The Block Cipher Thuça

Isaiah Makwakwa*

March 31, 2011

Abstract

We present a 64-bit (128-bit key) byte-oriented block cipher. It is a Feistel Network in which the diffusion layer of the round function is based on the extended diffusion block (e-block).

Keywords
e-block, affine transformation, circular rotations

1 Introduction

Thuça is a 64-bit Feistel Network in which the round permutation has three layers: key addition, substitution and diffusion.

It uses a 128-bit master key from which 32-bit subkeys are derived. The Thuça substitution layer uses fixed S-boxes based on the inverse function and 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, Thuça 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 [9]. 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 $f(x)$ [2].

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) [2, 7].

2.3 Linear Cryptanalysis

Linear cryptanalysis of block ciphers was introduced by Matsui in [10]. 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 [2].

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) [7].

2.4 Wide Trail Strategy

In [6], 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 [7].

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 Pseudo-Hadarmard Transform 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 [1]. 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 Thuça Cipher

3.1 Representation of State in Thuça

Let x be a 64-bit vector. State [7, 2] in Thuça is respresented as an 8 byte vector $x = (x_0, x_1, x_2, x_3) \in (\mathbb{F}_2^{16})^4$ where the 16-bit component vectors, x_i, are defined as $x_i = (x_{i,0}, x_{i,1}) \in (\mathbb{F}_2^8)^2$.

3.2 The Thuça Substitution Layer

The substitution layer in Thuça is based on the inverse map over $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/(x^8 + x^4 + x^4 + x^3 + x^2 + 1)$, affine equivalence of S-boxes [5, 4] and the isomorphism between the field $\mathbb{F}_{2^8}$ and the vector space $\mathbb{F}_2^8$ [3].

In particular [2], let $a = (a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0) \in \mathbb{F}_2^8$, define

$$a(x) = \sum_{i=0}^{7} a_i x^i.$$

Let $v_i(x), u_i(x), c_i(x) \in \mathbb{F}_2[x]/(x^8 + 1)$ be defined by

$$\begin{aligned} v_0(x) &= x^7 + x^5 + x^3 + x + 1 \\ v_1(x) &= x^7 + x^6 + x^5 + x^2 + 1 \\ c_0(x) &= x^7 + x^4 + x + 1 \\ c_1(x) &= x^7 + x^5 + x^4 + x^3 + x + 1. \end{aligned}$$

Then for any $a(x) \in \mathbb{F}_{2^8}$, define affine permutations, ϑ_i, on $\mathbb{F}_{2^8}$ by

$$\vartheta_i(a(x)) = a(x)v_i(x) + v_i(x)c_i(x) \ mod \ x^8 + 1; \quad 0 \leq i \leq 1 \qquad (1)$$

Further, let $\pi : \mathbb{F}_{2^8} \rightarrow \mathbb{F}_{2^8}$ be the inverse map and set $\pi(0) = 0$ (where 0 is the zero polynomial). Then the Thuça S-boxes, φ_i, are defined by

$$\varphi_i(a(x)) = \pi \circ \vartheta_i(a(x)); \quad 0 \leq i \leq 1. \tag{2}$$

The S-boxes, φ_0 and φ_1 are given in **Table 1** and **Table 2** 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	F4	05	56	23	C0	F0	FE	95	8A	4C	CD	F6	42	A5	E5	CA
10	0D	1A	EF	34	0B	62	92	BB	9E	19	15	94	67	1D	96	C2
20	2E	76	5E	55	03	0F	A2	BE	B7	8D	D6	40	E3	EA	8F	47
30	79	9C	89	C1	5B	1C	2C	D5	10	D0	52	FF	7B	74	24	C8
40	77	8C	33	CC	6D	48	B1	A4	06	5F	9D	01	72	DE	A0	AD
50	53	25	B9	1E	CE	3A	FC	FD	7C	3C	7F	AC	84	49	D4	58
60	D3	50	36	3E	F9	D9	F8	73	32	8E	A7	80	DF	18	EC	4F
70	FB	38	F3	B2	09	B6	39	68	4B	63	59	66	E4	2B	0C	46
80	6A	12	27	70	AF	5D	6B	0E	08	78	61	1F	2F	B4	6E	88
90	F7	16	C3	00	86	4D	7A	EB	28	DD	3D	E0	69	43	31	AE
A0	E2	B0	9B	A3	90	04	26	75	F2	8B	22	44	21	3B	C5	BA
B0	13	93	91	BF	A8	35	82	87	9F	CF	D1	07	60	17	B8	4E
C0	C9	AB	57	83	E8	B3	A1	E7	7E	BC	64	AA	14	30	DA	6C
D0	C4	A9	F5	3F	5C	85	A6	29	E1	41	0A	FA	1B	54	EE	ED
E0	37	11	20	65	97	99	C6	D2	C7	E6	6F	BD	F1	45	DC	7D
F0	B5	2D	4A	2A	D7	71	DB	98	51	CB	D8	5A	81	9A	E9	02

Table 2: The φ_1 S-box

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

The choice of $v_i(x)$ and $c_i(x)$ ensure that the resultant φ_0 and φ_1 have no fixed points. Both S-boxes have maximum differential propagation ratio 2^{-6} and maximum linear correlation ratio 2^{-3} [5, 4].

