Pseudo-code of optimized SNI refresh gadgets

Gaëtan Cassiers   Benjamin Grégoire

The input (resp., output) sharing is denoted as $\mathbf{x}$ (resp., $\mathbf{y}$). All r_i variables are independent uniform random elements, and $\mathbf{s}^i$ are vectors of d independent randoms elements. The $(\cdot \gg i)$ operator applied to a vector denotes a rotation of its elements: the 1st element becomes the $i+1$-th, etc. Registers are denoted as $\mathsf{R}[\cdot]$.

$d = 2$

$y_0 \leftarrow \mathsf{R}[x_0 + r_0]$
$y_1 \leftarrow \mathsf{R}[x_1 + r_0]$

$d = 3$

$t_0 \leftarrow \mathsf{R}[r_0 + r_1]$
$y_0 \leftarrow \mathsf{R}[x_0 + r_0]$
$y_1 \leftarrow \mathsf{R}[x_1 + r_1]$
$y_2 \leftarrow \mathsf{R}[x_2 + t_0]$

$d = 4, 5$

$\mathbf{t^0} \leftarrow \mathsf{R}\left[\mathbf{s^0} + (\mathbf{s^0} \gg 1)\right]$
$\mathbf{y} \leftarrow \mathsf{R}\left[\mathbf{x} + \mathbf{t^0}\right]$

$d = 6$

$\mathbf{t^0} \leftarrow \mathsf{R}\left[\mathbf{s^0} + (\mathbf{s^0} \gg 1)\right]$
$t_0^0 \leftarrow \mathsf{R}\left[t_0^0 + r_0\right]$
$t_3^0 \leftarrow \mathsf{R}\left[t_3^0 + r_0\right]$
$\mathbf{y} \leftarrow \mathsf{R}\left[\mathbf{x} + \mathbf{t^0}\right]$

$d = 7$

$\mathbf{t^0} \leftarrow \mathsf{R}\left[\mathbf{s^0} + (\mathbf{s^0} \gg 1)\right]$
$t_0^0 \leftarrow \mathsf{R}\left[t_0^0 + r_0\right]$
$t_2^0 \leftarrow \mathsf{R}\left[t_2^0 + r_1\right]$
$t_4^0 \leftarrow \mathsf{R}\left[t_4^0 + r_0\right]$
$t_6^0 \leftarrow \mathsf{R}\left[t_6^0 + r_1\right]$
$\mathbf{y} \leftarrow \mathsf{R}\left[\mathbf{x} + \mathbf{t^0}\right]$

$d = 8$

$\mathbf{t^0} \leftarrow \mathsf{R}\left[\mathbf{s^0} + (\mathbf{s^0} \gg 1)\right]$
$t_0^0 \leftarrow \mathsf{R}\left[t_0^0 + r_0\right]$
$t_1^0 \leftarrow \mathsf{R}\left[t_1^0 + r_1\right]$
$t_2^0 \leftarrow \mathsf{R}\left[t_2^0 + r_2\right]$
$t_4^0 \leftarrow \mathsf{R}\left[t_4^0 + r_0\right]$
$t_5^0 \leftarrow \mathsf{R}\left[t_5^0 + r_1\right]$
$t_6^0 \leftarrow \mathsf{R}\left[t_6^0 + r_2\right]$
$\mathbf{y} \leftarrow \mathsf{R}\left[\mathbf{x} + \mathbf{t^0}\right]$

$d = 9$

$\mathbf{t^0} \leftarrow \mathsf{R}\left[\mathbf{s^0} + (\mathbf{s^0} \gg 1)\right]$
$t_0^0 \leftarrow \mathsf{R}\left[t_0^0 + r_0\right]$
$t_1^0 \leftarrow \mathsf{R}\left[t_1^0 + r_1\right]$
$t_3^0 \leftarrow \mathsf{R}\left[t_3^0 + r_2\right]$
$t_4^0 \leftarrow \mathsf{R}\left[t_4^0 + r_0\right]$
$t_6^0 \leftarrow \mathsf{R}\left[t_6^0 + r_1\right]$
$t_7^0 \leftarrow \mathsf{R}\left[t_7^0 + r_2\right]$
$\mathbf{y} \leftarrow \mathsf{R}\left[\mathbf{x} + \mathbf{t^0}\right]$

