Block Ciphers Based on Modular Arithmetic

Joan Daemen, René Govaerts and Joos Vandewalle

Katholieke Universiteit Leuven, Laboratorium ESAT
Kardinaal Mercierlaan 94, B-3001 Heverlee, Belgium
email: daemen@esat.kuleuven.ac.be

Abstract

The block ciphers PES and IPES were originally designed with the ambition to become the successor of DES as a standard. In this paper we point out why this would be a bad idea. On one hand a new block cipher (called MMB) is proposed, that uses similar primitive operations as (I)PES but can be more efficiently implemented both in hardware and in software. On the other hand classes of weak keys (with size up to 2^{51}) have been found for IPES.

1 Introduction

In May 1990, a modular arithmetic based block cipher was introduced called PES, with block length 64 bits and key length 128 bits [1]. The nonlinearity and diffusion are realized by the design concept of "mixing operations from different algebraic groups". The group operations involved are addition modulo 2^{16}, multiplication modulo $2^{16}+1$ and bitwise XOR of 16-bit words. The round function of the algorithm is designed to realize very high diffusion. The confusion is guaranteed by the order of the operations in the computational graph and the "incompatibility" of the different operations. Triggered by the emergence of differential cryptanalysis a modification of PES was presented in April 1991, called IPES [2]. This algorithm has been commercialized under the name IDEA. The result is a block cipher that allows fast implementations both in hardware and software.

The original ambition of the designers of (I)PES was to provide an alternative for DES as a standard block cipher. It is the main goal of our paper to point out that IPES would make a poor choice for this purpose. Our argument is backed by a new block cipher proposal that is comparable to IPES in that it is described in terms of modular arithmetic and bitwise XORs. However, it is claimed that it is superior to IPES with respect to efficiency both in software and hardware implementations. Moreover, large classes of weak keys have been found for IPES.

In the following sections we will present and motivate our own block cipher design MMB. In Sect.4 undesirable properties of IPES are discussed and in Sect.5 IPES and MMB are compared with respect to their implementation suitability.

Appeared in *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography*, W. Wolfowicz (ed.), Fondazione Ugo Bordoni, pp. 80–89, 1993.

2 MMB : A New Block Cipher.

MMB (Modular Multiplication based Block cipher) is a block cipher with both block- and key length 128 bits.

2.1 Specification

All operations are performed on 32-bit words. Let $\oplus$ denote bitwise XOR.
For $0 < \gamma < 2^{32} - 1$ and x a word let

$$\gamma \times x = \begin{cases} \gamma \cdot x \bmod (2^{32} - 1) & \text{if} \quad x < 2^{32} - 1 \\ 2^{32} - 1 & \text{if} \quad x = 2^{32} - 1 \end{cases}$$

Encryption is performed by applying an iterative transformation on a 4-word plaintext block with the 4-word key $k_0k_1k_2k_3$ as a parameter. A nonlinear round function $\mathrm{f_r}$ is applied 6 times alternated by (linear) key XORing. Lower indices must be taken modulo 4.

$$\begin{array}{ll} x_i = x_i \oplus k_i & \text{for} \quad 0 \le i < 4 \\ \mathrm{f_r}(x_0x_1x_2x_3) & \\ x_i = x_i \oplus k_{i+1} & \text{for} \quad 0 \le i < 4 \\ \mathrm{f_r}(x_0x_1x_2x_3) & \\ x_i = x_i \oplus k_{i+2} & \text{for} \quad 0 \le i < 4 \\ \mathrm{f_r}(x_0x_1x_2x_3) & \\ x_i = x_i \oplus k_{i+3} & \text{for} \quad 0 \le i < 4 \\ \mathrm{f_r}(x_0x_1x_2x_3) & \\ x_i = x_i \oplus k_i & \text{for} \quad 0 \le i < 4 \\ \mathrm{f_r}(x_0x_1x_2x_3) & \\ x_i = x_i \oplus k_{i+1} & \text{for} \quad 0 \le i < 4 \\ \mathrm{f_r}(x_0x_1x_2x_3) & \\ x_i = x_i \oplus k_{i+2} & \text{for} \quad 0 \le i < 4 \end{array}$$

