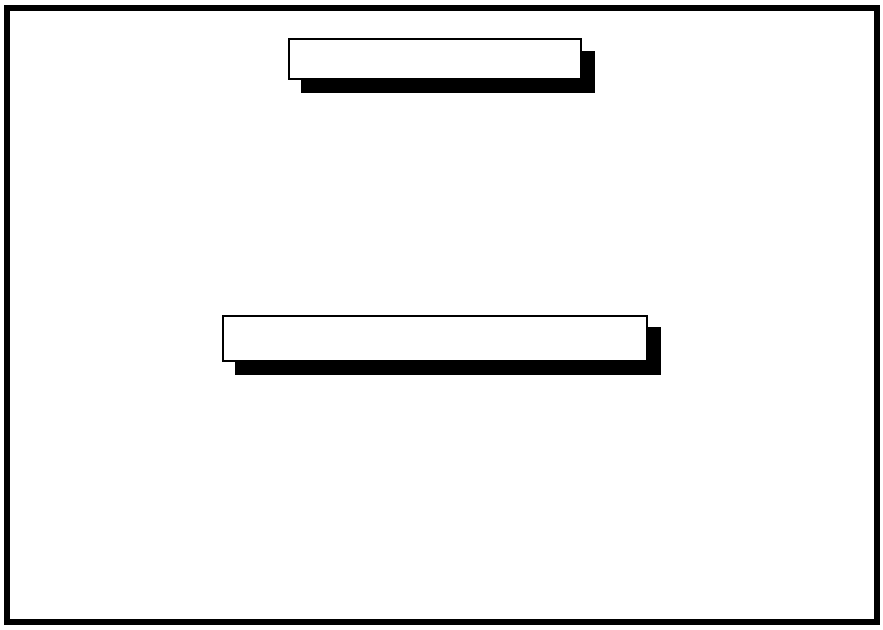
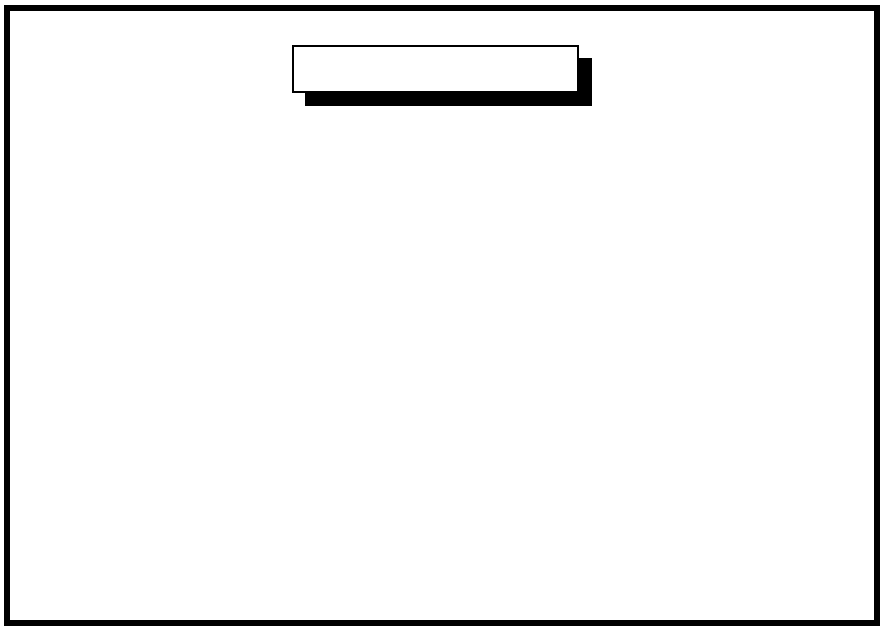
Road Map

80

- $\rightsquigarrow$ $\rightsquigarrow$ $\rightsquigarrow$ 2^{152}
- $\rightsquigarrow$ $\rightsquigarrow$ 2^{97}
- $\rightsquigarrow$ 2^{62}

