only elements in a minimal chain for $2^a + 2^b$ are of the form $2^i$ with $i \leq a - b$, or $2^{a-b-1} + 1$, or $2^k(2^{a-b} + 1)$ where $k \leq b$.*

*Proof.* Let us consider the chains

$$c_1 = \{1,\ 2,\ ,\cdots,\ 2^{a-b},\ 2^{a-b} + 1, 2(2^{a-b} + 1),\ \cdots,\ 2^b(2^{a-b} + 1) = n\}$$

and

$$c_2 = \{1,\ 2,\ ,\cdots,\ 2^{a-b-1},\ 2^{a-b-1} + 1,\ 2^{a-b} + 1, 2(2^{a-b} + 1),\ \cdots,\ 2^b(2^{a-b} + 1) = n,\}$$

which are minimal Lucas addition-subtraction chains for $n$. We will prove that they are the only possible such chains for $n$. For that, we assume we have some other minimal chain for $n$ and examine the first non-doubling step:

$$c' = \{1,\ 2,\ ,\cdots,\ 2^\alpha,\ c'_{\alpha+1},\ \cdots,\ n\}.$$

We note the possible values for $c'_{\alpha+1}$ are $2^\alpha + 1$ or $2^\alpha - 2^\beta$ or $2^\alpha + 2^\beta$ and the total number of steps left (after $c'_{\alpha+1}$) to reach $n$ is

$$r = a + 1 - (\alpha + 1) = a - \alpha.$$

We will investigate the three cases and show they lead to the desired result.

**Case I:** $c'_{\alpha+1} = 2^\alpha - 2^\beta$ and thus the maximal value that we can reach from $c_{\alpha+1}$ is $2^r(c_{\alpha+1}) = 2^{a-\alpha}(2^\alpha - 2^\beta) = 2^a - 2^{a-\alpha+\beta} < n$, which shows that this case is not possible.

**Case II:** $c'_{\alpha+1} = 2^\alpha + 2^\beta$**,** with $\beta \geq 1$. This means that $2^\alpha - 2^\beta$ belongs to the chain and is consequently a power of 2. The only possibility is $\beta = \alpha - 1$.
So the chain $c'$ is of the form

$$c' = \{1,\ 2,\ ,\cdots,\ 2^\alpha,\ 2^\alpha + 2^{\alpha-1},\ \cdots,\ n\}$$

Let us assume that there is a second non-doubling step. The chain $c'$ will now look like:

$$c = \{1,\ 2,\ ,\cdots,\ 2^{\alpha},\ \underbrace{2^{\alpha}+2^{\alpha-1}}_{non-doubling1},\ \cdots, 2^{\beta}(2^{\alpha}+2^{\alpha-1}),\ \underbrace{c'_{\alpha+\beta+2}}_{non-doubling2},\ \overbrace{\cdots,\ n}^{a-\alpha-\beta-1 \text{ steps}}\ \}$$

and

$$c'_{\alpha+\beta+2} = \begin{cases} 2^{\beta}(2^{\alpha}+2^{\alpha-1})+1, & \\ 2^{\beta}(2^{\alpha}+2^{\alpha-1})+2^{\gamma}, & \text{with } 2^{\beta}(2^{\alpha}+2^{\alpha-1})-2^{\gamma} \in c' \text{ and } \gamma \leq \alpha \\ 2^{\beta}(2^{\alpha}+2^{\alpha-1})-2^{\gamma}, & \text{and } \gamma \leq \alpha \\ 2^{\beta}(2^{\alpha}+2^{\alpha-1})+2^{\gamma}(2^{\alpha}+2^{\alpha-1}), & \text{with } (2^{\alpha}+2^{\alpha-1})(2^{\beta}-2^{\gamma}) \in c' \text{ and } \gamma \leq \beta \\ 2^{\beta}(2^{\alpha}+2^{\alpha-1})-2^{\gamma}(2^{\alpha}+2^{\alpha-1}), & \text{and } \gamma \leq \beta. \end{cases}$$

