T400 Twisted GFSR

based on $GFSR(25, x^{25} + x^{11} + 1)$

n=25 words x w=16 bits = 400 bits, twisting vector $\mathbf{a} = \mathbf{0xA875}$ (a 16 bits vector)

twisting matrix $A = \begin{bmatrix} 0_{15x1} & I_{15x15} \\ \mathbf{a_{1x16}} \end{bmatrix}$ (a 16x16 bits array)

if we let $x = [x_0 \dots x_{w-2} x_{w-1}]$ then the block multiplication is

$$[x_0 \dots x_{w-2} \mid x_{w-1}] \, . \, \left[\begin{array}{cc} 0_{15x1} & I_{15x15} \\ \hline a_0 & a_1 \dots a_{15} \end{array} \right] = [\, x_{w-1} . a_0 \quad x_0 + x_{w-1} * a_1 \dots x_{w-2} + x_{w-1} * a_{16} \,]$$
$$= [\, x_{w-1} . \mathbf{a}_{1x16} \oplus shiftright(\mathbf{x}) \,]$$

The form of A is dictated by the necessity to make it simple to multiply by it :

$$\mathbf{x} . \mathbf{A} \; = \; if \; (x_{w-1} \; = \; 0) \; then \; shiftright(\mathbf{x}) \; else \; shiftright(\mathbf{x}) \oplus \mathbf{a}$$

(Matsumoto, Kurita, 1992) Theorem : if $\varphi_A(x)$ is the characteristic polynomial of the $w \times w$ bits matrix A and $\varphi_A(t^n + t^m)$ is of degree nw and is primitive then the period of :

$$x_{l+n} = x_{l+m} \oplus x_l . A$$

is $2^{nw} - 1$.

This generator returns the random floats $\frac{x}{2^{16}}$

In [26]:
```
a_15_ident:diagmatrix(15,1)$
```

Out[26]:
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

In [27]:
```
a_15_zero_row:[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]
```

Out[27]:
$$[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$$

In [28]:
```
a_15_zero_col:transpose(a_15_zero_row)
```

Out[28]:

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

In [29]:
```
a_16_zero_row:addcol(matrix(a_15_zero_row),matrix([0]))
```

Out[29]:

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

In [ ]:
```

```

In [30]:
```
a_16_vector_a:[1,0,1,0,1,0,0,0,0,1,1,1,0,1,0,1]
```

Out[30]:

$$\begin{bmatrix} 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1 \end{bmatrix}$$

In [31]:
```
a_15x16:addcol(a_15_zero_col,a_15_ident)$
```

Out[31]:

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

In [32]:
```
shiftright_16x16:addrow(a_15x16,a_16_zero_row)
```

Out[32]:

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

In [33]:
```
a_16x16:addrow(a_15x16,a_16_vector_a)
```

Out[33]:

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

In [34]:
```
phi:charpoly(a_16x16,t^25+t^11)
```

Out[34]:

$$\left(-t^{25}-t^{11}\right)^{2}$$

$$\left(\left(-t^{25}-t^{11}\right)^{2}\left(\left(-t^{25}-t^{11}\right)^{5}\left(\left(-t^{25}-t^{11}\right)\left(\left(-t^{25}-t^{11}\right)\left(\left(\left(-t^{25}-t^{11}\right)^{2}\left(-t^{25}-t^{11}+1\right)+1\right)\right.\right.\right.\right.\right.$$

$$-1$$

In [35]:
```
phi:expand(phi)
```

Out[35]:

$$t^{400}+16\,t^{386}-t^{375}+120\,t^{372}-15\,t^{361}+560\,t^{358}-105\,t^{347}+1820\,t^{344}-455\,t^{333}+4368\,t^{330}-t^{325}$$
$$-13\,t^{311}-3003\,t^{305}+11440\,t^{302}-78\,t^{297}-5005\,t^{291}+12870\,t^{288}-286\,t^{283}-6435\,t^{277}-t^{275}+$$
$$-6435\,t^{263}-11\,t^{261}+8008\,t^{260}-1287\,t^{255}-t^{250}-5005\,t^{249}-55\,t^{247}+4368\,t^{246}-1716\,t^{241}-10$$
$$t^{233}+1820\,t^{232}-1716\,t^{227}-t^{225}-45\,t^{222}-1365\,t^{221}-330\,t^{219}+560\,t^{218}-1287\,t^{213}-9\,t^{211}-12$$
$$t^{205}+120\,t^{204}-715\,t^{199}-36\,t^{197}-210\,t^{194}-105\,t^{193}-462\,t^{191}+16\,t^{190}-286\,t^{185}-84\,t^{183}-252$$
$$+t^{176}-78\,t^{171}-126\,t^{169}-210\,t^{166}-t^{165}-165\,t^{163}-13\,t^{157}-126\,t^{155}-120\,t^{152}-55\,t^{149}-t^{143}-$$
$$t^{135}-36\,t^{127}-10\,t^{124}-t^{121}-9\,t^{113}-t^{110}-t^{100}-t^{99}-4\,t^{86}-6\,t^{72}-4\,t^{58}-t^{50}-t^{44}-$$

In [36]:
```
gf_primitive_poly_p(phi,2)
```

Out[36]: **true**

In [37]:
```
hipow(phi,t)
```

Out[37]: 400

In [46]:
```
x:matrix([1,0,1,0,1,1,1,1,0,1,0,1,0,0,0,1])
```

Out[46]: $\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$

In [47]:
```
a_16_vector_a_m:matrix(a_16_vector_a)
```

Out[47]: $\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$

In [48]:
```
mod(x . a_16x16,2)
```

Out[48]: $\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$

In [60]:
```
if (x[1][16] = 0) then (x . shiftright_16x16) else mod(x . shiftright_16x16 + a_16_vector_a_
m,2)
```

Out[60]: $\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$

In [ ]:
```

```