Supplementary Material

Anonymous Submission

1 Reconstructed Expressions of 4-bit S-boxes

Reconstructed expressions of some S-boxes are provided here, where the 4-bit S-box inputs are denoted (d, c, b, a) (LSB-first), and the outputs are denoted (t, z, y, x).

SKINNY S-box

$x = b + (a + c + d)(a + c) + (a + c + d)(1 + c)(1 + b)$
$y = c + (1 + b)(a + c) + (d)(1 + c)(1 + b)$
$z = d + (1 + c)(1 + b)$
$t = 1 + a + c + (d)(1 + c)$

PRESENT S-box

$x = a + c + d + (1 + b + c)(b)$
$y = a + c + d + (1 + a + d)(a + b + c) + (1 + b + d)(1 + b + c)(a + b + c)$
$z = 1 + b + c + d + (1 + a + d)(b) + (1 + a + d)(1 + b + c)(a + b + c)$
$t = b + (1 + b + d)(1 + b + c) + (1 + a + d)(a + b + c) + (1 + b + d)(1 + b + c)(a + b + c)$

RECTANGLE S-box

$x = a + c + d + (1 + a + b)(b)$
$y = 1 + a + b + c + (d)(b)$
$z = a + b + (1 + c)(1 + a + b + c + d) + (1 + a + b)(b)(1 + c)$
$t = 1 + a + c + (1 + a + b)(1 + a + b + c + d) + (d)(b)(1 + c)$

CLASS-13 S-box

$x = c + (a)(b)$
$y = a + b + (a)(1 + c + d) + (b + c)(a)(b)$
$z = c + d + (b + c)(b)$
$t = a + (d)(1 + c + d) + (d)(a)(b)$

Prøst S-box

$x = c + (1 + a + b + c)(b) + (1 + a + d)(d) + (1 + a + d)(d)(c)$
$y = d + (1 + a + b + c)(b) + (1 + a + b + c)(d)(c)$
$z = a + (c)(b)$
$t = b + (d)(c)$

PRINCE S-box

$x = 1 + b + c + d + (b)(1 + a + c + d) + (a + b + c)(1 + a + c + d) + (a + b + c)(b)(b + c)$
$y = 1 + c + (a + b + c)(b + c) + (1 + a + c + d)(b + c)(b)$
$z = d + (b + c)(1 + a + c + d) + (a + b + c)(1 + b + c + d) + (a + b + c)(b)(1 + a + c + d)$
$t = 1 + d + (b)(b + c) + (b)(1 + a + c + d) + (a + b + c)(b + c)(1 + a + c + d)$

2 Reconstructed [Can05]-based AES S-box Expressions

The AES S-box input is an 8-bit vector (h, g, f, e, d, c, b, a) (LSB-first), and its output is (q, p, n, m, t, z, y, x).

2-Cycle AES S-box: $GF(2^4)$ **Square-Scale-Multiplier**

$x = a + e + ae + be + ce + af + df + ag + cg + bh + dh$

$y = 1 + d + h + ae + be + de + af + cf + df + bg + ah + bh$

$z = a+b+c+d+e+f+g+h+ae+be+ce+de+af+cf+ag+bg+dg+ah+ch+dh$

$t = b + d + f + h + ae + ce + bf + df + ag + cg + dg + bh + ch$

2-Cycle AES S-box: $GF(2^4)$ **Inversion-Multipliers**

The 4-bit vector (l, k, j, i) (LSB-first) is the output of $GF(2^4)$ square-scale-multiplier.

$x = f+h+(e(i+j+k))+(e(j+k))+(ek)+(el)+(f(j+k))+(fk)+(g(i+j+k))+(g(j+k))+(gl)+(h(j+k))+(hl)+(e(i+j+k)l)+(e(j+k)l)+(ekl)+(f(i+j+k)k)+(f(i+j+k)l)+(f(j+k)k)+(fkl)+(g(j+k)k)+(g(j+k)l)+(gkl)+(h(i+j+k)k)+(h(j+k)k)+(hkl)+(e(i+j+k)(j+k)k)+(e(i+j+k)(j+k)l)+(e(j+k)kl)+(f(i+j+k)(j+k)l)+(f(j+k)kl)+(g(i+j+k)(j+k)k)+(g(i+j+k)(j+k)l)+(g(i+j+k)kl)+(h(i+j+k)(j+k)l)$

