$b = 8$

$a = \text{RandomInteger}[\{2, b\}];$

$\{a, \text{GCD}[a, 8]\}$

8

$\{3, 1\}$

$\text{ket}_0 = \{\{1\}, \{0\}\};$

$\text{ket}_1 = \{\{0\}, \{1\}\};$

$\text{Id} = \text{IdentityMatrix}[2];$

$X = \text{PauliMatrix}[1];$

$Y = \text{PauliMatrix}[2];$

$Z = \text{PauliMatrix}[3];$

$H = \text{HadamardMatrix}[2];$

$P_0 = \text{ket}_0.\text{ConjugateTranspose}\left[\text{ket}_0\right];$

$P_1 = \text{ket}_1.\text{ConjugateTranspose}\left[\text{ket}_1\right];$

$R[\phi\_] := P_0 + e^{i\phi} P_1;$

$\text{CNOT} = \text{KroneckerProduct}\left[P_0, \text{Id}\right] + \text{KroneckerProduct}\left[P_1, X\right];$

$\text{CR}[\phi\_] := \text{KroneckerProduct}\left[P_0, \text{Id}\right] + \text{KroneckerProduct}\left[P_1, R[\phi]\right];$

$\text{CR13}[\phi\_] := \text{KroneckerProduct}\left[P_0, \text{Id}, \text{Id}\right] + \text{KroneckerProduct}\left[P_1, \text{Id}, R[\phi]\right];$

$\text{ket}[\text{n}\_] := \text{Table}[\{n == i - 1\}, \{i, 1, 16\}] /. \{\text{True} \to 1, \text{False} \to 0\};$

$\text{Ure}[\text{x}\_, \text{N}\_] := \text{Sum}\left[\text{KroneckerProduct}\left[\text{ket}[i].\text{ConjugateTranspose}[\text{ket}[i]], \text{ket}\left[\text{Mod}\left[\text{Mod}\left[x^i, N\right] + j, 16\right]\right].\text{Conju}\right.\right.$

$\rho[\psi\_] := \psi.\text{ConjugateTranspose}[\psi];$

$\text{rt} = \text{Table}[0, \{i, 0, 50\}];$

$\text{For}[j = 1, j \leq 50, j{+}{+},$

$\psi 0 = \text{KroneckerProduct}\left[\text{ket}_0, \text{ket}_0, \text{ket}_0, \text{ket}_0\right];$

$\psi = \text{KroneckerProduct}\left[\text{ket}_0, \text{ket}_0, \text{ket}_0, \text{ket}_0\right];$

$\psi\mathrm{t} = N[\mathrm{KroneckerProduct}[\psi 0, \psi]];$

$\psi\mathrm{t} = N[\mathrm{KroneckerProduct}[H, H, H, H, \mathrm{Id}, \mathrm{Id}, \mathrm{Id}, \mathrm{Id}].\psi\mathrm{t}];$

$\psi\mathrm{t} = \mathrm{Ure}[a, b].\psi\mathrm{t};$

$\mathrm{For}[i = 0, i < 16, i{+}{+}, \mathrm{sub0} = \mathrm{Mod}[i, 2];$

$\mathrm{sub1} = \mathrm{Which}[i == 0, 0, \mathrm{Mod}[i, 2] == 0\&\&\mathrm{sub1} == 0, 1, \mathrm{Mod}[i, 2] == 0\&\&\mathrm{sub1} == 1, 0, \mathrm{True}, \mathrm{sub1}];$

$\mathrm{sub2} = \mathrm{Which}\left[i == 0, 0, \mathrm{Mod}\left[i, 2^2\right] == 0\&\&\mathrm{sub2} == 0, 1, \mathrm{Mod}\left[i, 2^2\right] == 0\&\&\mathrm{sub2} == 1, 0, \mathrm{True}, \mathrm{sub2}\right];$

$\mathrm{sub3} = \mathrm{Which}\left[i == 0, 0, \mathrm{Mod}\left[i, 2^3\right] == 0\&\&\mathrm{sub3} == 0, 1, \mathrm{Mod}\left[i, 2^3\right] == 0\&\&\mathrm{sub3} == 1, 0, \mathrm{True}, \mathrm{sub3}\right];$

