Exploring Decryption Failures of BIKE: New Class of Weak Keys and Key Recovery Attacks

Tianrui Wang[1] Anyu Wang[2,3] Xiaoyun Wang[2,3]

[1]Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing, China

[2]Institute for Advanced Study, BNRist, Tsinghua University, Beijing, China

[3]Zhongguancun Laboratory, Beijing, China

CRYPTO'23 August 22, 2023

Contents

1. Background
2. Gathering Property and DFR of QC-MDPC
3. Decryption failure attack for QC-MDPC
4. Conclusion

Background of Public Cryptology

Post Quantum Algorithms

- In 1994, Shor's algorithm
  - Integer Factorization & Discrete Logarithm
- Current Pub Key Algorithm
- NIST competition
  - Pub Key: Lattice, **Code**, Multivariable, Symmetric...

NIST Candidates

NIST Candidates

Candidates in NIST Competition

Class	Code	NIST 2nd	NIST 3rd	NIST 4th
McEliece/Niederreiter	Classic McEliece NTS-KEM			Classic McEliece
Rank-Code Schemes	Rollo RQC	Algebraic attack		
Quasi-Cyclic Schemes	HQC			HQC
LDPC Schemes	LEDACrypt	Weak key		
MDPC Schemes	BIKE			BIKE

BIKE with QC-MDPC

QC-MDPC

- MDPC(Moderate Density Parity Check) invented in 2013
  - McEliece with MDPC
  - Quasi-Cyclic $\rightarrow$ smaller size & faster speed (BIKE)
- CPA security
  - Private Key: $(h_0, h_1) \in \mathrm{K}(w)$
  - Public Key: $h = h_1 h_0^{-1}$
  - Encryption: $(e_0, e_1) \in \mathrm{E}(t)$, $s = e_0 + e_1 h$
  - Decryption: $decoder(sh_0, h_0, h_1)$
  - where $\mathcal{R} := \mathbb{F}_2[x]/(x^r - 1)$, $y = y_0 + y_1 x + \cdots + y_{r-1} x^{r-1}$ $\iff$ $\mathbf{y} = (y_0, \cdots, y_{r-1})$
  - $\mathrm{K}(w) := \{(h_0, h_1) \in \mathcal{R}^2 | w_H(h_0) = w_H(h_1) = w/2\}$, $\mathrm{E}(t) := \{(e_0, e_1) \in \mathcal{R}^2 | w_H(e_0) + w_H(e_1) = t\}$
- Decoder: $e_0 h_0 + e_1 h_1 = sh_0 \rightarrow (H_0, H_1) \cdot (e_0, e_1)^T = sh_0$

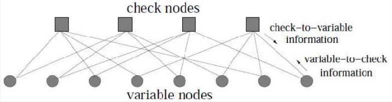
Bit-Flipping

- Bit-Flipping
  - Flip a position if more parity checks are satisfied, iterate until all set
  - UPC(unsatisfied parity check): $\mathtt{UPC}(\mathbf{e}, i) = |\mathrm{Supp}(\mathbf{s}) \cap \mathrm{Supp}(\mathbf{h_i})|$ where h_i is the i-th column of $\mathbf{H}$
- MDPC usage
  - Bit-Flipping has high decryption failure rate
  - Black-Gray-Flip: fine-grained thresholds, check before really flip (used in BIKE)

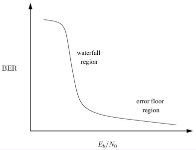
Algorithm 1: The Bit Flipping Algorithm

Input: $\mathbf{H} \in \mathbb{F}_2^{m \times n}, \mathbf{s} \in \mathbb{F}_2^m$
Output: $\mathbf{e} \in \mathbb{F}_2^n$ s.t. $\mathbf{He} = \mathbf{s}$

```
e = 0
while i < NIter do
  for j from 0 to n − 1 do
    if UPC(e, j) ≥ τ then
      Flip the j-th position of e
    end if
  end for
  i = i + 1
end while
return e
```



Researches on DFR



- High DFR(2^{-30}) on small parameters
- No accurate DFR
  - Existing Attacks
    - 2016,Guo: DFR is relevant with distance spectrum of key
    - Distance spectrum: the set of distances between any two 1's in the secret key
    - Decryption failure $\rightarrow$ spectrum information $\rightarrow$ key recovery
    - Need high DFR to construct distance spectrum model

BIKE KEM

- Application in BIKE
  - 128 bit security $\rightarrow$ DFR $< 2^{-128}$

Security Level	r	w	t	Decryption Failure Rate
128-bit	12323	142	134	2^{-128}
192-bit	24659	206	199	2^{-192}
256-bit	40973	274	264	2^{-256}

  - Fujisaki-Okamoto Transform $\rightarrow$ CCA security
- KEM

– KeyGen ():
  - Randomly generate $h_0, h_1 \in \mathcal{R}$ such that $w_H(h_0) = w_H(h_1) = w/2$.
  - Compute $h = h_1 h_0^{-1} \in \mathcal{R}$.
  - Output (h_0, h_1, σ) as the secret key, and h as the public key.