Where the round function $\mathrm{f_r}$ establishes a 3-step transformation of its argument:

$$\begin{array}{lll} \text{step 1 :} & x_i = \gamma_i \times x_i & \text{for } 0 \le i < 4 \\ \text{step 2 :} & \text{if } \mathrm{lsb}(x_0) = 1 : x_0 = x_0 \oplus \delta & \\ & \text{if } \mathrm{lsb}(x_3) = 0 : x_3 = x_3 \oplus \delta & \\ \text{step 3 :} & x_i = x_{i-1} \oplus x_i \oplus x_{i+1} & \text{for } \ 0 \le i < 4 \end{array}$$

Step 2 and 3 are their own inverse. The inverse of a component of step 1 is given by $x_i = \gamma_i^{-1}x_i$ where γ_i^{-1} is defined by $\gamma_i \times \gamma_i^{-1} = 1$. The γ_i and δ are 32-bit constants. In hexadecimal notation:

$$\begin{array}{lll} \gamma_0 = 025\mathrm{F1CDB} & \gamma_0^{-1} = 0\mathrm{DAD4694} & \delta = 2\mathrm{AAAAAAA} \\ \gamma_1 = 2 \times \gamma_0 & \gamma_2 = 2^3 \times \gamma_0 & \gamma_3 = 2^7 \times \gamma_0 \end{array}$$

Appeared in *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography*, W. Wolfowicz (ed.), Fondazione Ugo Bordoni, pp. 80–89, 1993.

2.2 Cryptographic Claim for MMB

Suppose cryptanalist D has access to an encryptor/decryptor module ED that has been loaded with a secret key k, chosen randomly from the keyspace according to a publicly known probability distribution Ω. The module ED must not be seen as a conceptual model, but as an implementation of MMB with existing (or expected in the future) technology. It is possible for D to obtain from ED the ciphertext corresponding to any number of plaintext blocks and vice versa. It is not possible for D to read bits of k at the outputs of ED. The cryptanalist must be situated in the real world where computer hardware, software, computing power, etc. are for sale.

Let $\mathcal{P}$ denote the set of all possible plaintexts and $\mathcal{C}$ the set of all possible ciphertexts. The set of plaintexts whose ciphertexts are obtained from ED is denoted by $\mathcal{X}$, the set of the corresponding ciphertexts by $\mathrm{e}_k(\mathcal{X})$. The set of ciphertexts whose plaintexts are obtained from ED are denoted by $\mathcal{Y}$, the set of the corresponding plaintexts by $\mathrm{d}_k(\mathcal{Y})$.

If no information was given on the algorithm embedded in ED, the cheapest attack would be collecting a few ciphertext/plaintext pairs and subsequently trying the keys in the order of the a priori probabilities until the correct key is identified by checking the ciphertext/plaintext pairs. This attack is generally referred to as *exhaustive keysearch*.

The authors make the following cryptographic claim for MMB.

Claim 1 *For any choice of $\mathcal{X}$ and $\mathcal{Y}$, the cheapest way of gaining information about the mapping between $\mathcal{P} \setminus (\mathcal{X} \cup \mathrm{d}_k(\mathcal{Y}))$ and $\mathcal{C} \setminus (\mathcal{Y} \cup \mathrm{e}_k(\mathcal{X}))$ for cryptanalist D is and always will be exhaustive keysearch, for any probability distribution Ω.*

3 Motivation for the Specific Design of MMB

3.1 Symmetry and Parallelism

Symmetry has been applied to obtain a very simple cipher specification and uniform information propagation. In steps 1 and 3 of the round function and in the key application all words are treated in the same way. All operations in a single step can be done in parallel to make high speed implementations possible. (see Sect.5.1)

The symmetry is also present at the bit level since multiplication modulo $2^n - 1$ exhibits shift invariance [4], i.e. (with $\ll k$ denoting cyclic shift to the left over k positions)

$$a \times (x \ll k) = a \times 2^k \times x = (a \ll k) \times x = (a \times x) \ll k \ . \tag{1}$$

To thwart attacks that would exploit the symmetry step 2 has been introduced.

