McEliece Cryptosystem

→ Sender Alice → talks to bob → no noise now but there is some eve's dropper Eve listening in

Alice wants to send info to bob but doesn't want eve to hear it.

→ First everyone has a public key and a secret key
  ↳ Alice encrypts the message with bob's public key
  ↳ Only bob's secret key can decode this info

→ How will bob generate his public and secret key

→ Bob first chooses a generator matrix:

Binary Goppa code ← $G \in \mathbb{F}_2^{n \times k}$, → appropriate linear code that is efficiently decodable for upto t errors

→ Choose a random invertible matrix $S \in \mathbb{F}_2^{k \times k}$ and a random permutation matrix $P \in \mathbb{F}_2^{n \times n}$ → Entries 0, 1 such that if you multiply the matrix with a vector it permutes the coordinates of that vector → Exactly 1 1 in every row and col

→ From this bob assembles his secret key and public key

→ Secret key (S, G, P)

→ Public key $(S \times G \times P) = \hat{G}$ and t

Alice now to send a message to bob:

→ ~~a~~ message $x \in \mathbb{F}_2^k$ to bob

→ Choose random vector $e \in \mathbb{F}_2^n$ of weight t

→ Sends $\hat{G} * x + e$ to bob

To decrypt this message

• Bob computes $P^{-1}(\hat{G}x + e) = \underbrace{|G \cdot S \cdot x + P^{-1}e|}_{e' \text{ is some vector of weight } t} = |\underbrace{G(Sx) + e'}_{\text{just a corrupted codeword}}|$

decode this code to obtain Sx and can compute $S^{-1}(Sx) = x$

What ~~does~~ does eve see through all of this:

→ Message that alice sent $\hat{G}x + e$ and has $\hat{G}$

→ given this eve cannot ~~recover~~ recover x

→ First we hope that $\hat{G}$ looks like a completely random matrix to eve

→ Decoding a random linear code is hard

↳ Are these reasonable → Yes (Many experts)