A MODIFICATION OF A BROKEN PUBLIC-KEY CIPHER

John J. Cade
24 Ginn Rd.
Winchester, MA 01890

Abstract

A possible public-key cipher is described and its security against various cryptanalytic attacks is considered.

1. Introduction

In this paper, we describe a possible public-key cipher. It is a modification of the public-key cipher that was proposed by the author [2] in April 1985, was broken by Berkovits [1] in August 1985, and was broken independently by James, Lidl, and Niederreiter [3] in October 1985.

This modified cipher, like the original, is a block substitution cipher that operates on binary messages. With this cipher, for a suitably large value of n, n-blocks of binary digits are identified with elements of the finite field $GF(2^n)$, and elements of $GF(2^n)$ are enciphered by means of a permutation of $GF(2^n)$ whose public description is as a polynomial function on $GF(2^n)$ which has a very high degree but only a few terms.

We consider several possible cryptanalytic attacks against the cipher. The most obvious attack consists of solving the polynomial equations of high degree over $GF(2^n)$ which relate corresponding n-blocks of plaintext and ciphertext. Another possible attack consists of solving the system of polynomial equations of high degree over $GF(2^n)$ that expresses the public key for the enciphering permutation in terms of secret trapdoor information about this permutation.

A.M. Odlyzko (Ed.): Advances in Cryptology - CRYPTO '86, LNCS 263, pp. 64-83, 1987.

For each cryptanalytic attack that we consider, we give an estimate of the amount of computation required as a function of the cipher's block-length n. The estimates for all but one of the attacks are based on fairly complete and satisfying analyses of the attacks in question. Unfortunatley, however, for the attack by solving the system of equations that expresses the public key in terms of trapdoor information, the estimate is based only on indirect evidence obtained by an analysis of a simpler related system of equations. This attack will require further study, perhaps with the aid of a computer algebra system. On the basis of the estimates of the amounts of computation required by the various cryptanalytic attacks, it appears that the cipher provides adequate security with a block-length of $n \geq 150$.

This paper is organized as follows. In section 2 below, we describe our modified cipher. In section 3, we prove that the enciphering and deciphering permutations used in the cipher are indeed mutually inverse permutations. In sections 4 - 6, we describe various methods of cryptanalyzing the cipher and we estimate the amounts of computation required by these methods. Finally, in section 7, we summarize these estimates and use them to determine a suitable block-length for the cipher.

2. Description of the cipher

Our cipher is designed to encipher binary messages. Each such message is enciphered one n-block at a time, for a specified block-length n, by substituting for each plaintext n-block x a corresponding ciphertext n-block y which is given by $y = P(x)$, where P is a certain kind of permutation of the set of all binary n-blocks.

Because of the particular form of the enciphering permutations used in the cipher, the block-length n must be an integer for which there exist integers δ, γ, and β such that $n = 2\delta$ and $\delta = 2\gamma = 3\beta$. Note that an integer n satisfies this requirement if and only if n is a multiple of 12. In the following, n, δ, γ, and β are understood to be as just described.

For the operation of the cipher, the set of all binary n-blocks must be identified in some specified way with the finite field $GF(2^n)$. Then the public description of the enciphering permutation P consists of a 16-term polynomial formula for P having the form

$$P(x) = \sum_{g=0}^{3} \sum_{h=0}^{3} p_{gh} x^{2^{\gamma g+\beta} + 2^{\gamma h}}. \tag{2.1}$$

The coefficients p_{gh} in this formula are publicly revealed elements of $GF(2^n)$ which constitute the public key for P.

Although P is a polynomial function of very high degree, P(x) can nevertheless be computed quite efficiently for each $x \in GF(2^n)$. One way to do this is to use formula (2.1) written in the form

$$P(x) = \sum_{h=0}^{3} \left(\sum_{g=0}^{3} p_{gh} x^{2^{\gamma g+\beta}} \right) x^{2^{\gamma h}}$$

and to compute the powers of x of the form x^{2^k} apearing in this formula by doing k successive squarings. Computing P(x) this way requires a total of just (11/12)n squarings, 20 multiplications, and 15 additions in $GF(2^n)$.

P(x) can be computed even more efficiently by using matrix-vector multiplication to compute various quantities which are the values of linear functions on $GF(2^n)$, where $GF(2^n)$ is regarded as a vector space over its smallest subfield GF(2). To compute P(x) this way, first compute the quantities $u_0, \ldots, u_3$ and v_1, v_2, v_3 given by

$$u_h = \sum_{g=0}^{3} p_{gh} x^{2^{\gamma g+\beta}}, \text{ for } h = 0, \ldots, 3,$$

and $v_h = x^{2^{\gamma h}}$, for h = 1, 2, 3. Each of these quantities is a GF(2)-linear function of x, and so can be computed by doing a single matrix-vector multiplication involving an n x n matrix over GF(2) and an n-element vector over GF(2). Then compute P(x) by using the formula

$$P(x) = u_0x + \sum_{h=1}^{3} u_h v_h.$$

Computing $P(x)$ this way requires a total of just 7 matrix-vector multiplications over $GF(2)$, together with 4 multiplications and 3 additions in $GF(2^n)$.

