QC-MDPC:
A Timing Attack and a CCA2 KEM

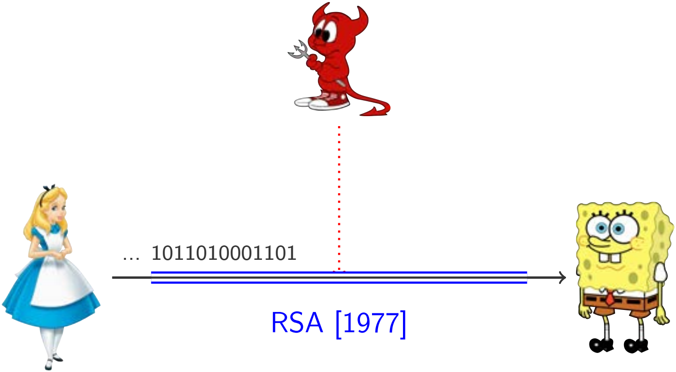
PQCrypto – April 9, 2018

Edward Eaton[1], Matthieu Lequesne[2,3],
Alex Parent[1] and Nicolas Sendrier[3]

1 - ISARA Corporation, Waterloo, Canada
2 - Sorbonne Université Paris, France
3 - Inria Paris, France – team Secret

Context

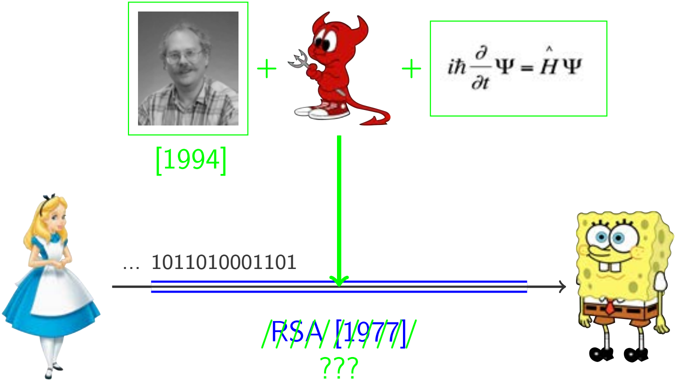
Public Key Cryptography



... 1011010001101

RSA [1977]

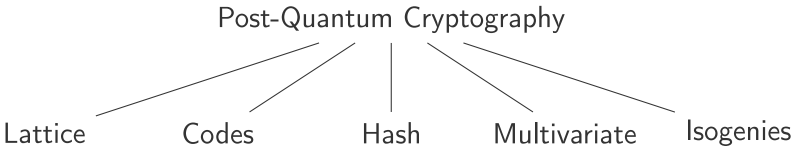
Public Key Cryptography



$$i\hbar\frac{\partial}{\partial t}\Psi = \hat{H}\Psi$$

NIST

Post-Quantum Cryptography


Post-Quantum Cryptography

Lattice

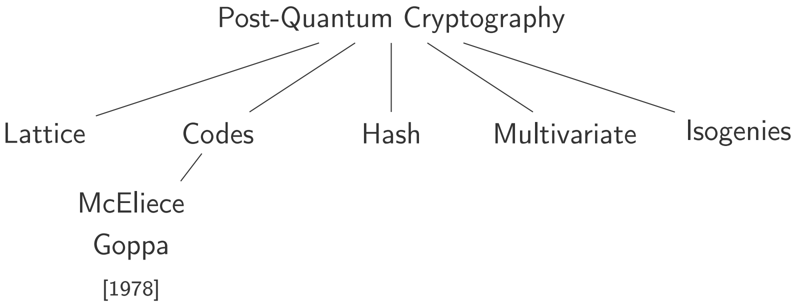
Codes

Hash

Multivariate

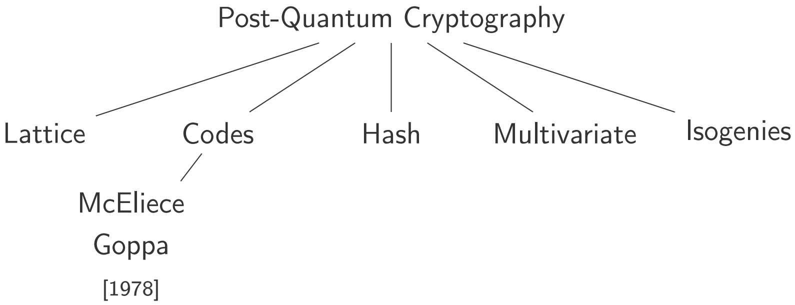
Isogenies

Post-Quantum Cryptography



Code-based cryptosystem (à la McEliece)

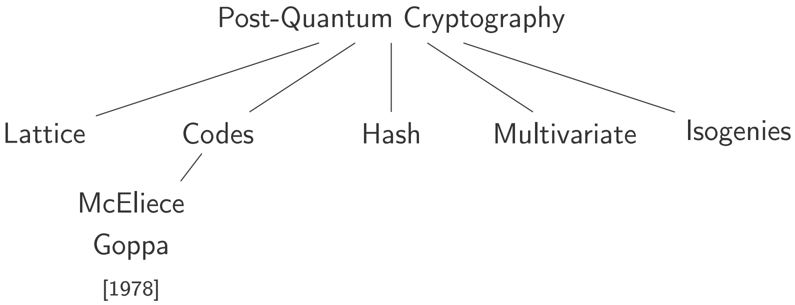
Post-Quantum Cryptography



Code-based cryptosystem (à la McEliece)

Goal: achieve relatively short keys

Post-Quantum Cryptography

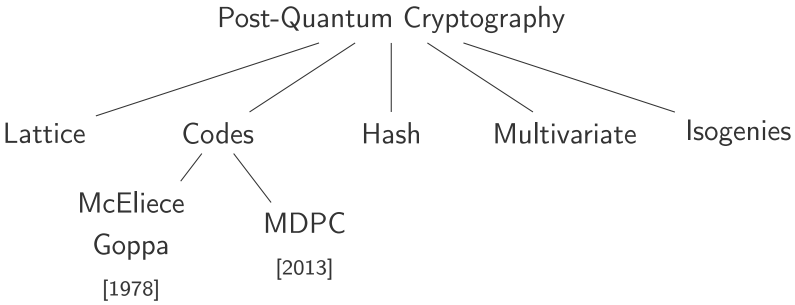


Code-based cryptosystem (à la McEliece)

Goal: achieve relatively short keys

Idea: use (quasi)-cyclic structure.

