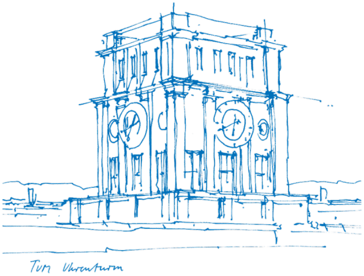
Non-Random Codes
in
Code-Based Cryptography

Sebastian Bitzer
TUM

PICS



Coding and Cryptography (COD)

Professor

Antonia

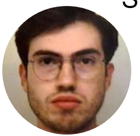
Hugo

Anna

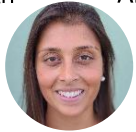
Stefan

Anmoal

me :)



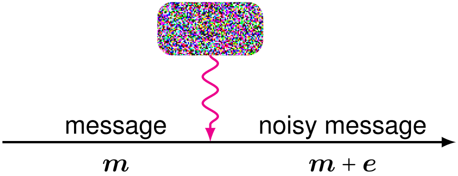
Gökberk



Emma

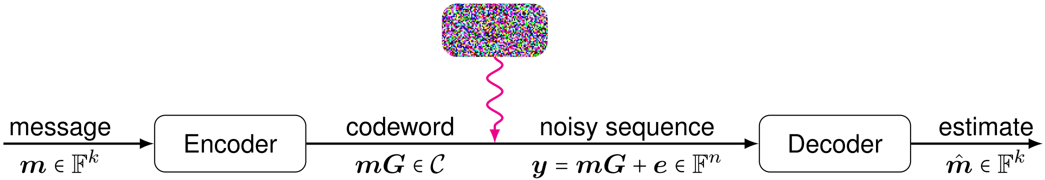
Sebastian

Channel Coding

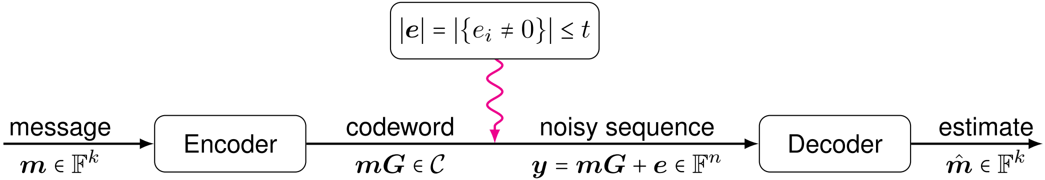


$\boldsymbol{m}$ $\quad$ $\boldsymbol{m} + \boldsymbol{e}$

Channel Coding



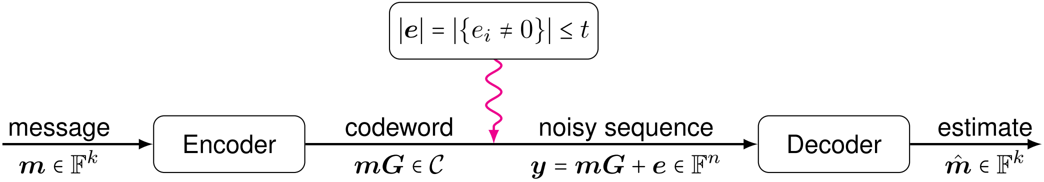
Channel Coding



Notations & Definitions

- $\mathcal{C} = \{\boldsymbol{mG} \mid \boldsymbol{m} \in \mathbb{F}^k\} = \{\boldsymbol{c} \mid \boldsymbol{cH}^\top = \boldsymbol{0}\} \subset \mathbb{F}^n$
- Generator matrix $\boldsymbol{G} \in \mathbb{F}^{k \times n}$
- Parity-check matrix $\boldsymbol{H} \in \mathbb{F}^{(n-k) \times n}$

Channel Coding



Notations & Definitions

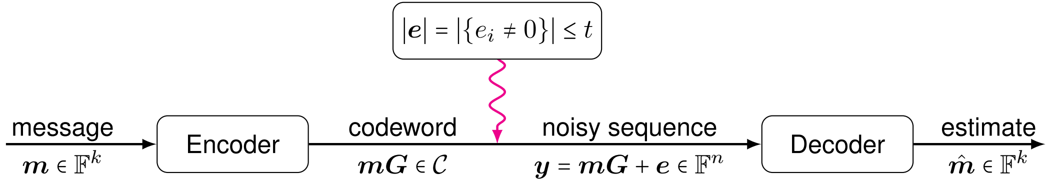
- $\mathcal{C} = \{\boldsymbol{mG} \mid \boldsymbol{m} \in \mathbb{F}^k\} = \{\boldsymbol{c} \mid \boldsymbol{cH}^\top = \boldsymbol{0}\} \subset \mathbb{F}^n$
- Generator matrix $\boldsymbol{G} \in \mathbb{F}^{k \times n}$
- Parity-check matrix $\boldsymbol{H} \in \mathbb{F}^{(n-k) \times n}$

75 Years of Coding

RS, Goppa, polar, convolutional, . . . codes

➔ structure allows efficient decoding

Channel Coding



Notations & Definitions

- $\mathcal{C} = \{\boldsymbol{mG} \mid \boldsymbol{m} \in \mathbb{F}^k\} = \{\boldsymbol{c} \mid \boldsymbol{cH}^\top = \boldsymbol{0}\} \subset \mathbb{F}^n$
- Generator matrix $\boldsymbol{G} \in \mathbb{F}^{k \times n}$
- Parity-check matrix $\boldsymbol{H} \in \mathbb{F}^{(n-k) \times n}$

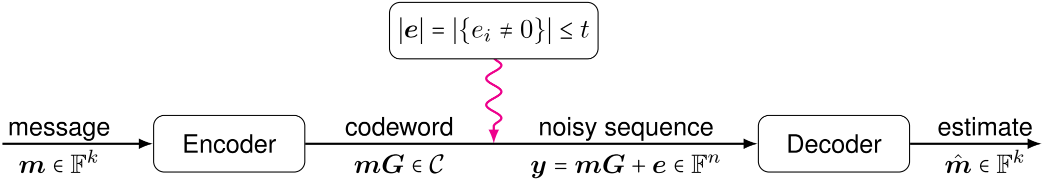
75 Years of Coding

RS, Goppa, polar, convolutional, ... codes

➔ structure allows efficient decoding

Coded computation, post-quantum cryptography, DNA storage, network coding

Channel Coding



Notations & Definitions

- $\mathcal{C} = \{\boldsymbol{mG} \mid \boldsymbol{m} \in \mathbb{F}^k\} = \{\boldsymbol{c} \mid \boldsymbol{cH}^\top = \boldsymbol{0}\} \subset \mathbb{F}^n$
- Generator matrix $\boldsymbol{G} \in \mathbb{F}^{k \times n}$
- Parity-check matrix $\boldsymbol{H} \in \mathbb{F}^{(n-k) \times n}$