$y = e+f+g+h+(e(j+k))+(ek)+(f(i+j+k))+(fl)+(g(j+k))+(gl)+(h(i+j+k))+(e(i+j+k)k)+(e(i+j+k)l)+(e(j+k)k)+(ekl)+(f(i+j+k)k)+(f(j+k)k)+(f(j+k)l)+(g(i+j+k)k)+(g(j+k)k)+(gkl)+(h(i+j+k)k)+(h(j+k)l)+(e(i+j+k)(j+k)l)+(e(j+k)kl)+(f(i+j+k)(j+k)k)+(g(i+j+k)(j+k)l)+(h(i+j+k)(j+k)k)+(h(i+j+k)kl)$

$z = f + g + (e(i + j + k)) + (e(j + k)) + (el) + (f(j + k)) + (fl) + (g(i + j + k)) + (gk) + (h(i + j + k)) + (h(j + k)) + (hk) + (e(j + k)k) + (e(j + k)l) + (ekl) + (f(i + j + k)k) + (f(j + k)k) + (fkl) + (g(i + j + k)k) + (g(i + j + k)l) + (g(j + k)k) + (g(j + k)l) + (h(i + j + k)l) + (h(j + k)k) + (h(j + k)l) + (hkl) + (e(i + j + k)(j + k)k) + (e(i + j + k)(j + k)l) + (e(i + j + k)kl) + (f(i + j + k)(j + k)l) + (g(i + j + k)(j + k)k) + (g(j + k)kl) + (h(i + j + k)(j + k)k) + (h(i + j + k)(j + k)l) + (h(i + j + k)kl) + (h(j + k)kl)$

$t = e + f + h + (e(j + k)) + (el) + (f(i + j + k)) + (g(i + j + k)) + (g(j + k)) + (gk) + (h(j + k)) + (e(i + j + k)k) + (e(j + k)k) + (ekl) + (f(i + j + k)k) + (f(j + k)l) + (g(i + j + k)l) + (g(j + k)k) + (g(j + k)l) + (gkl) + (h(i + j + k)k) + (hkl) + (e(i + j + k)(j + k)l) + (f(i + j + k)(j + k)k) + (f(i + j + k)kl) + (g(i + j + k)(j + k)k) + (g(i + j + k)(j + k)l) + (g(i + j + k)kl) + (g(j + k)kl) + (h(i + j + k)(j + k)l) + (h(i + j + k)kl)$

$m = b+d+(a(i+j+k))+(a(j+k))+(ak)+(al)+(b(j+k))+(bk)+(c(i+j+k))+(c(j+k))+(cl)+(d(j+k))+(dl)+(a(i+j+k)l)+(a(j+k)l)+(akl)+(b(i+j+k)k)+(b(i+j+k)l)+(b(j+k)k)+(bkl)+(c(j+k)k)+(c(j+k)l)+(ckl)+(d(i+j+k)k)+(d(j+k)k)+(dkl)+(a(i+j+k)(j+k)k)+(a(i+j+k)(j+k)l)+(a(j+k)kl)+(b(i+j+k)(j+k)l)+(b(j+k)kl)+(c(i+j+k)(j+k)k)+(c(i+j+k)(j+k)l)+(c(i+j+k)kl)+(d(i+j+k)(j+k)l)$

$n = a+b+c+d+(a(j+k))+(ak)+(b(i+j+k))+(bl)+(c(j+k))+(cl)+(d(i+j+k))+(a(i+j+k)k)+(a(i+j+k)l)+(a(j+k)k)+(akl)+(b(i+j+k)k)+(b(j+k)k)+(b(j+k)l)+(c(i+j+k)k)+(c(j+k)k)+(ckl)+(d(i+j+k)k)+(d(j+k)l)+(a(i+j+k)(j+k)l)+(a(j+k)kl)+(b(i+j+k)(j+k)k)+(c(i+j+k)(j+k)l)+(d(i+j+k)(j+k)k)+(d(i+j+k)kl)$

