Algebraic Attacks on Combiners with Memory

Frederik Armknecht and Matthias Krause

Theoretische Informatik
Universität Mannheim
68131 Mannheim, Germany
{Armknecht,Krause}@th.informatik.uni-mannheim.de

Abstract. Recently, algebraic attacks were proposed to attack several cryptosystems, e.g. AES, LILI-128 and Toyocrypt. This paper extends the use of algebraic attacks to combiners with memory. A (k, l)-combiner consists of k parallel linear feedback shift registers (LFSRs), and the nonlinear filtering is done via a finite automaton with k input bits and l memory bits. It is shown that for (k, l)-combiners, nontrivial canceling relations of degree at most $\lceil k(l+1)/2 \rceil$ exist. This makes algebraic attacks possible. Also, a general method is presented to check for such relations with an even lower degree. This allows to show the invulnerability of certain (k, l)-combiners against this kind of algebraic attacks. On the other hand, this can also be used as a tool to find improved algebraic attacks.

Inspired by this method, the E_0 keystream generator from the Bluetooth standard is analyzed. As it turns out, a secret key can be recovered by solving a system of linear equations with $2^{23.07}$ unknowns. To our knowledge, this is the best published attack on the E_0 keystream generator yet.

1 Introduction

Stream ciphers are designed for online encryption of secret plaintext bitstreams $E = (e_1, e_2, \cdots)$ which have to pass an insecure channel. Depending on a given secret information $x^* \in \{0, 1\}^n$, the stream cipher produces a keystream $Z(x^*) = (z_1, z_2, \cdots)$ which is bitwise XORed with E. Knowing x^*, the decryption can be performed by using the same rule. It is common to evaluate the security of a stream cipher relative to the pessimistic scenario that an attacker has access not only to the encrypted bitstream, but even to a sufficiently long piece of keystream. Thus, the cryptanalysis problem of a given stream cipher consists in computing the secret information x^* from a sufficiently long prefix of $Z(x^*)$.

We call a stream cipher LFSR-based, if it consists of a certain number k of linear feedback shift registers (LFSRs) and an additional device, called the nonlinear combiner, which transforms the internal linear bitstream, produced by the LFSRs, into a nonlinear output keystream. Because of the simplicity of LFSRs and the excellent statistical properties of bitstreams produced by well-chosen LFSRs, LFSR-based stream ciphers are widely used in practice. A lot of different nontrivial approaches to the cryptanalysis of LFSR-based stream ciphers (fast correlation attacks, backtracking attacks, time-space tradeoffs, BDD-based

D. Boneh (Ed.): CRYPTO 2003, LNCS 2729, pp. 162–175, 2003.

attacks etc.) were discussed in the relevant literature, and a lot of corresponding design criterions (correlation immunity, large period and linear complexity, good local statistics etc.) for such stream ciphers were developed (see, e.g., Rueppel (1991)).

A (k,l)-combiner consists of k LFSRs and a finite Mealy automaton with k input bits, one output bit and l memory bits. Let n be the sum of the lengths of the k LFSRs. Starting from a secret initial assignment $x^* \in \{0,1\}^n$, the LFSRs produce an internal linear bitstream $L(x^*)$, built by blocks x^t of k parallel bits for each clock t. Starting from a secret initial assignment $c^1 \in \{0,1\}^l$ to the memory bits, in each clock t the automaton produces the t-th keystream bit z_t corresponding to x^t and c^t and changes the inner state to c^{t+1} (see figure 1). The secret information is given by x^* and c^1. Numerous ciphers of this type are used in practice. Note, e.g., that the E_0 keystream generator used in the Bluetooth wireless LAN system (see Bluetooth SIG (2001)) is a $(4,4)$-combiner.

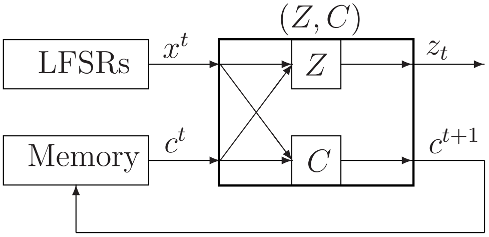

Fig. 1. A (k,l)-combiner

The aim of this paper is to analyze the security of (k,l)-combiners with respect to algebraic attacks, a new method for attacking stream and block ciphers. Algebraic attacks exist against AES and Serpent (Courtois and Pieprzyk (2002)) and Toyocrypt (Courtois (2002)). Related algebraic attacks were used to attack the HFE public key cryptosystem (Courtois (2001), cf. also Kipnis and Shamir (1999)).

Courtois and Meier (2003) discussed algebraic attacks on general LFSR-based stream ciphers and presented the best known attacks on Toyocrypt and LILI-128 so far. Very recently, Courtois introduced fast algebraic attacks on LFSR-based stream ciphers, an improved version of the algebraic attacks (Courtois (2003)).

An algebraic attack is based on a nontrivial low degree relation p for r clocks, i.e. a relation which holds for any sequence of r consecutive bits of the keystream and the corresponding kr internal bits. Given such a relation p of small degree d and a sufficiently long piece of a keystream $Z(x^*, c^1)$, p can be used to produce an overdefined system of T nonlinear equations in the initial bits of the LFSRs, which can be thought of as system of linear equations in the monomials of length at most d. If T is large enough then we get a unique solution which is induced by x^*, and from which x^* can be derived in a straightforward way.

Obviously, a higher value of d increases the running time significantly. Consequently, the nonexistence of nontrivial low degree relations is an important design criterion for (k, l)-combiners. One contribution of this paper is to provide an algorithm *FindRelation* which computes for a given (k, l)-combiner, represented by its automaton, and given d and r the set of all nontrivial degree d relation for r clocks (Section 3). One consequence is that nontrivial relations of degree $\lceil k(l+1)/2 \rceil$ relations for $l+1$ clocks (Theorem 1) cannot be avoided. Note that the running time is only polynomial in n if k and l are supposed to be constant. Hence, for each (k, l)-combiner exists a value n', such that the algebraic attack is more efficient than exhaustive search if $n \geq n'$.

