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 interger 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 probabilisticly 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 transfered messages has few members.

Journal of Information & Optimization Sciences
Vol. 23 (2002), No. 1, pp. 19-36

0252-2667/02 $2.00+.25

In this paper, we suggest a new cipher which has no above weekness. 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 deails are described in the following sections.

2. BASIC CONCEPTS AND NOTATIONS

2.1 *Notations and Vector Operations*

The symbol $|\mathbf{X}|$ 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 $\mathbf{V}$ and v is defined as $\mathbf{V} \cdot v = \{v \cdot v_i \mid v \in \mathbf{V}\}$. The operation is trivially commutative.

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

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

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

2.2 *Number Representations*

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

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

$v_b = <b_1, b_2, \ldots, b_n>$ is called the **base vector** and $v_u = <u_1, u_2, \ldots, u_n>$ is called the **boundary vector.** We also define that: $\mathbf{T}_{(v_b, v_u)} = \{i \mid 0 \le i \le v_b \cdot v_u\}$.

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

For simplicity, throughout this paper we use $(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)$ to denote a number representation system [4].

For a number representation system $(\mathbf{S}_{(\upsilon_b, \upsilon_u)}, \upsilon_b, \upsilon_u)$, we can construct a mapping $f_{(\mathbf{S}_{(\upsilon_b, \upsilon_u)}, \upsilon_b, \upsilon_u)}$ from $\mathbf{S}_{(\upsilon_b, \upsilon_u)}$ to $2^{C(\upsilon_u)}$ as $f_{(\mathbf{S}_{(\upsilon_b, \upsilon_u)}, \upsilon_b, \upsilon_u)}(r) = \{\upsilon \mid \upsilon \cdot \upsilon_b = r, \upsilon \in C(\upsilon_u)\}$, and another mapping $g_{(\mathbf{S}_{(\upsilon_b, \upsilon_u)}, \upsilon_b, \upsilon_u)}$ from $C(\upsilon_u)$ to $\mathbf{S}_{(\upsilon_b, \upsilon_u)}$ as $g_{(\mathbf{S}_{(\upsilon_b, \upsilon_u)}, \upsilon_b, \upsilon_u)}(\upsilon) = \upsilon \cdot \upsilon_b$.

Results 2.2.1

a) $|f_{(\mathbf{S}_{(\upsilon_b, \upsilon_u)}, \upsilon_b, \upsilon_u)}(r)| \geq 1 \quad \forall r \in \mathbf{S}_{(\upsilon_b, \upsilon_u)}$

b) $|f_{(\mathbf{S}_{(\upsilon_b, \upsilon_u)}, \upsilon_b, \upsilon_u)}(r)| = 0 \quad \forall r \in \mathbf{T}_{(\upsilon_b, \upsilon_u)} - \mathbf{S}_{(\upsilon_b, \upsilon_u)}$.

c) $g_{(\mathbf{S}_{(\upsilon_b, \upsilon_u)}, \upsilon_b, \upsilon_u)}$ is onto from $C(\upsilon_u)$ to $\mathbf{S}_{(\upsilon_b, \upsilon_u)}$.

d) $g_{(\mathbf{S}_{(\upsilon_b, \upsilon_u)}, \upsilon_b, \upsilon_u)}$ is not onto from $C(\upsilon_u)$ to $\mathbf{T}_{(\upsilon_b, \upsilon_u)}$ unless $\mathbf{T}_{(\upsilon_b, \upsilon_u)} = \mathbf{S}_{(\upsilon_b, \upsilon_u)}$.

Example 2.2.1 Let $(\mathbf{S}_{(\upsilon_b, \upsilon_u)}, \upsilon_b, \upsilon_u)$ be a number representation system, $\upsilon_b = <7, 1, 2>$ and $\upsilon_u = <1, 2, 1>$, we have

Table 2.1
A Number Representation

0	<000>	6	
1	<010>	7	<100>
2	<001>, <020>	8	<110>
3	<011>	9	<101>, <120>
4	<021>	10	<111>
5		11	<121>

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

$\mathbf{S}_{(\upsilon_b, \upsilon_u)} = \{0, 1, 2, 3, 4, 7, 8, 9, 10, 11\}$.

