

[Redacted]

$2^{62}$

[Redacted]

$$f : \begin{cases} b_k = \sum_{i=0}^n \sum_{j=i}^n \lambda_{ijk} a_i a_j \\ \text{with } k = 1..m, \quad a_0 = 1 \end{cases}$$

$$n = m = 1$$

$$K = N$$

$N$

$$K = GF(q)$$

$K$

$$K = GF(2)$$

$\rightsquigarrow$

$$\left\{ \begin{array}{l} 0 = x \vee y \vee z \\ 1 = \neg t \end{array} \right. \quad \left\{ \begin{array}{l} 0 = xyz + xy + yz + xz + x + y + z \\ 1 = 1 + t \end{array} \right.$$

$\rightsquigarrow$

$$\begin{array}{l} \diamond \quad y_{ij} = x_i x_j \\ \diamond \quad 0 = y_{ij} - x_i x_j \end{array}$$



**Case**  $m > \frac{n^2}{2}$ :

- $y_{ij} = x_i x_j$
- $m$   $m$

**Case**  $m = \varepsilon \frac{n^2}{2}$ :

$$n^{\mathcal{O}(1/\sqrt{\varepsilon})}$$

**Case**  $m \approx n$ :

$n$

$n$

$n > 100$

◇

◇

◇

$K$

$K = GF(q) \quad q = p^\alpha$

$\exists \quad GF(q^n) = K[X]/P(X)$

$P \quad n \quad K$

$GF(q^n) \cong K^n$

$x \in GF(q^n) \quad (x_1, \dots, x_n)$

$K[X] \quad P$

$f : K^n \rightarrow K^n$

◇

◇  $n \quad n \quad K$

[Redacted]

$$b = f(a) = a^{q^s} \quad b_i = f_i(a_1, \dots, a_n) \quad K$$

$$f(a) = \sum a^{q^s + q^t} \quad f_i$$

[Redacted]  $GF(2)$

$$b = f(a) = a + a^3 + a^5 =$$

$$(a_2X^2 + a_1X + a_0) + (a_2X^2 + a_1X + a_0)^3 + (a_2X^2 + a_1X + a_0)^5 \text{ mod } X^3 + X^2 + 1 =$$

$$(a_2 + a_2a_1 + a_2a_0 + a_1)X^2 + (a_2a_1 + a_1a_0 + a_2)X + (a_0 + a_2 + a_1a_0 + a_2a_0)$$

$$\begin{cases} b_2 & = & a_2 + a_2a_1 + a_2a_0 + a_1 \\ b_1 & = & a_2a_1 + a_1a_0 + a_2 \\ b_0 & = & a_0 + a_2 + a_1a_0 + a_2a_0 \end{cases}$$

[Redacted]

$$f(a) = \sum_{q^s + q^t \leq d} \gamma_{st} a^{q^s + q^t}$$

- $n$
- $f : \{ b_i = f_i(a_1, \dots, a_n) \}_{i=1..n}$

- $f$
- $S \quad T$

$$g = T \circ f \circ S$$

$$g : x \xrightarrow{S} a \xrightarrow{f} b \xrightarrow{T} y$$

Slide 13

$n$

$g : \{ y_i = g_i(x_1, \dots, x_n) \}_{i=1..n}$

$T \quad S \quad f$

$f$

$g^{-1}$

$x \xleftarrow{S^{-1}} a \xleftarrow{f^{-1}} b \xleftarrow{T^{-1}} y$

$g$

$g \quad y$

$x$

$K^n \quad g$

$\neq$

$\exists$

S T

$f \quad \exists \quad q^{n/2}$

$f \quad 99\% \quad d \ll q^n - 1$

$g \quad f$

$G \quad F$

$$g(x) = \sum_{i=0}^{n-1} \sum_{j=i}^{n-1} G_{ij} x^{q^i + q^j}$$

$G \quad n \quad F \quad r = \log d$

$T^{-1} \circ g \stackrel{?}{=} f \circ S$

$f \circ S$

$G' = WGW^t$

$T^{-1} \circ g = \sum_{k=0}^{n-1} t_k G^{*k}$

$G^{*k}$

$T$

$T^{-1} \circ g$

$t_k \in K^n$

$Rank\left(\sum_{k=0}^{n-1} t_k G^{*k}\right) = r$





$(n, n, m, r, K)$

$m$   $n \times n$   $K$   $M_1, \dots, M_m$   
 $\alpha$   $M_i$   $\leq r$

$$\text{Rank}\left(\sum_i \alpha_i M_i\right) \leq r.$$



•  $r(n-r)$   $K^n$   $n(n-r)$   
 $2^{152}$   
 $2^{80}$

•  $(r+1)(r+1)$   
 $2^{97}$

[Redacted]

- $D^*$
- 
- 
- 
- 
- $D^*$
- 

$$\begin{matrix} C^* & [C] \\ C^{*-} & \end{matrix}$$

$g$

◇

$x \quad g(x)$

◇

$(x_i)$

$x_i = 0 \quad 1$

[Redacted]



