The Gomẽgo Block Cipher

Isaiah Makwakwa*

March 31, 2011

Abstract

We present a 128-bit (128-bit key) byte-oriented block cipher. It is a Feistel Network based on a 32-bit composite primitive. Gomẽgo is a byte-oriented cipher employing two operations: exclusive-or and table lookup.

Keywords
e-block, composite primitive, random involutionary S-boxes

1 Introduction

Gomẽgo is a byte-oriented 128-bit Feistel Network in which the round permutation has three layers: key addition, substitution and diffusion.

It uses a 128-bit master key. The substitution layer is based on random involutionary S-boxes on 8 bits while the diffusion layer is based on the *extended diffusion block* (e-block).

*Email: imakwakwa@gmail.com

2 Preliminaries

2.1 Finite Fields

A field, $\mathbb{F}$, is an abelian group under addition and under multiplication of nonzero elements. The ring of integers modulo some prime p is called a prime field, denoted $\mathbb{F}_p$.

Let n be any integer. An extension field, $\mathbb{F}_q$ ($q = p^n$), of $\mathbb{F}_p$ of index n can be defined as the field of all polynomials over $\mathbb{F}_p$ modulo an irreducible polynomial of degree n. It can also be defined as an n dimensional vector space over $\mathbb{F}_p$ [3].

In particular, Gomeğo assumes an isomorphism between binary extension fields, $\mathbb{F}_{2^m}$, and vector spaces, $\mathbb{F}_2^m$, by specifying a generator polynomial for $\mathbb{F}_{2^m}$ over the binary field.

2.2 Differential Cryptanalysis

Differential cryptanalysis of block ciphers was introduced by Biham and Shamir [6]. It exploits the existence of ordered pairs (α, β) of binary strings such that for any random plaintext x,

$$Prob(f(x) \oplus f(x \oplus \alpha) = \beta) > Prob(f(x) \oplus f(x \oplus \alpha) = \zeta)$$

for any random ζ and n-bit block cipher $f(x)$ [1].

The *propagation ratio* of a difference sequence, for any iterated block cipher, is the total probability that a given difference sequence will result into a particular output XOR.

The attack is successful if

$$Prob(f(x) \oplus f(x \oplus \alpha) = \beta) > 2^{1-n}$$

for some ordered pair (α, β) [1, 5].

2.3 Linear Cryptanalysis

Linear cryptanalysis of block ciphers was introduced by Matsui in [8]. It exploits the existence of a pair of ordered binary strings (α, β) such that for any random plaintext x,

$$Prob(\alpha \cdot x \oplus f(x) \cdot \beta = 0) \neq \frac{1}{2}$$

where $f(x)$ is an n-bit block cipher and $\cdot$ is the inner product of binary vectors [1].

The *linear correlation ratio* between a plaintext/ciphertext pair is the total probability that a linear function (often the dot product of binary vectors or the trace function over a finite Field) of the ciphertext is equal to a linear (or affine) function of the plaintext. A successful linear attack can be mounted if

$$Prob(\alpha \cdot x \oplus f(x) \cdot \beta = 0) > 2^{-\frac{n}{2}}$$

for some ordered pair (α, β) [5].

2.4 Wide Trail Strategy

In [4], it was shown that the propagation ratio (resp. linear correlation ratio) of a differential trail (resp. linear trail) can be approximated by simply multiplying the propagation (resp. correlation) ratios in the differential trail.

Therefore, the propagation ratio (resp. correlation ratio) of a differential trail (resp. linear trail) can be approximated using the number of active S-boxes in the trail [5].

2.5 The Extended Diffusion Block

Let $\mathbb{F}_2^{2n} = \mathbb{F}_2^n \times \mathbb{F}_2^n$ be a binary vector space of dimension $2n$. Let $a \in \mathbb{F}_2^n$, we define the extended diffusion block (e-block) on $\mathbb{F}_2^{2n}$ by the involution

$$e_{n,a}(x_0, x_1) = a(x_0 \oplus x_1) \oplus x_0, a(x_0 \oplus x_1) \oplus x_1$$

where $(x_0, x_1) \in \mathbb{F}_2^{2n}$, $a \notin \{0, 1\}$ and multiplication takes place over $\mathbb{F}_{2^n}$.

