



```
source code:
t = a[0] ^ a[1] ^ a[2] ^ a[3]
u = a[0]
a[0] ^= t ^ xtime(a[0] ^ a[1])
a[1] ^= t ^ xtime(a[1] ^ a[2])
a[2] ^= t ^ xtime(a[2] ^ a[3])
a[3] ^= t ^ xtime(a[3] ^ u)
```