$\psi\mathrm{t}_i = N\left[\mathrm{KroneckerProduct}\left[\mathrm{Id}, \mathrm{Id}, \mathrm{Id}, \mathrm{Id}, P_{\mathrm{sub3}}, P_{\mathrm{sub2}}, P_{\mathrm{sub1}}, P_{\mathrm{sub0}}\right].\psi\mathrm{t}\right];$

$\mathrm{pt}_i = N\left[\mathrm{ConjugateTranspose}\left[\psi\mathrm{t}_i\right].\psi\mathrm{t}_i\right];]$

$\psi\mathrm{t} = \mathrm{Table}\left[\psi\mathrm{t}_i, \{i, 0, 15\}\right];$

$\mathrm{pt} = \mathrm{Table}\left[\mathrm{pt}_i[[1, 1]], \{i, 0, 15\}\right];$

$\mathrm{c1} = \mathrm{RandomChoice}[\mathrm{pt} \to \mathrm{Table}[i, \{i, 1, 16\}]];$

$\psi\mathrm{t} = \psi\mathrm{t}[[\mathrm{c1}]];$

$\psi\mathrm{t} = \psi\mathrm{t}/\mathrm{Norm}[\psi\mathrm{t}];$

$\psi\mathrm{t} = N[\mathrm{KroneckerProduct}[\mathrm{FourierMatrix}[16], \mathrm{IdentityMatrix}[16]].\psi\mathrm{t}];$

$\mathrm{For}[i = 0, i < 16, i{+}{+}, \mathrm{sub0} = \mathrm{Mod}[i, 2];$

$\mathrm{sub1} = \mathrm{Which}[i == 0, 0, \mathrm{Mod}[i, 2] == 0\&\&\mathrm{sub1} == 0, 1, \mathrm{Mod}[i, 2] == 0\&\&\mathrm{sub1} == 1, 0, \mathrm{True}, \mathrm{sub1}];$

$\mathrm{sub2} = \mathrm{Which}\left[i == 0, 0, \mathrm{Mod}\left[i, 2^2\right] == 0\&\&\mathrm{sub2} == 0, 1, \mathrm{Mod}\left[i, 2^2\right] == 0\&\&\mathrm{sub2} == 1, 0, \mathrm{True}, \mathrm{sub2}\right];$

$\mathrm{sub3} = \mathrm{Which}\left[i == 0, 0, \mathrm{Mod}\left[i, 2^3\right] == 0\&\&\mathrm{sub3} == 0, 1, \mathrm{Mod}\left[i, 2^3\right] == 0\&\&\mathrm{sub3} == 1, 0, \mathrm{True}, \mathrm{sub3}\right];$

$\psi\mathrm{t}_i = N\left[\mathrm{KroneckerProduct}\left[P_{\mathrm{sub3}}, P_{\mathrm{sub2}}, P_{\mathrm{sub1}}, P_{\mathrm{sub0}}, \mathrm{Id}, \mathrm{Id}, \mathrm{Id}, \mathrm{Id}\right].\psi\mathrm{t}\right];$

$\text{pt}_i = N\,[\text{ConjugateTranspose}\,[\psi \text{t}_i]\,.\psi \text{t}_i]\,;]$

$\psi\text{t} = \text{Table}\,[\psi\text{t}_i, \{i, 0, 15\}]\,;$

$\text{pt} = \text{Table}\,[\text{pt}_i[[1,1]], \{i, 0, 15\}]\,;$

$\text{c2} = \text{RandomChoice}[\text{pt} \to \text{Table}[i, \{i, 1, 16\}]];$

$\psi\text{t} = \psi\text{t}[[\text{c2}]];$

$\psi\text{t} = \psi\text{t}/\text{Norm}[\psi\text{t}];$

$(\text{c2} - 1)/16; (\text{*s/r*})$

$c = \text{ContinuedFraction}[(\text{c2} - 1)/16];$

$r = \text{Last}[\text{Convergents}[c]];$

$r = \text{Denominator}[r];$

$\text{rt}[[j]] = r;]$

$\text{Counts}[\text{rt}]$

$\text{Counts}\left[\text{GCD}\left[a^{\text{rt}/2} + 1, b\right]\right]$

$\text{Counts}\left[\text{GCD}\left[a^{\text{rt}/2} - 1, b\right]\right]$

$2 \to 26, 1 \to 24, 0 \to 1$

$4 \to 26, \text{GCD}\left[8, 1 + \sqrt{3}\right] \to 24, 2 \to 1$

$2 \to 26, \text{GCD}\left[8, -1 + \sqrt{3}\right] \to 24, 8 \to 1$

$\text{ket[n\_]:=Table}[\{n == i - 1\}, \{i, 1, 16\}]/.\{\text{True} \to 1, \text{False} \to 0\};$