Post-Quantum Cryptography

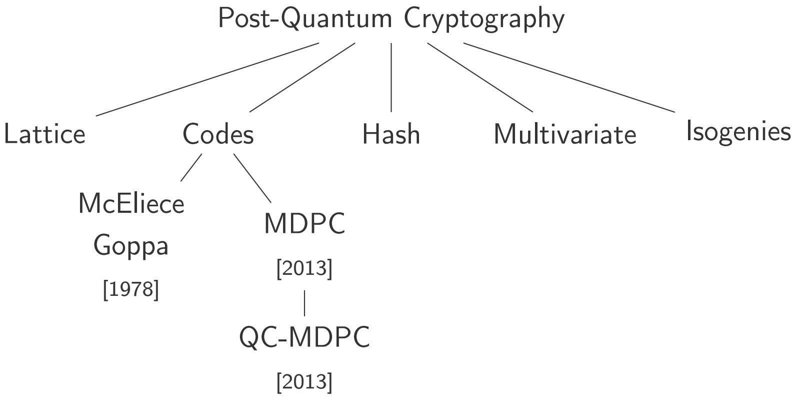


Code-based cryptosystem (à la McEliece)

Goal: achieve relatively short keys

Idea: use (quasi)-cyclic structure.

Post-Quantum Cryptography



Code-based cryptosystem (à la McEliece)

Goal: achieve relatively short keys

Idea: use (quasi)-cyclic structure.

QC-MDPC McEliece

QC-MDPC scheme

$k, d, t \in \mathbb{N}$ parameters

(k prime, d odd, $2d \sim t \sim \sqrt{2k}$)

$$\mathcal{R} = \mathbb{F}_2[X]/(X^k - 1)$$

QC-MDPC scheme

$k, d, t \in \mathbb{N}$ parameters

(k prime, d odd, $2d \sim t \sim \sqrt{2k}$)

$$\mathcal{R} = \mathbb{F}_2[X]/(X^k - 1)$$

$$\overbrace{(h_0, h_1)}^{\text{private key}} \leftarrow \mathcal{R}$$

$$|h_0| = |h_1| = d$$

QC-MDPC scheme

$$k, d, t \in \mathbb{N} \text{ parameters}$$

$(k$ prime, d odd, $2d \sim t \sim \sqrt{2k})$

$$\mathcal{R} = \mathbb{F}_2[X]/(X^k - 1)$$

$\overbrace{(h_0, h_1)}^{\text{private key}} \leftarrow \mathcal{R}$

$|h_0| = |h_1| = d$

$$\xrightarrow{\overbrace{q = h_1 \cdot h_0^{-1}}^{\text{public key}}}$$

QC-MDPC scheme

$$k, d, t \in \mathbb{N} \text{ parameters}$$

$(k \text{ prime}, d \text{ odd}, 2d \sim t \sim \sqrt{2k})$

$$\mathcal{R} = \mathbb{F}_2[X]/(X^k - 1)$$

$\overbrace{(h_0, h_1)}^{\text{private key}} \leftarrow \mathcal{R}$

$|h_0| = |h_1| = d$

$$\xrightarrow{\overbrace{q = h_1 \cdot h_0^{-1}}^{\text{public key}}}$$

$(e_0, e_1) \leftarrow \mathcal{R}$

$|e_0| + |e_1| = t$

QC-MDPC scheme

$k, d, t \in \mathbb{N}$ parameters

(k prime, d odd, $2d \sim t \sim \sqrt{2k}$)

$$\mathcal{R} = \mathbb{F}_2[X]/(X^k - 1)$$

$\overbrace{(h_0, h_1)}^{\text{private key}} \leftarrow \mathcal{R}$

$|h_0| = |h_1| = d$

$$\xrightarrow{\overbrace{q = h_1 \cdot h_0^{-1}}^{\text{public key}}}$$

$(e_0, e_1) \leftarrow \mathcal{R}$

$|e_0| + |e_1| = t$

$$\xleftarrow{c = e_0 + e_1 \cdot q}$$

QC-MDPC scheme

$k, d, t \in \mathbb{N}$ parameters

(k prime, d odd, $2d \sim t \sim \sqrt{2k}$)

$$\mathcal{R} = \mathbb{F}_2[X]/(X^k - 1)$$

$\overbrace{(h_0, h_1)}^{\text{private key}} \leftarrow \mathcal{R}$

$|h_0| = |h_1| = d$

$$\xrightarrow{\overbrace{q = h_1 \cdot h_0^{-1}}^{\text{public key}}}$$

$(e_0, e_1) \leftarrow \mathcal{R}$

$|e_0| + |e_1| = t$

$$\xleftarrow{c = e_0 + e_1 \cdot q}$$

$c \cdot h_0 = e_0 h_0 + e_1 h_1$

$(e_0, e_1) = \text{Decode}(h_0, h_1, e_0 h_0 + e_1 h_1)$

QC-MDPC scheme

$k, d, t \in \mathbb{N}$ parameters

(k prime, d odd, $2d \sim t \sim \sqrt{2k}$)

$$\mathcal{R} = \mathbb{F}_2[X]/(X^k - 1)$$

$\overbrace{(h_0, h_1)}^{\text{private key}} \leftarrow \mathcal{R}$

$|h_0| = |h_1| = d$

$$\xrightarrow{\overbrace{q = h_1 \cdot h_0^{-1}}^{\text{public key}}}$$

$(e_0, e_1) \leftarrow \mathcal{R}$

$|e_0| + |e_1| = t$

$$\xleftarrow{c = e_0 + e_1 \cdot q}$$

$c \cdot h_0 = e_0 h_0 + e_1 h_1$

$(e_0, e_1) = \text{Decode}(h_0, h_1, e_0 h_0 + e_1 h_1)$

Shared secret: (e_0, e_1).