75 Years of Coding

RS, Goppa, polar, convolutional, . . . codes

➔ structure allows efficient decoding

Coded computation, post-quantum cryptography, DNA storage, network coding

Code-based Cryptography

Decoding Problem

Given: $\boldsymbol{y} \in \mathbb{F}^n$ and $\boldsymbol{G} \in \mathbb{F}^{k \times n}$
Find: $\boldsymbol{m} \in \mathbb{F}^k$ s.t. $\boldsymbol{y} = \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e}$ with $|\boldsymbol{e}| \leq t$

Code-based Cryptography

Decoding Problem

Given: $\boldsymbol{y} \in \mathbb{F}^n$ and $\boldsymbol{G} \in \mathbb{F}^{k \times n}$
Find: $\boldsymbol{m} \in \mathbb{F}^k$ s.t. $\boldsymbol{y} = \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e}$ with $|\boldsymbol{e}| \leq t$

Syndrome Decoding Problem

Given: $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}^{(n-k) \times n}$
Find: $\boldsymbol{e} \in \mathbb{F}^n$ s.t. $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$ and $|\boldsymbol{e}| \leq t$

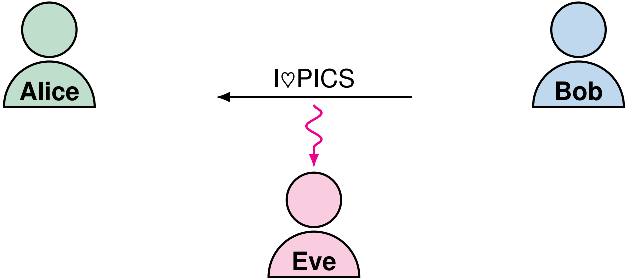
Code-based Cryptography

Decoding Problem

Given: $\boldsymbol{y} \in \mathbb{F}^n$ and $\boldsymbol{G} \in \mathbb{F}^{k \times n}$
Find: $\boldsymbol{m} \in \mathbb{F}^k$ s.t. $\boldsymbol{y} = \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e}$ with $|\boldsymbol{e}| \leq t$

Syndrome Decoding Problem

Given: $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}^{(n-k) \times n}$
Find: $\boldsymbol{e} \in \mathbb{F}^n$ s.t. $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$ and $|\boldsymbol{e}| \leq t$



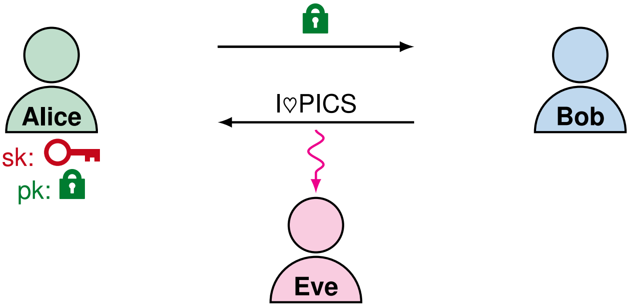
Code-based Cryptography

Decoding Problem

Given: $\boldsymbol{y} \in \mathbb{F}^n$ and $\boldsymbol{G} \in \mathbb{F}^{k \times n}$
Find: $\boldsymbol{m} \in \mathbb{F}^k$ s.t. $\boldsymbol{y} = \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e}$ with $|\boldsymbol{e}| \leq t$

Syndrome Decoding Problem

Given: $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}^{(n-k) \times n}$
Find: $\boldsymbol{e} \in \mathbb{F}^n$ s.t. $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$ and $|\boldsymbol{e}| \leq t$



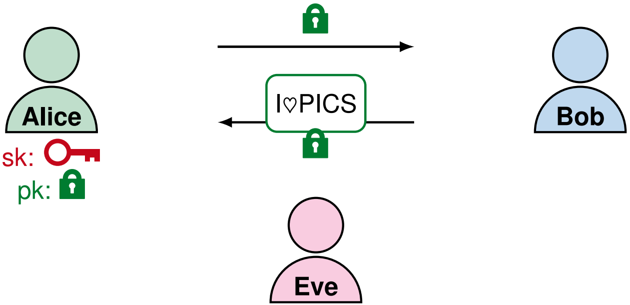
Code-based Cryptography

Decoding Problem

Given: $\boldsymbol{y} \in \mathbb{F}^n$ and $\boldsymbol{G} \in \mathbb{F}^{k \times n}$
Find: $\boldsymbol{m} \in \mathbb{F}^k$ s.t. $\boldsymbol{y} = \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e}$ with $|\boldsymbol{e}| \leq t$

Syndrome Decoding Problem

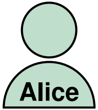
Given: $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}^{(n-k) \times n}$
Find: $\boldsymbol{e} \in \mathbb{F}^n$ s.t. $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$ and $|\boldsymbol{e}| \leq t$

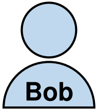


Public-Key Encryption à la McEliece

message $\boldsymbol{m} \in \mathbb{F}^k$

Public-Key Encryption à la McEliece





sk: $\mathcal{C}$, $\mathcal{C}$.DEC corrects t errors

message $\boldsymbol{m} \in \mathbb{F}^k$

Public-Key Encryption à la McEliece

Alice

Bob

sk: $\mathcal{C}$, $\mathcal{C}$.DEC corrects t errors

message $\boldsymbol{m} \in \mathbb{F}^k$

pk: Generic $\boldsymbol{G} \in \mathbb{F}^{k \times n}$ of $\mathcal{C}$

pk: $\boldsymbol{G}$ →

Public-Key Encryption à la McEliece

Alice

sk: $\mathcal{C}$, $\mathcal{C}$.DEC corrects t errors

pk: Generic $\boldsymbol{G} \in \mathbb{F}^{k \times n}$ of $\mathcal{C}$

pk: $\boldsymbol{G}$ →

← ct: $\boldsymbol{y}$

Bob

message $\boldsymbol{m} \in \mathbb{F}^k$

$\boldsymbol{e} \in \mathbb{F}^n$ with $|\boldsymbol{e}| \leq t$

$\boldsymbol{y} \leftarrow \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e} \in \mathbb{F}^n$

Public-Key Encryption à la McEliece

Alice

sk: $\mathcal{C}$, $\mathcal{C}.\textsc{Dec}$ corrects t errors

pk: Generic $\boldsymbol{G} \in \mathbb{F}^{k \times n}$ of $\mathcal{C}$

$\hat{\boldsymbol{m}} \leftarrow \mathcal{C}.\textsc{Dec}(\boldsymbol{y})$

Bob

message $\boldsymbol{m} \in \mathbb{F}^k$

$\boldsymbol{e} \in \mathbb{F}^n$ with $|\boldsymbol{e}| \leq t$

$\boldsymbol{y} \leftarrow \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e} \in \mathbb{F}^n$