E.g., this general bound implies a nontrivial degree 10 relation for 5 clocks for the E_0 generator, which yields, for $n = 128$, an algebraic attack of running time 2^{141}, which is much worse than exhaustive key-search. The algebraic attack would be better than exhaustive search if $n \geq 142$. Surprisingly, a nontrivial degree-4 relation for 4 clocks (Section 4) exists. This implies an algebraic attack of running time around $2^{67.58}$ and represents a serious weakness of this stream cipher. On the other hand, by using our method we can prove the nonexistence of nontrivial relations of degree smaller than 4, at least for 4 and 5 clocks. In the following section 2, we give basic definitions on boolean functions, LFSRs, and some notions around algebraic attacks.

2 Basics

2.1 Boolean Functions and $GF(2)$-Polynomials

In the following, we consider for all $k \geq 1$ the set B_k of k-ary boolean functions $f : \{0,1\}^k \longrightarrow \{0,1\}$ as a 2^k-dimensional vector space over the field $GF(2)$. It is a well known fact that each $f \in B_k$ has a unique representation as $GF(2)$-polynomial

$$p(x_1, \cdots, x_k) = \bigoplus_{\alpha \in \{0,1\}^k} a_\alpha m_\alpha, \qquad (1)$$

where for all $\alpha \in \{0,1\}^k$ the monomial m_α is defined as $m_\alpha = \Pi_{i, \alpha_i = 1} x_i$, and $a_\alpha \in GF(2)$. Let us denote $|\alpha| = |\{i, \alpha_i = 1\}|$ for all $\alpha \in \{0,1\}^k$. The degree $\deg(p)$ of the polynomial p is defined as $\max\{|\alpha|, a_\alpha = 1\}$. For all $f \in B_k$ we denote by $\deg(f)$ the degree of the unique $GF(2)$-polynomial for f. Given a set $B \subseteq B_k$ we denote by $\mathcal{H}(B)$ the set of all linear combinations of functions from B. Note that the set of all k-ary boolean functions of degree at most d equals $\mathcal{H}(\mathcal{M}(k, d))$, where $\mathcal{M}(k, d) = \{m_\alpha, \alpha \in \{0,1\}^k, |\alpha| \leq d\}$. The crucial computational problem here is $FindNullspace(B, X)$, where $B \subseteq B_k$ and $X \subseteq \{0,1\}^k$ for some $k \geq 1$, which consists in the computation of all $h \in \mathcal{H}(B)$ for which $h(x) = 0$ for all $x \in X$. Clearly, all $h \in \mathcal{H}(B)$ can be represented as $h = \sum_{b \in B} a(h)_b b$, and the set of all coefficient vectors $a(h) \in GF(2)^B$ solving $FindNullspace(B, X)$ equals the set of solutions of the system

$$\sum_{b\in B} a(h)_b b(x) = 0, \quad \text{for all } x \in X, \tag{2}$$

of $GF(2)$-linear equations.

As usual, we call a boolean function $f \in B_k$ to be an implicant of another boolean function $g \in B_k$ if $f(x) = 1$ implies $g(x) = 1$ for all inputs $x \in \{0,1\}^k$.

2.2 LFSRs and (k,l)-Combiners

Let $k > 0$ and $l \geq 0$ be integers. A (k,l)-combiner $\mathcal{C} = (Z, C)$ consists of k linear feedback shift registers (LFSRs) $L_1, \cdots, L_k$ and a finite Mealy automaton which is defined by an output function $Z : \{0,1\}^k \times \{0,1\}^l \longrightarrow \{0,1\}$ and a feedback function $C : \{0,1\}^k \times \{0,1\}^l \longrightarrow \{0,1\}^l$. In this paper, we assume that the following reasonable condition holds: For each $c \in \{0,1\}^l$ exist $x, x' \in \{0,1\}^k$ with $Z(x,c) = 0$ and $Z(x',c) = 1$. Notice that all known (k,l)-combiners used in cryptosystems are of this kind.

For each $i, 1 \leq i \leq k$, LFSR L_i is defined by its length $n(i)$ and a generator polynomial $L_i = (L_{i,1}, \cdots, L_{i,n(i)}) \in GF(2)^{n(i)}$. Let $n = n(1) + \cdots + n(k)$. It is common to suppose that the generator polynomials of the LFSRs are public.

Given an initial assignment $x_i^* = (x_{i,1}^*, \cdots, x_{i,n(i)}^*) \in \{0,1\}^{n(i)}$ to each LFSR L_i, $1 \leq i \leq k$, the LFSRs compute at each clock t a block $x^t = (x_1^t, \cdots, x_k^t)$ of internal bits, where for each $i, 1 \leq i \leq k$, it holds $x_i^t = x_{t,i}^*$ if $t \leq n(i)$, and

$$x_i^t = L_{i,1}x_i^{t-1} \oplus L_{i,2}x_i^{t-2} \oplus \cdots \oplus L_{i,n(i)}x_i^{t-n(i)} \tag{3}$$

if $t > n(i)$. The bitstream $L(x^*) = (x^1, x^2, \cdots)$ is called the internal linear bitstream generated on the initial assignment $x^* = (x_1^*, \cdots, x_k^*)$. Note that for all $t \geq 0$, the $GF(2)$-linear mapping $L^t : GF(2)^n \longrightarrow GF(2)^n$ which assigns to x^* the t-th block x^t of the corresponding linear bitstream can be efficiently computed from the generator polynomials.

Given such an internal bitstream $x = (x^1, x^2, \cdots)$ and an initial assignment $c^1 \in \{0,1\}^l$ to the memory bits, the corresponding output bitstream $(Z,C)(x, c^1) = (z_1, z_2, \cdots)$ is defined according to

$$z^t = Z(x^t, c^t) \quad \text{and} \quad c^{t+1} = C(x^t, c^t), \tag{4}$$

for all $t \geq 1$. For all $r \geq 1$ let us denote by $(Z,C)^r(x^1, \cdots, x^r, c^1)$ the first r output bits of the keystream generated according to x and c^1.

Given the combiner $\mathcal{C} = (Z, C)$, the cryptanalysis problem consists in discovering the secret initial assignment $x^* \in \{0,1\}^n$ to the LFSRs and the secret initial assignment $c^1 \in \{0,1\}^l$ to the memory bits from a sufficiently long prefix of the output keystream $(Z,C)(L(x^*), c^1)$. Our results are motivated by an approach due to Courtois and Pieprzyk (2002) to this problem, which consists in performing a so-called algebraic attack, and which is based on finding nontrivial low-degree relations which hold for any sequence of r consecutive output bits and the corresponding kr bits of the internal bitstream, for some $r \geq 1$. Let us now give an outline of this kind of attack.

