

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

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

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

$$\begin{array}{ccc} \mathbb{F}_p & & p \\ 2 & & 2 \\ \mathbb{F}_{2^{503}} & & ? \end{array}$$

$$c \approx 1.4$$

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

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

$$\eta$$

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

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

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

$$\begin{array}{ccccccc}
 & & K & & \mathbb{F}_{2^n} & & \\
 & \mathbb{F}_2[X]/(f(X)) & & f & & K & \\
 n & \mathbb{F}_2 & & & & & \\
 \hline
 & & K & & 0 & & n-1
 \end{array}$$

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

$$\begin{matrix} f & X^n+f_1 & f_1 \\ f_1 & & f_1 \\ & O(\log n) & \end{matrix}$$

$${\mathcal B}$$

$$\prod\nolimits_{i=1}^l\pi_i^{e_i}\,=\,1\qquad\qquad\qquad\pi_i$$

$$(\mathbb{R}^d,\|\cdot\|)$$

$$\mathfrak{f}_\mathrm{c} = 1$$

$$\mathfrak{f}_\mathrm{c} = 1$$

$$\boldsymbol{K}$$

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

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

$$\begin{gathered} C=AX^h+B,\\ D=C^k=A^kX^{hk}+B^k\equiv A^kX^{hk-n}f_1+B^kf_1\,\,[f]. \end{gathered}$$

$$\begin{matrix} C & D \\ \sqrt{nd_A} & \\ (C,D) & \\ \mathcal{B} & \end{matrix}$$

$$\begin{matrix} \mathcal{B} & \pi_i, \,\, 1 \leq i \leq \#\mathcal{B} & \alpha_i \\ \beta_i & & \end{matrix}$$

$$\begin{aligned} C=\prod_i\pi_i^{\alpha_i},D=\prod_i\pi_i^{\beta_i},\Rightarrow DC^{-k}=\prod_i\pi_i^{\beta_i-k\alpha_i}=1,\\ \Rightarrow\sum_i(\beta_i-k\alpha_i)\log\pi_i\equiv0\,\,[2^n-1] \end{aligned}$$

$$\mathscr{B}$$

$$\begin{array}{ccccc}
& & b & & \\
n^{1/3}(\log n)^{2/3} & & & & \\
& b & & & \\
& b & & 1 & \\
\\
& d_A & d_B & & \\
& b & \star & & \\
& 2^{d_A+d_B+1} & & (A,B) & \\
& & d_A & d_B & \\
D & & & & C \\
& d_A & & & d_B \\
& \frac{hk-n+\deg f_1}{k} & & & \\
& & & C & D \\
& & & & \\
& k & C & D & \\
n^{2/3}(\log n)^{1/3} & & & & \\
& & k & & \\
& & & k & 2 \\
& & & & \sqrt{\frac{n}{d_A}} = \left(\frac{n}{\log n}\right)^{\frac{1}{3}} \\
& & & k=4 & \\
& n=607 & & & \\
k=4 & k=8 & k=8 & & -k \\
& k & & & \\
& \hline & & & \\
& * & & &
\end{array}$$

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

$$1 \\$$

$$k \\$$

$$\begin{matrix} f_1 \\ & \begin{matrix} f_1 \\ \deg D \end{matrix} \\ & f_1 \end{matrix}$$

$$\begin{matrix} n=607 \\ b=23 \qquad \# \mathcal{B}=766,150 \qquad d_A=21,d_B=28,k=4,h=152 \\ f_1 \qquad \qquad \qquad X^9+X^7+X^6+X^3+X+1 \\ f_1 \qquad \qquad \qquad \begin{matrix} (X+1)^2(X^2+X+1)^2(X^3+X+1) \\ C \qquad D \qquad 173 \qquad 112 \end{matrix} \end{matrix}$$

$$\begin{matrix} A \\ & \begin{matrix} B \\ \star \end{matrix} \\ & \begin{matrix} \deg g \\ B \equiv AX^h\ [g]. \end{matrix} \end{matrix}$$

$$\begin{matrix} g \\ & \begin{matrix} x & l(x) \\ & x \end{matrix} \\ & \begin{matrix} AX^h \mod g \\ d_B \\ B_0 = AX^h \mod g \qquad B_i = B_{i-1} + X^{l(i)}g \\ \qquad \qquad \qquad X^jg \end{matrix} \\ & \qquad \qquad \qquad l(1)=0,l(2)=1 \end{matrix}$$