QC-MDPC scheme

$k, d, t \in \mathbb{N}$ parameters

(k prime, d odd, $2d \sim t \sim \sqrt{2k}$)

$$\mathcal{R} = \mathbb{F}_2[X]/(X^k - 1)$$

$\underbrace{(h_0, h_1)}^{\text{private key}} \leftarrow \mathcal{R}$

$|h_0| = |h_1| = d$

$$\xrightarrow{\overbrace{q = h_1 \cdot h_0^{-1}}^{\text{public key}}}$$

$(e_0, e_1) \leftarrow \mathcal{R}$

$|e_0| + |e_1| = t$

$$\xleftarrow{c = e_0 + e_1 \cdot q}$$

$c \cdot h_0 = e_0 h_0 + e_1 h_1$

$(e_0, e_1) = \underline{\underline{\text{Decode}}}(h_0, h_1, e_0 h_0 + e_1 h_1)$

Shared secret: (e_0, e_1).

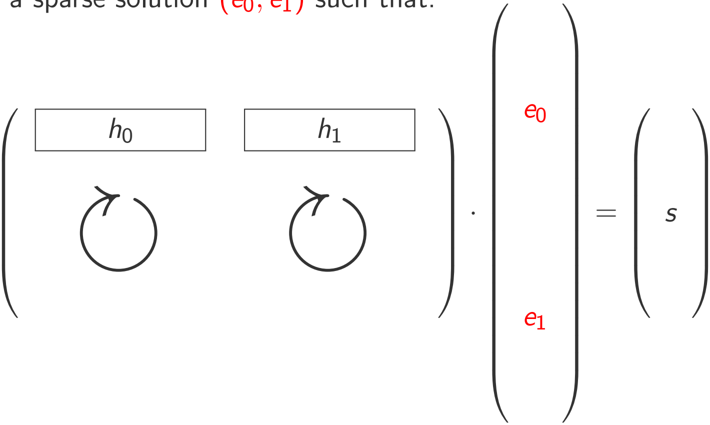
QC-MDPC McEliece: Bit Flip Decoding

$$(e_0, e_1) = \text{Decode}(h_0, h_1, \underbrace{e_0 h_0 + e_1 h_1}_{s})$$

QC-MDPC McEliece: Bit Flip Decoding

$$(e_0, e_1) = \text{Decode}(h_0, h_1, \underbrace{e_0 h_0 + e_1 h_1}_{s})$$

Find a sparse solution (e_0, e_1) such that:



QC-MDPC McEliece: Bit Flip Syndrome Decoding

```
Input: $H$ the parity-check matrix of the code $\mathcal{C}$,
       $s$ the syndrome
Output: An error $e$ of small weight such that $He^\intercal = s$
  $e \leftarrow 0$; $s' \leftarrow s - He^\intercal$
  while $s' \neq 0$ do
      for $j = 1, \ldots, n$ do
          if $\sigma_j = \langle s', h_j \rangle \geq \mathrm{threshold}$ then
              Flip($e_j$)
      $s' \leftarrow s - He^\intercal$
  return $e$
```

QC-MDPC McEliece: Bit Flip Syndrome Decoding

```
Input: $H$ the parity-check matrix of the code $\mathcal{C}$,
       $s$ the syndrome
Output: An error $e$ of small weight such that $He^{\intercal} = s$
  $e \leftarrow 0$; $s' \leftarrow s - He^{\intercal}$
  while $s' \neq 0$ do
      for $j = 1, \ldots, n$ do
          if $\sigma_j = \langle s', h_j \rangle \geq \mathrm{threshold}$ then
              Flip($e_j$)
      $s' \leftarrow s - He^{\intercal}$
  return $e$
```

- While loop: variable number of iterations.

QC-MDPC McEliece: Bit Flip Syndrome Decoding

```
Input: $H$ the parity-check matrix of the code $\mathcal{C}$,
       $s$ the syndrome
Output: An error $e$ of small weight such that $He^\intercal = s$
  $e \leftarrow 0$; $s' \leftarrow s - He^\intercal$
  while $s' \neq 0$ do
      for $j = 1, \ldots, n$ do
          if $\sigma_j = \langle s', h_j \rangle \geq \mathrm{threshold}$ then
              Flip($e_j$)
      $s' \leftarrow s - He^\intercal$
  return $e$
```

- While loop: variable number of iterations.
- Decoding algorithm fails with a small probability (DFR).

QC-MDPC McEliece: Bit Flip Syndrome Decoding

```
Input: $H$ the parity-check matrix of the code $\mathcal{C}$,
       $s$ the syndrome
Output: An error $e$ of small weight such that $He^\intercal = s$
  $e \leftarrow 0$; $s' \leftarrow s - He^\intercal$
  while $s' \neq 0$ do
      for $j = 1, \ldots, n$ do
          if $\sigma_j = \langle s', h_j \rangle \geq \text{threshold}$ then
              Flip($e_j$)
      $s' \leftarrow s - He^\intercal$
  return $e$
```

- While loop: variable number of iterations.
- Decoding algorithm fails with a small probability (DFR).
- Thresholds?

The GJS Attack

The GJS Attack

[GJS] Guo, Johansson, Stankovski, Asiacrypt 2016

Observation [GJS]

When two non-zero bits appear at a distance δ both in the secret key and in the error vector, a decoding failure is *less* likely to occur.

