IBM Research

# GROUP THEORETIC REMARKS ON CRYPTOGRAPHIC SYSTEMS BASED ON TWO TYPES OF ADDITION

Edna Grossman

February 26, 1974

RC 4742



Yorktown Heights, New York

San Jose, California

Zurich, Switzerland

# Group Theoretic Remarks on Cryptographic Systems Based On Two Types of Addition

Edna Grossman

Mathematical Sciences Department
IBM Watson Research Center
Yorktown Heights, New York

ABSTRACT: This paper studies from a group theoretic point of view certain cryptographic systems acting on blocks of n binary digits. The systems in question add to the message block successive blocks of key but the type of addition used alternates between $\oplus$ (add mod 2) and $+$ (add mod $2^n$). It is proved that the totality of such transformations constitutes a group whose order grows exponentially with n. The order of the group in question is $2^{2^{n-1}+n-1}$.

RC 4742 (#21102)
February 26, 1974
Mathematics

Copies may be requested from:
IBM Thomas J. Watson Research Center
Post Office Box 218
Yorktown Heights, New York 10598

## § 1 INTRODUCTION

In this paper we consider certain cryptographic systems which act on blocks of binary data of fixed length n. The general cipher we have in mind successively adds to the message block blocks of binary key. Two different types of addition alternate with each other: addition mod 2 ( $\oplus$ ) and addition mod $2^n$ (+, or "add with carry"). Adding key bits mod 2 to message is just an affine transformation of message space and, as such, would be cryptographically weak. But addition mod $2^n$ is a non-linear function of message and key. It is generally believed that alternating linear with non-linear transformations for many rounds can lead to strong cryptographic systems. In this paper we consider the order of the group of permutations of message space (a set of order $2^n$) generated by the two operations " $\oplus$ key bits" and "+ key bits". We will show that the order of this group is $2^{2^{n-1}+n-1}$, and give interpretations of this result. In a future paper we will examine the structure of this group more closely to see if an opponent could try to attack such a system by such things as elements of low order.

We begin by giving in §2 some general group theoretic background.

## §2 SEMI DIRECT PRODUCTS AND WREATH PRODUCTS

Definition: If $N$ and $Q$ are groups, an extension of $N$ by $Q$ is a group $G$ such that $N \triangleleft G$ ($N$ is a normal subgroup of $G$) and $G/N \cong Q$.

Note that if $G$ is an extension of $N$ by $Q$, $|G| = |N|\ |Q|$. The most well known type of extension is the direct product $N \oplus Q$. In this case we also have $Q$ embedded in $G$ as a normal subgroup and $Q \cap N = 1$.

Def: An extension $G$ of $N$ by $Q$ is a semi-direct product, if $Q \subset G$ (or there is an isomorphic copy of $Q$ embedded in $G$, but not necessarily normally) and $Q \cap N = 1$.

Unlike the direct product, the semi-direct product is not in general unique for any $N$ and $Q$. In order to specify which semi-direct product we have in mind we must specify how elements of $Q$ conjugate elements of $N$. For $q \in Q$, $q: N \to N$, $n \to qnq^{-1}$ since $N$ is normal. Thus, we must give a homomorphism $f: Q \to \mathrm{Aut}(N)$, where $\mathrm{Aut}(N)$ denotes the automorphism group of $N$. It is sufficient to give the value of $f$ on a set of generators $q_1, \ldots, q_k$ of $Q$, and the value $f(q_i)$ being an automorphism of $N$ is specified once we know its action on a set of generators $n_1, \ldots, n_r$ of $N$. Thus we must specify

$q_i n_j q_i^{-1} = W_{ij}(n_1, \ldots n_r)$, $\forall i, j$; here $W_{ij}$ is a word in the generators

$n_1, \ldots, n_r$ of N. Note that $W_{ij}$ cannot be chosen arbitrarily. Two conditions must be met: (1) The assignment $n_j \to W_{ij}(n_1, \ldots, n_r)$ must be an automorphism of N for all i, j, (2) The assignment $q \to \mathrm{Aut}(N)$ must be a homomorphism from Q. If these conditions are met, the semi-direct product $N \times_f Q$ is generated by $n_1, \ldots, n_r, q_1, \ldots, q_k$; the relations of N hold among the $\{n_j\}$, those of Q hold among the $\{q_i\}$, and we need only add the relations $q_i n_j q_i^{-1} = W_{ij}(n_1, \ldots, n_r)$. Note that when the homomorphism $f: Q \to \mathrm{Aut}(N)$ is trivial, $N \times_f Q = N \oplus Q$.