$\leq$





2^{62}

K

m **n** K

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

$n = m = 1$

$K =$ $_N$ N

$K = GF(q)$

K

$K = GF(2)$

$\rightsquigarrow$

$$\begin{cases} 0 = x \vee y \vee z \\ 1 = \neg t \end{cases} \qquad \begin{cases} 0 = xyz + xy + yz + xz + x + y + z \\ 1 = 1 + t \end{cases}$$

$\rightsquigarrow$

- $y_{ij} = x_i x_j$
- $0 = y_{ij} - x_i x_j$

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 $K = GF(q)$ q $q = p^{\alpha}$

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

P n K

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

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

$K[X]$ P

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

◇

◇ n n K

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

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

$GF(2)$

$b = f(a) = a + a^3 + a^5 =$
$(a_2X^2 + a_1X + a_0) + (a_2X^2 + a_1X + a_0)^3 + (a_2X^2 + a_1X +$
$a_0)^5 \ mod \ X^3 + X^2 + 1 =$
$(a_2+a_2a_1+a_2a_0+a_1)X^2+(a_2a_1+a_1a_0+a_2)X+(a_0+a_2+a_1a_0+a_2a_0)$

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

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

- n

  $f : \left\{ \ \ b_i = f_i(a_1, \ldots, a_n) \ \ \right\}_{i=1..n}$

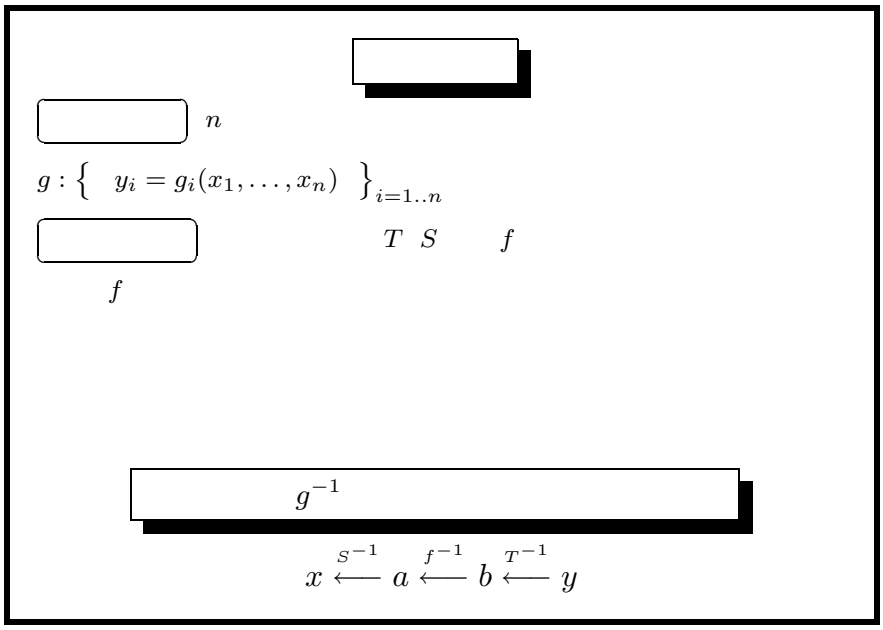
- f

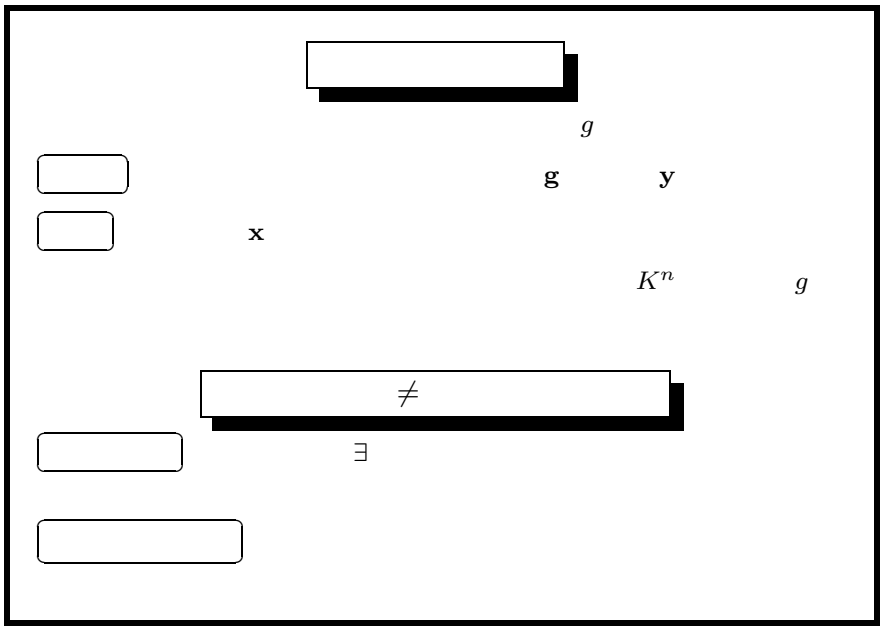
  S T

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

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

Slide 13


n