$$\begin{matrix} \deg g & B's \\ & g \\ C=AX^h+B \\ \hline & A \end{matrix}$$

$$\frac{g^j}{g,g^2,\ldots,g^j} \qquad \frac{j\deg g}{C} \qquad \frac{\deg C}{}$$

$$\frac{C}{\deg C} \qquad \frac{}{C}$$

$$C$$

$$C$$

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

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

$$\frac{\begin{matrix}C\\D\\C\end{matrix}}{\deg D} \qquad \frac{D}{4} \qquad \frac{\mathbb{F}_{2^{607}}}{C} \qquad \frac{k}{D} \qquad \frac{D}{\deg C}$$

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

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

$$D$$

$$\mathfrak{d}_\mathrm{c}$$

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

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

$$\begin{matrix} &C&&D\\&&10&&\\&&&&30\\&&C&&\end{matrix}$$

$$\begin{matrix}&&&&\\&&&&\\2^{d_B+1}&&&&d_B=28\\512&&&&\end{matrix}$$

$$B \qquad \qquad \qquad B$$

$$A_f\qquad B_f\qquad\qquad A\qquad B$$

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

$$\begin{matrix}2^7=128\\2^{25}\\32\end{matrix}$$

$$\begin{matrix}32\\2^{-\gamma}\times 32\end{matrix}\qquad \qquad \begin{matrix}2^\gamma\\ \gamma\end{matrix}$$

$$\begin{matrix}AX^h\mod g\\2^\gamma\end{matrix}\qquad \qquad \qquad \begin{matrix}g\end{matrix}$$

$$\begin{matrix}A\\A\\g\end{matrix}\qquad \qquad \qquad \begin{matrix}B\end{matrix}$$

F₂₆₀₇

$$g \qquad A$$

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

$$A \quad \epsilon \quad \epsilon \leq \delta_A + 1$$

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

$$\begin{array}{ccc} \mathbb{V} = F \oplus G & F = \langle 1, X, X^2, \dots X^{\delta_B} \rangle & G = \langle X^h, \dots X^{h+\epsilon-1} \rangle \\ & \mathbb{S} \dim \mathbb{S} = \delta_B + 1 + \epsilon - d_g & \mathbb{F}_2 \\ & \mathbb{F}_2 & \mathbb{S} \end{array}$$

$$\begin{array}{cccccc}
d_g \leq \delta_B + 1 & \mathbb{S} & s_0 + \mathbb{S}' & & & \\
s_0 = AX^h + B_f X^{\delta_B+1} \mod g & & & & & \mathbb{S}' \\
X^i g & 0 \leq i \leq \delta_B - d_g & & X^{h+i} + (X^{h+i} \mod g) & 0 \leq i < \\
& \epsilon & & & & \\
& & X^h \mod g & & & \\
X^{h+i} \mod g & & & & 2^\epsilon &
\end{array}$$

$$\begin{array}{ccccccccc}
d_g > \delta_B + 1 & & \mathbb{V} & \bar{\mathbb{V}} = \bar{F} \oplus G & \bar{F} = F \oplus \langle X^{\delta_B+1}, \dots X^{d_g-1} \rangle \\
\bar{\mathbb{S}} & & & \bar{\mathbb{V}} & \bar{s}_0 & \bar{\mathbb{S}} & \bar{\mathbb{S}}' & u + \phi(u) \\
u \in G \quad \phi & & & & G & F & & \\
& g & & & & & s_0 \in \mathbb{S} & \\
\bar{s}_0 & \bar{\mathbb{S}}' & & & & & \mathbb{S}' & \\
& \mathbb{S} & & u + \phi(u) & & u \in \phi^{-1}(F) & & \\
(\dim \bar{F} - \dim F) \times \epsilon & & & & & & d_g > \delta_B + 1 & \\
& & & & & & \deg g &
\end{array}$$