We turn now to the group theoretic construction known as Wreath Products. Suppose A and B are sets on which the groups G and H, respectively, act as permutation groups. The wreath product of G by H, denoted by $G \wr H$ will be defined to be a group of permutations of $A \times B$. For a fixed $\pi \in H$ and an arbitrary function $f: B \to G$ we define the permutation $\sigma_{f,\pi}$ of $A \times B$ by:

$$(a, b)\, \sigma_{f,\pi} = (af(b), b\pi) \ .$$

The collection of all $\sigma_{f,\pi}$ for $\pi \in H$ and $f : B \to G$ forms a group of permutations of $A \times B$, the wreath product of G by H. To see that these permutations form a group consider:

$$(a, b)\, \sigma_{f,\pi}\, \sigma_{g,\rho} = (af(b), b\pi)\, \sigma_{g,\rho} = (af(b)g(b\pi), b\pi\rho)$$

$$= (a, b)\, \sigma_{h,\pi\rho} \ , \quad h : B \to G$$

$$b \to f(b)g(b\pi)$$

$$(a,b)\,\sigma_{f,\pi}\,\sigma_{h,\pi^{-1}} = (a,b)\,, \qquad h: B \to G$$
$$b \to (f(b\pi^{-1}))^{-1}.$$

These equations show closure under multiplication and inversion. Note that $|G \wr H| = |H|\,|G|^{|B|}$.

The wreath product can also be viewed as a semi-direct product of appropriate groups, as we now show. Let $e \in H$ denote the identity permutation. Then $\{\sigma_{f,e} \mid f: B \to G\}$ forms a subgroup of $G \wr H$ which we call $G^*$. Note that $G^* \cong \underbrace{G \oplus \ldots \oplus G}_{|B| \text{ times}}$.

Let $i : B \to G$ be defined by $i(b) = e$ for all $b$, then $\{\sigma_{i,\pi} \mid \pi \in H\}$ forms a subgroup of $G \wr H$ which we call $\bar{H}$. $\bar{H} \cong H$. Note $\bar{H} \cap G^* = 1$. $\bar{H}$ and $G^*$ together generate $G \wr H$ since

$$\sigma_{f,1}\,\sigma_{i,\pi} = \sigma_{f,\pi}\,.$$

In fact $G^* \lhd G \wr H$. To prove this we must show that $G^*$ is stabilized under conjugation by $\bar{H}$. This follows from:

$$\sigma_{i,\pi}^{-1}\,\sigma_{f,1}\,\sigma_{i,\pi} = \sigma_{i,\pi^{-1}}\,\sigma_{f,1}\,\sigma_{i,\pi} = \sigma_{f\circ\pi^{-1},\pi^{-1}}\,\sigma_{i,\pi} = \sigma_{f\circ\pi^{-1},1}\,.$$

When this equation is viewed in terms of the isomorphism of $G^*$ with $\underbrace{G \oplus \ldots \oplus G}_{|B| \text{ times}}$, we have

$$\sigma_{i,\pi}^{-1} (g_b)_{b\in B} \sigma_{i,\pi} = (g_{b\pi^{-1}})_{b\in B} .$$

These remarks show that $G \wr H$ is actually a semidirect product of $\underbrace{G \oplus \dots \oplus G}_{|B| \text{ times}}$ by $H$, with the action of $H$ described by:

$$\pi : G \oplus \dots \oplus G \to G \oplus \dots \oplus G$$

$$(g_b) \qquad \to \qquad (g_{b\pi^{-1}}) \quad , \quad \pi \in H.$$

## § 3 THE SUBGROUPS $T_n$ of $S_{2^n}$

$S_{2^n}$ refers to the symmetric group on $2^n$ symbols, that is the group of all possible permutations of a set of order $2^n$. We will think of this set as the integers $0, 1, \ldots, 2^n-1$ in their binary representation. By $T_n$ we mean the subgroup of $S_{2^n}$ generated by performing the two operations $\oplus$ and $+$.