For the construction of enciphering permutations, $GF(2^n)$ and its subfield $GF(2^\delta)$ are regarded as vector spaces, of dimensions 4 and 2 respectively, over their common subfield $GF(2^\gamma)$. To construct an enciphering permutation, one first chooses at random two secret bases a_1, $\ldots$, a_4 and $b_1, \ldots, b_4$ of $GF(2^n)$ over $GF(2^\gamma)$. One also chooses a basis e_1, e_2 of $GF(2^\delta)$ over $GF(2^\gamma)$. This last basis need not be kept secret and can be chosen to be whatever is most convenient. The sequence $a_1, \ldots, a_4, b_1, \ldots, b_4, e_1, e_2$ formed by these three bases constitutes secret trapdoor information about an enciphering permutation P that is specified by this sequence. We will call this sequence a trapdoor sequence for the permutation P.

This permutation is constructed as follows. First, let S_1 and S_2 be the $GF(2^\gamma)$-linear functions from $GF(2^\delta)$ into $GF(2^n)$ such that $S_1(e_j) = a_j$ and $S_2(e_j) = a_{j+2}$, for $j = 1, 2$. Next, let T_1 and T_2 be the $GF(2^\gamma)$-linear functions from $GF(2^n)$ into $GF(2^\delta)$ such that

$$T_1(b_j) = \begin{cases} e_j, & \text{for } j = 1, 2 \\ 0, & \text{for } j = 3, 4 \end{cases}$$

and

$$T_2(b_j) = \begin{cases} 0, & \text{for } j = 1, 2 \\ e_{j-2}, & \text{for } j = 3, 4. \end{cases}$$

Finally, let M be the permutation of $GF(2^\delta)$ given by

$$M(x) = x^{2^\beta+1}. \qquad (2.2)$$

Then the enciphering permutation P specified by the trapdoor sequence $a_1, \ldots, a_4, b_1, \ldots, b_4, e_1, e_2$ is the function from $GF(2^n)$ into $GF(2^n)$ given by

$$P(x) = S_1MT_1(x) + S_2MT_2(x). \qquad (2.3)$$

Here and in the following, we denote the composition of two or more functions by the juxtaposition of their symbols. Thus, for $i = 1, 2$,

$$S_iMT_i(x) = S_i \circ M \circ T_i(x) = S_i(M(T_i(x))).$$

We note that the enciphering permutation P just described does not determine a unique trapdoor sequence which specifies it. Indeed, it can be shown that for each enciphering permutation, there are a very large number of trapdoor sequences which specify it.

For the public description of the enciphering permutation P described above, P must be expressed as a polynomial function. To do this, first the functions S_i and T_i are expressed as polynomial functions. The functions S_i are given by the polynomial formulas

$$S_i(x) = a_{i0}x + a_{i1}x^{2^{\gamma}}, \tag{2.4}$$

where the coefficients a_{ik} are the elements of $GF(2^n)$ uniquely determined by the system of linear equations

$$a_{i0}e_j + a_{i1}e_j^{2^{\gamma}} = S_i(e_j), \text{ for } j = 1, 2.$$

The functions T_i are given by the polynomial formulas

$$T_i(x) = \sum_{k=0}^{3} b_{ik}x^{2^{\gamma k}}, \tag{2.5}$$

where the coefficients b_{ik} are the elements of $GF(2^n)$ uniquely determined by the system of linear equations

$$\sum_{k=0}^{3} b_{ik}b_j^{2^{\gamma k}} = T_i(b_j), \text{ for } j = 1, \ldots, 4.$$

Once the elements a_{ik} and b_{ik} have been determined, the enciphering permutation P is given by the polynomial formula (2.1), where the coefficients p_{gh} are given by

$$p_{gh} = \sum_{i=1}^{2} \sum_{k=0}^{1} a_{ik}(b_{i,g-k})^{2^{\gamma k+\beta}}(b_{i,h-k})^{2^{\gamma k}}, \tag{2.6}$$

where $b_{i,-1} = b_{i,3}$, for $i = 1, 2$.

We note that this polynomial formula for P can be derived by substituting the polynomial formulas (2.4), (2.5), and (2.2) for the functions S_i, T_i, and M into formula (2.3) and expanding the resulting expression for $P(x)$ as a polynomial in x, taking into account that repeated squarings are automorphisms of $GF(2^n)$, and using the identity $x^{2^n} = x$ to reduce the degree of this polynomial to less than 2^n. We also note that the coefficients a_{ik} and b_{ik} in the polynomial formulas (2.4) and (2.5) for the functions S_i and T_i must be kept secret because a trapdoor sequence for P can be computed from them quite easily.