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

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

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

$$T$$

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

$$\begin{matrix} & & & T \\ \mathbb{S}' & & & 0 \\ \bar{s}_0 & & & X^{25} \\ & E' & & \mathbb{V} \\ & & & \end{matrix}$$

$$\begin{matrix} & & \gamma & \epsilon \\ 2^{\delta_A+1+\gamma-\epsilon} & & 2^{\delta_B+1+\epsilon-\gamma} \\ & \gamma & & \epsilon \\ & & & \end{matrix}$$

$$\gamma = \epsilon = 0$$

$$\begin{matrix} & & 128 \\ & \gamma & \epsilon \\ & & \end{matrix}$$

$$\begin{matrix} \gamma > 0 \\ & \deg g \\ & g \\ \gamma & \epsilon \end{matrix}$$

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

$${\mathcal C}({\mathcal D})$$

$$\mathbf{G}^{\mathrm{I}}_{\mathrm{R}}(\omega)$$

$$\mathcal{C}^{\mathrm{I}}_{\mathrm{R}}(\omega)$$

$$\mathcal{C}^{\mathrm{II}}_{\mathrm{R}}(\omega)$$

$$\mathcal{C}^{\mathrm{III}}_{\mathrm{R}}(\omega)$$

$$\mathcal{C}^{\mathrm{IV}}_{\mathrm{R}}(\omega)$$

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

	$\epsilon = 0$	$\epsilon = 1$	$\epsilon = 2$	$\epsilon = 3$
$\gamma = 0$				
$\gamma = 1$				
$\gamma = 2$				
$\gamma = 3$				
$\gamma = 4$				

$\gamma \qquad \epsilon$

$$C$$

$$D$$

$$D$$

$$D$$

$$b$$

$$D$$

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

$$b$$

$$D$$

$$D_{\text{smooth}}$$

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

$$\mathcal{L}$$

$$2\mathcal{L}$$

$$\mathcal{L}$$

$$D$$

$$D \qquad \qquad C \qquad D$$

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

$$\begin{array}{ccc}
X & & \\
X+1 & & (X+1)^{16} = X^{16} + 1 \\
& \mathbb{F}_2 & \\
& \frac{X^{16} + 1}{\frac{\deg P}{32} + 3} & 32 \\
Q & & \nu(Q) \quad \nu \\
& & \nu_g(P \bmod X^{16} + 1) = \nu_g(P) \\
P \equiv 0 [X^{16} + 1] & & \leq \\
X+1 & &
\end{array}$$

$$n = 607 \quad C \quad D$$

F₂

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

$$\frac{s}{DC^{-k}} \stackrel{(C,D)}{\longrightarrow} \varepsilon$$

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

$$67.7$$

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

$$\pm 1$$

$$\pm k$$

$$d\,$$

$$\frac{1}{2^d} \leq \frac{1}{2^{\ell_1}} < \frac{1}{2^{\ell_2}} \leq \dots \leq \frac{1}{2^{\ell_{k-1}}} < \frac{1}{2^{\ell_k}} = \frac{1}{2^d}$$

$$\left(\frac{1}{2},\frac{1}{2}\right) \times \left(\frac{1}{2},\frac{1}{2}\right) \times \cdots \times \left(\frac{1}{2},\frac{1}{2}\right) \times \left(\frac{1}{2},\frac{1}{2}\right) \times \cdots \times \left(\frac{1}{2},\frac{1}{2}\right)$$

$$\pm k$$

$$\left(\frac{1}{2},\frac{1}{2}\right) \times \left(\frac{1}{2},\frac{1}{2}\right) \times \cdots \times \left(\frac{1}{2},\frac{1}{2}\right) \times \left(\frac{1}{2},\frac{1}{2}\right) \times \cdots \times \left(\frac{1}{2},\frac{1}{2}\right)$$

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

$$\left(\frac{1}{2},\frac{1}{2}\right) \times \left(\frac{1}{2},\frac{1}{2}\right) \times \cdots \times \left(\frac{1}{2},\frac{1}{2}\right) \times \left(\frac{1}{2},\frac{1}{2}\right) \times \cdots \times \left(\frac{1}{2},\frac{1}{2}\right)$$

$$\left(\frac{1}{2},\frac{1}{2}\right) \times \left(\frac{1}{2},\frac{1}{2}\right) \times \cdots \times \left(\frac{1}{2},\frac{1}{2}\right) \times \left(\frac{1}{2},\frac{1}{2}\right) \times \cdots \times \left(\frac{1}{2},\frac{1}{2}\right)$$