$g : \{ \quad y_i = g_i(x_1, \ldots, x_n) \quad \}_{i=1..n}$
T S f
f
g^{-1}
$x \overset{S^{-1}}{\longleftarrow} a \overset{f^{-1}}{\longleftarrow} b \overset{T^{-1}}{\longleftarrow} y$


g
g y
x
K^n g
≠
∃

S T

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

f 99% $d << q^n - 1$

g f

G F

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

G n F $r = \log d$

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

$f \circ S$

$G' = WGW^t$ r

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

g^{q^k}

T

$T^{-1} \circ g$

$t_k \in K^n$

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

(n, n, m, r, K)

m $n \times n$ K $M_1, \ldots M_m$

α M_i $\leq r$

$$Rank(\sum_i \alpha_i M_i) \leq r.$$

- $n(n-r)$
  $r(n-r)$ K^n
  $\mathbf{2^{152}}$
  2^{80}
- $(r+1)$ $(r+1)$
  $\mathbf{2^{97}}$

- D^*
-
-

-
- C^* $[C]$
- D^* C^{*-}
-

g

◇

x $g(x)$

◇

(x_i)

$x_i = 0$ 1

G_j x_i g

$G_j = 0$

x

G_j x_i

G_j x_i

G_j

$G_j = 0$ x_i

◇

◇

◇ 840

$1 + x + y + x^2y + xy^2 + x^3y + x^2y^2$

2^{62} 390

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

d

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

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

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

◇

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

◇ $n \geq 127 \;\; d > 96$

◇

–

◇

f n

$\sigma = f^{-1}(\ H(m)\ )$

$2^{n/2}$

$m_1, \ldots, m_{2^{n/2}}$

$2^{n/2}$ $f(\sigma_j)$ σ_j

(i, j)