To decipher a message which has been enciphered using the enciphering permutation P, each ciphertext n-block y is replaced by the corresponding plaintext n-block x which is given by $x = P^{-1}(y)$, where P^{-1} is the inverse of the permutation P. To obtain a formula for the deciphering permutation P^{-1}, one must know a trapdoor sequence $a_1, \ldots, a_4, b_1, \ldots, b_4, e_1, e_2$ for P. The permutation P^{-1} is specified by this trapdoor sequence as follows. Let U_1 and U_2 be the $GF(2^\gamma)$-linear functions from $GF(2^\delta)$ into $GF(2^n)$ such that $U_1(e_j) = b_j$ and $U_2(e_j) = b_{j+2}$, for $j = 1, 2$. Let V_1 and V_2 be the $GF(2^\gamma)$-linear functions from $GF(2^n)$ into $GF(2^\delta)$ such that

$$V_1(a_j) = \begin{cases} e_j, & \text{for } j = 1, 2 \\ 0, & \text{for } j = 3, 4 \end{cases}$$

and

$$V_2(a_j) = \begin{cases} 0, & \text{for } j = 1, 2 \\ e_{j-2}, & \text{for } j = 3, 4. \end{cases}$$

Finally, let M^{-1} be the inverse of the permutation M of $GF(2^\delta)$, which means that M^{-1} is given by

$$M^{-1}(y) = y^\epsilon, \tag{2.7}$$

where $\epsilon = 2^{\beta-1}(2^{2\beta} + 2^\beta - 1)$. Then the deciphering permutation P^{-1} is given by

$$P^{-1}(y) = U_1M^{-1}V_1(y) + U_2M^{-1}V_2(y). \tag{2.8}$$

Like the functions S_i and T_i, the functions U_i and V_i can be expressed as polynomial functions. The functions U_i are given by the polynomial formulas

$$U_i(y) = c_{i0}y + c_{i1}y^{2^\gamma}, \tag{2.9}$$

where the coefficients c_{ik} are the elements of $GF(2^n)$ uniquely determined by the system of linear equations

$$c_{i0}e_j + c_{i1}e_j^{2^{\gamma}} = U_i(e_j), \text{ for } j = 1, 2.$$

The functions V_i are given by the polynomial formulas

$$V_i(y) = \sum_{k=0}^{3} d_{ik}y^{2^{\gamma k}}, \tag{2.10}$$

where the coefficients d_{ik} are the elements of $GF(2^n)$ uniquely determined by the system of linear equations

$$\sum_{k=0}^{3} d_{ik}a_j^{2^{\gamma k}} = V_i(a_j), \text{ for } j = 1, \ldots, 4.$$

The coefficients c_{ik} and d_{ik} in the polynomial formulas (2.9) and (2.10) for the functions U_i and V_i can be regarded as a secret private key for the deciphering permutation P^{-1}.

$P^{-1}(y)$ can be computed for each $y \in GF(2^n)$ by using formula (2.8) together with the polynomial formulas (2.9), (2.10), and (2.7) for the functions U_i, V_i, and M^{-1}. An efficient way of doing this is based on the following formula:

$$M^{-1}V_i(y) = V_i(y)^{2^{3\beta-1}} V_i(y)^{2^{2\beta-1}} / V_i(y)^{2^{\beta-1}}$$

$$= \frac{\left(\sum_{k=0}^{3} (d_{i,k-1})^{2^{3\beta-1}} y^{2^{\gamma k+\gamma-1}}\right)\left(\sum_{k=0}^{3} (d_{i,k-1})^{2^{2\beta-1}} y^{2^{\gamma k+\alpha-1}}\right)}{\sum_{k=0}^{3} (d_{ik})^{2^{\beta-1}} y^{2^{\gamma k+\beta-1}}},$$

where $d_{i,-1} = d_{i,3}$ and $\alpha = n/12$. To compute $P^{-1}(y)$ efficiently using this formula, first compute the quantities z_1 and z_2 given by $z_i = M^{-1}V_i(y)$ by using the above formula and computing the powers of y of the form y^{2^k} appearing in this formula by doing k successive squarings. Then compute the quantities $U_i(z_i)$ by using the polynomial formulas (2.9) for the functions U_i and again computing powers of the z_i by repeated squaring. Finally, compute $P^{-1}(y)$ by adding $U_1(z_1)$ and $U_2(z_2)$. Computing $P^{-1}(y)$ this way requires a total of just $(3/2)n - 1$ squarings, 30 multiplications, 2 divisions, and 21 additions in $GF(2^n)$.

$P^{-1}(y)$ can be computed even more efficiently by making use of matrix-vector multiplication. To compute $P^{-1}(y)$ this way, first compute the quantities t_i, u_i, and v_i for $i = 1, 2$, where these quantities are given by $t_i = V_i(y)^{2^{3\beta-1}}$, $u_i = V_i(y)^{2^{2\beta-1}}$, and $v_i = V_i(y)^{2^{\beta-1}}$. Each of these quantities is a GF(2)-linear function of y, and so can be computed by doing a single matrix-vector multiplication over GF(2). Next, compute the quantities w_1 and w_2 given by $w_i = M^{-1}V_i(y) = t_i u_i/v_i$. Then compute $U_1(w_1)$ and $U_2(w_2)$. For each i, the quantity $U_i(w_i)$ is a GF(2)-linear function of w_i, and so can be computed by doing a single matrix-vector multiplication over GF(2). Finally, compute $P^{-1}(y)$ by adding $U_1(w_1)$ and $U_2(w_2)$. Computing $P^{-1}(y)$ this way requires a total of just 8 matrix-vector multiplications over GF(2), together with 2 multiplications, 2 divisions, and 1 addition in $GF(2^n)$.