– Encaps (h):
  - Randomly choose $m \in \{0,1\}^{256}$.
  - Compute $(e_0, e_1) = \mathtt{H}(m) \in \mathcal{R}^2$ such that $w_H(e_0) + w_H(e_1) = t$.
  - Output the ciphertext $c = (e_0 + e_1 h, m \oplus \mathtt{L}(e_0, e_1))$, and the shared secret $\mathcal{K} = \mathtt{K}(m, c)$.

– Decaps $((h_0, h_1, \sigma), c)$:
  - Compute $e' = \mathtt{decoder}(c_0 h_0, h_0, h_1) \in \mathcal{R}^2$.
  - Compute $m' = c_1 \oplus L(e')$.
  - If $e' = \mathtt{H}(m')$ then output $\mathtt{K}(m', c)$, else output $\mathtt{K}(\sigma, c)$.

Researches on decoding failure of BIKE

- DFR of BIKE
  - Goal: CCA security needs DFR $< 2^{-128}$
  - Method: linear fit with experiments (without accuracy theory model)
- Existing Researches
  - Sendrier found weak keys with high DFR
  - Vasseur's classification does not disapprove the IND-CCA security of BIKE
- Questions
  - Are these classes of weak keys exhaustive?
  - A higher lower bound of DFR?

$$\mathrm{DFR}_{avg} \geq \frac{|W|}{|K|}\mathrm{DFR}_W$$

Contents

1 Background

2 Gathering Property and DFR of QC-MDPC

3 Decryption failure attack for QC-MDPC

4 Conclusion

Observation

- matrix parity check

$$e_0 h_0 + e_1 h_1 = s \rightarrow (rot(h_0), rot(h_1)) \cdot (e_0, e_1)^T = s$$

- the 1's in h_0 gathering in first m positions $\rightarrow$ UPC(i) is higher when $0 \leq i < m \rightarrow$ the first m positions are more likely to be flipped

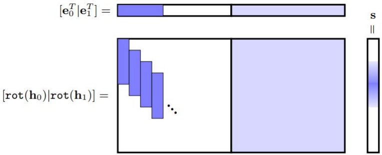


Figure 4: Gathering property.

Iteration	Average UPC of the first m positions	Average UPC of all positions
0	31.3864	26.4111
1	57.2082	42.7164
2	83.5507	56.5557
3	114.588	73.0108
4	148.179	93.1936

Figure 5: UPC table.

Gathering Property

Definition (gathering property)

Let $m < r$ be a positive integer and let $\epsilon \geq 0$ be a small integer, then $(y_0, y_1) \in \mathcal{R}^2$ is said to have the (m, ϵ)-gathering property if there exists an integer a such that

$$w_H(\mathbf{y}_0^{[a,a+m)}) = w_H(\mathbf{y}_0) - \epsilon.$$

where $\mathcal{R} := \mathbb{F}_2[x]/(x^r - 1)$ and $\mathbf{y}^{[a,b)} := (y_a, y_{a+1}, \cdots, y_{b-1})$

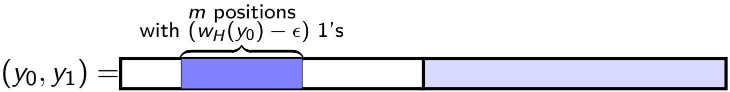
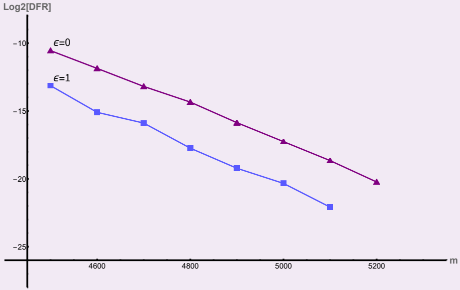