$\text{Urp[x\_, N\_]:=Sum[ket[Mod}[xi, N]].\text{ConjugateTranspose[ket}[i]], \{i, 0, N - 1\}] + \text{Sum[ket}[i].\text{ConjugateTranspose[k}$

$\text{Ure[x\_, N\_]:=Sum}\left[\text{KroneckerProduct}\left[\text{ket}[i].\text{ConjugateTranspose[ket}[i]], \text{ket}\left[\text{Mod}\left[\text{Mod}\left[x^i, N\right] + j, 16\right]\right].\text{Conju}\right.\right.$

$\text{Norm}\left[\left(\text{Urp}[7, 13].\text{ConjugateTranspose}[\text{Urp}[7, 13]] - \text{IdentityMatrix}\left[2^4\right]\right)\right]$

$\text{Norm}\left[\left(\text{Ure}[3, 15].\text{ConjugateTranspose}[\text{Ure}[3, 15]] - \text{IdentityMatrix}\left[2^8\right]\right)\right]$

2^7

0

0

128

Urp[3, 8]//MatrixForm

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

ket0 = $\mathbf{ket_0}$**;**

ket1 = $\mathbf{ket_1}$**;**

P0 = P_0**;**

P1 = P_1**;**

MUL3 = {{1, 0, 0, 0, 0, 0, 0, 0}, {0, 0, 0, 1, 0, 0, 0, 0}, {0, 0, 0, 0, 0, 0, 1, 0}, {0, 1, 0, 0, 0, 0, 0, 0}, {0, 0, 0, 0, 1, 0, 0, 0}, {

{0, 0, 1, 0, 0, 0, 0, 0}, {0, 0, 0, 0, 0, 1, 0, 0}};

SWAP23 = KroneckerProduct[Id, ket0, ket0].KroneckerProduct[Id, ket0, ket0] † +KroneckerProduct[Id, ket0, ke

KroneckerProduct[Id, ket1, ket0].KroneckerProduct[Id, ket0, ket1] † +KroneckerProduct[Id, ket1, ket1].Kronecke

SWAP13 = KroneckerProduct[ket0, Id, ket0].KroneckerProduct[ket0, Id, ket0] † +KroneckerProduct[ket0, Id, ke

KroneckerProduct[ket1, Id, ket0].KroneckerProduct[ket0, Id, ket1] † +KroneckerProduct[ket1, Id, ket1].Kronecke

SWAP12 = KroneckerProduct[ket0, ket0, Id].KroneckerProduct[ket0, ket0, Id] † +KroneckerProduct[ket0, ket1,

KroneckerProduct[ket1, ket0, Id].KroneckerProduct[ket0, ket1, Id] † +KroneckerProduct[ket1, ket1, Id].Kronecke

CNOT = KroneckerProduct[P0, Id] + KroneckerProduct[P1, X];

CNOT23 = KroneckerProduct[Id, CNOT];

CNOT13 = KroneckerProduct[P0, Id, Id] + KroneckerProduct[P1, Id, X];

CNOT12 = KroneckerProduct[CNOT, Id];

CNOTm = KroneckerProduct[Id, P0] + KroneckerProduct[X, P1];

CNOT32 = KroneckerProduct[Id, CNOTm];

CNOT31 = KroneckerProduct[Id, Id, P0] + KroneckerProduct[X, Id, P1];

CNOT21 = KroneckerProduct[CNOTm, Id];

CNOT3n21 = KroneckerProduct[X − Id, P1, P0] + KroneckerProduct[Id, Id, Id];

MUL3//MatrixForm

(*000 → 000 Id*)

(*001 → 011 CNOT32.CNOT21*)

(*010 → 110 CNOT21*)

(*011 → 001 CNOT32*)

(*100 → 100 Id*)

(*101 → 111 CNOT32*)

(*110 → 010 CNOT21*)

(*111 → 101 CNOT32*)

