An N-D cryptoscheme

Yi-Shiung Yeh
Wei-Shen Lai
I-Te Chen

Department of Computer Science and Information Engineering
National Chiao-Tung University
1001 Ta Hsueh Road
Hsinchu
Taiwan 30050
R.O.C.
E-mail: (ysyeh, wslai, itchen)@csie.nctu.edu.tw

ABSTRACT

In this paper, we construct a nondeterministic number representation (NNR) system which maps an integer to a set of vectors and a deterministic number representation (DNR) system which maps an integer to a single vector. Applying NNR system and DNR system, a cryptosystem named as an NNR-DNR Cipher (NDC) is constructed. The main property of NDC is that a plaintext may be probabilistically mapped to different ciphertexts for a given key, this feature increase the difficulty of cryptanalysis.

Keywords: Cryptography, NNR (Non-deterministic number representation), DNR (Deterministic number representation), NDC (NNR-DNR Cipher).

1 INTRODUCTION

For the ciphers which encrypt a plaintext to the same ciphertext as key is unchanged, an eavesdropper may determine the frequency of certain plaintext by counting the appearance frequency of the corresponding ciphertext, even he doesn’t know the exact plaintext [1, 3]. The information leakage may imperil the application system applying the ciphers if the set of transferred messages has few members.
In this paper, we suggest a new cipher which has no above weakness. The idea is that a value may have different representations in a number system. Thus, we can select the underlying number system to allow a plaintext mapping to multiple ciphertexts. The selected ciphertext corresponding to a plaintext may be different each time for a given key, thus the appearance frequency of a plaintext can be hidden. The details are described in the following sections.

2. BASIC CONCEPTS AND NOTATIONS

2.1 Notations and Vector Operations

The symbol $|X|$ denotes the number of elements in a set $X$ and $2^X$ is the power set of $X$.

**Definition 2.1.1** Let $V$ be a set of $n$-tuple vectors and $v$ be an $n$-tuple vector. The inner product of $V$ and $v$ is defined as $V \cdot v = \{ v \cdot v_i \mid v \in V \}$. The operation is trivially commutative.

**Definition 2.1.2** Let $v_p = <p_1, p_2, ..., p_n>$ and $v_q = <q_1, q_2, ..., q_n>$. We say that $v_p \leq v_q$ if and only if $p_i \leq q_i$ for $i = 1, 2, ..., n$.

**Definition 2.1.3** Let $v = <w_1, w_2, ..., w_n>$ be an $n$-tuple vector, $v$ is called a positive vector if $w_i > 0$, for $i = 1, 2, ..., n$. The complete set of the positive vector $v$ is defined as:

$$C(v) = \{ <z_1, z_2, ..., z_n> \mid 0 \leq z_i \leq w_i, \text{ for } i = 1, 2, ..., n \}.$$

2.2 Number Representations

**Definition 2.2.1** Given two positive vectors, $v_b$ and $v_u$, the range $S(v_b, v_u)$ of $v_u$ with respect to $v_b$ is defined as:

$$S(v_b, v_u) = \{ i \mid i \in C(v_u) \cdot v_b \}.$$

$v_b = <b_1, b_2, ..., b_n>$ is called the base vector and $v_u = <u_1, u_2, ..., u_n>$ is called the boundary vector. We also define that:

$$T(v_b, v_u) = \{ i \mid 0 \leq i \leq v_b \cdot v_u \}.$$

**Definition 2.2.2** The set $(S(v_b, v_u), v_b, v_u)$ together with $+$ (an addition), and $\cdot$ (a product), denoted as $(S(v_b, v_u), v_b, v_u, +, \cdot)$, is called a number representation system.

For simplicity, throughout this paper we use $(S(v_b, v_u), v_b, v_u)$ to denote a number representation system [4].
For a number representation system \((S(v_b, v_u), v_b, v_u)\), we can construct a mapping \(f(s_{v_b, v_u}, v_b, v_u)\) from \(S(v_b, v_u)\) to \(2\hat{C}(v_u)\) as \(f(s_{v_b, v_u}, v_b, v_u)(r) = \{u | u \cdot v_b = r, u \in C(v_u)\}\), and another mapping \(g(s_{v_b, v_u}, v_b, v_u)\) from \(C(v_u)\) to \(S(v_b, v_u)\) as \(g(s_{v_b, v_u}, v_b, v_u)(v) = v \cdot v_b\).

**Results 2.2.1**

a) \(|f(s_{v_b, v_u}, v_b, v_u)(r)| \geq 1\) \(\forall r \in S(v_b, v_u)\)

b) \(|f(s_{v_b, v_u}, v_b, v_u)(r)| = 0\) \(\forall r \in T(v_b, v_u) - S(v_b, v_u)\).

c) \(g(s_{v_b, v_u}, v_b, v_u)\) is onto from \(C(v_u)\) to \(S(v_b, v_u)\).

d) \(g(s_{v_b, v_u}, v_b, v_u)\) is not onto from \(C(v_u)\) to \(T(v_b, v_u)\) unless \(T(v_b, v_u) = S(v_b, v_u)\).

