Collective Encryption: Cryptosystems Based on the Commutator Collection Process for Certain Free Products.

by

Dimitri Vulis

A dissertation submitted to the Graduate Faculty in Mathematics

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy, The City University of New York

1995

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

April 16, 1995

Date

Michael Anshel

Chair of Examining Committee

April 13, 1995

Date

Executive Officer

Professor Michael Anshel

Michael Anshel

Professor Alphonse Vasquez

Professor Burton Randol

Supervisory Committee

The City University of New York

Abstract

Collective Encryption: Cryptosystems Based on the Commutator Collection Process for Certain Free Products.

by

Dimitri Vulis

Adviser: Professor Michael Anshel

We present some new public and innovative private key cryptosystems based on the collection process for the lower central series of the free product of finitely many Burnside groups of finite rank and of exponent 2. These groups are residually nilpotent, and their lower central series may be investigated using efficient group-theoretic algorithms. This allows us to create new and innovative methods for encrypting and decrypting data via computational group theory. We refer to the general methodology as *collective encryption.* We have performed various experiments centered on collective encryption and have related our methods to contemporary advances in cryptology. Applying the recent test by Ueli Maurer we demonstrate that the encrypted data appears fairly random. Computational experiments allow us to pose a conjecture about the complexity of our algorithm. We also state several open problems and indicate directions and methodology for future research.

Acknowledgments

I am greatly indebted to my mentor, Michael Anshel, for his extraordinary patience and kindness.

I thank my wife Marina Vulis, my son Daniel Vulis, and my mother-in-law Alla Inzel, whose love, support, and tolerance allowed me to complete this dissertation. I gratefully acknowledge Iris Anshel's help in preparing this manuscript. I also thank Burton Randol and Alphonse Vasquez, who have been my teachers for so many years; and of course Dennis Spellman, Anthony Gaglione, and Donald Knuth for many enjoyable and valuable communications.

Contents

List of Figures

1 Basic Commutators

This section will serve as a brief review of fundamental concepts from the theory of commutator calculus which was first developed by P. Hall [6]. We begin by defining and giving examples of the basic commutators as generators of the factor groups of the lower central series of a free group F on r generators which we denote by

$$F(r) = \langle x_1, x_2, \ldots, x_r \rangle.$$

The *commutator* of two elements a, b of a group H, denoted (a, b), is defined to be the element $a^{-1}b^{-1}ab$. Given subgroups H_1, H_2 of H, we let

$$[H_1, H_2] = \langle (h_1, h_2) | h_i \in H_i, i = 1, 2 \rangle$$

The *lower central series* of a group H [9, p. 293] is the descending series:

$$H_1 \supseteq H_2 \supseteq H_3 \supseteq \cdots$$

which is defined inductively: $H_1 = H$, $H_2 = [H, H]$, and for $n > 2$, $H_n = [H, H_{n-1}]$. Observe that for each n, H_n is normal in H_{n-1}.

We now define the basic commutators c_i, $i = 1, 2, \ldots$, their dimensions $D(c_i)$, and their ordering according to R. Prener [14, p. 9].

DEFINITION 1.1

i) The *basic commutators of dimension 1* are the generators: $c_i = x_i$, $i = 1, \ldots, r$, ordered by their subscripts: $c_i > c_j$ if and only if $i > j$. Note that they cannot, in general, be expressed as (a, b) commutators, where a, b are the elements of the group.

ii) Suppose we have defined basic commutators of dimension less than n and their ordering, as we have already done for dimension 1. Now we recursively define the *basic commutators of dimension* n to be the set of all commutators $c_k = (c_i, c_j)$ such that:

a) c_i and c_j are basic commutators the sum of whose dimensions, $D(c_i) + D(c_j)$, is n,

b) $c_i > c_j$ (where $>$ is the ordering already defined on commutators of dim $< n$),

c) if $c_i = (c_k, c_l)$ (i.e., $D(c_i) > 1$), then $c_j \geq c_l$.

iii) We define the ordering of the basic commutators of dimension $n > 1$ as follows: if $D(c_i) = D(c_j) = n > 1$ (that is, $c_i = (c_{i_1}, c_{j_1})$, $c_j = (c_{i_2}, c_{j_2})$, and c_{i_k}, c_{j_k} are of dimensions less than n), then $c_i > c_j$ if and only if either

a) $c_{i_1} > c_{i_2}$, or

b) $c_{i_1} = c_{i_2}$ and $c_{j_1} > c_{j_2}$.

iv) If $D(c_i) > D(c_j)$ then $c_i > c_j$.

It is intrinsic in the definition that any two basic commutators c_j's are comparable.

Following H. Waldinger [**17**], R. Prener imposed in his thesis [**14**] the formal order (iv), while M. Hall in his earlier definition [**5**, p. 165] defined the basic commutators of equal dimension to be ordered arbitrarily with respect to each other.

Basic commutators play an essential role in the lower central series of a free group. By that we mean that basic commutators of dimension n are the free generators of the free abelian quotients F_n/F_{n+1}. The number of basic commutators of dimension n is given by the Witt formula [**5**, p. 169],

$$M_r(n) = \frac{1}{n} \sum_{d|n} \mu(d) r^{n/d},$$

where $\mu(d)$ is the classical Möbius function:

$$\mu(n) = \begin{cases} 1 & n = 1, \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes}, \\ 0 & \text{otherwise.} \end{cases}$$

2 Crucial Commutators

In this section we introduce the crucial commutators which play a central role in our exposition. The collection process, which is an efficient algorithm for collecting words in a certain class of factor groups, was introduced by M. Hall in [5]. Let $G(r)$ denote the free product of r cyclic groups of order 2 whose presentation is given by

$$\langle x_1, \ldots, x_r; x_1^2, \ldots, x_r^2 \rangle,$$

and let $G(r,k)$ denote the quotient $G(r)/G(r)_k$.

The group $G(r,3)$ will be of central interest to us. We begin with the technical definition of the crucial commutators and their ordering.

We now define the set of *3-crucial commutators* of $G(r)$ and their ordering:

DEFINITION 2.1 An element $g \in G(r)$ is a crucial commutator if

i) $g = x_j$, one of the generators of $G(r)$; or

ii) $g = (x_j, x_i) = x_j^{-1} x_i^{-1} x_j x_i$, such that $1 \leq i < j \leq r$.

For two crucial commutators e_a, e_b of $G(r)$, we say that $e_a > e_b$ provided

iii) $e_a = x_i$, $e_b = x_j$, $i > j$; or

iv) $e_a = (x_j, x_i)$, $e_b = x_k$; or

v) $e_a = (x_i, x_j)$, $e_b = (x_k, x_l)$ and $i > k$ or $i = k$ and $j > l$.

We shall refer to the set of 3-crucial commutators e_i as simply *crucial commutators,* and denote it by $E(r)$.

As an illustration of the nature of the crucial commutators we consider some low values of r

$$\begin{aligned} E(3) &= \{x_1, x_2, x_3, (x_2, x_1), (x_3, x_1), (x_3, x_2)\} \\ E(4) &= \{x_1, x_2, x_3, x_4, (x_2, x_1), (x_3, x_1), (x_3, x_2), (x_4, x_1), (x_4, x_2), (x_4, x_3)\} \\ E(5) &= \{x_1, x_2, x_3, x_4, x_5, (x_2, x_1), (x_3, x_1), (x_3, x_2), (x_4, x_1), (x_4, x_2), (x_4, x_3), \\ &\quad (x_5, x_1), (x_5, x_2), (x_5, x_3), (x_5, x_4)\} \end{aligned}$$

A moment of observation yields the following basic lemma.

LEMMA 2.2 *Suppose the basic commutators are ordered as follows:*

$$x_1, x_2, \ldots, x_r, x_{r+1} = (x_2, x_1), x_{r+2} = (x_3, x_1), x_{r+3} = (x_3, x_2,), \ldots$$

Then the basic commutator (e_p, e_q) *can be written as*

$$(e_p, e_q) = e_{r+q+(p-1)(p-2)/2}.$$

3 Presentation for $G(r, 3)$

In this section we give the presentation for the group $G(r, 3)$, and demonstrate the uniqueness of the collection process in the group.

The proof of the following theorem is due to Dennis Spellman [**16**]:

THEOREM 3.1 *The quotient group $G(r,3)$ has the presentation:*

$$\langle x_1,\ldots,x_r; x_1^2=\cdots=x_r^2=1,((x_i,x_j),x_k)=1, i>j, j\leq k\leq r, i,j\geq 1\rangle \tag{3.2}$$

The order of the group is

$$|G/G_3)| = 2^{r(r+1)/2}. \tag{3.3}$$

Proof. By definition the group G is given by the presentation

$$\langle x_1,\ldots,x_r; x_1^2=\ldots=x_r^2=1\rangle$$

Let F be the free group $F=\langle x_1,\ldots,x_r\rangle$. Then

$$1\to K\to F\xrightarrow{\phi} G\to 1$$

is a short exact sequence, where K is the normal closure in F of the subgroup generated by $x_1^2,\ldots,x_r^2$, i.e.,

$$K=\{\bigcap N | N\lhd F, N\subseteq\{x_1^2,\ldots,x_r^2\}\}.$$

Let G_3 and F_3 be the third terms of the corresponding lower central series of the groups G and F. The natural homomorphism $\phi: F/K\to G$ induces the homomorphism on

$$\phi^*: F/F_3\to G/G_3,$$

$$\phi^*(xF_3)=\phi(x)G_3.$$

Notice that the kernel of ϕ^* is KF_3/F_3.

By the First Isomorphism Theorem [**5**, p. 27],

$$(F/F_3)/(KF_3/F_3)\cong G/G_3,$$

hence by the Third Isomorphism Theorem, [**5**, p. 28],

$$F/KF_3 \cong G/G_3.$$

Since K is the normal closure of the squares of the generators $x_1, x_2, \ldots, x_r$ of F, and F_3 is the normal closure in F of the basic commutators $((x_i, x_j), x_k)$, $(i > j,\ j \leq k \leq r,$ $i, j \geq 1)$ [**15**, p. 239], $G(r, 3)$ has the presentation:

$$\langle x_1, \ldots, x_r; x_1^2 = \ldots = x_r^2 = 1, ((x_i, x_j), x_k) = 1, i > j, j \leq k, 1 \leq i, j, k \leq r \rangle$$

We can realize $G(r, 3)$ concretely in the following manner. Consider the binary operation on the set $(Z_2)^r \times (Z_2)^{\binom{r}{2}}$

$$(m_1, \ldots, m_r; m_{2,1}, \ldots, m_{r,r-1}) \star (n_1, \ldots, n_r; n_{2,1}, \ldots, n_{r,r-1}) =$$

$$= (m_1 + n_1, \ldots, m_r + n_r; m_{2,1} + n_{2,1} + m_2 n_1, \ldots, m_{r,r-1} + n_{r,r-1} + m_r n_{r-1}) =$$

$$= (\ldots, m_i + n_i, \ldots; \ldots, m_{i,j} + n_{i,j} + m_j n_j, \ldots).$$

This operation is associative, and

$$1 = (0, \ldots, 0; 0, \ldots, 0)$$

serves as the identity. Furthermore,

$$(m_1, \ldots, m_r; m_{2,1} + m_2 m_1, \ldots, m_{r,r-1} + m_r m_{r-1}) = (\ldots, m_i \ldots; \ldots, m_{i,j} + m_i m_j, \ldots)$$

is the inverse of the element

$$(m_1, \ldots, m_r; m_{2,1}, \ldots, m_{r,r-1}).$$

Let $x_\nu = (0,\ldots,\underbrace{1}_{\nu},\ldots 0;0,\ldots,0)$. Then $x_v^2 = (0,\ldots 0;0,\ldots,0)$. Moreover, for $1 \leq \mu \leq \nu \leq r$, the commutator $[x_\nu, x_\mu]$ is given by

$$[x_\nu, x_\mu] = (0,\ldots,0;0,\ldots,\underbrace{1}_{(\nu,\mu)},\ldots 0).$$

Furthermore, for $0 \leq m \leq 1$, $1 \leq \nu \leq r$,

$$x_\nu^m = (0,\ldots,m,\ldots,0;0,\ldots,0)$$

and for $1 \leq \mu \leq \nu \leq r$,

$$[x_\nu, x_\mu]^m = (0,\ldots,0;0,\ldots,m,\ldots,0).$$

Thus, for $0 \leq m_j \leq 1$, $0 \leq i \leq r$, and $0 \leq m_{i,j} \leq 1$, $0 \leq j \leq i \leq r$,

$$x_1^{m_1}\ldots x_r^{m_r}[x_2,x_1]^{m_{2,1}}\ldots[x_r,x_{r-1}]^{m_{r,r-1}} = (m_1,\ldots,m_r;m_{2,1},\ldots,m_{r,r-1}).$$

Therefore, $x_1,\ldots,x_r$ generate a group of order $2^{\binom{r+1}{2}}$, and $x_i^2 = 1$, $i = 1,\ldots,r$.

It can be shown that given an arbitrary pair of elements in the group, y, z the commutator $[y,z]$ commutes with each of the generators. Thus the commutators are central, and the group is nilpotent of class 2, i.e. every commutator of dimension 3 is the identity. ∎

COROLLARY 3.4 *Every element of the group G may be uniquely written as the product of basic commutators mod G_3.*

Proof. The group G/G_3 has r generators and $r(r-1)/2$ commutators of dimension 2. Note that the commutators of dimension 3 and higher lie in G_3. The collection process is based on the simple identity:

$$xy = yx(x,y).$$

For example, for $r = 3$, the word $w = x_3x_1x_2$ is given in the following identities:

$$\begin{aligned} w &= x_3x_1x_2 = x_1x_3(x_3, x_1)x_2 = \\ &= x_1x_3(x_3, x_1)x_2 = x_1x_3x_2(x_3, x_1)((x_3, x_1)x_2) = \\ &= x_1x_2x_3(x_3, x_2)(x_3, x_1)((x_3, x_1)x_2) = \\ &= x_1x_2x_3(x_3, x_1)(x_3, x_2)((x_3, x_2)(x_3, x_1))((x_3, x_1)x_2) = \\ &= x_1x_2x_3(x_3, x_1)(x_3, x_2) \bmod G_3 \end{aligned}$$

In the group $G(r, 3)$ the order of each crucial commutator is 2. By applying the collection process an appropriate number of times to the word w, we will push the crucial commutators (of dimensions 1 and 2) to the left with indices in increasing order. The collection process results in creating commutators of dimension higher than 2, which clearly lie in G_3. In the end, the word w in G will be expressed as a product of the generators $x_1, \ldots, x_r$ and the commutators (x_m, x_n) of dimension 2 mod G_3. Since there are exactly $r(r+1)/2$ elements of G which are not in G_3, any word in G may be uniquely written as the product of basic commutators mod G_3. ∎

In light of Theorem 3.4, every word $g = e_{i_1}e_{i_2}\cdots e_{i_l}$ in crucial commutators of $G(r, 3)$ can be expressed uniquely in the form

$$g' = e_1^{\epsilon_1} \cdots e_n^{\epsilon_n} \tag{3.5}$$

which is termed the *collected form.* The *collection process* can be used to bring a given word $g \in G(r, 3)$ into collected form by replacing all "out of order" pairs:

$$e_{i_j}e_{i_k} \rightarrow e_{i_k}e_{i_j}(e_{i_j}, e_{i_k}). \tag{3.6}$$

In $G(r,3)$, each $\epsilon_i \in \{0,1\}$, since $e_i^2 = 1$. We conclude that every word g can be written as a product of distinct crucial commutators in increasing order

$$g = \prod e_{i_j},$$

where $i_j < i_k$ if $j < k$.

In our exposition we shall restrict our attention to terms of the lower central series up to G_3. Remarkably this focus allows us to develop our algorithms.

4 Collection Algorithm

In this section we view the collection process as a *rewriting system,* and present an efficient algorithm for collection in $G(3,3)$.

DEFINITION 4.1 A rewriting system is a pair (P,Σ), where Σ is an alphabet and P is a finite set of ordered pairs of words in the alphabet Σ. The elements (w,u) are referred to as *rewriting rules* or *productions* and are denoted by $w \rightarrow u$.

The collection process in $G(r,3)$ is a rewriting system where the alphabet is the set of the crucial commutators, and the productions are of the following five types:

i) $x_i^2 \rightarrow 1$, $1 \leq i \leq r$;

ii) $x_j x_i \rightarrow x_i x_j (x_j, x_i)$, $1 \leq j < i \leq r$;

iii) $(x_j, x_i)^2 \rightarrow 1$, $1 \leq j < i \leq r$;

iv) $(x_j, x_i) x_k \rightarrow x_k (x_j, x_i)$, $1 \leq j < i \leq r$, $1 \leq k \leq r$;

v) $(x_j, x_i)(x_l, x_k) \rightarrow (x_l, x_k)(x_j, x_i)$, $1 \leq j < i \leq r$, $1 \leq l < k \leq r$,

$(j > l$ or $(j = l$ and $i > k))$.

Cancellations i) and iii) follow immediately from the presentation for $G(r,3)$ given in (3.2). The other cases arise from (3.6), where the crucial commutators e_{i_j} and e_{i_k} may be either of the form x_i or (x_i, x_j). In case ii) there is no cancellation. In case iv),

$$(x_j, x_i)x_k \rightarrow x_k(x_j, x_i)((x_j, x_i), x_k) = x_k(x_j, x_i),$$

since $((x_j, x_i), x_k) \in G(r)_3$. In case v)

$$(x_j, x_i)(x_l, x_k) \rightarrow (x_l, x_k)(x_j, x_i)((x_i, x_j), (x_k, x_l)) = (x_l, x_k)(x_j, x_i),$$

since $((x_i, x_j), (x_k, x_l))$ also disappear in $G(r,3)$. Observe finally that a new commutator is added only by productions of type ii).

In Appendix A we explicitly list these rules for case $r = 3$ and illustrate their use by deriving the collected form of every element of $G(r,3)$. When $r > 3$, it becomes more efficient to search for out of order pairs by performing pairwise comparisons, rather than by explicitly listing all possible pairs that might trigger replacement. Figure 4.2 gives the algorithm that we actually programmed and used in our computational experiments. The notation employed here follows that of Donald Knuth [7].

We remark that a straightforward collection is reminiscent of *bubble sort*, in the sense that the smaller values bubble up through the sequence, moving only one position at a time. However when the left element in an out of order pair is of the form (e_p, e_q) (Step 13), we can use the more efficient insertion sort (Step 17), which adds elements to the sorted part of the sequence by taking the first item in the unsorted part and inserting it in its correct position in the sorted part (since the new commutator is of the

Input: $w = w_1 w_2 \ldots w_k$, a word in crucial commutators
Output: w, the equivalent word with the generators in order.
Working storage:
Indices i and j: to refer to the crucial commutators in w.
Boolean flag p: to ignore rewritings of type ii) during odd passes.
Boolean flag s: to indicate that a rewriting occurred during a pass.
Boolean flag r: to indicate that the pair w_i, w_{i+1} was collected.

1. $p \leftarrow$ **true.**
2. **while** $(\neg p) \vee s$**:**
3. $p \leftarrow \neg p$.
4. $i \leftarrow 0$.
5. $s \leftarrow$ **false.**
6. **while** $i <$ length(w)**:**
7. $r \leftarrow$ **false.**
8. **if** $w_i = w_{i+1}$**:** /* cancellation, type i) */
9. ⟨delete $w_i w_{i+1}$ from w⟩
10. $r \leftarrow$ **true.**
11. **else if** $w_i = w_{i+1}$**:**
12. **if** $w_i > e_r$**:** /* i.e., is of the form (e_p, e_q) */
13. $j \leftarrow 1$.
14. **while** $i + j <$ length$(w) \wedge w_i > w_{i+j}$**:**
15. ⟨increment j⟩
16. **end while.**
17. ⟨swap w_i and (w_{i+1} through w_{i+j})⟩ /* insertion sort */
18. $r \leftarrow$ **true.**
19. **else if** p**:** /* type ii) rewritings only during odd passes */
20. ⟨replace $w_i w_{i+1}$ by $w_{i+1} w_i (w_i, w_{i+1})$⟩
21. $r \leftarrow$ **true.**
22. **end if.**
23. **end if.**
24. **if** $p \vee (\neg r)$**:**
25. ⟨increment i⟩
26. **else if** $i > 0$ /* optimize for $x_m x_n x_n x_m$ */
27. ⟨decrement i⟩
28. **end if.**
29. $s \leftarrow s \vee r$.
30. **end while.**
31. **end while.**

Figure 4.2: Collection Algorithm

Number of replacements	Number of trials
0–9	22
10–19	152
20–29	546
30–39	3405
40–49	52700
50–59	364229
60–69	1018526
70–79	1629682
80–89	1849231
90–99	1681119
100–109	1307059
110–119	923258
120–129	578079
130–139	299297
140–149	165784
150–159	81895
160–169	26687
170–179	13597
180–189	3309
190–199	1159
200–209	222
210–219	42

Figure 4.3: Distribution of the number of collection steps

form $((e_p, e_q), (e_r, e_s))$ or $((e_p, e_q), e_r)$, and therefore disappears in $G(r, 3)$). It is an open problem to adapt other efficient sorting algorithms to collection.