$p = b + c + (a(i + j + k)) + (a(j + k)) + (al) + (b(j + k)) + (bl) + (c(i + j + k)) + (ck) + (d(i + j + k)) + (d(j + k)) + (dk) + (a(j + k)k) + (a(j + k)l) + (akl) + (b(i + j + k)k) + (b(j + k)k) + (bkl) + (c(i + j + k)k) + (c(i + j + k)l) + (c(j + k)k) + (c(j + k)l) + (d(i + j + k)l) + (d(j + k)k) + (d(j + k)l) + (dkl) + (a(i + j + k)(j + k)k) + (a(i + j + k)(j + k)l) + (a(i + j + k)kl) + (b(i + j + k)(j + k)l) + (c(i + j + k)(j + k)k) + (c(j + k)kl) + (d(i + j + k)(j + k)k) + (d(i + j + k)(j + k)l) + (d(i + j + k)kl) + (d(j + k)kl)$

$q = a + b + d + (a(j + k)) + (al) + (b(i + j + k)) + (c(i + j + k)) + (c(j + k)) + (ck) + (d(j + k)) + (a(i + j + k)k) + (a(j + k)k) + (akl) + (b(i + j + k)k) + (b(j + k)l) + (c(i + j + k)l) + (c(j + k)k) + (c(j + k)l) + (ckl) + (d(i + j + k)k) + (dkl) + (a(i + j + k)(j + k)l) + (b(i + j + k)(j + k)k) + (b(i + j + k)kl) + (c(i + j + k)(j + k)k) + (c(i + j + k)(j + k)l) + (c(i + j + k)kl) + (c(j + k)kl) + (d(i + j + k)(j + k)l) + (d(i + j + k)kl)$

3-Cycle AES S-box: $GF(2^4)$ Square-Scale-Multiplier
$x = a + e + ae + be + ce + af + df + ag + cg + bh + dh$
$y = 1 + d + h + ae + be + de + af + cf + df + bg + ah + bh$
$z = a+b+c+d+e+f+g+h+ae+be+ce+de+af+cf+ag+bg+dg+ah+ch+dh$
$t = b + d + f + h + ae + ce + bf + df + ag + cg + dg + bh + ch$

3-Cycle AES S-box: $GF(2^4)$ Inversion
$x = a + d + (b + c)(1 + c + d) + (c)(a + b + c) + (b + c)(c)(a + b + c)$
$y = b + c + d + (c)(a + b + c) + (c)(d) + (b + c)(c) + (b + c)(a + b + c)(d)$
$z = d + (b + c)(c) + (a + b + c)(c)(d)$
$t = c + d + (a + b + c)(d) + (b + c)(d)(c)$

3-Cycle AES S-box: $GF(2^4)$ Multiplier
The 4-bit vector (l, k, j, i) (LSB-first) is the output of $GF(2^4)$ Inversion.
$x = b + d + ai + ci + aj + bj + cj + dj + ck + al + bl$
$y = a + b + c + d + bi + di + aj + cj + dk + al$
$z = b + c + ai + ci + di + aj + bj + dj + ak + dk + cl + dl$
$t = a + b + d + bi + ci + aj + cj + dj + bk + ck + dk + cl$
$m = f + h + ei + gi + ej + fj + gj + hj + gk + el + fl$
$n = e + f + g + h + fi + hi + ej + gj + hk + el$
$p = f + g + ei + gi + hi + ej + fj + hj + ek + hk + gl + hl$
$q = e + f + h + fi + gi + ej + gj + hj + fk + gk + hk + gl$

3 Reconstructed [HB25]-based AES S-box Expressions

The AES S-box input is an 8-bit vector (h, g, f, e, d, c, b, a)(LSB-first), and its output is (q, p, n, m, t, z, y, x). Figure 1 illustrates the schematic of the 3-cycle, first-order PINI-secure AES S-box. As the nonlinear component of the AES S-box, the $GF(2^4)^2$ inversion is decomposed into three nonlinear subcomponents: a $GF(2^4)$ square-scale-multiplier-pow4, a $GF(2^4)$ multipliers-$GF(2^2)$ theta, and $GF(2^2)$ pointwise multipliers. These components are treated as three distinct nonlinear vectorial Boolean functions with the following input-output dimensions: $\mathbb{F}_2^8 \to \mathbb{F}_2^4$, $\mathbb{F}_2^{12} \to \mathbb{F}_2^{10}$, and $\mathbb{F}_2^{10} \to \mathbb{F}_2^8$, respectively. The formulas for each of these nonlinear components are provided below. The design requires a hardware area of 1978 GE and 32-bit randomness.