2.3 Nontrivial Relations and Algebraic Attacks

We use the same denotations as in the previous subsection.

Definition 1. *Let $r \geq 1$ and $z \in \{0,1\}^r$. A non-zero $GF(2)$-polynomial p in kr variables is called a z-relation for $\mathcal{C}$ if $p(x) = 0$ holds for all sequences $x = (x^1, x^2, \cdots, x^r) \in \left(\{0,1\}^k\right)^r$ of r consecutive blocks of the internal bitstream which have the property that $(Z,C)^r(x,c) = z$ for some initial assignments $c \in \{0,1\}^l$ to the memory bits.*

Let us suppose that $\mathcal{C}$ has a z-relation p of degree d for some $r \geq 1$. Fix arbitrary assignments $x^* \in \{0,1\}^n$ to the LFSRs and $c^1 \in \{0,1\}^l$ to the memory bits. Suppose that we have a sufficiently long prefix of the corresponding output bitstream $z^* = (Z,C)(L(x^*), c^1)$ and denote by $T(z)$ the set of all clocks t, for which $(z^*_t, \cdots, z^*_{t+(r-1)}) = z$. By the definitions, it holds for all $t \in T(z)$ that

$$P_t(x^*) := p(L^t(x^*), \cdots, L^{t+(r-1)}(x^*)) = 0. \tag{5}$$

P_t is a $GF(2)$-polynomial of degree d in n variables which can be efficiently computed. Consequently, the system

$$P_t(x_1, \cdots, x_n) = 0, \ t \in T(z) \tag{6}$$

of nonlinear equations can be considered as a system of linear equations in the unknowns $\{m_\alpha(x), \alpha \in \{0,1\}^n, |\alpha| \leq d\}$. If $|T(z)|$ is large enough then this system of linear equations has the unique solution $\{m_\alpha(x^*), |\alpha| \leq d\}$, from which the secret x^* can be easily derived. Obvously, $|T(z)|$ has to be at least $M(n,p)$. Here, $M(n,p)$ denotes the set of all monomials in $x_1, \cdots, x_n$ which can occur in a $GF(2)$-polynomial contained as equation in the system (6). Observe that $\Phi(n,p) := \sum_{i=0}^{d} \binom{n}{i}$ is a trivial upper bound for $|M(n,p)|$. Note that the minimum number of keystream bits which has to be available can be reduced if we know several degree-d z-relations for different strings z. In any case, it follows that the existence of low-degree z-relations implies a serious weakness of (k,l)-combiners. These attacks are called algebraic attacks. In Courtois and Meier (2003), the authors discuss algebraic attacks against combiners without memory. In this paper, we extend these attacks to combiners with memory.

3 On Constructing Nontrivial Relations

In this section, we show that for any (k,l)-combiner $\mathcal{C}$, $r \geq k(l+1)$, and $d \geq \lceil k(l+1)/2 \rceil$, the existence of z-relations of degree d for some $z \in \{0,1\}^r$ cannot be avoided. Moreover, we present an algorithm which allows to construct all z-relations of degree at most d for any given r, d. Note that this solves an open problem stated, e.g., by Courtois (2003). This algorithm can be used for estimating the vulnerability of given (k,l)-combiners with respect to algebraic attacks (known from Courtois and Meier (2003)).

We first illustrate the problem of constructing nontrivial relations by means of some special cases. Let as before $\mathcal{C} = (Z, C)$ denote a (k, l)-combiner with output function Z and feedback function C. If $l = 0$, the construction of canceling relations for one clock is straightforward, as

$$Z(x_1^t, \cdots, x_k^t) \oplus z_t \quad , t \geq 0 \tag{7}$$

is always fulfilled. By arguments which will be given below this implies the existence of relations of degree at most $\lceil k/2 \rceil$.

Another tractable case is if $l = 1$ and the output function Z is linear in the feedback bit, i.e., $Z(x, c) = Z'(x) \oplus c$. Then the relation

$$z_2 = Z(x^2, C(x^1, z_1 \oplus x^1)) \tag{8}$$

is always true, which gives z-relations for all $z \in \{0,1\}^2$. If $l \geq 1$ and the output function is nonlinear, the situation becomes more complicated as, via the feedback function C, z_t depends nonlinearly on $x^1, x^2, \cdots, x^t$ for all $t \geq 0$. One attempt for constructing nontrivial relations could be to consider the relation

$$\bigwedge_{c \in \{0,1\}^l} \left(Z(x^t, c) \oplus z_t \right), \tag{9}$$

which obviously gives 0 for all pairs of input and output streams generated via $\mathcal{C}$. The problem here is that this relation can become trivial. This is especially true if Z is linear in at least one memory bit, as is the case for the E_0 generator. We use a more systematic approach and show the following result.

Theorem 1. *Let $k \geq 1$, $l \geq 1$ and a (k, l)-combiner $\mathcal{C} = (Z, C)$ be arbitrarily fixed. Then for each $r > l$ there is a z-relation of degree $\lceil (k(l+1)/2 \rceil$ for $\mathcal{C}$ for some $z \in \{0,1\}^r$.*

For the proof of this theorem we need some more technical definitions.

Definition 2. *(i) For all $r \geq 1$, $z \in \{0,1\}^r$, and $x = (x^1, \cdots, x^r) \in \left(\{0,1\}^k\right)^r$, x is called z-critical for $\mathcal{C}$ if $(Z, C)^r(x, c) \neq z$ for all $c \in \{0,1\}^l$. We denote by $Crit_{\mathcal{C}}(z)$ the set of all $x \in \left(\{0,1\}^k\right)^r$ which are z-critical for $\mathcal{C}$, and by $NCrit_{\mathcal{C}}(z)$ the set of all x which are not.*

(ii) The pair $(x, z) \in \left(\{0,1\}^k\right)^r \times \{0,1\}^r$ is called r-critical for $\mathcal{C}$ if x is z-critical for $\mathcal{C}$. We denote by $Crit_{\mathcal{C}}(r)$ the set of all r-critical $(x, z) \in \left(\{0,1\}^k\right)^r \times \{0,1\}^r$ and by $NCrit_{\mathcal{C}}(r)$ the set of all (x, r) which are not. Especially, we have $Crit_{\mathcal{C}}(r) \dot\cup NCrit_{\mathcal{C}}(r) = \{0,1\}^{kr} \times \{0,1\}^r$.

