2025 KpqC 연구단 워크숍

# HQC (Hamming Quasi-Cyclic), the new KEM standard

국민대학교 FDL

김민지, 박동현, 김동현, 김예진, 김동찬

2025.07.15.

# 소개할 내용들

**NIST PQC 공모전**
**4라운드 암호 평가 결과**

SDP, IND-CCA2-secure KEM, DFR
**HQC 안전성**

**HQC 설계 사상과 규격**
QC 부호, Concatenated 부호

# 소개할 내용들

**NIST PQC 공모전**
**4라운드 암호 평가 결과**

SDP, IND-CCA2-secure KEM, DFR

**HQC 안전성**

**HQC 설계 사상과 규격**

QC 부호, Concatenated 부호

# NIST PQC 공모전 4라운드 암호 평가 기준

## NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption

March 11, 2025

- NIST has chosen a new algorithm for post-quantum encryption called HQC, which will serve as a backup for ML-KEM, the main algorithm for general encryption.
- HQC is based on different math than ML-KEM, which could be important if a weakness were discovered in ML-KEM.
- NIST plans to issue a draft standard incorporating the HQC algorithm in about a year, with a finalized standard expected in 2027.

1) Castryck, W ... puter Science, vol 14008. Spr

2) ALAGIC, Go ... , 2025.

# NIST PQC 공모전 4라운드 암호 평가

~~NIST IR.8545 - 4Round Report~~
~~NIST IR.8413 - 3Round Report~~

HQC

The rest of the KEM candidates selected (BIKE, Classic McEliece, HQC, SIKE) will all continue to be evaluated in the fourth round. Both BIKE and HQC are based on structured codes and would be suitable as a general-purpose KEM that is not based on lattices. NIST may select at most one of these two candidates for standardization at the conclusion of the fourth round.

BIKE

stable than that of BIKE. As such, NIST has not selected BIKE for standardization.

**HQC**

**BIKE**

부호 기반

**Classic McEliece**

~~**SIKE**~~
(broken in 2023[1])

아이소제니 기반

# 평가 결과. 안전성

**HQC, BIKE, Classic McEliece**

# IND-CCA2-secure in ROM

based on Fujisaki-Okamoto-like transformation

기반 문제의 계산론적 안전성을 가정하고 랜덤 오라클 모델에서 IND-CCA2 안전성 증명

# 평가 결과. 안전성 – 복호화 실패 확률DFR

**복호화 실패 확률DFR= 올바르게 암호화된 암호문이 올바르게 복호되지 않을 확률**

**HQC**

- 정교한 DFR 제시

**BIKE**

- 정교하지 않은 DFR 제시 → IND-CCA2 공격으로 연결[5)]
- DFR를 보완하였지만 HQC의 DFR 분석이 더 성숙하다고 판단함

**Classic McEliece**

- DFR=0 → 즉, 암호화를 통해 얻은 암호문은 확률 1로 복호됨

5) Wang T, Wang A, Wang X (2023) Exploring decryption failures of BIKE: New class of weak keys and key recovery attacks. Advances in Cryptology – CRYPTO 2023, eds Handschuh H, Lysyanskaya A (Springer Nature Switzerland, Cham), pp 70–100. https://doi.org/https://doi.org/10.1007/978-3-031-38548-3_3

# 평가 결과. 성능 - 데이터

(단위: byte)

| Parameter | Level | Encap. Key | Decap. Key | Ciphertext | Secret |
|---|---|---|---|---|---|
| ML-KEM-512 | I | 800 | 1 632 | 768 | 32 |
| ML-KEM-768 | III | 1 184 | 2 400 | 1 088 | 32 |
| ML-KEM-1024 | V | 1 568 | 3 168 | 1 568 | 32 |
| hqc-128 | I | 2 249 | 2 305 | 4 433 | 64 |
| hqc-192 | III | 4 522 | 4 586 | 8 978 | 64 |
| hqc-256 | V | 7 245 | 7 317 | 14 421 | 64 |
| BIKE Level 1 | I | 1 541 | 281 | 1 573 | 32 |
| BIKE Level 3 | III | 3 083 | 419 | 3 115 | 32 |
| BIKE Level 5 | V | 5 122 | 580 | 5 154 | 32 |
| mceliece348864 | I | 261 120 | 6 492 | 96 | 32 |
| mceliece460896 | III | 524 160 | 13 608 | 156 | 32 |
| mceliece6688128 | V | 1 044 992 | 13 932 | 208 | 32 |
| mceliece6960119 | V | 1 047 319 | 13 948 | 194 | 32 |
| mceliece8192128 | V | 1 357 824 | 14 120 | 208 | 32 |

