$\mathbb{F}_{\mathbf{2}^{\mathbf{607}}}$

$\mathbb{F}_{2^{503}}$ $\mathbb{F}_{2^{607}}$

$\mathbb{F}_p$ p

2 *

$\mathbb{F}_{2^{503}}$

2

2

$\mathbb{F}_{2^n}$ $O(\exp((c+o(1))n^{\frac{1}{3}}(\log n)^{\frac{2}{3}}))$

$c \approx 1.4$

n

$\mathbb{F}_{2^{607}}$

$\mathbb{F}_{2^{607}}$

$\mathbb{F}_{2^{521}}$

K $\mathbb{F}_{2^n}$

$\mathbb{F}_2[X]/(f(X))$ f

n $\mathbb{F}_2$ K

K

0 $n-1$

$\star$

$\mathbb{F}_{2^{607}}$

f $X^n + f_1$ f_1
f_1

f_1
$O(\log n)$

$\mathcal{B}$

$\prod_{i=1}^{l} \pi_i^{e_i} = 1$ π_i

K

$\mathcal{B}$
b $\mathcal{B}$ $\frac{2^{b+1}}{b}$

$\mathcal{B}$
A B d_A d_B
k 2 $\sqrt{n/d_A}$ $h = \lceil \frac{n}{k} \rceil$

$$C = AX^h + B,$$
$$D = C^k = A^k X^{hk} + B^k \equiv A^k X^{hk-n} f_1 + B^k \ [f].$$

C D
$\sqrt{n d_A}$
(C, D)
$\mathcal{B}$

$\mathcal{B}$ $\pi_i,\ 1 \leq i \leq \#\mathcal{B}$ α_i
β_i

$$C = \prod_i \pi_i^{\alpha_i}, D = \prod_i \pi_i^{\beta_i}, \Rightarrow DC^{-k} = \prod_i \pi_i^{\beta_i - k\alpha_i} = 1,$$
$$\Rightarrow \sum_i (\beta_i - k\alpha_i) \log \pi_i \equiv 0 \ [2^n - 1]$$

$\mathcal{B}$

b

$n^{1/3}(\log n)^{2/3}$

b

b b 1

d_A d_B

b *

$2^{d_A+d_B+1}$ (A, B)

