

KALE: A High-Degree Algebraic-Resistant Variant of The Advanced Encryption Standard

Spendon Gavekort

c/o Vakiopaine Bar
Kauppakatu 6, 40100 Jyväskylä FINLAND
mjos@iki.fi

Abstract. We have discovered that the S-Box of AES is in fact affine-equivalent to a trivial algebraic transform of low degree and short cycle; inversion operation in the finite field $\text{GF}(2^8)$. This transformation is an involution and hence has an unacceptably low cycle length. Furthermore the algebraic degree of the underlying permutation is extremely low, lower than zero: $\deg x^{-1} = -1$, making it vulnerable to Euclid-Courtois-Gavekort-Schneier (ECGS) algebraic attacks. We propose KALE, a more secure variant that replaces the algebraic component of the S-Box with square root operation $\sqrt{x}$ in the same finite field. All other parameters remain the same. We discuss the obvious security advantages of the new variant and show that it is provably secure.

Keywords: AES, KALE, Algebraic Cryptanalysis, Serpessence.

1 Introduction

The Rijndael algorithm was adopted as Advanced Encryption Standard (AES) by U. S. NIST in 2001 in FIPS-197 [6]. AES is currently widely deployed around the world and frequently used by unsuspecting users. In this note we show that a key component of AES in fact contains a backdoor the allows the Belgian Government and The Catholic Church (the forces behind Rijndael / AES design, who obviously hid the backdoor in the cipher) to secretly eavesdrop on all AES communications. This is why the National Security Agency has been actively promoting the use of AES in public networks [1, 5, 8, 10].



Fig. 1. This paper describes an extremely efficient potential algebraic attack against the U. S. Advanced Encryption Standard (AES).

2 Key Observation

We have discovered that the AES S-Box is in fact affine equivalent to a low-degree algebraic function. The government has tried to hide this fact by masking the function with a simple convolutional affine transform:

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \quad (1)$$

We may write the AES S-Box as composite function $S = A \circ S'$. When the bitwise affine transform $A : b \mapsto b'$ of Equation 1 is removed, we discovered that the underlying transform is in fact the inverse operation $S' : x \mapsto 1/x$ in the finite field $\text{GF}(2^8)$ defined by irreducible polynomial $p(x) = x^8 + x^4 + x^3 + x + 1$.

3 Security Analysis

We see that the algebraic degree of the underlying transform is $\deg S' = -1$. This degree is very low, in fact lower than zero, the degree recommended by the Chinese Government (“sinkhole transform”). For reference, the U.S. National Security Agency recommends degree 1 (“the identity transform”) for all but the most confidential data. AES has been clearly designed to offer even lower security than these proposals against Algebraic Attacks of Courtois [3].

Bruce Schneier (in joint work with Euclid) has developed an algorithm to compute multiplicative inverses in rings mod n , even when the factorization of n is not known. We see that $e = -1$ is clearly unsuitable for modern cryptography [11]. We call this the Euclid-Courtois-Gavekort-Schneier (ECGS) Algebraic Attack on AES. Based to extrapolations from reduced versions, we estimate that attack complexity against AES-128 is $2^{127.926535897932384626433832795028842}$ with 2^{127} precomputation.

4 New Technique: Irrational Algebraic Permutations

From RSA cryptanalysis we know that the exponent $e > 1$ must be coprime with $\phi(\mathbb{F})$, in other words $\gcd(e, 255) = 1$. This immediately rules out all smallest primes 3 and 5. However, the security of RSA has never been shown to be even equivalent to factoring, unlike the Rabin cryptosystem. RSA should not be considered to be a secure algorithm since (according to CRYPTO Program Committee) a cryptosystem cannot be secure unless it is provably secure under some arbitrary set of assumptions which can be freely chosen by the author.

Table 1. The S-Box of KALE.

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	63	7C	FF	E0	5D	42	C1	DE	6D	72	F1	EE	53	4C	CF	D0
1x	1F	00	83	9C	21	3E	BD	A2	11	0E	8D	92	2F	30	B3	AC
2x	48	57	D4	CB	76	69	EA	F5	46	59	DA	C5	78	67	E4	FB
3x	34	2B	A8	B7	0A	15	96	89	3A	25	A6	B9	04	1B	98	87
4x	9B	84	07	18	A5	BA	39	26	95	8A	09	16	AB	B4	37	28
5x	E7	F8	7B	64	D9	C6	45	5A	E9	F6	75	6A	D7	C8	4B	54
6x	B0	AF	2C	33	8E	91	12	0D	BE	A1	22	3D	80	9F	1C	03
7x	CC	D3	50	4F	F2	ED	6E	71	C2	DD	5E	41	FC	E3	60	7F
8x	02	1D	9E	81	3C	23	A0	BF	0C	13	90	8F	32	2D	AE	B1
9x	7E	61	E2	FD	40	5F	DC	C3	70	6F	EC	F3	4E	51	D2	CD
Ax	29	36	B5	AA	17	08	8B	94	27	38	BB	A4	19	06	85	9A
Bx	55	4A	C9	D6	6B	74	F7	E8	5B	44	C7	D8	65	7A	F9	E6
Cx	FA	E5	66	79	C4	DB	58	47	F4	EB	68	77	CA	D5	56	49
Dx	86	99	1A	05	B8	A7	24	3B	88	97	14	0B	B6	A9	2A	35
Ex	D1	CE	4D	52	EF	F0	73	6C	DF	C0	43	5C	E1	FE	7D	62
Fx	AD	B2	31	2E	93	8C	0F	10	A3	BC	3F	20	9D	82	01	1E