Figure 2 illustrates the schematic of the 2-cycle, first-order PINI-secure AES S-box, designed in the same style as Figure 1. Compared to the 3-cycle design in Figure 1, the 2-cycle implementation merges the $GF(2^4)$ multipliers-$GF(2^2)$ theta and the $GF(2^2)$ pointwise multipliers into a single nonlinear component, denoted as the $GF(2^4)$ multipliers-theta-pointwise multipliers, which operates as a function from $\mathbb{F}_2^{12}$ to $\mathbb{F}_2^8$. The formulas corresponding to each nonlinear component are presented below. The design requires a hardware area of 2519 GE and 30-bit randomness.

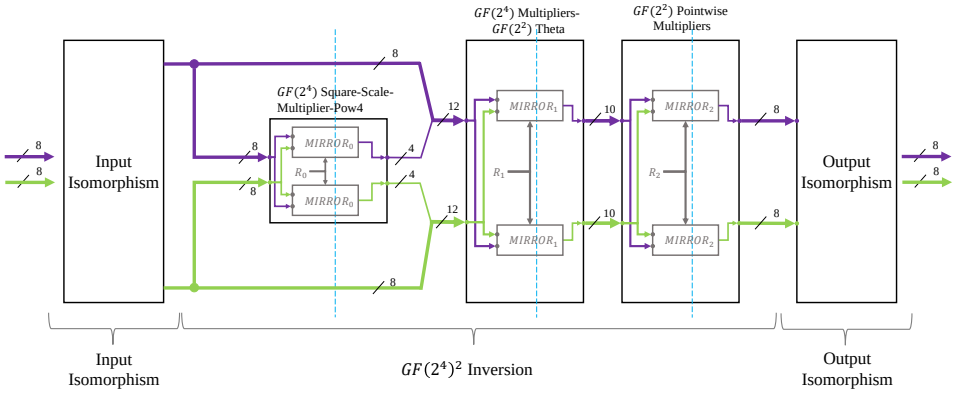


Figure 1: The schematic of the 3-cycle first-order PINI secure [HB25]-based AES S-box.

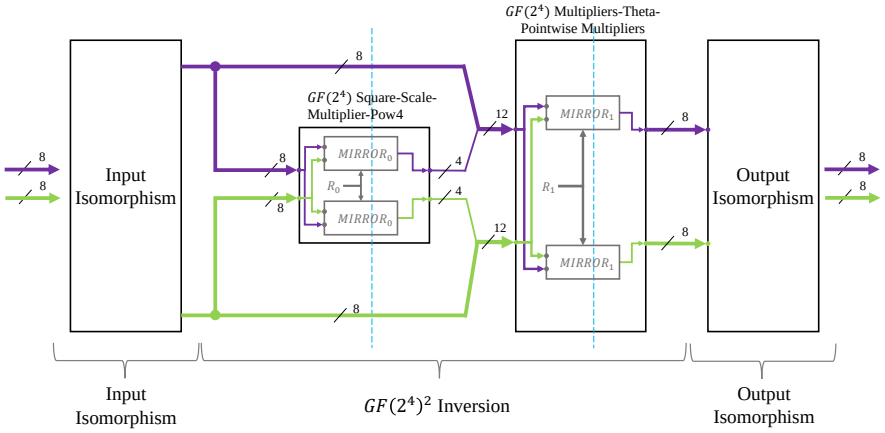


Figure 2: The schematic of the 2-cycle first-order PINI secure [HB25]-based AES S-box.