We reach Step 19 if $w_i > w_{i+1}$ and they are both generators, so a new crucial commutator would have to be inserted in Step 20. In practice, it turns out to be more efficient to collect such pairs only on alternate passes. For example, when collecting $x_2x_1x_1$, this enhancement will prevent (x_2, x_1) from being considered and then canceled.

In Step 20 we compute (w_i, w_{i+1}) by applying Lemma 2.2.

We have run this algorithm on 10,000,000 pseudo-random words in $G(15, 3)$ (120-bit binary strings encoded with the key (5.2), as described in the next section). Figure 4.3 gives the number of trials in which the number of replacements performed in Steps 9, 17, or 20 fell into a given range.

Our computation have lead to the following

CONJECTURE 4.4 *The number of replacements needed to bring a word in n commutators into collected form is $O(n \log n)$ in the worst case, and about $O(n)$ in most cases.*

The algorithm we have detailed can be run in parallel by several processors sharing the flags s, r, and p, and the index i. It is also necessary to detect collisions between the processors when rewriting w. For example, if w contains $x_ix_ix_i$, it would be a mistake for one processor to cancel the first pair while another cancels the second pair. Hence a locking mechanism needs to be used when altering w in Steps 9, 17 and 20. No locking is needed when w is merely examined. One of the possible strategies to resolve collisions is illustrated in the following possible scenario of a collection of a word on 3 generators by 3 processors.

w

P_1	P_2	P_3
	$x_3[P_1]x_2[P_2]x_2[P_3]x_2x_1x_2x_3$	
skip x_3x_2	cancel x_2x_2	detects x_2x_2,
(because p is false)		but yields to P_2
	$x_3[P_2]x_2[P_3]x_1x_2[P_1]x_3$	
assert x_2x_3 in order,	$x_3x_2 \mapsto x_2x_3(x_3, x_2)$	detects x_2x_1,
set $p =$ true		but yields to P_2
	$x_2x_3(x_3, x_2)[P_1]x_1[P_2]x_2[P_3]x_3$	
swap (x_3, x_2) and $x_1x_2x_3$	assert x_1x_2 in order	assert x_2x_3 in order,
		set $p =$ true
	$x_2[P_1]x_3[P_3]x_1[P_2]x_2x_3(x_3, x_2)$	
assert x_2x_3 in order	assert x_1x_2 in order	$x_3x_1 \mapsto x_1x_3(x_3, x_1)$
$x_2x_1x_3(x_3, x_1)[P_1]x_2[P_2]x_3[P_3](x_3, x_2)$		
swap (x_3, x_1) and x_2x_3	assert x_2x_3 in order	assert $x_3(x_3, x_2)$ in order,
		set $p =$ false
	$x_2[P_1]x_1[P_2]x_3[P_3]x_2x_3(x_3, x_1)(x_3, x_2)$	
skip x_2x_1	assert x_1x_3 in order	skip x_3x_2
	$x_2x_1x_3x_2[P_1]x_3[P_2](x_3, x_1)[P_3](x_3, x_2)$	
assert x_2x_3 in order	assert $x_3(x_3, x_1)$ in order	assert $(x_3, x_1)(x_3, x_2)$ in order,
		set $p =$ true

$$x_2[P_1]x_1[P_2]x_3[P_3]x_2x_3(x_3,x_1)(x_3,x_2)$$

$x_2x_1 \mapsto x_1x_2(x_2,x_1)$ assert x_1x_3 in order $x_3x_2 \mapsto x_2x_3(x_3,x_2)$

$$x_1[P_3]x_2(x_2,x_1)x_2x_3(x_3,x_2)x_3[P_1](x_3,x_1)[P_2](x_3,x_2)$$

assert $x_3(x_3,x_1)$ in order | assert $(x_3,x_1)(x_3,x_2)$ in order, set p = false | assert x_1x_2 in order

$$x_1x_2[P_1](x_2,x_1)[P_2]x_2x_3[P_3](x_3,x_2)x_3(x_3,x_1)(x_3,x_2)$$

assert $x_2(x_2,x_1)$ in order | swap (x_2,x_1) and x_2x_3 | assert x_2x_3 in order

$$x_1x_2x_2x_3(x_2,x_1)(x_3,x_2)[P_1]x_3[P_2](x_3,x_1)[P_3](x_3,x_2)$$

swap (x_3,x_2) and $x_3(x_3,x_1)$ | assert $x_3(x_3,x_1)$ in order | assert $(x_3,x_1)(x_3,x_2)$ in order, set p = true

$$x_1[P_1]x_2[P_2]x_2[P_3]x_3(x_2,x_1)x_3(x_3,x_1)(x_3,x_2)(x_3,x_2)$$

assert x_1x_2 in order | cancel x_2x_2 | assert x_2x_3 in order

$$x_1x_3[P_1](x_2,x_1)[P_2]x_3[P_3](x_3,x_1)(x_3,x_2)(x_3,x_2)$$

assert $x_3(x_2,x_1)$ in order | swap (x_2,x_1) and x_3 | assert $x_3(x_3,x_1)$ in order

$$x_1[P_3]x_3x_3(x_2,x_1)(x_3,x_1)[P_1](x_3,x_2)[P_2](x_3,x_2)$$

assert $(x_3,x_1)(x_3,x_2)$ | cancel $(x_3,x_2)(x_3,x_2)$, set p = false | assert x_1x_3 in order

$$x_1x_3[P_1]x_3[P_2](x_2,x_1)[P_3](x_3,x_1)$$

cancel x_3x_3 | assert $x_3(x_2,x_1)$ in order | assert $(x_2,x_1)(x_3,x_1)$ in order, set p = true

$x_1[P_1](x_2, x_1)[P_2](x_3, x_1)$

assert $x_1(x_2, x_1)$ in order assert $(x_2, x_1)(x_3, x_1)$ in order, terminates

$x_1(x_2, x_1)(x_3, x_1)$

terminates terminates —

Formally, several processes simultaneously wish to collect intersecting subwords of w. We resolve collisions in this example by giving precedence to the processor working with leftmost choice and delaying the other collection steps until the next pass. This strategy cannot lead to a deadlock since no processor ever enters a wait state and at least one collection step is executed.

5 Collective Encryption

We will now introduce a block coding cryptosystem in which bit strings, naturally identified with elements of the previously described class of groups, are encrypted by computing their images under automorphisms. The group automorphisms will serve as our set of secret keys.

The foundation of our cryptosystem is the collection process in $G(r, 3)$. We use the group $G(3, 3)$ (which has order 64 and is analyzed in detail in Appendix A) as the running example. We also use the group $G(15, 3)$ in other computational experiments.

Given an l-bit string m and a set $P = \{p_i\}$ of words in $G(r, 3)$, we set

$$u(m, P) = p_1^{m_1} \cdots p_l^{m_l}, \tag{5.1}$$

where m_i is the ith bit of m, p_i is the ith word of P, $p_i^0 = 1$, and $p_i^1 = e_i$. In essence, we concatenate only those words in P whose indices correspond to 1's in m. Notice that u is a bijection from the set of all l-bit strings to the set of collected words in $G(k,3)$.

For example, in $G(3,3)$,

$$u(110000, E(r)) = x_1 x_2.$$

On the other hand,

$$u(110100, E(r)) = x_1 x_2 (x_2, x_1),$$

which is of course the element $x_2 x_1$ in the collected form.

We now choose an automorphism $K \in \mathrm{Aut}(G(r,n))$ that will act as the secret key. In practical implementation we may express the key by listing the images of the r generators, or, for better efficiency, by pre-computing the images of all l crucial commutators:

$$K(E(r)) = \{K(e_i)\}.$$

We will frequently use the key K defined by

$$x_i \mapsto x_1 x_{i+1 \bmod r} x_1, \tag{5.2}$$

i.e., when each generator x_1 is replaced by x_{i+1} and the result is conjugated by x_1. In our running example, $r = 3$, K is specified by

$$\begin{aligned} x_1 &\mapsto x_1 x_2 x_1; \\ x_2 &\mapsto x_1 x_3 x_1; \\ x_3 &\mapsto x_1, \end{aligned}$$

and the images of the crucial commutators are

$$P = \{x_1x_2x_1,\ x_1x_3x_1,\ x_1,\ x_1x_3x_2x_2x_2x_1,\ x_2x_1x_2x_1,\ x_3x_1x_3x_1\}.$$

A similar key on 15 generators was used in most of our computational experiments.

To encrypt a bit string m, we compute

$$u(m, K(E)) = K(e_1)_1^m \cdots K(e_l)_l^m,$$

by concatenating the pre-computed images of the crucial commutators, collecting it, and letting c be the l-bit string of the exponents of the commutators in the collected word.

To decrypt c, we likewise compute $K^{-1}(u(c, E(r))$ and collect it to recover m.

Example 1. We will decrypt and encrypt the message `Hello!` using the key (5.2).

When expressed in binary using ASCII, the message becomes

$$010010000110010101101100011011000110111100100001.$$

For each block m of $l = 6$ bits we compute $u(m, P)$. For more efficient storage and transmission we collect the encrypted strings, and express them as bit strings again. The numbers above the $=$ signs refer to the rewriting rules in Figure A.1 in Appendix A. The first block is collected as follows:

$$u(010010, P) = x_1x_3x_1x_2x_1x_2x_1 \overset{4}{=} x_1x_3x_1x_1x_2(x_2,x_1)x_2x_1 \overset{1}{=} x_1x_3x_2(x_2,x_1)x_2x_1 \overset{4}{=}$$
$$x_1x_3x_2(x_2,x_1)x_1x_2(x_2,x_1) \overset{6}{=} x_1x_2x_3(x_3,x_2)(x_2,x_1)x_1x_2(x_2,x_1) \overset{10}{=}$$
$$x_1x_2x_3(x_3,x_2)x_1(x_2,x_1)x_2(x_2,x_1) \overset{11}{=} x_1x_2x_3(x_3,x_2)x_1x_2(x_2,x_1)(x_2,x_1) \overset{7}{=}$$
$$x_1x_2x_3(x_3,x_2)x_1x_2 \overset{16}{=} x_1x_2x_3x_1(x_3,x_2)x_2 \overset{5}{=} x_1x_2x_1x_3(x_3,x_1)(x_3,x_2)x_2 \overset{4}{=}$$
$$x_1x_1x_2(x_2,x_1)x_3(x_3,x_1)(x_3,x_2)x_2 \overset{1}{=} x_2(x_2,x_1)x_3(x_3,x_1)(x_3,x_2)x_2 \overset{12}{=}$$
$$x_2x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)x_2 \overset{17}{=} x_2x_3(x_2,x_1)(x_3,x_1)x_2(x_3,x_2) \overset{14}{=}$$
$$x_2x_3(x_2,x_1)x_2(x_3,x_1)(x_3,x_2) \overset{11}{=} x_2x_3x_2(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{6}{=}$$
$$x_2x_2x_3(x_3,x_2)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{2}{=} x_3(x_3,x_2)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{20}{=}$$
$$x_3(x_2,x_1)(x_3,x_2)(x_3,x_1)(x_3,x_2) \overset{21}{=} x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)(x_3,x_2) \overset{9}{=}$$
$$x_3(x_2,x_1)(x_3,x_1) = u(001110, E(3)).$$

The collection of the rest the blocks is illustrated in Appendix B. The encrypted bit string is given by

$$001110011011010110101111101110011011100111010110.$$

To decrypt the first block, 001110, we compute the inverse

$$K^{-1}(u(001110, E(3)) = K^{-1}(x_3, (x_2, x_1), (x_3, x_1)) =$$

$$= K^{-1}(x_3x_2x_1x_2x_1x_3x_1x_3x_1) = x_3x_2x_1x_3x_1x_3x_2x_3x_2x_3x_3,$$

and collect:

$$x_3x_2x_1x_3x_1x_3x_2x_3x_2x_3x_3 \overset{3}{=} x_3x_2x_1x_3x_1x_3x_2x_3x_2 \overset{4}{=} x_3x_1x_2(x_2,x_1)x_3x_1x_3x_2x_3x_2 \overset{5}{=}$$
$$x_1x_3(x_3,x_1)x_2(x_2,x_1)x_3x_1x_3x_2x_3x_2 \overset{5}{=} x_1x_3(x_3,x_1)x_2(x_2,x_1)x_1x_3(x_3,x_1)x_3x_2x_3x_2 \overset{6}{=}$$
$$x_1x_3(x_3,x_1)x_2(x_2,x_1)x_1x_3(x_3,x_1)x_2x_3(x_3,x_2)x_3x_2 \overset{6}{=}$$
$$x_1x_3(x_3,x_1)x_2(x_2,x_1)x_1x_3(x_3,x_1)x_2x_3(x_3,x_2)x_2x_3(x_3,x_2) \overset{10}{=}$$
$$x_1x_3(x_3,x_1)x_2x_1(x_2,x_1)x_3(x_3,x_1)x_2x_3(x_3,x_2)x_2x_3(x_3,x_2) \overset{4}{=}$$
$$x_1x_3(x_3,x_1)x_1x_2(x_2,x_1)(x_2,x_1)x_3(x_3,x_1)x_2x_3(x_3,x_2)x_2x_3(x_3,x_2) \overset{7}{=}$$
$$x_1x_3(x_3,x_1)x_1x_2x_3(x_3,x_1)x_2x_3(x_3,x_2)x_2x_3(x_3,x_2) \overset{13}{=}$$
$$x_1x_3x_1(x_3,x_1)x_2x_3(x_3,x_1)x_2x_3(x_3,x_2)x_2x_3(x_3,x_2) \overset{5}{=}$$
$$x_1x_1x_3(x_3,x_1)(x_3,x_1)x_2x_3(x_3,x_1)x_2x_3(x_3,x_2)x_2x_3(x_3,x_2) \overset{1}{=}$$
$$x_3(x_3,x_1)(x_3,x_1)x_2x_3(x_3,x_1)x_2x_3(x_3,x_2)x_2x_3(x_3,x_2) \overset{8}{=}$$
$$x_3x_2x_3(x_3,x_1)x_2x_3(x_3,x_2)x_2x_3(x_3,x_2) \overset{6}{=} x_2x_3(x_3,x_2)x_3(x_3,x_1)x_2x_3(x_3,x_2)x_2x_3(x_3,x_2) \overset{14}{=}$$
$$x_2x_3(x_3,x_2)x_3x_2(x_3,x_1)x_3(x_3,x_2)x_2x_3(x_3,x_2) \overset{6}{=}$$
$$x_2x_3(x_3,x_2)x_2x_3(x_3,x_2)(x_3,x_1)x_3(x_3,x_2)x_2x_3(x_3,x_2) \overset{15}{=}$$
$$x_2x_3(x_3,x_2)x_2x_3(x_3,x_2)x_3(x_3,x_1)(x_3,x_2)x_2x_3(x_3,x_2) \overset{17}{=}$$
$$x_2x_3x_2(x_3,x_2)x_3(x_3,x_2)x_3(x_3,x_1)(x_3,x_2)x_2x_3(x_3,x_2) \overset{6}{=}$$
$$x_2x_2x_3(x_3,x_2)(x_3,x_2)x_3(x_3,x_2)x_3(x_3,x_1)(x_3,x_2)x_2x_3(x_3,x_2) \overset{2}{=}$$
$$x_3(x_3,x_2)(x_3,x_2)x_3(x_3,x_2)x_3(x_3,x_1)(x_3,x_2)x_2x_3(x_3,x_2) \overset{9}{=}$$
$$x_3x_3(x_3,x_2)x_3(x_3,x_1)(x_3,x_2)x_2x_3(x_3,x_2) \overset{3}{=} (x_3,x_2)x_3(x_3,x_1)(x_3,x_2)x_2x_3(x_3,x_2) \overset{17}{=}$$
$$(x_3,x_2)x_3(x_3,x_1)x_2(x_3,x_2)x_3(x_3,x_2) \overset{14}{=} (x_3,x_2)x_3x_2(x_3,x_1)(x_3,x_2)x_3(x_3,x_2) \overset{6}{=}$$
$$(x_3,x_2)x_2x_3(x_3,x_2)(x_3,x_1)(x_3,x_2)x_3(x_3,x_2) \overset{17}{=}$$
$$x_2(x_3,x_2)x_3(x_3,x_2)(x_3,x_1)(x_3,x_2)x_3(x_3,x_2) \overset{18}{=}$$
$$x_2x_3(x_3,x_2)(x_3,x_2)(x_3,x_1)(x_3,x_2)x_3(x_3,x_2) \overset{9}{=} x_2x_3(x_3,x_1)(x_3,x_2)x_3(x_3,x_2) \overset{18}{=}$$
$$x_2x_3(x_3,x_1)x_3(x_3,x_2)(x_3,x_2) \overset{9}{=} x_2x_3(x_3,x_1)x_3 \overset{15}{=} x_2x_3x_3(x_3,x_1) \overset{3}{=} x_2(x_3,x_1) = u(010010)$$

and 010010 is indeed the original cleartext.

Let us recall the following:

DEFINITION 5.3 ([**13**, p. 281]) Let f be a function from strings to strings. We say that f is *one-way* provided the following conditions hold:

i) f is one-to-one, and for all $x \in \sum^*, |x|^{1/k} \leq |f(x)| \leq |x|^k$ for some $k > 0$. That is, $f(x)$ is at most polynomially longer or shorter than x,

ii) f can be computed in polynomial time,

iii) f^{-1} (the inverse of f) cannot be computed in polynomial time, i.e., there is no polynomial-time algorithm which, given y, either computes an x such that $f(x) = y$ or returns "no" if such x does not exist. Remark that since f is one-to-one, x can be uniquely recovered from $f(x)$ — for example, by trying all x's of appropriate length. We are assuming that there is no polynomial time algorithm that achieves this.

Example 2. Let $r = 8$. Consider the following permutation on eight generators which represents the solution of the 8-puzzle:

ψ:

1	2	3
4		5
6	7	8

$\rightarrow$

8	3	5
1		2
7	4	6

It follows from Lemma 2.2 that the remaining 28 crucial commutators of dimension two will be mapped in the following manner:

$$\begin{aligned}
e_9 &= (x_2, x_1) \rightarrow (x_3, x_8) = (x_8, x_3) = e_{8+3+(8-1)(8-2)/2} = e_{32} \\
e_{10} &= (x_3, x_1) \rightarrow (x_5, x_8) = (x_8, x_5) = e_{34} \\
e_{11} &= (x_3, x_2) \rightarrow (x_5, x_3) = e_{14} \\
e_{12} &= (x_4, x_1) \rightarrow (x_1, x_8) = (x_8, x_1) = e_{30} \\
e_{13} &= (x_4, x_2) \rightarrow (x_1, x_3) = (x_3, x_1) = e_{10} \\
e_{14} &= (x_4, x_3) \rightarrow (x_1, x_5) = (x_5, x_1) = e_{15}
\end{aligned}$$

$$
\begin{aligned}
e_{15} &= (x_5, x_1) \to (x_2, x_8) = (x_8, x_2) = e_{31} \\
e_{16} &= (x_5, x_2) \to (x_2, x_3) = (x_3, x_2) = e_{11} \\
e_{17} &= (x_5, x_3) \to (x_2, x_5) = (x_5, x_2) = e_{16} \\
e_{18} &= (x_5, x_4) \to (x_2, x_1) = e_9 \\
e_{19} &= (x_6, x_1) \to (x_7, x_8) = (x_8, x_7) = e_{36} \\
e_{20} &= (x_6, x_2) \to (x_7, x_3) = e_{26} \\
e_{21} &= (x_6, x_3) \to (x_7, x_5) = e_{28} \\
e_{22} &= (x_6, x_4) \to (x_7, x_1) = e_{24} \\
e_{23} &= (x_6, x_5) \to (x_7, x_2) = e_{25} \\
e_{24} &= (x_7, x_1) \to (x_4, x_8) = (x_8, x_4) = e_{33} \\
e_{25} &= (x_7, x_2) \to (x_4, x_3) = e_{14} \\
e_{26} &= (x_7, x_3) \to (x_4, x_5 = (x_5, x_4) = e_{18} \\
e_{27} &= (x_7, x_4) \to (x_4, x_1) = e_{12} \\
e_{28} &= (x_7, x_5) \to (x_4, x_2) = e_{13} \\
e_{29} &= (x_7, x_6) \to (x_4, x_7) = (x_7, x_4) = e_{27} \\
e_{30} &= (x_8, x_1) \to (x_6, x_8) = (x_8, x_6) = e_{35} \\
e_{31} &= (x_8, x_2) \to (x_6, x_3) = e_{21} \\
e_{32} &= (x_8, x_3) \to (x_6, x_5) = e_{23} \\
e_{33} &= (x_8, x_4) \to (x_6, x_1) = e_{19} \\
e_{34} &= (x_8, x_5) \to (x_6, x_2) = e_{20} \\
e_{35} &= (x_8, x_6) \to (x_6, x_7) = (x_7, x_6) = e_{29} \\
e_{36} &= (x_8, x_7) \to (x_6, x_4) = e_{22}
\end{aligned}
$$

Next, we take a string of 0s and 1s, divide it into blocks of length 36, and perform the collective encryption in each block:

1. Apply the mapping u (5.1) to obtain a word W in crucial commutators.

2. Apply the permutation ψ to the commutators $e_1, \ldots, e_{36}$ to obtain $V = \phi(W)$.

3. Collect the crucial commutators mod G_3 in the word V.

4. Convert the obtained word V into a string of 36 bits by applying the map u^{-1}.

The pivotal observation is that the function on the set of words in crucial commutators obtained as the result of applying the permutation ψ on the crucial commutators followed by collection is a one-way function the sense that computing f^{-1} is hard.

