02 Math

Po-Hsuan Huang
aben20807@gmail.com

January 9, 2023

Inline latex: $x \in_R \mathbb{Z}_{2^\ell}$, use $ to wrap.

$$(y_1, ..., y_n) \leftarrow \mathcal{F}(x_1, ..., x_n)$$

Test reference: Equation 1.

$$\begin{aligned}
\langle c \rangle^A &= \langle a \rangle^A \times \langle b \rangle^A && (1)\\
&= (\langle a \rangle_0^A + \langle a \rangle_1^A) \times (\langle b \rangle_0^A + \langle b \rangle_1^A) && (2)\\
&= \langle a \rangle_0^A \times \langle b \rangle_0^A + \langle a \rangle_1^A \times \langle b \rangle_1^A \\
&\quad + \underbrace{\langle a \rangle_0^A \times \langle b \rangle_1^A}_{\langle u \rangle^A} + \underbrace{\langle a \rangle_1^A \times \langle b \rangle_0^A}_{\langle v \rangle^A} && (3)\\
&= \langle a \rangle_0^A \times \langle b \rangle_0^A + \langle u \rangle_0^A + \langle v \rangle_0^A \\
&\quad + \langle a \rangle_1^A \times \langle b \rangle_1^A + \langle u \rangle_1^A + \langle v \rangle_1^A && (4)\\
&= \langle c \rangle_0^A + \langle c \rangle_1^A && (5)
\end{aligned}$$