Example: $\delta = 1$

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

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

Example: $\delta = 1$

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

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

Example: $\delta = 1$

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

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

The GJS Attack

[GJS] Guo, Johansson, Stankovski, Asiacrypt 2016

Observation [GJS]

When two non-zero bits appear at a distance δ both in the secret key and in the error vector, a decoding failure is *less* likely to occur.

$\Rightarrow$ By observing the DFR for different error paterns we can recover information on the key.

The Distance Spectrum [GJS]

Definition (Distance Spectrum)

$$h = 1001000001$$

The Distance Spectrum [GJS]

Definition (Distance Spectrum)

$$h = \underset{\uparrow}{1}00100000\underset{\uparrow}{1}$$

$$\Delta(h) \supseteq \{1\}$$

The Distance Spectrum [GJS]

Definition (Distance Spectrum)

$$h = \underset{\uparrow}{1}00\underset{\uparrow}{1}000001$$

$$\Delta(h) \supseteq \{1, 3\}$$

The Distance Spectrum [GJS]

Definition (Distance Spectrum)

$$h = 1001000001$$

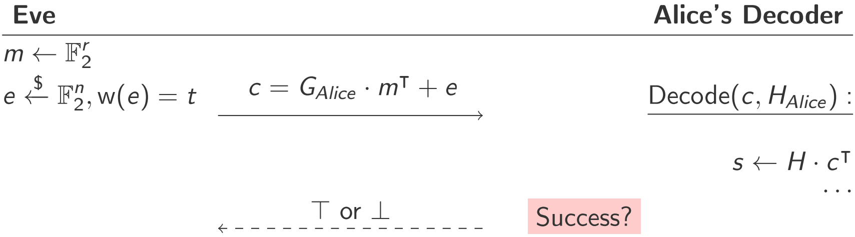
$$\Delta(h) = \{1, 3, 4\}$$

Generic Attack Pattern

Attack

1. Measure $\Delta(h)$;
2. Reconstruct h from $\Delta(h)$.

GJS Attack



Eve

Alice's Decoder

$m \leftarrow \mathbb{F}_2^r$

$e \xleftarrow{\$} \mathbb{F}_2^n, \mathrm{w}(e) = t$

$\xrightarrow{c = G_{Alice} \cdot m^\intercal + e}$

$\underline{\mathrm{Decode}(c, H_{Alice}):}$

$s \leftarrow H \cdot c^\intercal$

$\cdots$

$\xleftarrow{\top \text{ or } \bot}$

Success?

GJS Attack

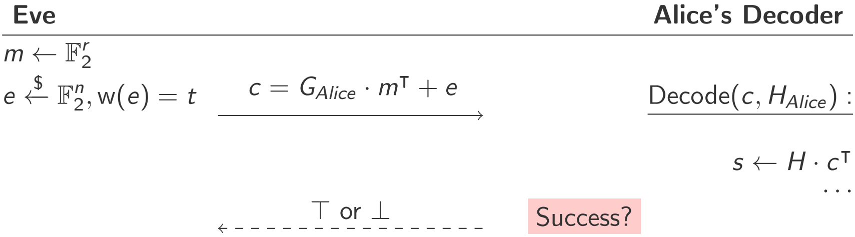
Main observation

For a fixed distance δ, if $\delta \in \Delta(e)$:

$$\mathbb{P}(\text{Decoding fails} \,|\, \delta \in \Delta(h)) < \mathbb{P}(\text{Decoding fails} \,|\, \delta \notin \Delta(h)).$$

Explaining the Leak

GJS Attack



Eve

Alice's Decoder

$m \leftarrow \mathbb{F}_2^r$

$e \overset{\$}{\leftarrow} \mathbb{F}_2^n, \mathrm{w}(e) = t$

$\xrightarrow{c = G_{Alice} \cdot m^\intercal + e}$

$\underline{\mathrm{Decode}(c, H_{Alice}) :}$

$s \leftarrow H \cdot c^\intercal$

$\cdots$

$\xleftarrow{\top \text{ or } \bot}$

Success?

Syndrome

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

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

Syndrome

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

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

Syndrome

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

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

Syndrome

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

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

Syndrome

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

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

Syndrome

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

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

Syndrome

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

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

Syndrome

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

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

Syndrome

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

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

Syndrome

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

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

Syndrome

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

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

Average syndrome weight?

Without any information

Average syndrome weight (MDPC)

$$|s| = k \cdot f(k, d, t, 1),$$

where:

$$f(k, d, t, b) := \mathbb{P}(\langle h, e \rangle = b) = \sum_{i=0,\ i \equiv b[2]} \frac{\binom{d}{i}\binom{r-d}{t-i}}{\binom{k}{t}}.$$

Example: $\delta = 1$

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

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

Consecutive bits set to 1

Extra assumption: h has ℓ times two consecutive bits set to 1.

shift(h) =	1	1	u, $\lvert u \rvert$ = d-2	ℓ times
shift(h) =	1	0	u, $\lvert u \rvert$ = d-1	$d - \ell$ times
shift(h) =	0	1	u, $\lvert u \rvert$ = d-1	$d - \ell$ times
shift(h) =	0	0	u, $\lvert u \rvert$ = d	$k - 2d + \ell$ times.

Consecutive bits set to 1

Extra assumption: h has ℓ times two consecutive bits set to 1.

$\mathrm{shift}(h) = \boxed{1}\boxed{1}\boxed{\text{u, } |u| = \text{d-2}}$ $\quad \ell$ times

$\mathrm{shift}(h) = \boxed{1}\boxed{0}\boxed{\text{u, } |u| = \text{d-1}}$ $\quad d - \ell$ times

$\mathrm{shift}(h) = \boxed{0}\boxed{1}\boxed{\text{u, } |u| = \text{d-1}}$ $\quad d - \ell$ times

$\mathrm{shift}(h) = \boxed{0}\boxed{0}\boxed{\text{u, } |u| = \text{d}}$ $\quad k - 2d + \ell$ times.