Example 3. Take $n = p \cdot q$, with $p = 3$ and $q = 11$. The number of the invertible elements in Z_{33} is $(p-1)(q-1) = 20$. In fact, they are relatively prime to 33 [**12**, p. 181]. Use them to relabel the generators $x_1, x_2, \ldots, x_{20}$ of the group $G(20)$ in the following manner:

$$x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7\ x_8\ x_9\ x_{10}\ x_{11}\ x_{12}\ x_{13}\ x_{14}\ x_{15}\ x_{16}\ x_{17}\ x_{18}\ x_{19}\ x_{20}$$

$$y_1\ y_2\ y_4\ y_5\ y_7\ y_8\ y_{10}\ y_{13}\ y_{14}\ y_{16}\ y_{17}\ y_{19}\ y_{20}\ y_{23}\ y_{25}\ y_{26}\ y_{28}\ y_{29}\ y_{31}\ y_{32}$$

Next, apply the mapping:

$$y_j \to y_{\phi(j)}, \quad \phi(j) = j^3 \bmod 33, \tag{5.4}$$

to y_j, and correspondingly to $x_1, \ldots, x_{20}$:

$$x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7\ x_8\ x_9\ x_{10}\ x_{11}\ x_{12}\ x_{13}\ x_{14}\ x_{15}\ x_{16}\ x_{17}\ x_{18}\ x_{19}\ x_{20}$$

$$x_1\ x_6\ x_{19}\ x_{16}\ x_8\ x_{11}\ x_7\ x_{12}\ x_4\ x_3\ x_{18}\ x_{17}\ x_9\ x_{14}\ x_{10}\ x_{13}\ x_5\ x_2\ x_{15}\ x_{20}$$

The group $G(20)$ has 210 crucial commutators. The above mapping ϕ induces the mapping on the 190 crucial commutators of dimension two as follows:

$$e_m = (x_s, x_t) \to (x_{\phi(s)}, x_{\phi(t)}) = e_n.$$

As in the example described above, divide a string of bits into 210-bits blocks, and perform the following steps for each block:

1. Apply the mapping u(5.1) to obtain a word W in crucial commutators.
2. Apply the automorphism ϕ to the commutators $e_1, \ldots, e_{210}$ to obtain $V = \phi(W)$.
3. Collect the crucial commutators mod G_3 in the word V.
4. Convert the obtained word V into a string of 210 bits by applying the map u^{-1}.

The obtained string of bits consisting of a block of length 210 is the encrypted version of the original string.

Computing the inverse for the function (5.4) is known to be a hard problem.

6 Computational Experiments with Collective Encryption

We now consider the notion of *cascading* the proposed collective encryption with a block cipher e in hopes of introducing *confusion*, i.e., making the ciphertext appear more like a random sequence. Let us consider the situation where the cleartext is first encrypted with another block cypher e and then post-encrypted with the collective encryption using a statistically independent key. It is shown in [**11**] that the resulting cascade is no less difficult to break that the first cipher, for, even if the enemy possessed an oracle that provided the key to the collective encryption, no information about the first cipher's key has been gained.

We first consider the Data Encryption Standard (DES) in the electronic codebook mode [**12**, p. 18] as the first cipher in the cascade. We briefly recall its operation.

Data is encrypted and decrypted in 64-bit blocks, which are independent of one another (that is, we do not consider record chaining here), using a 56-bit key K. For encryption, each block is subjected to the initial permutation IP, to 16 rounds of key-dependent manipulations, and then to a final permutation IP^{-1}. During each round of key-dependent manipulations, the 64-bit input from the previous round is separated

into 32-bit halves, L and R. In all but the last round, the 32-bit result of a computation f, described below, that involves R, the key, and the iteration number, is exclusively OR-ed with L and becomes the R of the next iteration, while the unchanged R becomes its L of the next iteration. In the last round the L and R halves are used as the input to the final permutation.

To compute f, the 32-bit R is expanded into 48 bits (with duplication) and exclusively OR-ed with 48 bits selected from the 56-bit key according to the key schedule that depends on the round number. The resulting 48 bits are compressed into 32 bits using a lookup table of 8 so-called S-boxes, each of which maps 6 bits into 4 bits.

The decryption is analogous, except that IP^{-1} is applied at the beginning, IP at the end, and the 48-bit sub-keys are selected in the reverse order.

We also consider a block cipher in which a 3-byte block m is replaced by

$$c = (m + 12345)^{12345} \pmod{2^{24}}.$$

The decryption is similar, with

$$m = c * 1440005641 - 4294954951 \pmod{2^{24}}.$$

We have used four diverse files for our tests. T_1 is the text of *The Return of Sherlock Holmes* by Sir Arthur Conan Doyle (English text coded in ASCII, size 486781 bytes). T_2 is the science fiction novel *Ulitka na Sklone* by A. and B. Strugatsky (Russian text text coded in ISO 8859-5, size 404935 bytes). T_3 is a collection of assorted FORTRAN language source code in card image format (ASCII, size 893226 bytes). T_4 is the musical theme "PS/2 it" (binary WAV format, size 342048 bytes).

The following table summarizes the results of two statistical tests that we applied to the ciphertexts to compare the distribution of byte values with that of a truly random sequence. In the "Test" column, d^n refers to n iterations of DES encryption using statistically independent keys. In the $d^{n\prime}$ tests, DES decryption, rather then encryption, was applied during even iterations (2 and 4). Likewise, r refers to the finite field cipher, and g^n refers to collection post-encryption with the same key (5.2). Note that Tg^{30} is equal to the cleartext T, for 30 is the order of the automorphism.

In Maurer's universal test [**10**] we viewed the file as a sequence of bytes s_n, $n = 1, \ldots, S$, where S is the file size. We defined a_n to be the number of bytes since the last occurrence of the value s_n (or n, the number of bytes since the beginning of the steam, if this byte value had not occurred before). We computed the quantity fTU, defined as the average of $\log_2(a_n)$, compared it to the expected value of the fTU for a truly random sequence (7.1836656 for 8-bit bytes), and computed y, their difference in terms of standard deviations. From y we computed the rejection rate $\rho = \mathrm{erf}(-y/\sqrt{2})+1$. For comparison, the distance y is about 130 and $\rho = 0$ for pseudo-random number sequences based on linear congruence, while y is about .32 and ρ is about 75% for the popular R250 generator.

We also used a χ^2 test to analyze the distribution of byte values. We first counted the number Y_i of occurrences in the file of each byte value $i = 0, \ldots, 255$ and computed

$$V = \frac{256}{S}\sum_{i=0}^{255} Y_i^2.$$

For a truly random sequence, there is a 99% chance that $V < 310.57$, a 95% chance that $V < 293.16$, a 75% chance that $V < 269.88$, a 50% chance that $V < 254.33$, and a 25%

chance that $V < 239.39$. We similarly counted the numbers $y_{i,j}$ of byte value pairs i, j, computed v_i as before for each fixed i, and recorded its maximum and minimum over all i.

Test	y	ρ	V	$\min(v_i)$	$\max(v_i)$
T_1	2116.450	0	8438480.06	119736.82	1875780.00
T_1g	218.304	0	285003.25	7166.66	86158.21
T_1g^2	224.685	0	312120.66	5934.74	169531.88
T_1g^3	173.702	0	241735.43	2623.56	56638.01
T_1g^4	258.463	0	326362.12	2421.61	86446.40
T_1g^5	106.141	0	129272.24	1499.93	52939.35
T_1g^6	71.9342	0	103761.11	1141.63	68537.38
T_1g^7	133.334	0	184932.24	645.44	43060.08
T_1g^8	140.314	0	193203.70	817.95	35499.51
T_1g^9	79.704	0	108911.21	697.13	40853.45
T_1g^{10}	81.2181	0	113141.59	832.05	45835.55
T_1g^{11}	81.5389	0	110585.55	688.71	50620.07
T_1g^{12}	73.4359	0	88642.60	749.65	40158.21
T_1g^{13}	60.4164	0	79287.26	529.50	59198.35
T_1g^{14}	59.2712	0	80757.07	665.43	47418.45
T_1g^{15}	83.1390	0	134112.48	656.80	86433.21
T_1g^{16}	37.0494	0	51489.50	689.28	29737.27
T_1g^{17}	36.6014	0	54837.82	494.65	87530.41
T_1g^{18}	29.4240	0	44971.23	433.35	55186.74

T_1g^{19}	46.7616	0	61952.01	497.94	59597.00
T_1g^{20}	65.4875	0	83886.47	536.86	47685.30
T_1g^{21}	76.7598	0	105950.83	466.60	90272.44
T_1g^{22}	137.024	0	192469.45	595.27	36973.87
T_1g^{23}	99.669	0	156435.80	746.85	39619.17
T_1g^{24}	114.460	0	154466.16	996.91	61875.41
T_1g^{25}	130.062	0	185967.37	1011.76	47932.87
T_1g^{26}	213.212	0	268235.87	1487.12	86125.27
T_1g^{27}	203.858	0	275887.97	1809.51	70261.17
T_1g^{28}	243.432	0	333172.78	2461.19	75597.82
T_1g^{29}	257.572	0	350185.39	3895.26	96436.86
T_1d^1	2.26218	0.0236865	995.31	311.44	7586.27
T_1d^1g	0.319152	0.749611	288.31	197.60	340.50
T_1d^2	6.24373	0	960.84	329.84	9483.57
T_1d^2g	1.0458	0.295655	285.92	189.88	376.47
$T_1d^{2\prime}$	3.0758	0.00209937	1003.40	336.58	5149.58
$T_1d^{2\prime}g$	0.472854	0.636318	270.01	204.69	342.19
T_1d^3	1.54864	0.121468	906.27	350.45	5770.16
T_1d^3g	0.552976	0.58028	307.81	206.13	385.80
$T_1d^{3\prime}$	2.28323	0.0224168	920.15	356.93	6335.50
$T_1d^{3\prime}g$	1.61247	0.10686	274.09	206.75	366.47
T_1d^4	2.15206	0.0313928	943.47	351.77	5695.69

T_1d^4g	0.711292	0.476903	236.71	189.15	379.61
$T_1d^{4\prime}$	4.71458	0	986.49	358.19	7381.00
$T_1d^{4\prime}g$	1.28309	0.19946	302.31	214.09	390.60
T_1r	416.421	0	771161.10	8504.49	339214.93
T_1rg	11.8256	0	15779.83	644.54	5345.28
T_2	1858.4	0	5890651.05	55480.34	2123130.00
T_2g	159.004	0	198865.02	3866.61	34723.24
T_2d^1	0.0195273	0.98442	430.37	258.95	1575.92
T_2d^1g	0.782947	0.433658	303.63	206.29	330.74
T_2d^2	2.65353	0.00796557	443.77	248.67	2837.35
T_2d^2g	1.85184	0.0640492	316.29	201.16	333.51
$T_2d^{2\prime}$	2.6573	0.00787685	443.77	248.67	2837.35
$T_2d^{2\prime}g$	1.83022	0.0672175	316.10	201.16	333.51
T_2d^3	3.51854	0.000433921	376.30	241.61	1624.09
T_2d^3g	0.58153	0.560883	275.31	185.95	319.06
$T_2d^{3\prime}$	3.50509	0.000456456	376.65	241.61	1623.41
$T_2d^{3\prime}g$	0.583914	0.559278	275.38	185.95	319.06
T_2d^4	1.48502	0.137538	412.78	254.24	1589.97
T_2d^4g	1.20372	0.228697	276.49	189.41	316.94
$T_2d^{4\prime}$	1.47362	0.140585	412.59	254.24	1589.97
$T_2d^{4\prime}g$	1.24217	0.214174	275.77	189.41	316.94
T_2r	275.736	0	457666.92	6292.03	390390.60

T_2rg	6.12008	0	9194.14	392.18	4720.84
T_3	4769.09	0	118396805.65	31342.10	143025844.80
T_3g	1987.14	0	11108085.62	5302.66	8814706.88
T_3d^1	1543.19	0	8774215.71	3436.47	15740536.12
T_3d^1g	216.093	0	568605.72	501.79	1355788.32
T_3d^2	1724.32	0	11098932.79	2740.07	15781290.11
T_3d^2g	277.91	0	726153.72	530.65	1421185.91
$T_3d^{2\prime}$	1724.32	0	11098933.67	2740.07	15781290.11
$T_3d^{2\prime}g$	277.913	0	726171.03	530.65	1421185.91
T_3d^3	1542.95	0	8796455.12	1364.76	15735491.68
T_3d^3g	200.943	0	558172.58	526.12	814383.82
$T_3d^{3\prime}$	1542.95	0	8796458.96	1364.76	15735491.68
$T_3d^{3\prime}g$	200.945	0	558174.20	526.12	814383.82
T_3d^4	1531.84	0	8726673.97	2950.25	15788520.61
T_3d^4g	249.084	0	668996.44	465.40	825077.56
$T_3d^{4\prime}$	1531.84	0	8726677.14	2950.25	15788520.61
$T_3d^{4\prime}g$	249.093	0	669005.68	465.40	825077.56
T_3r	3073.09	0	37658782.80	8021.23	36866422.22
T_3rg	615.645	0	1872156.57	1561.48	2058963.25
T_4	3275.24	0	49500589.23	13281.98	62704572.32
T_4g	1603.61	0	4685207.39	3927962.20	8196260.99
T_4d^1	1613.98	0	5490149.92	7666887.57	7751573.30

T_4d^1g	330.585	0	361163.79	428693.16	486939.17
T_4d^2	1612.25	0	5483064.27	7654475.63	7759327.13
T_4d^2g	290.968	0	335749.49	429338.24	486045.93
$T_4d^{2\prime}$	1612.26	0	5483064.44	7654475.63	7759327.13
$T_4d^{2\prime}g$	290.968	0	335749.49	429338.24	486045.93
T_4d^3	1611.99	0	5482324.75	7652560.57	7752534.47
T_4d^3g	341.14	0	412359.45	428235.31	950139.58
$T_4d^{3\prime}$	1612.01	0	5482370.88	7652560.57	7752534.47
$T_4d^{3\prime}g$	341.156	0	412359.60	428235.31	950139.58
T_4d^4	1612.37	0	5486664.56	7642585.62	7750275.82
T_4d^4g	508.321	0	562313.74	425922.61	954000.02
$T_4d^{4\prime}$	1612.34	0	5486663.43	7642585.62	7750275.82
$T_4d^{4\prime}g$	508.328	0	562304.30	425922.61	954000.02
T_4r	2381.54	0	17673870.07	37413.26	15693470.48
T_4rg	641.847	0	845480.23	920841.95	1003098.51

We observe that in every case the collective post-encryption substantially enhanced the randomness of the ciphertext.

Let us make some more detailed observations about the experimental data. The time required for encryption and decryption depends largely on the number of replacements, which in turn depends on the bit patterns and the key, and cannot be predicted. In our experiments, the speed of a preliminary C language implementation varied about 5,300

bytes per second, sometimes falling as low as 2,200 bps (T_3d^4g and T_2d^3g) and even as low as 1,800 bps (T_3d^4g). For comparison, a highly optimized software implementation of DES consistently processed 12,000 bps on the same hardware. A similarly optimized collection can be expected to yield comparable performance.

7 Open Problems

Our work has been motivated by studies of the free products of finite abelian groups [2] and [3]. It might be possible to extend the cryptoscheme by using other classes of groups and even more complex group-theoretic decision problems [1].

A central question for any cryptographic system is a proper choice of keys. One problem is to verify that the key employed in (5.2) is cryptographically robust. Clearly, it is fixed point free, that is, moves all but the identify element. In future work we will try to see what fixed point free automorphisms introduce better diffusion. Our preliminary experiments with other keys found no significant difference in the statistical characteristics of the ciphertext.

The key space, the automorphism groups of $G(r, n)$, is abundantly rich, making exhaustive search infeasible. For example, $\mathrm{Aut}(G(3, 3))$ has the order $2^9 \times 6$, and very little is known about the structure or the order of the automorphism groups for arbitrarily r's. This is an open problem that merits further investigation.

As described, the cryptoscheme uses the same private key K for encryption and decryption. We hope that it may be possible to adapt the proposed scheme to some

variation of a public-key scheme, where recipient would reveal the images of the l crucial commutators under a secret automorphism k, but at the same time it would be computationally infeasible for the other parties to find their images under the inverse automorphism K^{-1}, which serves as the secret key. For example, for $r = 3$, the public key corresponding to (5.2) would be

$$P = \{x_1x_2x_1,\ x_1x_3x_1,\ x_1,\ x_1x_3x_2x_2x_2x_1,\ x_2x_1x_2x_1,\ x_3x_1x_3x_1\}.$$

Any party knowing the public key P would encrypt an l-bit message m by computing $u(m, P) = p_1^{m_1} \cdots p_l^{m_l}$, that is, concatenating the words in the public key that correspond to 1's in m, collecting the resulting word, and letting the cipher c be the exponents of the crucial commutators, just as in the secret-key scheme.

To decrypt c, the recipient needs to find the subset of P whose product is $u(c, E(r))$. The complexity of this problem in its general form is not known. It is, in fact, a variant of the knapsack problem [**12**, p. 37]. However the set P is not an arbitrary set of words, but is an isomorphic image of the crucial commutators. A recipient must know the secret automorphism K^{-1} to the word $u(c, E(r))$ and then must collect it to recover m.

We do not know whether determining a method of computing K^{-1}, given only the set of images of the generators under k, is equivalent to a known hard problem. Yet for $r = 3$, we see no immediate way to decide from merely looking at the P in the example above that $K^{-1}(g)$ can be computed by conjugating g with x_3 and replacing each generator x_i by x_{i-1}.

We see two brute force techniques to break such a public-key system.

1) Test all automorphisms in the key space, which is quite feasible when $r = 3$. Appendix A illustrates how all the elements of $G(3,3)$ can be listed. As r grows, we conjecture that it becomes entirely infeasible.

2) If K is revealed in a public-key system, apply many iterations of k to the ciphertext, so that eventually some K^n will be the identity automorphism, and the plaintext will be revealed. The key (5.2) is not secure against this attack, since its order is clearly $2r$ (for odd r). When $r = 15$, we can construct keys with somewhat larger periods. For example, by permuting the generators of $G(15,3)$

$$(x_1, x_2, x_3)(x_4, x_5, x_6, x_7, x_8)(x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}),$$

we construct a key with period $3 \times 5 \times 7 = 105$; conjugating by any x_i doubles the period to 210. It is an open problem to construct keys with much larger periods that would make this attack infeasible.

It would be interesting to factor out only n-fold commutators (that is, to work in $G(r,n)$ for $n > 3$). However, because these factor groups contain some elements with non-trivial squares, it is not clear whether every word can be rewritten into an ordered product of some crucial elements with exponents 0 or 1, as is the case in $G(r,3)$.

It would be of further interest to apply sorting algorithms that are more efficient than insertion sort, such as quick-sort or heap-sort, to the collection process.