CNOT32.CNOT3n21//MatrixForm

MUL3 − CNOT32.CNOT3n21//MatrixForm

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Urp[7, 15] + Sum [KroneckerProduct [a1$_i$ket$_i$, a2$_j$ket$_j$, a3$_k$ket$_k$, a4$_l$ket$_l$] .KroneckerProduct [ket$_i$, ket$_j$, ket$_k$, ket$_l$] †

MatrixForm

$$
\left(\begin{array}{ccccccc}
1+\mathrm{a1}_0\mathrm{a2}_0\mathrm{a3}_0\mathrm{a4}_0 & 0 & 0 & 0 & 0 & 0 & \\
0 & \mathrm{a1}_0\mathrm{a2}_0\mathrm{a3}_0\mathrm{a4}_1 & 0 & 0 & 0 & 0 & \\
0 & 0 & \mathrm{a1}_0\mathrm{a2}_0\mathrm{a3}_1\mathrm{a4}_0 & 0 & 0 & 0 & \\
0 & 0 & 0 & \mathrm{a1}_0\mathrm{a2}_0\mathrm{a3}_1\mathrm{a4}_1 & 0 & 0 & \\
0 & 0 & 0 & 0 & \mathrm{a1}_0\mathrm{a2}_1\mathrm{a3}_0\mathrm{a4}_0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 1+\mathrm{a1}_0\mathrm{a2}_1\mathrm{a3}_0\mathrm{a4}_1 & \\
0 & 0 & 0 & 1 & 0 & 0 & \mathrm{a1}_0\mathrm{a2} \\
0 & 1 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 1 & 0 & \\
0 & 0 & 1 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 &
\end{array}\right.
$$

0000 → 0000(*Id*)

0001 → 0111(*SWAP14 X1 X2 X3 X4*)(**)

0010 → 1110(*SWAP34 X1 X2 X3 X4*)

0011 → 0110(*SWAP14 SWAP34 X1 X2 X3 X4*)(*0011 − 0010 − 0010—— − 0110*)

0100 → 1101(*SWAP23 X1 X2 X3 X4*)(*0100 − 1100 − 1101— − − − −—— − 1101*)

0101 → 0101(*Id*)

0110 → 1100(*SWAP12 SWAP23 X1 X2 X3 X4*)

0111 → 0100(*SWAP12 X1 X2 X3 X4*)

1000 → 1011(*SWAP12 X1 X2 X3 X4*)

1001 → 0011(*SWAP12 SWAP23 X1 X2 X3 X4*)

1010 → 1010(*Id*)

1011 → 0010(*SWAP23 X1 X2 X3 X4*)

1100 → 1001(*SWAP14 SWAP34 X1 X2 X3 X4*)

1101 → 0001(*SWAP34 X1 X2 X3 X4*)

1110 → 1000(*SWAP14 X1 X2 X3 X4*)

1111 → 1111(*Id*)

ket0 = {{1}, {0}};

ket1 = {{0}, {1}};

SWAP = KroneckerProduct[ket0, ket0].KroneckerProduct[ket0, ket0] † +KroneckerProduct[ket1, ket1].Kronecke

KroneckerProduct[ket1, ket0].KroneckerProduct[ket0, ket1] † +KroneckerProduct[ket0, ket1].KroneckerProduct

SWAP23 = KroneckerProduct[Id, SWAP, Id];

SWAP12 = KroneckerProduct[SWAP, Id, Id];

SWAP34 = KroneckerProduct[Id, Id, SWAP];

SWAP14 = KroneckerProduct[ket0, Id, Id, ket0].KroneckerProduct[ket0, Id, Id, ket0] † +KroneckerProduct[ket1

KroneckerProduct[ket1, Id, Id, ket0].KroneckerProduct[ket0, Id, Id, ket1] † +KroneckerProduct[ket0, Id, Id, ket1]

SWAP23 = KroneckerProduct[Id, SWAP, Id];

MUL7 = SWAP14.SWAP12.SWAP23.KroneckerProduct[X, X, X, X];

MUL7.KroneckerProduct[ket0, ket0, ket0, ket0]//MatrixForm

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

MUL7.MUL7 † //MatrixForm

$$\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{pmatrix}$$

Mod[1 7, 15]

7

Mod[%7, 15]

1