$\mathbf{T}_{(\upsilon_b, \upsilon_u)} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$f_{(\mathbf{S}_{(\upsilon_b, \upsilon_u)}, \upsilon_b, \upsilon_u)}(2) = \{<001>, <020>\}$.

$g_{(\mathbf{S}_{(\upsilon_b, \upsilon_u)}, \upsilon_b, \upsilon_u)}(<001>) = <001> \cdot \upsilon_b = <001><712> = 2$.

$|f_{(\mathbf{S}_{(\upsilon_b, \upsilon_u)}, \upsilon_b, \upsilon_u)}(2)| = 2$.

THEOREM 2.2.1 *Let* $(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)$ *be a number representation system, then* $f_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}(r) \cap f_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}(r') = \phi$ *for all* $r \neq r'$.

PROOF. If $f_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}(r) \cap f_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}(r') \neq \phi$ where $r \neq r'$, then there will be a $v \in C(v_u)$ so that $v \in f_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}(r)$ and $v \in f_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}(r')$.

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 $(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)$, if each integer in $\mathbf{S}_{(v_b, v_u)}$ maps to at most one vector in $C(v_u)$, that is $|f_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}(r)| \leq 1$ for all r in $\mathbf{S}_{(v_b, v_u)}$ we say that $(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)$ is a **deterministic number representation** (DNR) system.

Results 2.3

a) $|f_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}(r) = 1, \quad \forall r \in \mathbf{S}_{(v_b, v_u)}$.

b) For a DNR $(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)$, $g_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u}$ is a 1 and onto mapping from $C(v_u)$ to $\mathbf{S}_{(v_b, v_u)}$.

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

PROOF. Assume that $(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)$ is not a DNR system

Then $\exists\, v_m \neq v_l \quad s.t.\ v_m \cdot v_b = v_l \cdot v_b$.

Let $v_m = <z_{m1}, z_{m2} \quad z_{mn} \quad 0 \leq z_{mi} \leq u_i \quad \forall i = 1, 2,$

$v_l = <z_{l1}, z_{l2}, \ldots, z_{ln}>, \quad 0 \leq z_{li} \leq u_i \quad \forall i = 1, 2, \quad n$

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 $z_{mi} > z_{li}$.

$$\sum_{j=1}^{n} z_{mj} * b_j = \sum_{j=1}^{n} z_{lj} * b_j$$

$$* b_i + \sum_{\substack{j=1 \\ j \neq i}}^{n} z_{mj} * b_j = z_{li} * b_i + \sum_{\substack{j=1 \\ j \neq i}}^{n} z_{lj} * b_j$$

$$(z_{mi} - z_{li}) * b_i = \sum_{j=1}^{i-1} (z_{lj} - z_{mj}) * b_j + \sum_{j=i+1}^{n} (z_{lj} - z_{mj}) * b_j$$

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

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

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

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

THEOREM 2.3.2 *Let* $(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)$ *be a DNR system. If* $b_1 = 1$ *and* $b_i = \left(\sum_{j=1}^{i-1} u_j * b_j \right) + 1$, *for* $i = 2, 3, \ldots, n$, *then* $\mathbf{S}_{(v_b, v_u)} = \mathbf{T}_{(v_b, v_u)}$.

PROOF. It is obvious that $\mathbf{S}_{(v_b, v_u)} \subseteq \mathbf{T}_{(v_b, v_u)}$.

We shall prove $\mathbf{T}_{(v_b, v_u)} \subseteq \mathbf{S}_{(v_b, v_u)}$ 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 $v_b = <b_1>$.

$$\forall r \in [0, u_1 * b_1] = \mathbf{T}_{(v_b, v_u)}$$

$0 \leq r \leq u_1$ thus $<r> \in C(v_u)$.