$\mathcal{B}$

d_A d_B C

D

d_B

d_A C D

$\frac{hk-n+\deg f_1}{k}$

k C D

$n^{2/3}(\log n)^{1/3}$

k

k 2

k $\sqrt{\frac{n}{d_A}} = \left(\frac{n}{\log n}\right)^{\frac{1}{3}}$

$k = 4$

$n = 607$

$k = 4$ $k = 8$ $k = 8$

k $-k$

---

*

$\mathbb{F}_{2^{607}}$

1

k

f_1 f_1

f_1

$\deg D$

f_1

$n = 607$

$b = 23$ $\#\mathcal{B} = 766,150$ $d_A = 21, d_B = 28, k = 4, h = 152$

f_1 $X^9 + X^7 + X^6 + X^3 + X + 1$

f_1 $(X+1)^2(X^2+X+1)^2(X^3+X+1)$

C D 173 112

A

B g

$\deg g$

B ⋆

$$B \equiv AX^h \ [g].$$

g

x $l(x)$

x $l(1) = 0, l(2) = 1$

$AX^h \mod g$

d_B

$B_0 = AX^h \mod g$ $B_i = B_{i-1} + X^{l(i)}g$ $0 < i < 2^{1+d_B-d_g}$

$X^j g$

$\deg g$ $B's$ $B \equiv AX^h \ [g^j]$

g

$C = AX^h + B$

⋆ A

g^j $j \deg g$
$g, g^2, \ldots, g^j$ $\deg C$
C

C
$\deg C$
C

C

C

g^j g i
$2^{d_B+1-j\deg g}$

D
$B_0 = A(X^{hk-n} f_1)^{1/k}$
$\bmod g$ g
g
k
g^j D

D
C
D D
C $\deg C$
$\deg D$ $\mathbb{F}_{2^{607}}$ k
4 C D

$\mathbb{F}_{2^{607}}$

$\deg C$ $\mathbb{F}_{2^{997}}$
$k = 8$ $\deg D$
$\deg C$ D

D

$\deg C$ $\deg C - \mathcal{L}$
$\mathcal{L}$

1
$\star$

10^8
2.10^9

$\mathbb{F}_2$

$\star$
$\mathbb{F}_2$

$\mathbb{Z}/(2^n-1)\mathbb{Z}$

C D

10

30

C

2^{d_B+1} $d_B = 28$

512

B

B

A_f B_f A B

$$\begin{aligned}\text{chunk}(A_f, B_f) =& \{(A,B) = (A_f X^{\delta_A+1} + A_v, B_f X^{\delta_B+1} + B_v),\\ & \deg A_v \leq \delta_A, \deg B_v \leq \delta_B\}, \qquad \delta_A = 6, \delta_B = 24.\end{aligned}$$

$2^7 = 128$

2^{25} 32

32 2^γ γ

$2^{-\gamma} \times 32$

$AX^h \mod g$ g

2^γ

B

A

A g

$\mathbb{F}_{2^{607}}$

g

A

$$B_f X^{\delta_B+1} + B_v \equiv AX^h \ [g].$$

A ϵ $\epsilon \le \delta_A + 1$

$$B_v + \alpha X^h \equiv AX^h + B_f X^{\delta_B+1} \ [g], \qquad \deg \alpha < \epsilon.$$

$\mathbb{S}$ $\mathbb{F}_2$

$\mathbb{V} = F \oplus G$ $F = \langle 1, X, X^2, \dots X^{\delta_B} \rangle$ $G = \langle X^h, \dots X^{h+\epsilon-1} \rangle$

$\mathbb{S}$ $\dim \mathbb{S} = \delta_B + 1 + \epsilon - d_g$ $\mathbb{S}$

$\mathbb{F}_2$

$d_g \le \delta_B + 1$ $\mathbb{S}$ $s_0 + \mathbb{S}'$

$s_0 = AX^h + B_f X^{\delta_B+1} \mod g$ $\mathbb{S}'$

$X^i g$ $0 \le i \le \delta_B - d_g$ $X^{h+i} + (X^{h+i} \mod g)$ $0 \le i <$

ϵ

$X^h \mod g$

$X^{h+i} \mod g$

2^ϵ

$d_g > \delta_B + 1$ $\mathbb{V}$ $\bar{\mathbb{V}} = \bar{F} \oplus G$ $\bar{F} = F \oplus \langle X^{\delta_B+1}, \dots X^{d_g-1} \rangle$

$\bar{\mathbb{S}}$ $\bar{\mathbb{V}}$ $\bar{s}_0$ $\bar{\mathbb{S}}$

$\bar{\mathbb{S}}'$ $u + \phi(u)$

$u \in G$ ϕ G $\bar{F}$

g $s_0 \in \mathbb{S}$

$\bar{s}_0$ $\bar{\mathbb{S}}'$ $\mathbb{S}'$

$\mathbb{S}$ $u + \phi(u)$ $u \in \phi^{-1}(F)$

$(\dim \bar{F} - \dim F) \times \epsilon$

$d_g > \delta_B + 1$

$\deg g$

$$\begin{aligned} g &= (X^{14} + X^{13} + X^{12} + X^{10} + X^8 + X^5 + 1)^2, \\ \bar{s}_0 &= X^{27} + X^{26} + X^3 + 1, \\ h &= 152, \quad \delta_B = 24, \quad \epsilon = 3. \end{aligned}$$

$\dim \bar{F} - \dim F$

$u + \phi(u)$ $u = X^{h+i}$ $0 \le i < \epsilon$

$\bar{s}_0$

$$T = \begin{pmatrix} 0\,1\,0\,1 \\ 1\,0\,1\,1 \\ 0\,0\,0\,0 \end{pmatrix}$$

T

$$s_0 = \bar{s}_0 + X^h + \phi(X^h) + X^{h+1} + \phi(X^{h+1}) \in \mathbb{S},$$
$$\phi^{-1}(F) = \langle X^h + X^{h+2} \rangle.$$