For the security of the cipher, the trapdoor sequences used should be such that all the coefficients p_{gh}, a_{ik}, b_{ik}, c_{ik}, and d_{ik} in the polynomial formulas (2.1), (2.4), (2.5), (2.9), and (2.10) for the functions P, S_i, T_i, U_i, and V_i are nonzero. It can be shown that, given any basis e_1, e_2 of $GF(2^\delta)$ over $GF(2^\gamma)$, if elements $a_1, \ldots, a_4$, $b_1, \ldots, b_4$ are chosen at random from $GF(2^n)$, then it is virtually certain that $a_1, \ldots, a_4$ and $b_1, \ldots, b_4$ will both form bases of $GF(2^n)$ over $GF(2^\gamma)$ and that the sequence $a_1, \ldots, a_4, b_1, \ldots, b_4, e_1, e_2$ will form a trapdoor sequence that satisfies the security requirements just stated.

3. Invertibility of the enciphering and deciphering permutations

We now show that the enciphering and deciphering permutations given by formulas (2.3) and (2.8), respectively, are indeed mutually inverse permutations of $GF(2^n)$.

Since the invertibility of these functions depends on the invertibility of the function M given by formula (2.2), we first indicate why this function is a permutation of $GF(2^\delta)$ and why M^{-1} is given by formula (2.7). Using the Euclidean algorithm and the relation $\delta = 3\beta$, it can be calculated that $\gcd(2^{\delta} - 1, 2^{\beta} + 1) = 1$. Hence there exist numbers ϵ satisfying the congruence $(2^{\beta} + 1)\epsilon \equiv 1 \bmod(2^{\delta} - 1)$. If ϵ is any positive solution of this congruence, then it follows from the identity $x^{2^{\delta}-1} = 1$, which is satisfied by all nonzero $x \in GF(2^{\delta})$, that $M(x)^{\epsilon} = x^{(2^{\beta}+1)\epsilon} = x$ for all $x \in GF(2^{\delta})$. Thus M is a permutation of $GF(2^{\delta})$, and M^{-1} is given by $M^{-1}(y) = y^{\epsilon}$, where ϵ is any positive solution of the above congruence. It follows that M^{-1} is given by formula (2.7) provided that the number ϵ appearing in this formula satisfies the condition just given. The Euclidean algorithm calculations mentioned above can be used to find all the solutions of the congruence above. Of these solutions, the least positive one is exactly the number $\epsilon = 2^{\beta-1}(2^{2\beta} + 2^{\beta} - 1)$ appearing in formula (2.7). Thus M^{-1} is indeed given by formula (2.7).

Proposition. The enciphering function P given by formula (2.3) is a permutation of $GF(2^n)$ and the inverse of this permutation is the deciphering function given by formula (2.8).

Proof. Let Q denote the function on $GF(2^n)$ defined by formula (2.8). To prove the proposition, it suffices to show that $QP(x) = x$ for all $x \in GF(2^n)$. Let $a_1, \ldots, a_4, b_1, \ldots, b_4, e_1, e_2$ be a trapdoor sequence for P that specifies the $GF(2^{\gamma})$-linear functions S_i, T_i, U_i, and V_i appearing in formulas (2.3) and (2.8). Let X_1 and X_2 be the $GF(2^{\gamma})$-subspaces of $GF(2^n)$ spanned by b_1, b_2 and by b_3, b_4, respectively, and let Y_1 and Y_2 be the $GF(2^{\gamma})$-subspaces of $GF(2^n)$ spanned by a_1, a_2 and by a_3, a_4, respectively. Then $GF(2^n) = X_1 \oplus X_2 = Y_1 \oplus Y_2$. Now suppose that $x \in GF(2^n)$ is given, and let x_1 and x_2 be the unique elements of X_1 and X_2, respectively, such that $x = x_1 + x_2$. Then, for $i = 1, 2$,

$$T_i(x) = T_i(x_1 + x_2) = T_i(x_1) + T_i(x_2) = T_i(x_i),$$

where the last equality holds because $T_1(X_2) = T_2(X_1) = 0$ by the definition of the functions T_i. Also T_i maps X_i one-to-one onto $GF(2^{\delta})$,

M is a permutation of $GF(2^\delta)$, and S_i maps $GF(2^\delta)$ one-to-one onto Y_i, so S_iMT_i maps X_i one-to-one onto Y_i. Thus, letting $y_i = S_iMT_i(x_i)$, we have $P(x) = y_1 + y_2$, with $y_i \in Y_i$. Next, to compute $QP(x)$, we note that, for $i = 1, 2$,

$$V_iP(x) = V_i(y_1 + y_2) = V_i(y_1) + V_i(y_2) = V_i(y_i),$$

where the last equality holds because $V_1(Y_2) = V_2(Y_1) = 0$ by the definition of the functions V_i. Hence

$$QP(x) = U_1M^{-1}V_1(y_1) + U_2M^{-1}V_2(y_2)$$
$$= U_1M^{-1}V_1S_1MT_1(x_1) + U_2M^{-1}V_2S_2MT_2(x_2).$$