This primitive can be used to create diffusion blocks of block ciphers in which the block size is a multiple of $2n$. Just like in SAFER, the diffusion layer of larger blocks is created by multiple instances and layers of the e-block primitive [2]. That is, for a block length of 2^m, complete diffusion using e-block requires 2^{m-1} instances of e-block in m layers.

3 The Gomẽgo Cipher

3.1 Representation of State in Gomẽgo

Let x be a 128-bit vector. State [5, 1] in Gomẽgo is respresented as a 16 byte vector $x = (x_0, x_1, x_2, x_3) \in (\mathbb{F}_2^{32})^4$ where the 32-bit component vectors, x_i, are defined as $x_i = (x_{i,0}, x_{i,1}, x_{i,2}, x_{i,3}) \in (\mathbb{F}_2^8)^4 = \mathbb{F}_2^{32}$.

3.2 The Gomẽgo S-Boxes

The Gomẽgo S-boxes, φ_0 and φ_1 are random involutionary S-boxes on 8 bits with algebraic degree 7, 253 coefficients, maximum difference propagation ratio 2^{-5} and maximum linear correlation ratio $\frac{60}{256}$. These are given in **Table 1** and **Table 2** below respectively.

Table 1: The φ_0 S-box

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	C1	55	70	A4	38	73	CE	BD	D7	AE	86	98	B7	1A	E8	DE
10	A6	4D	6D	F4	93	D1	94	F1	CF	56	0D	74	43	B9	80	ED
20	26	CB	BF	AF	BB	8D	20	92	C4	E1	D0	F7	5D	79	F6	F5
30	9E	8A	E7	9F	A3	A8	72	E3	04	9B	64	AA	C0	E4	EA	C8
40	F3	85	5C	1C	B5	95	53	62	CC	54	6E	78	7D	11	B1	7B
50	A9	6A	DB	46	49	01	19	69	96	8F	97	7C	42	2C	9C	FA
60	7A	75	47	66	3A	FE	63	D3	AB	57	51	87	76	12	4A	8B
70	02	E0	36	05	1B	61	6C	E5	4B	2D	60	4F	5B	4C	A5	8E
80	1E	EC	B4	B0	EB	41	0A	6B	CA	DA	31	6F	A0	25	7F	59
90	EF	DC	27	14	16	45	58	5A	0B	B8	C2	39	5E	F2	30	33
A0	8C	DD	F0	34	03	7E	10	FD	35	50	3B	68	D5	C3	09	23
B0	83	4E	E9	DF	82	44	D4	0C	99	1D	BC	24	BA	07	C9	22
C0	3C	00	9A	AD	28	FB	E2	FF	3F	BE	88	21	48	E6	06	18
D0	2A	15	D9	67	B6	AC	FC	08	F8	D2	89	52	91	A1	0F	B3
E0	71	29	C6	37	3D	77	CD	32	0E	B2	3E	84	81	1F	F9	90
F0	A2	17	9D	40	13	2F	2E	2B	D8	EE	5F	C5	D6	A7	65	C7

Table 1: The φ_1 S-box

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	AD	91	E2	0E	E1	E9	EA	AE	EE	54	3A	2A	46	A4	03	6E
10	B0	ED	66	A8	9F	3F	FC	8F	C4	3D	5A	55	87	F4	52	4C
20	68	CC	E6	89	4A	A2	28	FB	26	92	0B	96	60	7D	8E	7A
30	58	33	DF	31	85	65	47	C8	43	B3	0A	E5	D2	19	C5	15
40	C7	4E	D4	38	74	D7	0C	36	F2	CD	24	A3	1F	78	41	E3
50	9D	86	1E	E8	09	1B	E4	6A	30	B5	1A	77	B4	A5	5F	5E
60	2C	71	FA	A6	C6	35	12	CA	20	B9	57	F1	FD	F8	0F	8B
70	EC	61	D5	D0	44	EB	D8	5B	4D	8D	2F	BA	E0	2D	F9	AF
80	B8	EF	BF	97	DB	34	51	1C	93	23	E7	6F	F7	79	2E	17
90	BC	01	29	88	BD	9B	2B	83	B6	DC	AC	95	D3	50	DD	14
A0	B7	F3	25	4B	0D	5D	63	C0	13	D6	CF	BB	9A	00	07	7F
B0	10	CB	DE	39	5C	59	98	A0	80	69	7B	AB	90	94	F5	82
C0	A7	C3	CE	C1	18	3E	64	40	37	D1	67	B1	21	49	C2	AA
D0	73	C9	3C	9C	42	72	A9	45	76	FE	F6	84	99	9E	B2	32
E0	7C	04	02	4F	56	3B	22	8A	53	05	06	75	70	11	08	81
F0	FF	6B	48	A1	1D	BE	DA	8C	6D	7E	62	27	16	6C	D9	F0