**Example 2.2.1** Let \((S(v_b, v_u), v_b, v_u)\) be a number representation system, \(v_b = <7, 1, 2>\) and \(v_u = <1, 2, 1>\), we have

**Table 2.1**

<table>
<thead>
<tr>
<th>Number</th>
<th>Representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>&lt;000&gt;</td>
</tr>
<tr>
<td>1</td>
<td>&lt;010&gt;</td>
</tr>
<tr>
<td>2</td>
<td>&lt;011&gt;, &lt;020&gt;</td>
</tr>
<tr>
<td>3</td>
<td>&lt;011&gt;</td>
</tr>
<tr>
<td>4</td>
<td>&lt;021&gt;</td>
</tr>
<tr>
<td>5</td>
<td>11</td>
</tr>
</tbody>
</table>

\(C(v_u) = \{<000>, <001>, <010>, <011>, <020>, <021>, <100>, <101>, <110>, <111>, <120>, <121>\}\).

\(S(v_b, v_u) = \{0, 1, 2, 3, 4, 7, 8, 9, 10, 11\}\).

\(T(v_b, v_u) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}\)

\(f(s_{v_b, v_u}, v_b, v_u)(2) = \{<001>, <020>\}\).

\(g(s_{v_b, v_u}, v_b, v_u)(<001>) = <001> \cdot v_b = <001><712> = 2\).

\(|f(s_{v_b, v_u}, v_b, v_u)(2)| = 2\).
Theorem 2.2.1 Let \((S_{(v_b, v_u)}, v_b, v_u)\) be a number representation system, then \(f_r(S_{(v_b, v_u)}, v_b, v_u)(r) \cap f_{r'}(S_{(v_b, v_u)}, v_b, v_u)(r') = \emptyset\) for all \(r \neq r'\).

Proof. If \(f_r(S_{(v_b, v_u)}, v_b, v_u)(r) \cap f_{r'}(S_{(v_b, v_u)}, v_b, v_u)(r') \neq \emptyset\) where \(r \neq r'\), then there will be a \(v \in C(v_u)\) so that \(v \in f_r(S_{(v_b, v_u)}, v_b, v_u)(r)\) and \(v \in f_{r'}(S_{(v_b, v_u)}, v_b, v_u)(r')\).

That is, \(v \cdot v_b = r\) and \(v \cdot v_b = r'\), a contradiction.

2.3 Deterministic Number Representations (DNR)

Definition 2.3.1 For a number representation system \((S_{(v_b, v_u)}, v_b, v_u)\), if each integer in \(S_{(v_b, v_u)}\) maps to at most one vector in \(C(v_u)\), that is \(|f_r(S_{(v_b, v_u)}, v_b, v_u)(r)| \leq 1\) for all \(r \in S_{(v_b, v_u)}\), we say that \((S_{(v_b, v_u)}, v_b, v_u)\) is a deterministic number representation (DNR) system.

Results 2.3

a) \(|f_r(S_{(v_b, v_u)}, v_b, v_u)(r)| = 1, \forall r \in S_{(v_b, v_u)}\).

b) For a DNR \((S_{(v_b, v_u)}, v_b, v_u)\), \(g: S_{(v_b, v_u)} v_b, v_u\) is a 1 to 1 mapping from \(C(v_u)\) to \(S_{(v_b, v_u)}\).

Theorem 2.3.1 Let \((S_{(v_b, v_u)}, v_b, v_u)\) be a number representation system. If \(b_1 = 1\) and \(b_i > \sum_{j=1}^{i-1} u_j * b_j\) for \(i = 2, \ldots, n\) then \((S_{(v_b, v_u)}, v_b, v_u)\) is a DNR system.

Proof. Assume that \((S_{(v_b, v_u)}, v_b, v_u)\) is not a DNR system.

Then \(\exists v_m \neq v_i\) s.t. \(v_m \cdot v_b = v_i \cdot v_b\).

Let \(v_m = <z_{m1}, z_{m2}, \ldots, z_{mn}>\) \(0 \leq z_{mi} \leq u_i\) \(\forall i = 1, 2, \ldots, n\).

Without loss of generality, we process them from \(n\) down to \(i\).