Also both V_iS_i and $M^{-1}M$ are the identity map on $GF(2^\delta)$, and U_iT_i is the identity map on X_i, so $U_iM^{-1}V_iS_iMT_i(x_i) = x_i$. Hence, for all $x \in GF(2^n)$, $QP(x) = x_1 + x_2 = x$. Thus P is a permutation of $GF(2^n)$, and $P^{-1} = Q$. <u>Q.E.D.</u>

<u>4. Cryptanalysis by solving the equation $P(x) = y$</u>

In this section and the next two sections, we describe some possible methods of cryptanalyzing our cipher by using public information about the enciphering permutation. For each method that we consider, we give an estimate of the amount of computation needed.

The first cryptanalytic attack that we consider consists of solving a given ciphertext message, enciphered using a known enciphering permutation P, by solving the equation $P(x) = y$ for each ciphertext n-block y to find the corresponding plaintext n-block x. We consider two methods of solving the equation $P(x) = y$. The first method is an exhaustive search procedure, while the second method is algebraic in nature.

The exhaustive search procedure that we consider for solving the equation $P(x) = y$ depends on the easily proved identity $P(wz) = M(w)P(z)$, which holds for all $w \in GF(2^\gamma)$ and $z \in GF(2^n)$. In view of this identity, if a nonzero $z \in GF(2^n)$ can be found such that $y/P(z) \in GF(2^\gamma)$, then the desired n-block x such that $P(x) = y$ is given by $x = M^{-1}(y/P(z))z$. A nonzero $z \in GF(2^n)$ has the property just described if and only if $(y/P(z))^{2^\gamma} = y/P(z)$. Such an element z can be found by an exhaustive search in which elements of $GF(2^n)$ are tested one-by-one until one is found that satisfies this last condition. A minimal subset of $GF(2^n)$ that is certain to contain an element z of the desired kind contains exactly one element of each different subset of $GF(2^n)$ of the form $\{wt\colon w \in GF(2^\gamma),\ w \neq 0\}$, where t is a nonzero element of $GF(2^n)$. There are approximately $2^{(3/4)n}$ such subsets of $GF(2^n)$, so the desired element z can be found after at most $2^{(3/4)n}$ trials. We will regard each trial needed to find this element z as a single operation. Then it follows that at most approximately $2^{(3/4)n}$ operations are required to solve the equation $P(x) = y$ by the exhaustive search procedure just described.

The second method that we consider for solving the equation $P(x) = y$ is to regard this equation as a polynomial equation in x and to solve this equation algebraically. It appears that the most efficient way of doing this is to use the Euclidean algorithm to compute the polynomial in x which is the greatest common divisor of the polynomials $P(x) - y$ and $x^{2^n} - x$. To see what this accomplishs, note that, since P is a permutation of $GF(2^n)$, the polynomial $P(x) - y$ has a unique root $x = r$ in $GF(2^n)$, and hence has a unique linear factor $x - r$ over $GF(2^n)$. On the other hand, the polynomial $x^{2^n} - x$ is the product of all the linear factors $x - a$, with $a \in GF(2^n)$. Hence the greatest common divisor of $P(x) - y$ and $x^{2^n} - x$ is exactly the linear factor $x - r$ such that $x = r$ is the desired solution of the equation $P(x) = y$. Thus to solve the equation $P(x) = y$, it is only necessary to compute this greatest common divisor. Using the Euclidean algorithm to do this, the required number of multiplications and divisions in $GF(2^n)$ is at most approximately $(\deg(P))^2/2$. Thus we conclude that the equation $P(x) = y$ can be solved algebraically using the method just described by doing at most approximately $2^{(11/6)n-1}$ operations.

5. Cryptanalysis by determining a polynomial or rational formula for P^{-1}

Next, we consider a method of cryptanalyzing the cipher that consists of determining a formula for the deciphering permutation P^{-1} by using public information about the enciphering permutation P. We describe two formulas for P^{-1} that can be determined this way. The first formula expresses P^{-1} as a polynomial function, while the second formula expresses P^{-1} as a rational function, that is, as a quotient of two polynomial functions. We describe how each of these formulas can be obtained and we give estimates of the amounts of computation needed to do this.

First, we describe how a polynomial formula for P^{-1} can be obtained. It can be shown that P^{-1} can be expressed as a polynomial function of the form

$$P^{-1}(y) = \sum_{k \in K} w_k y^k,$$

where the coefficients w_k are elements of $GF(2^n)$, the index set K is a subset of the set $\{0, \ldots, 2^n - 1\}$ which can be completely specified, and the number of elements in the set K satisfies $2^{n/3} \leq |K| \leq 2^{n/3+2}$. This formula for P^{-1} can be regarded as a system of 2^n linear equations which uniquely determines the coefficients w_k in the formula. By making the substitution $y = P(x)$ in this formula, an equivalent system of 2^n linear equations can be obtained which have the form