$<r> \cdot <b_1> = r * b_1 = r$ thus $r \in \mathbf{S}_{(v_b, v_u)}$

Hypothesis: Let $n = k$ and the result holds. That is,

$$\forall r \in \left[0, \sum_{j=1}^{k} u_j * b_j \right] = \mathbf{T}_{(v_b, v_u)} \quad \exists\, v_m = <z_1, z_2, \quad, z_k>, v_m \in C(v_u),$$

$$\text{s.t.} \quad r = v_m \cdot v_b = \sum_{j=1}^{k} z_j * b_j .$$

Consider $n = k + 1$:

$$b_{k+1} = \left(\sum_{j=1}^{k} u_j * b_j \right) + 1.$$

$$\forall r \in \left[0, \sum_{j=1}^{k+1} u_j * b_j \right] = \mathbf{T}_{(v_b, v_u)}.$$

Let $r' = r \bmod b_{k+1}$.

$$\text{Let } z_{k+1} = \left\lfloor \frac{r}{b_{k+1}} \right\rfloor \leq \left\lfloor \frac{u_{k+1} * b_{k+1} + \sum_{j=1}^{k} u_j * b_j}{b_{k+1}} \right\rfloor = u_{k+1}.$$

Then $r = z_{k+1} * b_{k+1} + r'$.

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

$$r' \leq \left(\sum_{j=1}^{k} u_j * b_j \right).$$

By induction hypothesis:

$$\exists\, v'_m = \langle z_1, z_2, \ldots, z_k \rangle \text{ s.t. } r' = v'_m \cdot v_b = \sum_{j=1}^{k} z_j * b_j .$$

Thus $\exists\, v_m = \langle z_1, z_2, \ldots, z_{k+1} \rangle$, $v_m \in C(v_u)$,

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

Therefore, $r \in \mathbf{S}_{(v_b, v_u)}$. □

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* $(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)$ *be a number representation system. If* $b_1 = 1$ *and* $b_i \le \sum_{j=1}^{i-1} u_j * b_j$ *for* $i = 2, \ldots, n$, *then* $(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)$ *is an NNR system.*

PROOF. Let $0 \le z_i \le u_i \quad \forall\ i = 3, 4, \ldots, n$, and let

$$v_m = <0, 1, z_3, \ldots, z_n>,$$

$$v_l = <b_2, 0, z_3, \ldots, z_n>.$$

Clearly, $v_m \ne v_l$.

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

$$v_m \cdot v_b = <0, 1, z_3, \ldots, z_n> \ <b_1, \ldots, b_n> = b_2 + \sum_{i=3}^{n} z_i * b_i.$$

$$v_l \cdot v_b = <b_2, 0, z_3, \ldots, z_n> \cdot <b_1, \ldots, b_n> = b_2 * b_1 + \sum_{i=3}^{n} z_i * b_i$$

$$= b_2 + \sum_{i=3}^{n} z_i * b_i.$$

The vectors v_m and v_l map to the same integer.

Therefore, $(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)$ is an NNR system (by Definition 2.4.1). □

THEOREM 2.4.2 *Let* $(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)$ *be an NNR system. If* $b_1 = 1$ *and* $b_i \le \sum_{j=1}^{i-1} u_j * b_j$ *for* $i = 2, \ldots, n$, *then* $\mathbf{S}_{(v_b, v_u)} = \mathbf{T}_{(v_b, v_u)}$.

PROOF. Clearly, $\mathbf{S}_{(v_b, v_u)} \subseteq \mathbf{T}_{(v_b, v_u)}$.

We shall show that $\mathbf{S}_{(v_b, v_u)} \supseteq \mathbf{T}_{(v_b, v_u)}$ by induction on the lengths v_B and v_U of v_b and v_u.

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

$$\forall\ r \in [0, u_1 * b_1] = \mathbf{T}_{(v_b, v_u)},$$

$0 \le r \le u_1$ thus $r \in C(v_u)$,

$<r> \cdot <b_1> = r * b_1 = r$, thus $r \in \mathbf{S}_{(v_b, v_u)}$.

Hypothesis: Let $n = k$ and the result holds.