$e = \boxed{1}\boxed{1}\boxed{\text{u, } |u| = \text{t-2}}$

Average syndrome weight (QC-MDPC, approximation)

$$
\begin{array}{rcll}
|s| & = & \ell & f(k-2, d-2, t-2, 1) \\
 & + & 2(d-\ell) & f(k-2, d-1, t-2, 0) \\
 & + & (k-2d+\ell) & f(k-2, d, t-2, 1).
\end{array}
$$

Side Channel Attack on Syndrome Weight

Main observation

For a fixed distance δ, if $\delta \in \Delta(e)$:

$$\mathbb{E}(\sigma \mid \delta \in \Delta(h)) < \mathbb{E}(\sigma \mid \delta \notin \Delta(h)).$$

Example: $\delta = 1$

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

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

Example: $\delta = 1$

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

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

Example: $\delta = 1$

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad s = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

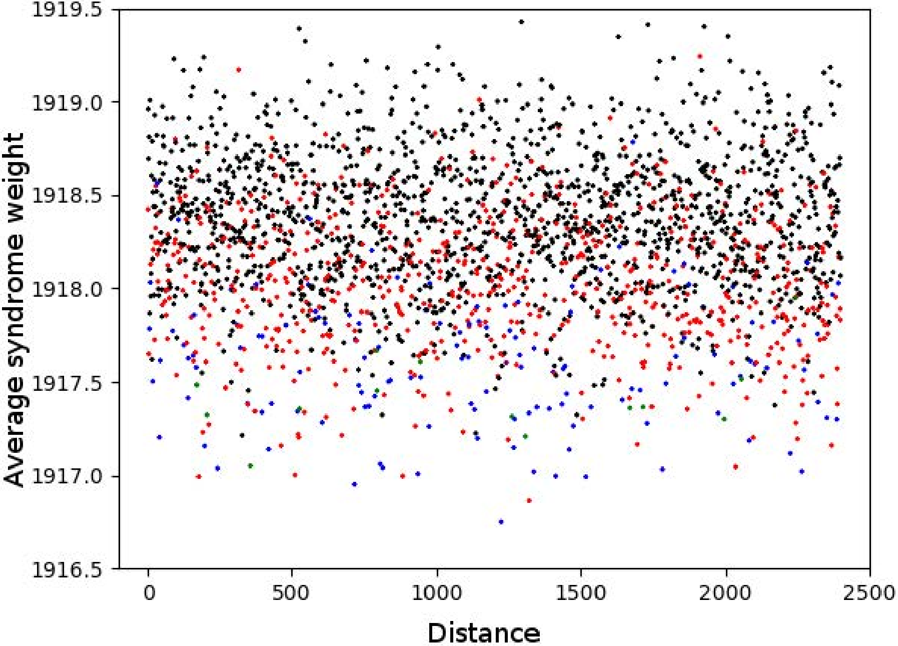
$$e = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

New Attacks

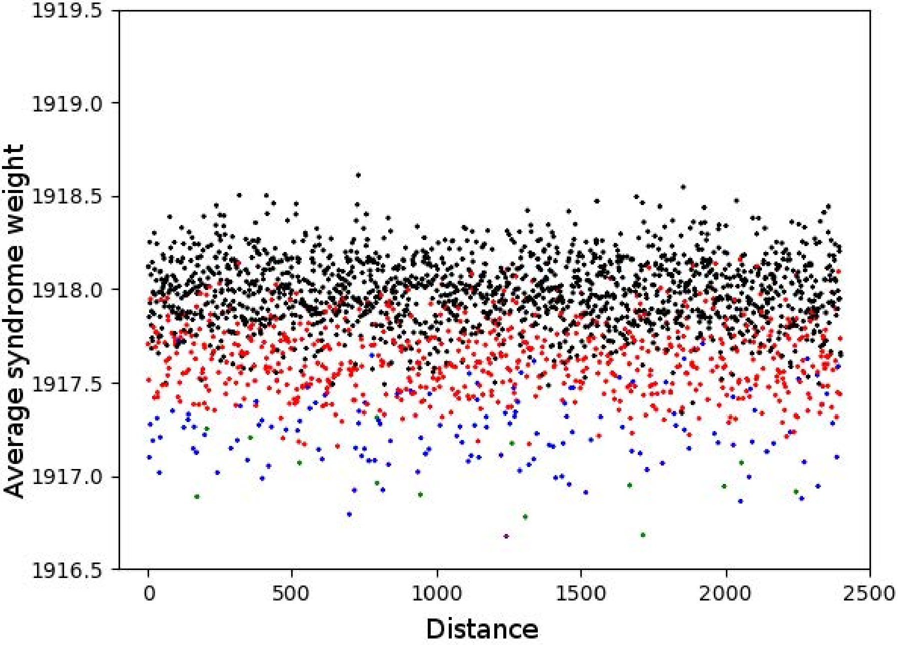
Side Channel Attack on Syndrome Weight

Eve		**Alice's Decoder**
$m \leftarrow \mathbb{F}_2^r$		
$e \xleftarrow{\$} \mathbb{F}_2^n, \mathrm{w}(e) = t$	$\xrightarrow{c = G_{Alice} \cdot m^\intercal + e}$	$\underline{\mathrm{Decode}(c, H_{Alice}):}$
		$s \leftarrow H \cdot c^\intercal$ $\sigma \leftarrow \mathrm{w}(s)$ $\ldots$
	$\xleftarrow{\sigma = \mathrm{w}(s)}$	