$$\sum_{k \in K} w_k P(x)^k = x.$$

Note that this second system of equations can be formulated using only public information about the enciphering permutation P. Since the rank of this second system is the same as the rank of the original system, which is $|K|$, and since $|K| < 2^n$, it follows that this second system can be reduced to a smaller system formed from it by choosing any subset of $|K|$ independent equations. We will assume that such a smaller system can be obtained without any significant computational effort, which may well be the case. Then the determination of the coefficients w_k in the polynomial formula for P^{-1} reduces to solving this smaller system of equations. This system consists of $|K|$ equations in $|K|$ unknowns, so to solve it requires at most approximately $|K|^3/3$ operations consisting of multiplications and divisions in $GF(2^n)$. Hence, since $|K| \geq 2^{n/3}$, we conclude that it takes at most approximately $(2^n)/3$ operations to solve for the coefficients w_k, and thus to determine a polynomial formula for P^{-1}.

Next, we describe how a rational formula for P^{-1} can be obtained. The rational formula that we consider has the same form as the rational formula for P^{-1} that is obtained by expanding formula (2.8) for $P^{-1}(y)$ as a rational function of y, making use of the polynomial formulas (2.9) and (2.10) for the functions U_i and V_i described in section 2, and expressing the function M^{-1} by the rational formula $M^{-1}(y) = y\ /y$, where $\zeta = 2^{\beta-1}(2^{2\beta} + 2^{\beta})$ and $\eta = 2^{\beta-1}$. The rational formula for P^{-1} just described has the form $P^{-1}(y) = Q(y)/R(y)$, where Q and R are both nonconstant polynomial functions, $Q(0) = 0$, and $R(y) \neq 0$ for all nonzero $y \in GF(2^n)$. Furthermore, it can be shown that Q and R are given by polynomial formulas having the forms

$$Q(y) = \sum_{k \in K_Q} w_Q(k) y^k$$

and

$$R(y) = \sum_{k \in K_R} w_R(k) y^k,$$

where the coefficients $w_Q(k)$ and $w_R(k)$ are elements of $GF(2^n)$, the index sets K_Q and K_R are subsets of the set $\{0, \ldots, 2^n - 1\}$ which can be completely specified, and the numbers of elements in the sets K_Q and K_R satisfy $2^{n/3} \leq |K_Q| \leq 2^{n/3+3} + 64$ and $4 \leq |K_R| \leq 16$. Now if the formula $P^{-1}(y) = Q(y)/R(y)$ is rewritten as $P^{-1}(y)R(y) - Q(y) = 0$, if the substitution $y = P(x)$ is made, and if the above polynomial formulas for the functions Q and R are used, then the result is the equation

$$\sum_{k \in K_R} x w_R(k) P(x)^k - \sum_{k \in K_Q} w_Q(k) P(x)^k = 0$$

which holds for all $x \in GF(2^n)$. This equation can be regarded as a system of 2^n homogeneous linear equations that are satisfied by the elements $w_Q(k)$ and $w_R(k)$ and that can be formulated using only public information about the enciphering permutation P. Conversely, if a set of elements $w_Q(k)$ and $w_R(k)$ of $GF(2^n)$ forms a nonzero solution of this system of equations and if the functions Q and R on $GF(2^n)$ are defined by the polynomial formulas given above, then the function R is not identically zero and P^{-1} is given by the rational formula $P^{-1}(y) = Q(y)/R(y)$ for all $y \in GF(2^n)$ such that $R(y) \neq 0$. Thus a rational formula for P^{-1} can be obtained by finding a nonzero solution of the system of linear equations given above, and furthermore such solutions exist.

Since the rank of this system of 2^n equations is at most $|K_Q| + |K_R| - 1$, which is less than 2^n, this system can be reduced to a smaller system which has the same rank and consists of equations chosen from the original system. We will assume that such a smaller system consisting of $|K_Q| + |K_R| - 1$ equations can be obtained from the original system without any significant computational effort. Then the determination of the coefficients $w_Q(k)$ and $w_R(k)$ in a rational formula for P^{-1} reduces to solving this smaller system of $|K_Q| + |K_R| - 1$ linear equations in $|K_Q| + |K_R|$ unknowns, which takes at most approximately $(|K_Q| + |K_R|)^3/3$ operations. Hence, since $|K_Q| + |K_R| > 2^{n/3}$, we conclude that it takes at most approximately $(2^n)/3$ operations to determine a rational formula for P^{-1} of the kind described above.

6. Cryptanalysis by finding a trapdoor sequence

The last method of cryptanalysis that we consider consists of using the public key for a given enciphering permutation P to determine a trapdoor sequence for it. We consider two ways of finding such a sequence: first by exhaustive search, and second by solving the system of equations (2.6) algebraically. We describe how each of these approachs might be carried out and we give estimates of the amounts of computation required.