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

where

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

Consider $n = k + 1$.

$$\forall\ r \in \left[0, \sum_{j=1}^{k+1} u_j * b_j \right] = \mathbf{T}_{(v_b, v_u)}.$$

Case I

$$\left\lfloor \frac{r}{b_{k+1}} \right\rfloor > u_{k+1},\ \text{let } r' = r - u_{k+1} * b_{k+1}.$$

$$r \le \sum_{j=1}^{k+1} u_j * b_j \Rightarrow r' \le \sum_{j=1}^{k+1} u_j * b_j - u_{k+1} * b_{k+1} = \sum_{j=1}^{k} u_j * b_j.$$

By induction hypothesis:

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

$$\text{s.t. } r' = \sum_{j=1}^{k} z_j * b_j.$$

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

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

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

Case II

$$\left\lfloor \frac{r}{b_{k+1}} \right\rfloor \le u_{k+1},\ \text{let } r' = r \bmod b_{k+1}.$$

$$r' < b_{k+1} \leq \sum_{j=1}^{k} u_j * b_j$$

By induction hypothesis:

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

$$\text{s.t. } r' = \sum_{j=1}^{k} z_j * b_j$$

$$\left\lfloor \frac{r'}{b_{k+1}} \right\rfloor \leq u_{k+1}, \text{ thus } <z_1, z_2 \quad ., z_k, \left\lfloor \frac{r}{b_{k+1}} \right\rfloor > \in C(v_u).$$

$$<z_1, z_2 \quad ., z_k, \left\lfloor \frac{r}{b_{k+1}} \right\rfloor > \cdot v_b = r' + \left\lfloor \frac{r}{b_{k+1}} \right\rfloor * b_{k+1} = r.$$

Thus, $r \in \mathbf{S}_{(v_b, v_u)}$. □

Example 2.4.1 Let $(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)$ 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 $f_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}$.

Table 2.2
An NNR System

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

(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> <1022><0113><0120>	30	<2213><2220>
14	<2011><1102><1023> <0200><0121>	31	<2221>
15	<2012><1110><0122> <0201><1103>	32	<2222>
16	<2013><2020><1111> <0202><0123>	33	<2223>

THEOREM 2.4.3 *Let* $(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)$ *be an NNR system. Let* $\mathbf{V}_r = f_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}(r)$ *for* r *in* $\mathbf{S}_{(v_b, v_u)}$, *and* $r_1, r_2, r_3 \in \mathbf{S}_{(v_b, v_u)}$ *where* $r_3 = r_1 + r_2$. *If the boundary vector* v_u *is unlimited,* $|\mathbf{V}_{r_3}| \geq Max\{|\mathbf{V}_{r_1}|, |\mathbf{V}_{r_2}|\}$.

PROOF. For any $v \in \mathbf{V}_{r_1}$ and $w \in \mathbf{V}_{r_2}$, $(v + w) \cdot v_b = v \cdot v_b + w \cdot v_b = r_1 + r_2 = r_3 \Rightarrow (v + w) \in \mathbf{V}_{r_3}$ under the condition that v_u is unlimited.

Thus, it is true that $P = \{v_1 + w_i \mid v_1 \in \mathbf{V}_{r_1}, w_i \in \mathbf{V}_{r_2} \text{ for all } i\} \subseteq \mathbf{V}_{r_3}$ and $|P| \leq |\mathbf{V}_{r_3}|$.

Because $|P| = |\mathbf{V}_{r_2}|$, this implies that $|\mathbf{V}_{r_2}| \leq |\mathbf{V}_{r_3}|$.

With the same method, we can derive that $|\mathbf{V}_{r_1}| \leq |\mathbf{V}_{r_3}|$.

That is, $|\mathbf{V}_{r_3}| \geq \text{Max}\{|\mathbf{V}_{r_1}|, |\mathbf{V}_{r_2}|\}$. □

2.5 *Combination of DNR and NNR*

Given a DNR system $(\mathbf{S}_{(v_{bD}, v_{uD})}, v_{bD}, v_{uD})$ and an NNR system $(\mathbf{S}_{(v_{bN}, v_{uN})}, v_{bN}, v_{uN})$, we can construct a mapping h from $\mathbf{S}_{(v_{bN}, v_{uN})}$ to $2^{\mathbf{S}_{(v_{bD}, v_{uD})}}$, where $h(r) = \{s \mid s = g_{(\mathbf{S}_{(v_{bD}, v_{uD})}, v_{bD}, v_{uD})}(v), v \in f_{(\mathbf{S}_{(v_{bN}, v_{uN})}, v_{bN}, v_{uN})}(r) \cap C(v_{uD})\}$, and a mapping k from $\mathbf{S}_{(v_{bD}, v_{uD})}$ to $\mathbf{S}_{(v_{bN}, v_{uN})}$, where $k(s) = g_{(\mathbf{S}_{(v_{bN}, v_{uN})}, v_{bN}, v_{uN})}(v)$ for $v \in f_{(\mathbf{S}_{(v_{bD}, v_{uD})}, v_{bD}, v_{uD})}(s)$.