T

$\mathbb{S}'$ 0

$\bar{s}_0$ X^{25}

E' $\mathbb{V}$

γ ϵ

$2^{\delta_A+1+\gamma-\epsilon}$ $2^{\delta_B+1+\epsilon-\gamma}$

γ ϵ

$\gamma = \epsilon = 0$

128

γ ϵ

$\gamma > 0$

$\deg g$

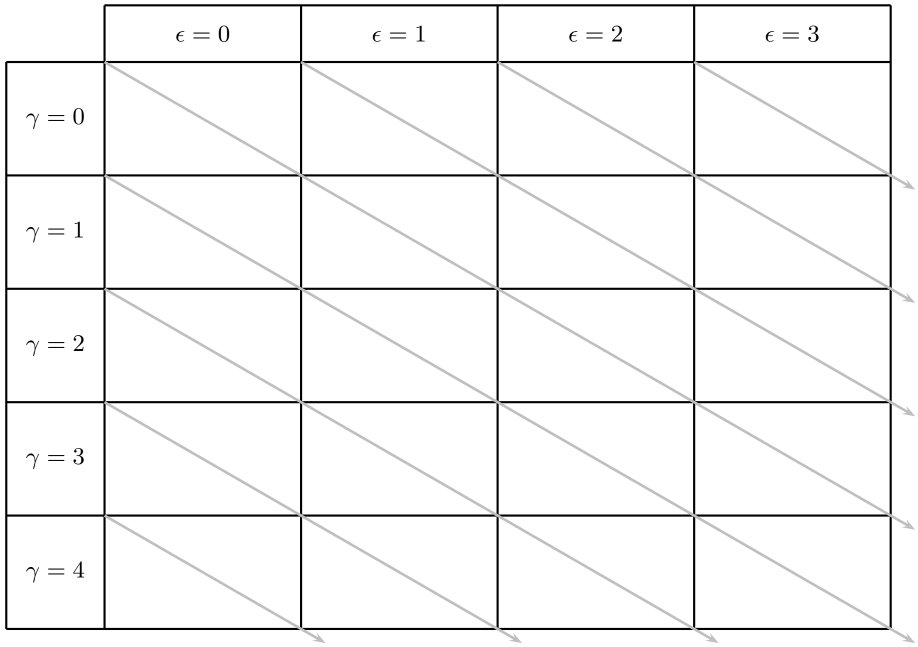
g g

γ ϵ

$$\gamma = 4,\ \epsilon = 3$$

(C, D)

$\mathbb{F}_{2^{607}}$



γ ϵ

C

D

D

D

b D

$$D_{\text{smooth}} = \gcd\left(D, D' \prod_{j=1+\lfloor \frac{b}{2} \rfloor}^{b} (X^{2^j} + X) \mod D\right).$$

D D_{smooth}

b $\frac{D}{D_{\text{smooth}}}$

$\mathcal{L}$

$2\mathcal{L}$

$\mathcal{L}$

D

D

C D

$\mathbb{F}_{2^{313}}$

X

$X+1$ $(X+1)^{16} = X^{16}+1$

$\mathbb{F}_2$

$X^{16}+1$ 32

$\frac{\deg P}{32}+3$

$\nu(Q)$ ν

Q $\nu_g(P)$

$\nu_g(P \mod X^{16}+1) = \nu_g(P)$

$P \equiv 0\ [X^{16}+1]$ $\leq$

$X+1$

4

$n = 607$ C D

$\mathbb{F}_2$

$\frac{2^{b+1}}{b}$

(C, D)

DC^{-k}

s s

DC^{-k}

$\mathbb{F}_{2^{607}}$

67.7

$\mathbb{Z}/(2^{607}-1)\mathbb{Z}$

± 1 $\pm k$

d

$\frac{1}{2^d}$

$\pm k$

$O(N^2)$ $O(N \log^2 N)$ 50

400

$\mathbb{F}_{2^{607}}$

19,000

8,000

1000

400 100

$d_B = 28$

10

815,726

2 40

650,000

3

217,867

1,033,593

67.7 524

120

904,004 765,427

64.3

$484,603 \times 484,603$

106.7

$2^{607} - 1$

$\mathbb{F}_{2^{607}}$

$\mathbb{F}_{2^{607}}$

≤ 2	

$\mathbb{F}_{2^{607}}$

$\mathbb{F}_{2^{997}}$

$\mathbb{F}_{2^n}$ n $1,000$
n $1,200$

C_{ab}

GF(2)

$\mathbb{F}_{2^{607}}$

m

$\mathrm{GF}(p)$

$\mathrm{GF}(p)$

$\mathrm{GF}(2^n)$

$\mathrm{GF}(2)$