(iii) For all $r \geq 1$ we denote by $\chi(\mathcal{C})_r : \left(\{0,1\}^k\right)^r \times \{0,1\}^r \longrightarrow \{0,1\}$ the critical function of $\mathcal{C}$, which is defined as $\chi(\mathcal{C})_r(x, z) = 1$ iff (x, z) is r-critical for $\mathcal{C}$. For all $z \in \{0,1\}^r$ we denote by $\chi(\mathcal{C})_r^z$ the subfunction $\chi(\mathcal{C})_r(\cdot, z)$ which outputs 1 on $x \in \left(\{0,1\}^k\right)^r$ iff x is z-critical.

Observe that for all $r \geq 1$ and $z \in \{0,1\}^r$, a nontrivial $GF(2)$-polynomial p in kr variables is a z-relation of $\mathcal{C}$ iff it outputs 0 for all $x \in NCrit_{\mathcal{C}}(z)$ and outputs 1 for at least one $x \in Crit_{\mathcal{C}}(z)$. This implies

Lemma 1. *For all $r \geq 1$ and $z \in \{0,1\}^r$ there is a z-relation for $\mathcal{C}$ iff $Crit_{\mathcal{C}}(z) \neq \emptyset$. If $Crit_{\mathcal{C}}(z) \neq \emptyset$ then $p : \left(\{0,1\}^k\right)^r \longrightarrow \{0,1\}$ is a z-relation for $\mathcal{C}$ if and only if it is a nontrivial implicant of $\chi(\mathcal{C})^z_r$.*

For each non-critical pair $(x,z) \in \left(\{0,1\}^k\right)^r \times \{0,1\}^r$ there exists at least one $c \in \{0,1\}^l$ such that $z = (Z,C)^r(x,c)$. Evidently, the number of non-critical pairs cannot exceed $2^{kr} \cdot 2^l$. We obtain

Lemma 2. *For all $r \geq 1$ it holds that $|NCrit_{\mathcal{C}}(r)| \leq 2^{kr+l}$.*

For $r = l+1$, we have

$$|NCrit_{\mathcal{C}}(l{+}1)| \leq 2^{k\cdot(l+1)+l} < 2^{k\cdot(l+1)+l+1} = |Crit_{\mathcal{C}}(l{+}1)| + |NCrit_{\mathcal{C}}(l{+}1)| \quad (10)$$

Therefore, $|Crit_{\mathcal{C}}(r)| \neq 0$ and there is some $z \in \{0,1\}^r$ such that $|Crit_{\mathcal{C}}(z)| \neq \emptyset$.

For all $d \geq 0$ let us denote by $\mathcal{M}(kr,d)$ the set of all monomials over the kr variables $x^1, \cdots, x^r$ of length at most d. We derived

Lemma 3. *For all $r \geq 1$ and $z \in \{0,1\}^r$ the set of all z-relations for $\mathcal{C}$ equals the set of non-zero solutions of $FindNullspace(\mathcal{M}(kr,d), NCrit_{\mathcal{C}}(z))$.*

Lemma 4. *For each $r \geq 0$ and $z \in \{0,1\}^r$ the set $NCrit_{\mathcal{C}}(z)$ is not empty.*

Proof. We show this proposition by complete induction. As said in the beginning, we consider only combiners for which the following condition is true:

$$\forall c \in \{0,1\}^l \; \exists x, x' \in \{0,1\}^k : Z(x,c) = 0 \text{ and } Z(x',c) = 1 \quad (11)$$

This assures the proposition for $r = 1$. Let the proposition be true for some r. Choose $z = (z_1, \ldots, z_{r+1}) \in \{0,1\}^{r+1}$ arbitrarily. Then $NCrit_{\mathcal{C}}((z_1, \ldots, z_r)) \neq \emptyset$ by assumption. Let $x = (x^1, \ldots, x^r) \in NCrit_{\mathcal{C}}((z_1, \ldots, z_r))$. Then there exists a $c^1 \in \{0,1\}^l$ with $(Z,C)^r(x^1, \ldots, x^r, c^1) = (z_1, \ldots, z_r)$. By (11) we know that there is a least one $x^{r+1} \in \{0,1\}^k$ with $Z(x^{r+1}, c^{r+1}) = z_{r+1}$. Therefore, $(Z,C)^r(x^1, \ldots, x^{r+1}, c^1) = (z_1, \ldots, z_{r+1})$ and $(x^1, \ldots, x^{r+1}) \in NCrit_{\mathcal{C}}(z)$.

For showing the degree bound observe that if $|\mathcal{M}(kr,d)| = \Phi(kr,d)$ is greater than $|NCrit_{\mathcal{C}}(z)|$ then $FindNullspace(\mathcal{M}(kr,d), NCrit_{\mathcal{C}}(z))$ has a nontrivial solution. It suffices to prove the degree bound for $r = l{+}1$. Lemma 2 implies that $|NCrit_{\mathcal{C}}(l+1)| \leq 2^{k(l+1)+l} = \frac{1}{2}2^{k(l+1)+l+1}$, i.e., at most one half of all possible pairs (x,z) are not $(l+1)$-critical. Consequently, there exists at least one $z \in \{0,1\}^{l+1}$ for which at most half of all possible x are z-critical, i.e., $|NCrit_{\mathcal{C}}(z)| \leq \frac{1}{2}2^{k(l+1)}$.On the other hand, by lemma 4 we know that $|NCrit_{\mathcal{C}}(z)| > 0$. Using the fact that $\Phi(N, \lceil N/2 \rceil) > \frac{1}{2}2^N$ for all $N \geq 2$, we obtain the theorem.

We derived the following algorithm for the problem $FindRelation(Z,C,z,d)$ of computing all z-relations p of degree at most d for a given (k,l)-combiner $\mathcal{C} = (Z,C)$.

```
1 Compute $Crit_{\mathcal{C}}(z)$ and $NCrit_{\mathcal{C}}(z)$.
2 If $Crit_{\mathcal{C}}(z) \neq \emptyset$ then solve $FindNullspace(\mathcal{M}(kr,d), NCrit_{\mathcal{C}}(z))$.
```

Note that the computation of $Crit_{\mathcal{C}}(z)$ and $NCrit_{\mathcal{C}}(z)$ can be done in an elegant way by using an ordered binary decision diagram (OBDD) of size at most $(kr+r)2^{k+l+1}$ for $\chi(\mathcal{C})_r$ (see, e.g., Krause (2002) for the details). Step 2 requires to solve a system of $GF(2)$-linear equations with $\mathcal{M}(kr,d)$ unknowns and at most 2^{kr+l} linear equations.