The round function of MMB is not an involution, as is the case in DES or IPES. However, step 2 and 3 are involutions and step 1 can be inverted by modular 'division' or multiplication by the multiplicative inverse of the factors γ. These are chosen such that $\gcd(\gamma, 2^{32} - 1) = 1$. The inverse γ^{-1} can be calculated with the extended algorithm of Euclid such that $\gamma^{-1} \times \gamma = 1$. The choice of the γ_i is based on resistance against differential cryptanalysis and will be explained in Sect.3.3.

Appeared in *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography*, W. Wolfowicz (ed.), Fondazione Ugo Bordoni, pp. 80–89, 1993.

j	P^0_j	j	P^0_j	j	P^0_j	j	P^0_j	j	P^0_j	j	P^0_j	j	P^0_j	j	P^0_j
0	.990	4	.312	8	.855	12	.196	16	.887	20	.055	24	.372	28	.148
1	.495	5	.844	9	.428	13	.902	17	.444	21	.972	25	.814	29	.074
2	.752	6	.578	10	.786	14	.452	18	.222	22	.486	26	.593	30	.037
3	.624	7	.289	11	.393	15	.225	19	.111	23	.743	27	.296	31	.018

Table 1: propagation probabilities for γ_0

j	P^0_j	j	P^0_j	j	P^0_j	j	P^0_j	j	P^0_j	j	P^0_j	j	P^0_j	j	P^0_j
0	.053	4	.746	8	.578	12	.411	16	.724	20	.830	24	.323	28	.854
1	.027	5	.627	9	.710	13	.206	17	.638	21	.585	25	.838	29	.427
2	.987	6	.313	10	.355	14	.897	18	.681	22	.707	26	.581	30	.213
3	.493	7	.843	11	.822	15	.551	19	.340	23	.646	27	.290	31	.106

Table 2: propagation probabilities for γ_0^{-1}

3.2 High Key-Independent Diffusion of the Round Function

To give an idea of the amount of information propagation or diffusion that is realized by the round function f_r, we will treat the effect of complementing a single bit of the input of f_r on the output. The most important contribution to the diffusion comes from the multiplication in step 1. Suppose the bits in a word are indexed from 0 (LSB) to 31 (MSB) and that the probability that complementing bit i of a results in complementation of bit j of $\gamma \times a$ is denoted by P^i_j. Because of the rotational invariance we have $P^{i+k}_{j+k} = P^i_j$ for any k where the indices are taken modulo 32. Table 1 lists these probabilities for γ_0 and Table 2 for its inverse. Since γ_1, γ_2 and γ_3 are cyclically shifted versions of γ_0, all probabilities for step 1 and its inverse can be deduced from the Tables 1,2. The sum of all the probabilities in Table 1 is the average number of bits that are complemented in $\gamma_0 \times a$ if one bit of a is complemented. This is called the *diffusion factor* of step 1. The diffusion factor of step 1 is 15.4 and of its inverse 17.4 .

The diffusion caused by step 2 is relatively small and will not be treated. Step 1 only allows diffusion between bits inside a word, step 3 only between bits from different words. Step 3 has a diffusion factor of 3. Since the diffusion in step 3 is independent of the diffusion of step 1 the diffusion factor of f_r is 46,2 and that of f_r^{-1} 52.2 .