We can find the first \(i\) s.t. \(z_{mi} \neq z_{li}\) and assume that \(z_{mi} > z_{li}\).

\[
\sum_{j=1}^{n} z_{mj} * b_j = \sum_{i=1}^{n} z_{ij} * b_j
\]
\[ * b_i + \sum_{j=1 \atop j \neq i}^{n} z_{mj} * b_j = z_{mi} * b_i + \sum_{j=1 \atop j \neq i}^{n} z_{ij} * b_j \]

\[(z_{mi} - z_{lj}) * b_l = \sum_{j=1}^{i-1} (z_{lj} - z_{mj}) * b_j + \sum_{j=i+1}^{n} (z_{lj} - z_{mj}) * b_j \]

\[z_{lj} = z_{mj} \quad \forall j = (i + 1), \quad n,\]

\[\sum_{j=i+1}^{n} (z_{lj} - z_{mj}) * b_j = 0\]

\[(z_{mi} - z_{li}) * b_i = \sum_{j=1}^{i-1} (z_{lj} - z_{mj}) * b_j,\]

\[b_i = \sum_{j=1}^{i-1} \frac{(z_{lj} - z_{mj})}{(z_{mi} - z_{li})} * b_j \leq \sum_{j=1}^{i-1} * b_j \quad \text{a contradiction.} \quad \square\]

**Theorem 2.3.2** Let \((S_{(v_b, v_u)}, \nu_b, \nu_u)\) be a DNR system. If \(b_1 = 1\) and

\[b_i = \left( \sum_{j=1}^{i-1} u_j * b_j \right) + 1, \text{ for } i = 2, 3, ..., n, \text{ then } S_{(v_b, v_u)} = T_{(v_b, v_u)}\]

**Proof.** It is obvious that \(S_{(v_b, v_u)} \subseteq T_{(v_b, v_u)}\).

We shall prove \(T_{(v_b, v_u)} \subseteq S_{(v_b, v_u)}\) by mathematical induction on the lengths of \(v_b\) and \(v_u\).

Basic of induction: let \(n = 1\), i.e., \(v_u = <u_1>\) and \(v_b = <b_1>\).

\[\forall r \in [0, u_1 * b_1] = T_{(v_b, v_u)}\]

\[0 \leq r \leq u_1 \quad \text{thus } <r> \in C(v_u).\]

\[<r> \cdot <b_1> = r * b_1 = r \quad \text{thus } r \in S_{(v_b, v_u)}\]

Hypothesis: Let \(n = k\) and the result holds. That is,

\[\forall r \in 0, \sum_{j=1}^{k} u_j * b_j = T_{(v_b, v_u)} \quad \exists \nu_m = <z_1, z_2, ..., z_k>, \nu_m \in C(v_u)\]
s.t. \( r = v_m \cdot v_b = \sum_{j=1}^{k} z_j \cdot b_j \).

Consider \( n = k + 1 \):

\[
b_{k+1} = \left( \sum_{j=1}^{k} u_j \cdot b_j \right) + 1.
\]

\[
\forall r \in \left[ 0, \sum_{j=1}^{k+1} u_j \cdot b_j \right] = T_{(v_b, v_r)}.
\]

Let \( r' = r \mod b_{k+1} \).

Let \( z_{k+1} = \frac{r}{b_{k+1}} \leq \frac{u_{k+1} \cdot b_{k+1} + \sum_{j=1}^{k} u_j \cdot b_j}{b_{k+1}} = u_{k+1} \).

Then \( r = z_{k+1} \cdot b_{k+1} + r' \).

\[
r' < b_{k+1} = \left( \sum_{j=1}^{k} u_j \cdot b_j \right) + 1.
\]

\[
r' \leq \left( \sum_{j=1}^{k} u_j \cdot b_j \right).
\]

By induction hypothesis:

\[
\exists v'_m = <z_1, z_2, \ldots, z_k> \text{ s.t. } r' = v'_m \cdot v_b = \sum_{j=1}^{k} z_j \cdot b_j.
\]

Thus \( \exists v_m = <z_1, z_2, \ldots, z_{k+1}>, v_m \in C(v_0), \)

\[
\text{s.t. } v_m \cdot v_b = \sum_{j=1}^{k+1} z_j \cdot b_j = z_{k+1} \cdot b_{k+1} + \sum_{j=1}^{k} z_j \cdot b_j = z_{k+1} \cdot b_{k+1} + r' = r.
\]

Therefore, \( r \in S_{(v_b, v_r)}. \) \( \square \)

2.4 Nondeterministic Number Representations (NNR)

Definition 2.4.1 A number representation system is a nondeterministic number representation (NNR) system if it is not a DNR.
THEOREM 2.4.1 Let \((S_{v_b}, v_b, v_u)\) be a number representation system. If \(b_1 = 1\) and \(b_i \leq \sum_{j=1}^{i-1} u_j \cdot b_j\) for \(i = 2, \ldots, n\), then \((S_{v_b}, v_b, v_u)\) is an NNR system.