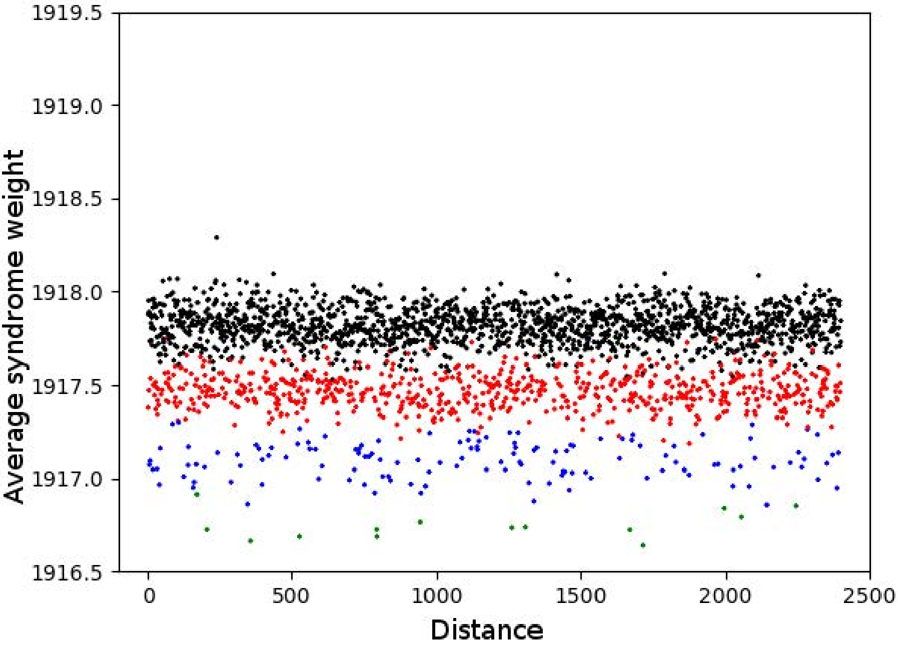
80 bits security, 2^{14} samples



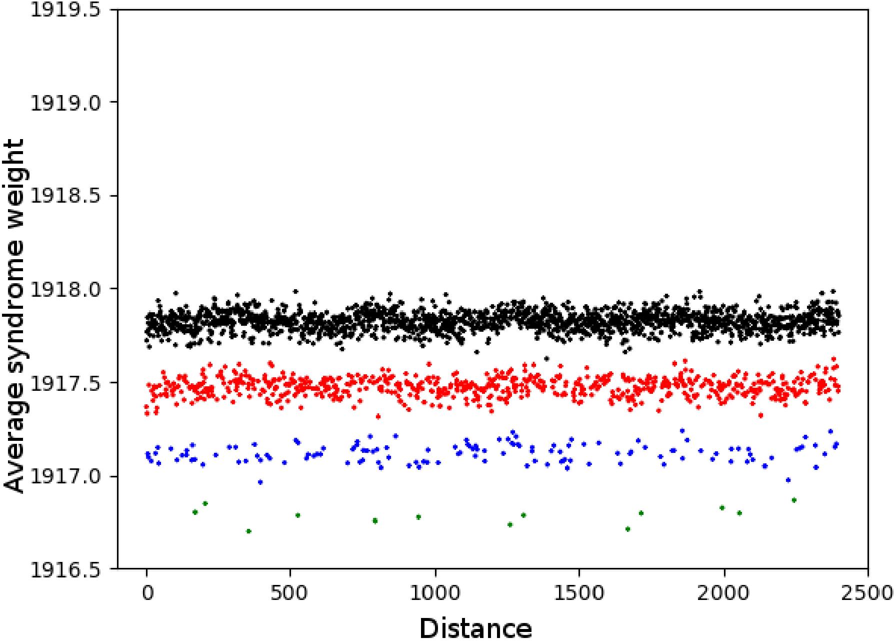
80 bits security, 2^{16} samples



80 bits security, 2^{18} samples



80 bits security, 2^{20} samples



Side Channel Attack on Syndrome Weight

Required number of samples to fully distinguish the specturm:

Security bits	80	128	256
Number of samples	2^{20}	2^{23}	2^{25}

Side Channel Attack on Syndrome Weight

Required number of samples to fully distinguish the specturm:

Security bits	80	128	256
Number of samples	2^{20}	2^{23}	2^{25}

- Works regardless of the DFR.

Side Channel Attack on Syndrome Weight

Required number of samples to fully distinguish the specturm:

Security bits	80	128	256
Number of samples	2^{20}	2^{23}	2^{25}

- Works regardless of the DFR.
- Any value correlated to the syndrome weight will leak information.

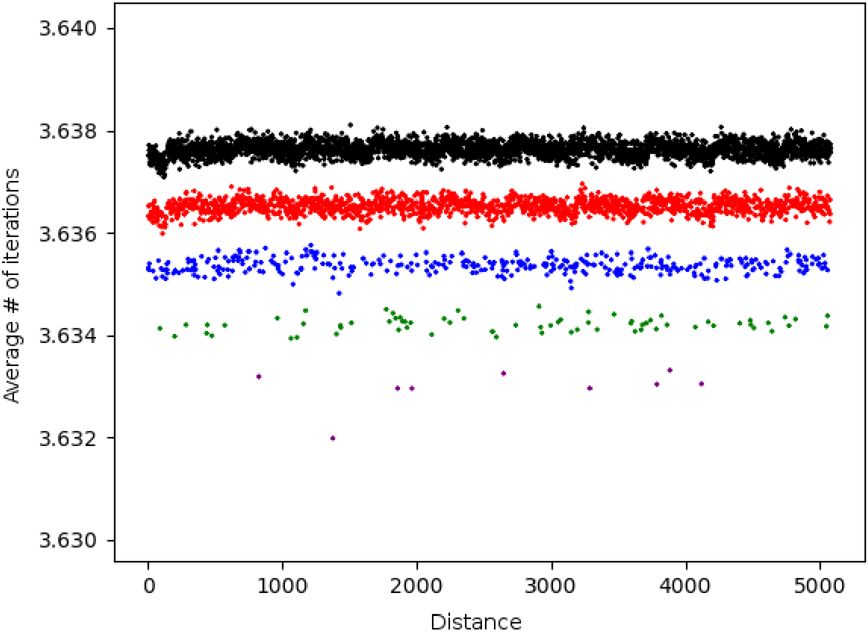
QC-MDPC McEliece: Bit Flip Syndrome Decoding

```
Input: $H$ the parity-check matrix of the code $\mathcal{C}$,
       $s$ the syndrome
Output: An error $e$ of small weight such that $He^\intercal = s$
  $e \leftarrow 0$; $s' \leftarrow s - He^\intercal$
  while $s' \neq 0$ do
      for $j = 1, \ldots, n$ do
          if $\sigma_j = \langle s', h_j \rangle \geq \mathrm{threshold}$ then
              Flip($e_j$)
      $s' \leftarrow s - He^\intercal$
  return $e$
```