A The analysis of the Group $G(3,3)$

We use the collection process to construct a multiplication table of $G(3,3)$ (more precisely, the table of collected forms of the products gx_i for all cosets g and generators x_i) and, from that, a Cayley graph of $G(3,3)$ with respect to the generators x_1, x_2, x_3.

As before, the numbers above the $=$ signs refer to the strings replacements in Figure A.1.

$u(000000, E(3)) \cdot x_1 = x_1 = u(100000, E(3))$

$u(000000, E(3)) \cdot x_2 = x_2 = u(010000, E(3))$

$u(000000, E(3)) \cdot x_3 = x_3 = u(001000, E(3))$

$u(000001, E(3)) \cdot x_1 = (x_3, x_2)x_1 \overset{16}{=} x_1(x_3, x_2) = u(100001, E(3))$

$u(000001, E(3)) \cdot x_2 = (x_3, x_2)x_2 \overset{17}{=} x_2(x_3, x_2) = u(010001, E(3))$

$u(000001, E(3)) \cdot x_3 = (x_3, x_2)x_3 \overset{18}{=} x_3(x_3, x_2) = u(001001, E(3))$

$u(000010, E(3)) \cdot x_1 = (x_3, x_1)x_1 \overset{13}{=} x_1(x_3, x_1) = u(100010, E(3))$

$u(000010, E(3)) \cdot x_2 = (x_3, x_1)x_2 \overset{14}{=} x_2(x_3, x_1) = u(010010, E(3))$

$u(000010, E(3)) \cdot x_3 = (x_3, x_1)x_3 \overset{15}{=} x_3(x_3, x_1) = u(001010, E(3))$

$u(000011, E(3)) \cdot x_1 = (x_3, x_1)(x_3, x_2)x_1 \overset{16}{=} (x_3, x_1)x_1(x_3, x_2) \overset{13}{=} x_1(x_3, x_1)(x_3, x_2) =$

$u(100011, E(3))$

$u(000011, E(3)) \cdot x_2 = (x_3, x_1)(x_3, x_2)x_2 \overset{17}{=} (x_3, x_1)x_2(x_3, x_2) \overset{14}{=} x_2(x_3, x_1)(x_3, x_2) =$

$u(010011, E(3))$

$u(000011, E(3)) \cdot x_3 = (x_3, x_1)(x_3, x_2)x_3 \overset{18}{=} (x_3, x_1)x_3(x_3, x_2) \overset{15}{=} x_3(x_3, x_1)(x_3, x_2) =$

$u(001011, E(3))$

$u(000100, E(3)) \cdot x_1 = (x_2, x_1)x_1 \overset{10}{=} x_1(x_2, x_1) = u(100100, E(3))$

$u(000100, E(3)) \cdot x_2 = (x_2, x_1)x_2 \overset{11}{=} x_2(x_2, x_1) = u(010100, E(3))$

$u(000100, E(3)) \cdot x_3 = (x_2, x_1)x_3 \overset{12}{=} x_3(x_2, x_1) = u(001100, E(3))$

1. $x_1^2 \to 1$
2. $x_2^2 \to 1$
3. $x_3^2 \to 1$
4. $x_2x_1 \to x_1x_2(x_2, x_1)$
5. $x_3x_1 \to x_1x_3(x_3, x_1)$
6. $x_3x_2 \to x_2x_3(x_3, x_2)$
7. $(x_2, x_1)^2 \to 1$
8. $(x_3, x_1)^2 \to 1$
9. $(x_3, x_2)^2 \to 1$
10. $(x_2, x_1)x_1 \to x_1(x_2, x_1)$
11. $(x_2, x_1)x_2 \to x_2(x_2, x_1)$
12. $(x_2, x_1)x_3 \to x_3(x_2, x_1)$
13. $(x_3, x_1)x_1 \to x_1(x_3, x_1)$
14. $(x_3, x_1)x_2 \to x_2(x_3, x_1)$
15. $(x_3, x_1)x_3 \to x_3(x_3, x_1)$
16. $(x_3, x_2)x_1 \to x_1(x_3, x_2)$
17. $(x_3, x_2)x_2 \to x_2(x_3, x_2)$
18. $(x_3, x_2)x_3 \to x_3(x_3, x_2)$
19. $(x_3, x_1)(x_2, x_1) \to (x_2, x_1)(x_3, x_1)$
20. $(x_3, x_2)(x_2, x_1) \to (x_2, x_1)(x_3, x_2)$
21. $(x_3, x_2)(x_3, x_1) \to (x_3, x_1)(x_3, x_2)$

Figure A.1: The Collection in $G(3, 3)$

$u(000101, E(3)) \cdot x_1 = (x_2, x_1)(x_3, x_2)x_1 \overset{16}{=} (x_2, x_1)x_1(x_3, x_2) \overset{10}{=} x_1(x_2, x_1)(x_3, x_2) =$

$u(100101, E(3))$

$u(000101, E(3)) \cdot x_2 = (x_2, x_1)(x_3, x_2)x_2 \overset{17}{=} (x_2, x_1)x_2(x_3, x_2) \overset{11}{=} x_2(x_2, x_1)(x_3, x_2) =$

$u(010101, E(3))$

$u(000101, E(3)) \cdot x_3 = (x_2, x_1)(x_3, x_2)x_3 \overset{18}{=} (x_2, x_1)x_3(x_3, x_2) \overset{12}{=} x_3(x_2, x_1)(x_3, x_2) =$

$u(001101, E(3))$

$u(000110, E(3)) \cdot x_1 = (x_2, x_1)(x_3, x_1)x_1 \overset{13}{=} (x_2, x_1)x_1(x_3, x_1) \overset{10}{=} x_1(x_2, x_1)(x_3, x_1) =$

$u(100110, E(3))$

$u(000110, E(3)) \cdot x_2 = (x_2, x_1)(x_3, x_1)x_2 \overset{14}{=} (x_2, x_1)x_2(x_3, x_1) \overset{11}{=} x_2(x_2, x_1)(x_3, x_1) =$

$u(010110, E(3))$

$u(000110, E(3)) \cdot x_3 = (x_2, x_1)(x_3, x_1)x_3 \overset{15}{=} (x_2, x_1)x_3(x_3, x_1) \overset{12}{=} x_3(x_2, x_1)(x_3, x_1) =$

$u(001110, E(3))$

$u(000111, E(3)) \cdot x_1 = (x_2, x_1)(x_3, x_1)(x_3, x_2)x_1 \overset{16}{=} (x_2, x_1)(x_3, x_1)x_1(x_3, x_2) \overset{13}{=}$

$(x_2, x_1)x_1(x_3, x_1)(x_3, x_2) \overset{10}{=} x_1(x_2, x_1)(x_3, x_1)(x_3, x_2) = u(100111, E(3))$

$u(000111, E(3)) \cdot x_2 = (x_2, x_1)(x_3, x_1)(x_3, x_2)x_2 \overset{17}{=} (x_2, x_1)(x_3, x_1)x_2(x_3, x_2) \overset{14}{=}$

$(x_2, x_1)x_2(x_3, x_1)(x_3, x_2) \overset{11}{=} x_2(x_2, x_1)(x_3, x_1)(x_3, x_2) = u(010111, E(3))$

$u(000111, E(3)) \cdot x_3 = (x_2, x_1)(x_3, x_1)(x_3, x_2)x_3 \overset{18}{=} (x_2, x_1)(x_3, x_1)x_3(x_3, x_2) \overset{15}{=}$

$(x_2, x_1)x_3(x_3, x_1)(x_3, x_2) \overset{12}{=} x_3(x_2, x_1)(x_3, x_1)(x_3, x_2) = u(001111, E(3))$

$u(001000, E(3)) \cdot x_1 = x_3x_1 \overset{5}{=} x_1x_3(x_3, x_1) = u(101010, E(3))$

$u(001000, E(3)) \cdot x_2 = x_3x_2 \overset{6}{=} x_2x_3(x_3, x_2) = u(011001, E(3))$

$u(001000, E(3)) \cdot x_3 = x_3x_3 \overset{3}{=} e = u(000000, E(3))$

$u(001001, E(3)) \cdot x_1 = x_3(x_3, x_2)x_1 \overset{16}{=} x_3x_1(x_3, x_2) \overset{5}{=} x_1x_3(x_3, x_1)(x_3, x_2) = u(101011, E(3))$

$u(001001, E(3)) \cdot x_2 = x_3(x_3, x_2)x_2 \overset{17}{=} x_3x_2(x_3, x_2) \overset{6}{=} x_2x_3(x_3, x_2)(x_3, x_2) \overset{9}{=} x_2x_3 =$

$u(011000, E(3))$

$u(001001, E(3)) \cdot x_3 = x_3(x_3, x_2)x_3 \overset{18}{=} x_3x_3(x_3, x_2) \overset{3}{=} (x_3, x_2) = u(000001, E(3))$

$u(001010, E(3)) \cdot x_1 = x_3(x_3, x_1)x_1 \overset{13}{=} x_3x_1(x_3, x_1) \overset{5}{=} x_1x_3(x_3, x_1)(x_3, x_1) \overset{8}{=} x_1x_3 =$

$u(101000, E(3))$

$u(001010, E(3)) \cdot x_2 = x_3(x_3, x_1)x_2 \overset{14}{=} x_3x_2(x_3, x_1) \overset{6}{=} x_2x_3(x_3, x_2)(x_3, x_1) \overset{21}{=}$

$x_2x_3(x_3, x_1)(x_3, x_2) = u(011011, E(3))$

$u(001010, E(3)) \cdot x_3 = x_3(x_3, x_1)x_3 \overset{15}{=} x_3x_3(x_3, x_1) \overset{3}{=} (x_3, x_1) = u(000010, E(3))$

$u(001011, E(3)) \cdot x_1 = x_3(x_3, x_1)(x_3, x_2)x_1 \overset{16}{=} x_3(x_3, x_1)x_1(x_3, x_2) \overset{13}{=} x_3x_1(x_3, x_1)(x_3, x_2) \overset{5}{=}$

$x_1x_3(x_3, x_1)(x_3, x_1)(x_3, x_2) \overset{8}{=} x_1x_3(x_3, x_2) = u(101001, E(3))$

$u(001011, E(3)) \cdot x_2 = x_3(x_3, x_1)(x_3, x_2)x_2 \overset{17}{=} x_3(x_3, x_1)x_2(x_3, x_2) \overset{14}{=} x_3x_2(x_3, x_1)(x_3, x_2) \overset{6}{=}$

$x_2x_3(x_3, x_2)(x_3, x_1)(x_3, x_2) \overset{21}{=} x_2x_3(x_3, x_1)(x_3, x_2)(x_3, x_2) \overset{9}{=} x_2x_3(x_3, x_1) = u(011010, E(3))$

$u(001011, E(3)) \cdot x_3 = x_3(x_3, x_1)(x_3, x_2)x_3 \overset{18}{=} x_3(x_3, x_1)x_3(x_3, x_2) \overset{15}{=} x_3x_3(x_3, x_1)(x_3, x_2) \overset{3}{=}$

$(x_3, x_1)(x_3, x_2) = u(000011, E(3))$

$u(001100, E(3)) \cdot x_1 = x_3(x_2, x_1)x_1 \overset{10}{=} x_3x_1(x_2, x_1) \overset{5}{=} x_1x_3(x_3, x_1)(x_2, x_1) \overset{19}{=}$

$x_1x_3(x_2, x_1)(x_3, x_1) = u(101110, E(3))$

$u(001100, E(3)) \cdot x_2 = x_3(x_2, x_1)x_2 \overset{11}{=} x_3x_2(x_2, x_1) \overset{6}{=} x_2x_3(x_3, x_2)(x_2, x_1) \overset{20}{=}$

$x_2x_3(x_2, x_1)(x_3, x_2) = u(011101, E(3))$

$u(001100, E(3)) \cdot x_3 = x_3(x_2, x_1)x_3 \overset{12}{=} x_3x_3(x_2, x_1) \overset{3}{=} (x_2, x_1) = u(000100, E(3))$

$u(001101, E(3)) \cdot x_1 = x_3(x_2, x_1)(x_3, x_2)x_1 \overset{16}{=} x_3(x_2, x_1)x_1(x_3, x_2) \overset{10}{=} x_3x_1(x_2, x_1)(x_3, x_2) \overset{5}{=}$

$x_1x_3(x_3, x_1)(x_2, x_1)(x_3, x_2) \overset{19}{=} x_1x_3(x_2, x_1)(x_3, x_1)(x_3, x_2) = u(101111, E(3))$

$u(001101, E(3)) \cdot x_2 = x_3(x_2, x_1)(x_3, x_2)x_2 \overset{17}{=} x_3(x_2, x_1)x_2(x_3, x_2) \overset{11}{=} x_3x_2(x_2, x_1)(x_3, x_2) \overset{6}{=}$

$x_2x_3(x_3, x_2)(x_2, x_1)(x_3, x_2) \overset{20}{=} x_2x_3(x_2, x_1)(x_3, x_2)(x_3, x_2) \overset{9}{=} x_2x_3(x_2, x_1) = u(011100, E(3))$

$u(001101, E(3)) \cdot x_3 = x_3(x_2, x_1)(x_3, x_2)x_3 \overset{18}{=} x_3(x_2, x_1)x_3(x_3, x_2) \overset{12}{=} x_3x_3(x_2, x_1)(x_3, x_2) \overset{3}{=}$

$(x_2, x_1)(x_3, x_2) = u(000101, E(3))$

$u(001110, E(3)) \cdot x_1 = x_3(x_2, x_1)(x_3, x_1)x_1 \overset{13}{=} x_3(x_2, x_1)x_1(x_3, x_1) \overset{10}{=} x_3x_1(x_2, x_1)(x_3, x_1) \overset{5}{=}$

$x_1x_3(x_3, x_1)(x_2, x_1)(x_3, x_1) \overset{19}{=} x_1x_3(x_2, x_1)(x_3, x_1)(x_3, x_1) \overset{8}{=} x_1x_3(x_2, x_1) = u(101100, E(3))$

$u(001110, E(3)) \cdot x_2 = x_3(x_2, x_1)(x_3, x_1)x_2 \overset{14}{=} x_3(x_2, x_1)x_2(x_3, x_1) \overset{11}{=} x_3x_2(x_2, x_1)(x_3, x_1) \overset{6}{=}$

$x_2x_3(x_3,x_2)(x_2,x_1)(x_3,x_1) \overset{\mathbf{20}}{=} x_2x_3(x_2,x_1)(x_3,x_2)(x_3,x_1) \overset{\mathbf{21}}{=} x_2x_3(x_2,x_1)(x_3,x_1)(x_3,x_2) =$

$u(011111, E(3))$

$u(001110, E(3)) \cdot x_3 = x_3(x_2,x_1)(x_3,x_1)x_3 \overset{\mathbf{15}}{=} x_3(x_2,x_1)x_3(x_3,x_1) \overset{\mathbf{12}}{=} x_3x_3(x_2,x_1)(x_3,x_1) \overset{\mathbf{3}}{=}$

$(x_2,x_1)(x_3,x_1) = u(000110, E(3))$

$u(001111, E(3)) \cdot x_1 = x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)x_1 \overset{\mathbf{16}}{=} x_3(x_2,x_1)(x_3,x_1)x_1(x_3,x_2) \overset{\mathbf{13}}{=}$

$x_3(x_2,x_1)x_1(x_3,x_1)(x_3,x_2) \overset{\mathbf{10}}{=} x_3x_1(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{\mathbf{5}}{=}$

$x_1x_3(x_3,x_1)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{\mathbf{19}}{=} x_1x_3(x_2,x_1)(x_3,x_1)(x_3,x_1)(x_3,x_2) \overset{\mathbf{8}}{=}$

$x_1x_3(x_2,x_1)(x_3,x_2) = u(101101, E(3))$

$u(001111, E(3)) \cdot x_2 = x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)x_2 \overset{\mathbf{17}}{=} x_3(x_2,x_1)(x_3,x_1)x_2(x_3,x_2) \overset{\mathbf{14}}{=}$

$x_3(x_2,x_1)x_2(x_3,x_1)(x_3,x_2) \overset{\mathbf{11}}{=} x_3x_2(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{\mathbf{6}}{=}$

$x_2x_3(x_3,x_2)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{\mathbf{20}}{=} x_2x_3(x_2,x_1)(x_3,x_2)(x_3,x_1)(x_3,x_2) \overset{\mathbf{21}}{=}$

$x_2x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)(x_3,x_2) \overset{\mathbf{9}}{=} x_2x_3(x_2,x_1)(x_3,x_1) = u(011110, E(3))$

$u(001111, E(3)) \cdot x_3 = x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)x_3 \overset{\mathbf{18}}{=} x_3(x_2,x_1)(x_3,x_1)x_3(x_3,x_2) \overset{\mathbf{15}}{=}$

$x_3(x_2,x_1)x_3(x_3,x_1)(x_3,x_2) \overset{\mathbf{12}}{=} x_3x_3(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{\mathbf{3}}{=} (x_2,x_1)(x_3,x_1)(x_3,x_2) =$

$u(000111, E(3))$

$u(010000, E(3)) \cdot x_1 = x_2x_1 \overset{\mathbf{4}}{=} x_1x_2(x_2,x_1) = u(110100, E(3))$

$u(010000, E(3)) \cdot x_2 = x_2x_2 \overset{\mathbf{2}}{=} e = u(000000, E(3))$

$u(010000, E(3)) \cdot x_3 = x_2x_3 = u(011000, E(3))$

$u(010001, E(3)) \cdot x_1 = x_2(x_3,x_2)x_1 \overset{\mathbf{16}}{=} x_2x_1(x_3,x_2) \overset{\mathbf{4}}{=} x_1x_2(x_2,x_1)(x_3,x_2) = u(110101, E(3))$

$u(010001, E(3)) \cdot x_2 = x_2(x_3,x_2)x_2 \overset{\mathbf{17}}{=} x_2x_2(x_3,x_2) \overset{\mathbf{2}}{=} (x_3,x_2) = u(000001, E(3))$

$u(010001, E(3)) \cdot x_3 = x_2(x_3,x_2)x_3 \overset{\mathbf{18}}{=} x_2x_3(x_3,x_2) = u(011001, E(3))$

$u(010010, E(3)) \cdot x_1 = x_2(x_3,x_1)x_1 \overset{\mathbf{13}}{=} x_2x_1(x_3,x_1) \overset{\mathbf{4}}{=} x_1x_2(x_2,x_1)(x_3,x_1) = u(110110, E(3))$

$u(010010, E(3)) \cdot x_2 = x_2(x_3,x_1)x_2 \overset{\mathbf{14}}{=} x_2x_2(x_3,x_1) \overset{\mathbf{2}}{=} (x_3,x_1) = u(000010, E(3))$

$u(010010, E(3)) \cdot x_3 = x_2(x_3,x_1)x_3 \overset{\mathbf{15}}{=} x_2x_3(x_3,x_1) = u(011010, E(3))$

$u(010011, E(3)) \cdot x_1 = x_2(x_3,x_1)(x_3,x_2)x_1 \overset{\mathbf{16}}{=} x_2(x_3,x_1)x_1(x_3,x_2) \overset{\mathbf{13}}{=} x_2x_1(x_3,x_1)(x_3,x_2) \overset{\mathbf{4}}{=}$

$x_1x_2(x_2,x_1)(x_3,x_1)(x_3,x_2) = u(110111, E(3))$

$u(010011, E(3)) \cdot x_2 = x_2(x_3,x_1)(x_3,x_2)x_2 \overset{17}{=} x_2(x_3,x_1)x_2(x_3,x_2) \overset{14}{=} x_2x_2(x_3,x_1)(x_3,x_2) \overset{2}{=}$

$(x_3,x_1)(x_3,x_2) = u(000011, E(3))$

$u(010011, E(3)) \cdot x_3 = x_2(x_3,x_1)(x_3,x_2)x_3 \overset{18}{=} x_2(x_3,x_1)x_3(x_3,x_2) \overset{15}{=} x_2x_3(x_3,x_1)(x_3,x_2) =$

$u(011011, E(3))$

$u(010100, E(3)) \cdot x_1 = x_2(x_2,x_1)x_1 \overset{10}{=} x_2x_1(x_2,x_1) \overset{4}{=} x_1x_2(x_2,x_1)(x_2,x_1) \overset{7}{=} x_1x_2 =$

$u(110000, E(3))$

$u(010100, E(3)) \cdot x_2 = x_2(x_2,x_1)x_2 \overset{11}{=} x_2x_2(x_2,x_1) \overset{2}{=} (x_2,x_1) = u(000100, E(3))$