3.3 Differential Cryptanalysis

The confusion is realized by combining modular multiplication and bitwise XOR. An important design criterion for MMB is the resistance against differential cryptanalysis [3],

Appeared in *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography*, W. Wolfowicz (ed.), Fondazione Ugo Bordoni, pp. 80–89, 1993.

where the difference is defined as bitwise XOR. In our opinion this is the appropriate definition in the case of MMB. Step 1 of f_r can be seen as the application of 32-bit invertible substitution boxes. After designing the overall structure of the block cipher, the factors γ_i were chosen. In the following of this section we will explain the criteria that were used.

If we have a pair of numbers v, v^* their XOR is denoted by $v' = v \oplus v^*$. Their difference modulo $2^n - 1$ is denoted by $\hat{v} = v - v^*$. Essentially $\hat{v} \in Z_{2^n-1}$ is a modular number and $v' \in Z_2^n$ is a bit pattern.

If we have an input pair x, x^* to a multiplicative function, the difference of the output pair $\hat{y} = y - y^*$ is fixed by the difference of the inputs $\hat{x}$. The output difference y' is not fixed by x' but depends on the specific values of x and x^*.

The input XOR and the output XOR form a *characteristic*. The probability associated with a characteristic is the probability that a random pair with the chosen input XOR has the output XOR specified by the characteristic. The relation between XOR and modular difference can be used to explain the observed probabilities. The γ_i have been chosen to minimize the probability of the most probable nontrivial characteristic. This characteristic and its probability will be denoted in the following by the term *critical*. By trivial characteristics are meant the characteristics with all-zero or all-one input XORs x', that lead to respectively all-zero and all-one output XORs y' with probability 1. Since the number of input-output combinations is 2^{64} for $n = 32$, an analytical approach is necessary. In the following of this section we will give an outline of our search strategy. More details can be found in [4].

Definition 1 *An XOR v' and a modular difference $\hat{v}$ are called* compatible*, denoted by $v' \| \hat{v}$, if there exist $a_i \in \{+1, -1\}$ such that $\hat{v} = \sum_{v'_i=1} a_i 2^i$.*

If the non-zero bits of v' are replaced by the $a_i \in \{1, -1\}$ in the definition, the result can be considered as a redundant ternary representation of $\hat{v}$. This ternary representation is denoted by $\dot{v}$. The Hamming weight of this representation is the number of non-zero symbols, hence $w(\dot{v}) = w(v')$. From the definition it is also clear that from $v' \| \hat{v}$ follows $v' \| -\hat{v}$.

Proposition 1 *$v' \| \hat{v}$ if they can be defined by the same pair v, v^*. Moreover v' and $\hat{v}$ fix the bits of v and v^* at the positions where $v'_i = 1$ and impose no restrictions on the other bits of v or equivalently v^*.*

Proposition 2 *If $v' \| \hat{v}$ and $\hat{v} \neq 0$ we have $p(v'|\hat{v}) = p(\hat{v}|v') = 2^{-w(v')}$.*

If $x' = 1$ the resulting characteristics and their probabilities describe the effect of complementing bit 0 of the input. If we consider all pairs with $x_0 = 1$ we have $x' = 1 \Rightarrow \hat{x} = 1 \Rightarrow \hat{y} = \gamma$. It follows that all possible y' corresponding to $x' = 1$ must be compatible with γ. If we allow the input XOR x' to be any pattern, the situation is more complex. There are $2^{w(x')}$ equiprobable values $\hat{x}$ compatible with x'. Each of these values $\hat{x}$ gives rise to a different $\hat{y} = \gamma \times \hat{x}$. Only patterns y' compatible with one of the $\hat{y}$ can occur.

Appeared in *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography*, W. Wolfowicz (ed.), Fondazione Ugo Bordoni, pp. 80–89, 1993.