# 평가 결과. 성능 - 속도[3)]

**(단위: kilocycles)**

| Parameter | Level | Keygen | Encaps | Decaps |
|---|---|---|---|---|
| ML-KEM-512 | I | 23 | 25 | 29 |
| ML-KEM-768 | III | 38 | 39 | 46 |
| ML-KEM-1024 | V | 53 | 54 | 64 |
| hqc-128 | I | 105 | 197 | 360 |
| hqc-192 | III | 244 | 460 | 746 |
| hqc-256 | V | 447 | 844 | 1 410 |
| BIKE Level 1 | I | 637 | 111 | 1 428 |
| BIKE Level 3 | III | 1 892 | 251 | 4 313 |
| BIKE Level 5 | V | 4 535 | 505 | 10 382 |
| mceliece348864 | I | 137 345 | 49 | 120 |
| mceliece460896 | III | 114 189 | 45 | 120 |
| mceliece6688128 | V | 430 364 | 91 | 232 |
| mceliece6960119 | V | 313 600 | 92 | 231 |
| mceliece8192128 | V | 674 012 | 196 | 273 |

3) Open quantum safe (OQS) algorithm performance visualizations. Available at https://openquantumsafe.org/benchmarking.

# 소개할 내용들

NIST PQC 공모전
4라운드 암호 평가 결과

SDP, IND-CCA2-secure KEM, DFR
HQC 안전성

## HQC 설계 사상과 규격

QC 부호, Concatenated 부호

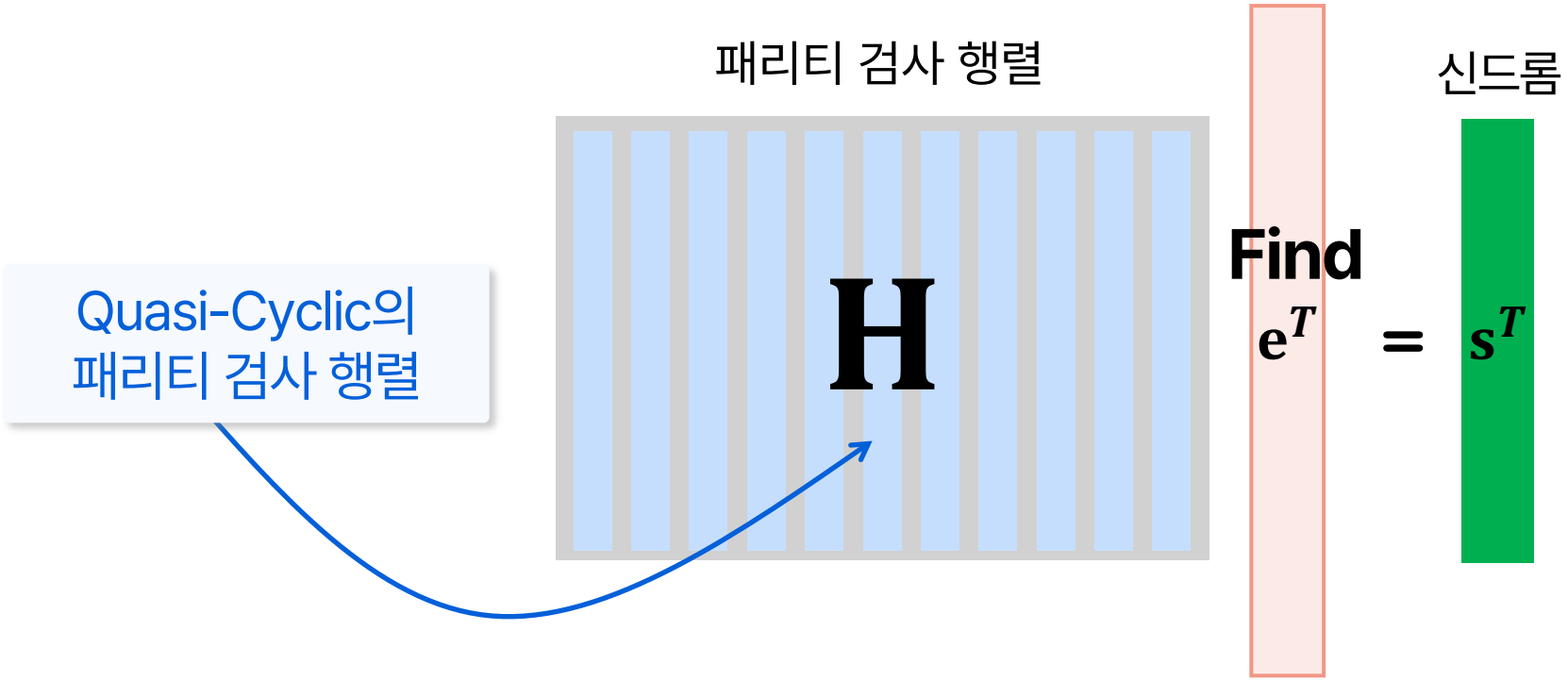
# HQC (Hamming Quasi-Cyclic)