Timing Attack

Eve		**Alice's Decoder**
$m \leftarrow \mathbb{F}_2^r$		
$e \xleftarrow{\$} \mathbb{F}_2^n, \mathrm{w}(e) = t$	$\xrightarrow{c = G_{Alice} \cdot m^\intercal + e}$	$\underline{\mathrm{Decode}(c, H_{Alice}) :}$
		$s \leftarrow H \cdot c^\intercal$ $\sigma \leftarrow \mathrm{w}(s)$
		$\dots$
		Algorithm runs in N iterations
	$\xleftarrow{N}$	

128 bits security, 2^{25} samples



Timing Attack

Required number of samples to fully distinguish the spectrum (variable thresholds):

Security bits	80	128	256
Number of samples	2^{25}	2^{25}	2^{28}

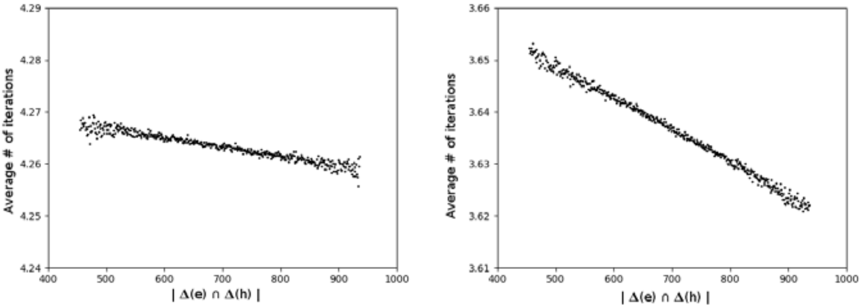
Timing Attack

Required number of samples to fully distinguish the spectrum (variable thresholds):

Security bits	80	128	256
Number of samples	2^{25}	2^{25}	2^{28}

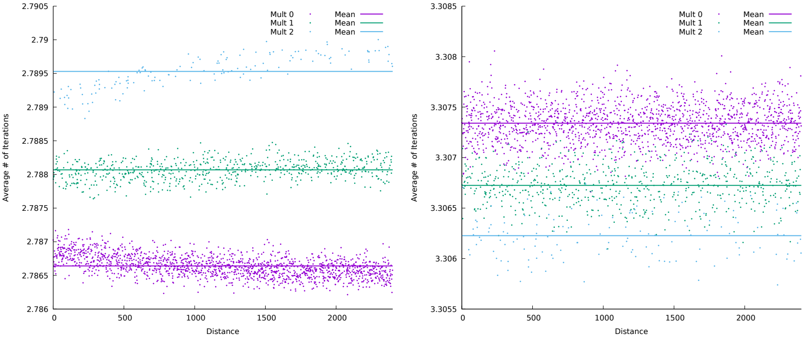
- Correlation depends strongly on the decoder.

Fixed vs. variable thresholds decoder



Average number of iterations depending on $|\Delta(e) \cap \Delta(h)|$,
fixed thresholds (left) vs. variable thresholds (right),
128 bits security, 2^{29} samples

In-place vs. out-of-place decoder



Average number of iterations per distance,
in-place decoder (left) vs. out-of-place decoder (right),
80 bits security, 2^{25} samples

Analysis

Analysis

Definition

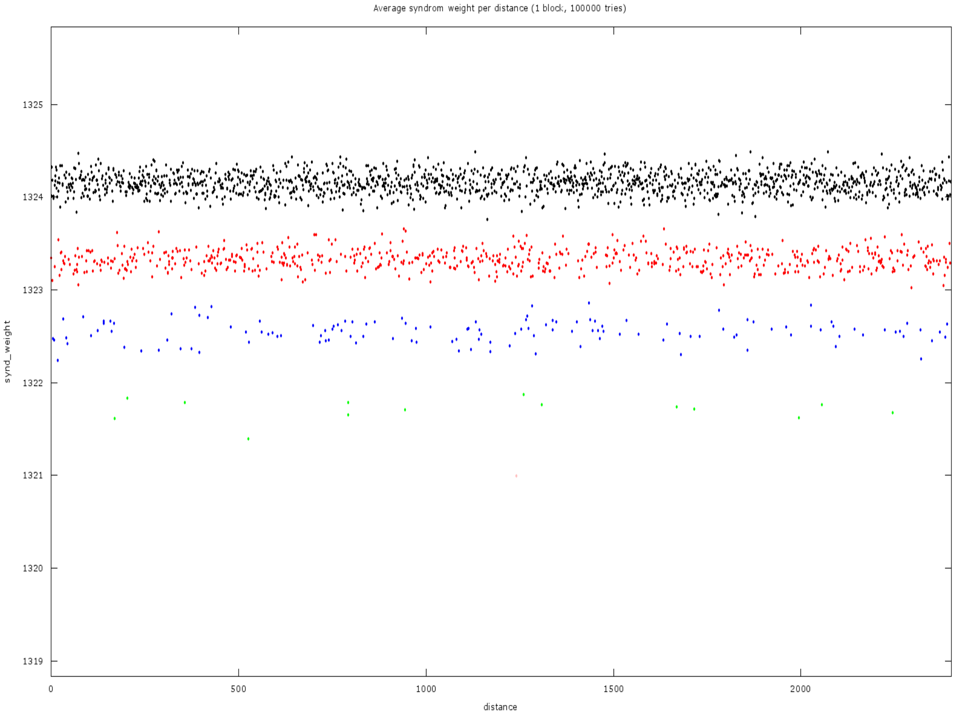
$$\bar{\sigma}_\ell = \mathbb{E}(\sigma \mid \delta \in \Delta(e), \mu_h(\delta) = \ell)$$