$$\left(\frac{1}{2},\frac{1}{2}\right) \times \left(\frac{1}{2},\frac{1}{2}\right) \times \cdots \times \left(\frac{1}{2},\frac{1}{2}\right) \times \left(\frac{1}{2},\frac{1}{2}\right) \times \cdots \times \left(\frac{1}{2},\frac{1}{2}\right)$$

$$\left(\frac{1}{2},\frac{1}{2}\right) \times \left(\frac{1}{2},\frac{1}{2}\right) \times \cdots \times \left(\frac{1}{2},\frac{1}{2}\right) \times \left(\frac{1}{2},\frac{1}{2}\right) \times \cdots \times \left(\frac{1}{2},\frac{1}{2}\right)$$

$$\left(\frac{1}{2},\frac{1}{2}\right) \times \left(\frac{1}{2},\frac{1}{2}\right) \times \cdots \times \left(\frac{1}{2},\frac{1}{2}\right) \times \left(\frac{1}{2},\frac{1}{2}\right) \times \cdots \times \left(\frac{1}{2},\frac{1}{2}\right)$$

$$\left(\frac{1}{2},\frac{1}{2}\right) \times \left(\frac{1}{2},\frac{1}{2}\right) \times \cdots \times \left(\frac{1}{2},\frac{1}{2}\right) \times \left(\frac{1}{2},\frac{1}{2}\right) \times \cdots \times \left(\frac{1}{2},\frac{1}{2}\right)$$

$$400\,$$

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

$$\begin{matrix} & 19,000 \\ & 8,000 \\ 1000 & \end{matrix}$$

$$\begin{matrix} 400 \\ & 100 \\ d_B=28 & \end{matrix}$$

$$10\,$$

$$\begin{matrix} & 815,726 \\ 2 & 40 \\ \end{matrix}$$

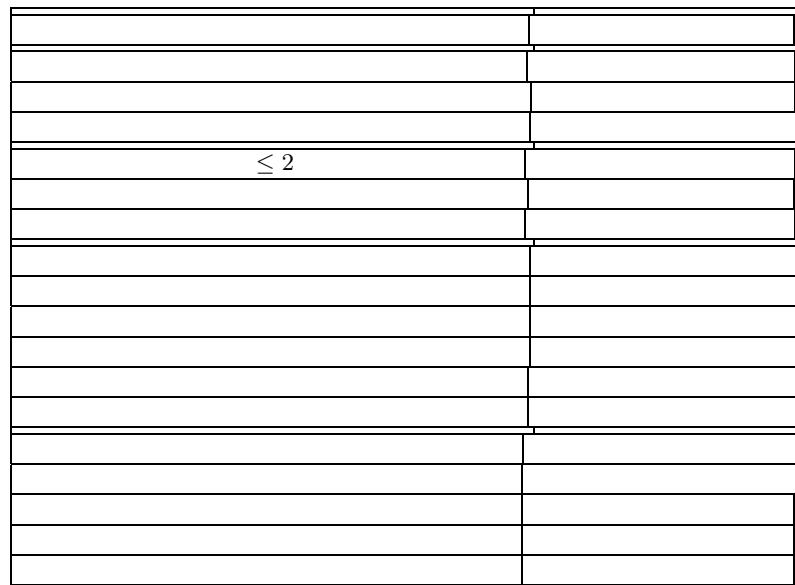
$$\begin{matrix} & 650,000 \\ 3 & \\ & 217,867 \\ & \\ 67.7 & 524 \\ & \\ & 120 \\ & 904,004 \\ & 64.3 \\ & \\ & 765,427 \\ & \end{matrix}$$

$$\begin{matrix} & 484,603\times484,603 \\ 106.7 & \end{matrix}$$

$$2^{607}-1$$

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

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



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

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

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

$$= \frac{1}{2} \left(\frac{\partial^2 \mathcal{L}}{\partial x^2} \right)_{\rm eq} \left(\frac{\partial x}{\partial t} \right)^2 + \frac{1}{2} \left(\frac{\partial^2 \mathcal{L}}{\partial p^2} \right)_{\rm eq} \left(\frac{\partial p}{\partial t} \right)^2$$

$$\mathbb{R}^{n+1}_+$$

$$\mathbb{R}^n_+$$

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

$$m\,$$

$${\rm GF}(p)$$

$${\rm GF}(p)$$

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

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

