Range: finite field Fp

(Note: x: scalar; **x**: vector; **X**: matrix)

#case1 : Standard scalar

INPUT

S_0: Choose random numbers a_0, b_0, c_0, and set a vector $X=(a_0b_0, a_0, b_0, 1, c_0)=(x_0,...,x_4)$

S_1: Choose random numbers a_1, b_1, and set a vector $Y=(1, b_1, a_1, a_1b_1, -1)=(y_0,...y_4)$

COMPUTE

S_1: Choose a random vector $R=(r_0, ..., r_4)$, and a random number r;

Compute $Z=Y-R=(z_0, ..., z_4)$, where $z_i=y_i-r_i$;

Compute $W=rZ=(w_0, ..., w_4)$, where $w_i=rz_i$

S_0: Compute $u=R.X=r_0x_0+...+r_4x_4$

Compute $v=W.X=w_0x_0+...+w_4x_4$

S_1: Compute $c_1=u+r^{-1}v$

OUTPUT

S_0: (a_0, b_0, c_0)

S_1: (a_1, b_1, c_1)

CORRECTNESS

$c_1=(a_0+a_1)(b_0+b_1)-c_0$

$=a_0b_0+a_0b_1+a_1b_0+a_1b_1-c_0$

$=(a_0b_0,a_0,b_0,1,c_0)\cdot(1,b_1,a_1,a_1b_1,-1)$

#case2: matrix for LSTM training

INPUT

I: **I** is the identity matrix of order n

S0: Choose random matrices mxd **A**0, dxn **B**0, mxn **C**0,

and set an array X=(**A**0**B**0, **A**0, **B**0, **I**, **C**0)=(**X**0, ..., **X**4)

where **X**0=**A**0**B**0 mxn, **X**1=**A**0 mxd, **X**2=**B**0 dxn, **X**3=**I**, **X**4=**C**0 mxn

S1: Choose random matrices mxd **A**1, dxn **B**1,

and set an array Y=(**I**, **B**1, **A**1, **A**1**B**1, -**I**)=(**Y**0, ..., **Y**4)

where **Y**0=**I** nxn, **Y**1=**B**1 dxn, **Y**2=**A**1 mxd, **Y**3=**A**1**B**1 mxn, **Y**4=-**I** nxn

COMPUTE

S1: Choose a random array R=(**R**0, ..., **R**4), and a random number r;

Where **R**0 nxn, **R**1 dxn, **R**2 mxd, **R**3 mxn, **R**4 nxn

Compute Z=Y-R=(**Z**0, ..., **Z**4), where **Z**i=**Y**i-**R**i ;

Compute W=rZ=(**W**0, ..., **W**4), where **W**i=r**Z**i;

S0: Compute

U mxn=X.R=**X**0mxn**R**0nxn+**X**1mxd**R**1dxn+**R**2mxd**X**2dxn+**R**3mxn**X**3 nxn +**X**4mxn**R**4 nxn

Compute

V mxn=X.W=**X**0mxn**W**0nxn +**X**1mxd**W**1dxn+**W**2mxd**X**2dxn+**W**3mxn**X**3nxn +**X**4mxn**W**4 nxn

S1: Compute **C**1=**U**+r^(-1)**V** mxn

OUTPUT

S0: (**A**0, **B**0, **C**0)

S1: (**A**1, **B**1, **C**1)

CORRECTNESS

$C1=(A0+A1)(B0+B1)-C0$

$=A0B0+A0B1+A1B0+A1B1-C0$

$=(A0B0, A0, B0, I, C0)\cdot(I, B1, A1, A1B1, -I)$