All operations $+$ can be generated by $+00\ldots1$, which corresponds to the permutation $x = (0\ 1\ 2 \quad\quad 2^n-1)$

(Note: A notation such as (ijk) stands for the permutation $\pi$ for which $i\pi = j$, $j\pi = k$, $k\pi = i$). All operations $\oplus$ can be generated by

$$\begin{array}{l} \oplus \quad 0\ 0\ \ldots\ 1 \\ \oplus \quad 0\ 0\ \ldots\ 10 \\ \vdots \\ \oplus \quad 1\ 0\ \ldots\ 00\ . \end{array}$$

The last operation, however may be omitted as it is equivalent to $+1\ 0\ \ldots\ 0$. These operations correspond to the permutations

$$y_1 = (01)(23)(45)\ldots\ldots$$

$$y_2 = (02)(13)(46)\ldots\ldots$$

$$\vdots$$

$$y_{n-1} = (0\,2^{n-2})(1\ 2^{n-2}+1)\ldots(2^{n-2}-1\ 2^{n-1}-1)(2^{n-1}\ 2^{n-1}+1\ 2^{n-2})\ldots$$
$$(2^{n-1}+2^{n-2}-1 \quad\quad 2^n-1)\ .$$

Theorem : $x, y_1, \ldots, y_{n-1}$ generate a subgroup $T_n$ of $S_{2^n}$ of order $2^{2^{n-1}+n-1}$.

Proof: The proof is inductive in nature and we proceed by examining in detail the situation for low values of n.

If $n = 1$, the subgroup of $S_2 \cong Z_2$ (cyclic group of order 2) we're interested in is just $S_2$ of order $2 = 2^{2^0+0}$.

If $n = 2$, we're interested in the subgroup of $S_4$ generated by $x = (0123)$ and $y = (01)(23)$. It's easy to check that the relations $x^4 = y^2 = 1$ and $y^{-1}xy = x^{-1}$ are satisfied. These are the relations of $D_4$ the dihedral group of order 8. In fact $T_2$ is isomorphic to $D_4$. Every element has a unique expression in the form $x^k y^\epsilon$, $k=0, 1, 2,$ or 3, $\epsilon = 0$ or 1. Note that $8 = 2^{2+1}$. Also note that in this case x generates a normal subgroup of $T_2$.

If $n = 3$, we're interested in the subgroup of $S_8$ generated by

$x = (0\ 1\ 2\ 3\ 4\ 5\ 6\ 7)$

$y_1 = (01)(23)(45)(67)$

$y_2 = (02)(13)(46)(57)$.

Express each number in $\{0, \ldots 7\}$ as $2a+b$ where $a \in \{0, 1, 2, 3\} = A$, $b \in \{0, 1\} = B$. Then $\{0, \ldots, 7\} \cong A \times B$. $T_2$ acts on A and $Z_2$ acts on B. Relabel the generators of $T_2$ to be $s = (0123)$, $t = (01)(23)$. Then we see that $x, y_1, y_2$ are all in $T_2 \wr Z_2$ acting on $A \times B$ as follows:

$x = \sigma_{f,(01)}$ $\quad f: 0 \to e,\ 1 \to s$

$2a \to 2a+1$

$2a+1 \to 2(as)$ ,

$y_1 = \sigma_{i,(01)}$ $\quad i: 0 \to e,\ 1 \to e$

$2a \to 2a+1$

$2a+1 \to 2a$

$y_2 = \sigma_{g,\ e}$ $\quad g: 0 \to t,\ 1 \to t$

$2a \to 2(at)$

$2a+1 \to 2(at)+1$ .

So $T_3 \subset T_2 \wr Z_2$, but which subgroup is it? Viewing $T_2 \wr Z_2$ as a semi-direct product of $T_2 \oplus T_2$ by $Z_2$, we can think of any element of $T_3$ to be of the form

$$(\tau, \tau') \times y_1^{\varepsilon} \qquad\qquad \tau, \tau' \in T_2 \ , \ \varepsilon = 0 \text{ or } 1$$

where the first coordinate, $\tau$, is thought of as acting on the even numbers, $2a$, the second is thought of acting on the odd numbers $2a+1$, and the presence or abscence of $y_1$ tells whether or not the evens and odds are to be switched via $(2a\ \ 2a+1)$. Note that the discussion of extensions and wreath products tells us how to multiply, since

$$y_1 \cdot (\tau, \tau') = (\tau', \tau) \times y_1 \ .$$

In this notation,

$$x = (e, s) \times y_1$$

$$y_1 = (e, e) \times y_1 \cong y_1$$

$$y_2 = (t, t) \qquad .$$

$T_3$ is thus the subgroup of $T_2 \wr Z_2$ generated by $y_1$ and $(e, s)$, $(t, t)$. If $N$ is the subgroup of $T_2 \oplus T_2$ generated by