Alice → Bob: pk: $\boldsymbol{G}$

Bob → Alice: ct: $\boldsymbol{y}$

Public-Key Encryption à la McEliece

Alice

sk: $\mathcal{C}$, $\mathcal{C}$.DEC corrects t errors

pk: Generic $\boldsymbol{G} \in \mathbb{F}^{k \times n}$ of $\mathcal{C}$

$\hat{\boldsymbol{m}} \leftarrow \mathcal{C}.\text{DEC}(\boldsymbol{y})$

pk: $\boldsymbol{G}$ →

← ct: $\boldsymbol{y}$

Bob

message $\boldsymbol{m} \in \mathbb{F}^k$

$\boldsymbol{e} \in \mathbb{F}^n$ with $|\boldsymbol{e}| \leq t$

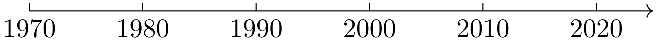
$\boldsymbol{y} \leftarrow \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e} \in \mathbb{F}^n$

Code Requirements

- pk $\boldsymbol{G}$ needs to seem random
- sk $\mathcal{C}$.DEC not revealed by $\boldsymbol{G}$

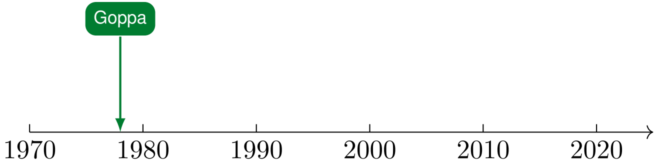
A Brief History of McEliece

Weger, V., et al. (2022). A survey on code-based cryptography. *Lect. Notes Math.*



A Brief History of McEliece

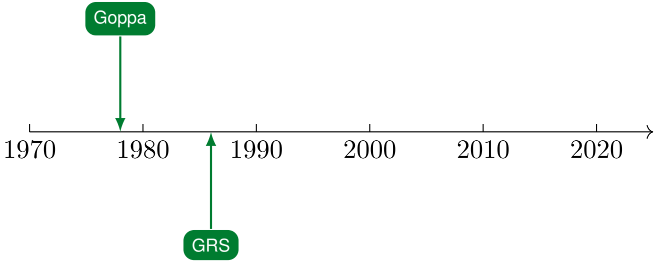
Weger, V., et al. (2022). A survey on code-based cryptography. *Lect. Notes Math.*



Goppa codes proposed in 1978

A Brief History of McEliece

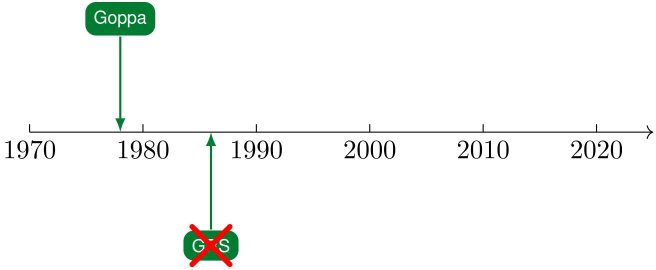
Weger, V., et al. (2022).A survey on code-based cryptography. *Lect. Notes Math.*



GRS codes proposed in 1986

A Brief History of McEliece

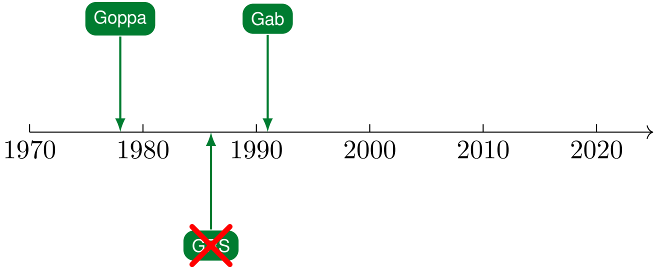
Weger, V., et al. (2022). A survey on code-based cryptography. *Lect. Notes Math.*



GRS codes proposed in 1986, broken in 1992

A Brief History of McEliece

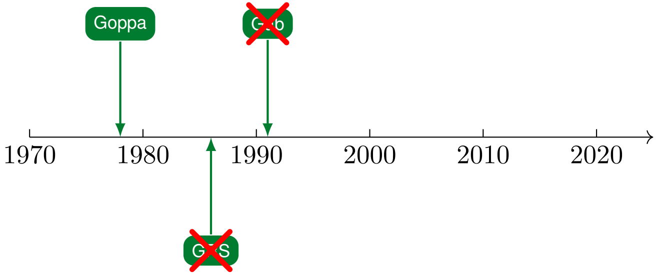
Weger, V., et al. (2022). A survey on code-based cryptography. *Lect. Notes Math.*



Gabidulin codes proposed in 1991

A Brief History of McEliece

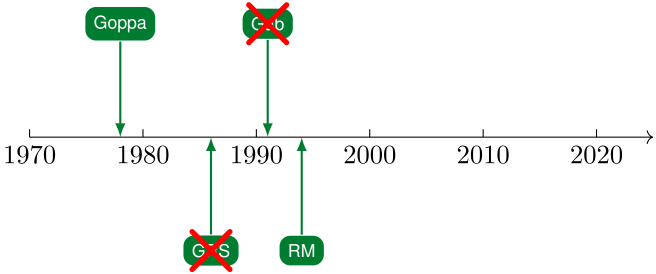
Weger, V., et al. (2022). A survey on code-based cryptography. *Lect. Notes Math.*



Gabidulin codes proposed in 1991, broken in 2008

A Brief History of McEliece

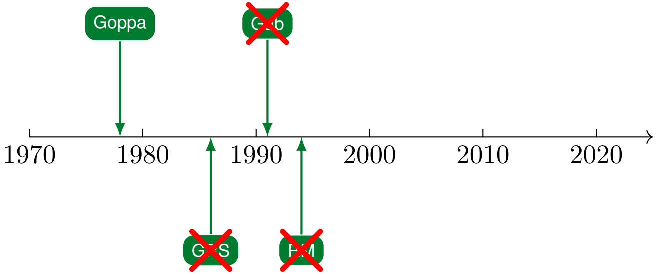
Weger, V., et al. (2022). A survey on code-based cryptography. *Lect. Notes Math.*



Reed-Muller codes proposed in 1994

A Brief History of McEliece

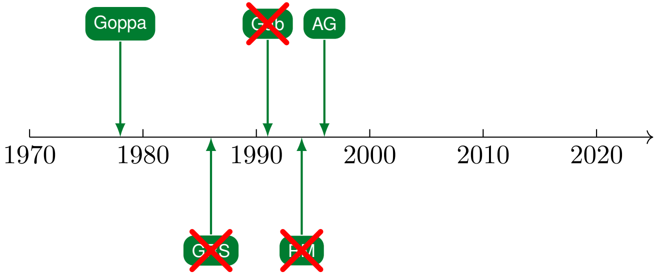
Weger, V., et al. (2022). A survey on code-based cryptography. *Lect. Notes Math.*