Examining each of these $5$ cases shows they aren't possible because even if the remaining steps are all doublings, then the maximum value in the chain that will be reached is of the form

$$2^{a-\alpha-\beta-1}(c_{\alpha+\beta+2}) = 2^{a-1}+\cdots < 2^{a} < n.$$

So all the remaining steps must be doublings, and we have

$$n = 2^{r}(c_{\alpha+1}) = 2^{a-\alpha}(2^{\alpha}+2^{\alpha-1}) = 2^{a}+2^{a-1}.$$

This is impossible if $a > b+1$, and so we must have $b = a-1$. We conclude that every element of the chain is one of the desired forms.

**Case III:** $c'_{\alpha+1} = 2^{\alpha}+1$**.** If $\alpha = a-b$ then the remaining steps must all be doublings, else the chain's maximum value will be less than $n$. If $\alpha = a-b-1$, then $c'_{\alpha+1} = 2^{a-b-1}+1$, $c'_{\alpha+2} = c'_{\alpha}+c'_{\alpha+1} = 2^{a-b}+1$, followed by $b$ doublings.
If $\alpha > a-b$, then the maximum value that the chain can reach is $2^{a-\alpha}(2^{\alpha}+1) = 2^{a}+2^{a-\alpha} < n$.
If $\alpha < a-b-1$, then the maximum value that the chain can reach is $2^{a-\alpha}(2^{\alpha}+1) = 2^{a}+2^{a-\alpha} > n$. However, this means that the minimal chain for $n$ must contain a back step (a step involving subtraction). Using a result from [14], we have that

$$n \leq 2^{d-1}F_{f+3},$$

with $d$ and $f$ being respectively the number of doubling and the number of back steps, and $(F_n)$ is the $n$-th Fibonacci number. Having $f \geq 1$ implies that $n \leq 2^{a}$ which leads to a contradiction.

□

# 3 The main result

Our main result compares $\ell_L^-(n/2)$ and $\ell_L^-(n)$, for even integers with low Hamming weight.

**Theorem 3.1.** *If the Hamming weight of an even integer $n$ is $\leq 4$, then*

$$\ell_L^-(n/2) + 1 = \ell_L^-(n). \tag{2}$$

*Proof.* Let $n$ be an even integer. When the Hamming weight of $n$ is three or less, the results easily follow from Theorem 6 and the fact that $s_2(n) = s_2(n/2)$. For example, if $n = 2^a + 2^b$, then $\ell_L^-(n) = a + 1 = \ell_L^-(2^{a-1} + 2^{b-1}) + 1 = \ell_L^-(n/2) + 1$. Similarly, if the minimal weight is three or less it is easy to see the result holds. If $\overline{s}_2(n) = 2$, we use Proposition 2.1.1. When $\overline{s}_2(n) = 3$, then $n = 2^x \pm 2^y \pm 2^z$ and $\ell_L^-(2^x \pm 2^y \pm 2^z) = x+2$, except when $y = x-3,\ z = \{x-4,\ x-5\}$ and then $\ell_L^-(2^x - 2^{x-3} - 2^z) = x + 1$ (see [13, 14]). In either case, $\ell_L^-(n) = \ell_L^-(n/2) + 1$.

We now turn to the more difficult case when $s_2(n) = 4$, i.e., $n = 2^a + 2^b + 2^c + 2^d$. From above, we can also take the minimal weight $\overline{s}_2(n)$ to be at least 4. By Proposition 2.1.3, we know that $\ell_L^-(n) = a + 2$ or $a + 3$. Assume first that the minimal chain is of length $a + 3$. Then $n/2 = 2^{a-1} + 2^{b-1} + 2^{c-1} + 2^{d-1}$, and so $\ell_L^-(n/2) = a+1$ or $a+2$. If it were $a+1$, then we could obviously create a chain for $n$ of length $a + 2$, by simply appending $n$. This is a contradiction, and so $\ell_L^-(n/2) = a + 2$ and equation (2) holds.