In [9] Rabin shows that computation of square root in a finite ring is actually equivalent to factoring a large composite number. We therefore choose $x \mapsto \sqrt{x}$ as our fundamental transform. The main drawback of the Rabin cryptosystem is that in prime fields each element x has two square roots $\pm\sqrt{x}$, and effort has to be made in order to identify the correct root. This would also make the S Box non-surjective, and therefore vulnerable to Impossible Differential Attacks such as the Impossible Boomerang Attack (IBA) which are especially dangerous as impossible boomerangs are truly impossible while regular boomerangs are possible boomerangs [2].

However, finite fields of characteristic two (such as our $\text{GF}(2^8)$) have an unique $\sqrt{x}$ for each x , including -1 . Since $\sqrt{-1}$ is clearly defined, we call the resulting S-Box an **Irrational Permutation** (IP).

4.1 High-Degree Variant KALE

Figure 4 shows the S-Box used by KALE. The S-Box is the only difference between KALE and AES. Appendix A gives a full trace of KALE-128 execution that can be used to verify implementation correctness. There are no other modifications to the Key Schedule, number of rounds, etc. Note that the very first elements are unchanged since zero mapped to zero in the AES inversion and $\sqrt{0} = 0$, and furthermore $1^{-1} = \sqrt{1}$. The same masking constant **0x63** is used.

The algebraic degree of $\sqrt{x}$ in real and complex fields is $\frac{1}{2}$, but in a multiplicative subgroup of finite field of size $2n$ it is actually n . Therefore the degree is actually 128. We may write interchangeably $\sqrt{x} = x^{128}$. The cycling properties are also greatly improved for S' .

5 Conclusions and Discussion

We have discovered that the AES S-Box can be decomposed into two affine and algebraic parts: $S = A \circ S'$, where A is an binary affine transform and S' is a low degree inversion transform $S' : x \mapsto x^{-1}$. The degree of hidden algebraic transform is therefore $\deg S' = -1$. Having a degree lower than zero is of course extremely dangerous and makes AES immediately highly vulnerable to potential advanced Euclid-Courtois-Gavekort-Schneier (ECGS) attacks.

We have proposed a minor tweak to AES that replaces the algebraic transform $S' : x \mapsto x^{-1}$ with a secure discrete square root transform $S' : x \mapsto \sqrt{x}$. The square root transform has been proven secure by Rabin. Furthermore its algebraic degree is 128, making it highly resistant to ECGS attacks..

As the ECGA attack is based on Algebraic Cryptanalysis and since the culprits behind the AES backdoor allegedly worked for a Catholic University in Leuven, Belgium, we suspect that Papal and Belgian Secret Service pressure explains why the Courtois' highly effective AES attacks were never fully disclosed in the open literature [3].

The security of KALE against post-quantum [4], neuromorphic and optogenetic [7], and other postmodern attacks is unknown at this point. However, the use of complex numbers should rule out any real or rational quantum attacks.

References

1. BURGIN, K., AND PECK, M. Suite B Profile for Internet Protocol Security (IPsec). IETF RFC 6380, October 2011.
2. CHOY, J., AND YAP, H. Impossible boomerang attack for block cipher structures. In *IWSEC 2009* (2009), T. Takagi and M. Mambo, Eds., vol. 5824 of *LNCS*, Springer, pp. 22–37.
3. COURTOIS, N. How fast can be algebraic attacks on block ciphers? IACR ePrint 2006/168, eprint.iacr.org/2006/168, May 2006.
4. FINIASZ, M. Syndrome based collision resistant hashing. In *Post-Quantum Cryptography: Second International Workshop, PQCrypto 2008* (2008), J. Buchmann and J. Ding, Eds., vol. 5299 of *LNCS*, Springer, pp. 137–147.
5. IGOE, K. Suite B Cryptographic Suites for Secure Shell (SSH). IETF RFC 6239, May 2011.
6. NIST. Advanced Encryption Standard (AES). FIPS 197, 2001.
7. NSA. Annual report 2014 NSA TC, IEEE CAS society. http://ewh.ieee.org/soc/icss/committees/nsatc/reports/2014_NSATC_Annual_Report.pdf, May 2014.
8. NSA. Suite B Cryptography. www.nsa.gov/ia/programs/suiteb_cryptography, June 2014.
9. RABIN, M. C. Digitalized signatures and public-key functions as intractable as factorization. Tech. Rep. 212, Massachusetts Institute of Technology / LCS, 1979.
10. SALTER, M., AND HOUSLEY, R. Suite B Profile for Transport Layer Security (TLS). IETF RFC 6460, January 2012.
11. SCHNEIER, B. *Applied Cryptography*. John Wiley & Sons, 1994.