2-Cycle AES S-box: $GF(2^4)$ Square-Scale-Multiplier-Pow4

$$x = b + d + f + h + ae + ag + bf + bh + ce + cg + ch + df + dg$$
$$y = a + c + e + g + af + ah + be + bf + bg + bh + cf + cg + de + df + dh$$
$$z = a + e + ae + af + ag + be + bh + ce + cg + df + dh$$
$$t = a + b + e + f + ae + ah + bf + bg + bh + cf + ch + de + df + dg + dh$$

2-Cycle AES S-box: $GF(2^4)$ Multipliers-Theta-Pointwise Multipliers

The 4-bit vector (l, k, j, i) (LSB-first) is the output of $GF(2^4)$ square-scale-multiplier-pow4.

$x = (e(i+j)) + (e(j+k)) + (el) + (f(i+j)) + (g(i+j)) + (g(j+k)) + (gk) + (h(i+j)) + (hk) + (hl) + (e(j+k)k) + (f(i+j)l) + (f(j+k)k) + (f(j+k)l) + (g(i+j)l) + (g(j+k)k) + (gkl) + (h(i+j)k) + (h(i+j)l) + (h(j+k)l) + (e(i+j)(j+k)l) + (f(i+j)(j+k)k) + (f(j+k)kl) + (g(i+j)(j+k)l) + (g(i+j)kl) + (g(j+k)kl) + (h(i+j)(j+k)k) + (h(i+j)kl) + (h(j+k)kl)$

$y = (e(i+j)) + (f(j+k)) + (fl) + (g(i+j)) + (gk) + (gl) + (h(j+k)) + (hl) + (e(i+j)l) + (e(j+k)k) + (e(j+k)l) + (f(i+j)l) + (f(j+k)l) + (g(i+j)k) + (g(i+j)l) + (g(j+k)l) + (h(i+j)k) + (h(j+k)k) + (h(j+k)l) + (hkl) + (e(i+j)(j+k)k) + (e(j+k)kl) + (f(i+j)(j+k)k) + (f(i+j)(j+k)l) + (f(j+k)kl) + (g(i+j)(j+k)k) + (g(i+j)kl) + (g(j+k)kl) + (h(i+j)(j+k)k) + (h(i+j)(j+k)l)$

$z = (e(i+j))+(e(j+k))+(ek)+(f(i+j))+(fk)+(fl)+(g(j+k))+(gk)+(h(i+j))+(h(j+k))+(hl)+(e(i+j)l)+(e(j+k)k)+(ekl)+(f(i+j)k)+(f(i+j)l)+(f(j+k)l)+(g(i+j)k)+(g(i+j)l)+(g(j+k)k)+(g(j+k)l)+(h(i+j)k)+(h(i+j)l)+(hkl)+(e(i+j)(j+k)l)+(e(i+j)kl)+(e(j+k)kl)+(f(i+j)(j+k)k)+(f(i+j)kl)+(f(j+k)kl)+(g(i+j)(j+k)k)+(g(i+j)(j+k)l)+(g(i+j)kl)+(g(j+k)kl)+(h(i+j)(j+k)l)+(h(j+k)kl)$

$t = (e(i+j)) + (ek) + (el) + (f(j+k)) + (fl) + (g(i+j)) + (g(j+k)) + (gl) + (h(i+j)) + (hk) + (hl) + (e(i+j)k) + (e(i+j)l) + (e(j+k)l) + (f(i+j)k) + (f(j+k)k) + (f(j+k)l) + (fkl) + (g(i+j)k) + (g(i+j)l) + (gkl) + (h(j+k)k) + (h(j+k)l) + (hkl) + (e(i+j)(j+k)k) + (e(i+j)kl) + (e(j+k)kl) + (f(i+j)(j+k)k) + (f(i+j)(j+k)l) + (g(i+j)(j+k)l) + (g(j+k)kl) + (h(i+j)(j+k)k) + (h(i+j)kl)$

$m = (a(i+j))+(a(j+k))+(al)+(b(i+j))+(c(i+j))+(c(j+k))+(ck)+(d(i+j))+(dk)+(dl)+(a(j+k)k)+(b(i+j)l)+(b(j+k)k)+(b(j+k)l)+(c(i+j)l)+(c(j+k)k)+(ckl)+(d(i+j)k)+(d(i+j)l)+(d(j+k)l)+(a(i+j)(j+k)l)+(b(i+j)(j+k)k)+(b(j+k)kl)+(c(i+j)(j+k)l)+(c(i+j)kl)+(c(j+k)kl)+(d(i+j)(j+k)k)+(d(i+j)kl)+(d(j+k)kl)$