$u(010100, E(3)) \cdot x_3 = x_2(x_2,x_1)x_3 \overset{12}{=} x_2x_3(x_2,x_1) = u(011100, E(3))$

$u(010101, E(3)) \cdot x_1 = x_2(x_2,x_1)(x_3,x_2)x_1 \overset{16}{=} x_2(x_2,x_1)x_1(x_3,x_2) \overset{10}{=} x_2x_1(x_2,x_1)(x_3,x_2) \overset{4}{=}$

$x_1x_2(x_2,x_1)(x_2,x_1)(x_3,x_2) \overset{7}{=} x_1x_2(x_3,x_2) = u(110001, E(3))$

$u(010101, E(3)) \cdot x_2 = x_2(x_2,x_1)(x_3,x_2)x_2 \overset{17}{=} x_2(x_2,x_1)x_2(x_3,x_2) \overset{11}{=} x_2x_2(x_2,x_1)(x_3,x_2) \overset{2}{=}$

$(x_2,x_1)(x_3,x_2) = u(000101, E(3))$

$u(010101, E(3)) \cdot x_3 = x_2(x_2,x_1)(x_3,x_2)x_3 \overset{18}{=} x_2(x_2,x_1)x_3(x_3,x_2) \overset{12}{=} x_2x_3(x_2,x_1)(x_3,x_2) =$

$u(011101, E(3))$

$u(010110, E(3)) \cdot x_1 = x_2(x_2,x_1)(x_3,x_1)x_1 \overset{13}{=} x_2(x_2,x_1)x_1(x_3,x_1) \overset{10}{=} x_2x_1(x_2,x_1)(x_3,x_1) \overset{4}{=}$

$x_1x_2(x_2,x_1)(x_2,x_1)(x_3,x_1) \overset{7}{=} x_1x_2(x_3,x_1) = u(110010, E(3))$

$u(010110, E(3)) \cdot x_2 = x_2(x_2,x_1)(x_3,x_1)x_2 \overset{14}{=} x_2(x_2,x_1)x_2(x_3,x_1) \overset{11}{=} x_2x_2(x_2,x_1)(x_3,x_1) \overset{2}{=}$

$(x_2,x_1)(x_3,x_1) = u(000110, E(3))$

$u(010110, E(3)) \cdot x_3 = x_2(x_2,x_1)(x_3,x_1)x_3 \overset{15}{=} x_2(x_2,x_1)x_3(x_3,x_1) \overset{12}{=} x_2x_3(x_2,x_1)(x_3,x_1) =$

$u(011110, E(3))$

$u(010111, E(3)) \cdot x_1 = x_2(x_2,x_1)(x_3,x_1)(x_3,x_2)x_1 \overset{16}{=} x_2(x_2,x_1)(x_3,x_1)x_1(x_3,x_2) \overset{13}{=}$

$x_2(x_2,x_1)x_1(x_3,x_1)(x_3,x_2) \overset{10}{=} x_2x_1(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{4}{=}$

$x_1x_2(x_2,x_1)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{7}{=} x_1x_2(x_3,x_1)(x_3,x_2) = u(110011, E(3))$

$u(010111, E(3)) \cdot x_2 = x_2(x_2,x_1)(x_3,x_1)(x_3,x_2)x_2 \overset{17}{=} x_2(x_2,x_1)(x_3,x_1)x_2(x_3,x_2) \overset{14}{=}$

$x_2(x_2,x_1)x_2(x_3,x_1)(x_3,x_2) \overset{11}{=} x_2x_2(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{2}{=} (x_2,x_1)(x_3,x_1)(x_3,x_2) =$

$u(000111, E(3))$

$u(010111, E(3)) \cdot x_3 = x_2(x_2,x_1)(x_3,x_1)(x_3,x_2)x_3 \overset{18}{=} x_2(x_2,x_1)(x_3,x_1)x_3(x_3,x_2) \overset{15}{=}$

$x_2(x_2,x_1)x_3(x_3,x_1)(x_3,x_2) \overset{12}{=} x_2x_3(x_2,x_1)(x_3,x_1)(x_3,x_2) = u(011111, E(3))$

$u(011000, E(3)) \cdot x_1 = x_2x_3x_1 \overset{5}{=} x_2x_1x_3(x_3,x_1) \overset{4}{=} x_1x_2(x_2,x_1)x_3(x_3,x_1) \overset{12}{=}$

$x_1x_2x_3(x_2,x_1)(x_3,x_1) = u(111110, E(3))$

$u(011000, E(3)) \cdot x_2 = x_2x_3x_2 \overset{6}{=} x_2x_2x_3(x_3,x_2) \overset{2}{=} x_3(x_3,x_2) = u(001001, E(3))$

$u(011000, E(3)) \cdot x_3 = x_2x_3x_3 \overset{3}{=} x_2 = u(010000, E(3))$

$u(011001, E(3)) \cdot x_1 = x_2x_3(x_3,x_2)x_1 \overset{16}{=} x_2x_3x_1(x_3,x_2) \overset{5}{=} x_2x_1x_3(x_3,x_1)(x_3,x_2) \overset{4}{=}$

$x_1x_2(x_2,x_1)x_3(x_3,x_1)(x_3,x_2) \overset{12}{=} x_1x_2x_3(x_2,x_1)(x_3,x_1)(x_3,x_2) = u(111111, E(3))$

$u(011001, E(3)) \cdot x_2 = x_2x_3(x_3,x_2)x_2 \overset{17}{=} x_2x_3x_2(x_3,x_2) \overset{6}{=} x_2x_2x_3(x_3,x_2)(x_3,x_2) \overset{2}{=}$

$x_3(x_3,x_2)(x_3,x_2) \overset{9}{=} x_3 = u(001000, E(3))$

$u(011001, E(3)) \cdot x_3 = x_2x_3(x_3,x_2)x_3 \overset{18}{=} x_2x_3x_3(x_3,x_2) \overset{3}{=} x_2(x_3,x_2) = u(010001, E(3))$

$u(011010, E(3)) \cdot x_1 = x_2x_3(x_3,x_1)x_1 \overset{13}{=} x_2x_3x_1(x_3,x_1) \overset{5}{=} x_2x_1x_3(x_3,x_1)(x_3,x_1) \overset{4}{=}$

$x_1x_2(x_2,x_1)x_3(x_3,x_1)(x_3,x_1) \overset{8}{=} x_1x_2(x_2,x_1)x_3 \overset{12}{=} x_1x_2x_3(x_2,x_1) = u(111100, E(3))$

$u(011010, E(3)) \cdot x_2 = x_2x_3(x_3,x_1)x_2 \overset{14}{=} x_2x_3x_2(x_3,x_1) \overset{6}{=} x_2x_2x_3(x_3,x_2)(x_3,x_1) \overset{2}{=}$

$x_3(x_3,x_2)(x_3,x_1) \overset{21}{=} x_3(x_3,x_1)(x_3,x_2) = u(001011, E(3))$

$u(011010, E(3)) \cdot x_3 = x_2x_3(x_3,x_1)x_3 \overset{15}{=} x_2x_3x_3(x_3,x_1) \overset{3}{=} x_2(x_3,x_1) = u(010010, E(3))$

$u(011011, E(3)) \cdot x_1 = x_2x_3(x_3,x_1)(x_3,x_2)x_1 \overset{16}{=} x_2x_3(x_3,x_1)x_1(x_3,x_2) \overset{13}{=}$

$x_2x_3x_1(x_3,x_1)(x_3,x_2) \overset{5}{=} x_2x_1x_3(x_3,x_1)(x_3,x_1)(x_3,x_2) \overset{4}{=}$

$x_1x_2(x_2,x_1)x_3(x_3,x_1)(x_3,x_1)(x_3,x_2) \overset{8}{=} x_1x_2(x_2,x_1)x_3(x_3,x_2) \overset{12}{=} x_1x_2x_3(x_2,x_1)(x_3,x_2) =$

$u(111101, E(3))$

$u(011011, E(3)) \cdot x_2 = x_2x_3(x_3,x_1)(x_3,x_2)x_2 \overset{17}{=} x_2x_3(x_3,x_1)x_2(x_3,x_2) \overset{14}{=}$

$x_2x_3x_2(x_3,x_1)(x_3,x_2) \overset{6}{=} x_2x_2x_3(x_3,x_2)(x_3,x_1)(x_3,x_2) \overset{2}{=} x_3(x_3,x_2)(x_3,x_1)(x_3,x_2) \overset{21}{=}$

$x_3(x_3,x_1)(x_3,x_2)(x_3,x_2) \overset{9}{=} x_3(x_3,x_1) = u(001010, E(3))$

$u(011011, E(3)) \cdot x_3 = x_2x_3(x_3, x_1)(x_3, x_2)x_3 \overset{18}{=} x_2x_3(x_3, x_1)x_3(x_3, x_2) \overset{15}{=}$

$x_2x_3x_3(x_3, x_1)(x_3, x_2) \overset{3}{=} x_2(x_3, x_1)(x_3, x_2) = u(010011, E(3))$

$u(011100, E(3)) \cdot x_1 = x_2x_3(x_2, x_1)x_1 \overset{10}{=} x_2x_3x_1(x_2, x_1) \overset{5}{=} x_2x_1x_3(x_3, x_1)(x_2, x_1) \overset{4}{=}$

$x_1x_2(x_2, x_1)x_3(x_3, x_1)(x_2, x_1) \overset{12}{=} x_1x_2x_3(x_2, x_1)(x_3, x_1)(x_2, x_1) \overset{19}{=}$

$x_1x_2x_3(x_2, x_1)(x_2, x_1)(x_3, x_1) \overset{7}{=} x_1x_2x_3(x_3, x_1) = u(111010, E(3))$

$u(011100, E(3)) \cdot x_2 = x_2x_3(x_2, x_1)x_2 \overset{11}{=} x_2x_3x_2(x_2, x_1) \overset{6}{=} x_2x_2x_3(x_3, x_2)(x_2, x_1) \overset{2}{=}$

$x_3(x_3, x_2)(x_2, x_1) \overset{20}{=} x_3(x_2, x_1)(x_3, x_2) = u(001101, E(3))$

$u(011100, E(3)) \cdot x_3 = x_2x_3(x_2, x_1)x_3 \overset{12}{=} x_2x_3x_3(x_2, x_1) \overset{3}{=} x_2(x_2, x_1) = u(010100, E(3))$

$u(011101, E(3)) \cdot x_1 = x_2x_3(x_2, x_1)(x_3, x_2)x_1 \overset{16}{=} x_2x_3(x_2, x_1)x_1(x_3, x_2) \overset{10}{=}$

$x_2x_3x_1(x_2, x_1)(x_3, x_2) \overset{5}{=} x_2x_1x_3(x_3, x_1)(x_2, x_1)(x_3, x_2) \overset{4}{=}$

$x_1x_2(x_2, x_1)x_3(x_3, x_1)(x_2, x_1)(x_3, x_2) \overset{12}{=} x_1x_2x_3(x_2, x_1)(x_3, x_1)(x_2, x_1)(x_3, x_2) \overset{19}{=}$

$x_1x_2x_3(x_2, x_1)(x_2, x_1)(x_3, x_1)(x_3, x_2) \overset{7}{=} x_1x_2x_3(x_3, x_1)(x_3, x_2) = u(111011, E(3))$

$u(011101, E(3)) \cdot x_2 = x_2x_3(x_2, x_1)(x_3, x_2)x_2 \overset{17}{=} x_2x_3(x_2, x_1)x_2(x_3, x_2) \overset{11}{=}$

$x_2x_3x_2(x_2, x_1)(x_3, x_2) \overset{6}{=} x_2x_2x_3(x_3, x_2)(x_2, x_1)(x_3, x_2) \overset{2}{=} x_3(x_3, x_2)(x_2, x_1)(x_3, x_2) \overset{20}{=}$

$x_3(x_2, x_1)(x_3, x_2)(x_3, x_2) \overset{9}{=} x_3(x_2, x_1) = u(001100, E(3))$

$u(011101, E(3)) \cdot x_3 = x_2x_3(x_2, x_1)(x_3, x_2)x_3 \overset{18}{=} x_2x_3(x_2, x_1)x_3(x_3, x_2) \overset{12}{=}$

$x_2x_3x_3(x_2, x_1)(x_3, x_2) \overset{3}{=} x_2(x_2, x_1)(x_3, x_2) = u(010101, E(3))$

$u(011110, E(3)) \cdot x_1 = x_2x_3(x_2, x_1)(x_3, x_1)x_1 \overset{13}{=} x_2x_3(x_2, x_1)x_1(x_3, x_1) \overset{10}{=}$

$x_2x_3x_1(x_2, x_1)(x_3, x_1) \overset{5}{=} x_2x_1x_3(x_3, x_1)(x_2, x_1)(x_3, x_1) \overset{4}{=}$

$x_1x_2(x_2, x_1)x_3(x_3, x_1)(x_2, x_1)(x_3, x_1) \overset{12}{=} x_1x_2x_3(x_2, x_1)(x_3, x_1)(x_2, x_1)(x_3, x_1) \overset{19}{=}$

$x_1x_2x_3(x_2, x_1)(x_2, x_1)(x_3, x_1)(x_3, x_1) \overset{7}{=} x_1x_2x_3(x_3, x_1)(x_3, x_1) \overset{8}{=} x_1x_2x_3 = u(111000, E(3))$

$u(011110, E(3)) \cdot x_2 = x_2x_3(x_2, x_1)(x_3, x_1)x_2 \overset{14}{=} x_2x_3(x_2, x_1)x_2(x_3, x_1) \overset{11}{=}$

$x_2x_3x_2(x_2, x_1)(x_3, x_1) \overset{6}{=} x_2x_2x_3(x_3, x_2)(x_2, x_1)(x_3, x_1) \overset{2}{=} x_3(x_3, x_2)(x_2, x_1)(x_3, x_1) \overset{20}{=}$

$x_3(x_2, x_1)(x_3, x_2)(x_3, x_1) \overset{21}{=} x_3(x_2, x_1)(x_3, x_1)(x_3, x_2) = u(001111, E(3))$

$u(011110, E(3)) \cdot x_3 = x_2x_3(x_2, x_1)(x_3, x_1)x_3 \overset{15}{=} x_2x_3(x_2, x_1)x_3(x_3, x_1) \overset{12}{=}$

$x_2x_3x_3(x_2,x_1)(x_3,x_1) \overset{3}{=} x_2(x_2,x_1)(x_3,x_1) = u(010110, E(3))$

$u(011111, E(3)) \cdot x_1 = x_2x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)x_1 \overset{16}{=} x_2x_3(x_2,x_1)(x_3,x_1)x_1(x_3,x_2) \overset{13}{=}$

$x_2x_3(x_2,x_1)x_1(x_3,x_1)(x_3,x_2) \overset{10}{=} x_2x_3x_1(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{5}{=}$

$x_2x_1x_3(x_3,x_1)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{4}{=} x_1x_2(x_2,x_1)x_3(x_3,x_1)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{12}{=}$

$x_1x_2x_3(x_2,x_1)(x_3,x_1)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{19}{=}$

$x_1x_2x_3(x_2,x_1)(x_2,x_1)(x_3,x_1)(x_3,x_1)(x_3,x_2) \overset{7}{=} x_1x_2x_3(x_3,x_1)(x_3,x_1)(x_3,x_2) \overset{8}{=}$

$x_1x_2x_3(x_3,x_2) = u(111001, E(3))$

$u(011111, E(3)) \cdot x_2 = x_2x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)x_2 \overset{17}{=} x_2x_3(x_2,x_1)(x_3,x_1)x_2(x_3,x_2) \overset{14}{=}$

$x_2x_3(x_2,x_1)x_2(x_3,x_1)(x_3,x_2) \overset{11}{=} x_2x_3x_2(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{6}{=}$

$x_2x_2x_3(x_3,x_2)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{2}{=} x_3(x_3,x_2)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{20}{=}$

$x_3(x_2,x_1)(x_3,x_2)(x_3,x_1)(x_3,x_2) \overset{21}{=} x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)(x_3,x_2) \overset{9}{=} x_3(x_2,x_1)(x_3,x_1) =$

$u(001110, E(3))$

$u(011111, E(3)) \cdot x_3 = x_2x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)x_3 \overset{18}{=} x_2x_3(x_2,x_1)(x_3,x_1)x_3(x_3,x_2) \overset{15}{=}$

$x_2x_3(x_2,x_1)x_3(x_3,x_1)(x_3,x_2) \overset{12}{=} x_2x_3x_3(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{3}{=} x_2(x_2,x_1)(x_3,x_1)(x_3,x_2) =$

$u(010111, E(3))$

$u(100000, E(3)) \cdot x_1 = x_1x_1 \overset{1}{=} e = u(000000, E(3))$

$u(100000, E(3)) \cdot x_2 = x_1x_2 = u(110000, E(3))$

$u(100000, E(3)) \cdot x_3 = x_1x_3 = u(101000, E(3))$

$u(100001, E(3)) \cdot x_1 = x_1(x_3,x_2)x_1 \overset{16}{=} x_1x_1(x_3,x_2) \overset{1}{=} (x_3,x_2) = u(000001, E(3))$

$u(100001, E(3)) \cdot x_2 = x_1(x_3,x_2)x_2 \overset{17}{=} x_1x_2(x_3,x_2) = u(110001, E(3))$

$u(100001, E(3)) \cdot x_3 = x_1(x_3,x_2)x_3 \overset{18}{=} x_1x_3(x_3,x_2) = u(101001, E(3))$

$u(100010, E(3)) \cdot x_1 = x_1(x_3,x_1)x_1 \overset{13}{=} x_1x_1(x_3,x_1) \overset{1}{=} (x_3,x_1) = u(000010, E(3))$

$u(100010, E(3)) \cdot x_2 = x_1(x_3,x_1)x_2 \overset{14}{=} x_1x_2(x_3,x_1) = u(110010, E(3))$

$u(100010, E(3)) \cdot x_3 = x_1(x_3,x_1)x_3 \overset{15}{=} x_1x_3(x_3,x_1) = u(101010, E(3))$

$u(100011, E(3)) \cdot x_1 = x_1(x_3,x_1)(x_3,x_2)x_1 \overset{16}{=} x_1(x_3,x_1)x_1(x_3,x_2) \overset{13}{=} x_1x_1(x_3,x_1)(x_3,x_2) \overset{1}{=}$

$(x_3, x_1)(x_3, x_2) = u(000011, E(3))$

$u(100011, E(3)) \cdot x_2 = x_1(x_3, x_1)(x_3, x_2)x_2 \overset{17}{=} x_1(x_3, x_1)x_2(x_3, x_2) \overset{14}{=} x_1x_2(x_3, x_1)(x_3, x_2) =$

$u(110011, E(3))$

$u(100011, E(3)) \cdot x_3 = x_1(x_3, x_1)(x_3, x_2)x_3 \overset{18}{=} x_1(x_3, x_1)x_3(x_3, x_2) \overset{15}{=} x_1x_3(x_3, x_1)(x_3, x_2) =$

$u(101011, E(3))$

$u(100100, E(3)) \cdot x_1 = x_1(x_2, x_1)x_1 \overset{10}{=} x_1x_1(x_2, x_1) \overset{1}{=} (x_2, x_1) = u(000100, E(3))$

$u(100100, E(3)) \cdot x_2 = x_1(x_2, x_1)x_2 \overset{11}{=} x_1x_2(x_2, x_1) = u(110100, E(3))$

$u(100100, E(3)) \cdot x_3 = x_1(x_2, x_1)x_3 \overset{12}{=} x_1x_3(x_2, x_1) = u(101100, E(3))$

$u(100101, E(3)) \cdot x_1 = x_1(x_2, x_1)(x_3, x_2)x_1 \overset{16}{=} x_1(x_2, x_1)x_1(x_3, x_2) \overset{10}{=} x_1x_1(x_2, x_1)(x_3, x_2) \overset{1}{=}$

$(x_2, x_1)(x_3, x_2) = u(000101, E(3))$

$u(100101, E(3)) \cdot x_2 = x_1(x_2, x_1)(x_3, x_2)x_2 \overset{17}{=} x_1(x_2, x_1)x_2(x_3, x_2) \overset{11}{=} x_1x_2(x_2, x_1)(x_3, x_2) =$

$u(110101, E(3))$

$u(100101, E(3)) \cdot x_3 = x_1(x_2, x_1)(x_3, x_2)x_3 \overset{18}{=} x_1(x_2, x_1)x_3(x_3, x_2) \overset{12}{=} x_1x_3(x_2, x_1)(x_3, x_2) =$