Using the algebraic properties we can derive

$$\begin{aligned} p(y' = m|x' = j) &= p(y' = m \ll k|x' = j \ll k) && (2)\\ &= p(y' = \bar{m}|x' = \bar{j}) && (3)\\ &= p(x' = j|y' = m) && (4) \end{aligned}$$

An important measure for multiplication factors in the given context is the minimum ternary Hamming weight:

Definition 2 *The minimum ternary representation of a (modular) number a is a ternary representation with no neighboring non-zero symbols. Its Hamming weight is called minimum ternary Hamming weight and is denoted by $w_m(a)$.*

It can be proved that the minimum ternary representation is unique and has minimum Hamming weight. Moreover $w_m(x) \leq \frac{n}{2}$.

Proposition 3 *The highest probability for a characteristic with $w(x') = 1$ can be approximated by $2^{-w_m(\gamma)}$. For a characteristic with $w(y') = 1$ this is $2^{-w_m(\gamma^{-1})}$.*

Large deviations only occur for factors with a *simple* form such as 3 and 5. For these values analysis at the bit level allows the exact calculation of the probabilities. As a consequence of this proposition, the critical probability can never be smaller than $2^{-\lfloor \frac{n}{2} \rfloor}$. The critical probability for a given factor a has lower bound $\min(2^{-w_m(\gamma)}, 2^{-w_m(\gamma^{-1})})$. The Hamming weight of a characteristic is defined as the sum of the weights of x' and y'.

Proposition 4 *The Hamming weight α_c of a critical characteristic x'_c, y'_c is limited by $\alpha_c \leq \min(w_m(a), w_m(a^{-1})) + 1$ and the critical probability can be approximated by $2^{1-\alpha_c}$.*

This proposition is the consequence of the fact that a critical characteristic is compatible with $(\hat{u}, a \times \hat{u})$ with minimum $w_m(\hat{u}) + w_m(a \times \hat{u})$. Although the validity of this proposition has been observed for all invertible multiplication factors modulo $2^n - 1$ with $n \leq 16$, no rigid proof is available. The proposition has been used to construct an algorithm that efficiently searches for the factor(s) with the highest α_c. The result of this search is γ_0 that has $\alpha_c = 10$ and therefore a critical probability of about 2^{-9}. Together with the 'forced' propagation in step 3 and the asymmetric step 2 it can easily be checked that (XOR) differential cryptanalysis will be no more successful than exhaustive keysearch.

4 Discussion on IPES

4.1 Complexity of the Cryptographic Claim

For a block cipher proposal to make sense, it **must** be accompanied by a claim of its cryptographic security. If no explicit claim of security is given by the authors, cryptanalytic success or failure depends on an *implicit* understanding of what a block cipher with the given parameters should do. Differences in these implicit understandings can give rise to

Appeared in *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography*, W. Wolfowicz (ed.), Fondazione Ugo Bordoni, pp. 80–89, 1993.

lengthy discussions whether or not weaknesses have been found for a given cipher. The goal of the cryptanalist is finding weaknesses in the cipher that refute the claim. The single way for a block cipher to gain credibility is the absence of cryptanalytic attacks that refute its cryptographic claim, despite the commitment of a large number of cryptologists. A claim of cryptographic security should be *practical* and *clear* at the same time: the claim should be usable to clearly attribute a level of security to the block cipher if used in a practical situation. This makes its formulation a very difficult task.

We did not find an explicit cryptographic claim for PES in [1], neither for IPES in [2]. This is no surprise, since we think it is extremely difficult to formulate a clear and practical claim that justifies a keylength of twice the blocklength. A claim as in the case of MMB, based on exhaustive keysearch for all possible a priori key distributions is not possible since table reconstruction for a given key only takes 2^{64} encryptions and exhaustive keysearch for a uniform distribution takes about 2^{128} encryptions. An explicit claim of security must answer questions like "Should differential cryptanalysis take more effort than exhaustive keysearch or than table reconstruction to be called *effective*?". The task of formulating a cryptographic claim for IPES will not be made easier by the classes of *weak keys* we discovered. These will be treated in Sect.4.3 .