PROOF. Let \(0 \leq z_i \leq u_i \quad \forall i = 3, 4, \ldots, n\), and let\
\[v_m = \langle 0, 1, z_3, \ldots, z_n \rangle,\]
\[v_l = \langle b_2, 0, z_3, \ldots, z_n \rangle.\]

Clearly, \(v_m \neq v_l\).

Since \(b_2 \leq \sum_{j=1}^{2-1} u_j \cdot b_j = u_1\), then both \(v_m\) and \(v_l\) are in \(C(v_u)\).

\[v_m \cdot v_b = \langle 0, 1, z_3, \ldots, z_n \rangle \cdot \langle b_1, \ldots, b_n \rangle = b_2 + \sum_{i=3}^{n} z_i \cdot b_i.\]

\[v_l \cdot v_b = \langle b_2, 0, z_3, \ldots, z_n \rangle \cdot \langle b_1, \ldots, b_n \rangle = b_2 \cdot b_1 + \sum_{i=3}^{n} z_i \cdot b_i\]

\[= b_2 + \sum_{i=3}^{n} z_i \cdot b_i.\]

The vectors \(v_m\) and \(v_l\) map to the same integer.

Therefore, \((S_{v_b}, v_b, v_u)\) is an NNR system (by Definition 2.4.1). \(\square\)

THEOREM 2.4.2 Let \((S_{v_b}, v_b, v_u)\) be an NNR system. If \(b_1 = 1\) and \(b_i \leq \sum_{j=1}^{i-1} u_j \cdot b_j\) for \(i = 2, \ldots, n\), then \(S_{v_b} = T_{v_b}\).

PROOF. Clearly, \(S_{v_b} \subseteq T_{v_b}\).

We shall show that \(S_{v_b} \supseteq T_{v_b}\) by induction on the lengths \(v_B\) and \(v_U\) of \(v_b\) and \(v_u\).

Basic of induction: let \(n = 1\), i.e. \(v_u = \langle u_1 \rangle\) and \(v_b = \langle b_1 \rangle\).

\(\forall r \in [0, u_1 \cdot b_1] = T_{v_b}\).
\[ 0 \leq r \leq u_1 \text{ thus } r \in C(v_u), \]
\[ <r> \cdot <b_1> = r \cdot b_1 = r, \text{ thus } r \in S_{(v_b, v_u)}. \]

**Hypothesis:** Let \( n = k \) and the result holds.

\[ \forall \ r \in \left[ 0, \sum_{j=1}^{k} u_j \cdot b_j \right] = T_{(v_b, v_u)}, \ \exists \ v_m = <z_1, z_2, \ldots, z_k> \]

where

\[ 0 \leq z_j \leq u_j \ \forall j = 1, 2, \ldots, k \] (i.e. \( v_m \in C(v_u) \)) s.t. \( r = v_m \cdot v_b = \sum_{j=1}^{k} z_j \cdot b_j. \)

Consider \( n = k + 1. \)

\[ \forall \ r \in \left[ 0, \sum_{j=1}^{k+1} u_j \cdot b_j \right] = T_{(v_b, v_u)}. \]

**Case I**

\[ \frac{r}{b_{k+1}} > u_{k+1}, \text{ let } r' = r - u_{k+1} \cdot b_{k+1}. \]

\[ r \leq \sum_{j=1}^{k+1} u_j \cdot b_j \Rightarrow r' \leq \sum_{j=1}^{k+1} u_j \cdot b_j - u_{k+1} \cdot b_{k+1} = \sum_{j=1}^{k} u_j \cdot b_j. \]

By induction hypothesis:

\[ \exists <z_1, z_2, \ldots, z_k> \text{ where } 0 \leq z_j \leq u_j \ \forall j = 1, 2, \ldots, k, \]

s.t. \( r' = \sum_{j=1}^{k} z_j \cdot b_j. \)

Clearly, \( <z_1, z_2, \ldots, z_k, u_{k+1}> \in C(v_u) \) and

\[ <z_1, z_2, \ldots, z_k, u_{k+1}> \cdot v_b = r' + u_{k+1} \cdot b_{k+1} = r. \]

Thus, \( r \in S_{(v_b, v_u)}. \)

**Case II**

\[ \frac{r}{b_{k+1}} \leq u_{k+1}, \text{ let } r' = r \mod b_{k+1}. \]
AN N-D CRYPTOSCHEME

\[ r' < b_{k+1} \leq \sum_{j=1}^{k} u_j \cdot b_j \]

By induction hypothesis:

\[ \exists <z_1, z_2, \ldots, z_k> \text{ where } 0 \leq z_j \leq u_j \quad \forall \ j = 1, 2, \ldots, k, \]

s.t. \[ r' = \sum_{j=1}^{k} z_j \cdot b_j. \]

\[ |\bar{b}_{k+1}| \leq u_{k+1}, \text{ thus } <z_1, z_2, \ldots, z_k, \left| \frac{r}{b_{k+1}} \right| > \in C(v_u). \]