For the remainder of the proof we therefore assume $\ell_L^-(n) = a + 2$. Let

$$C = \{c_0,\ c_1,\ c_2,\ \cdots,\ c_{a+1},\ c_{a+2}\}$$

be a minimal Lucas addition-subtraction chain for $n$. We have four possible relations between $c_{a+1}$ and $c_{a+2}$ (see Definition 4). If $c_{a+2} = c_{a+1} + 1$, then $c_{a+1}$ also has Hamming weight at least 4, and so $\ell_L^-(c_{a+1}) \geq a + 2$, a contradiction. If $c_{a+2} = 2c_{a+1}$, then $\{c_0,\ c_1,\ c_2,\ \cdots,\ c_{a+1}\}$ is a chain for $n/2$ and clearly $\ell_L^-(n/2) + 1 = \ell_L^-(n)$.

The remaining two cases are when $c_{a+2} = c_{a+1} \pm c_f$, for some $c_f$ in the chain. For the first case, $c_{a+2} = c_{a+1} - c_f$, then $c_{a+1} > n$. It must be that $c_{a+1}$ has Hamming weight less than three, since otherwise $\ell_L^-(c_{a+1}) \geq a + 2$, which contradicts that we already have a chain for $c_{a+1}$ of length $a + 1$. If the Hamming weight of $c_{a+1}$ were 1, then it follows $c_{a+1} = 2^{a+1}$ and $c_l = 2^l$ for all $l = 1,\ \cdots,\ a + 1$. This means that $n$ is of the form $2^{a+1} - 2^k$, for some $k$, and so $\overline{s}_2(n) = 2$, a case we already dealt with. The remaining possibility in this case is that the Hamming weight of $c_{a+1}$ is 2, so $c_{a+1} = 2^a + 2^j$, for some $j > b$. Note that we know $c_{a+1} \neq 2^{a+1} + 2^j$, as with $a + 1$ steps, the maximum value in a chain is $2^{a+1}$. By Lemma 2.2, the only steps in a chain for integers of the form $2^a + 2^j$ are of the form $2^i$, $2^i(2^{a-j} + 1)$, or $2^{a-j-1} + 1$. We get that $n$ must be of the form:

$$n = 2^a + 2^j - 2^i \ \text{ or } n = 2^a + 2^j - 2^i(2^{a-j} + 1) \ \text{ or } n = 2^a + 2^j - 2^{a-j-1} - 1.$$

Since $c_{a+1} \geq 2^a$, we know that any minimal chain for it must have length at least $a + 1$. But it is easy to see that no matter which of the first two forms $n$ has, there are chains of length $a + 1$ for $n/2$, showing that $\ell_L^-(n/2) = a + 1$. More concretely, for $n = 2^a + 2^j - 2^i$, perform $a - j$ doublings, do one +1 step, then $j - 1$ more doublings, followed by a back step of subtracting $2^{i-1}$.

Similarly, for $n = 2^a + 2^j - 2^i(2^{a-j}+1)$, begin with $a-j$ doublings, then do a +1 step, then $j-1$ doublings and finally a back step of subtracting $2^{i-1}(2^{a-j}+1)$. The case $n = 2^a + 2^j - 2^{a-j-1} - 1$ is not possible since $n$ is even.

The final case left to consider is $c_{a+2} = c_{a+1} + c_f$, which implies that $\ell_L^-(c_{a+1}) \leq a+1$. We examine several subcases depending on whether $\ell_L^-(c_{a+1}) < a$, $\ell_L^-(c_{a+1}) = a$, or $\ell_L^-(c_{a+1}) = a+1$.

1. $\ell_L^-(c_{a+1}) < a$, meaning that $c_{a+1} \leq 2^{a-1}$. From this we can deduce that $c_f = 2^a$, or $2^{a-1} + 2^\eta$, since $c_f \geq 2^{a-1} + 2^b + 2^c + 2^d$ and $\ell_L^-(c_f) \leq a$. If $c_f = 2^{a-1} + 2^\eta$, then $c_{a+1} = n - c_f = 2^{a-1} + 2^b + 2^c + 2^d - 2^\eta \leq 2^{a-1}$. In fact, the inequality must be strict as we cannot have $2^b + 2^c + 2^d = 2^\eta$. However, then we can conclude that $\ell_L^-(c_{a+1}) \geq \ell^-(c_{a+1}) \geq \lfloor \log(c_{a+1}) \rfloor + 2 = a$ which contradicts $\ell_L^-(c_{a+1}) < a$.