3.3 Key Addition Layer

Let κ denote the $24 \times 2 \times 4$ subkey table from the key schedule algorithm. For any $x_k = (x_{k,0}, x_{k,1}, x_{k,2}, x_{k,3}) \in \mathbb{F}_2^{32}$ define the round key addition function

$$\psi_{i,j}(x_k) = (x_{k,0} \oplus \kappa[i]_{j,0}, x_{k,1} \oplus \kappa[i]_{j,1}, x_{k,2} \oplus \kappa[i]_{j,2}, x_{k,3} \oplus \kappa[i]_{j,3})$$

where $j \in \{0, 1\}$, $\kappa[i]_{j,r}$ is the r^{th} byte of $\kappa[i]_j$ (a 4 *byte vector*) and $x_{k,r}$ is the r^{th} byte of x_k.

3.4 The Diffusion Layer

Let $x_k = (x_{k,0}, x_{k,1}, x_{k,2}, x_{k,3}) \in \mathbb{F}_2^{32}$. Define the 32-bit linear function ϕ by

$$\phi(x) \quad = \quad e_{8,5}(y_{k,0}, y_{k,2}), e_{8,3}(y_{k,1}, y_{k,3})$$

where

$$y \quad = \quad e_{8,3}(x_{k,0}, x_{k,1}), e_{8,5}(x_{k,2}, x_{k,3}).$$

Then ϕ has the following properties

1. ϕ is a linear permutation on $\mathbb{F}_2^{32}$.
2. The sum of the number of active bytes in any non-zero input and output difference sequence is at least 4.

Clearly, ϕ can be implemented using 16 operations and one temporary variable in either direction (encryption and decryption) using XORs and table lookups only.

3.5 The G Composite Primitive

Let $x_k = (x_{k,0}, x_{k,1}, x_{k,2}, x_{k,3}) \in \mathbb{F}_2^{32}$. We define the Gomeğo 32-bit round function $G_{i,k}$ by

$$G_{i,k}(x_k) = \varphi_1 \circ \psi_{i,k} \circ \phi \circ \varphi_0(x_k) \tag{1}$$

where φ_0 and φ_1 are applied byte-wise.

By the diffusion properties of ϕ, the sum of active S-boxes in any non-zero input and output difference sequence is at least 4.

3.6 The Interleaving e-Block Function

Let $x = (x_k, x_j) \in (\mathbb{F}_2^{32})^2$. We define the interleaving e-block function, I_e, by the involution

$$I_e(x) = (e_{8,3}(x_{k,0}, x_{j,0}), e_{8,5}(x_{k,1}, x_{j,1}), e_{8,5}(x_{k,2}, x_{j,2}), e_{8,3}(x_{k,3}, x_{j,3}))\,.$$

3.7 Word Swapping Function

Let $x = (x_0, x_1, x_2, x_3) \in (\mathbb{F}_2^{32})^4$. Define the word swapping involution, λ, by

$$\lambda(x) = x_2 x_3 x_0 x_1.$$

This involution is also used in the Twofish block cipher [7].

3.8 The Number of Rounds

Gomeõ is an iterative block cipher with 18 rounds. Therefore, since complete diffusion in Gomeõ takes place after 3 rounds, Gomeõ has 6 complete diffusions.