Definition 2.5.1 Let $(\mathbf{S}_{(v_{bD}, v_{uD})}, v_{bD}, v_{uD})$ be a DNR system and let $(\mathbf{S}_{(v_{bN}, v_{uN})}, v_{bN}, v_{uN})$ be an NNR system. We say that the mapping h is **nice** if and only if $v_{uN} \leq v_{uD}$ and $\mathbf{S}_{(v_{bN}, v_{uN})} = \mathbf{T}_{(v_{bN}, v_{uN})}$.

PROPERTIES 2.5.1 *Let* $(\mathbf{S}_{(v_{bD}, v_{uD})}, v_{bD}, v_{uD})$ *and* $(\mathbf{S}_{(v_{bN}, v_{uN})}, v_{bN}, v_{uN})$ *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* $\mathbf{S}_{(v_{bN}, v_{uN})}$.

b) $h(r) \cap h(r') = \phi$ *for all* $r \neq r'$.

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

PROOF. a) $\forall r \in \mathbf{S}_{(v_{bN}, v_{uN})}, |f_{(\mathbf{S}_{(v_{bN}, v_{uN})}, v_{bN}, v_{uN})}(r)| \geq 1$ (by Results 2.2.1 (a))

Since $v_{uN} \leq v_{uD}$ and $g_{(\mathbf{S}_{(v_{bD}, v_{uD})}, v_{bD}, v_{uD})}$ is a 1-1 and onto mapping from $C(v_{uD})$ to $(\mathbf{S}_{(v_{bD}, v_{uD})}$ (by Results 2.3.1 (b)), so that $\forall\ r \in (\mathbf{S}_{(v_{bN}, v_{uN})}, |h(r)| \geq 1$.

b) Since $f_{(\mathbf{S}_{(v_{bN}, v_{uN})}, v_{bN}, v_{uN})}(r) \cap f_{(\mathbf{S}_{(v_{bN}, v_{uN})}, v_{bN}, v_{uN})}(r') = \phi$ for all $r \neq r'$ (by Theorem 2.2.1), and $g_{(\mathbf{S}_{(v_{bD}, v_{uD})}, v_{bD}, v_{uD})}$ is a 1-1 and onto mapping from $C(v_{uD})$ to $\mathbf{S}_{(v_{bD}, v_{uD})}$ (by Results 2.3.1), so that $h(r) \cap h(r') = \phi$ for all $r \neq r'$.

c) For $c \in h(r)$, $\exists v \in f_{(\mathbf{S}_{(v_{bN}, v_{uN})}, v_{bN}, v_{uN})}(r) \cap C(v_{uD})$

s.t. $c = g_{(\mathbf{S}_{(v_{bD}, v_{uD})}, v_{bD}, v_{uD})}(v)$.

Thus $v \in f_{(\mathbf{S}_{(v_{bD}, v_{uD})}, v_{bD}, v_{uD})}(c)$ and $g_{(\mathbf{S}_{(v_{bN}, v_{uN})}, v_{bN}, v_{uN})}(v) = r$, then r. □

THEOREM 2.5.1 *Let* $(\mathbf{S}_{(v_{bD}, v_{uD})}, v_{bD}, v_{uD})$ *and* $(\mathbf{S}_{(v_{bN}, v_{uN})}, v_{bN}, v_{uN})$ *be the same as in Definition* 2.5.1. *If h is* ***nice,*** *then* $|\mathbf{S}_{(v_{bD}, v_{uD})}| > |\mathbf{S}_{(v_{bN}, v_{uN})}|$.

PROOF. $(\mathbf{S}_{(v_{bN}, v_{uN})}, v_{bN}, v_{uN})$ is an NNR. It is obvious that $|\mathbf{S}_{(v_{bN}, v_{uN})}| < |C(v_{uN})|$.