$u(101101, E(3))$

$u(100110, E(3)) \cdot x_1 = x_1(x_2, x_1)(x_3, x_1)x_1 \overset{13}{=} x_1(x_2, x_1)x_1(x_3, x_1) \overset{10}{=} x_1x_1(x_2, x_1)(x_3, x_1) \overset{1}{=}$

$(x_2, x_1)(x_3, x_1) = u(000110, E(3))$

$u(100110, E(3)) \cdot x_2 = x_1(x_2, x_1)(x_3, x_1)x_2 \overset{14}{=} x_1(x_2, x_1)x_2(x_3, x_1) \overset{11}{=} x_1x_2(x_2, x_1)(x_3, x_1) =$

$u(110110, E(3))$

$u(100110, E(3)) \cdot x_3 = x_1(x_2, x_1)(x_3, x_1)x_3 \overset{15}{=} x_1(x_2, x_1)x_3(x_3, x_1) \overset{12}{=} x_1x_3(x_2, x_1)(x_3, x_1) =$

$u(101110, E(3))$

$u(100111, E(3)) \cdot x_1 = x_1(x_2, x_1)(x_3, x_1)(x_3, x_2)x_1 \overset{16}{=} x_1(x_2, x_1)(x_3, x_1)x_1(x_3, x_2) \overset{13}{=}$

$x_1(x_2, x_1)x_1(x_3, x_1)(x_3, x_2) \overset{10}{=} x_1x_1(x_2, x_1)(x_3, x_1)(x_3, x_2) \overset{1}{=} (x_2, x_1)(x_3, x_1)(x_3, x_2) =$

$u(000111, E(3))$

$u(100111, E(3)) \cdot x_2 = x_1(x_2, x_1)(x_3, x_1)(x_3, x_2)x_2 \overset{17}{=} x_1(x_2, x_1)(x_3, x_1)x_2(x_3, x_2) \overset{14}{=}$

$x_1(x_2, x_1)x_2(x_3, x_1)(x_3, x_2) \overset{11}{=} x_1x_2(x_2, x_1)(x_3, x_1)(x_3, x_2) = u(110111, E(3))$

$u(100111, E(3)) \cdot x_3 = x_1(x_2, x_1)(x_3, x_1)(x_3, x_2)x_3 \overset{18}{=} x_1(x_2, x_1)(x_3, x_1)x_3(x_3, x_2) \overset{15}{=}$

$x_1(x_2, x_1)x_3(x_3, x_1)(x_3, x_2) \overset{12}{=} x_1x_3(x_2, x_1)(x_3, x_1)(x_3, x_2) = u(101111, E(3))$

$u(101000, E(3)) \cdot x_1 = x_1x_3x_1 \overset{5}{=} x_1x_1x_3(x_3, x_1) \overset{1}{=} x_3(x_3, x_1) = u(001010, E(3))$

$u(101000, E(3)) \cdot x_2 = x_1x_3x_2 \overset{6}{=} x_1x_2x_3(x_3, x_2) = u(111001, E(3))$

$u(101000, E(3)) \cdot x_3 = x_1x_3x_3 \overset{3}{=} x_1 = u(100000, E(3))$

$u(101001, E(3)) \cdot x_1 = x_1x_3(x_3, x_2)x_1 \overset{16}{=} x_1x_3x_1(x_3, x_2) \overset{5}{=} x_1x_1x_3(x_3, x_1)(x_3, x_2) \overset{1}{=}$

$x_3(x_3, x_1)(x_3, x_2) = u(001011, E(3))$

$u(101001, E(3)) \cdot x_2 = x_1x_3(x_3, x_2)x_2 \overset{17}{=} x_1x_3x_2(x_3, x_2) \overset{6}{=} x_1x_2x_3(x_3, x_2)(x_3, x_2) \overset{9}{=} x_1x_2x_3 =$

$u(111000, E(3))$

$u(101001, E(3)) \cdot x_3 = x_1x_3(x_3, x_2)x_3 \overset{18}{=} x_1x_3x_3(x_3, x_2) \overset{3}{=} x_1(x_3, x_2) = u(100001, E(3))$

$u(101010, E(3)) \cdot x_1 = x_1x_3(x_3, x_1)x_1 \overset{13}{=} x_1x_3x_1(x_3, x_1) \overset{5}{=} x_1x_1x_3(x_3, x_1)(x_3, x_1) \overset{1}{=}$

$x_3(x_3, x_1)(x_3, x_1) \overset{8}{=} x_3 = u(001000, E(3))$

$u(101010, E(3)) \cdot x_2 = x_1x_3(x_3, x_1)x_2 \overset{14}{=} x_1x_3x_2(x_3, x_1) \overset{6}{=} x_1x_2x_3(x_3, x_2)(x_3, x_1) \overset{21}{=}$

$x_1x_2x_3(x_3, x_1)(x_3, x_2) = u(111011, E(3))$

$u(101010, E(3)) \cdot x_3 = x_1x_3(x_3, x_1)x_3 \overset{15}{=} x_1x_3x_3(x_3, x_1) \overset{3}{=} x_1(x_3, x_1) = u(100010, E(3))$

$u(101011, E(3)) \cdot x_1 = x_1x_3(x_3, x_1)(x_3, x_2)x_1 \overset{16}{=} x_1x_3(x_3, x_1)x_1(x_3, x_2) \overset{13}{=}$

$x_1x_3x_1(x_3, x_1)(x_3, x_2) \overset{5}{=} x_1x_1x_3(x_3, x_1)(x_3, x_1)(x_3, x_2) \overset{1}{=} x_3(x_3, x_1)(x_3, x_1)(x_3, x_2) \overset{8}{=}$

$x_3(x_3, x_2) = u(001001, E(3))$

$u(101011, E(3)) \cdot x_2 = x_1x_3(x_3, x_1)(x_3, x_2)x_2 \overset{17}{=} x_1x_3(x_3, x_1)x_2(x_3, x_2) \overset{14}{=}$

$x_1x_3x_2(x_3, x_1)(x_3, x_2) \overset{6}{=} x_1x_2x_3(x_3, x_2)(x_3, x_1)(x_3, x_2) \overset{21}{=} x_1x_2x_3(x_3, x_1)(x_3, x_2)(x_3, x_2) \overset{9}{=}$

$x_1x_2x_3(x_3, x_1) = u(111010, E(3))$

$u(101011, E(3)) \cdot x_3 = x_1x_3(x_3, x_1)(x_3, x_2)x_3 \overset{18}{=} x_1x_3(x_3, x_1)x_3(x_3, x_2) \overset{15}{=}$

$x_1x_3x_3(x_3, x_1)(x_3, x_2) \overset{3}{=} x_1(x_3, x_1)(x_3, x_2) = u(100011, E(3))$

$u(101100, E(3)) \cdot x_1 = x_1x_3(x_2, x_1)x_1 \overset{10}{=} x_1x_3x_1(x_2, x_1) \overset{5}{=} x_1x_1x_3(x_3, x_1)(x_2, x_1) \overset{1}{=}$

$x_3(x_3, x_1)(x_2, x_1) \overset{19}{=} x_3(x_2, x_1)(x_3, x_1) = u(001110, E(3))$

$u(101100, E(3)) \cdot x_2 = x_1x_3(x_2, x_1)x_2 \overset{11}{=} x_1x_3x_2(x_2, x_1) \overset{6}{=} x_1x_2x_3(x_3, x_2)(x_2, x_1) \overset{20}{=}$

$x_1x_2x_3(x_2, x_1)(x_3, x_2) = u(111101, E(3))$

$u(101100, E(3)) \cdot x_3 = x_1x_3(x_2, x_1)x_3 \overset{12}{=} x_1x_3x_3(x_2, x_1) \overset{3}{=} x_1(x_2, x_1) = u(100100, E(3))$

$u(101101, E(3)) \cdot x_1 = x_1x_3(x_2, x_1)(x_3, x_2)x_1 \overset{16}{=} x_1x_3(x_2, x_1)x_1(x_3, x_2) \overset{10}{=}$

$x_1x_3x_1(x_2, x_1)(x_3, x_2) \overset{5}{=} x_1x_1x_3(x_3, x_1)(x_2, x_1)(x_3, x_2) \overset{1}{=} x_3(x_3, x_1)(x_2, x_1)(x_3, x_2) \overset{19}{=}$

$x_3(x_2, x_1)(x_3, x_1)(x_3, x_2) = u(001111, E(3))$

$u(101101, E(3)) \cdot x_2 = x_1x_3(x_2, x_1)(x_3, x_2)x_2 \overset{17}{=} x_1x_3(x_2, x_1)x_2(x_3, x_2) \overset{11}{=}$

$x_1x_3x_2(x_2, x_1)(x_3, x_2) \overset{6}{=} x_1x_2x_3(x_3, x_2)(x_2, x_1)(x_3, x_2) \overset{20}{=} x_1x_2x_3(x_2, x_1)(x_3, x_2)(x_3, x_2) \overset{9}{=}$

$x_1x_2x_3(x_2, x_1) = u(111100, E(3))$

$u(101101, E(3)) \cdot x_3 = x_1x_3(x_2, x_1)(x_3, x_2)x_3 \overset{18}{=} x_1x_3(x_2, x_1)x_3(x_3, x_2) \overset{12}{=}$

$x_1x_3x_3(x_2, x_1)(x_3, x_2) \overset{3}{=} x_1(x_2, x_1)(x_3, x_2) = u(100101, E(3))$

$u(101110, E(3)) \cdot x_1 = x_1x_3(x_2, x_1)(x_3, x_1)x_1 \overset{13}{=} x_1x_3(x_2, x_1)x_1(x_3, x_1) \overset{10}{=}$

$x_1x_3x_1(x_2, x_1)(x_3, x_1) \overset{5}{=} x_1x_1x_3(x_3, x_1)(x_2, x_1)(x_3, x_1) \overset{1}{=} x_3(x_3, x_1)(x_2, x_1)(x_3, x_1) \overset{19}{=}$

$x_3(x_2, x_1)(x_3, x_1)(x_3, x_1) \overset{8}{=} x_3(x_2, x_1) = u(001100, E(3))$

$u(101110, E(3)) \cdot x_2 = x_1x_3(x_2, x_1)(x_3, x_1)x_2 \overset{14}{=} x_1x_3(x_2, x_1)x_2(x_3, x_1) \overset{11}{=}$

$x_1x_3x_2(x_2, x_1)(x_3, x_1) \overset{6}{=} x_1x_2x_3(x_3, x_2)(x_2, x_1)(x_3, x_1) \overset{20}{=} x_1x_2x_3(x_2, x_1)(x_3, x_2)(x_3, x_1) \overset{21}{=}$

$x_1x_2x_3(x_2, x_1)(x_3, x_1)(x_3, x_2) = u(111111, E(3))$

$u(101110, E(3)) \cdot x_3 = x_1x_3(x_2, x_1)(x_3, x_1)x_3 \overset{15}{=} x_1x_3(x_2, x_1)x_3(x_3, x_1) \overset{12}{=}$

$x_1x_3x_3(x_2, x_1)(x_3, x_1) \overset{3}{=} x_1(x_2, x_1)(x_3, x_1) = u(100110, E(3))$

$u(101111, E(3)) \cdot x_1 = x_1x_3(x_2, x_1)(x_3, x_1)(x_3, x_2)x_1 \overset{16}{=} x_1x_3(x_2, x_1)(x_3, x_1)x_1(x_3, x_2) \overset{13}{=}$

$x_1x_3(x_2, x_1)x_1(x_3, x_1)(x_3, x_2) \overset{10}{=} x_1x_3x_1(x_2, x_1)(x_3, x_1)(x_3, x_2) \overset{5}{=}$

$x_1x_1x_3(x_3, x_1)(x_2, x_1)(x_3, x_1)(x_3, x_2) \overset{1}{=} x_3(x_3, x_1)(x_2, x_1)(x_3, x_1)(x_3, x_2) \overset{19}{=}$

$x_3(x_2, x_1)(x_3, x_1)(x_3, x_1)(x_3, x_2) \overset{8}{=} x_3(x_2, x_1)(x_3, x_2) = u(001101, E(3))$

$u(101111, E(3)) \cdot x_2 = x_1x_3(x_2, x_1)(x_3, x_1)(x_3, x_2)x_2 \overset{17}{=} x_1x_3(x_2, x_1)(x_3, x_1)x_2(x_3, x_2) \overset{14}{=}$

$x_1x_3(x_2, x_1)x_2(x_3, x_1)(x_3, x_2) \overset{11}{=} x_1x_3x_2(x_2, x_1)(x_3, x_1)(x_3, x_2) \overset{6}{=}$

$x_1x_2x_3(x_3,x_2)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{20}{=} x_1x_2x_3(x_2,x_1)(x_3,x_2)(x_3,x_1)(x_3,x_2) \overset{21}{=}$

$x_1x_2x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)(x_3,x_2) \overset{9}{=} x_1x_2x_3(x_2,x_1)(x_3,x_1) = u(111110, E(3))$

$u(101111, E(3)) \cdot x_3 = x_1x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)x_3 \overset{18}{=} x_1x_3(x_2,x_1)(x_3,x_1)x_3(x_3,x_2) \overset{15}{=}$

$x_1x_3(x_2,x_1)x_3(x_3,x_1)(x_3,x_2) \overset{12}{=} x_1x_3x_3(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{3}{=} x_1(x_2,x_1)(x_3,x_1)(x_3,x_2) =$

$u(100111, E(3))$

$u(110000, E(3)) \cdot x_1 = x_1x_2x_1 \overset{4}{=} x_1x_1x_2(x_2,x_1) \overset{1}{=} x_2(x_2,x_1) = u(010100, E(3))$

$u(110000, E(3)) \cdot x_2 = x_1x_2x_2 \overset{2}{=} x_1 = u(100000, E(3))$

$u(110000, E(3)) \cdot x_3 = x_1x_2x_3 = u(111000, E(3))$

$u(110001, E(3)) \cdot x_1 = x_1x_2(x_3,x_2)x_1 \overset{16}{=} x_1x_2x_1(x_3,x_2) \overset{4}{=} x_1x_1x_2(x_2,x_1)(x_3,x_2) \overset{1}{=}$

$x_2(x_2,x_1)(x_3,x_2) = u(010101, E(3))$

$u(110001, E(3)) \cdot x_2 = x_1x_2(x_3,x_2)x_2 \overset{17}{=} x_1x_2x_2(x_3,x_2) \overset{2}{=} x_1(x_3,x_2) = u(100001, E(3))$

$u(110001, E(3)) \cdot x_3 = x_1x_2(x_3,x_2)x_3 \overset{18}{=} x_1x_2x_3(x_3,x_2) = u(111001, E(3))$

$u(110010, E(3)) \cdot x_1 = x_1x_2(x_3,x_1)x_1 \overset{13}{=} x_1x_2x_1(x_3,x_1) \overset{4}{=} x_1x_1x_2(x_2,x_1)(x_3,x_1) \overset{1}{=}$

$x_2(x_2,x_1)(x_3,x_1) = u(010110, E(3))$

$u(110010, E(3)) \cdot x_2 = x_1x_2(x_3,x_1)x_2 \overset{14}{=} x_1x_2x_2(x_3,x_1) \overset{2}{=} x_1(x_3,x_1) = u(100010, E(3))$

$u(110010, E(3)) \cdot x_3 = x_1x_2(x_3,x_1)x_3 \overset{15}{=} x_1x_2x_3(x_3,x_1) = u(111010, E(3))$

$u(110011, E(3)) \cdot x_1 = x_1x_2(x_3,x_1)(x_3,x_2)x_1 \overset{16}{=} x_1x_2(x_3,x_1)x_1(x_3,x_2) \overset{13}{=}$

$x_1x_2x_1(x_3,x_1)(x_3,x_2) \overset{4}{=} x_1x_1x_2(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{1}{=} x_2(x_2,x_1)(x_3,x_1)(x_3,x_2) =$

$u(010111, E(3))$

$u(110011, E(3)) \cdot x_2 = x_1x_2(x_3,x_1)(x_3,x_2)x_2 \overset{17}{=} x_1x_2(x_3,x_1)x_2(x_3,x_2) \overset{14}{=}$

$x_1x_2x_2(x_3,x_1)(x_3,x_2) \overset{2}{=} x_1(x_3,x_1)(x_3,x_2) = u(100011, E(3))$

$u(110011, E(3)) \cdot x_3 = x_1x_2(x_3,x_1)(x_3,x_2)x_3 \overset{18}{=} x_1x_2(x_3,x_1)x_3(x_3,x_2) \overset{15}{=}$

$x_1x_2x_3(x_3,x_1)(x_3,x_2) = u(111011, E(3))$

$u(110100, E(3)) \cdot x_1 = x_1x_2(x_2,x_1)x_1 \overset{10}{=} x_1x_2x_1(x_2,x_1) \overset{4}{=} x_1x_1x_2(x_2,x_1)(x_2,x_1) \overset{1}{=}$

$x_2(x_2,x_1)(x_2,x_1) \overset{7}{=} x_2 = u(010000, E(3))$

$u(110100, E(3)) \cdot x_2 = x_1x_2(x_2, x_1)x_2 \overset{11}{=} x_1x_2x_2(x_2, x_1) \overset{2}{=} x_1(x_2, x_1) = u(100100, E(3))$

$u(110100, E(3)) \cdot x_3 = x_1x_2(x_2, x_1)x_3 \overset{12}{=} x_1x_2x_3(x_2, x_1) = u(111100, E(3))$

$u(110101, E(3)) \cdot x_1 = x_1x_2(x_2, x_1)(x_3, x_2)x_1 \overset{16}{=} x_1x_2(x_2, x_1)x_1(x_3, x_2) \overset{10}{=}$

$x_1x_2x_1(x_2, x_1)(x_3, x_2) \overset{4}{=} x_1x_1x_2(x_2, x_1)(x_2, x_1)(x_3, x_2) \overset{1}{=} x_2(x_2, x_1)(x_2, x_1)(x_3, x_2) \overset{7}{=}$

$x_2(x_3, x_2) = u(010001, E(3))$

$u(110101, E(3)) \cdot x_2 = x_1x_2(x_2, x_1)(x_3, x_2)x_2 \overset{17}{=} x_1x_2(x_2, x_1)x_2(x_3, x_2) \overset{11}{=}$

$x_1x_2x_2(x_2, x_1)(x_3, x_2) \overset{2}{=} x_1(x_2, x_1)(x_3, x_2) = u(100101, E(3))$

$u(110101, E(3)) \cdot x_3 = x_1x_2(x_2, x_1)(x_3, x_2)x_3 \overset{18}{=} x_1x_2(x_2, x_1)x_3(x_3, x_2) \overset{12}{=}$

$x_1x_2x_3(x_2, x_1)(x_3, x_2) = u(111101, E(3))$

$u(110110, E(3)) \cdot x_1 = x_1x_2(x_2, x_1)(x_3, x_1)x_1 \overset{13}{=} x_1x_2(x_2, x_1)x_1(x_3, x_1) \overset{10}{=}$

$x_1x_2x_1(x_2, x_1)(x_3, x_1) \overset{4}{=} x_1x_1x_2(x_2, x_1)(x_2, x_1)(x_3, x_1) \overset{1}{=} x_2(x_2, x_1)(x_2, x_1)(x_3, x_1) \overset{7}{=}$

$x_2(x_3, x_1) = u(010010, E(3))$

$u(110110, E(3)) \cdot x_2 = x_1x_2(x_2, x_1)(x_3, x_1)x_2 \overset{14}{=} x_1x_2(x_2, x_1)x_2(x_3, x_1) \overset{11}{=}$

$x_1x_2x_2(x_2, x_1)(x_3, x_1) \overset{2}{=} x_1(x_2, x_1)(x_3, x_1) = u(100110, E(3))$

$u(110110, E(3)) \cdot x_3 = x_1x_2(x_2, x_1)(x_3, x_1)x_3 \overset{15}{=} x_1x_2(x_2, x_1)x_3(x_3, x_1) \overset{12}{=}$

$x_1x_2x_3(x_2, x_1)(x_3, x_1) = u(111110, E(3))$

$u(110111, E(3)) \cdot x_1 = x_1x_2(x_2, x_1)(x_3, x_1)(x_3, x_2)x_1 \overset{16}{=} x_1x_2(x_2, x_1)(x_3, x_1)x_1(x_3, x_2) \overset{13}{=}$

$x_1x_2(x_2, x_1)x_1(x_3, x_1)(x_3, x_2) \overset{10}{=} x_1x_2x_1(x_2, x_1)(x_3, x_1)(x_3, x_2) \overset{4}{=}$

$x_1x_1x_2(x_2, x_1)(x_2, x_1)(x_3, x_1)(x_3, x_2) \overset{1}{=} x_2(x_2, x_1)(x_2, x_1)(x_3, x_1)(x_3, x_2) \overset{7}{=}$