A Trace of Execution for KALE-128

The test trace contains intermediate values and all subkeys. The format is similar to that of Appendix C.1 of FIPS 197 [6].

PLAINTEXT BLOCK	00 11 22 33	44 55 66 77	88 99 AA BB	CC DD EE FF
SECRET KEY DATA	00 01 02 03	04 05 06 07	08 09 0A 0B	0C 0D 0E 0F
round[0].input	00 11 22 33	44 55 66 77	88 99 AA BB	CC DD EE FF
round[0].k_sch	00 01 02 03	04 05 06 07	08 09 0A 0B	0C 0D 0E 0F
round[1].start	00 10 20 30	40 50 60 70	80 90 A0 B0	C0 D0 E0 F0
round[1].s_box	63 1F 48 34	9B E7 B0 CC	02 7E 29 55	FA 86 D1 AD
round[1].s_row	63 E7 29 AD	9B 7E D1 34	02 86 48 CC	FA 1F B0 55
round[1].s_col	70 60 3A 2A	4A 3B 00 71	11 01 5B 4B	2B 5A 61 10
round[1].k_sch	4D CE D2 50	49 CB D4 57	41 C2 DE 5C	4D CF D0 53
round[2].start	3D AE E8 7A	03 F0 D4 26	50 C3 85 17	66 95 B1 43
round[2].s_box	1B 85 DF 5E	E0 AD B8 EA	E7 79 23 A2	12 5F 4A 18
round[2].s_row	1B AD 23 18	E0 79 4A 5E	E7 5F DF EA	12 85 B8 A2
round[2].s_col	E1 27 D8 93	44 92 EF B4	01 C9 38 7D	AA 72 01 54
round[2].k_sch	06 48 B6 E4	4F 83 62 B3	0E 41 BC EF	43 8E 6C BC
round[3].start	E7 6F 6E 77	0B 11 8D 07	0F 88 84 92	E9 FC 6D E8
round[3].s_box	6C 03 1C 71	EE 00 2D DE	D0 0C 3C E2	C0 9D 9F DF
round[3].s_row	6C 00 3C DF	EE 0C 9F 71	D0 9D 1C DE	C0 03 2D E2
round[3].s_col	3B F7 6E 2D	3D 3D 54 58	C5 0B 0C 4D	51 53 A4 AA
round[3].k_sch	AC C8 D3 FC	E3 4B B1 4F	ED 0A 0D A0	AE 84 61 1C
round[4].start	97 3F BD D1	DE 76 E5 17	28 01 01 ED	FF D7 C5 B6
round[4].s_box	C3 87 7A 99	2A 6E F0 A2	46 7C 7C FE	1E 3B DB F7
round[4].s_row	C3 6E 7C F7	2A 7C DB 99	46 3B 7A A2	1E 87 F0 FE
round[4].s_col	A4 6C 57 B9	92 3D 4B F0	19 1C 74 D4	A0 FE 7B B2
round[4].k_sch	98 67 FC 79	7B 2C 4D 36	96 26 40 96	38 A2 21 8A
round[5].start	3C 0B AB C0	E9 11 06 C6	8F 3A 34 42	98 5C 5A 38
round[5].s_box	04 EE A4 FA	C0 00 C1 58	B1 A6 0A 07	70 D7 75 3A
round[5].s_row	04 00 0A 3A	C0 A6 75 FA	B1 D7 A4 58	70 EE C1 07
round[5].s_col	38 20 5E 72	E5 F2 99 67	E7 AB DD 0B	0F E8 0E B1
round[5].k_sch	3D 30 6C 43	46 1C 21 75	D0 3A 61 E3	E8 98 40 69
round[6].start	05 10 32 31	A3 EE B8 12	37 91 BC E8	E7 70 4E D8
round[6].s_box	42 1F A8 2B	AA 7D 5B 83	89 61 65 DF	6C CC 37 88
round[6].s_row	42 7D 65 88	AA 61 37 2B	89 CC A8 83	6C 1F 5B DF
round[6].s_col	EE 9F 76 D5	F0 1A D8 E5	6D 6A 90 F9	7D 60 BF 55
round[6].k_sch	6D AB CD 9C	2B B7 EC E9	FB 8D 8D 0A	13 15 CD 63
round[7].start	83 34 BB 49	DB AD 34 0C	96 E7 1D F3	6E 75 72 36
round[7].s_box	81 0A D8 8A	0B 06 0A 53	DC 6C 30 2E	1C ED 50 96
round[7].s_row	81 06 30 96	0B 6C 50 8A	DC ED D8 53	1C 0A 0A 2E
round[7].s_col	B5 4B 46 99	78 A9 42 2E	04 3D 6F EC	02 38 70 78
round[7].k_sch	13 7E FE 00	38 C9 12 E9	C3 44 9F E3	D0 51 52 80