For one block

$$\begin{aligned} \bar{\sigma}_\ell \quad = \quad & \ell & f(r-2, d-2, t-2, 1) \\ + \quad & 2(d-\ell) & f(r-2, d-1, t-2, 0) \\ + \quad & (r-2d+\ell) & f(r-2, d, t-2, 1). \end{aligned}$$

where:

$$f(r,d,t,b) := \mathbb{P}(\langle h, e\rangle = b) = \sum_{i=0,\ i\equiv b[2]} \frac{\binom{d}{i}\binom{r-d}{t-i}}{\binom{r}{t}}.$$


Average syndrom weight per distance (1 block, 100000 tries)
synd_weight
1325
1324
1323
1322
1321
1320
1319
0
500
1000
1500
2000
distance

Analysis

- We can compute the values of $\bar{\sigma}_0$, $\bar{\sigma}_1$ and $\varepsilon = \frac{\bar{\sigma}_0 - \bar{\sigma}_1}{\bar{\sigma}_0}$.

Analysis

- We can compute the values of $\bar{\sigma}_0$, $\bar{\sigma}_1$ and $\varepsilon = \frac{\bar{\sigma}_0 - \bar{\sigma}_1}{\bar{\sigma}_0}$.
- **Chernoff (Hypothesis testing):** need $N \sim \frac{1}{\varepsilon^2}$ Bernouilli trials to guess correctly.

Analysis

- We can compute the values of $\bar{\sigma}_0$, $\bar{\sigma}_1$ and $\varepsilon = \frac{\bar{\sigma}_0 - \bar{\sigma}_1}{\bar{\sigma}_0}$.
- **Chernoff (Hypothesis testing):** need $N \sim \frac{1}{\varepsilon^2}$ Bernouilli trials to guess correctly.
- Gives a polynomial estimate of the number of samples needed to recover the spectrum.

DFR Elimination: ParQ

ParQ - Encapsulation

```
Input: PublicKey $pk$, a seed $s \in \{0,1\}^k$.
  for $i = 1$ to $P$ do
      Let $e_i = \mathrm{ErrGen}(s||i)$.
      Compute $x_i = s \oplus \mathrm{PRF}(e_i||i)$.
      Compute $c_i = \mathrm{QCMDPC.Enc}(pk, x_i, e_i)$.
  Return SharedSecret $= \mathcal{H}(s)$, Ciphetext $= (c_1, \ldots, c_P)$.
```

ParQ - Decapsulation

```
Input: SecretKey $sk$, Ciphertext $(c_1, \ldots, c_P)$.
  for $i = 1$ to $P$ [in random order] do
      Run $(x_i, e_i) \leftarrow \mathrm{QCMDPC.Dec}(sk, c_i)$.
      if QCMDPC.Dec succesful then
          Compute $s = x_i \oplus \mathrm{PRF}(e_i || i)$.
          if $c_j$ valid for all $j \neq i$ then
              Return SharedSecret $= \mathcal{H}(s)$.
          else
              Return $\perp$.
  if QCMDPC.Dec failed to decode for $i = 1$ to $P$ then
      Return $\perp$.
```

ParQ - Consequences

- Same key sizes as QC-MDPC KEM.
- Ciphertext size and time complexity $\times P$.
- DFR → DFR^P (QC-MDPC: $2^{-23} \xrightarrow{P=12}$ ParQ: 2^{-276})
- IND-CCA2 in model including DFR.

Conclusion

Conclusion

- Theoretical analysis:
  - Understand the GJS attack;
  - Identify the origin of the leak.

Conclusion

- Theoretical analysis:
  - Understand the GJS attack;
  - Identify the origin of the leak.
- Generic attack pattern:
  - Quasi-cyclic structure induces correlations in the syndrome;
  - Even number of errors don't appear in the scalar product;
  - Any parameter correlated with σ can lead to an attack.

Conclusion

- Theoretical analysis:
  - Understand the GJS attack;
  - Identify the origin of the leak.
- Generic attack pattern:
  - Quasi-cyclic structure induces correlations in the syndrome;
  - Even number of errors don't appear in the scalar product;
  - Any parameter correlated with σ can lead to an attack.
- Experimental work:
  - Successful side-channel attack on the syndrome weight;
  - First timing attack on QC-MDPC codes.

Conclusion

- Theoretical analysis:
  - Understand the GJS attack;
  - Identify the origin of the leak.
- Generic attack pattern:
  - Quasi-cyclic structure induces correlations in the syndrome;
  - Even number of errors don't appear in the scalar product;
  - Any parameter correlated with σ can lead to an attack.
- Experimental work:
  - Successful side-channel attack on the syndrome weight;
  - First timing attack on QC-MDPC codes.
- Countermesures:
  - Masking sensitive parameters in implementation;
  - Bound the number of allowed queries;
  - Improve the decoding algorithm;
  - New KEM: ParQ.

Thank you for your attention.

Questions?