Cryptanalysis of cascaded convolutional transducers with local propagation

M. A. Orumiechiha, S. F. Mohebipoor

***Abstract*—**Recently, the idea of design of dynamic symmetric cryptosystems is proposed. According to this idea, the property of cipher system is varied related to secret key. But unfortunately this cipher is not safer than whatever is claimed. In this paper, two attacks on the proposed design are investigated. The first attack is a partial key recovery which for a (k,k,m) q- cascaded convolutional transducers is determined a fragment of ciphertext without calculating master key with complexity $O(k^6)$. In addition, a weak key on this system is announced that one can recover longer fragment of plaintexts with complexity $O(2\times k^6)$.

***Keywords*—** Convolution Codes, Cryptanalysis, Symmetric Cryptosystem, Sequential and parallel cascaded convolutional encryption.

I. INTRODUCTION

SYMMETRIC cryptosystems such as triple DES , AES and others have been all designed as static ciphers, in the sense that their structure do not change at all during encryption/decryption. Recently, a dynamic symmetric cryptosystem [1,2] is proposed that whose structure is based on invertible convolution codes. The scheme is considered to two versions. The first one uses linear combinations of convolution codes and the other one exploits more complicated and nonlinear combinations.

In this paper, we propose a partial attack which recovers the part of plaintext without determining secret key. This attack is applicable on both versions. For simplicity, we focus attack for vesion1 and then expand to vesion2. Also, we show that there are weak keys which can obtain partially information of cipher block.

The paper is organized as follows. In section 2, we provide a brief introduction to convolutional codes and globally invertible convolutional transducer. And then, a new partial attack and one weak key for this systeam is described (section 3).

Manuscript received February 25, 2007; Revised version March 30, 2007

Mohammad Ali Orumiehchiha is with Zaeim Electronic Ind. R&D Department, No. 21, Nilo St., Brazil St., Vanak Sq., Tehran, Iran, phone: +98-021-88773551; fax: +98-021-88776355; e-mail: orumiehchi@ {zaeim.co.ir or yahoo.com}.

S. Fahimeh Mohebbipoor is with Zaeim Electronic Ind. R&D Department, No. 21, Nilo St., Brazil St., Vanak Sq., Tehran, Iran, phone: +98-021-88773551; fax: +98-021-88776355; (e-mail: mohebbipoor @ {zaeim.co.ir }).

II. SEQUENTIAL AND PARALLEL CASCADED CONVOLUTIONAL ENCRYPTION PROCEDURE FOR PAPER SUBMISSION

In [1,2] were proposed a class of convolutional transducers, called cascaded convolutional transducers with local propagation. These designs are based on q-cascaded dynamic convolutional transducers, and are comprised in the following definition. Note that the following scheme is the -for example $\mathrm{vect}([0\,0],[1\,1]) = [0\,0\,1\,1]$.

Definition 2.1.Let n, k, and m be nonzero natural numbers. An (n,k,m) convolutional transducer is a function $t:\bigcup_{i=1}^{\infty} B_{1\times ki} \to \bigcup_{i=1}^{\infty} B_{1\times ni}$ given by

$$t(u) = uG_{t,|u|}$$

Where

$$G_{t,kp} = \begin{bmatrix} G_{t,0} & G_{t,1} & \cdots & G_{t,m} & & \\ & G_{t,0} & G_{t,1} & \cdots & G_{t,m} & \\ & & \ddots & \ddots & \cdots & \ddots \\ & & & G_{t,0} & G_{t,1} & \cdots & G_{t,m} \end{bmatrix} \quad (1)$$

is an element of $B_{kp\times(pn+mn)}$, $G_{t,i} \in B_{k\times n}$ for all $i \in \{0,1,\cdots,m\}$, and the arithmetic in (1) is carried out over the binary field GF(2). The entries blank are assumed to be filled in with zeros.