4 Analyzing the E_0 Keystream Generator

In this section, we apply our results to the E_0 keystream generator. The E_0 keystream generator is part of the Bluetooth encryption system, used for wireless communication (see, e.g., Bluetooth SIG (2001)). It is a $(4,4)$-combiner. Applying our results yields the existence of a nontrivial 5-relation of degree 10. The number of monomials is $T \leq \Phi(n,10)$. Therefore, the secret key can be recovered by solving a system of linear equations in T unknowns. The fastest practial algorithm we are aware of to solve a system of linear equations is the algorithm by Strassen (1969). It requires about $7 \cdot T^{\log_2 7}$ operations. Our attack is more efficient than exhaustive search, if the following inequality holds:

$$2^n > 7 \cdot (\Phi(n,10))^{\log_2 7}. \tag{12}$$

This is the case for $n \geq 142$. Notice, that in the Bluetooth encryption system the length of the secret key is $n = 128$.

If the E_0 keystream generator were optimally resistant against algebraic attacks, no canceling relations for $r < 5$ or $d < 10$ should exist. Surprisingly, for $d = 4$ and $r = 4$ such a relation can be found. In this case, it is even possible to show the existence directly.

Let us first recall the definitions of the keystream generator. The keystream generator consists of $k = 4$ regularly clocked LFSRs and $l = 4$ memory bits. With each clock, an output bit z_t is produced depending on the outputs $x^t = (x_1^t, x_2^t, x_3^t, x_4^t)$ of the four LFSRs and the four memory bits $c^t = (q^t, p^t, q^{t-1}, p^{t-1})$. Then, the next memory bits $c^{t+1} = (q^{t+1}, p^{t+1}, q^t, p^t)$ are calculated and so on. We see that the memory bits q^t and p^t are used in both clocks t and $t+1$. Let $\pi_s(t)$ be the symmetric $GF(2)$-polynomial over $x_1^t, x_2^t, x_3^t, x_4^t$ which consists of the sum of all monomials of length $s \leq 4$. Then the output bit z_t and the memory bits are computed by the following equations

$$\begin{aligned} z_t &= \pi_1(t) \oplus p^t && (13)\\ c^{t+1} &= (q^{t+1}, p^{t+1}, q^t, p^t) && (14)\\ &= (\mathcal{S}_1^{t+1} \oplus q^t \oplus p^{t-1}, \mathcal{S}_0^{t+1} \oplus p^t \oplus q^{t-1} \oplus p^{t-1}, q^t, p^t), && (15) \end{aligned}$$

where

$$\mathcal{S}_{t+1} = (\mathcal{S}_{t+1}^1, \mathcal{S}_{t+1}^0) = \left\lfloor \frac{x_1^t + x_2^t + x_3^t + x_4^t + 2 \cdot q^t + p^t}{2} \right\rfloor. \tag{16}$$

The values for c^1 and the contents of the LFSRs must be set before the start, the other values will then be calculated. Obviously, the value of q^{t+1} depends only on x^t, q^t, p^t and p^{t-1} and the value of p^{t+1} on x^t, q^t, q^{t-1}, p^t and p^{t-1}. The calculations of q^{t+1} and p^{t+1} are done via the following equations (see appendix A for details)

$$\begin{aligned} q^{t+1} &= \pi_4(t) \oplus \pi_3(t)p^t \oplus \pi_2(t)q^t \oplus \pi_1(t)p^t q^t \oplus q^t \oplus p^{t-1} & (17)\\ p^{t+1} &= \pi_2(t) \oplus \pi_1(t)p^t \oplus q^t \oplus q^{t-1} \oplus p^{t-1} \oplus p^t & (18)\end{aligned}$$

If we define the following additional variables

$$\begin{aligned} a(t) &= \pi_4(t) \oplus \pi_3(t)p^t \oplus p^{t-1}\\ b(t) &= \pi_2(t) \oplus \pi_1(t)p^t \oplus 1,\end{aligned}$$

equations (17) and (18) can be rewritten to

$$\begin{aligned} q^{t+1} &= a(t) \oplus b(t)q^t & (19)\\ p^{t+1} &= b(t) \oplus 1 \oplus p^{t-1} \oplus p^t \oplus q^t \oplus q^{t-1}. & (20)\end{aligned}$$

By multiplying (19) with $b(t)$ we get another equation

$$0 = b(t)(a(t) \oplus q^t \oplus q^{t+1}). \tag{21}$$

Equation (20) is equivalent to

$$q^t \oplus q^{t-1} = b(t) \oplus 1 \oplus p^{t-1} \oplus p^t \oplus p^{t+1}. \tag{22}$$

Now we insert (22) into (21) with index $t+1$ instead of t and get

$$0 = b(t)\left(a(t) \oplus b(t+1) \oplus 1 \oplus p^t \oplus p^{t+1} \oplus p^{t+2}\right).$$

Using (13), we eliminate all memory bits in the equation and get the following equation which holds for every clock t:

$$\begin{aligned} 0 = {} & 1 \oplus z_{t-1} \oplus z_t \oplus z_{t+1} \oplus z_{t+2}\\ & \oplus \pi_1(t) \cdot (z_t z_{t+2} \oplus z_t z_{t+1} \oplus z_t z_{t-1} \oplus z_{t-1} \oplus z_{t+1} \oplus z_{t+2} \oplus 1)\\ & \oplus \pi_2(t) \cdot (1 \oplus z_{t-1} \oplus z_t \oplus z_{t+1} \oplus z_{t+2}) \oplus \pi_3(t)z_t \oplus \pi_4(t)\\ & \oplus \pi_1(t-1) \oplus \pi_1(t-1)\pi_1(t)(1 \oplus z_t) \oplus \pi_1(t-1)\pi_2(t)\\ & \oplus \pi_1(t+1)z_{t+1} \oplus \pi_1(t+1)\pi_1(t)z_{t+1}(1 \oplus z_t) \oplus \pi_1(t+1)\pi_2(t)z_{t+1}\\ & \oplus \pi_2(t+1) \oplus \pi_2(t+1)\pi_1(t)(1 \oplus z_t) \oplus \pi_2(t+1)\pi_2(t)\\ & \oplus \pi_1(t+2) \oplus \pi_1(t+2)\pi_1(t)(1 \oplus z_t) \oplus \pi_1(t+2)\pi_2(t)\end{aligned}$$

This gives a nontrivial degree-4 z-relation p for 4 clocks for any $z \in \{0,1\}^4$. The number $M(128, p)$ of monomials occuring in the corresponding system of nonlinear equations (see subsection 2.2) can not exceed $\Phi(128, 4) \approx 2^{23.39}$. In fact, if we look closely at p, we can see that not all monomials of $\mathcal{M}(kr, d)$ occur. Thus, we have $M(128, p) \leq T := 8,824,350 \approx 2^{23.07}$ (see appendix B for details).

