ELSEVIER

Information Processing Letters 68 (1998) 215–217

Information Processing Letters

# A modified version of the Rao–Nam algebraic-code encryption scheme

Yi Chang Cheng [a,*], Erl Huei Lu [b,1], Shaw Woei Wu [a]

[a] *Department of Electrical Engineering, Chung Cheng Institute of Technology, Ta-Hsi, Tao-Yuan, Taiwan*
[b] *Chang Gung University, Kwei-San, Tao-Yuan, Taiwan*

Received 21 November 1997
Communicated by J.L. Fiadeiro

*Keywords:* Private-key algebraic-code cryptosystem; Chaining mode; Cryptography

## 1. Introduction

In 1984, Rao [1] introduced a private-key algebraic-code cryptosystem, which is similar to the McEliece's public-key cryptosystem [2], with the encryption matrix as secret information. The private-key cryptosystem can be implemented using a very simple error-correcting code. Thus, it requires much lower computational overhead as compared to the McEliece's system. Later on, Rao and Nam presented a chosen-plaintext attack to break the original cryptosystem, and also proposed a modified scheme, called the Rao–Nam scheme, to overcome this attack [3,4]. The Rao–Nam scheme encrypts plaintext in the following operation:

$$C = (MG' + Z)P, \tag{1}$$

where

$$G' = SG, \tag{2}$$

$M$ = a plaintext with $k$-symbol length;

$C$ = a ciphertext with $n$-symbol length;

$Z$ = a random error vector with $n$-symbol length selected from a syndrome-error table;

$S$ = a random $k \times k$ nonsingular matrix;

$G$ = a $k \times n$ generator matrix of a $t$-error-correcting code;

$P$ = an $n \times n$ permutation matrix.

Note that the vector $Z$ is randomly selected from a predetermined syndrome-error table. Since the weight of each $Z$ in the table is selected to be approximately $n/2$, the Rao–Nam scheme can withstand the chosen-plaintext attack introduced in Section I-B1 of [4]. Moreover, Rao and Nam suggested to use appropriate code (such as the Reed–Solomon code or the nonlinear Preparata code) to implement their scheme to prevent the Struik–Tilburg chosen-plaintext attack [5,6]. In addition, there are several modified versions of the Rao–Nam scheme, which have been proposed to enhance the security of the scheme [5,7]. Each of these modified versions needs to use a secret invertible function to shuffle the plaintext before it is encoded by the error-correcting code. In this paper, instead of using the syndrome-error table approach as in the Rao–Nam scheme, we propose to use a public linear operation to implement it. Thus, any nonbinary code (such as

* Tel.: 03-3809991, ext 43; fax: 03-3801407.
[1] Tel.: 03-3283016, ext 5322; fax: 03-3283031.


PII: S0020-0190(98)00156-2