Thus, \[ r \in S_{(v_b, v_u)}. \]

\[ \square \]

Example 2.4.1 Let \((S_{(v_b, v_u)}, v_b, v_u)\) be a number representation system with \(v_b = <5, 7, 3, 1>\) and \(v_u = <2, 2, 2, 3>\). Table 2.2 lists the map of \(f_{S_{(v_b, \ldots, v_u)}}\).

\[ \text{Table 2.2} \]

An NNR System

<table>
<thead>
<tr>
<th>0</th>
<th>&lt;0000&gt;</th>
<th>17</th>
<th>&lt;2012&gt;&lt;2100&gt;&lt;1112&gt;</th>
<th>&lt;0203&gt;&lt;0210&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>&lt;0001&gt;</td>
<td>18</td>
<td>&lt;2101&gt;&lt;2022&gt;&lt;1113&gt;</td>
<td>&lt;1120&gt;&lt;0211&gt;</td>
</tr>
<tr>
<td>2</td>
<td>&lt;0002&gt;</td>
<td>19</td>
<td>&lt;2102&gt;&lt;2023&gt;&lt;1200&gt;</td>
<td>&lt;1121&gt;&lt;0212&gt;</td>
</tr>
<tr>
<td>3</td>
<td>&lt;0010&gt;&lt;0003&gt;</td>
<td>20</td>
<td>&lt;2103&gt;&lt;2110&gt;&lt;1201&gt;</td>
<td>&lt;1122&gt;&lt;0213&gt;&lt;0220&gt;</td>
</tr>
<tr>
<td>4</td>
<td>&lt;0011&gt;</td>
<td>21</td>
<td>&lt;2111&gt;&lt;1202&gt;&lt;1123&gt;</td>
<td>&lt;0221&gt;</td>
</tr>
<tr>
<td>5</td>
<td>&lt;0012&gt;&lt;1000&gt;</td>
<td>22</td>
<td>&lt;2112&gt;&lt;1203&gt;&lt;1210&gt;</td>
<td>&lt;0222&gt;</td>
</tr>
<tr>
<td>6</td>
<td>&lt;0013&gt;&lt;1001&gt;&lt;0020&gt;</td>
<td>23</td>
<td>&lt;2113&gt;&lt;2120&gt;&lt;1211&gt;</td>
<td>&lt;0223&gt;</td>
</tr>
<tr>
<td>7</td>
<td>&lt;0100&gt;&lt;1002&gt;&lt;0021&gt;</td>
<td>24</td>
<td>&lt;2200&gt;&lt;2121&gt;&lt;1212&gt;</td>
<td></td>
</tr>
</tbody>
</table>

(Table 2.2 Contd.)
| 8 | <1010><0101><1003> <0022> | 25 | <2201><2122><1213><1220> |
| 9 | <1011><0102><0023> | 26 | <2202><2123><1221> |
| 10 | <2000><1012><0110> <0103> | 27 | <2203><2210><1222> |
| 11 | <2001><1020><1013> <0111> | 28 | <2211><1223> |
| 12 | <2002><1100><1021> <0112> | 29 | <2212> |
| 13 | <2010><2003><1101> <0122><0013> | 30 | <2213><2220> |
| 14 | <2011><1102><1023> <0020><0121> | 31 | <2211> |
| 15 | <2012><1110><0122> <0201><1103> | 32 | <2222> |
| 16 | <2013><2020><1111> <0202><0123> | 33 | <2223> |

**Theorem 2.4.3** Let \((S_{(v_b, v_u)}, v_b, v_u)\) be an NNR system. Let \(V_r = f(s(v_b, v_u), v_b, v_u)(r)\) for \(r\) in \(S_{(v_b, v_u)}\), and \(r_1, r_2, r_3 \in S_{(v_b, v_u)}\) where \(r_3 = r_1 + r_2\). If the boundary vector \(v_u\) is unlimited, \(|V_r| \geq \text{Max}\{|V_{r_1}|, |V_{r_2}|\}.

**Proof.** For any \(v \in V_{r_1}\) and \(w \in V_{r_2}\), \((v + w) \cdot v_b = v \cdot v_b + w \cdot v_b = r_1 + r_2 = r_3 \Rightarrow (v + w) \in V_{r_3}\) under the condition that \(v_u\) is unlimited.

Thus, it is true that \(P = \{v_1 + w_i | v_1 \in V_{r_1}, w_i \in V_{r_2} \text{ for all } i \} \subseteq V_{r_3}\) and \(|P| \leq |V_{r_3}|\).

Because \(|P| = |V_{r_2}|\), this implies that \(|V_{r_2}| \leq |V_{r_3}|\).

With the same method, we can derive that \(|V_{r_1}| \leq |V_{r_3}|\).