With each clock t, we get a new equation in the bits of the secret key. If we have at least $M(128, p)$ linearly independent equations, x^* can be recovered by solving the system of linear equations. Using Strassen's algorithm, the secret key can be recovered with work $\leq 7 \cdot T^{\log_2 7} \approx 2^{67.58}$. The memory complexity is more or less the size of the matrix which is about $2^{46.14}$.

Obviously, to get enough linearly independent equations, we have to clock at least $M(128, p)$ times. The question is whether we have to clock more often. Until now, there is no satisfying answer to this question. Our assumption is that approximately T clocks should be enough, meaning that about $2^{23.07}$ key stream bits would be sufficient to mount the attack. We did some simulations for the same cryptosystem but with shorter LFSRs. The results can be seen in Table 1. Each time, the initial values of the LFSRs were successfully reconstructed. In all cases the number of clocks needed to reconstruct the secret key was close (or even equal) to $T + 3$.[1]

Table 1. Algebraic attacks on smaller E_0 crypto systems

$n(1), n(2), n(3), n(4)$	Initial Values	Feedback Taps	T	Clocks
1, 2, 3, 5	1 11 011 11110	1 11 101 10100	477	483
1, 2, 3, 5	1 10 101 01101	1 11 101 10100	477	481
1, 2, 3, 5,	1 01 010 01001	1 11 101 11011	477	480
1, 2, 3, 5	1 11 111 01111	1 11 101 11110	477	483
1, 2, 3, 5,	1 01 010 10100	1 11 110 11011	477	484
2, 3, 5, 7	10 010 11110 1100110	11 110 11101 1000100	2643	2647
2, 3, 5, 7	11 101 01101 0010011	11 101 10100 1101010	2643	2649
2, 3, 5, 7	10 100 10001 0010001	11 110 11110 1111000	2643	2647

Of course, a lower degree d would decrease the value of T and therefore allow a better attack. Applying our algorithm showed the non-existence of nontrivial relations of degree $d = 3$ for $r = 4$ and $r = 5$. Nevertheless, lower degree relations for $r > 5$ may exist.

It is important to mention that in the Bluetooth encryption system the secret key is changed after 2745 clocks. Therefore, we will never get enough equations in pratice. Note that the best published attack against the E_0 was proposed by Krause (2002) with time and memory effort of $\approx 2^{77}$, given only 128 known key stream bits. The attack by Fluhrer and Lucks (2001) needs about 2^{73} operations if 2^{43} bits are available. The memory needed is very small: about 10638 bits.

Recently, Courtois developed an improved version of algebraic attacks: fast algebraic attacks (Courtois (2003)). They allow an even better attack on the E_0 keystream generator. The estimation is that about 2^{49} operations are enough.

[1] As we need 4 succesive clocks to produce one equation the number of clocks needed is at least $T + 3$

We want to point out one remarkable fact. The output function was chosen to be linear in one memory bit to achieve maximum correlation immunity. The same attribute made it possible to eliminate the same memory bit in our relation. This may be a hint that some tradeoff between correlation immunity of the output function and resistance against algebraic attacks exists.

5 Discussion

We have seen that for all (k, l)-combiners, nontrivial relations of degree at most $\lceil k(l+1)/2 \rceil$ exist. This fact extends the attacks described by Courtois and Meier (2003) to combiners with memory. In consequence, each combiner is vulnerable against algebraic attacks if the length of the secret key n is large enough. E.g., for the E_0 keystream generator this is the case for $n \geq 142$. A (k, l)-combiner should be designed in such a way that an algebraic attack never becomes faster than exhaustive key-search. For this purpose, it should be checked if the automaton induces nontrivial degree-d relations for critical values of d. This can be done by applying the algorithm *FindRelation* presented in this paper, at least for a reasonable set of clocks.

The analysis of the E_0 generator shows that it may be dangerous to use a linear output function, since this may help replacing the memory bits and deriving nontrivial low-degree relations. It turns out that a nontrivial relation of degree 4 exists. This makes it possible to recover the secret key by solving a system of linear equations in at most $2^{23.07}$ unknowns.

Algebraic attacks work successfully only for LFSR-based stream ciphers which are oblivious in the sense that the attacker always knows which bit of the keystream depends on which bits of the internal bitstream. It would be interesting to know if similar attacks can also be applied to non-oblivious ciphers like the A5 generator or the shrinking generator.

Acknowledgment. The authors would like to thank Nicolas Courtois, Erik Zenner, Stefan Lucks and some unknown referees for helpful comments and discussions.

References

1. Bluetooth SIG, *Specification of the Bluetooth system*, Version 1.1, 1 February 22, 2001, available at http://www.bluetooth.com/.
2. Nicolas Courtois: *Higher Order Correlation Attacks, XL Algorithm and Cryptanalysis of Toyocrypt*, 5th International Conference on Information Security and Cryptology: ICISC 2002, November 2002, Seoul, Korea, Springer LNCS 2587. An updated version is available at http://eprint.iacr.org/2002/087.
3. Nicolas Courtois and Willi Meier: *Algebraic Attacks on Stream Ciphers with Linear Feedback*, Proceedings of Eurocrypt 2003, Warsaw, Poland, Springer LNCS 2656.
4. Nicolas Courtois: *Fast Algebraic Attacks on Stream Ciphers with Linear Feedback*, these proceedings.