Reed-Muller codes proposed in 1994, broken in 2007

A Brief History of McEliece

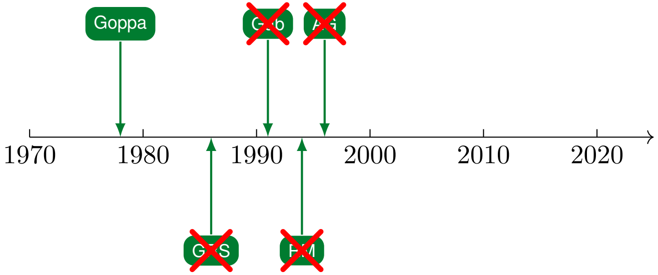
Weger, V., et al. (2022).A survey on code-based cryptography. *Lect. Notes Math.*



AG codes proposed in 1996

A Brief History of McEliece

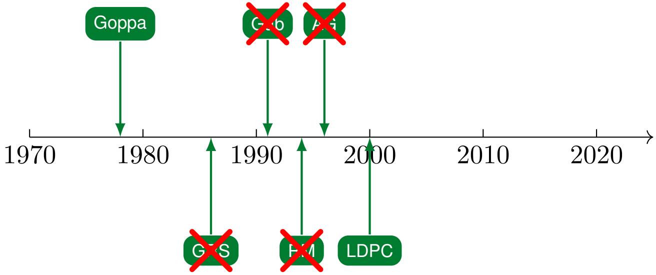
Weger, V., et al. (2022). A survey on code-based cryptography. *Lect. Notes Math.*



AG codes proposed in 1996, broken in 2014

A Brief History of McEliece

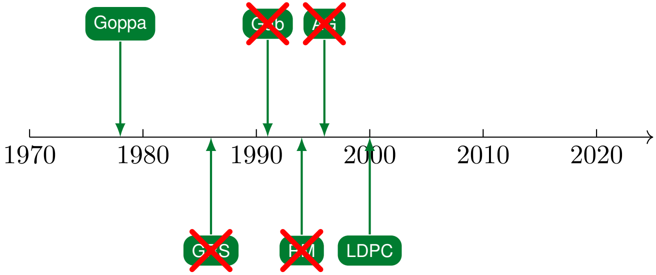
Weger, V., et al. (2022). A survey on code-based cryptography. *Lect. Notes Math.*



LDPC codes proposed in 2000

A Brief History of McEliece

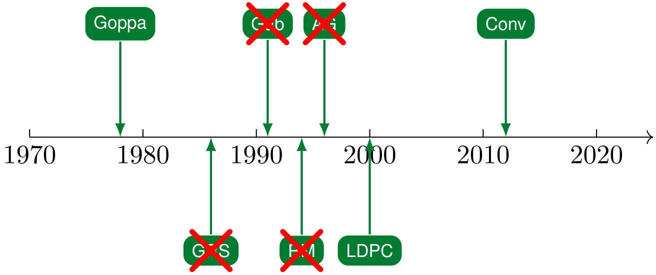
Weger, V., et al. (2022). A survey on code-based cryptography. *Lect. Notes Math.*



LDPC codes proposed in 2000, modifications required

A Brief History of McEliece

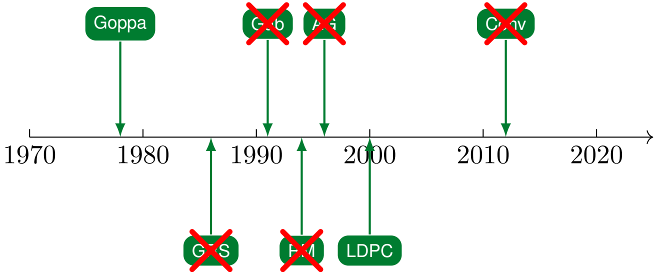
Weger, V., et al. (2022). A survey on code-based cryptography. *Lect. Notes Math.*



Convolutional codes proposed in 2012

A Brief History of McEliece

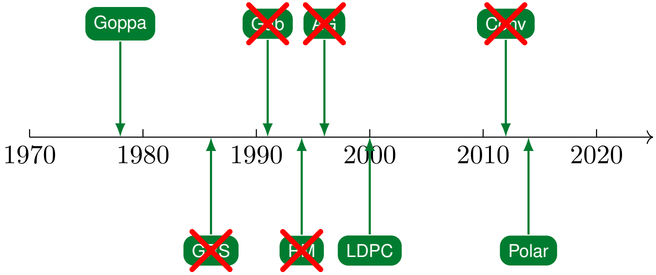
Weger, V., et al. (2022). A survey on code-based cryptography. *Lect. Notes Math.*



Convolutional codes proposed in 2012, broken in 2013

A Brief History of McEliece

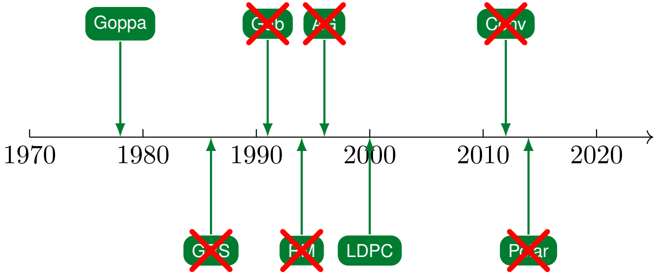
Weger, V., et al. (2022). A survey on code-based cryptography. *Lect. Notes Math.*



Polar codes proposed in 2014

A Brief History of McEliece

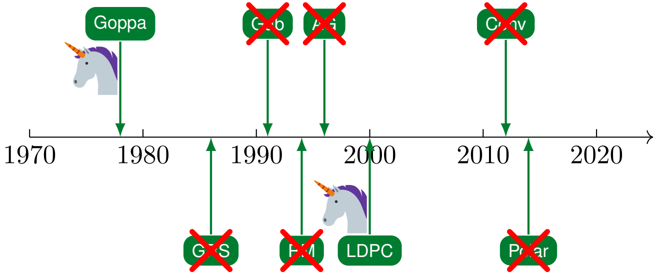
Weger, V., et al. (2022). A survey on code-based cryptography. *Lect. Notes Math.*



Polar codes proposed in 2014, broken in 2018

A Brief History of McEliece

- Weger, V., et al. (2022). A survey on code-based cryptography. *Lect. Notes Math.*