- 부호 기반 KEM
  - Quasi-cyclic 부호의 신드롬 디코딩 문제SDP에 기반함
- 복호화 실패 가능성이 있음
- 파라미터 구성

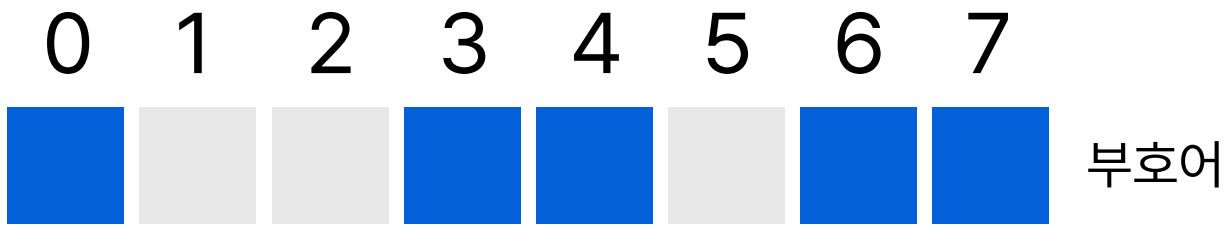
| 파라미터 | hqc-128 | hqc-192 | hqc-256 |
|---|---|---|---|
| 보안강도 (bit) | 128 | 192 | 256 |
| DFR | $< 2^{-128}$ | $< 2^{-192}$ | $< 2^{-256}$ |

# 신드롬 디코딩 문제(Syndrome Decoding Problem; SDP)

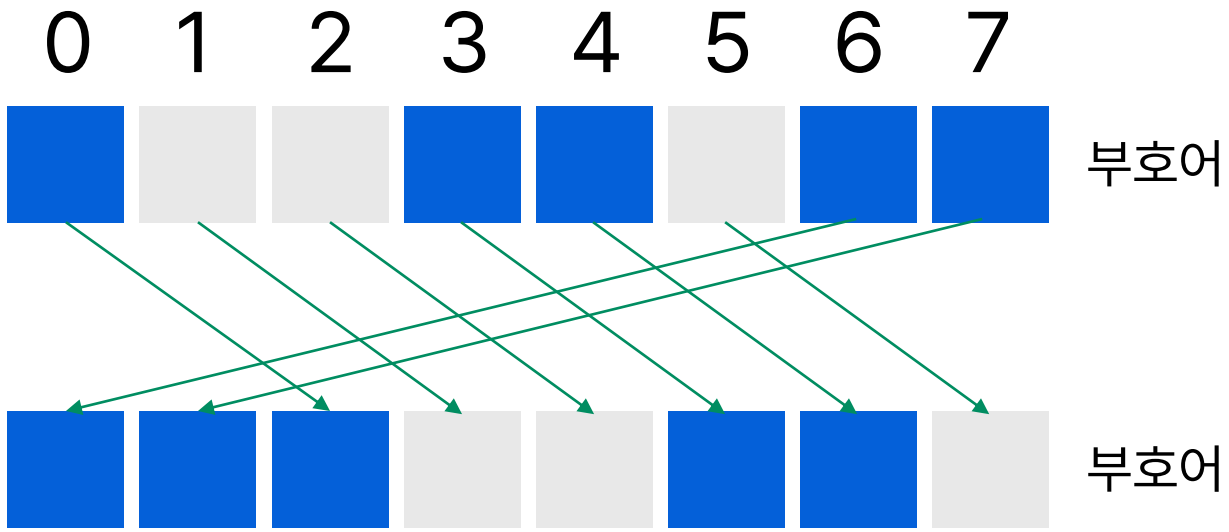
주어진 $(\mathbf{H}, \mathbf{s})$에 대해, 특정 해밍 무게 조건을 만족하면서 $\mathbf{He}^{\mathbf{T}} = \mathbf{s}^{\mathbf{T}}$가 성립하는 $\mathbf{e}$를 찾는 문제