3.3 Key Addition Layer

Let κ denote the 20×4 subkey table from the key schedule algorithm. For any $x = (x_j, x_k) \in (\mathbb{F}_2^{16})^2$ define the round key addition function

$$\psi_i(x) = (x_{j,0} \oplus \kappa[i]_0, x_{j,1} \oplus \kappa[i]_1, x_{k,0} \oplus \kappa[i]_2, x_{k,1} \oplus \kappa[i]_3)$$

where $\kappa[i]_r$ is the rth byte of $\kappa[i]$ and $x_{r,s}$ is the sth byte of x_r.

3.4 The Diffusion Layer

Let $x = (x_j, x_k) \in (\mathbb{F}_2^{16})^2$. Define the 32-bit linear function ϕ by

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

where

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

Then ϕ has the following properties

1. ϕ is a linear permutation on $(\mathbb{F}_2^8)^4$.
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 Word Swapping Function

Let $x = (x_0, x_1, x_2, x_3) \in (\mathbb{F}_2^{16})^4$, be an 8 byte vector. Define the word swapping involution, λ, by

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

This function is also used in the Twofish cipher [8].

3.6 The Number of Rounds

Thuça is an iterative block cipher with 16 rounds. Therefore, since complete diffusion in Thuça takes place after 3 rounds, Thuça has 5 complete diffusions.

3.7 Circular Rotations

Some algebraic attacks (e.g. the Square attack) on byte-oriented block ciphers exploit the existence of byte boundaries in the ciphertext. Thuça implements circular rotations on the first and last 16-bit words of the data in each round to erase byte boundaries.

A single right circular rotation in Thuça is denoted τ_r while as a single left circular rotation is denoted τ_l.

3.8 Initial And Final Whitening

Let $x = (x_0, x_1, x_2, x_3) \in (\mathbb{F}_2^{16})^4$, then the initial whitening key addition function, ω_0, is defined by

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

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

$$\omega_1(x) = (\psi_{22}(x_0, x_1), \psi_{23}(x_2, x_3)) .$$

3.9 Encryption Function

Let $x = (x_0, x_1, x_2, x_3) \in (\mathbb{F}_2^{16})^4$, define

$$\nu_i(x) = (\chi_0 \oplus \tau_r(x_0))x_1x_2(\chi_1 \oplus \tau_r(x_3))$$

where

$$\chi_0, \chi_1 = \phi \circ \varphi \circ \psi_i(x_2, x_1)$$

and

$$\varphi(x_j, x_k) = \varphi_0(x_j), \varphi_1(x_k)$$

with φ_i and $\oplus$ applied byte-wise.

The Thuça encryption round function is defined by

$$\theta_i = \lambda \circ \nu_i(x)$$

Therefore, the Thuça encryption function is defined as

$$f(x) = \omega_1 \circ \lambda \circ \left(\bigcirc_{i=0}^{15} \theta_i\right) \circ \omega_0(x)$$

3.10 Decryption Function

Let $y = (y_0, y_1, y_2, y_3) \in (\mathbb{F}_2^{16})^4$, define

$$\nu_i^{-1}(y) = \tau_l(\chi_0 \oplus y_0)y_1y_2\tau_l(\chi_1 \oplus y_3)$$

where

$$\chi_0, \chi_1 = \phi \circ \varphi \circ \psi_i(y_2, y_1)$$

and

$$\varphi(y_j, y_k) = \varphi_0(y_j), \varphi_1(y_k)$$

with φ_i and $\oplus$ applied byte-wise.

The Thuça decryption round function is defined by

$$\theta_i^{-1} = \lambda \circ \nu_i^{-1}(y)$$

Thus, the Thuça decryption function is defined by

$$f^{-1}(y) = \omega_0 \circ \lambda \circ \left(\bigcirc_{i=15}^{0} \theta_i^{-1}\right) \circ \omega_1(y)$$

3.11 Thuça Constants

The Thuça round constants, C_i, $(0 \leq i \leq 5)$, are defined by

$$C_{i,j} = \varphi_1(7i + (16 - i)j), \quad 0 \leq j \leq 15$$

where $C_{i,j}$ is the jth byte of C_i and φ_1 is applied byte-wise.