Figure 6: Gathering Property

DFR with gathering property

- Consider error and key with gathering property
  - Under BIKE-128 parameters, DFR : $2^{-128} \rightarrow 2^{-10} \sim 2^{-25}$



- Weak keys
  - When $(m = 5100, \epsilon = 1)$, $\text{DFR}_K^{m,\epsilon} \geq 2^{-22.08} \cdot 2^{-75.58} = 2^{-97.66}$
  - $\Pr((h_0, h_1)\ \textit{weak})$ is too low to affect DFR_{avg}

Isomorphism to expand weak keys

- Observation
  - $\phi_i : y(x) \to y(x^i)$
  - $(\mathbf{h_0}, \mathbf{h_1})$ and $(\mathbf{e_0}, \mathbf{e_1})$ cause a failure iff $(\phi_i(\mathbf{h_0}), \phi_i(\mathbf{h_1}))$ and $(\phi_i(\mathbf{e_0}), \phi_i(\mathbf{e_1}))$ cause a failure
  - weak key set under isomorphism

$$\mathrm{K}_{m,\epsilon}^{\phi_i}(w) := \{(\phi_i(h_0), \phi_i(h_1)) : (h_0, h_1) \in \mathrm{K}_{m,\epsilon}(w)\}. \tag{1}$$

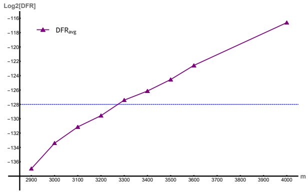
- Define weak key set

$$\mathrm{K}_{m,\epsilon}^{\texttt{union}}(w) := \bigcup_{1 \leq i < r/2} \mathrm{K}_{m,\epsilon}^{\phi_i}(w). \tag{2}$$

- Question: size of weak key set?

Expanded Weak key with high DFR

$$\mathrm{DFR}_{\mathrm{avg}} \geq 2 \cdot \mathrm{DFR}_{(h_0,h_1) \xleftarrow{\$} \mathrm{K}^{\mathtt{union}}_{m,\epsilon}(w)} \cdot \frac{|\mathrm{K}^{\mathtt{union}}_{m,\epsilon}(w)|}{|\mathrm{K}(w)|}, \tag{3}$$



- When $(m = 4000, \epsilon = 1)$, $\mathrm{DFR}_{avg} \geq 2^{-29.33} \cdot 2^{-87.28} = 2^{-116.61}$
- Much higher than 2^{-128}
- CCA security claim? Recovery Attack?

(m,ϵ)	$(2900,1)$	$(3100,1)$	$(3200,1)$	$(3400,1)$	$(3500,1)$	$(3600,1)$	$(4000,1)$
N	2996871	5459695	32903584	165860000	214960000	315470000	8745860000
F	16	16	31.5^*	25.5^*	13.5^*	11	13
DFR	−17.52	−18.38	−19.99	−22.63	−23.92	−24.77	−29.33
p	−119.45	−112.76	−109.58	−103.51	−100.62	−97.80	−87.28

Contents

1. Background
2. Gathering Property and DFR of QC-MDPC
3. Decryption failure attack for QC-MDPC
4. Conclusion

Attack Model without ciphertexts reusing

- Principle: $\mathrm{DFR}_{\texttt{weak}} >> \mathrm{DFR}_{avg}$
- Model
  - 1.Construct ciphertexts: for a target T, generate $1/\mathrm{DFR}_{\texttt{weak}}$ ciphertexts
  - 2.Query: decrypt those ciphertexts. If a failure occurs, jump to 3. Or change a target and return 1.
  - 3.Recover: If T has a decryption failure, T's key is probably a weak one. Try to recover it using ISD with extra information.
- False Positive: decryption failure but not weak key
  - cannot recover false positive cases
  - can measure/estimate the number of false positive

Key Recovery

Problem

Given $\mathbf{H} \in \mathbb{F}_2^{r\times 2r}, \mathbf{s} \in \mathbb{F}_2^r$ *and positive integers* w, m *and* $\epsilon \geq 0$, *find* $\mathbf{e} = (\mathbf{h}_1^T, \mathbf{h}_0^T)^T$ *such that* $\mathbf{He} = \mathbf{s}$, $w_H(\mathbf{h_0}) = w_H(\mathbf{h_1}) = w/2$ *and there exists an integer* a *such that* $w_H(\mathbf{h}_0^{[a,a+m)}) = w/2 - \epsilon$.