$n = (a(i+j)) + (b(j+k)) + (bl) + (c(i+j)) + (ck) + (cl) + (d(j+k)) + (dl) + (a(i+j)l) + (a(j+k)k) + (a(j+k)l) + (b(i+j)l) + (b(j+k)l) + (c(i+j)k) + (c(i+j)l) + (c(j+k)l) + (d(i+j)k) + (d(j+k)k) + (d(j+k)l) + (dkl) + (a(i+j)(j+k)k) + (a(j+k)kl) + (b(i+j)(j+k)k) + (b(i+j)(j+k)l) + (b(j+k)kl) + (c(i+j)(j+k)k) + (c(i+j)kl) + (c(j+k)kl) + (d(i+j)(j+k)k) + (d(i+j)(j+k)l)$

$p = (a(i+j))+(a(j+k))+(ak)+(b(i+j))+(bk)+(bl)+(c(j+k))+(ck)+(d(i+j))+(d(j+k))+(dl)+(a(i+j)l)+(a(j+k)k)+(akl)+(b(i+j)k)+(b(i+j)l)+(b(j+k)l)+(c(i+j)k)+(c(i+j)l)+(c(j+k)k)+(c(j+k)l)+(d(i+j)k)+(d(i+j)l)+(dkl)+(a(i+j)(j+k)l)+(a(i+j)kl)+(a(j+k)kl)+(b(i+j)(j+k)k)+(b(i+j)kl)+(b(j+k)kl)+(c(i+j)(j+k)k)+(c(i+j)(j+k)l)+(c(i+j)kl)+(c(j+k)kl)+(d(i+j)(j+k)l)+(d(j+k)kl)$

$q = (a(i+j)) + (ak) + (al) + (b(j+k)) + (bl) + (c(i+j)) + (c(j+k)) + (cl) + (d(i+j)) + (dk) + (dl) + (a(i+j)k) + (a(i+j)l) + (a(j+k)l) + (b(i+j)k) + (b(j+k)k) + (b(j+k)l) + (bkl) + (c(i+j)k) + (c(i+j)l) + (ckl) + (d(j+k)k) + (d(j+k)l) + (dkl) + (a(i+j)(j+k)k) + (a(i+j)kl) + (a(j+k)kl) + (b(i+j)(j+k)k) + (b(i+j)(j+k)l) + (c(i+j)(j+k)l) + (c(j+k)kl) + (d(i+j)(j+k)k) + (d(i+j)kl)$