The most efficient exhaustive search procedure for finding a trapdoor sequence for P appears to be as follows. First, choose the elements e_1, e_2 of the sequence to be any convenient basis of $GF(2^\delta)$ over $GF(2^\gamma)$. Next, test one-by-one bases $b_1, \ldots, b_4$ of $GF(2^n)$ over $GF(2^\gamma)$ until a basis is found which is the $b_1, \ldots, b_4$ part of a trapdoor sequence for P whose e_1, e_2 elements are the ones just chosen. To test a given basis $b_1, \ldots, b_4$ for this property, let the $GF(2^\gamma)$-linear functions T_1 and T_2 be defined in terms of $b_1, \ldots, b_4, e_1, e_2$ as described in section 2, and solve for the coefficients b_{ik} in the polynomial formulas for these functions given by equation (2.5). Next, find all the solutions for the elements a_{ik} in the system of equations (2.6). Note that these solutions can be found by linear algebra, since this system is linear in the a_{ik}. The solutions, if any, of this system are then tested one-by-one to determine whether any of them is such that $GF(2^n)$ can be expressed as $GF(2^n) = S_1(GF(2^\delta)) + S_2(GF(2^\delta))$, where S_1 and S_2 are the $GF(2^\gamma)$-linear functions from $GF(2^n)$ into $GF(2^n)$ defined in terms of the elements a_{ik} by formula (2.3). Now the basis $b_1, \ldots, b_4$, which is being tested for the property of being the $b_1, \ldots, b_4$ part of a trapdoor sequence for P whose e_1, e_2 elements are the ones chosen, has this property if and only if there exists a set of elements a_{ik} that satisfies the system of equations (2.5) and that satisfies the condition stated above. As soon as such a basis $b_1, \ldots, b_4$ and a set of elements a_{ik} has been found, a complete trapdoor sequence for P can be produced. The $b_1, \ldots, b_4, e_1, e_2$ part has already been obtained, and the $a_1, \ldots, a_4$ part of the sequence is given by $a_j = S_1(e_j)$, for $j = 1, 2$, and by $a_j = S_2(e_{j-2})$, for $j = 3, 4$, where the functions S_i are as described above.

A minimal set of bases $b_1, \ldots, b_4$ that is certain to contain a basis of the desired kind includes, for each different enciphering permutation, exactly one basis that is the $b_1, \ldots, b_4$ part of a trapdoor sequence for the permutation whose e_1, e_2 elements are the ones chosen. It can be shown that such a set of bases contains approximately 2^{3n-3} bases, so at most approximately 2^{3n-3} trials are required to find a trapdoor sequence for P by the exhaustive search procedure described above. It appears likely that, for each basis $b_1, \ldots, b_4$ tested, either there is no solution at all for the elements a_{ik}, or else the basis is the $b_1, \ldots, b_4$ part of a trapdoor sequence for P of the desired kind and there is only one solution for the elements a_{ik}. In view of this, we will consider the testing of a single basis as being a single operation. Thus we conclude that at most approximately 2^{3n-3} operations are required to find a trapdoor sequence for P by the exhaustive search procedure described above.

Finally, we consider finding a trapdoor sequence for a given enciphering permutation P by solving algebraically for a set of elements a_{ik} and b_{ik} of $GF(2^n)$ satisfying the system of equations (2.6). First, we note the connection between solutions of this system of equations and trapdoor sequences for P. If a set of elements a_{ik} and b_{ik} of $GF(2^n)$ satisfies this system of equations and if $GF(2^\gamma)$-linear functions S_i and T_i from $GF(2^n)$ into $GF(2^n)$ are defined in terms of these elements by equations (2.4) and (2.5), respectively, then P can be expressed in terms of these functions by equation (2.3). Furthermore, there exists a trapdoor sequence for P which specifies these functions if and only if these functions satisfy the conditions

$$GF(2^n) = S_1(GF(2^\delta)) \oplus S_2(GF(2^\delta)) = \ker(T_1) \oplus \ker(T_2)$$

and $GF(2^\delta) = \mathrm{range}(T_1) = \mathrm{range}(T_2)$. If the functions S_i and T_i satisfy these conditions and if e_1, e_2 is any basis of $GF(2^\delta)$ over $GF(2^\gamma)$, then a trapdoor sequence for P which specifies these functions is given by $a_1, \ldots, a_4, b_1, \ldots, b_4, e_1, e_2$, where, for $j = 1, 2$, $a_j = S_1(e_j)$, and, for $j = 3, 4$, $a_j = S_2(e_{j-2})$, and where, for $j = 1, 2$, b_j is the unique element of $\ker(T_2)$ satisfying $T_1(b_j) = e_j$, and, for $j = 3, 4$, b_j is the unique element of $\ker(T_1)$ satisfying $T_2(b_j) = e_{j-2}$. It follows that the system of equations (2.6) has many solutions for the elements a_{ik} and b_{ik}, since there is a different solution arising from each different trapdoor sequence for P having fixed e_1, e_2 elements, and there are perhaps other solutions as well that do not arise from any trapdoor sequence for P. We will assume that all solutions for the elements a_{ik} and b_{ik} do in fact arise from trapdoor sequences for P. Then, to find a trapdoor sequence for P, it suffices to find a single solution of the system of equations (2.6) for the elements a_{ik} and b_{ik}.