4 Key Schedule Algorithm

4.1 Key Addition Function

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

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

where $C_{i,k}$ is the kth byte of C_i.

Note that we abuse notation on $x_k \in (\mathbb{F}_2^8)^4$ (a 4 *byte vector*) to indicate the position of its *first byte*, the $4k^{th}$ byte, in a 128 bit string. Such a notation is useful in the definition of the key schedule round function below.

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 The ϕ Linear Transformation

Let $x_k = (x_{4k}, x_{4k+1}, x_{4k+2}, x_{4k+3}) \in (\mathbb{F}_2^8)^4$. Define the 32-bit linear transformation ϕ by

$$\phi(x_k) \quad = \quad e_{8,5}(y_{4k}, y_{4k+2}), e_{8,3}(y_{4k+1}, y_{4k+3})$$

where

$$y \quad = \quad e_{8,3}(x_{4k}, x_{4k+1}), e_{8,5}(x_{4k+2}, x_{4k+3}).$$

4.4 The G Function

Let $x_k = (x_{4k}, x_{4k+1}, x_{4k+2}, x_{4k+3}) \in (\mathbb{F}_2^8)^4$, define a composite primitive

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

where φ_i is applied byte-wise.

4.5 The Thuça Key Schedule

Let $x = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \in ((\mathbb{F}_2^8)^4)^4$, the Thuça key schedule round function is defined by

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

where ϕ is applied row-wise.

Let $a_{-1} \in ((\mathbb{F}_2^8)^4)^4$ be the master key, define

$$a_0 = \rho_0(a_{-1})$$

Initialise $i = 1$, then a round of the 2 round Thuça key schedule is defined by

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

Define the 20×4 subkey table

$$\kappa[4i + k]_j = a_{i,r}, \;\; k = (r/4); \;\; j = (r\%4); \tag{3}$$

for $0 \leq i \leq 4$, $a_{i,s}$ is the sth byte of a_i and $\kappa[r]_s$ is the sth byte of $\kappa[r]$.

5 Cryptanalysis of Thuça

5.1 Differential Cryptanalysis

We use the wide trail strategy to consider the possibility of a differential attack against Thuça. Consider an XOR difference in round i with one active byte in either x_1 or x_2 (otherwise simply set $i = i + 1$). By the diffusion characteristics of ϕ, the output XOR will have 4 active bytes (in x_0 and x_3).

Since x_0 and x_3 become the middle word in round $i+1$, the diffusion layer guarantees that in round $i+1$ at least one of x_1 and x_2 will be XOR'ed with at least one active byte. Therefore, any $i + 1$ differential trail involving x_1 and/or x_2 will have at least 4 active S-boxes. Hence, by the $(i + 2)^{th}$ round, any differential trail will have at least 4 active S-boxes. Consequently, any three round diferential trail will have at least 4 active S-boxes.

Therefore, after 10 rounds any Thuça differential trail will have propagation ratio at most 2^{-72}.

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

5.2 Linear Cryptanalysis

As in the case of differential cryptanalysis above, any three round linear trail will have at least 4 active S-boxes. This implies that any 10 round linear trail will have correlation ratio at most 2^{-36}.

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

5.3 Interpolation Attack

The Interpolation attack was introduced by Jackobsen and Knudsen in [11]. 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 $\mathbb{F}_{2^8}$ [8, 7].

In Thuça, φ_0 has algebraic degree 7 and 253 coefficients while φ_1 has degree 7 and 254 coefficients. This limits efficient polynomial representation of the Thuça primitive to a few rounds.

Therefore, an interpolation attack against the full version Thuça is unlikely.

5.4 Related-Key Attacks

Related-key attacks [12] are successful in key schedules with low diffusion and non-linearity. The Thuça key schedule is based on the high non-linearity and complete diffusion in the ρ permutation.

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

6 Conclusions and Future Work

We have presented a new cryptographic algorithm based on the Feistel framework. This algorithm acts on 64-bit blocks (128-bit key) using key based S-boxes.

Further work can be done on defining a 128-bit Substitution Permutation Network based on the key schedule algorithm.

References

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

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

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

[4] C. Carlet et al: *Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems*, Design Codes and Cryptography, Kluwer Academic Publishers, 1998

[5] K. Nyberg: *Differential Uniform Mappings for Cryptology*, Advances in Cryptology, Proceedings Eurocrypt'93, LNCS 765, Springer Verlag, pp 55-64, 1994

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

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

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

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

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

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

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