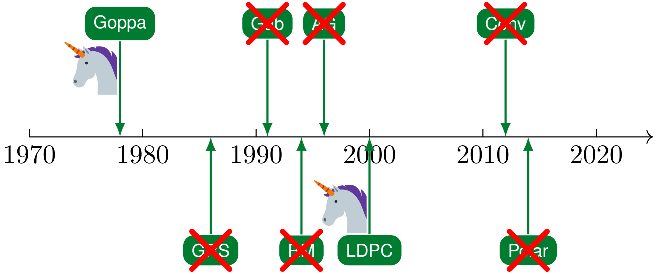


Codes in McEliece

Many have been proposed, almost all insecure

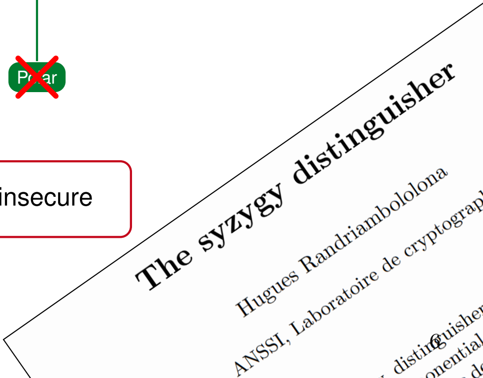
A Brief History of McEliece

Weger, V., et al. (2022). A survey on code-based cryptography. *Lect. Notes Math.*



Codes in McEliece

Many have been proposed, almost all insecure

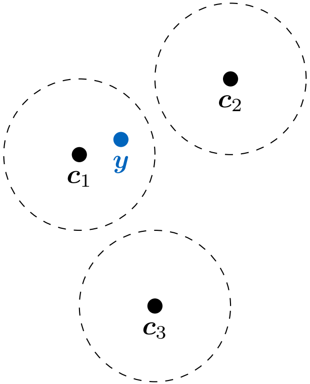

The syzygy distinguisher

Hugues Randriambololona

A Fresh Idea

McEliece's Idea

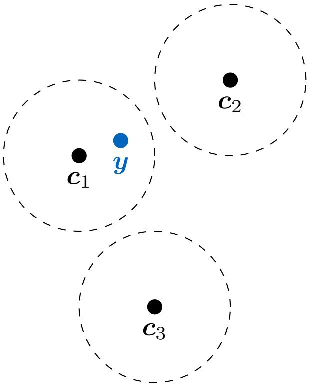
Efficient decoder but not leaked by $\boldsymbol{G}$



A Fresh Idea

McEliece's Idea

Efficient decoder but not leaked by $\boldsymbol{G}$



- Aguilar-Melchor, C., et al. (2017). Hamming quasi-cyclic (HQC). *NIST PQC Competition*
- Aguilar-Melchor, C., et al. (2018). Efficient encryption from random quasi-cyclic codes. *IEEE T-IT*

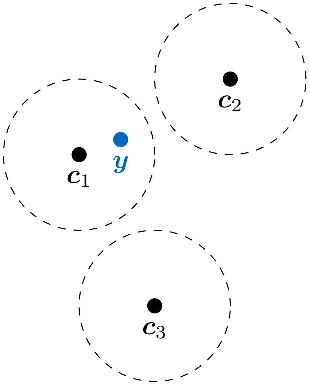
A Fresh Idea

McEliece's Idea

Efficient decoder but not leaked by G

HQC Idea

- Structured code (RS+RM)
- Public decoder
- Secret key reduces error weight



Aguilar-Melchor, C., et al. (2017). Hamming quasi-cyclic (HQC). *NIST PQC Competition*

Aguilar-Melchor, C., et al. (2018). Efficient encryption from random quasi-cyclic codes. *IEEE T-IT*

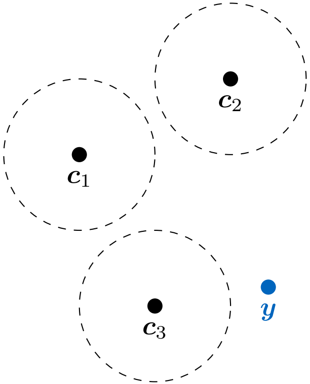
A Fresh Idea

McEliece's Idea

Efficient decoder but not leaked by $\boldsymbol{G}$

HQC Idea

- Structured code (RS+RM)
- Public decoder
- Secret key reduces error weight



Aguilar-Melchor, C., et al. (2017). Hamming quasi-cyclic (HQC). *NIST PQC Competition*

Aguilar-Melchor, C., et al. (2018). Efficient encryption from random quasi-cyclic codes. *IEEE T-IT*

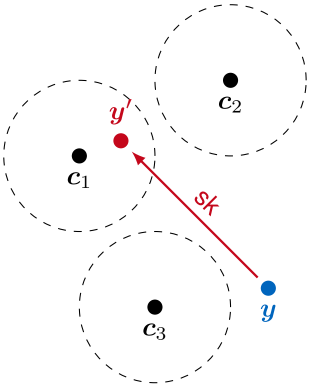
A Fresh Idea

McEliece's Idea

Efficient decoder but not leaked by G

HQC Idea

- Structured code (RS+RM)
- Public decoder
- Secret key reduces error weight



Aguilar-Melchor, C., et al. (2017).Hamming quasi-cyclic (HQC). *NIST PQC Competition*

Aguilar-Melchor, C., et al. (2018).Efficient encryption from random quasi-cyclic codes. *IEEE T-IT*

Put a Ring on It

$$\mathbb{F}^n \qquad\qquad \mathcal{R}_n \coloneqq \mathbb{F}[x]/(x^n - 1)$$

$$\boldsymbol{v} = (v_0, \ldots, v_{n-1}) \qquad\qquad v(x) = \sum_{i=0}^{n-1} v_i x^i$$

Put a Ring on It

$$\mathbb{F}^n$$

$$\boldsymbol{v} = (v_0, \ldots, v_{n-1})$$

$$\mathcal{R}_n \coloneqq \mathbb{F}[x]/(x^n - 1)$$

$$v(x) = \sum_{i=0}^{n-1} v_i x^i$$

Syndrome Decoding Problem

Given: $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}^{(n-k)\times n}$

Find: $\boldsymbol{e} \in \mathbb{F}^n$ s.t. $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$ and $|\boldsymbol{e}| \le t$

Quasi-Cyclic (QC) SDP

Given: $\boldsymbol{s} \in \mathcal{R}_n$ and $\boldsymbol{h} \in \mathcal{R}_n$

Find: $\boldsymbol{e}_1, \boldsymbol{e}_2$ s.t. $\boldsymbol{e}_1 + \boldsymbol{e}_2\boldsymbol{h} = \boldsymbol{s}$ and $|\boldsymbol{e}_1| + |\boldsymbol{e}_2| \le t$

Put a Ring on It

$$\mathbb{F}^n \qquad\qquad \mathcal{R}_n := \mathbb{F}[x]/(x^n - 1)$$

$$\boldsymbol{v} = (v_0, \ldots, v_{n-1}) \qquad\qquad v(x) = \sum_{i=0}^{n-1} v_i x^i$$