5. Nicolas Courtois, Josef Pieprzyk: *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations*, Proceedings of Asiacrypt '02, Springer LNCS 2501, 2002, pp. 267–287.
6. Nicolas Courtois: *Personal communication*, 2003
7. Scott R. Fluhrer, Stefan Lucks: *Analysis of the E_0 Encryption System*, Proceedings of Selected Areas of Cryptography '01, Springer LNCS 2259, 2001, pp. 38–48.
8. Matthias Krause: *BDD-Based Cryptanalysis of Keystream Generators*; Proceedings of Eurocrypt '02, Springer LNCS 2332, 2002, pp. 222–237.
9. Rainer A. Rueppel: *Stream Ciphers*; Contemporary Cryptology: The Science of Information Integrity. G. Simmons ed., IEEE Press New York, 1991.
10. Adi Shamir, Aviad Kipnis: *Cryptanalysis of the HFE Public Key Cryptosystem*; Proceedings of Crypto '99, Springer LNCS 1666, 1999, pp. 19–30.
11. Adi Shamir, Jacques Patarin, Nicolas Courtois, Alexander Klimov: *Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations*, Proceedings of Eurocrypt '00, Springer LNCS 1807, pp. 392–407.
12. Volker Strassen: *Gaussian Elimination is Not Optimal*; Numerische Mathematik, vol 13, pp 354–356, 1969.

A The Equations for q_{t+1} and p_{t+1}

In this section we prove the correctness of equations (17) resp. (18) for q^{t+1} resp. p^{t+1}. Let us recall the equation for c^{t+1}

$$\begin{aligned} c^{t+1} &= (q^{t+1}, p^{t+1}, q^t, p^t) && (23)\\ &= (\mathcal{S}_1^{t+1} \oplus q^t \oplus p^{t-1}, \mathcal{S}_0^{t+1} \oplus p^t \oplus q^{t-1} \oplus p^{t-1}, q^t, p^t) && (24) \end{aligned}$$

where

$$\mathcal{S}_{t+1} = (\mathcal{S}_{t+1}^1, \mathcal{S}_{t+1}^0) = \left\lfloor \frac{x_1^t + x_2^t + x_3^t + x_4^t + 2 \cdot q^t + p^t}{2} \right\rfloor \qquad (25)$$

Let f_0 resp. f_1 be the two boolean functions for which the equations

$$\mathcal{S}_{t+1}^i = f_i(x_1^t, x_2^t, x_3^t, x_4^t, q^t, p^t) \qquad (26)$$

hold for $i \in \{0, 1\}$. f_0 and f_1 can be found with the help of computers. If we write down f_0 and f_1 in algebraic normal form, we get

$$\begin{aligned} f_1 &= \pi_4(t) \oplus \pi_3(t)p^t \oplus \pi_2(t)q^t \oplus \pi_1(t)p^t q^t && (27)\\ f_0 &= \pi_2(t) \oplus \pi_1(t)p^t \oplus q^t && (28) \end{aligned}$$

See section 4 for the definition of $\pi_k(t)$. In table 2, f_0 and f_1 are evaluated for all possible inputs and compared with $\mathcal{S}_{t+1}$. It is easy to see that f_0 and f_1 fulfill the requirements. Together with (24), we get the following expressions for q^{t+1} and p^{t+1}

$$\begin{aligned} q^{t+1} &= S_{t+1}^1 \oplus q^t \oplus p^{t-1} && (29)\\ &= \pi_4(t) \oplus \pi_3(t)p^t \oplus \pi_2(t)q^t \oplus \pi_1(t)p^t q^t \oplus q^t \oplus p^{t-1} && (30)\\ p^{t+1} &= \mathcal{S}_{t+1}^0 \oplus p^t \oplus q^{t-1} \oplus p^{t-1} && (31)\\ &= \pi_2(t) \oplus \pi_1(t)p^t \oplus q^t \oplus q^{t-1} \oplus p^t \oplus p^{t-1} && (32) \end{aligned}$$

Table 2. f_0 and f_1 evaluated for all possible inputs and compared with $\mathcal{S}_{t+1}$

a_t	b_t	c_t	d_t	Q_t	P_t	S_{t+1}	f_1	f_0		a_t	b_t	c_t	d_t	Q_t	P_t	S_{t+1}	f_1	f_0
0	0	0	0	0	0	0	0	0		1	0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	0	0		1	0	0	0	0	1	1	0	1
0	0	0	0	1	0	1	0	1		1	0	0	0	1	0	1	0	1
0	0	0	0	1	1	1	0	1		1	0	0	0	1	1	2	1	0
0	0	0	1	0	0	0	0	0		1	0	0	1	0	0	1	0	1
0	0	0	1	0	1	1	0	1		1	0	0	1	0	1	1	0	1
0	0	0	1	1	0	1	0	1		1	0	0	1	1	0	2	1	0
0	0	0	1	1	1	2	1	0		1	0	0	1	1	1	2	1	0
0	0	1	0	0	0	0	0	0		1	0	1	0	0	0	1	0	1
0	0	1	0	0	1	1	0	1		1	0	1	0	0	1	1	0	1
0	0	1	0	1	0	1	0	1		1	0	1	0	1	0	2	1	0
0	0	1	0	1	1	2	1	0		1	0	1	0	1	1	2	1	0
0	0	1	1	0	0	1	0	1		1	0	1	1	0	0	1	0	1
0	0	1	1	0	1	1	0	1		1	0	1	1	0	1	2	1	0
0	0	1	1	1	0	2	1	0		1	0	1	1	1	0	2	1	0
0	0	1	1	1	1	2	1	0		1	0	1	1	1	1	3	1	1
0	1	0	0	0	0	0	0	0		1	1	0	0	0	0	1	0	1
0	1	0	0	0	1	1	0	1		1	1	0	0	0	1	1	0	1
0	1	0	0	1	0	1	0	1		1	1	0	0	1	0	2	1	0
0	1	0	0	1	1	2	1	0		1	1	0	0	1	1	2	1	0
0	1	0	1	0	0	1	0	1		1	1	0	1	0	0	1	0	1
0	1	0	1	0	1	1	0	1		1	1	0	1	0	1	2	1	0
0	1	0	1	1	0	2	1	0		1	1	0	1	1	0	2	1	0
0	1	0	1	1	1	2	1	0		1	1	0	1	1	1	3	1	1
0	1	1	0	0	0	1	0	1		1	1	1	0	0	0	1	0	1
0	1	1	0	0	1	1	0	1		1	1	1	0	0	1	2	1	0
0	1	1	0	1	0	2	1	0		1	1	1	0	1	0	2	1	0
0	1	1	0	1	1	2	1	0		1	1	1	0	1	1	3	1	1
0	1	1	1	0	0	1	0	1		1	1	1	1	0	0	2	1	0
0	1	1	1	0	1	2	1	0		1	1	1	1	0	1	2	1	0
0	1	1	1	1	0	2	1	0		1	1	1	1	1	0	3	1	1
0	1	1	1	1	1	3	1	1		1	1	1	1	1	1	3	1	1