By definition 2.5.1, if h is **nice** then

$$v_{uN} \leq v_{uD} \Rightarrow |C(v_{uN})| \leq |C(v_{uD})|$$

$(\mathbf{S}_{(v_{bD}, v_{uD})}, v_{bD}, v_{uD})$ is a DNR, it is obvious that

$$C(v_{uD})| = |\mathbf{S}_{(v_{bD}, v_{uD})}$$

Collecting above relations derives that

$$|\mathbf{S}_{(v_{bD}, v_{uD})}| > |\mathbf{S}_{(v_{bN}, v_{uN})} \quad \square$$

CRYPTOSYSTEM

The mappings $f_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}$ and $g_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}$ 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 $f_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}$ 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 $g_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}$ forms a cipher [6] which is also thought to be insecure [1, 4, 5]. Combining a $f_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}$ and a $g_{(\mathbf{S}_{(v_{b'}, v_{u'})}, v_{b'}, v_{u'})}$, 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

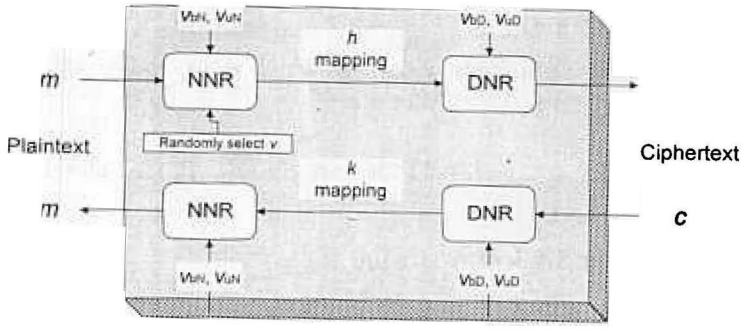

Figure 3.1. NDC cipher

vectors (v_{bN}, v_{uN}, v_{bD}, v_{uD}) of the underlying NNR and DNR system. They should be kept secret. In the cryptosystem, $\mathbf{S}_{(v_{bN}, v_{uN})}$ is the plaintext space and $\mathbf{S}_{(v_{bD}, v_{uD})}$ 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 $\mathbf{S}_{(v_{bN}, v_{uN})}$ has at least a ciphertext in $\mathbf{S}_{(v_{bD}, v_{uD})}$ (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:

vector $v_{uN} = <u_1, u_2, \ldots, u_n>$.

Output:

base vector $v_{bN} = <b_1, b_2, \ldots, b_n>$

Process:

Begin:

1. Let $b_1 = 1$
2. For $j = 2$ to n

   Randomly [2] choose a number for b_j such that

$$b_{(j-1)} < b_j \leq \sum_{i=1}^{j-1} b_i * u_i$$

End

3.3 *Selection of Ciphertext*

The $f_{(\mathbf{S}_{(v_{bN}, v_{uN})}, v_{bD}, v_{uD})}$ 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 $v_b = <b_{t1}, b_{t2}, \quad b_{tn}>$,

a boundary vector $v_u = <u_{t1}, u_{t2}, \quad u_{tn}>$.

Output:

a vector $v = <v_1, v_2, \quad v_n> \in C(v_u)$.

Process:

Begin

$m = x$.

For $i = n$ down to 2 do

Begin

$$temp\_m = m - \sum_{j=1}^{i-1} u_{tj} * b_{tj}$$

if $temp\_m \leq 0$ then $lower = 0$

else $lower = \left\lfloor \frac{temp\_m}{b_{ti}} \right\rfloor + 1$

$$upper = \min\left(\left\lfloor \frac{m}{b_{ti}} \right\rfloor , u_{ti} \right)$$

v_i = a random number in the range [*lower*, *upper*]

$m = m - v_i \cdot b_{ti}$

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 preceder. 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.

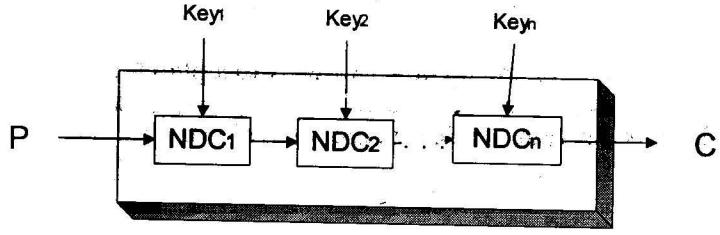

Figure 3.2. Concatenation of NDCs

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.