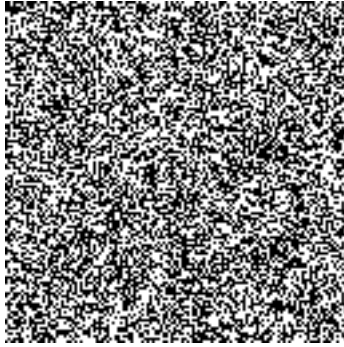
round[8].start	A6 35 B8 99 40 60 50 C7 C7 79 F0 0F D2 69 22 F8
round[8].s_box	8B 15 5B 6F 9B B0 E7 47 47 DD AD D0 1A A1 D4 A3
round[8].s_row	8B B0 AD A3 9B DD D4 6F 47 A1 5B 47 1A 15 E7 D0
round[8].s_col	C8 BF 84 C6 EA 32 44 61 6A B4 99 BD 3C D2 B1 67
round[8].k_sch	6B 05 FC 86 53 CC EE 6F 90 88 71 8C 40 D9 23 0C
round[9].start	A3 BA 78 40 B9 FE AA 0E FA 3C E8 31 7C 0B 92 6B
round[9].s_box	AA C7 C2 9B 44 01 BB CF 3F 04 DF 2B FC EE E2 3D
round[9].s_row	AA 01 DF 3D 44 04 E2 9B 3F EE C2 CF FC C7 BB 2B
round[9].s_col	AE EF 49 41 FD EA 29 07 5A 6A 04 E8 21 94 2B 35
round[9].k_sch	E7 CE AF 1D B4 02 41 72 24 8A 30 FE 64 53 13 F2
round[10].start	49 21 E6 5C 49 E8 68 75 7E E0 34 16 45 C7 38 C7
round[10].s_box	8A 57 73 D7 8A DF BE ED 60 D1 0A BD BA 47 3A 47
round[10].s_row	8A DF 0A 47 8A D1 3A D7 60 47 73 ED BA 57 BE BD
round[10].k_sch	B5 52 9E 93 01 50 DF E1 25 DA EF 1F 41 89 FC ED
round[10].output	3F 8D 94 D4 8B 81 E5 36 45 9D 9C F2 FB DE 42 50

B Serpessence (Spoiler)

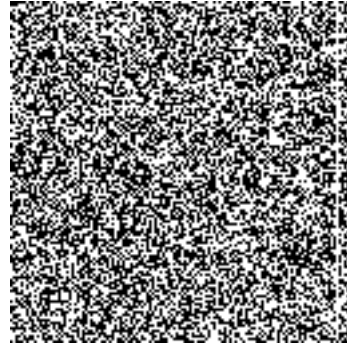
Since the squaring operation $x \mapsto x^2$ in any binary field is bitwise linear, so is its inverse, the “square root” operation. As AES contains no other nonlinear parts apart from its S-Box, the KALE transform is actually fully linear. The encryption of some given plaintext for any number of rounds can be written as a $128 \times k$ matrix M (and constant 128-bit vector addition) where k is the key size in bits. The key for (say) KALE-128 with ten million rounds can usually be recovered via a single known plaintext block and a binary matrix multiplication with M^{-1} . We have verified this to work.

So unless a code reviewer is capable of checking the properties of a random-looking S-Box lookup table, you’re screwed. The actual code is 100 % AES.

For 10-round KALE with full key schedule, here’s the matrix that can be used to “encrypt” a zero block with any 128-bit key, and its inverse which yields the original key from ciphertext with 50 % probability (one bit wouldn’t invert). These matrices are really random-looking – but don’t be fooled, the transform is fully linear and therefore broken.



Encryption matrix M :
 $\text{KALE} - 128_K(0) = M \cdot K \oplus C.$



Key recovery matrix M^{-1} :
 $M^{-1} \cdot (\text{KALE} - 128_K(0) \oplus C) = K.$