That is, \(|V_{r_3}| \geq \text{Max}\{|V_{r_1}|, |V_{r_2}|\}. \quad \square\)

### 2.5 Combination of DNR and NNR

Given a DNR system \((S_{(v_{bd}, v_{ud})}, v_{bd}, v_{ud})\) and an NNR system \((S_{(v_{bn}, v_{un})}, v_{bn}, v_{un})\), we can construct a mapping \(h\) from \(S_{(v_{bn}, v_{un})}\) to \(2^S_{(v_{bd}, v_{ud})}\), where \(h(r) = \{s | s = g(s_{(v_{bd}, v_{ud})}, v_{bd}, v_{ud})(v), v \in f(s_{(v_{bn}, v_{un})}, v_{bn}, v_{un})(r) \cap C(v_{ud})\}\), and a mapping \(k\) from \(S_{(v_{bd}, v_{ud})}\) to \(S_{(v_{bn}, v_{un})}\), where \(k(s) = g(s_{(v_{bn}, v_{un})}, v_{bn}, v_{un})(v)\) for \(v \in f(s_{(v_{bd}, v_{ud})}, v_{bd}, v_{ud})(s)\).
Definition 2.5.1 Let \((S_{(v_{ud}, v_{ud})}, v_{bd}, v_{ud})\) be a DNR system and let \((S_{(v_{kn}, v_{kn})}, v_{ln}, v_{ln})\) be an NNR system. We say that the mapping \(h\) is **nice** if and only if \(v_{uN} \leq v_{ud}\) and \(S_{(v_{kn}, v_{kn})} = T_{(v_{kn}, v_{kn})}\).

**Properties 2.5.1** Let \((S_{(v_{ud}, v_{ud})}, v_{bd}, v_{ud})\) and \((S_{(v_{kn}, v_{kn})}, v_{ln}, v_{ln})\) be the same as in Definition 2.5.1. If the mapping \(h\) is nice, then the following properties hold:

a) \(|h(r)| \geq 1\) for all \(r\) in \(S_{(v_{kn}, v_{kn})}\).

b) \(h(r) \cap h(r') = \emptyset\) for all \(r \neq r'\).

c) \(k(c) = r\) for \(c \in h(r)\).

**Proof.**

a) Since \(v_{uN} \leq v_{ud}\) and \(g_{(S_{(v_{ud}, v_{ud})}, v_{bd}, v_{ud})}\) is a 1-1 and onto mapping from \(C(v_{ud})\) to \((S_{(v_{ud}, v_{ud})}\) (by Results 2.3.1 (b)), so that \(\forall r \in (S_{(v_{kn}, v_{kn})}, |h(r)| \geq 1\).

b) Since \(f_{(S_{(v_{kn}, v_{kn})}, v_{kn}, v_{kn})}(r) = \emptyset\) for all \(r \neq r'\) (by Theorem 2.2.1), and \(g_{(S_{(v_{ud}, v_{ud})}, v_{bd}, v_{ud})}\) is a 1-1 and onto mapping from \(C(v_{ud})\) to \(S_{(v_{kn}, v_{kn})}\) (by Results 2.3.1), so that \(h(r) \cap h(r') = \emptyset\) for all \(r \neq r'\).

c) For \(c \in h(r)\), \(\exists u \in f_{(S_{(v_{kn}, v_{kn})}, v_{kn}, v_{kn})}(r) \cap C(v_{ud})\)

\[s.t. c = g_{(S_{(v_{ud}, v_{ud})}, v_{bd}, v_{ud})}(u)\]

Thus \(v \in f_{(S_{(v_{bd}, v_{bd})}, v_{bd}, v_{ud})}(c)\) and \(g_{(S_{(v_{kn}, v_{kn})}, v_{kn}, v_{kn})}(v) = r\), then \(r\).

**Theorem 2.5.1** Let \((S_{(v_{ud}, v_{ud})}, v_{bd}, v_{ud})\) and \((S_{(v_{kn}, v_{kn})}, v_{ln}, v_{ln})\) be the same as in Definition 2.5.1. If \(h\) is nice, then \(|S_{(v_{kn}, v_{kn})}| > |S_{(v_{bd}, v_{bd})}|\).

**Proof.** \((S_{(v_{kn}, v_{kn})}, v_{ln}, v_{ln})\) is an NNR. It is obvious that \(|S_{(v_{kn}, v_{kn})}| = |C(v_{ln})|\).