[Redacted]

}

$$WF = n^{3 \log d}$$

$d$

$$d = n^{\mathcal{O}(1)}$$

$$WF = n^{\mathcal{O}(\log n)}$$

$$WF = e^{\mathcal{O}(\log^2 n)}$$

[Redacted]

◇

$$e^{\log^2 n}$$

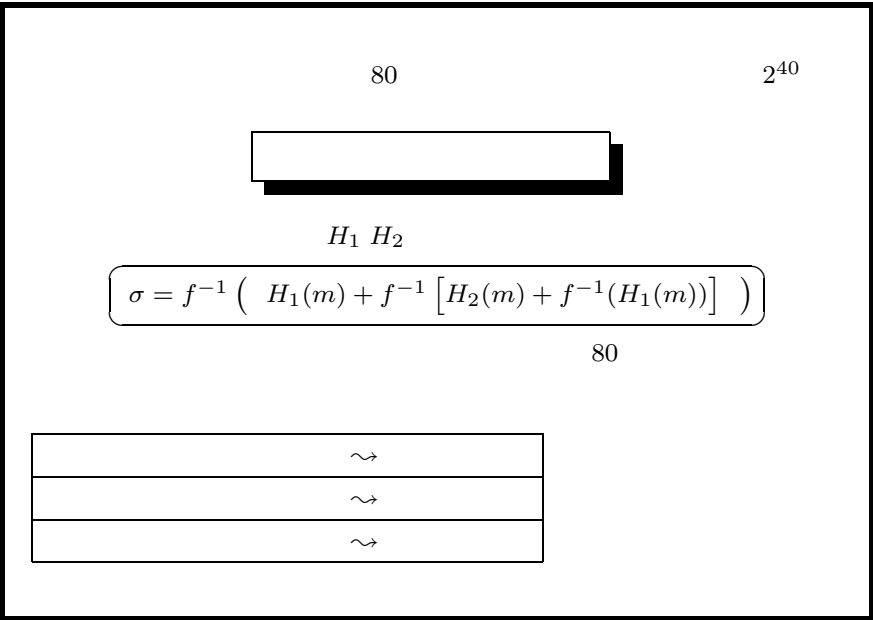
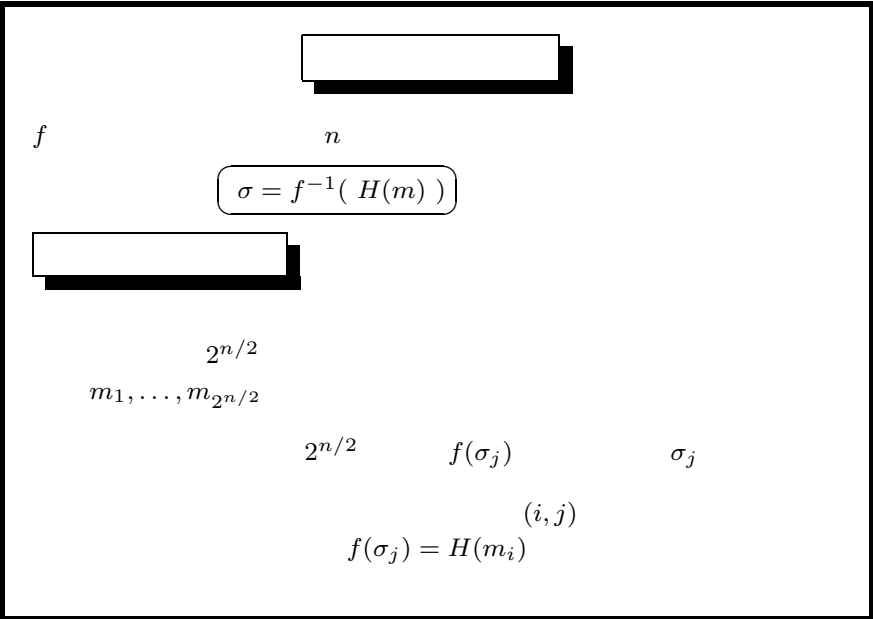
◇

$$n \geq 127 \quad d > 96$$

◇

-

◇




[Redacted]


$$= 1024 + 256 + 128$$

[Redacted]

- 
- 
- 
-



- 
- 
- 




$m$   $n \times n$

$GF(q)$   $M_1, \dots, M_m$

$\alpha \in GF(q)^n$   $M = \sum \alpha_i \cdot M_i$

$r < n$



$2^{122}$

$K = GF(65521)$   $n = 7$   $m = 7$   $r = 5$

10  $7 \times 7$



- $S \quad T$
- $n \times n \quad X$
- $\beta_{1i} \quad M_i$   
 $N_1 = \sum \beta_{1i} \cdot M_i$   
 $M \quad N_2 = M + N_1$   
 $N_2 = \sum \beta_{2i} \cdot M_i$   
 $(TN_2S + X) - (TN_1S + X) = T(N_2 - N_1)S = TMS.$