3.9 Initial And Final Whitening

Let $x = (x_0, x_1, x_2, x_3) \in (\mathbb{F}_2^{32})^4$, then the initial whitening key addition function, ω_0, is defined by

$$\omega_0(x) = (\psi_{20,0}(x_0), \psi_{20,1}(x_1), \psi_{21,0}(x_2), \psi_{21,1}(x_3))$$

and the final whitening key addition function, ω_1, is defined by

$$\omega_0(x) = (\psi_{22,0}(x_0), \psi_{22,1}(x_1), \psi_{23,0}(x_2), \psi_{23,1}(x_3))\,.$$

3.10 Encryption Function

Let $x = (x_0, x_1, x_2, x_3) \in (\mathbb{F}_2^{32})^4$. The i^{th} round of encryption in Gomeõ, θ_i is defined by

$$\theta_i(x) = \lambda(y)$$

where

$$\begin{aligned} y_1, y_2 &= I_e(x_1, x_2) \\ y_0 &= G_{i,1}(y_2) \oplus x_0 \\ y_3 &= G_{i,0}(y_1) \oplus x_3. \end{aligned}$$

Therefore, the Gomeğo encryption function is defined as

$$f(x) = \omega_1 \circ \left(\bigcirc_{i=0}^{17} \theta_i\right) \circ \omega_0(x).$$

3.11 Decryption Function

Let $y = (y_0, y_1, y_2, y_3) \in (\mathbb{F}_2^{32})^4$. The i^{th} decryption round in Gomeğo, θ_i^{-1} is defined by

$$\theta_i^{-1}(y) = a$$

where

$$\begin{aligned} a_3 &= G_{i,0}(x_1) \oplus x_3 \\ a_0 &= G_{i,1}(x_2) \oplus x_0 \\ a_1, a_2 &= I_e(x_1, x_2), \end{aligned}$$

and

$$x = \lambda(y).$$

Thus, the Gomeğo decryption function is defined by

$$f^{-1}(y) = \omega_0 \circ \left(\bigcirc_{i=17}^{0} \theta_i^{-1}\right) \circ \omega_1(y).$$

3.12 Gomeğo Round Constants

Define the Gomeğo round constants, $C_i \in (\mathbb{F}_2^8)^{16}$, $0 \leq i \leq 11$ by

$$C_{i,j} = \varphi_0(7i + (16 - i)j), \quad 0 \leq j \leq 15 \tag{2}$$

where $C_{i,j}$ is the j^{th} byte of C_i and φ_0 is applied byte-wise.

4 Key Schedule Algorithm

4.1 Key Addition Function

Let $x_k = (x_{k,0}, x_{k,1}, x_{k,2}, x_{k,3}) \in (\mathbb{F}_2^8)^4$ and C_i the i^{th} round constant, define the key schedule key addition function

$$\psi_{i,k}(x) = (x_{k,0} \oplus C_{i,4k}, x_{k,1} \oplus C_{i,4k+1}, x_{k,2} \oplus C_{i,4k+2}, x_{k,3} \oplus C_{i,4k+3})$$

where $C_{i,j}$ is the j^{th} byte of C_i.

4.2 The σ Transformation

Let (b_{ij}) be a square matrix, denote by σ the matrix transpose function

$$(b_{ij})^\sigma = (b_{ji}).$$

4.3 Representation of State in the Key Schedule

State in the Gomeğo key schedule algorithm is represented as a 4×32 bit matrix

$$x = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

where $x_i = (x_{i,0}, x_{i,1}, x_{i,2}, x_{i,3}) \in (\mathbb{F}_2^8)^4$.

4.4 The Gomeğo Key Schedule

Let x be a 128-bit vector, the Gomeğo key schedule round function is defined by

$$g_i(x) = \phi \circ \begin{pmatrix} G_{i,0}(x_0) \\ G_{i,1}(x_1) \\ G_{i,2}(x_2) \\ G_{i,3}(x_3) \end{pmatrix}^\sigma$$

where ϕ is applied row-wise.

Let a_{-1} be the master key and initialise $i = -1$, a round of the 6 round Gomeğo key schedule is defined by

$$\begin{aligned} a_{i+1} &= g_{i+1}(a_i) \\ a_{i+2} &= g_{i+2}(a_i \oplus a_{i+1}) \\ i &= i+2 \end{aligned}$$

Define the $24 \times 2 \times 4$ subkey table

$$\kappa[2i+k]_{j,t} = a_{i,r},\ \ k = r/8;\ \ j = (r/4)\%2;\ \ t = r\%4;\ \ 0 \leq r \leq 15;$$

where $0 \leq i \leq 11$, $a_{i,r}$ is the r^{th} byte of a_i, $\kappa[i]_{j,t}$ is the t^{th} byte of the 4 byte array $\kappa[i]_j$ and a_i is considered as a 16 byte vector.