By definition 2.5.1, if \(h\) is nice then \(v_{uN} \leq v_{ud} \Rightarrow C(v_{uN}) \leq |C(v_{ud})|\)

\((S_{(v_{bd}, v_{bd})}, v_{bd}, v_{ud})\) is a DNR, it is obvious that
Collecting above relations derives that
\[ |S_{(v_{bd}, v_{nd})}| > |S_{(v_{bn}, v_{nn})}| \]

CRYPTOSYSTEM

The mappings \( f(s_{v_{bn}, r_{bn}, v_{bn}, v_{bn}}) \) and \( g(s_{v_{bn}, r_{bn}, v_{bn}, v_{bn}}) \) can be used to construct encryption algorithms by keeping the base and boundary vectors as the secret keys. An encryption algorithm which bases on a \( f(s_{v_{bn}, r_{bn}, v_{bn}, v_{bn}}) \) maps a plaintext to a set of vector-type ciphertexts. However, such cryptosystem is insecure because the information of the underlying base and boundary vectors are easily analyzed, even though they are kept secret. An encryption algorithm which bases on a \( g(s_{v_{bn}, r_{bn}, v_{bn}, v_{bn}}) \) forms a cipher [6] which is also thought to be insecure [1, 4, 5]. Combining a \( f(s_{v_{bn}, r_{bn}, v_{bn}, v_{bn}}) \) and a \( g(s_{v_{bn}, r_{bn}, v_{bn}, v_{bn}}) \), that is a \( h \) mapping, seems to work well.

3. NDC

An NNR followed by a DNR determine a mapping \( h \) which maps an integer to a set of different integers. A cryptosystem bases on a nice mapping \( h \) is called an NNR-DNR cipher (NDC), as depicted in Figure 3.1, which may map a plaintext to a different ciphertext each time for a given key. The key value includes the base and boundary

![Figure 3.1. NDC cipher](image-url)
vectors \((v_{bN}, v_{uN}, v_{bD}, v_{uD})\) of the underlying NNR and DNR system. They should be kept secret. In the cryptosystem, \(S_{(v_{bN}, v_{uN})}\) is the plaintext space and \(S_{(v_{bD}, v_{uD})}\) is the ciphertext space. For decryption, the corresponding \(k\) mapping is utilized (by Properties 2.5.1 (c)).

3.2 Key Generation

The key value \((v_{bN}, v_{uN}, v_{bD}, v_{uD})\) should be selected so that the corresponding \(h\) mapping is nice (Definition 2.5.1), thus each plaintext in \(S_{(v_{bN}, v_{uN})}\) has at least a ciphertext in \(S_{(v_{bD}, v_{uD})}\) (Properties 2.5.1 (a)). A method of key generation is as follows:

1) Select a boundary vector \(v_u\) which should be positive.
2) Set both \(v_{uN}\) and \(v_{uD}\) to the value of \(v_u\).
3) Select the base vector of the underlying NNR, \(v_{bN}\), by Algorithm 3.2.1 (according to Theorem 2.4.1).
4) Select the base vector of the underlying DNR, \(v_{bD}\), by an algorithm similar to step 3 (according to Theorem 2.3.1).

Algorithm 3.2.1 (select base vector \(v_{bN}\)) [7]

Input:

\[\text{vector } v_{uN} = \langle u_1, u_2, \ldots, u_n \rangle.\]

Output:

\[\text{base vector } v_{bN} = \langle b_1, b_2, \ldots, b_n \rangle.\]

Process:

Begin:

1. Let \(b_1 = 1\)
2. For \(j = 2\) to \(n\)

Randomly [2] choose a number for \(b_j\) such that

\[b_{(j-1)} < b_j \leq \sum_{i=1}^{j-1} b_i \cdot u_i\]

End

3.3 Selection of Ciphertext

The \(f_{S_{(v_{bN}, v_{uN})}, v_{bN}}\) mapping of the underlying NNR may map an integer to multiple vectors. While encrypting, just one of the resultant vectors is selected. Algorithm 3.3.1 represents a selection method.
Algorithm 3.3.1 [7]

Input:
- integer \( x \) (the plaintext)
- a base vector \( v_b = \langle b_{i1}, b_{i2}, \ldots, b_{in} \rangle \)
- a boundary vector \( v_u = \langle u_{i1}, u_{i2}, \ldots, u_{in} \rangle \)

Output:
- a vector \( v = \langle v_1, v_2, \ldots, v_n \rangle \in C(v_u) \)

Process:

Begin

\[ m = x. \]

For \( i = n \) down to 2 do

Begin

\[ temp_m = m - \sum_{j=1}^{i-1} u_{ij} \cdot b_{ij} \]

if \( temp_m \leq 0 \) then \( lower = 0 \)

else \( lower = \left\lfloor \frac{temp_m}{b_{ii}} \right\rfloor + 1 \)

\[ upper = \min \left( \left\lfloor \frac{m}{b_{ii}} \right\rfloor, u_{ii} \right) \]

\( v_i = \) a random number in the range \([lower, upper]\)

\[ m = m - v_i \cdot b_{ii} \]

End

\( v_1 = m \)

End.