$x_2(x_3, x_1)(x_3, x_2) = u(010011, E(3))$

$u(110111, E(3)) \cdot x_2 = x_1x_2(x_2, x_1)(x_3, x_1)(x_3, x_2)x_2 \overset{17}{=} x_1x_2(x_2, x_1)(x_3, x_1)x_2(x_3, x_2) \overset{14}{=}$

$x_1x_2(x_2, x_1)x_2(x_3, x_1)(x_3, x_2) \overset{11}{=} x_1x_2x_2(x_2, x_1)(x_3, x_1)(x_3, x_2) \overset{2}{=} x_1(x_2, x_1)(x_3, x_1)(x_3, x_2) =$

$u(100111, E(3))$

$u(110111, E(3)) \cdot x_3 = x_1x_2(x_2, x_1)(x_3, x_1)(x_3, x_2)x_3 \overset{18}{=} x_1x_2(x_2, x_1)(x_3, x_1)x_3(x_3, x_2) \overset{15}{=}$

$x_1x_2(x_2, x_1)x_3(x_3, x_1)(x_3, x_2) \overset{12}{=} x_1x_2x_3(x_2, x_1)(x_3, x_1)(x_3, x_2) = u(111111, E(3))$

$u(111000, E(3)) \cdot x_1 = x_1x_2x_3x_1 \overset{5}{=} x_1x_2x_1x_3(x_3, x_1) \overset{4}{=} x_1x_1x_2(x_2, x_1)x_3(x_3, x_1) \overset{1}{=}$

$x_2(x_2, x_1)x_3(x_3, x_1) \overset{12}{=} x_2x_3(x_2, x_1)(x_3, x_1) = u(011110, E(3))$

$u(111000, E(3)) \cdot x_2 = x_1x_2x_3x_2 \overset{6}{=} x_1x_2x_2x_3(x_3, x_2) \overset{2}{=} x_1x_3(x_3, x_2) = u(101001, E(3))$

$u(111000, E(3)) \cdot x_3 = x_1x_2x_3x_3 \overset{3}{=} x_1x_2 = u(110000, E(3))$

$u(111001, E(3)) \cdot x_1 = x_1x_2x_3(x_3, x_2)x_1 \overset{16}{=} x_1x_2x_3x_1(x_3, x_2) \overset{5}{=} x_1x_2x_1x_3(x_3, x_1)(x_3, x_2) \overset{4}{=}$

$x_1x_1x_2(x_2, x_1)x_3(x_3, x_1)(x_3, x_2) \overset{1}{=} x_2(x_2, x_1)x_3(x_3, x_1)(x_3, x_2) \overset{12}{=}$

$x_2x_3(x_2, x_1)(x_3, x_1)(x_3, x_2) = u(011111, E(3))$

$u(111001, E(3)) \cdot x_2 = x_1x_2x_3(x_3, x_2)x_2 \overset{17}{=} x_1x_2x_3x_2(x_3, x_2) \overset{6}{=} x_1x_2x_2x_3(x_3, x_2)(x_3, x_2) \overset{2}{=}$

$x_1x_3(x_3, x_2)(x_3, x_2) \overset{9}{=} x_1x_3 = u(101000, E(3))$

$u(111001, E(3)) \cdot x_3 = x_1x_2x_3(x_3, x_2)x_3 \overset{18}{=} x_1x_2x_3x_3(x_3, x_2) \overset{3}{=} x_1x_2(x_3, x_2) = u(110001, E(3))$

$u(111010, E(3)) \cdot x_1 = x_1x_2x_3(x_3, x_1)x_1 \overset{13}{=} x_1x_2x_3x_1(x_3, x_1) \overset{5}{=} x_1x_2x_1x_3(x_3, x_1)(x_3, x_1) \overset{4}{=}$

$x_1x_1x_2(x_2, x_1)x_3(x_3, x_1)(x_3, x_1) \overset{1}{=} x_2(x_2, x_1)x_3(x_3, x_1)(x_3, x_1) \overset{8}{=} x_2(x_2, x_1)x_3 \overset{12}{=}$

$x_2x_3(x_2, x_1) = u(011100, E(3))$

$u(111010, E(3)) \cdot x_2 = x_1x_2x_3(x_3, x_1)x_2 \overset{14}{=} x_1x_2x_3x_2(x_3, x_1) \overset{6}{=} x_1x_2x_2x_3(x_3, x_2)(x_3, x_1) \overset{2}{=}$

$x_1x_3(x_3, x_2)(x_3, x_1) \overset{21}{=} x_1x_3(x_3, x_1)(x_3, x_2) = u(101011, E(3))$

$u(111010, E(3)) \cdot x_3 = x_1x_2x_3(x_3, x_1)x_3 \overset{15}{=} x_1x_2x_3x_3(x_3, x_1) \overset{3}{=} x_1x_2(x_3, x_1) = u(110010, E(3))$

$u(111011, E(3)) \cdot x_1 = x_1x_2x_3(x_3, x_1)(x_3, x_2)x_1 \overset{16}{=} x_1x_2x_3(x_3, x_1)x_1(x_3, x_2) \overset{13}{=}$

$x_1x_2x_3x_1(x_3, x_1)(x_3, x_2) \overset{5}{=} x_1x_2x_1x_3(x_3, x_1)(x_3, x_1)(x_3, x_2) \overset{4}{=}$

$x_1x_1x_2(x_2, x_1)x_3(x_3, x_1)(x_3, x_1)(x_3, x_2) \overset{1}{=} x_2(x_2, x_1)x_3(x_3, x_1)(x_3, x_1)(x_3, x_2) \overset{8}{=}$

$x_2(x_2, x_1)x_3(x_3, x_2) \overset{12}{=} x_2x_3(x_2, x_1)(x_3, x_2) = u(011101, E(3))$

$u(111011, E(3)) \cdot x_2 = x_1x_2x_3(x_3, x_1)(x_3, x_2)x_2 \overset{17}{=} x_1x_2x_3(x_3, x_1)x_2(x_3, x_2) \overset{14}{=}$

$x_1x_2x_3x_2(x_3, x_1)(x_3, x_2) \overset{6}{=} x_1x_2x_2x_3(x_3, x_2)(x_3, x_1)(x_3, x_2) \overset{2}{=} x_1x_3(x_3, x_2)(x_3, x_1)(x_3, x_2) \overset{21}{=}$

$x_1x_3(x_3, x_1)(x_3, x_2)(x_3, x_2) \overset{9}{=} x_1x_3(x_3, x_1) = u(101010, E(3))$

$u(111011, E(3)) \cdot x_3 = x_1x_2x_3(x_3, x_1)(x_3, x_2)x_3 \overset{18}{=} x_1x_2x_3(x_3, x_1)x_3(x_3, x_2) \overset{15}{=}$

$x_1x_2x_3x_3(x_3, x_1)(x_3, x_2) \overset{3}{=} x_1x_2(x_3, x_1)(x_3, x_2) = u(110011, E(3))$

$u(111100, E(3)) \cdot x_1 = x_1x_2x_3(x_2, x_1)x_1 \overset{10}{=} x_1x_2x_3x_1(x_2, x_1) \overset{5}{=} x_1x_2x_1x_3(x_3, x_1)(x_2, x_1) \overset{4}{=}$

$x_1x_1x_2(x_2, x_1)x_3(x_3, x_1)(x_2, x_1) \overset{1}{=} x_2(x_2, x_1)x_3(x_3, x_1)(x_2, x_1) \overset{12}{=}$

$x_2x_3(x_2, x_1)(x_3, x_1)(x_2, x_1) \overset{19}{=} x_2x_3(x_2, x_1)(x_2, x_1)(x_3, x_1) \overset{7}{=} x_2x_3(x_3, x_1) = u(011010, E(3))$

$u(111100, E(3)) \cdot x_2 = x_1x_2x_3(x_2, x_1)x_2 \overset{11}{=} x_1x_2x_3x_2(x_2, x_1) \overset{6}{=} x_1x_2x_2x_3(x_3, x_2)(x_2, x_1) \overset{2}{=}$

$x_1x_3(x_3, x_2)(x_2, x_1) \overset{20}{=} x_1x_3(x_2, x_1)(x_3, x_2) = u(101101, E(3))$

$u(111100, E(3)) \cdot x_3 = x_1x_2x_3(x_2, x_1)x_3 \overset{12}{=} x_1x_2x_3x_3(x_2, x_1) \overset{3}{=} x_1x_2(x_2, x_1) = u(110100, E(3))$

$u(111101, E(3)) \cdot x_1 = x_1x_2x_3(x_2, x_1)(x_3, x_2)x_1 \overset{16}{=} x_1x_2x_3(x_2, x_1)x_1(x_3, x_2) \overset{10}{=}$

$x_1x_2x_3x_1(x_2, x_1)(x_3, x_2) \overset{5}{=} x_1x_2x_1x_3(x_3, x_1)(x_2, x_1)(x_3, x_2) \overset{4}{=}$

$x_1x_1x_2(x_2, x_1)x_3(x_3, x_1)(x_2, x_1)(x_3, x_2) \overset{1}{=} x_2(x_2, x_1)x_3(x_3, x_1)(x_2, x_1)(x_3, x_2) \overset{12}{=}$

$x_2x_3(x_2, x_1)(x_3, x_1)(x_2, x_1)(x_3, x_2) \overset{19}{=} x_2x_3(x_2, x_1)(x_2, x_1)(x_3, x_1)(x_3, x_2) \overset{7}{=}$

$x_2x_3(x_3, x_1)(x_3, x_2) = u(011011, E(3))$

$u(111101, E(3)) \cdot x_2 = x_1x_2x_3(x_2, x_1)(x_3, x_2)x_2 \overset{17}{=} x_1x_2x_3(x_2, x_1)x_2(x_3, x_2) \overset{11}{=}$

$x_1x_2x_3x_2(x_2, x_1)(x_3, x_2) \overset{6}{=} x_1x_2x_2x_3(x_3, x_2)(x_2, x_1)(x_3, x_2) \overset{2}{=} x_1x_3(x_3, x_2)(x_2, x_1)(x_3, x_2) \overset{20}{=}$

$x_1x_3(x_2, x_1)(x_3, x_2)(x_3, x_2) \overset{9}{=} x_1x_3(x_2, x_1) = u(101100, E(3))$

$u(111101, E(3)) \cdot x_3 = x_1x_2x_3(x_2, x_1)(x_3, x_2)x_3 \overset{18}{=} x_1x_2x_3(x_2, x_1)x_3(x_3, x_2) \overset{12}{=}$

$x_1x_2x_3x_3(x_2, x_1)(x_3, x_2) \overset{3}{=} x_1x_2(x_2, x_1)(x_3, x_2) = u(110101, E(3))$

$u(111110, E(3)) \cdot x_1 = x_1x_2x_3(x_2, x_1)(x_3, x_1)x_1 \overset{13}{=} x_1x_2x_3(x_2, x_1)x_1(x_3, x_1) \overset{10}{=}$

$x_1x_2x_3x_1(x_2, x_1)(x_3, x_1) \overset{5}{=} x_1x_2x_1x_3(x_3, x_1)(x_2, x_1)(x_3, x_1) \overset{4}{=}$

$x_1x_1x_2(x_2, x_1)x_3(x_3, x_1)(x_2, x_1)(x_3, x_1) \overset{1}{=} x_2(x_2, x_1)x_3(x_3, x_1)(x_2, x_1)(x_3, x_1) \overset{12}{=}$

$x_2x_3(x_2, x_1)(x_3, x_1)(x_2, x_1)(x_3, x_1) \overset{19}{=} x_2x_3(x_2, x_1)(x_2, x_1)(x_3, x_1)(x_3, x_1) \overset{7}{=}$

$x_2x_3(x_3, x_1)(x_3, x_1) \overset{8}{=} x_2x_3 = u(011000, E(3))$

$u(111110, E(3)) \cdot x_2 = x_1x_2x_3(x_2, x_1)(x_3, x_1)x_2 \overset{14}{=} x_1x_2x_3(x_2, x_1)x_2(x_3, x_1) \overset{11}{=}$

$x_1x_2x_3x_2(x_2, x_1)(x_3, x_1) \overset{6}{=} x_1x_2x_2x_3(x_3, x_2)(x_2, x_1)(x_3, x_1) \overset{2}{=} x_1x_3(x_3, x_2)(x_2, x_1)(x_3, x_1) \overset{20}{=}$

$x_1x_3(x_2, x_1)(x_3, x_2)(x_3, x_1) \overset{21}{=} x_1x_3(x_2, x_1)(x_3, x_1)(x_3, x_2) = u(101111, E(3))$

$u(111110, E(3)) \cdot x_3 = x_1x_2x_3(x_2, x_1)(x_3, x_1)x_3 \overset{15}{=} x_1x_2x_3(x_2, x_1)x_3(x_3, x_1) \overset{12}{=}$

$x_1x_2x_3x_3(x_2,x_1)(x_3,x_1) \overset{3}{=} x_1x_2(x_2,x_1)(x_3,x_1) = u(110110, E(3))$

$u(111111, E(3)) \cdot x_1 = x_1x_2x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)x_1 \overset{16}{=} x_1x_2x_3(x_2,x_1)(x_3,x_1)x_1(x_3,x_2) \overset{13}{=}$

$x_1x_2x_3(x_2,x_1)x_1(x_3,x_1)(x_3,x_2) \overset{10}{=} x_1x_2x_3x_1(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{5}{=}$

$x_1x_2x_1x_3(x_3,x_1)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{4}{=} x_1x_1x_2(x_2,x_1)x_3(x_3,x_1)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{1}{=}$

$x_2(x_2,x_1)x_3(x_3,x_1)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{12}{=} x_2x_3(x_2,x_1)(x_3,x_1)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{19}{=}$

$x_2x_3(x_2,x_1)(x_2,x_1)(x_3,x_1)(x_3,x_1)(x_3,x_2) \overset{7}{=} x_2x_3(x_3,x_1)(x_3,x_1)(x_3,x_2) \overset{8}{=} x_2x_3(x_3,x_2) =$

$u(011001, E(3))$

$u(111111, E(3)) \cdot x_2 = x_1x_2x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)x_2 \overset{17}{=} x_1x_2x_3(x_2,x_1)(x_3,x_1)x_2(x_3,x_2) \overset{14}{=}$

$x_1x_2x_3(x_2,x_1)x_2(x_3,x_1)(x_3,x_2) \overset{11}{=} x_1x_2x_3x_2(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{6}{=}$

$x_1x_2x_2x_3(x_3,x_2)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{2}{=} x_1x_3(x_3,x_2)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{20}{=}$

$x_1x_3(x_2,x_1)(x_3,x_2)(x_3,x_1)(x_3,x_2) \overset{21}{=} x_1x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)(x_3,x_2) \overset{9}{=}$

$x_1x_3(x_2,x_1)(x_3,x_1) = u(101110, E(3))$

$u(111111, E(3)) \cdot x_3 = x_1x_2x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)x_3 \overset{18}{=} x_1x_2x_3(x_2,x_1)(x_3,x_1)x_3(x_3,x_2) \overset{15}{=}$

$x_1x_2x_3(x_2,x_1)x_3(x_3,x_1)(x_3,x_2) \overset{12}{=} x_1x_2x_3x_3(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{3}{=}$

$x_1x_2(x_2,x_1)(x_3,x_1)(x_3,x_2) = u(110111, E(3))$

This multiplication table permits us to draw the Cayley graph of the group $G(3,3)$.

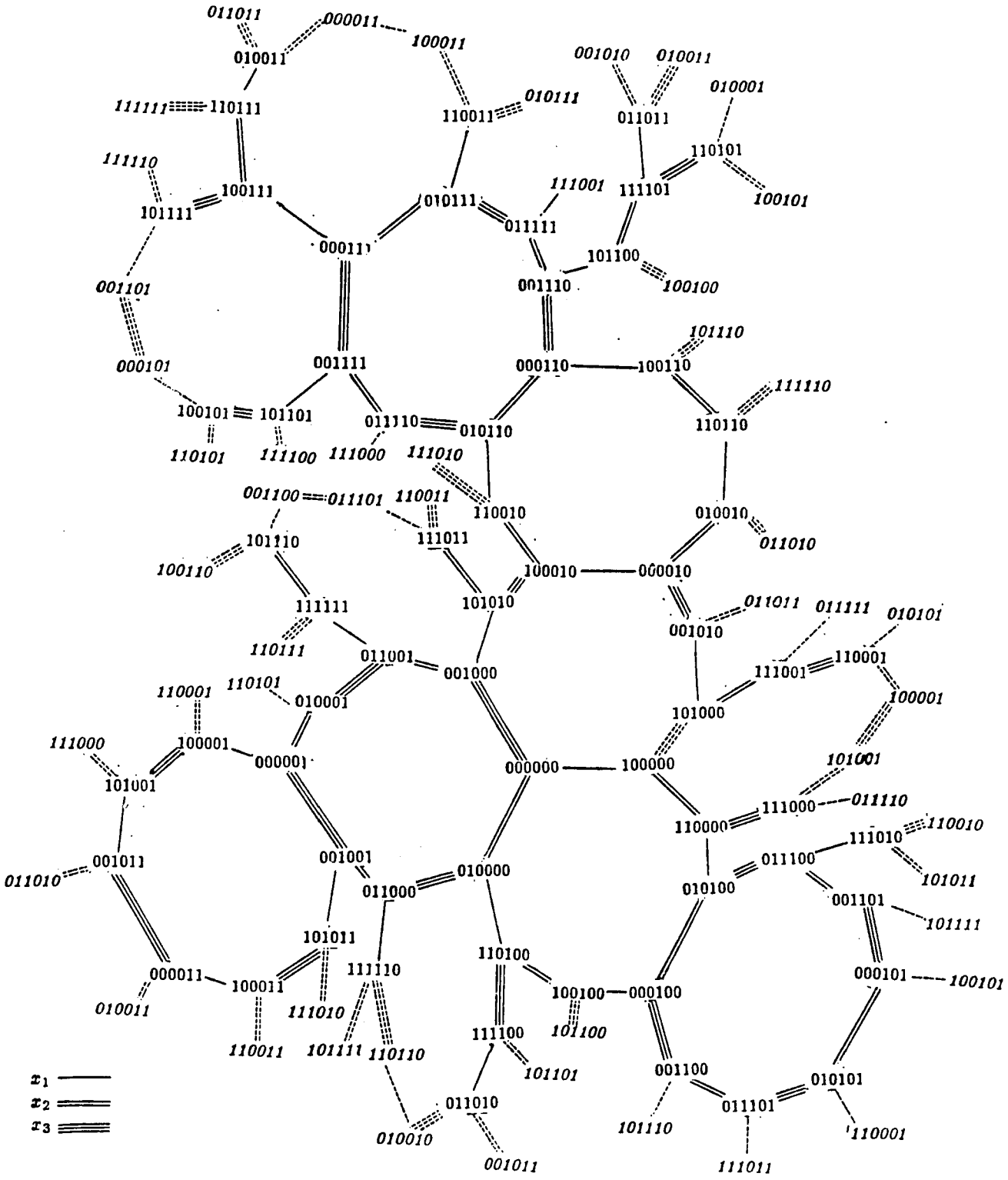

Figure A.2: The Cayley graph of $G(3,3)$

B An Example of Encryption in $G(3,3)$

We present the computer-generated trace of the collections required to encrypt the ASCII string `Hello!` using the key (5.2), as explained in section 5.