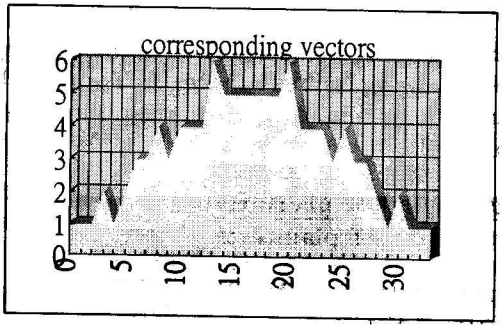

Figure 3.3. Distribution map of the NNR in Example 2.4.1

3.5.1 *Use the Middle Part of* $\mathbf{S}_{(v_b, v_u)}$

Consider an NNR with mapping $f_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}$, which has the properties described in Theorem 2.4.1. By Theorem 2.4.3 we know that $|f_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}(r)|$ 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, $|f_{(\mathbf{S}_{(v_b, v_u)}, v_b, v_u)}(r)|$ 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 $S_{(v_b, v_u)}$ as an increasingly sequence, the middle part of $S_{(v_b, v_u)}$ 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.

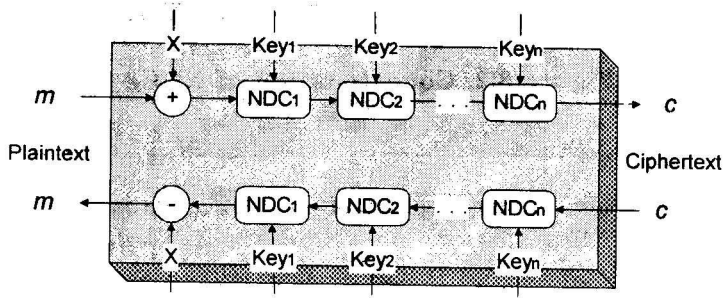

Figure 3.4. The cryptosystem with plaintext offset

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 quantitating 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

$$\frac{\log_2((v_{bN} \cdot v_{uN})!)}{v_{bN} \cdot v_{uN}} \text{ and } \frac{\log_2((v_{bD} \cdot v_{uD})!)}{v_{bD} \cdot v_{uD}}, \text{ respectively.}$$

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

$$\frac{(v_{bN1} \cdot v_{uN1}) \cdot \log_2((v_{bDt} \cdot v_{uDt})!)}{(v_{bDt} \cdot v_{uDt}) \cdot \log_2((v_{bN1} \cdot v_{uN1})!)}$$

where (v_{bN1}, v_{uN1}) are the NNR's base and boundary vectors of the first NDC, (v_{bDt}, v_{uDt}) 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 probabilisticly 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/chosen-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 nodeterministic 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

1. B. Schneier, *Applied Cryptography*, 2nd edition, John Wiley & Sons, Inc, 1996.
2. M. Bellare, S. Goldwasser and D. Micciancio, Pseudo-Random Number Generation within Cryptographic Algorithms: The DSS Case, *Advances in Cryptology-CRYPT'97 Proceedings*, Springer-Verlag, 1997, pp. 277-291.

E. F. Brickell and A. M. Odlyzko, Cryptanalysis: A Survey of Recent Results, in *Contemporary Cryptology: The Science of Information Integrity*, G. J. Simmons (ed.), IEEE Press, 1991, pp. 501-540.

H. R. Kenneth, *Elementary Number Theory and its Applications*, 3rd Ed., Addision-Wesley publishing Company, U.S.A., 1993.

5. T. Jakobsen, Cryptanalysis of block ciphers with probabilistic non-linear relations of low degree, in *Advances in Cryptology-CRYPT' 98 Proceedings*, Vol. 1462, Lecture Notes in Computer Science, Springer-Verlag, 1998, p. 212-222.

6. V. Niemi, A New trapdoor in Knapsacks, in *Advances in Cryptology - EUROCRYPT' 90*, Springer-Verlag, 1991, pp. 405-411.

Yi-Shiung Yeh, Chan-Chi Wang and Tzyy-Geng Su, An NNR Cryptoscheme, *Proceeding of the fifth National Conference on Information Security*, Taipei, 1995, pp. 176-182.

Received March, 2001