   If instead $c_f = 2^a$, then $c_{a+1} = 2^b + 2^c + 2^d$. The only possible chain is

$$C = \{1,\ 2,\ 4,\ \cdots,\ c_f = c_a = 2^a,\ c_{a+1},\ c_{a+2}\}.$$

   Then (for some $i$ and $j$) we have $c_{a+1} = 2^i \pm 2^j = 2^b + 2^c + 2^d$ which is only possible when $i - j = 3$ and $b = c + 1 = d + 2$. We can then write $n$, as well as $n/2$, in the form $2^a + 7 \cdot 2^d$. By Lemma 2.1.6, the desired result holds.

2. If $c_{a+1} \leq n/2$ and $\ell_L^-(c_{a+1}) = \{a,\ a+1\}$, then necessarily $c_f \geq n/2$ which means that $a \geq \ell_L^-(c_f) \geq \ell^-(c_f) \geq \lceil \log(c_f) \rceil \geq a$. But then $c_f$ is either $2^a$ or $2^{a-1} + 2^\alpha$ with $\alpha > b-1$.

   If $c_f = 2^a$, then $c_{a+1} = 2^i \pm 2^j$ with $a \geq i > j \geq 0$ since $c_{a+1}$ is obtained from the minimal chain for $c_f$. However, this implies $2^b + 2^c + 2^d = 2^i \pm 2^j$, which leads to the desired result as shown above in the last case.

   If $c_f = 2^{a-1} + 2^\alpha$, then the only possibilities for $c_s = c_f - c_{a+1}$ are $2^i$ or $2^i(2^{a-1-\alpha}+1)$ or $2^{a-1-\alpha}+1$ and so $n = c_{a+1} + c_f = 2c_f - c_s$ has the following possibilities $2^a + 2^{\alpha+1} - 2^k$ or $2^a + 2^{\alpha+1} + 2^k(2^{a-\alpha-1}+1)$ or $2^a + 2^{\alpha+1} - 2^{a-1-\alpha} - 1$. If $n = 2^a + 2^{\alpha+1} - 2^k$, then as seen above it must be that $n = 2^a + 7 \cdot 2^d$. If $n = 2^a + 2^{\alpha+1} - 2^k(2^{a-\alpha-1}+1) = 2^{\alpha+1}(2^{a-\alpha-1}+1) - 2^k(2^{a-\alpha-1}+1)$, then

$$c = \{1,\ 2,\ \cdots, 2^{a-\alpha-1},\ 2^{a-\alpha-1}+1,\ 2(2^{a-\alpha-1}+1,\ \cdots,\ 2^k(2^{a-\alpha-1}+1),\ \cdots,$$
$$2^{\alpha+1}(2^{a-\alpha-1}+1),\ n = 2^{\alpha+1}(2^{a-\alpha-1}+1) - 2^k(2^{a-\alpha-1}+1)\},$$

   which is a chain for $n$ of length $a+2$. We can similarly construct a chain for $n/2$ of length $a+1$ (we just replace $\alpha$ by $\alpha - 1$ and $k$ by $k-1$ in the expression of $n$ to get $n/2$). The case $n = 2^a + 2^{\alpha+1} - 2^{a-1-\alpha} - 1$ is not possible since $n$ is even.

3. $\ell_L^-(c_{a+1}) = a$ and $c_{a+1} > n/2$.