$d = 10$

$\mathbf{t^0} \leftarrow \mathsf{R}\left[\mathbf{s^0} + (\mathbf{s^0} \gg 1)\right]$
$t_0^0 \leftarrow \mathsf{R}\left[t_0^0 + r_0\right]$
$t_1^0 \leftarrow \mathsf{R}\left[t_1^0 + r_1\right]$
$t_2^0 \leftarrow \mathsf{R}\left[t_2^0 + r_2\right]$
$t_3^0 \leftarrow \mathsf{R}\left[t_3^0 + r_3\right]$
$t_4^0 \leftarrow \mathsf{R}\left[t_4^0 + r_4\right]$
$t_5^0 \leftarrow \mathsf{R}\left[t_5^0 + r_0\right]$
$t_6^0 \leftarrow \mathsf{R}\left[t_6^0 + r_1\right]$
$t_7^0 \leftarrow \mathsf{R}\left[t_7^0 + r_2\right]$
$t_8^0 \leftarrow \mathsf{R}\left[t_8^0 + r_3\right]$
$t_9^0 \leftarrow \mathsf{R}\left[t_9^0 + r_4\right]$
$\mathbf{y} \leftarrow \mathsf{R}\left[\mathbf{x} + \mathbf{t^0}\right]$

$d = 11$

$\mathbf{t^0} \leftarrow \mathsf{R}\left[\mathbf{s^0} + (\mathbf{s^0} \gg 1)\right]$
$t_0^0 \leftarrow \mathsf{R}\left[t_0^0 + r_0\right]$
$t_1^0 \leftarrow \mathsf{R}\left[t_1^0 + r_1\right]$
$t_2^0 \leftarrow \mathsf{R}\left[t_2^0 + r_2\right]$
$t_3^0 \leftarrow \mathsf{R}\left[t_3^0 + r_3\right]$
$t_4^0 \leftarrow \mathsf{R}\left[t_4^0 + r_4\right]$
$t_5^0 \leftarrow \mathsf{R}\left[t_5^0 + r_0\right]$
$t_6^0 \leftarrow \mathsf{R}\left[t_6^0 + r_1\right]$
$t_7^0 \leftarrow \mathsf{R}\left[t_7^0 + r_2 + r_5\right]$
$t_8^0 \leftarrow \mathsf{R}\left[t_8^0 + r_3\right]$
$t_9^0 \leftarrow \mathsf{R}\left[t_9^0 + r_4\right]$
$t_{10}^0 \leftarrow \mathsf{R}\left[t_{10}^0 + r_5\right]$
$\mathbf{y} \leftarrow \mathsf{R}\left[\mathbf{x} + \mathbf{t^0}\right]$

$d = 12$

$\mathbf{t^0} \leftarrow \mathsf{R}\left[\mathbf{s^0} + (\mathbf{s^0} \gg 1)\right]$
$t_0^0 \leftarrow \mathsf{R}\left[t_0^0 + r_0\right]$
$t_1^0 \leftarrow \mathsf{R}\left[t_1^0 + r_1\right]$
$t_2^0 \leftarrow \mathsf{R}\left[t_2^0 + r_2 + r_6\right]$
$t_3^0 \leftarrow \mathsf{R}\left[t_3^0 + r_3\right]$
$t_4^0 \leftarrow \mathsf{R}\left[t_4^0 + r_4\right]$
$t_5^0 \leftarrow \mathsf{R}\left[t_5^0 + r_5 + r_6\right]$
$t_6^0 \leftarrow \mathsf{R}\left[t_6^0 + r_0\right]$
$t_7^0 \leftarrow \mathsf{R}\left[t_7^0 + r_1\right]$
$t_8^0 \leftarrow \mathsf{R}\left[t_8^0 + r_2 + r_7\right]$
$t_9^0 \leftarrow \mathsf{R}\left[t_9^0 + r_3\right]$
$t_{10}^0 \leftarrow \mathsf{R}\left[t_{10}^0 + r_4\right]$
$t_{11}^0 \leftarrow \mathsf{R}\left[t_{11}^0 + r_5 + r_7\right]$
$\mathbf{y} \leftarrow \mathsf{R}\left[\mathbf{x} + \mathbf{t^0}\right]$

$d = 13, \ldots, 16$

$\mathbf{t^0} \leftarrow \mathsf{R}\left[\mathbf{s^0} + (\mathbf{s^0} \gg 1)\right]$
$\mathbf{t^1} \leftarrow \mathsf{R}\left[\mathbf{s^1} + (\mathbf{s^1} \gg 3)\right]$
$\mathbf{t^2} \leftarrow \mathsf{R}\left[\mathbf{t^0} + \mathbf{t^1}\right]$
$\mathbf{y} \leftarrow \mathsf{R}\left[\mathbf{x} + \mathbf{t^2}\right]$