Definition 2.2. Let *k* and *m* be nonzero natural numbers. A (k, k, m) linear q-cascaded convolutional transducer with propagation is an $(q+1)$-tuple $(t, S_1, S_2, \cdots, S_q)$, where *t* is a function given by

$$t(u) = uH^1_{t,kp}(v_0)H^2_{t,kp}(v_1)\ldots H^q_{t,kp}(v_{q-1}), \quad (2)$$

for all $u \in B_{1\times kp}$, where $v_0 = u$, $v_i = v_{i-1}H^i_{t,kp}(v_{i-1})$ for all $i \in \{1, 2, \ldots, q\}$, $H^i_{t,kp}(w)$ is the restriction of

$$G^i_{t,kp}(z) = \begin{bmatrix} G^{i,0}_{t,0,z} & G^{i,1}_{t,1,z} & \cdots & G^{i,m}_{t,m,z} & & \\ & \ddots & & & \ddots & \\ & & G^{i,p-1}_{t,0,z} & G^{i,p}_{t,1,z} & \cdots & G^{i,m+p-1}_{t,m,z} \end{bmatrix} \quad (3)$$

to the first kp columns, $z = \mathrm{vect}(w,[0\ldots0])$, $G^{i,0}_{t,j,z} = G^i_{t,j}$, $G^{i,r}_{t,j,z} = G^i_{t,j}(f(r-1,z))$ for all $r \in \{1, 2, \ldots, m+p-1\}$,

$f(s,z) = (z_{sk+1:(s+1)k}[1] + \ldots + z_{sk+1:(s+1)k}[k]) \bmod 2$,

and

$S_i = \{G^i_{t,j}(0) \mid j \in \{0,1,...,m\}\} \bigcup \{G^i_{t,j}(1) \mid j \in \{0,1,...,m\}\}$,

is the set of state matrices corresponding to the *i*-th transducer of the cascade, $i = 1, \cdots, q$. As usual, all the operations are performed over the binary field GF(2). And also $G^i_{t,j}(0), G^i_{t,j}(1) \in B_{k\times k}$ and are invertible. The entries left blank in $G^i_{t,kp}(z)$ are assumed to be filled in with zeros.

Definition 2.3. A (k,k,m) linear q-cascaded convolutional cryptosystem with propagation is a globally invertible (k,k,m) q-cascaded convolutional transducer with propagation with encryption function *t* in which the sets $S_1, \cdots, S_q$ are kept private.

III. CRYPTANALYSIS OF SCHEME

The idea design of cipher is attractive but unfortunately cipher is not as safe as is claimed. The claimed security is comparable to a homogeneous strong block cipher.

In [1,2] is claimed that security of design is based privacy

Description of Algorithm
Input: vector *u* as plaintext.
Output: vector *v* as ciphertext.
Private key: the sets
$S_i = \{G^i_{t,j}(0) \mid j \in \{0,1,...,m\}\} \bigcup \{G^i_{t,j}(1) \mid j \in \{0,1,...,m\}\}$
, $i \in \{1,...,q\}$.

1. set $p = \dfrac{lenght\ \ pla\,\text{int}\,ext\ u}{k}$,
2. $v_0 = u$,
3. For *i=1* to *q* do
   3.1. $H^i_{t,kp}(v_{i-1})$ is Constructed by the restriction of matrix (3) to the first kp columns,
   3.2. $v_i = v_{i-1} H^i_{t,kp}(v_{i-1})$,
   end do;
4. $v = v_q$.

Fig. 1Description of algorithm

of the sets $S_1, \cdots, S_q$. But, in this section is shown that attacker can easily obtain the first sub-block plaintext without any information from the sets $S_1, \cdots, S_q$. Also, if these sets are chosen improper then one recovers more sub-block plaintexts.

A. Partial attack

In this system, the first output sub-block ciphertext is constructed only by multiplying the first input sub-block plaintext (denote u^1) and matrix

$A^1 = G^1_{t,0}(0) G^2_{t,0}(0) \cdots G^q_{t,0}(0)$.

Therefore, with changing the other input sub-blocks and fixing the first input sub-block, the first cipher sub-block remains fixed. And also, the contents of matrixes $G^1_{t,0}(0), G^2_{t,0}(0), \cdots, G^q_{t,0}(0)$ are always fixed, and hence A^1 is fixed for all of arbitrary plaintext. The number of contents of matrix A^1 is K^2, hence one can determine all of contents A^1. By using about K^2 output bits belong to the first output sub-blocks and write a linear system and solve it. Therefore, for each ciphertext one can calculate the first sub-block of plaintext without recovering master key.