   As $c_{a+1} > n/2$, then it follows that $c_{a+1} = 2^a$ or $2^{a-1} + 2^\alpha$, with $\alpha < a - 1$; otherwise $c_{a+1} > n$ which contradicts our assumption that $n$ isn't obtained from a subtraction step. Note also that $\alpha \geq b$, otherwise $c_{a+1} < n/2$. We suppose first $c_{a+1} = 2^a$, and so $c_f = 2^b + 2^c + 2^d$ and the chain for $n$ must be

$$C = \{c_0,\ c_1,\ c_2,\ \cdots,\ \underbrace{2^b + 2^c + 2^d}_{c_f}, \cdots,\ \underbrace{2^a}_{c_{a+1}},\ \underbrace{n}_{c_{a+2}}\}.$$

We note that $2^a$ has been reached with $a+1$ steps, meaning the only non doubling step involves $c_f$. But then $c_f = 2^b + 2^c + 2^d$ can only be obtained from the sum or the difference of two powers of 2. We have already observed this is only possible if $b = c+1 = d+2$, meaning $n = 2^a + 2^{d+2} + 2^{d+1} + 2^d = 2^a + 7 \cdot 2^d$. The result now follows from an appeal to Lemma 2.1.6.

The remaining possibility in this subcase is if $c_{a+1} = 2^{a-1} + 2^\alpha$, which makes $c_f = 2^{a-1} + 2^b + 2^c + 2^d - 2^\alpha$. If $\alpha$ is equal to one of $b, c$, or $d$, then $c_f$ has Hamming weight 3. By Theorem 2.1, $\ell_L^-(c_f) = (a-1)+2 = a+1$. This is a contradiction, since $c_f$ appeared in the chain $C$ before $a+1$ steps. On the other hand, if $\alpha \neq b$ and $\alpha \neq c$ and $\alpha \neq d$ then it's not hard to check that $s^-(c_f) \geq 3$ (the assumption $2^{a-1} + 2^b + 2^c - 2^\alpha = 2^i \pm 2^j$ leads to a contradiction). Then using Volger's inequality

$$\ell_L^-(c_f) \geq \ell^-(c_f) \geq \lfloor \log(c_f) \rfloor + 2 = (a-1) + 2 = a+1.$$

This is again a contradiction.

4. $\ell_L^-(c_{a+1}) = a+1$, and $c_{a+1} > n/2$. Since $c_{a+1} > n/2$, we must have that either $c_{a+1} = 2^{a-1} + 2^\alpha + 2^\beta$ or $c_{a+1} = 2^a + 2^\alpha$ (with $\alpha, \beta < a$). Here, we have omitted the cases $c_{a+1} = 2^a - 2^\alpha$ and $c_{a+1} = 2^{a-1} + 2^\alpha - 2^\beta$ with $\alpha > b$ to keep the condition $c_{a+1} > n/2$. If $c_{a+1} = 2^a - 2^\alpha$, then $n = 2^a - 2^\alpha + 2^i$ or $n = 2^a - 2^\alpha + 2^i(2^{a-\alpha} - 1) = 2^i(2^{\alpha - i} + 1)(2^{a-\alpha} - 1)$. The case $n = 2^a - 2^\alpha + 2^i$ is not possible since $\overline{s}_2(n) = 4$. The case $n = 2^i(2^{\alpha-i} + 1)(2^{a-\alpha} - 1)$ is possible and we obtain the appropriate chain using the factor method. If $c_{a+1} = 2^{a-1} + 2^\alpha - 2^\beta$, then $c_f = 2^{a-1} + 2^b + 2^c + 2^d - 2^\alpha + 2^\beta$. This case will be simultaneously studied with $c_{a+1} = 2^{a-1} + 2^\alpha + 2^\beta$ leading to $c_f = 2^{a-1} + 2^b + 2^c + 2^d - 2^\alpha - 2^\beta$.

