The Design Of Rijndael – Errata

Version: 30 July 2009

p5, l-3: remove second that

p11, (2.10): replace second $(a \odot v)$ by $(b \odot v)$

p12, l19: replace te by the

p18, l-12: replace $(n-k) \times k$ by $(n-k) \times n$

p22, (2.44): left bracket is missing in $b_{(i,m)}$ and $a_{(i,m)}$

p32, l-7: replace $k_{4,1}$ by $k_{0,2}$

p36, l-2 and l-1: Replace the text on these lines by: The affine transformation f can also be described as a linearized polynomial over $\mathrm{GF}(2^8)$, followed by the addition (in $\mathrm{GF}(2^8)$) with a constant. This is explained in Appendix C,

p51, Fig 3.12: also in the second round, SubBytes should be depicted before ShiftRows

p56, l14: remove that after they

p60, l-10: remove a before self-inverse

p64, l7: remove storage after memory

p65, l-8: remove the before Sect.

p67, l-1: replace $a_{0,i-j}$ by $a_{0,j-i}$

p69, l-1: remove in before modulo

p72, l18: replace efficiently generating by to generate efficiently

p75, l-16: replace nth by rth

p78, l-8: replace $i+1$ by $i-1$

p82, l-4: replace $a_1 + 2a_6$ by $2a_1 + a_6$ and replace $a_2 + 2a_3 + 4a_4 + 8a_5$ by $8a_2 + 4a_3 + 2a_4 + a_5$

p93, l8: remove the

p96, l9: replace $\mathrm{C}_{u,v}^{(h^{(2)})}$ by $\mathrm{C}_{\mathbf{u},\mathbf{v}}^{(h^{(2)})}$

p96, (7.28): change the order of $h^{(1)}$ and $h^{(2)}$

p97, l-9 and l-7: matrix C is in the wrong font

p97, l-11 and l-9 and l-5: replace n by 2^n

p97, (7.33): replace $(-1)^{\mathbf{w}^{\mathrm{T}} a}$ by $(-1)^{\mathbf{w}^{\mathrm{T}} \mathbf{a}}$

p107, l2: replace $\mathrm{U}_i \oplus \mathrm{U}_j^{\mathrm{T}}$ by $(\mathrm{U}_i \oplus \mathrm{U}_j)^{\mathrm{T}}$

p116, (8.14): replace $C^{\mathrm{u,w}2}$ by $\mathrm{C}^2_{\mathrm{u,w}}$

p116, (8.15): replace C by C, replace w by w, replace u by u

p118, l11: replace "the differential steps of a linear trails" by "the steps of a differential trail"

p124, l17: replace trial by trail

p128, l-4: replace not need not by need not

p128, l-1: third element of the vector should be $a_1 \oplus a_3 \oplus a_4 \oplus a_5$

p131, l17: remove each before permutations

p132, equation (9.9): $\mathcal{B}(\phi) = ...$

p134, Fig 9.3: in the second round, replace $\mathrm{k}^{(1)}$ by $\mathrm{k}^{(2)}$

p136, l4: second matrix is $\mathrm{C}_{\xi(1)}$

p144, l2: replace A by A^{T}

p144, l4: replace two times A^t by A

p144, l17: replace "all sets of two columns in $\mathrm{H} = [-\mathrm{A}^t\ \mathrm{I}]$ are independent, but no set of three independent columns exists" by "all columns in but two $\mathrm{H} = [-\mathrm{A}\ \mathrm{I}]$ are independent, but two columns are equal, hence dependent.

p144, l-5: $[\mathrm{I}\ \mathrm{A}^{\mathrm{T}}]$ is a generator matrix for $\mathcal{C}_\theta$ and $[\mathrm{A}\ \mathrm{I}]$ is a generator matrix for the dual.

p144, l-3: replace [A^{T} I] by [A I]
p150, l7: replace byte transposition MixColumns by byte transposition ShiftRows
p153, l-9 and l-4: replace ciphertexts by plaintexts
p168, l11: remove and before is defined
p177, (A.3): replace $\oplus$ by $+$
p178, l-5: replace $2^{1-n}r$ by $2^{1-n}r - 1$
p180, (A.28): replace two times Tr by f
p196, l-4: replace "by x_ξ" by "by x_ξ"
p206, l12: replace the by The
p206, l-3: replace trails a with of weight by trails with weight
p212, l-15: replace polynomials by polynomial
p227, l-8: replace Encrypt by Decrypt
p227, l-7: replace 4 by BC

Acknowledgements

These errata were contributed by Dave, Nicolas T. Courtois, Praveen Gauravaram, Jorge Nakahara Jr., Ralph Wernsdorf, Shengbo Xu, Uyama Yasumasa.