3-Cycle AES S-box: $GF(2^4)$ Square-Scale-Multiplier-Pow4

$x = b + d + f + h + ae + ag + bf + bh + ce + cg + ch + df + dg$

$y = a + c + e + g + af + ah + be + bf + bg + bh + cf + cg + de + df + dh$

$z = a + e + ae + af + ag + be + bh + ce + cg + df + dh$

$t = a + b + e + f + ae + ah + bf + bg + bh + cf + ch + de + df + dg + dh$

3-Cycle AES S-box: $GF(2^4)$ Multipliers-$GF(2^2)$ Theta

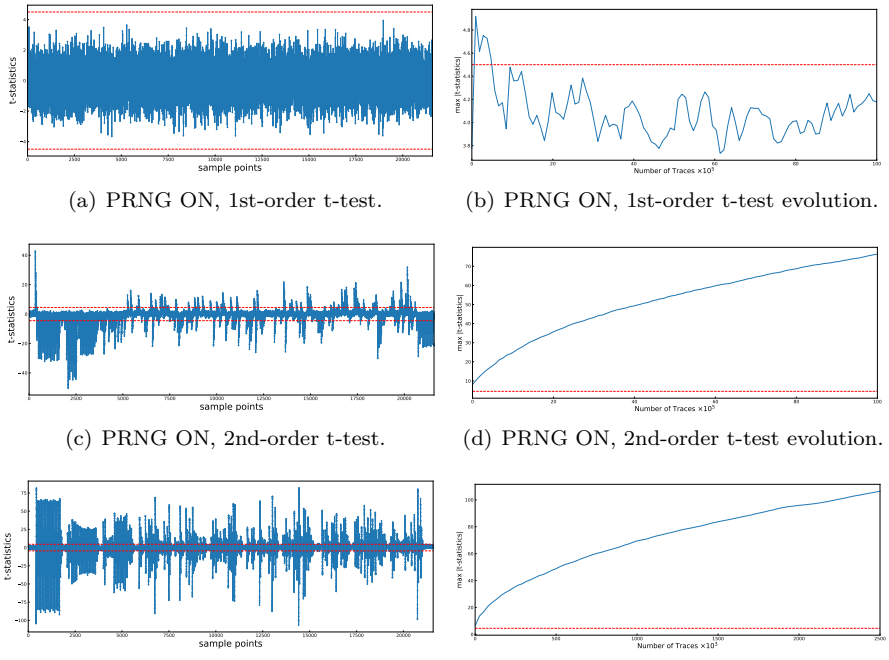
The 4-bit vector (l, k, j, i) (LSB-first) is the output of $GF(2^4)$ square-scale-multiplier-pow4.

$x = ai + aj + ak + bi + bl + ci + ck + dj + dl$
$y = ai + al + bj + bk + bl + cj + cl + di + dj + dk + dl$
$z = ai + ak + bj + bl + ci + ck + cl + dj + dk$
$t = aj + al + bi + bj + bk + bl + cj + ck + di + dj + dl$
$m = j + l + (i + j + l)k + (1 + i + k + l)l$
$n = k + l + (1 + i + k + l)j + (i + j + l)i$
$p = ei + ej + ek + fi + fl + gi + gk + hj + hl$
$q = ei + el + fj + fk + fl + gj + gl + hi + hj + hk + hl$
$r = ei + ek + fj + fl + gi + gk + gl + hj + hk$
$s = ej + el + fi + fj + fk + fl + gj + gk + hi + hj + hl$

3-Cycle AES S-box: $GF(2^2)$ Pointwise Multipliers

$ej + fi + fj$
$ei + ej + fi$
$gj + hi + hj$
$gi + gj + hi$
$aj + bi + bj$
$ai + aj + bi$
$cj + di + dj$
$ci + cj + di$

4 Experimental Results of Multi-Cycle AES S-box



(a) PRNG ON, 1st-order t-test.
(b) PRNG ON, 1st-order t-test evolution.
(c) PRNG ON, 2nd-order t-test.
(d) PRNG ON, 2nd-order t-test evolution.
(e) PRNG OFF, 1st-order t-test.
(f) PRNG OFF, 1st-order t-test evolution.

Figure 3: The AES byte-serial encryption, 2-cycle first-order S-box of MCM_{SMT}.

To assess the practical security of the multi-cycle AES S-box, we incorporate the 2-cycle masked S-box generated by the MCM_{SMT} technique into a byte-serial AES design [MPL+11]. The t-test analyses in Figures 3(a) and 3(c) confirm that our design maintains first-order security, while exhibiting observable second-order leakage. It is observed that when the number of traces is relatively small, the maximum absolute value of the t-statistic in Figure 3(b) may temporarily exceed the threshold of 4.5 due to statistical fluctuations. However, as more traces are collected, the t-statistic remains consistently below the threshold of 4.5 throughout all observed fluctuations, confirming the practical first-order security of the design. The results in Figure 3(e) further confirm the validity of our experimental setup by demonstrating the presence of first-order leakage.

References

[Can05] David Canright. A very compact s-box for AES. In Josyula R. Rao and Berk Sunar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2005, 7th International Workshop, Edinburgh, UK, August 29 - September 1, 2005, Proceedings*, volume 3659 of *Lecture Notes in Computer Science*, pages 441–455. Springer, 2005.

[HB25] Vedad Hadzic and Roderick Bloem. Efficient and composable masked AES s-box designs using optimized inverters. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2025(1):656–683, 2025.

[MPL+11] Amir Moradi, Axel Poschmann, San Ling, Christof Paar, and Huaxiong Wang. Pushing the limits: A very compact and a threshold implementation of AES. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 69–88. Springer, 2011.