- Syndrome Decoding with Extra Information
- ISD with Extra Information
- Recover secret key $(\mathbf{h_0}, \mathbf{h_1})$
  - Suppose there exists i s.t. $(\phi_i^{-1}(\mathbf{h_0}), \phi_i^{-1}(\mathbf{h_1}))$ has gathering property
  - Try to recover $(\mathbf{h_0}, \mathbf{h_1})$ with any i
  - Succeed or fail when the key is a false positive one

ISD with Extra Information

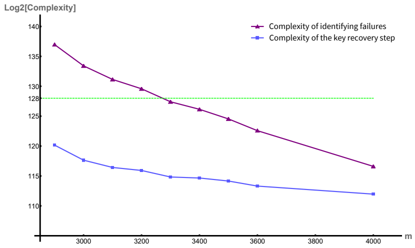
- Classical ISD
  - Syndrome Decoding $He = s$
  - Class: Prange,Stern-Dumer,MMT,BJMM,MO...
  - Step: **Random Permutation** (try to split e into (e_1, e_2) where $w_H(e_1) = w - p$, $w_H(e_2) = p$), Gauss Elimination, Column Match, Recover
- ISD with Extra Information
  - Extra Information: $w_H(\mathbf{y}_0^{[a,a+m)}) = w_H(\mathbf{y}_0) - \epsilon$
  - Modification:
    - guess beginning index a,
    - gather the m positions of y_0 (high weight) in e_1,
    - gather the remaining positions of y_0 (low weight) in e_2,
    - permute others randomly

Complexity Analysis

- Complexity

Theorem

The complexity of attack $C_{total} = (\mathrm{DFR}^{weak}_{m,\epsilon} \cdot p^{weak}_{m,\epsilon})^{-1} + p^{-1}_{true} \cdot r \cdot T_{ISD}$ *, where* $p_{true} = p^{weak}_{m,\epsilon} \cdot \mathrm{DFR}^{weak}_{m,\epsilon} \cdot \mathrm{DFR}^{-1}_{avg}$.



- When $m = 4000, \epsilon = 1$, $C_{\text{total}} = 2^{116.61}$
- **116.61<128**

Attack Model with ciphertexts reusing

- Ciphertexts Reusing
  - BIKE has no multi-target protection
  - Preprocess: generate weak ciphertexts with gathering property
- Attack Model
  - $\mathrm{DFR}_{m,\epsilon}$ denotes to the DFR when key and error have (m, ϵ) property
  - 1. generate ciphertexts randomly and collect $1/DFR_{m,\epsilon}$ ones with gathering property
  - 2. choose a target T, decrypt those ciphertexts with T's oracle. If a decryption failure occurs, jump to 3. Or change a target and return 2.
  - 3. If T has a decryption failure, T's key is probably a weak one. Try to recover it using ISD with extra information.

Complexity Analysis

- Complexity

Theorem

The complexity $C_{total} = (\mathrm{DFR}_{m,\epsilon} \cdot q_{m,\epsilon})^{-1} + (\mathrm{DFR}_{m,\epsilon} \cdot p_{m,\epsilon})^{-1} + p_{true}^{-1} \cdot T_{ISD}$, *where* $p_{true} = \mathrm{DFR}_{m,\epsilon} \cdot p_{m,\epsilon} / \mathrm{DFR}_{avg}^{e \sim (m,\epsilon)}$

- when $m = 5100, \epsilon = 1$, $C_{\text{total}} = 2^{98.77}$
- **20 bits** advantage

Table 1: Complexity of two models

	Without reusing	With reusing
Total Complexity	$\mathbf{2^{116.61}}$	$\mathbf{2^{98.77}}$
Targets Number	$2^{87.28}$	$2^{76.69}$
Queries Times	$2^{29.33}$	$2^{22.08}$
Identifying Failures	$2^{116.61}$	$2^{98.77}$
Key Recovery	$2^{111.96}$	$2^{94.81}$
Preprocessing	-	$2^{97.66}$

Summary and Future Work

- Summary
  - An estimate of DFR based on weak keys
  - A decryption failure attack on BIKE
- Solutions for BIKE
  - Estimate DFR more accurate (theoretically or experimentally)
  - Avoid ciphertexts reusing
- Future Work
  - More effective attack with larger m, ϵ (over 2^{30} *decryption*)
  - $w_H(e_0) = w_H(e_1) = t/2 \rightarrow w_H(e_0) + w_H(e_1) = t$
  - Theoretical model between Gathering Property and Bit-Flipping

Thanks for your attention!

Q & A