Supposing first that $c_{a+1} = 2^a + 2^\alpha$, we know by Lemma 2.2 that $c_f$ is of the form $2^i$ or $2^j(2^{a-\alpha} + 1)$or $2^{a-\alpha-1} + 1$, for some $i$ or $j$. If $c_f = 2^i$, then $n = c_{a+1} + c_f = 2^a + 2^\alpha + 2^i$, which would contradict $n$ having Hamming weight 4. If $c_f = 2^{a-\alpha-1} + 1$ then $n = 2^a + 2^\alpha + 2^{a-\alpha-1} + 1$, which contradicts $n$ being even. Alternatively, if $c_f = 2^j(2^{a-\alpha} + 1)$ then

$$n = 2^a + 2^b + 2^c + 2^d = 2^a + 2^\alpha + 2^{a-\alpha+j} + 2^j.$$

Checking the possible combinations, we must either have ($b = \alpha$ and $c = a - \alpha + j$ and $d = j$), or alternatively ($b = a - \alpha + j, c = \alpha$, and $d = j$). In both situations, we see that this implies $a - b = c - d$. By Proposition 2.1.4, $\ell_L^-(n) = a+2$. But then Proposition 2.1.4 also applies to $n/2$, which proves the result we want.

The final subcase to investigate is when $c_{a+1} = 2^{a-1} + 2^\alpha \pm 2^\beta$. It follows that $\{c_0, c_1, c_2, \cdots, c_{a+1}\}$ is a minimal Lucas addition-subtraction chain for $c_{a+1}$. Since $c_{a+2} = c_{a+1} + c_f$, then

$$c_f = 2^{a-1} + 2^b + 2^c + 2^d - 2^\alpha \pm 2^\beta.$$

We investigate $c_f$ depending on the possibilities for $\alpha$ and $\beta$. First, one can notice that $c_f > 2^{a-2}$ and $\ell_L^-(c_f) \leq a$, and so therefore $\ell_L^-(c_f)$ is either $a, a-1$ or $a-2$, implying

$\overline{s}_2(c_f) \leq 3$. On the other hand, it is easy to check that:

$$\overline{s}_2(c_f) = \begin{cases} 2 & \text{when } \alpha = b \text{ and } \beta = c \text{ or } \beta = d, \\ 2 & \text{when } \alpha = b+1 \text{ and } 2^c + 2^d + 2^\beta = 2^b - 2^I, \\ 3 & \text{when } \alpha = b \text{ and } \beta = \{c \pm 1,\ d \pm 1\}, \\ 3 & \text{when } \alpha = b \text{ and } 2^c + 2^d + 2^\beta = 2^I - 2^J, \\ 3 & \text{when } \alpha = b+1 \text{ and } 2^c + 2^d + 2^\beta = 2^{b-1} - 2^I, \\ 3 & \text{when } \alpha = b+1 \text{ and } \beta = c \text{ or } \beta = d, \\ 3 & \text{when } \alpha > b+1 \text{ and } 2^b + 2^c + 2^d + 2^\beta = 2^I - 2^J \text{ and } I = \alpha - 1, \\ \geq 4 & \text{in all others general cases and they aren't of interest here.} \end{cases}$$

when $c_f = 2^{a-1} + 2^b + 2^c + 2^d - 2^\alpha \pm 2^\beta$.

We conclude by examining each of the possibilities for $c_f$. The possibilities for $\overline{s}_2(c_f) = 2$ are:

- $c_f = 2^{a-1} + 2^c$,
- $c_f = 2^{a-1} + 2^d$,
- $c_f = 2^{a-1} - 2^I$ with $2^c + 2^d + 2^\beta = 2^b - 2^I$ ($I = b - 3$).
- $c_f = 2^{a-1} - 2^J$ with $2^b + 2^c + 2^d + 2^\beta = 2^I - 2^J$ and $I = \alpha = a - 2$.