B The Number of Terms

In this section, we estimate the maximum number T of different monomials in the algebraic attack against the E_0 crypto system. With each clock t the following equation is produced

$$\begin{aligned}0 = 1 &\oplus z_{t-1} \oplus z_t \oplus z_{t+1} \oplus z_{t+2}\\ &\oplus \pi_1(t) \cdot (z_t z_{t+2} \oplus z_t z_{t+1} \oplus z_t z_{t-1} \oplus z_{t-1} \oplus z_{t+1} \oplus z_{t+2} \oplus 1)\\ &\oplus \pi_2(t) \cdot (1 \oplus z_{t-1} \oplus z_t \oplus z_{t+1} \oplus z_{t+2}) \oplus \pi_3(t) z_t \oplus \pi_4(t)\\ &\oplus \pi_1(t-1) \oplus \pi_1(t-1)\pi_1(t)(1 \oplus z_t) \oplus \pi_1(t-1)\pi_2(t)\\ &\oplus \pi_1(t+1) z_{t+1} \oplus \pi_1(t+1)\pi_1(t) z_{t+1}(1 \oplus z_t) \oplus \pi_1(t+1)\pi_2(t) z_{t+1}\end{aligned}$$

$$\oplus\pi_2(t+1) \oplus \pi_2(t+1)\pi_1(t)(1 \oplus z_t) \oplus \pi_2(t+1)\pi_2(t)$$
$$\oplus\pi_1(t+2) \oplus \pi_1(t+2)\pi_1(t)(1 \oplus z_t) \oplus \pi_1(t+2)\pi_2(t).$$

As we can see, every occurring term has to be one of the following types

$$a, b, c, d, ab, ac, ad, bc, bd, cd, abc, acd, abd, bcd, abcd, aa'bc, aa'cd, aa'bd,$$
$$bb'ac, bb'cd, bb'ad, cc'ab, cc'ad, cc'bd, dd'ab, dd'ac, dd'bc, aa'bb', aa'cc',$$
$$aa'dd', bb'cc', bb'dd', cc'dd', aa'b, aa'c, aa'd, bb'a, bb'c, bb'd, cc'a, cc'b,$$
$$cc'd, dd'a, dd'b, dd'c, aa', bb', cc', dd'$$

Here, $a, a' \in \{x^*_{1,1}, \ldots, x^*_{1,n_1}\}$ with $a \neq a'$, etc. In table 3 the number of possible terms for each type is presented depending on the length n_1, n_2, n_3, and n_4 of the four LFSRs. In addition, we give for each type one product in which it can occur. Note that some terms may occur in other products too[2]. Of course, these types have to be counted only once. The sum is the number of possible terms T. In E_0, the lengths are $n_1 = 25$, $n_2 = 31$, $n_3 = 33$ and $n_4 = 39$, so $T = 8,824,350$, which is approximately $2^{23.07}$.

Table 3. All possible terms and their number depending on n_i

type	occur in	number
a,b, c, d	$\pi_1(t)$	$n_1 + n_2 + n_3 + n_4$
ab, ac, ad, bc, bd, cd	$\pi_2(t)$	$n_1(n_2 + n_3 + n_4) + n_2(n_3 + n_4) + n_3n_4$
abc, acd, abd, bcd	$\pi_3(t)$	$n_1(n_2n_3 + n_2n_4 + n_3n_4) + n_2n_3n_4$
$abcd$	$\pi_4(t)$	$n_1n_2n_3n_4$
aa', bb', cc', dd'	$\pi_1(t) \cdot \pi_1(t')$	$\sum_{i=1}^4 \frac{1}{2}n_i(n_i - 1)$
$aa'b, aa'c, aa'd$	$\pi_1(t) \cdot \pi_2(t')$	$\frac{1}{2}n_1(n_1 - 1)(n_2 + n_3 + n_4)$
$bb'a, bb'c, bb'd$	$\pi_1(t) \cdot \pi_2(t')$	$\frac{1}{2}n_2(n_2 - 1)(n_1 + n_3 + n_4)$
$cc'a, cc'b, cc'd$	$\pi_1(t) \cdot \pi_2(t')$	$\frac{1}{2}n_3(n_3 - 1)(n_1 + n_2 + n_4)$
$dd'a, dd'b, dd'c$	$\pi_1(t) \cdot \pi_2(t')$	$\frac{1}{2}n_4(n_4 - 1)(n_1 + n_2 + n_3)$
$aa'bc, aa'cd, aa'bd$	$\pi_2(t) \cdot \pi_2(t')$	$\frac{1}{2}n_1(n_1 - 1)(n_2n_3 + n_2n_4 + n_3n_4)$
$bb'ac, bb'cd, bb'ad$	$\pi_2(t) \cdot \pi_2(t')$	$\frac{1}{2}n_2(n_2 - 1)(n_1n_3 + n_1n_4 + n_3n_4)$
$cc'ab, cc'ad, cc'bd$	$\pi_2(t) \cdot \pi_2(t')$	$\frac{1}{2}n_3(n_3 - 1)(n_1n_2 + n_1n_4 + n_2n_4)$
$dd'ab, dd'ac, dd'bc$	$\pi_2(t) \cdot \pi_2(t')$	$\frac{1}{2}n_4(n_4 - 1)(n_1n_2 + n_1n_3 + n_2n_3)$
$aa'bb', aa'cc', aa'dd'$	$\pi_2(t) \cdot \pi_2(t')$	$\frac{1}{2}n_1(n_1 - 1)\left(\sum_{i=2}^4 \frac{1}{2}n_i(n_i - 1)\right)$
$bb'cc', bb'dd'$	$\pi_2(t) \cdot \pi_2(t')$	$\frac{1}{4}n_2(n_2 - 1)\left[n_3(n_3 - 1) + n_4(n_4 - 1)\right]$
$cc'dd'$	$\pi_2(t) \cdot \pi_2(t')$	$\frac{1}{4}n_3(n_3 - 1)n_4(n_4 - 1)$

[2] For example, a term of type abc can occur in $\pi_1(t)\pi_2(t')$ and in $\pi_2(t)\pi_2(t')$