4.2 Key-dependence of the Confusion Mechanism

The amount of nonlinearity and diffusion realized by the round function of IPES depends strongly on the value of the round keys. The effect of key multiplications with keys that represent a power of 2 modulo $2^{16}+1$ can be approximated very well by an (easy to find) affine transformation in the vector space $Z_{2^{16}}$. This category comprises all multiplicative keys with a single 1-bit. For all the 32 keys that fall into the category, it can be easily checked that the expected Hamming distance between the correct output and the affine approximation is smaller than 1 bit and that the probability that the approximation matches the correct output is larger than 0.5 .

The contribution of the key additions to the confusion is on the average small compared to the key multiplications. If an additive key is chosen randomly from $Z_{2^{16}}$, the expected Hamming distance between the modular sum and the best affine approximation is 1,75 bits. For a given additive key the distance is always smaller than half the minimum ternary weight of the key (as defined in Sect.3.3).

The round keys are substrings of the global key, defined by the key schedule. All global keys in the (albeit very small) set of 128-bit strings consisting of only few 1's separated by long enough blocks of 0's give rise to only 'weak' round keys. For these keys the cryptographic security of the cipher comes to rely mainly on the nonlinearity of the additions modulo 2^{16} in the MA-structure of the round function. An example of weak round keys leading to weak global keys is given in the following subsection.

Appeared in *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography*, W. Wolfowicz (ed.), Fondazione Ugo Bordoni, pp. 80–89, 1993.

4.3 Weak Keys for IPES

Linearities in the addition modulo 2^{16} and multiplication by certain keys can be exploited to identify the membership of a global key in classes of *weak* keys. We use the following two properties ($+$ denotes addition modulo 2^{16}, $\oplus$ denotes XOR and $\times$ denotes multiplication modulo $2^{16}+1$ and ν is the 16-bit vector 8000 (HEX)):

- If $a + b = c$, we have $(a \oplus \nu) + b = a + (b \oplus \nu) = c \oplus \nu$.
- If $(-)1 \times a = b$, we have $(-)1 \times (a \oplus \nu) = b \oplus \nu$. Multiplicative key -1 corresponds to 0000 (HEX) and 1 to 0001 (HEX).

In other words key addition and multiplication with factor $(-)1$ do not cause diffusion or nonlinearity for the MSB bit. Suppose a given round is executed for two different inputs X and X^* that only differ in the MSB of the 1st 16-bit word and the 3rd word. If round key $Z_1 \in \{0000, 0001\}$, the intermediate results after the application of Z_1, Z_2, Z_3, Z_4 will only differ in the MSB of the 1st and 3rd word. The output of the MA function is the same for X and X^* since the inputs don't differ. It can easily be seen that the corresponding outputs Y and Y^* differ only in the MSB of the 1st word and the 2nd word. *Observe that the only condition for this guaranteed XOR propagation is that the 15 LSB bits of Z_1 be zero.* A similar argument applies to all input pairs that only differ in the MSB bits. For every of the 16 possibilities this results in conditions on the values of bits of multiplicative keys. Using these mechanisms large classes of *weak* keys were found. The term weak is used to denote that the workload of identifying that a key belonging to a class of weak keys is used is relatively very small. After this identification, applying other XORs allows efficient calculation of the exact value of the key. Since the described mechanism was only identified a few days ago while writing this final paper, further study is expected to reveal even larger classes of weak keys. We list our most important preliminary results:

- For all keys where only bits with indices in 33–40 or 92–115 may differ from 0, the input XOR 0000800080000000 (HEX) gives rise to output XOR 0000800000008000 with probability 1. This class contains 2^{32} keys. The workload consists of two encryptions.
- For all keys where only bits with indices in 26–40 or 72–83 or 99-122 may differ from 0, the outputs corresponding to two inputs with XOR 0000800000008000 (HEX) lead to a set of nonlinear equations with 16 equations and 12 binary variables that must have a solution. This class contains 2^{51} keys. The workload consists of two encryptions and solving the set of nonlinear equations.

Apart from these two classes several smaller classes were found.