5 Cryptanalysis of Gomeğo

5.1 Differential Cryptanalysis

We use the wide trail strategy to consider the possibility of a differential attack against Gomeğo. In particular, we need only count the number of active Gs in any differential trail in order to approximate the number of active S-boxes in such a trail. Consider an XOR difference in round i with one active byte in either x_1 or x_2 (otherwise simply set $i = i + 1$). Then in the i^{th} round, we have exactly one active G.

In the worst case, suppose each round has exactly one active G. Then an 8 round differential trail will have at least 8 active Gs. Thus a 10 round differential trail will have at least 32 active S-boxes.

Therefore, any 10 round differential trail will have at least 32 active S-boxes giving a propagation ratio of at most 2^{-160}.

We conclude, a differential attack on Gomeğo with $r \geq 10$ rounds is unlikely.

5.2 Linear Cryptanalysis

As in the case of differential cryptanalysis above, any 10 round linear trail will have at least 32 active S-boxes. This implies that any 10 round linear trail will have correlation ratio at most 2^{-64}.

Therefore, a linear attack on $r \geq 10$ round Gomeõ is unlikely.

5.3 Interpolation Attack

The Interpolation attack was introduced by Jackobsen and Knudsen in [9]. The attack seeks to construct polynomial equivalents to a cipher using plaintext/ciphertext pairs. The attack can also be modified to obtain the key.

The attack is feasible if the cost of constructing the polynomials (i.e. finding the coefficients) is less than the cost of encrypting plaintexts needed for the attack, that is, if the round functions have low algebraic degree and/or have a sparce polynomial representation over $\mathbb{F}_{2^8}$ [5, 7].

The high algebraic degree of the φ_i (7), and their compact expression over $\mathbb{F}_{2^8}$ (253 coefficients) and the double layer of non-linearity in G ensures that the interpolation attack against the full version Gomeõ is unlikely.

5.4 Related-Key Attacks

Related-key attacks [10] are successful in key schedules with low diffusion and non-linearity. The Gomeõ key schedule is based on the high non-linearity and complete diffusion in the g permutation.

These properties plus the chaining of successive outputs (subkeys) ensure that related-key attacks on Gomeõ is unlikely.

6 Conclusions and Future Work

We have presented a new cryptographic algorithm based on the Feistel Network. This algorithm acts on 128-bit blocks (128-bit key).

Further work can be done on defining a variable length key schedule algorithm.

References

[1] D. Stinson: *Cryptography, Theory and Practice*, Chapman & Hall/CRC, Second Edition, pp 78, 2002

[2] B. Schneier: *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Inc., 1996

[3] F. J. MacWilliams N. Sloane: *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library, Volume 16, pp 93-124, 2006

[4] J. Daemen: *Cipher and Hash Function Design Strategies Based on Linear and Differential Cryptanalysis*, PHD Desertation, K.U. Leuven, March 1995

[5] V. Rijmen and J. Daemen: *The Design of Rijndael*, Information Security and Cryptography, Springer-Verlag, Vol xvii No. 238, p. 48-, 2002

[6] E. Biham and Shamir: *Differential Cryptanalysis of DES-like Cryptosystems*, Journal of Cryptology, Vol. 4 No. 1, pp 3-72, 1991

[7] B. Schneier et al: *The Twofish Encryption Algorithm*, John Wiley & Sons, 1996

[8] M. Matsui: *Linear Cryptanalysis Method for DES Cipher*, Advances in Cryptology, Proceedings Eurocrypt'93, LNCS 765, Springer Verlag, pp 386-397, 1994

[9] T. Jacobsen and L. R. Knudsen: *The Interpolation Attack on Block Ciphers*, Fast Software Encryption, LNCS 1267, Springer-Verlag, pp 28-40, 1997

[10] E. Biham: *New Types of Cryptanalytic Attacks Using Related Keys*, Journal of Cryptology, Vol. 7 No. 4, pp 229-246, 1994