3.4 Concatenation of NDCs

The NDC ciphers can be concatenated as depicted in Figure 3.2 if the successor accepts all outputs of the predecessor. For example, given two NDC ciphers, NDC\(_1\) and NDC\(_2\), with mappings \( h_1 \) and \( h_2 \), respectively, the cipher, NDB\(_1\) followed by NDB\(_2\), works well if the input set of \( h_2 \) covers the output set of \( h_1 \).
3.5 Enhanced NDC

The nondeterministic property of an NDC derives from the underlying NNR system. However, an NNR does not distribute uniformly. For example, the distribution map of the NNR in Example 2.4.1 is graphically shown in Figure 3.3. In this example, there are 8 integers each mapped to exactly one vector. Such situation violates the requirement of nondeterministic mapping of NDC. Thus, some enhancement is necessary for validating an NDC.

Figure 3.3. Distribution map of the NNR in Example 2.4.1

3.5.1 Use the Middle Part of $S(v_b, v_w)$

Consider an NNR with mapping $f(s_{v_b, v_w}, v_b, v_w)$, which has the properties described in Theorem 2.4.1. By Theorem 2.4.3 we know that $|f(s_{v_b, v_w}, v_b, v_w)(r)|$ will increase with respect to $r$ if the boundary vector $v_{bN}$ is unlimited. Although, in a practical case, the boundary vector is always limited, $|f(s_{v_b, v_w}, v_b, v_w)(r)|$ is likely to just drop at tail if the
value of $v_{bN}$ is not too small, for instance Example 2.4.1. Thus, order $S_{(v_{bN}, v_{uN})}$ as an increasingly sequence, the middle part of $S_{(v_{bN}, v_{uN})}$ can be used.

The method is to add an offset value $X$ to a plaintext $m$ before encrypting, as depicted in Figure 3.4. Plaintexts are also limited below a threshold to prevent the low mappings values.

![Diagram of the cryptosystem with plaintext offset](image)

**Figure 3.4. The cryptosystem with plaintext offset**

### 3.6 Data Expansion

By Theorem 2.5.1, we know that the ciphertext space of an NDC is always larger than its plaintext space. This means that data expansion occurs while encrypting. As quantifying the data expansion rate of a cipher being

\[
\frac{\text{average length of ciphertexts}}{\text{average length of plaintexts}},
\]

the data expansion rate of an NDC is as below:

For an NDC with key $(v_{bN}, v_{uN}, v_{bD}, v_{uD})$, assuming plaintexts with equivalent frequency, the average length of a plaintext and a ciphertext will be

\[
\frac{\log_2((v_{bN} \cdot v_{uN})!)}{v_{bN} \cdot v_{uN}} \quad \text{and} \quad \frac{\log_2((v_{bD} \cdot v_{uD})!)}{v_{bD} \cdot v_{uD}},
\]

respectively.

Then the data expansion rate is

\[
\frac{(v_{bN} \cdot v_{uN}) \cdot \log_2((v_{bD} \cdot v_{uD})!)}{(v_{bD} \cdot v_{uD}) \cdot \log_2((v_{bN} \cdot v_{uN})!)}.
\]
As concatenating multiple NDCs, the data expansion rate will be

\[
\frac{(u_{bN1} \cdot v_{uN1}) \cdot \log_2((v_{D1} \cdot v_{uD1})!)}{(u_{D1} \cdot v_{uD1}) \cdot \log_2((v_{bN1} \cdot v_{uN1})!)}
\]

where \((u_{bN1}, v_{uN1})\) are the NNR's base and boundary vectors of the first NDC, \((u_{D1}, v_{uD1})\) are the DNR's base and boundary vectors of the last NDC.

4. SECURITY ANALYSIS

The security of an NDC heavily depend on the underlying NNR system which is a nonlinear transformation.

A well-designed NDC may probabilistically map a plaintext to different ciphertexts each time for a given key. The information of the frequency of a plaintext appearing are hidden. This straitens the cryptanalysis.

The base and boundary vectors are kept secret, thus an NDC forms a black box that maps an integer to another integer. If the secret keys are large enough, an attacker is difficult to analyze the intermediate vector value for a given plaintext-ciphertext pair. Since the NDC scheme is not a cipher of iterating weak functions, such as the Feistel structure ciphers, the famous known/unknown-text attacks like the linear and differential attacks seem to be difficult to apply on it.

5. CONCLUSIONS

An NDC cipher may map a plaintext to different ciphertexts each time for a given key. If the underlying NNR and DNR system are chosen appropriately to contain the high nondeterministic property, the cryptanalysis is difficult.

Multiple NDCs can be concatenated together to be a more complicated and secure cipher. However, data expansion increases also.

NDCs are secret-key ciphers, all the underlying base and boundary vectors should be kept secret.

REFERENCES


Received March, 2001