McNie

NIST Postquantum Cryptography Project

Carl Miller

May 3, 2018

The Basics

- It's a public key encryption scheme based on the McEliece scheme.
- "McNie" = "McEliece" + "Niederreiter"
- It uses Low **Rank** Parity Check (LRPC) codes.

McEliece Encryption

McEliece Encryption

Low Rank Parity Check Codes

LRPC Codes

LDPC code = “Low Density Parity Check code”

LRPC code = “Low **Rank** Parity Check code”

LRPC Codes

Let q^m be a prime power (e.g., 2^{37}). A **low rank parity check matrix** H over $\mathbb{F}_{q^m}$ is a matrix whose entries span a low rank subspace of $\mathbb{F}_{q^m}$.

Such a matrix H is also **quasi-cyclic** if it can be decomposed into square blocks H_{ij} such that each H_{ij} is a circulant matrix:

$$H_{ij} = \begin{bmatrix} h_{ij}^1 & h_{ij}^2 & h_{ij}^3 & \cdots & h_{ij}^r \\ h_{ij}^2 & h_{ij}^3 & h_{ij}^4 & \cdots & h_{ij}^1 \\ \vdots & & & & \\ h_{ij}^r & h_{ij}^1 & h_{ij}^2 & \cdots & h_{ij}^{r-1} \end{bmatrix}$$

✓ EASY TO STORE

The Encryption Algorithm

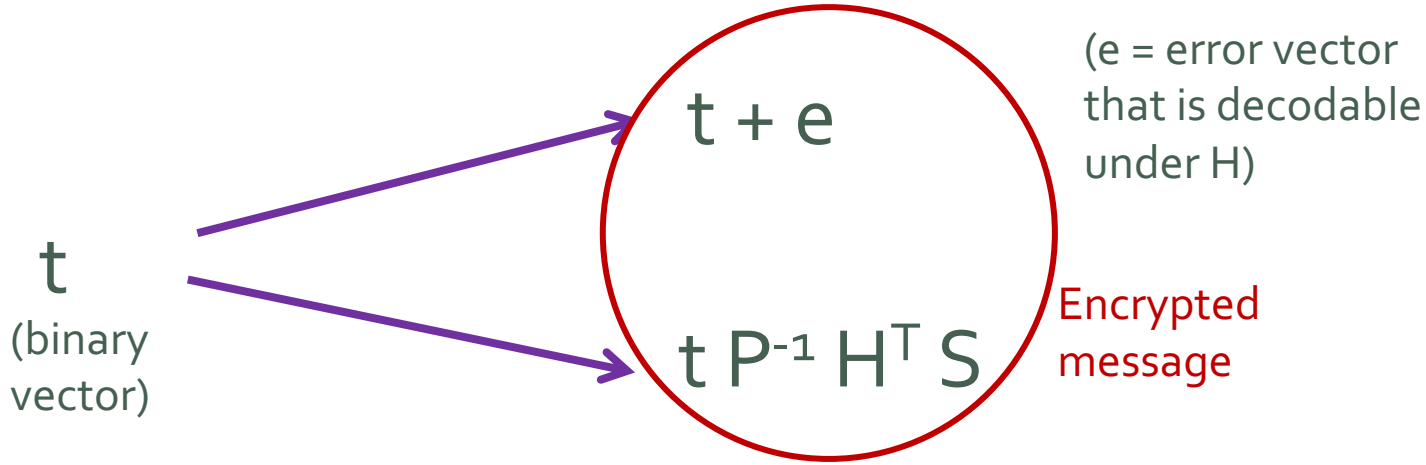
McNie Encryption

We work over the finite field of q^m elements.

Let H = quasi-cyclic LRPC matrix, efficiently decodable

P = random permutation matrix

S = random invertible matrix



Note that given P, H, S, we can recover t.

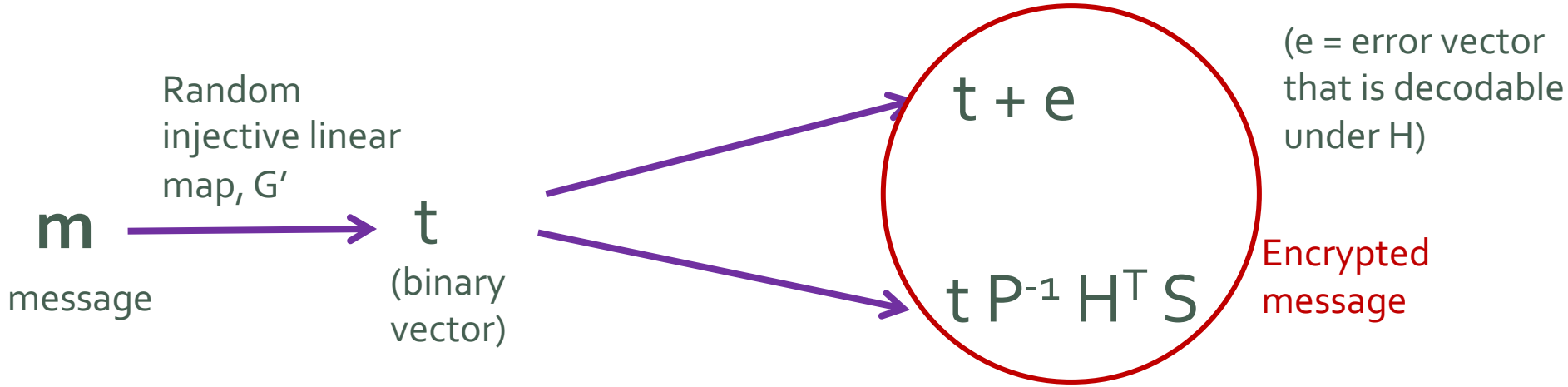
McNie Encryption

We work over the finite field of q^m elements.