$$(e, s) \quad , \quad (s, e) \quad , \quad (t, t)$$

then every element of $T_3$ is uniquely expressible in the form

$$n \times y_1^{\varepsilon} \qquad \text{where } n \in N .$$

Therefore $|T_3| = 2|N|$. We are thus left with the problem of determining the order of a subgroup of $T_2 \oplus T_2$. Consider any word in $(e, s)$, $(s, e)$ and $(t, t)$. The subgroup generated by $s$ is normal in $T_2$ and as a result its easy to see that any such word must have the form $(s^k t^{\varepsilon}, s^{\ell} t^{\varepsilon})$ $\varepsilon = 0$ or $1$, $k, \ell = 0, 1, 2$, or $3$. That is, the two components differ only by the power of $s$. This shows that $|N| = 4 \times 4 \times 2$, and $|T_3| = 64 = 2^{2^2+2}$.

Every element is uniquely expressible as

$$(\tau, s^k \tau) \times y_1^{\varepsilon} \qquad \tau \in T_2, \; k = 0, 1, 2, 3, \; \varepsilon = 0, 1 .$$

For general $n$ the situation is analogous but a bit more complicated since in $T_3$, $s = (01234567)$ no longer generates a normal subgroup. Suppose we know $|T_n|$ generated by $s, t_1, \ldots, t_{n-1}$. $T_{n+1}$ is generated by $x, y_1, \ldots, y_n$. Again $T_{n+1} \subseteq T_n \wr Z_2$ acting on $\{0, 1, 2, \ldots 2^n - 1\}$ regarded as $A \times B$, $A = \{0, 1, \ldots 2^{n-1} - 1\}$, $B = \{0, 1\}$.

Again

$$y_1 = \sigma_{i,(01)}$$

$$\begin{aligned} 2a &\to 2a+1 \\ 2a+1 &\to 2a \end{aligned}$$

and in the semi-direct product notation

$$x = (e, s) \times y_1$$

$$y_2 = (t_1, t_1)$$

$$y_3 = (t_2, t_2)$$

$$\vdots$$

$$y_n = (t_{n-1}, t_{n-1}) .$$

$T_{n+1}$ is the subgroup of $T_n \wr Z_2$ generated by

$$y_1, (e, s), (t_1, t_1), \ldots (t_{n-1}, t_{n-1}) .$$

Again we see that every element is uniquely expressible as

$$n \times y_1^{\varepsilon} \quad \varepsilon = 0, 1, \quad n \in N$$

where $N$ is the subgroup of $T_n \oplus T_n$ generated by

$$(e, s) , (s, e) , (t_1, t_1) , \ldots (t_{n-1}, t_{n-1}) .$$

We must therefore compute $|N|$ , since $|T_{n+1}| = 2|N|$ . Any word in the above generators of $N$ will have both components identical as far as the $t_i$ are concerned but the components will differ in the powers of $s$ that are interspersed with the $t_i$. We see then that any such word has the form

$$(\tau, r\tau) \quad \tau \in T_n, \quad r \in R$$

where $R$ is the normal closure of $s$ in $T_n$, i.e. the smallest normal subgroup of $T_n$ containing $s$. $|T_{n+1}| = 2 \times |T_n| \times |R|$ .

How do we compute the order of the normal closure of $s$ in $T_n$? One way is to find its index in $T_n$; that is, to ask what quotient group do we get when we factor out the normal subgroup generated by $s$? This is equivalent to asking what groups results from adding to a presentation for $T_n$ the relation $s = 1$.

$$T_n = \langle s, t_1, \ldots, t_{n-1}; t_i^2 = 1, \ t_i t_j = t_j t_i \ , \ s^{2^n} = 1, \ W_\nu(t_i, s) = 1 \rangle \ .$$

Intuitively we feel that the group we get by adding $s = 1$ is just $Z_2 \underbrace{\oplus \ \ldots \ \oplus}_{n-1 \text{ times}} Z_2$. However, it is possible that if we let $s = 1$ in some $W_\nu(t_i, s)$ we will get a relation such as $t_i t_j^{-1} = 1$ or $t_i = t_j$. If we can prove that this does not occur, then $|T_{n+1}| = 2 \times |T_n| \times \frac{|T_n|}{2^{n-1}} = |T_n|^2 \times 2^{2-n}$. If $|T_j| = 2^{k_j}$ then $k_{n+1} = 2k_n + 2 - n = 2(k_n + 1) - n$ and this yields $k_n = 2^{n-1} + n - 1$, as asserted in the statement of the theorem.

We are left to prove the following assertion: If in $T_j$, $W(y_i, x) = 1$, then $W$ has even exponent sum on each $y_i$.