Appeared in *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography*, W. Wolfowicz (ed.), Fondazione Ugo Bordoni, pp. 80–89, 1993.

	IPES(16 bit)		MMB(32 bit)	
	1 round	all rounds	1 round	all rounds
mult :	3	25	1	6
add :	2	16	-	-
xor :	2	16	3	19

Table 3: critical path of operations for IPES versus MMB

5 Implementation Suitability of IPES versus MMB

5.1 Hardware: Possibilities for Parallelism

For both algorithms the cipher structure allows a hardware implementation by means of a limited number of modules. For IPES in the encryption mode the key schedule can be implemented by storing the 128-bit global key in a cyclic shiftregister. For the decryption mode however, fast operation requires precomputation and storage of the 52 16-bit round subkeys. On-chip precomputation complicates the chip structure, off-chip precomputation complicates the security problem. In MMB these problems are avoided because the decrypting keys are the same as the encrypting keys.

A lower limit for the time between feeding the plaintext (ciphertext) at the input and the appearance of the ciphertext (plaintext) at the output is given by the 'critical path' in the computational graph. The order of the operations in terms of delay time is : multiplication (very slow), addition (slow) and bitwise XOR (fast). A comparison between IPES and MMB is made in Table 3. It must be added that the MMB operations take 32-bit strings while IPES takes 16-bit strings. On the other hand the modular multiplications and additions in IPES take two 16-bit variables, while in MMB only a single 32-bit variable is taken in MMB (there is essentially just one multiplication factor in all the algorithm). If the modular multiplications are implemented by means of tables and additions, the complexity (both in table size and delay) of the modular multiplications in PES and MMB are the same. Moreover, one IPES computation encrypts 64 bits of ciphertext, while one MMB computation encrypts 128 bits.

5.2 Software: Total Workload

Since the word length in most modern processors is 32 bits, the choice of 16 as the word length in (I)PES seems somewhat outdated.

For multiplication modulo $2^{16}+1$ as defined in [1], a test has to be performed to find out if one of the arguments is 0 (prob. 2^{-16}). For multiplication modulo $2^{32}-1$ it can easily be shown that no extra test is necessary.

The speed of single-processor software implementations is limited by the total number of operations in the algorithm. These are given in Table 4.

Appeared in *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography*, W. Wolfowicz (ed.), Fondazione Ugo Bordoni, pp. 80–89, 1993.

	IPES(16 bit)		MMB(32 bit)	
	1 round	all rounds	1 round	all rounds
mult	4	34	4	24
add	4	34	-	-
xor	6	48	12	76

Table 4: total workload for IPES versus MMB

6 Acknowledgements

We would like to thank Dr. Xuejia Lai for his comments on the preliminary version of this paper.

7 Conclusions

IPES is contrasted with a new, comparable block cipher called MMB. Serious weaknesses have been identified for IPES. Moreover, the authors claim that MMB allows more efficient implementations both in hardware and software and has better cryptographic properties than IPES.

References

[1] X. Lai and J.L. Massey, A Proposal for a New Block Encryption Standard, in *Advances in Cryptology–Eurocrypt' 90*, Springer-Verlag, Berlin 1991, pp. 389–404 .

[2] X. Lai, J.L. Massey and S. Murphy, Markov Ciphers and Differential Cryptanalysis, in *Advances in Cryptology–Eurocrypt' 91*, Springer-Verlag, Berlin 1991, pp. 17–38 .

[3] E. Biham and A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, *Journal of Cryptology* (1991) **4** : 3–72.

[4] J. Daemen, L. Van Linden, R. Govaerts and J. Vandewalle, Propagation Properties of Multiplication Modulo $2^n - 1$, *Proceedings of the 13th Symposium on Information Theory in the Benelux* (1992), Werkgemeenschap voor informatie- en Communicatietheorie, Enschede, The Netherlands.

Appeared in *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography*, W. Wolfowicz (ed.), Fondazione Ugo Bordoni, pp. 80–89, 1993.