

Let n as the bit-width of the ring, f as the fractional bit-width, k as the integer bit width and $m = n - f$.

With the restriction that $n \geq 1 + 1 + k + 2f$ and the pre-generated randomness $[r]^m$, $[r]$ and $[r^{msb}]$ (r is an m bit random number, $[r]^m$ is the m bit ASS of r , $[r]$ is the n bit ASS of r and $[r^{msb}]$ is the n bit ASS of the MSB of r), we can extend the m bit secret-share, denoted as $[x]^m$, into n bit secret share through:

1. $\hat{x} = REC([x]^m + [r]^m \bmod 2^m)$
2. $\hat{x}' = \hat{x} + 2^{m-2} \bmod 2^m$
3. $t = (1 - MSB(\hat{x}')) \cdot 2^m$
4. $[x^{ext}] = \sigma \cdot (\hat{x}' - 2^{m-2}) - [r] + t \cdot [r^{msb}]$

Note that σ is the party number.

With the above setting, we can optimize the element-wise multiplication and decrease the overhead of multiplication & Zero Extend into $n-f$ bits:

Denote that $[r^x]^m$, $[r^x]$ and $[r^{xmsb}]$ is the extension triple that needed by x which satisfy the above restriction and $[r^y]^m$, $[r^y]$ and $[r^{ymsb}]$ is the extension triple for y .

Like Beaver Triple, we first reconstruct:

1. $\hat{x} = REC([x]^m + [r^x]^m \bmod 2^m)$
2. $\hat{x}' = \hat{x} + 2^{m-2} \bmod 2^m$
3. $\hat{y} = REC([y]^m + [r^y]^m \bmod 2^m)$
4. $\hat{y}' = \hat{y} + 2^{m-2} \bmod 2^m$

A slight difference here is that we do not need to extend the bit-width to n . Instead, we implement m bit reconstruction

Now, denote $t^x = (1 - MSB(\hat{x}')) \cdot 2^m$ and $t^y = (1 - MSB(\hat{y}')) \cdot 2^m$

$$\begin{aligned} x^{ext} \cdot y^{ext} &= ((\hat{x}' - 2^{m-2}) - r^x + t^x \cdot r^{xmsb}) \cdot ((\hat{y}' - 2^{m-2}) - r^y + t^y \cdot r^{ymsb}) \\ &= (\hat{x}' - 2^{m-2}) \cdot (\hat{y}' - 2^{m-2}) - (\hat{x}' - 2^{m-2}) \cdot r^y + (\hat{x}' - 2^{m-2}) \cdot t^y \cdot r^{ymsb} - r^x \cdot (\hat{y}' - 2^{m-2}) \\ &\quad + r^x \cdot r^y - r^x \cdot t^y \cdot r^{ymsb} + t^x \cdot r^{xmsb} \cdot (\hat{y}' - 2^{m-2}) - t^x \cdot r^{xmsb} \cdot r^y + t^x \cdot r^{xmsb} \cdot t^y \cdot r^{ymsb} \end{aligned}$$

For element-wise matmul and scalar multiplication, we have:

$$\begin{aligned} r^x \cdot t^y \cdot r^{ymsb} &= r^x \cdot r^{ymsb} \cdot t^y \\ t^x \cdot r^{xmsb} \cdot t^y \cdot r^{ymsb} &= t^x \cdot t^y \cdot r^{xmsb} \cdot r^{ymsb} \end{aligned}$$

The following elements are computable without extra requirement:

1. $(\hat{x}' - 2^{m-2}) \cdot (\hat{y}' - 2^{m-2})$
2. $(\hat{x}' - 2^{m-2}) \cdot r^y$
3. $(\hat{x}' - 2^{m-2}) \cdot t^y \cdot r^{ymsb}$
4. $r^x \cdot (\hat{y}' - 2^{m-2})$
5. $t^x \cdot r^{xmsb} \cdot (\hat{y}' - 2^{m-2})$

For element like:

1. $r^x \cdot r^y$
2. $r^x \cdot t^y \cdot r^{ymsb} = r^x \cdot r^{ymsb} \cdot t^y$
3. $t^x \cdot r^{xmsb} \cdot t^y \cdot r^{ymsb} = t^x \cdot t^y \cdot r^{xmsb} \cdot r^{ymsb}$
4. $t^x \cdot r^{xmsb} \cdot r^y$

We can generate these correlated randomness during the offline phase and secret share them over the n bit ring:

1. $r^{xy} = r^x \cdot r^y$
2. $r^{xymbsb} = r^x \cdot r^{ymsb}$
3. $r^{xmsb ymsb} = r^{xmsb} \cdot r^{ymsb}$
4. $r^{xmsby} = r^{xmsb} \cdot r^y$

We can conclude that:

$$[x^{ext} \cdot y^{ext}] = \sigma \cdot (\hat{x}' - 2^{m-2}) \cdot (\hat{y}' - 2^{m-2}) - (\hat{x}' - 2^{m-2}) \cdot [r^y] + (\hat{x}' - 2^{m-2}) \cdot t^y \cdot [r^{ymsb}] - [r^x] \cdot (\hat{y}' - 2^{m-2}) + [r^{xy}] - t^y \cdot [r^{xymbsb}] + t^x \cdot [r^{xmsb}] \cdot (\hat{y}' - 2^{m-2}) - t^x \cdot [r^{xmsby}] + t^x \cdot t^y \cdot [r^{xmsb ymsb}]$$