Syndrome Decoding Problem

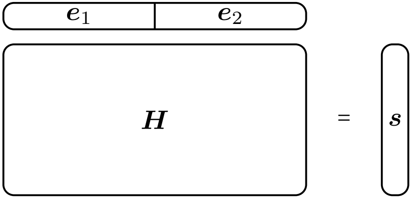
Given: $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}^{(n-k)\times n}$

Find: $\boldsymbol{e} \in \mathbb{F}^n$ s.t. $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$ and $|\boldsymbol{e}| \le t$

Quasi-Cyclic (QC) SDP

Given: $\boldsymbol{s} \in \mathcal{R}_n$ and $\boldsymbol{h} \in \mathcal{R}_n$

Find: $\boldsymbol{e}_1, \boldsymbol{e}_2$ s.t. $\boldsymbol{e}_1 + \boldsymbol{e}_2\boldsymbol{h} = \boldsymbol{s}$ and $|\boldsymbol{e}_1| + |\boldsymbol{e}_2| \le t$



Put a Ring on It

$\mathbb{F}^n$

$\boldsymbol{v} = (v_0, \dots, v_{n-1})$

$\mathcal{R}_n := \mathbb{F}[x]/(x^n - 1)$

$v(x) = \sum_{i=0}^{n-1} v_i x^i$

Syndrome Decoding Problem

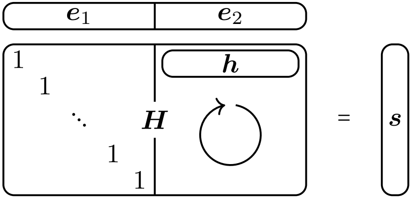
Given: $\boldsymbol{s} \in \mathbb{F}^{n-k}$ and $\boldsymbol{H} \in \mathbb{F}^{(n-k)\times n}$

Find: $\boldsymbol{e} \in \mathbb{F}^n$ s.t. $\boldsymbol{e}\boldsymbol{H}^\top = \boldsymbol{s}$ and $|\boldsymbol{e}| \leq t$

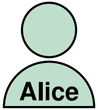
Quasi-Cyclic (QC) SDP

Given: $\boldsymbol{s} \in \mathcal{R}_n$ and $\boldsymbol{h} \in \mathcal{R}_n$

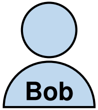
Find: $\boldsymbol{e}_1, \boldsymbol{e}_2$ s.t. $\boldsymbol{e}_1 + \boldsymbol{e}_2\boldsymbol{h} = \boldsymbol{s}$ and $|\boldsymbol{e}_1| + |\boldsymbol{e}_2| \leq t$



HQC in a Nutshell



$$\mathcal{R}_n = \mathbb{F}[x]/(x^n - 1)$$



message $\boldsymbol{m} \in \mathbb{F}^k$

HQC in a Nutshell

$\mathcal{R}_n = \mathbb{F}[x]/(x^n - 1)$

Alice

Bob

$\boldsymbol{h} \in \mathcal{R}_n$

message $\boldsymbol{m} \in \mathbb{F}^k$

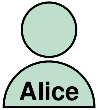
sk: $\boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathcal{R}_n$ of wt w_u

pk: $\boldsymbol{s} \leftarrow \boldsymbol{u}_1 + \boldsymbol{h}\boldsymbol{u}_2$

pk: $(\boldsymbol{h}, \boldsymbol{s})$ →

HQC in a Nutshell

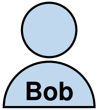
$$\mathcal{R}_n = \mathbb{F}[x]/(x^n - 1)$$



$\boldsymbol{h} \in \mathcal{R}_n$

sk: $\boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathcal{R}_n$ of wt w_u

pk: $\boldsymbol{s} \leftarrow \boldsymbol{u}_1 + \boldsymbol{h}\boldsymbol{u}_2$



message $\boldsymbol{m} \in \mathbb{F}^k$

pk: $(\boldsymbol{h}, \boldsymbol{s})$ →

$\boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3 \in \mathcal{R}_n$ of wt w_r

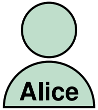
$\boldsymbol{y}_1 \leftarrow \boldsymbol{m}\boldsymbol{G} + \boldsymbol{s}\boldsymbol{r}_2 + \boldsymbol{r}_3$

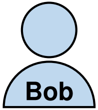
$\boldsymbol{y}_2 \leftarrow \boldsymbol{r}_1 + \boldsymbol{h}\boldsymbol{r}_2$

← ct: $(\boldsymbol{y}_1, \boldsymbol{y}_2)$

HQC in a Nutshell

$$\mathcal{R}_n = \mathbb{F}[x]/(x^n - 1)$$





Alice:

$\boldsymbol{h} \in \mathcal{R}_n$

sk: $\boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathcal{R}_n$ of wt w_u

pk: $\boldsymbol{s} \leftarrow \boldsymbol{u}_1 + \boldsymbol{h}\boldsymbol{u}_2$

Alice → Bob: pk: $(\boldsymbol{h}, \boldsymbol{s})$

Bob:

message $\boldsymbol{m} \in \mathbb{F}^k$

$\boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3 \in \mathcal{R}_n$ of wt w_r

$\boldsymbol{y}_1 \leftarrow \boldsymbol{m}\boldsymbol{G} + \boldsymbol{s}\boldsymbol{r}_2 + \boldsymbol{r}_3$

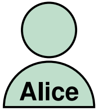
$\boldsymbol{y}_2 \leftarrow \boldsymbol{r}_1 + \boldsymbol{h}\boldsymbol{r}_2$

Bob → Alice: ct: $(\boldsymbol{y}_1, \boldsymbol{y}_2)$

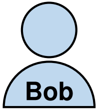
Alice:

$\hat{\boldsymbol{m}} \leftarrow \mathcal{C}.\textsc{Dec}(\boldsymbol{y}_1 - \boldsymbol{y}_2\boldsymbol{u}_2)$

HQC in a Nutshell



$\mathcal{R}_n = \mathbb{F}[x]/(x^n - 1)$



$\boldsymbol{h} \in \mathcal{R}_n$

message $\boldsymbol{m} \in \mathbb{F}^k$

sk: $\boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathcal{R}_n$ of wt w_u

pk: $\boldsymbol{s} \leftarrow \boldsymbol{u}_1 + \boldsymbol{h}\boldsymbol{u}_2$

pk: $(\boldsymbol{h}, \boldsymbol{s})$ →

$\boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3 \in \mathcal{R}_n$ of wt w_r

$\boldsymbol{y}_1 \leftarrow \boldsymbol{m}\boldsymbol{G} + \boldsymbol{s}\boldsymbol{r}_2 + \boldsymbol{r}_3$

$\hat{\boldsymbol{m}} \leftarrow \mathcal{C}.\textsc{Dec}(\boldsymbol{y}_1 - \boldsymbol{y}_2\boldsymbol{u}_2)$