$u(010010,P) = x_1x_3x_1x_2x_1x_2x_1 \overset{4}{=} x_1x_3x_1x_1x_2(x_2,x_1)x_2x_1 \overset{1}{=} x_1x_3x_2(x_2,x_1)x_2x_1 \overset{4}{=}$

$x_1x_3x_2(x_2,x_1)x_1x_2(x_2,x_1) \overset{6}{=} x_1x_2x_3(x_3,x_2)(x_2,x_1)x_1x_2(x_2,x_1) \overset{10}{=}$

$x_1x_2x_3(x_3,x_2)x_1(x_2,x_1)x_2(x_2,x_1) \overset{11}{=} x_1x_2x_3(x_3,x_2)x_1x_2(x_2,x_1)(x_2,x_1) \overset{7}{=}$

$x_1x_2x_3(x_3,x_2)x_1x_2 \overset{16}{=} x_1x_2x_3x_1(x_3,x_2)x_2 \overset{5}{=} x_1x_2x_1x_3(x_3,x_1)(x_3,x_2)x_2 \overset{4}{=}$

$x_1x_1x_2(x_2,x_1)x_3(x_3,x_1)(x_3,x_2)x_2 \overset{1}{=} x_2(x_2,x_1)x_3(x_3,x_1)(x_3,x_2)x_2 \overset{12}{=}$

$x_2x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)x_2 \overset{17}{=} x_2x_3(x_2,x_1)(x_3,x_1)x_2(x_3,x_2) \overset{14}{=}$

$x_2x_3(x_2,x_1)x_2(x_3,x_1)(x_3,x_2) \overset{11}{=} x_2x_3x_2(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{6}{=}$

$x_2x_2x_3(x_3,x_2)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{2}{=} x_3(x_3,x_2)(x_2,x_1)(x_3,x_1)(x_3,x_2) \overset{20}{=}$

$x_3(x_2,x_1)(x_3,x_2)(x_3,x_1)(x_3,x_2) \overset{21}{=} x_3(x_2,x_1)(x_3,x_1)(x_3,x_2)(x_3,x_2) \overset{9}{=}$

$x_3(x_2,x_1)(x_3,x_1) = u(001110,E(3))$

$u(000110,P) = x_1x_3x_2x_2x_2x_1x_2x_1x_2x_1 \overset{2}{=} x_1x_3x_2x_1x_2x_1x_2x_1 \overset{4}{=}$

$x_1x_3x_1x_2(x_2,x_1)x_2x_1x_2x_1 \overset{4}{=} x_1x_3x_1x_2(x_2,x_1)x_1x_2(x_2,x_1)x_2x_1 \overset{4}{=}$

$x_1x_3x_1x_2(x_2,x_1)x_1x_2(x_2,x_1)x_1x_2(x_2,x_1) \overset{5}{=}$

$x_1x_1x_3(x_3,x_1)x_2(x_2,x_1)x_1x_2(x_2,x_1)x_1x_2(x_2,x_1) \overset{1}{=}$

$x_3(x_3,x_1)x_2(x_2,x_1)x_1x_2(x_2,x_1)x_1x_2(x_2,x_1) \overset{10}{=}$

$x_3(x_3,x_1)x_2x_1(x_2,x_1)x_2(x_2,x_1)x_1x_2(x_2,x_1) \overset{4}{=}$

$x_3(x_3,x_1)x_1x_2(x_2,x_1)(x_2,x_1)x_2(x_2,x_1)x_1x_2(x_2,x_1) \overset{7}{=}$

$x_3(x_3,x_1)x_1x_2x_2(x_2,x_1)x_1x_2(x_2,x_1) \overset{2}{=} x_3(x_3,x_1)x_1(x_2,x_1)x_1x_2(x_2,x_1) \overset{10}{=}$

$x_3(x_3,x_1)x_1x_1(x_2,x_1)x_2(x_2,x_1) \overset{1}{=} x_3(x_3,x_1)(x_2,x_1)x_2(x_2,x_1) \overset{11}{=}$

$x_3(x_3,x_1)x_2(x_2,x_1)(x_2,x_1) \overset{7}{=} x_3(x_3,x_1)x_2 \overset{14}{=} x_3x_2(x_3,x_1) \overset{6}{=} x_2x_3(x_3,x_2)(x_3,x_1) \overset{21}{=}$

$x_2x_3(x_3,x_1)(x_3,x_2) = u(011011,E(3))$

$u(010101,P) = x_1x_3x_1x_1x_3x_2x_2x_2x_1x_3x_1x_3x_1 \overset{1}{=} x_1x_3x_3x_2x_2x_2x_1x_3x_1x_3x_1 \overset{2}{=}$

$x_1x_3x_3x_2x_1x_3x_1x_3x_1 \overset{3}{=} x_1x_2x_1x_3x_1x_3x_1 \overset{4}{=} x_1x_1x_2(x_2,x_1)x_3x_1x_3x_1 \overset{1}{=}$

$x_2(x_2,x_1)x_3x_1x_3x_1 \overset{5}{=} x_2(x_2,x_1)x_1x_3(x_3,x_1)x_3x_1 \overset{5}{=} x_2(x_2,x_1)x_1x_3(x_3,x_1)x_1x_3(x_3,x_1) \overset{10}{=}$

$x_2x_1(x_2,x_1)x_3(x_3,x_1)x_1x_3(x_3,x_1) \overset{4}{=} x_1x_2(x_2,x_1)(x_2,x_1)x_3(x_3,x_1)x_1x_3(x_3,x_1) \overset{7}{=}$

$x_1x_2x_3(x_3,x_1)x_1x_3(x_3,x_1) \overset{13}{=} x_1x_2x_3x_1(x_3,x_1)x_3(x_3,x_1) \overset{5}{=}$

$x_1x_2x_1x_3(x_3,x_1)(x_3,x_1)x_3(x_3,x_1) \overset{4}{=} x_1x_1x_2(x_2,x_1)x_3(x_3,x_1)(x_3,x_1)x_3(x_3,x_1) \overset{1}{=}$

$x_2(x_2,x_1)x_3(x_3,x_1)(x_3,x_1)x_3(x_3,x_1) \overset{8}{=} x_2(x_2,x_1)x_3x_3(x_3,x_1) \overset{3}{=} x_2(x_2,x_1)(x_3,x_1) =$

$u(010110,E(3))$

$u(101100,P) = x_1x_2x_1x_1x_1x_3x_2x_2x_2x_1 \overset{1}{=} x_1x_2x_1x_3x_2x_2x_2x_1 \overset{2}{=} x_1x_2x_1x_3x_2x_1 \overset{4}{=}$

$x_1x_1x_2(x_2,x_1)x_3x_2x_1 \overset{1}{=} x_2(x_2,x_1)x_3x_2x_1 \overset{4}{=} x_2(x_2,x_1)x_3x_1x_2(x_2,x_1) \overset{5}{=}$

$x_2(x_2,x_1)x_1x_3(x_3,x_1)x_2(x_2,x_1) \overset{10}{=} x_2x_1(x_2,x_1)x_3(x_3,x_1)x_2(x_2,x_1) \overset{4}{=}$

$x_1x_2(x_2,x_1)(x_2,x_1)x_3(x_3,x_1)x_2(x_2,x_1) \overset{7}{=} x_1x_2x_3(x_3,x_1)x_2(x_2,x_1) \overset{14}{=}$

$x_1x_2x_3x_2(x_3,x_1)(x_2,x_1) \overset{6}{=} x_1x_2x_2x_3(x_3,x_2)(x_3,x_1)(x_2,x_1) \overset{2}{=}$

$x_1x_3(x_3,x_2)(x_3,x_1)(x_2,x_1) \overset{19}{=} x_1x_3(x_3,x_2)(x_2,x_1)(x_3,x_1) \overset{20}{=}$

$x_1x_3(x_2,x_1)(x_3,x_2)(x_3,x_1) \overset{21}{=} x_1x_3(x_2,x_1)(x_3,x_1)(x_3,x_2) = u(101111,E(3))$

$u(011011,P) = x_1x_3x_1x_1x_2x_1x_2x_1x_3x_1x_3x_1 \overset{1}{=} x_1x_3x_2x_1x_2x_1x_3x_1x_3x_1 \overset{4}{=}$

$x_1x_3x_1x_2(x_2,x_1)x_2x_1x_3x_1x_3x_1 \overset{4}{=} x_1x_3x_1x_2(x_2,x_1)x_1x_2(x_2,x_1)x_3x_1x_3x_1 \overset{5}{=}$

$x_1x_1x_3(x_3,x_1)x_2(x_2,x_1)x_1x_2(x_2,x_1)x_3x_1x_3x_1 \overset{1}{=}$

$x_3(x_3,x_1)x_2(x_2,x_1)x_1x_2(x_2,x_1)x_3x_1x_3x_1 \overset{5}{=}$

$x_3(x_3,x_1)x_2(x_2,x_1)x_1x_2(x_2,x_1)x_1x_3(x_3,x_1)x_3x_1 \overset{5}{=}$

$x_3(x_3,x_1)x_2(x_2,x_1)x_1x_2(x_2,x_1)x_1x_3(x_3,x_1)x_1x_3(x_3,x_1) \overset{10}{=}$

$x_3(x_3,x_1)x_2x_1(x_2,x_1)x_2(x_2,x_1)x_1x_3(x_3,x_1)x_1x_3(x_3,x_1) \overset{4}{=}$

$x_3(x_3,x_1)x_1x_2(x_2,x_1)(x_2,x_1)x_2(x_2,x_1)x_1x_3(x_3,x_1)x_1x_3(x_3,x_1) \overset{7}{=}$

$x_3(x_3,x_1)x_1x_2x_2(x_2,x_1)x_1x_3(x_3,x_1)x_1x_3(x_3,x_1) \overset{2}{=}$

$x_3(x_3,x_1)x_1(x_2,x_1)x_1x_3(x_3,x_1)x_1x_3(x_3,x_1) \overset{10}{=}$

$x_3(x_3,x_1)x_1x_1(x_2,x_1)x_3(x_3,x_1)x_1x_3(x_3,x_1) \overset{1}{=} x_3(x_3,x_1)(x_2,x_1)x_3(x_3,x_1)x_1x_3(x_3,x_1) \overset{12}{=}$

$x_3(x_3,x_1)x_3(x_2,x_1)(x_3,x_1)x_1x_3(x_3,x_1) \overset{13}{=} x_3(x_3,x_1)x_3(x_2,x_1)x_1(x_3,x_1)x_3(x_3,x_1) \overset{10}{=}$

$x_3(x_3,x_1)x_3x_1(x_2,x_1)(x_3,x_1)x_3(x_3,x_1) \overset{5}{=}$

$x_3(x_3,x_1)x_1x_3(x_3,x_1)(x_2,x_1)(x_3,x_1)x_3(x_3,x_1) \overset{13}{=}$

$x_3x_1(x_3,x_1)x_3(x_3,x_1)(x_2,x_1)(x_3,x_1)x_3(x_3,x_1) \overset{5}{=}$

$x_1x_3(x_3,x_1)(x_3,x_1)x_3(x_3,x_1)(x_2,x_1)(x_3,x_1)x_3(x_3,x_1) \overset{8}{=}$

$x_1x_3x_3(x_3,x_1)(x_2,x_1)(x_3,x_1)x_3(x_3,x_1) \overset{3}{=} x_1(x_3,x_1)(x_2,x_1)(x_3,x_1)x_3(x_3,x_1) \overset{15}{=}$

$x_1(x_3,x_1)(x_2,x_1)x_3(x_3,x_1)(x_3,x_1) \overset{8}{=} x_1(x_3,x_1)(x_2,x_1)x_3 \overset{12}{=} x_1(x_3,x_1)x_3(x_2,x_1) \overset{15}{=}$

$x_1x_3(x_3,x_1)(x_2,x_1) \overset{19}{=} x_1x_3(x_2,x_1)(x_3,x_1) = u(101110,E(3))$

$u(000110,P) = x_1x_3x_2x_2x_2x_1x_2x_1x_2x_1 \overset{2}{=} x_1x_3x_2x_1x_2x_1x_2x_1 \overset{4}{=}$

$x_1x_3x_1x_2(x_2,x_1)x_2x_1x_2x_1 \overset{4}{=} x_1x_3x_1x_2(x_2,x_1)x_1x_2(x_2,x_1)x_2x_1 \overset{4}{=}$

$x_1x_3x_1x_2(x_2,x_1)x_1x_2(x_2,x_1)x_1x_2(x_2,x_1) \overset{5}{=}$

$x_1x_1x_3(x_3,x_1)x_2(x_2,x_1)x_1x_2(x_2,x_1)x_1x_2(x_2,x_1) \overset{1}{=}$

$x_3(x_3,x_1)x_2(x_2,x_1)x_1x_2(x_2,x_1)x_1x_2(x_2,x_1) \overset{10}{=}$

$x_3(x_3,x_1)x_2x_1(x_2,x_1)x_2(x_2,x_1)x_1x_2(x_2,x_1) \overset{4}{=}$

$x_3(x_3,x_1)x_1x_2(x_2,x_1)(x_2,x_1)x_2(x_2,x_1)x_1x_2(x_2,x_1) \overset{7}{=}$

$x_3(x_3,x_1)x_1x_2x_2(x_2,x_1)x_1x_2(x_2,x_1) \overset{2}{=} x_3(x_3,x_1)x_1(x_2,x_1)x_1x_2(x_2,x_1) \overset{10}{=}$

$x_3(x_3,x_1)x_1x_1(x_2,x_1)x_2(x_2,x_1) \overset{1}{=} x_3(x_3,x_1)(x_2,x_1)x_2(x_2,x_1) \overset{11}{=}$

$x_3(x_3,x_1)x_2(x_2,x_1)(x_2,x_1) \overset{7}{=} x_3(x_3,x_1)x_2 \overset{14}{=} x_3x_2(x_3,x_1) \overset{6}{=} x_2x_3(x_3,x_2)(x_3,x_1) \overset{21}{=}$

$x_2x_3(x_3,x_1)(x_3,x_2) = u(011011,E(3))$

$u(111100,P) = x_1x_3x_1x_1x_2x_1x_1x_1x_3x_2x_2x_2x_1 \overset{1}{=} x_1x_3x_2x_1x_1x_1x_3x_2x_2x_2x_1 \overset{1}{=}$

$x_1x_3x_2x_1x_3x_2x_2x_2x_1 \overset{2}{=} x_1x_3x_2x_1x_3x_2x_1 \overset{4}{=} x_1x_3x_1x_2(x_2,x_1)x_3x_2x_1 \overset{4}{=}$

$x_1x_3x_1x_2(x_2,x_1)x_3x_1x_2(x_2,x_1) \overset{5}{=} x_1x_1x_3(x_3,x_1)x_2(x_2,x_1)x_3x_1x_2(x_2,x_1) \overset{1}{=}$

$x_3(x_3,x_1)x_2(x_2,x_1)x_3x_1x_2(x_2,x_1) \overset{5}{=} x_3(x_3,x_1)x_2(x_2,x_1)x_1x_3(x_3,x_1)x_2(x_2,x_1) \overset{10}{=}$

$x_3(x_3,x_1)x_2x_1(x_2,x_1)x_3(x_3,x_1)x_2(x_2,x_1) \overset{4}{=}$

$x_3(x_3,x_1)x_1x_2(x_2,x_1)(x_2,x_1)x_3(x_3,x_1)x_2(x_2,x_1) \overset{7}{=} x_3(x_3,x_1)x_1x_2x_3(x_3,x_1)x_2(x_2,x_1) \overset{13}{=}$

$x_3x_1(x_3,x_1)x_2x_3(x_3,x_1)x_2(x_2,x_1) \overset{5}{=} x_1x_3(x_3,x_1)(x_3,x_1)x_2x_3(x_3,x_1)x_2(x_2,x_1) \overset{8}{=}$

$x_1x_3x_2x_3(x_3,x_1)x_2(x_2,x_1) \overset{6}{=} x_1x_2x_3(x_3,x_2)x_3(x_3,x_1)x_2(x_2,x_1) \overset{14}{=}$

$x_1x_2x_3(x_3,x_2)x_3x_2(x_3,x_1)(x_2,x_1) \overset{6}{=} x_1x_2x_3(x_3,x_2)x_2x_3(x_3,x_2)(x_3,x_1)(x_2,x_1) \overset{17}{=}$

$x_1x_2x_3x_2(x_3,x_2)x_3(x_3,x_2)(x_3,x_1)(x_2,x_1) \overset{6}{=}$

$x_1x_2x_2x_3(x_3,x_2)(x_3,x_2)x_3(x_3,x_2)(x_3,x_1)(x_2,x_1) \overset{2}{=}$

$x_1x_3(x_3,x_2)(x_3,x_2)x_3(x_3,x_2)(x_3,x_1)(x_2,x_1) \overset{9}{=} x_1x_3x_3(x_3,x_2)(x_3,x_1)(x_2,x_1) \overset{3}{=}$

$x_1(x_3,x_2)(x_3,x_1)(x_2,x_1) \overset{19}{=} x_1(x_3,x_2)(x_2,x_1)(x_3,x_1) \overset{20}{=} x_1(x_2,x_1)(x_3,x_2)(x_3,x_1) \overset{21}{=}$

$x_1(x_2,x_1)(x_3,x_1)(x_3,x_2) = u(100111, E(3))$

$u(100001, P) = x_1x_2x_1x_3x_1x_3x_1 \overset{4}{=} x_1x_1x_2(x_2,x_1)x_3x_1x_3x_1 \overset{1}{=} x_2(x_2,x_1)x_3x_1x_3x_1 \overset{5}{=}$

$x_2(x_2,x_1)x_1x_3(x_3,x_1)x_3x_1 \overset{5}{=} x_2(x_2,x_1)x_1x_3(x_3,x_1)x_1x_3(x_3,x_1) \overset{10}{=}$

$x_2x_1(x_2,x_1)x_3(x_3,x_1)x_1x_3(x_3,x_1) \overset{4}{=} x_1x_2(x_2,x_1)(x_2,x_1)x_3(x_3,x_1)x_1x_3(x_3,x_1) \overset{7}{=}$

$x_1x_2x_3(x_3,x_1)x_1x_3(x_3,x_1) \overset{13}{=} x_1x_2x_3x_1(x_3,x_1)x_3(x_3,x_1) \overset{5}{=}$

$x_1x_2x_1x_3(x_3,x_1)(x_3,x_1)x_3(x_3,x_1) \overset{4}{=} x_1x_1x_2(x_2,x_1)x_3(x_3,x_1)(x_3,x_1)x_3(x_3,x_1) \overset{1}{=}$

$x_2(x_2,x_1)x_3(x_3,x_1)(x_3,x_1)x_3(x_3,x_1) \overset{8}{=} x_2(x_2,x_1)x_3x_3(x_3,x_1) \overset{3}{=} x_2(x_2,x_1)(x_3,x_1) =$

$u(010110, E(3))$

References

[1] Iris Lee Anshel and Michael Anshel. "From the Post-Markov Theorem through Decision Problems to Public-Key Cryptography." *American Mathematical Monthly,* **100** #9 (November 1993), pp. 835–844.

[2] Michael Anshel and Dorian Goldfeld. "Partitions, Egyptian Fractions, and Free Products of Finite Abelian Groups." *Proceedings of the AMS,* **111**, #4 (April 1991), pp. 889-899.

[3] Michael Anshel and Robert Prener. "On Free Products of Finite Abelian Groups." *Proceedings of the AMS,* **34** (1972), pp. 343–345.

[4] Whitfield Diffie and Martin E. Hellman. "New Directions in Cryptography." *IEEE Transactions on Information Theory,* **IT-22**, #6, pp. 644–654, 1976.

[5] M. Hall, Jr. *The Theory of Groups.* New York: Chelsea Publishing Company, 1976.

[6] P. Hall. "A Contribution to the Theory of Groups of Prime Power Order." *Proceedings of London Mathematical Society,* **36**, 1934, 29–95.

[7] Donald Knuth. *Literate Programming.* Stanford: Center for the Study of Language and Information, 1992.

[8] Jan van Leeuwen, ed. *Handbook of Theoretical Computer Science, Vol. A: Algorithms and Complexity.* Cambridge: MIT Press, 1990.

[9] Wilhelm Magnus, Abraham Karrass, Donald Solitar. *Combinatorial Group Theory.* New York: Dover, 1976.

[10] Ueli M. Maurer. "A Universal Statistical Test for Random Bit Generators." *Journal of Cryptology,* **5** (1992), pp. 89–105.

[11] Ueli M. Maurer and James L. Massey. "Cascade Ciphers: the Importance of Being First." *Journal of Cryptology,* **6** (1993), pp. 55-61.

[12] Wayne Patterson. *Mathematical Cryptology for Computer Scientists and Mathematicians.* Totowa, N.J.: Rowman and Littlefield, 1987.

[13] Christos Papadimitriou. *Computational Complexity.* New York: Addison-Wesley, 1994.

[14] Robert Prener. *The Lower Central Series of Special Groups Generated by Elements of Order Two.* Ph.D. Dissertation, The Polytechnic Institute of Brooklyn, 1969.

[15] Charles Sims. "Verifying Nilpotence." *Journal of Symbolic Computations,* **3** (1987), pp. 231–247.

[16] Dennis Spellman, private communications.

[17] Herman V. Waldinger. "A Natural Ordering of Basic Commutators." *Proceedings of the AMS,* **12** (1961), pp. 140–147.

[18] Herman V. Waldinger and Anthony Gaglione. "Factor Groups of the Lower Central series of Free Products of Finitely Generated Abelian Groups." *Proceedings of Groups St. Andrews 1985,* 164–203. Cambridge: Cambridge University Press, 1986.