$f(\sigma_j) = H(m_i)$

80 2^{40}

H_1 H_2

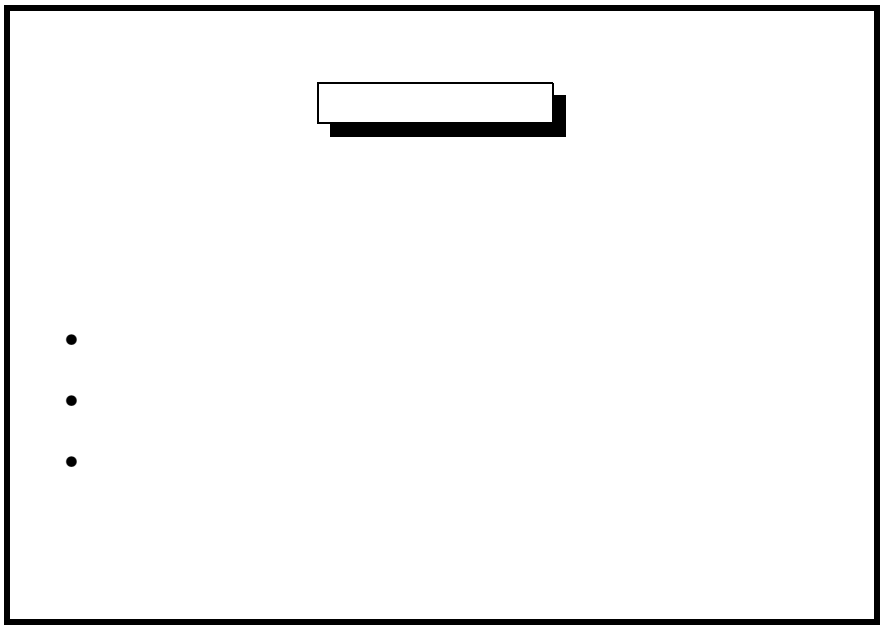
$$\sigma = f^{-1}\left(\ H_1(m) + f^{-1}\left[H_2(m) + f^{-1}(H_1(m))\right]\ \right)$$

80

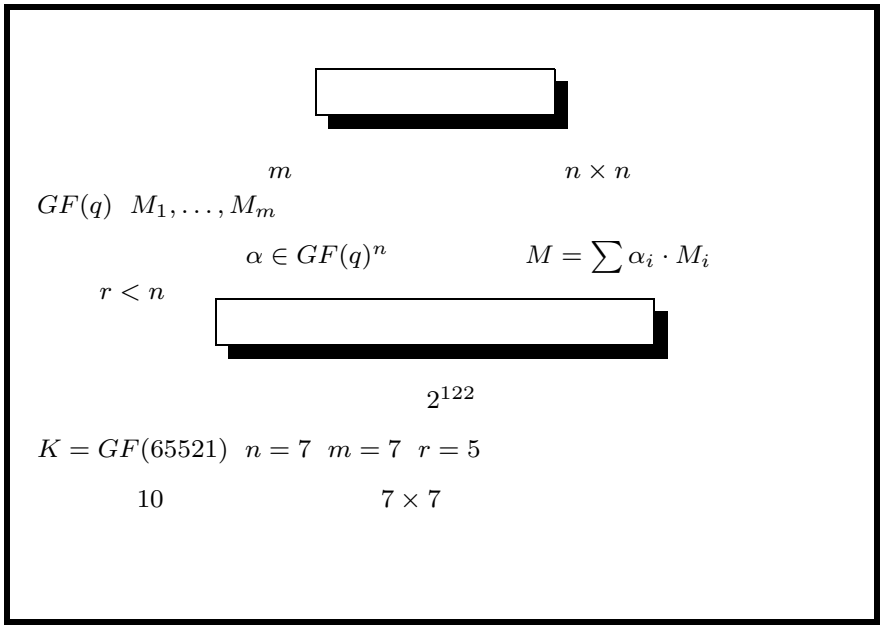
$\rightsquigarrow$
$\rightsquigarrow$
$\rightsquigarrow$

$$= \quad 1024 + 256 + 128$$

-
-
-
-



-
-
-



m $n \times n$

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

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

$r < n$

2^{122}

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

10 7×7

- S T
- $n \times n$ X
- β_1 M_i

$$N_1 = \sum \beta_{1i} \cdot M_i$$

M $N_2 = M + N_1$

$$N_2 = \sum \beta_{2i} \cdot M_i$$

$$(TN_2S + X) - (TN_1S + X) \;=\; T(N_2 - N_1)S \;=\; TMS.$$

$$\longrightarrow$$

$$H(X),\ H(TN_1S + X),\ H(TN_2S + X),\ H(S, T)$$

$$\longleftarrow$$

$$q \in \{0, 1, 2\}$$

$q = 0$

$$\longrightarrow$$

$$(TN_1S + X),\ (TN_2S + X)$$

$q = 1, 2$

$$\longrightarrow$$

$$S,\ T,\ \beta_q, X$$