The case when $c_f = 2^{a-1} + 2^d$, meaning that $c_{a+1} = 2^{a-1} + 2^b + 2^c$, is not possible since we cannot obtain $c_{a+1}$ from a minimal Lucas addition-subtraction chain for $c_f$ due to the fact that $b > c > d$. Similar logic holds for when $c_f = 2^{a-1} + 2^c$. If $c_f = 2^{a-1} - 2^I$, then $I = b-3$ and $\alpha = a-2,\ \beta = \{b+1,\ b-1,\ b-2,\ b-3\}$. Then $n$ will be $2^a + 2^{a-1} + 2^{b+1} - 2^{b-3} - 2^\beta$ and it leads to contradictions with the fact that $n = 2^a + 2^b + 2^c + 2^d$ for all the values of $\beta$ except $\beta = b + 1$ which leads to $n = 2^a + 7 \cdot 2^{a-4}$ for which the proof holds. If $c_f = 2^{a-1} - 2^J$ then $I = a - 2,\ J = a - 6,\ \beta = \{b+1,\ b-1,\ b-2,\ b-3\}$ and it leads to $n \in \{71 \cdot 2^{k+6},\ 39 \cdot 2^{k+5},\ 75.2^{k+6},\ 77 \cdot 2^{k+6}\}$ and the proof holds for all these possibilities of $n$. For example, one can easily see that $\ell_L^-(71 \cdot 2^{k+6}) = \ell_L^-(71) + k + 6$, and the main result clearly holds for numbers of this form.

The possibilities for $\overline{s}_2(c_f) = 3$ are:

- $c_f = 2^{a-1} - 2^c + 2^d$, $c_f = 2^{a-1} + 2^c - 2^d$,
- $c_f = 2^{a-1} + 2^{c-1} + 2^d$, $c_f = 2^{a-1} + 2^c + 2^{d-1}$,
- $c_f = 2^{a-1} + 2^I - 2^J$ when $2^c + 2^d + 2^\beta = 2^I - 2^J$ ,
- $c_f = 2^{a-1} - 2^b + 2^c$, $c_f = 2^{a-1} - 2^b + 2^d$,
- $c_f = 2^{a-1} - 2^{b-1} - 2^I$ when $2^c + 2^d + 2^\beta = 2^I - 2^J$ with $I = b - 1$,
- $c_f = 2^{a-1} - 2^I - 2^J$ when $2^b + 2^c + 2^d + 2^\beta = 2^I - 2^J$ with $I = \alpha - 1$,
- $c_f = 2^{a-2} + 2^I - 2^J$ when $2^b + 2^c + 2^d + 2^\beta = 2^I - 2^J$ with $I \neq a - 2$.

All these cases lead to $\ell_L^-(c_f) = a+1 > a$ which is impossible, except for $c_f = 2^{a-1} - 2^{b-1} - 2^I$ or $c_f = 2^{a-1} - 2^I - 2^J$ or $c_f = 2^{a-2} + 2^I - 2^J$ for which $\ell_L^-(c_f) = a$. If $c_f = 2^{a-1} - 2^{b-1} - 2^I$ or $c_f = 2^{a-1} - 2^I - 2^J$, then $b-1 = a-1-3$, $I = \{a-1-4,\ a-1-5\}$ or $I = a-1-3,\ J = \{a-1-4,\ a-1-5\}$. One can easily see that these two cases are also impossible since $I = b-1$ in the first case and $I - J > 3$ in the second case. If $c_f = 2^{a-2} + 2^I - 2^J$, then $c_{a+1} = 2^{a-1} + 2^{a-2} - 2^\beta$ since $\alpha = a-2$ and $I = \max b,\ \beta + 1 > \beta \geq J$. If $\beta = J$, then $n = 2^a + 2^I - 2^{I-3} = 2^a + 7 \cdot 2^{I-3}$ and the proof holds. If $\beta > J$, then $n = \{2^a + 2^{I-1} + 2^J,\ 2^a + 2^{I-2} + 2^J\}$ and both cases are impossible.

Having exhausted all possibilities, we see that in every case we have demonstrated that if $h(n) \leq 4$, then $\ell_L^-(2n) = \ell_L^-(n) + 1$.