Additionally, if plaintext is chosen such that the first sub-block be equal to zero and other sub-blocks of plaintext be random then always the first sub-block will be zero and is distinguishable with probability 1 from a random sequence.

B. Weak key

In this system, If matrices $G^1_{t,0}(0), G^2_{t,0}(0), \cdots, G^q_{t,0}(0)$ in the sets $S_1, \cdots, S_q$ be equal, means that $A^1 = (G^1_{t,0}(0))^q$, and so we can obtain matrix A^1 and $G^1_{t,0}$. Regarding that the hamming weight of $u^1, v^1_0, v^1_1, \cdots, v^1_q$ are either even or odd, we can parse all possible first sub-blocks u^1 to 2^q classes. Let which for this matrix only second column is unknown. Hence, by using about $2\times K^2$ output bits belong to the second output sub-block, attacker can write a linear system and solve it, so A^2 can be determined. Therefore with determining u^1, we can deduce the second sub-block.

If this weak point continues for system, attacker can decrypt longer fragments of ciphertexts. This attack is described in the following example.

Example1 Let $t : \bigcup_{i=1}^{\infty} B_{1\times ki} \mapsto \bigcup_{i=1}^{\infty} B_{1\times ni}$ be a (2, 2, 2) 2-cascaded convolutional transducer, where

$$
\begin{aligned}
G^1_{t,0}(0) &= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad G^1_{t,0}(1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \\
G^1_{t,1}(0) &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \qquad G^1_{t,1}(1) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \\
G^1_{t,2}(0) &= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad G^1_{t,2}(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
G^2_{t,0}(0) &= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad G^2_{t,0}(1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \\
G^2_{t,1}(0) &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \qquad G^2_{t,1}(1) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \\
G^2_{t,2}(0) &= \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \qquad G^2_{t,2}(1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}
\end{aligned} \tag{4}
$$

In this example, the matrices $G^1_{t,0}(0) = G^2_{t,0}(0)$ are identical. Hence, $A^1 = (G^1_{t,0}(0))^2$ and so we can obtain matrix A^1 and $G^1_{t,0}(0)$. Regarding that the hamming weight of

$u^1, v_0^1,$ are either even or odd, we can parse all possible first sub-block u^1 to 2^2 classes.

Let $A^2 = \begin{bmatrix} G_{t,0}^1(0) & G_{t,1,z}^{1,1} \\ 0 & G_{t,0,z}^{1,1} \end{bmatrix} \begin{bmatrix} G_{t,0}^1(0) & G_{t,1,z}^{2,1} \\ 0 & G_{t,0,z}^{2,1} \end{bmatrix}$ which for this matrix only second column is unknown. Hence, by using about $2 \times K^2$ output bits belong to the second output sub-block, attacker can write a linear system and solve it, so can determine A^2 and then the second sub-block plaintexts are recovered too.

Example2 Let a (16,16,1) 2- cascaded convolutional transducer that proposed in [1]. For an input vector of length 64, if the key be weak, as mentioned before, then for any output block, we can calculate the first 32 bits of input block and also if the key is not week, then can determine the first 16 bits of input block.

IV. Conclusion

In this paper, we investigated two attacks on the proposed design. The first attack is a partial key recovery which for a (k,k,m) q-cascade was determined a fragment of ciphertext without calculating master key with complexity $O(k^6)$. In addition, a weak key on this system was found that one could recover longer fragment of plaintexts with complexity $O(2 \times k^6)$.

References

[1] D. Trinc˘a," Sequential and Parallel Cascaded Convolutional Encryption with Local Propagation: Toward Future Directions in Symmetric Cryptography," *the 3rd International Conference on Information Technology: USA*, 2006, pp. 464–469, *IEEE Computer Society Press*.G. O. Young, "Synthetic structure of industrial plastics (Book style with paper title and editor)," in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.

[2] D. Trinc˘a, "Efficient FPGA Implementations and Cryptanalysis of Automata-based Dynamic Convolutional Cryptosystems," Available: http://www.eprint.iacr.org/2006/263.