← ct: $(\boldsymbol{y}_1, \boldsymbol{y}_2)$

$\boldsymbol{y}_2 \leftarrow \boldsymbol{r}_1 + \boldsymbol{h}\boldsymbol{r}_2$

$\mathcal{C}$ needs to decode $\boldsymbol{y}_1 - \boldsymbol{y}_2\boldsymbol{u}_2 = \boldsymbol{c} + \underbrace{\boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3}_{\text{error } \boldsymbol{e}}$

Decryption Failure Is Not an Option

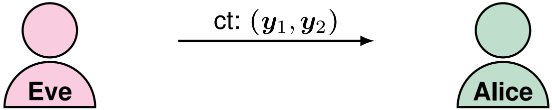
Security Issues

- IND-CCA security
- Reaction attacks

Decryption Failure Is Not an Option

Security Issues

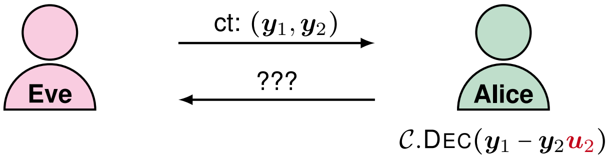
- IND-CCA security
- Reaction attacks



Decryption Failure Is Not an Option

Security Issues

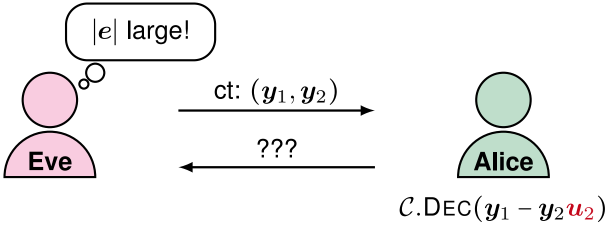
- IND-CCA security
- Reaction attacks



Decryption Failure Is Not an Option

Security Issues

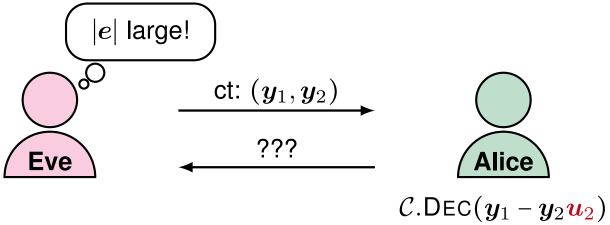
- IND-CCA security
- Reaction attacks



Decryption Failure Is Not an Option

Security Issues

- IND-CCA security
- Reaction attacks



Guo, Q., & Johansson, T. (2020). A new decryption failure attack against HQC.

→ DFR needs to be $\leq 2^{-128}$

A First Look at the Error

$P(|\boldsymbol{e}| = w)$ difficult for $\boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3$

$\rho = P(e_i = 1)$ simple

A First Look at the Error

$P(|\boldsymbol{e}| = w)$ difficult for $\boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3$

$\rho = P(e_i = 1)$ simple

BSC Approximation

Under the independence assumption,

$$P(|\boldsymbol{e}| = w) \approx \binom{n}{w}\rho^w(1-\rho)^{n-w}.$$

A First Look at the Error

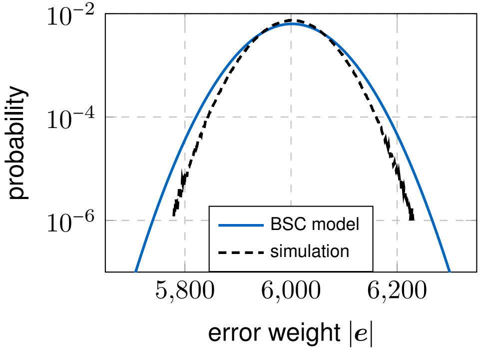
$P(|\boldsymbol{e}| = w)$ difficult for $\boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3$

$\rho = P(e_i = 1)$ simple

BSC Approximation

Under the independence assumption,

$$P(|\boldsymbol{e}| = w) \approx \binom{n}{w}\rho^w(1-\rho)^{n-w}.$$



A First Look at the Error

$P(|\boldsymbol{e}| = w)$ difficult for $\boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3$

$\rho = P(e_i = 1)$ simple

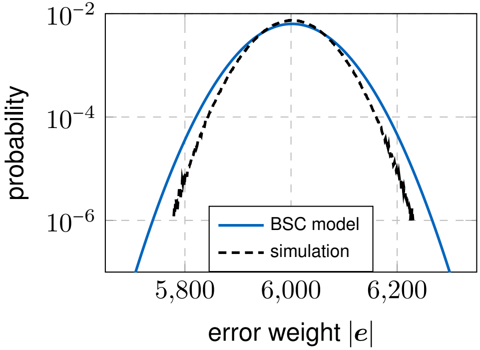
BSC Approximation

Under the independence assumption,

$$P(|\boldsymbol{e}| = w) \approx \binom{n}{w}\rho^w(1-\rho)^{n-w}.$$

Refined Approximation

Heuristic for weight after multiplication



A First Look at the Error

$P(|\boldsymbol{e}| = w)$ difficult for $\boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3$

$\rho = P(e_i = 1)$ simple

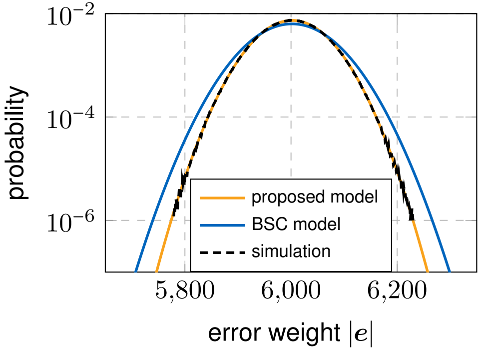
BSC Approximation

Under the independence assumption,

$$P(|\boldsymbol{e}| = w) \approx \binom{n}{w}\rho^w(1-\rho)^{n-w}.$$

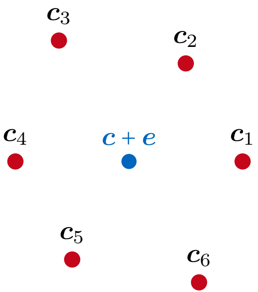
Refined Approximation

Heuristic for weight after multiplication



Beyond the BSC

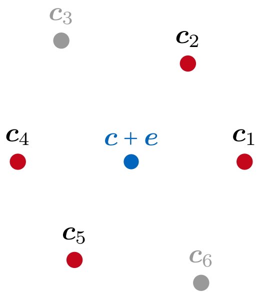
plausible for BSC



Beyond the BSC

plausible for BSC

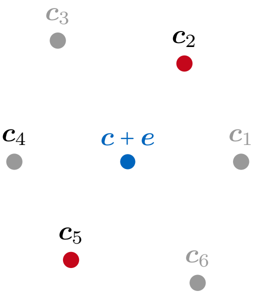
for proposed model



Beyond the BSC

plausible for BSC

for proposed model

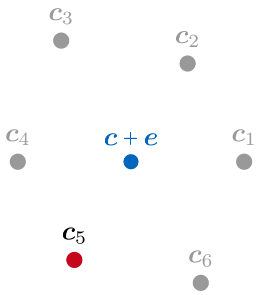


$$\boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3$$

Beyond the BSC

plausible for BSC

for proposed model



$\boldsymbol{e} = \boldsymbol{u}_1 \boldsymbol{r}_2 + \boldsymbol{u}_2 \boldsymbol{r}_1 + \boldsymbol{r}_3$

with known $\boldsymbol{u}_1, \boldsymbol{u}_2$

How Much Can Be Gained?

