ON STRUIK-TILBURG CRYPTANALYSIS OF RAO-NAM SCHEME

T.R.N Rao
The Center for Advanced Computer Studies
University of Southwestern Louisiana
Lafayette, Louisiana 70504

Introduction

A private-key cryptosystem using algebraic codes was presented in CRYPTO 86 [1] and it is referred later [2] and also here as Rao-Nam Scheme. Subsequently, a chosen-plaintext attack was presented by Struik and Tilburg in a rump session of CRYPTO 87 and appears in this issue [2]. This note addresses a major difference between the types of chosen-plaintext attacks on private-key algebraic code cryptosystems vs. the other more conventional private key schemes, and presents a rebuttal to the conclusions given in [2].

Chosen-Plaintext Attacks

In a conventional private-key cryptosystem, the ciphertext for a given message, M with a key K is given by

$$C = E_k(M) .$$

The ciphertext C is a constant for any given M and K. However, in algebraic-code cryptosystem as given in [1]

$$C = MG'' + Z',$$

where G'' is a matrix combinationally equivalent to generator matrix G of a Linear Code and Z' is a selected error vector Z appropriately permuted by a secret function P. See details [1].

Since Z is a randomly selected error vector, it is conceivable that for a given M and encryption algorithm, many ciphertexts say $C_1, C_2, \cdots$ can be obtained. This is a major difference and it can be exploited in a chosen-plaintext attack as follows. The cryptanalyst would obtain all possible ciphertexts $C_1, C_2, \cdots$ for a given M (under the same encryption key) in an exhaustive manner. This will enable him to draw information on the error vectors $Z_1, Z_2, \cdots$ which then are used to break the code. This line of attack was actually suggested by Rao-Nam [1] and was indeed pursued rather vigorously by Struik-Tilburg [2]. However, the basic contention would be on "how many different ciphertexts are indeed required for one particular M in order to break code ?" In other words, "what are these numbers (in any specified environment of network of users) to designate a scheme to be secure or unsecure ?" Without some consideration for these numbers it would be meaningless to designate a scheme as "weak" or as "insecure". We take Struik-Tilburg analysis to determine these numbers as follows.

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, pp. 458-460, 1988.

Struik-Tilburg Analysis [2] and Discussion

In order to obtain information on Z's sufficient to break the code we obtain all different ciphertexts $C_1, C_2, \cdots, C_N$ exhaustively for a given plaintext M, where N is the number of all distinct error vectors. The expected number of attempts to obtain all distinct C_i are shown to be $N \ln N$. (Struik-Tilburg give $N \log N$ in their rump session paper.) Since this procedure is to be repeated for the k unit vectors (u_i , $u_i = 1,2, \cdots, k$) the total number of ciphertexts required for chosen plaintexts is $O(kN \log N)$. Struik-Tilburg analyze as follows. For the ATE method of Rao-Nam Scheme, since $N \leq n$, This number is rather small and hence the scheme is easily broken. Also for syndrome-error table method (of Rao-Nam Scheme) using codes with high information rates, $N = 2^{n-k}$ is also small enough that the scheme is not very secure according to [2]. We show below by a consideration of two examples that this analysis is flawed and that the conclusions of [2] are wrong.

The argument we advance here in this paper is as follows. In any practical network operations, for any chosen-plaintext M under a specific key it would be impossible to obtain thousands of different ciphertexts. For example, if the network administrator is distributing a specific bulletin or message to all users then a common key may be used but then the same ciphertext will be distributed to all users. Alternately, secret keys may be used individually for each user. In either of these scenarios, there is no way a large number (thousands) ciphertexts for any one particular bulletin will be made available. For more frequently used blocks of message items it is conceivable for the cryptanalyst to gather some number of ciphertexts but it would be near impossible to obtain tens of thousands of ciphertexts as required by analysis of [2]. The code examples below exlain these numbers required for analysis.

Examples

Consider (72, 64, 4) Hamming Code with Z-errors selected randomly from the standard-array table as suggested in [1]. For this case the $N = 2^{n-k} = 2^8$ and $N \log N$ is 2024, and $kN \log N = 129{,}000$. Consider as another example, a (32, 28, 5) Reed-Solomon Code over GF(2^8) with information ratio IR=28/32=.875. The corresponding parameters in GF(2) are $n = 32 \times 8 = 256$, $k = 28 \times 8 = 224$ and $n - k = 32$. For this code the number of different Z-vectors are $N = 2^{32}$ and $N \log N = 2^{37}$, and $kN \log N \approx 2^{46}$. These figures are so large that any chosen-plaintext attack along the lines of [2] is practically impossible.

Conclusion

This discussion and the examples show clearly that Rao-Nam scheme appears very secure under chosen-plaintext attacks of this type. There is more to be encouraged about the security of the scheme after this cryptoanalysis.

References

[1] T.R.N. Rao and K.H. Nam, "Private-Key Algebraic-Code Cryptosystems", Lecture Notes in Computer Science, Advances in Cryptology-CRYPTO '86, pp. 35-48, (Editor A.M. Odlyzko), Springer-Verlag 1987.

[2] R. Struik and J. Van Tilburg, "The Rao-Nam Scheme is insecure against a chosen-plaintext attack", A Rump Session paper, CRYPTO '87. A revised version appears in this issue.