In order to estimate the amount of computation required to solve this system of equations algebraically, it is first necessary to determine the most efficient method of algebraic solution. As already noted, this system of equations is linear in the elements a_{ik}. Hence it appears that the most efficient way to solve this system is to first simplify it as much as possible by eliminating these unknowns. This is exactly the method that was used by Berkovits and by James, Lidl, and Niederreiter to solve the corresponding system of equations associated with the original version of our cipher. It was in this way that they broke that cipher.

For the system of equations (2.6), there are many possible ways in which the unknowns a_{ik} can be eliminated, and each of these ways must be tried in order to find the best way of simplifying the system. Unfortunately, to try all these ways would require a forbidding amount of computation, although it could probably be done fairly easily using a suitable computer algebra system. To get around these difficulties in analyzing this system of equations, we consider instead a different system of equations that presumably requires less computation to solve. This system of equations is associated with a class of permutations of $GF(2^n)$ that are somewhat simpler than the enciphering permutations used in our cipher but which have the same general structure. These simpler permutations are obtained by modifying the enciphering permutation construction described in section 2 by changing the relationship between δ and γ from $\delta = 2\gamma$ to $\delta = \gamma$. The effect of this change is to convert the polynomial formulas (2.4) and (2.5) for the functions S_i and T_i from 2 terms to 1 term and from 4 terms to 2 terms, respectively. The resulting permutation P is then given by a polynomial formula having just 4 terms, rather than 16 terms as in our cipher. The system of equations that corresponds to the system of equations (2.6) and that relates the polynomial coefficients p_{gh} of P to the polynomial coefficients a_{ik} and b_{ik} of the functions S_i and T_i has the form

$$p_{gh} = a_{10}b_{1g}^{2^\beta}b_{1h} + a_{20}b_{2g}^{2^\beta}b_{2h}, \text{ for } g, h = 0, 1.$$

Now we consider how this system of equations can be solved. Note that, like the more complicated system of equations (2.6), the above system of equations is linear in the unknowns a_{10} and a_{20}. Hence it appears that the most efficient way to solve this system is to first simplify it as much as possible by eliminating these unknowns. Of the various ways to do this, the best way appears to be one that leads fairly directly to a single polynomial equation $R(B_1) = 0$ of degree $2^{2\beta} + 1$ in the single unknown $B_1 = b_{10}/b_{11}$. It appears that the amount of computation required to solve this equation is at least the amount required to compute the greatest common divisor of the polynomials $R(B_1)$ and $B_1^{2^n} - B_1$. This requires approximately $\deg(R(B_1))^2/2$ operations, which is approximately $2^{(2/3)n-1}$ operations. We will take this amount as our estimate of the amount of computation required to find a trapdoor sequence by solving the system of equations (2.6) algebraically.

An obvious question now arises. Since the estimate just given is based solely on the properties of the corresponding system of equations for the simpler permutations described above, why not use these simpler permutations as enciphering permutations? Unfortunately, this cannot be done. The reason for this is that, for such enciphering permutations, the deciphering permutations can be expressed by a rational formula corresponding to the rational formula described in section 5 for the deciphering permutations used in our cipher, and there are at most 12 terms in this formula. Thus, as indicated in section 5, the coefficients in this formula can be determined by doing at most approximately $12^3/3$ operations. This number of operations is far too small to provide any security, and hence the simpler permutations described above cannot be used as enciphering permutations.

7. Summary of the cryptanalytic attacks and conclusions

The following table summarizes the estimates of the amounts of computation required by the various cryptanalytic attacks discussed in sections 4 - 6.

method of attack	maximum number of operations required
1. solving the equation $P(x)= y$:	
a. by exhaustive search	$2^{(3/4)n}$
b. algebraically	$2^{(11/6)n-1}$
2. finding a formula for P^{-1}:	
a. polynomial	$(2^n)/3$
b. rational	$(2^n)/3$
3. finding a trapdoor sequence:	
a. by exhaustive search	2^{3n-3}
b. algebraically	$2^{(2/3)n-1}$

According to the above table, the most effective attack against our cipher is to solve algebraically for a trapdoor sequence for the enciphering permutation. This attack is estimated to require at most $2^{(2/3)n-1}$ operations, so the block-length n of the cipher must be chosen so that this amount of computation is unfeasible. We will assume, somewhat arbitrarily, that the maximum feasible amount of computation is the number of operations performed by a computer that does 10^9 operations per second for a period of 10 years. This amounts to a total of 3×10^{17} operations. We multiply this by a safety factor of 10^{12} to arrive at the figure of 3×10^{29} operations as an unfeasible amount of computation. Hence the block-length n must be such that $2^{(2/3)n-1} \geq 3 \times 10^{29} \cong 2^{98}$. Thus we conclude that a suitable block-length for our cipher is $n \geq 150$.

References

1. Shimshon Berkovits (Uni. of Lowell, Dept. of Computer Science), private communication, Aug., 1985.

2. John J. Cade, A new public-key cipher which allows signatures, talk given at the Second S.I.A.M. Conference on Applied Linear Algebra, Raleigh, NC, Apr. 30 - May 2, 1985.

3. N. S. James, R. Lidl, and H. Niederreiter, Breaking the Cade cipher, preprint, 1986.