Loeliger, H.-A. (1994). On the basic averaging arguments for linear codes. *Comm. and Crypto.*

$$\mathcal{E} = \{\boldsymbol{e} \mid \boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3\}$$

$$\Delta\mathcal{E} = \{\boldsymbol{e} - \boldsymbol{e}' \mid \boldsymbol{e}, \boldsymbol{e}' \in \mathcal{E}\}$$

How Much Can Be Gained?

Loeliger, H.-A. (1994). On the basic averaging arguments for linear codes. *Comm. and Crypto.*

$$\mathcal{E} = \{\boldsymbol{e} \mid \boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3\}$$

$$\Delta\mathcal{E} = \{\boldsymbol{e} - \boldsymbol{e}' \mid \boldsymbol{e}, \boldsymbol{e}' \in \mathcal{E}\}$$

GV-like Bound

$$n \leq k + \log_q(|\Delta\mathcal{E}|)$$

How Much Can Be Gained?

Loeliger, H.-A. (1994). On the basic averaging arguments for linear codes. *Comm. and Crypto.*

$$\mathcal{E} = \{\boldsymbol{e} \mid \boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3\}$$

$$\Delta\mathcal{E} = \{\boldsymbol{e} - \boldsymbol{e}' \mid \boldsymbol{e}, \boldsymbol{e}' \in \mathcal{E}\}$$

GV-like Bound

$$n \leq k + \log_q(|\Delta\mathcal{E}|)$$

Here: $|\Delta\mathcal{E}| \leq w_r^3 \binom{n}{2w_r}^3 \binom{n}{w_u}^2$

How Much Can Be Gained?

Loeliger, H.-A. (1994). On the basic averaging arguments for linear codes. *Comm. and Crypto.*

$$\mathcal{E} = \{\boldsymbol{e} \mid \boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3\}$$

$$\Delta\mathcal{E} = \{\boldsymbol{e} - \boldsymbol{e}' \mid \boldsymbol{e}, \boldsymbol{e}' \in \mathcal{E}\}$$

GV-like Bound

$$n \leq k + \log_q(|\Delta\mathcal{E}|)$$

Here: $|\Delta\mathcal{E}| \leq w_r^3 \binom{n}{2w_r}^3 \binom{n}{w_u}^2$

	length	error model	decoder
HQC	17669	BSC	multistage

How Much Can Be Gained?

Loeliger, H.-A. (1994). On the basic averaging arguments for linear codes. *Comm. and Crypto.*

$$\mathcal{E} = \{\boldsymbol{e} \mid \boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3\}$$

$$\Delta\mathcal{E} = \{\boldsymbol{e} - \boldsymbol{e}' \mid \boldsymbol{e}, \boldsymbol{e}' \in \mathcal{E}\}$$

GV-like Bound

$$n \leq k + \log_q(|\Delta\mathcal{E}|)$$

Here: $|\Delta\mathcal{E}| \leq w_r^3 \binom{n}{2w_r}^3 \binom{n}{w_u}^2$

	length	error model	decoder
HQC	17669	BSC	multistage
SPB	≥ 13438	BSC	ML

How Much Can Be Gained?

Loeliger, H.-A. (1994). On the basic averaging arguments for linear codes. *Comm. and Crypto.*

$$\mathcal{E} = \{\boldsymbol{e} \mid \boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3\}$$

$$\Delta\mathcal{E} = \{\boldsymbol{e} - \boldsymbol{e}' \mid \boldsymbol{e}, \boldsymbol{e}' \in \mathcal{E}\}$$

GV-like Bound

$$n \leq k + \log_q(|\Delta\mathcal{E}|)$$

Here: $|\Delta\mathcal{E}| \leq w_r^3 \binom{n}{2w_r}^3 \binom{n}{w_u}^2$

	length	error model	decoder
HQC	17669	BSC	multistage
SPB	≥ 13438	BSC	ML
GVB	≤ 3800	structured	???

How Much Can Be Gained?

Loeliger, H.-A. (1994).On the basic averaging arguments for linear codes. *Comm. and Crypto.*

$$\mathcal{E} = \{\boldsymbol{e} \mid \boldsymbol{e} = \boldsymbol{u}_1\boldsymbol{r}_2 + \boldsymbol{u}_2\boldsymbol{r}_1 + \boldsymbol{r}_3\}$$

$$\Delta\mathcal{E} = \{\boldsymbol{e} - \boldsymbol{e}' \mid \boldsymbol{e}, \boldsymbol{e}' \in \mathcal{E}\}$$

GV-like Bound

$$n \leq k + \log_q(|\Delta\mathcal{E}|)$$

Here: $|\Delta\mathcal{E}| \leq w_r^3 \binom{n}{2w_r}^3 \binom{n}{w_u}^2$

	length	error model	decoder
HQC	17669	BSC	multistage
SPB	≥ 13438	BSC	ML
GVB	≤ 3800	structured	???

- ☺ No DFR, no heuristics
- ☺ better parameters
- (!) explicit code needed
- (!) efficient decoder needed

Conclusion

Non-random codes in code-based cryptography:

- ☺ McEliece has strong code requirements
- ☺ HQC allows public decoder
- ☺ Error structure of HQC

my website

Conclusion

Non-random codes in code-based cryptography:

- ☺ McEliece has strong code requirements
- ☺ HQC allows public decoder
- ☺ Error structure of HQC

Research questions:

- ? Are Goppa codes secure?
- ? Efficient codes for HQC?
- ? HQC in Hamming and rank metric – sum-rank HQC?
- ? More lattice-based inspiration?

my website

Conclusion

Non-random codes in code-based cryptography:

- ☺ McEliece has strong code requirements
- ☺ HQC allows public decoder
- ☺ Error structure of HQC

Research questions:

- ? Are Goppa codes secure?
- ? Efficient codes for HQC?
- ? HQC in Hamming and rank metric – sum-rank HQC?
- ? More lattice-based inspiration?

my website

Thank you!

Questions?