We prove this inductively. For $T_2 = \langle x, y \mid x^4 = y^2 = 1, \ yxy^{-1}x = 1 \rangle$, this is true.

Assume we have proved the assertion for $T_n$, generated by $\{s, t_i\}$ and wish to verify it for $T_{n+1}$. Note that there is a homomorphism $T_{n+1} \to T_n$. This is because $T_{n+1}$ as a permutation group is imprimitive

we can find a partition of $\{0, 1, \ldots, 2^{n+1}-1\}$ into sets of equal size such that each permutation in $T_{n+1}$ permutes these sets as entities. More specifically, the subsets $\{0, 2^n\}$, $\{1, 2^n+1\}, \ldots \{2^n-1, 2^{n+1}-1\}$ are permuted as sets by $T_{n+1}$. $T_{n+1}$ thus can be mapped onto a group of permutations of $2^n$ symbols. In fact under this homomorphism we have:

$$x \to s$$

$$y_1 \to t_1$$

$$y_2 \to t_2$$

$$y_{n-1} \to t_{n-1}$$

$$y_n \to s^{2^{n-1}} \quad .$$

Then if $W(x, y_1, \ldots, y_n) = 1$ in $T_{n+1}$, we would have

$W(s, t_1, \ldots, t_{n-1}, s^{2^{n-1}}) = 1 = W'(s, t_1, \ldots, t_{n-1})$ in $T_n$. But $W$ and $W'$ have the same exponent sums on $t_1, \ldots, t_{n-1}$ and by induction these sums are all even. This means $W$ has even exponent sum on $y_1, \ldots, y_{n-1}$. The only case left to consider is if $W(x, y_i)$ reduces to $y_n = 1$, upon addition of $x = 1$. This would mean that $y_n$ is in the normal closure of $x$ in $T_{n+1}$. $y_n$ has the form $(t_{n-1}, t_{n-1})$, and $x$ has the form $(e, s) \times y_1$. Any element in the normal closure of $x$ will be

$\prod_1^{\ell} W_i^{-1} x^{k_i} W_i$, $W_i \in T_{n+1}$. But

$$x^k = \begin{cases} (s^r, s^r) & k = 2r \\ (s^r, s^{r+1}) \times y_1 & k = 2r+1 \end{cases} .$$

If $W = (N\tau, \tau) \times y_1^\delta$ is an arbitrary element of $T_{n+1}$ with $N$ in the normal closure of $s$ in $T_n$, then in every case $W^{-1} x^k W = (L, M) \times y_1^\varepsilon$ where $L$, $M$ are in the normal closure of $s$ in $T_n$. Then $\prod_1^\ell W_i^{-1} x^{k_i} W_i = (L, M) \times y_1^\varepsilon$, and if $(L, M) \times y_1^\varepsilon = (t_{n-1}, t_{n-1})$ then $\varepsilon = 0$ and $t_{n-1}$ is in the normal closure of $s$ in $T_n$. This contradicts the inductive hypothesis.

## § 4 CRYPTOGRAPHIC INTERPRETATIONS

If we were to build a cryptographic system based merely on $+$ and $\oplus$ and if we were to run it as many rounds as necessary to generate the full group then the security of the system would be good - against a deterministic attack. The key would in fact have $2^{n-1}+n-1$ bits and if an opponent had corresponding input-output pairs each one could give him at most $n$ bits of information. He would need at least $\frac{2^{n-1}+n-1}{n} \cong \frac{2^{n-1}}{n}$ corresponding pairs to break the system. However, the number of rounds we would have to go through to generate the entire group grows exponentially with $n$ as well and it would be infeasible to build such a system. It would be a very difficult problem to decide how large a set of transformations is obtained by limiting the device to a fixed number, $k$, of rounds. The set of transformations in question would no longer form a group or even a semi-group and the usual algebraic methods could not be used.

We must also note that while $|T_n| = 2^{2^{n-1}+n-1}$, $|S_{2^n}| = 2^n!$. Even though $|T_n|$ grows exponentially with $n$, $T_n$ becomes a smaller and smaller part of $S_{2^n}$. In fact, the 2-sylow subgroups of $S_{2^n}$ (subgroups with order a maximal power of 2) have order $2^{2^n-1}$, so that as $n$ gets large, $T_n$ becomes a smaller and smaller part of the 2-sylow subgroup in which it's contained. This suggests that there might be a basis for a

statistical type analysis of such a system which would work no matter how many rounds the system were allowed to run. This possibility will be explored in future work.