□

As an immediate corollary, we have the following:

**Corollary 3.1.1.** *If $s_2(n) \leq 4$, then $\ell_L^-(2^k n) = \ell_L^-(n) + k$.*

# 4 Conclusion

We can ask a question related to Hansen numbers [6]: Is there any integer $n$ such that $\ell_L^-(2n) < \ell_L^-(n)$? This conjecture is known to be true for addition chains. Namely, for $n = 375404703$, $\ell(n) = 35 > 34 = \ell(2n)$, see [2]. The analogous question remains open for addition-subtraction chains, and Lucas addition chains. Our paper has proven that there is no number verifying the conjecture with Hamming weight $\leq 4$. In fact, we also proved that $|\ell^-(2n) - \ell^-(n)| \leq 1$ for all Hamming weight $\leq 4$. One can investigate if $\ell^-(2n) = \ell^-(n) = a+2$ for some integers $n$ of Hamming weight $4$.

The techniques used in the proofs of this paper could also be investigated further in order to design a polynomial-time algorithm for computing fast exponentiations. We leave this for future work.

# Acknowledgements

The authors would like to acknowledge the precious support of Maurice Mignotte. This work was finalized during a research visit of one of the authors at the Max-Planck Institute for Mathematik in Bonn MPIM.

# References

[1] M. Ciet, M. Joye, K. Lauter,and P. L. Montgomery, Trading inversions for multiplications in elliptic curve cryptography, *Des. Codes Cryptogr.* **39** (2006), 189-206.

[2] N. Cliff, Shortest addition chains, 2011. Available at http://wwwhomes.uni-bielefeld.de/achim/addition_chain.html.

[3] V. Dimitrov, L. Imbert, and P. K. Mishra, Efficient and secure elliptic curve point multiplication using double-base chains, in *Advances in Cryptology - ASIACRYPT 2005*, Lect. Notes in Comp. Sci., Vol. **3788**, Springer-Verlag, 2005, pp. 59-78.

[4] P. Downey, B. Leong and R. Sethi, Computing sequences with addition chains', *SIAM J. Comput.* 10 (1981), 638-646.

[5] D.M. Gordon, A survey of fast exponentiation methods, *Journal of Algorithms* **27** (1998), 129-146.

[6] D. Knuth, *The art of computer programming*, 2nd ed., Addison-Wesley, 1969.

[7] K. Koyama, Y Tsuruoka, Speeding elliptic cryptosystems using a signed binary window method, in *Advances in Cryptology - CRYPTO 1993*, Lect. Notes in Comput. Sci. Vol. 740, Springer-Verlag, 1993, pp. 345-357.

[8] D. Le, Fast quadrupling of a point in elliptic curve cryptography, preprint, 2011, https://eprint.iacr.org/2011/039.

[9] P. Montgomery, Evaluating recurrences of form $X_{m+n} = f(X_m,\ X_n,\ X_{m-n})$ via Lucas chains, preprint, 1992, ftp://ftp.cwi.nl/pub/pmontgom/Lucas.ps.gz.

[10] F. Morain, and J. Olivos, Speeding up the computation on an elliptic curve using addition-subtaction chains, *RAIRO Theor. Inform. Appl.* **24** (1990), 531-543.

[11] Y. Sakai, and K. Sakurai, Efficient scalar multiplication on elliptic curve with direct computations of several doublings, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* **84** (2001), 120-129.

[12] T. Takagi, D. Reis, S. Yen and B. Wu, Radix-r non-adjacent form and its application to pairing-based cryptosystem, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* **89** (2006), 115-123.

[13] A. Tall, A generalization of Lucas addition chains, *Bull. Math. Soc. Sci. Math. Roumanie* **55** (2013), 1. Available at https://eprint.iacr.org/2011/378.pdf.

[14] H. Volger, Some results on addition/subtraction chains, *Inform. Process. Lett.* **20** (1985), 155-160.

[15] C. Wang, C. Chang and C. Lin, *A method for computing Lucas sequences*, Comput. Math. Appl. **38** (1999), 187-196.

[16] Y. Yacobi, *Exponentiating faster with addition chains*, in *Advances in Cryptology - EUROCRYPT 1990* Lect. Notes in Comput. Sci., Vol. **473**, Springer-Verlag, 1991, pp. 222 - 229.