Let H = quasi-cyclic LRPC matrix, efficiently decodable

P = random permutation matrix

S = random invertible matrix



The initial msg is also modified by an initial linear map, G'.

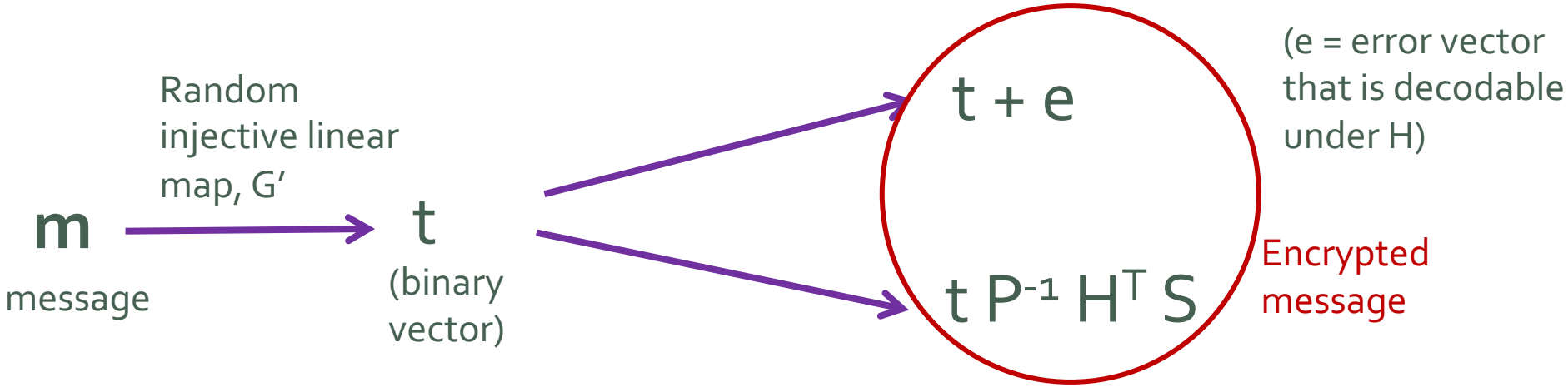
McNie Encryption

We work over the finite field of q^m elements.

Let H = quasi-cyclic LRPC matrix, efficiently decodable

P = random permutation matrix

S = random invertible matrix



Let $F = P^{-1} H^T S$. Public key is G', F. Secret key is P, H, S.

Performance

Attack

From: Jon-Lark Kim <ctryggoggo1@gmail.com>
Sent: Tuesday, December 26, 2017 12:09 PM
To: pqc-forum
Cc: gaborit@unilim.fr; Perlner, Ray (Fed)
Subject: Re: [pqc-forum] OFFICIAL COMMENT: McNie

Dear Ray,

Philippe Gaborit reported us that our security can be reduced by a factor of 2(called Attack 1) We have reviewed his argument and think that he is correct.

Furthermore Philippe mentioned his new algorithm for ISD attack for rank metric codes written in the paper https://www.unilim.fr/pages_perso/philippe.gaborit/newGRS.pdf

Based on this new attack(called Attack 2), our security level decreases by about 30 bits more.

New Size Parameters (from conference talk)

n	l	k	d	r	m	q	failure	Key Size (bytes)	security
120	80	80	3	8	53	2	-23	795	128
138	92	92	3	10	67	2	-25	1156	192
156	104	104	3	12	71	2	-27	1385	256

Table: New suggested parameters for McNie using 3-quasi-cyclic LRPC code

Old Speed Parameters (before attack)

Table 5.1: Implementation results for McNie using 3-quasi-cyclic LRPC codes

n	k	l	blk	d	r	m	q	security	key gen. (ms)	encryption (ms)	decryption (ms)
93	62	62	31	3	5	37	2	128	62	1.087	1.595
105	70	70	35	3	5	37	2	128	91.5	1.358	2.016
111	74	74	37	3	7	41	2	192	121.8	1.660	2.473
123	82	82	41	3	7	41	2	192	163.5	1.996	2.934
111	74	74	37	3	7	59	2	256	171.1	2.299	3.366
141	94	94	47	3	9	47	2	256	288.5	2.941	4.352

Advantages & Limitations

- Claimed to achieve smaller key sizes than related protocols. (Don’t know if this still applies?)

- Decryption can fail, but authors imply that the probability of failure can be made very small.

McNie

NIST Postquantum Cryptography Project

Carl Miller

May 3, 2018