McEliece Cryptosystem

permutation matrix: a row-permutation of Id matrix

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

Alice

message $x \in \mathbb{F}_2^k$

Encrypt:

random $e \in \mathbb{F}_2^k$

$wt(e) = t$

(correctable error)

$y = xG_1 + e$

codeword + error

G_1

public key G_1

secret

Bob

Choose ① G $k \times n$ gen. matrix for a binary linear $[n,k]$-code with $d = d(C)$

② $S = k \times k$ invertible matrix over $\mathbb{F}_2$

③ $P = n \times n$ permutation matrix over $\mathbb{F}_2$

$G_1 = SGP$ ($k \times n$ matrix)

y ciphertext

Decrypt:

$y_1 = yP^{-1}$

$= (xG_1 + e)P^{-1}$

$= \underbrace{xSG}_{\text{codeword for } G} + e'$ + error

still $wt(e') = wt(e)$

Hard Problem:

decoding w.r.t. G_1

Bob choose G to have efficient decoding.

decode y_1

get $x_1 = xSG$

find x_0 s.t. $x_0 G = x_1$

compute $x = x_0 S^{-1}$

$\mathcal{L}$(decrypted plaintext)