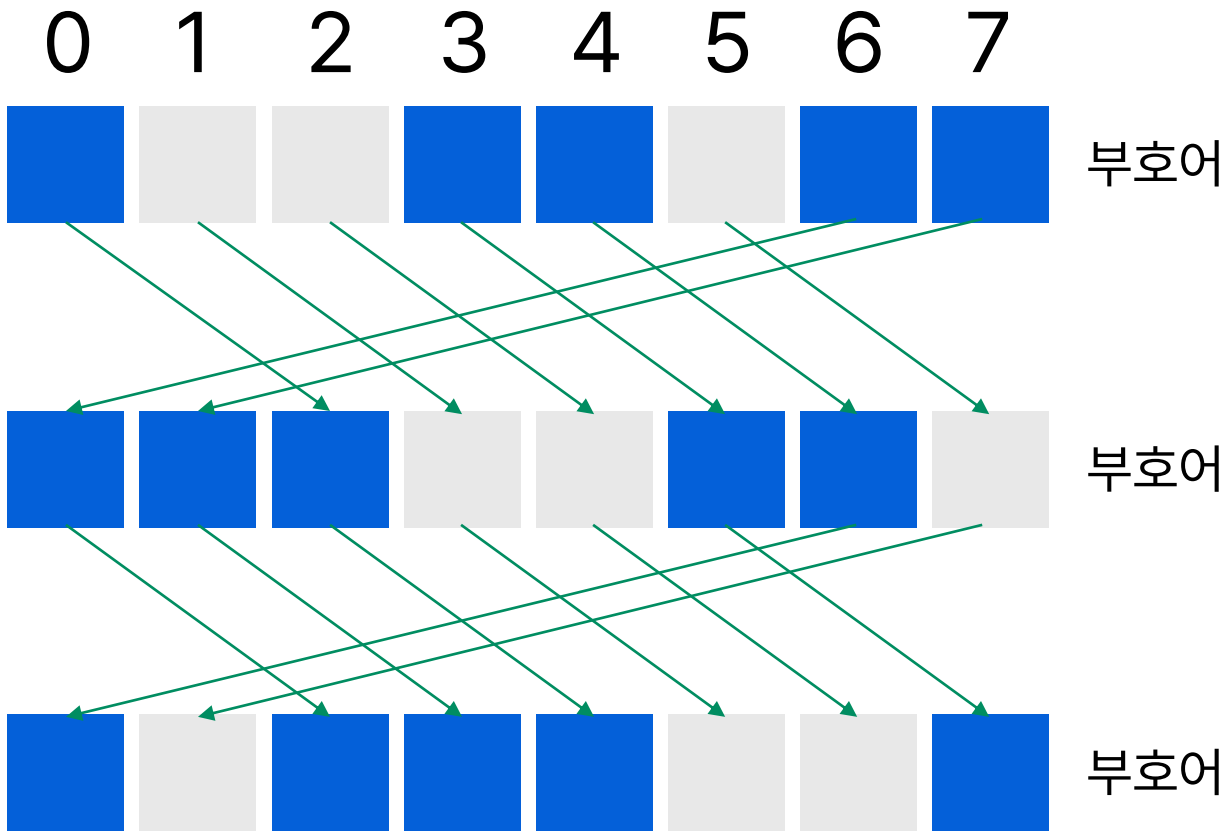
# Quasi-Cyclic 부호



# Quasi-Cyclic 부호

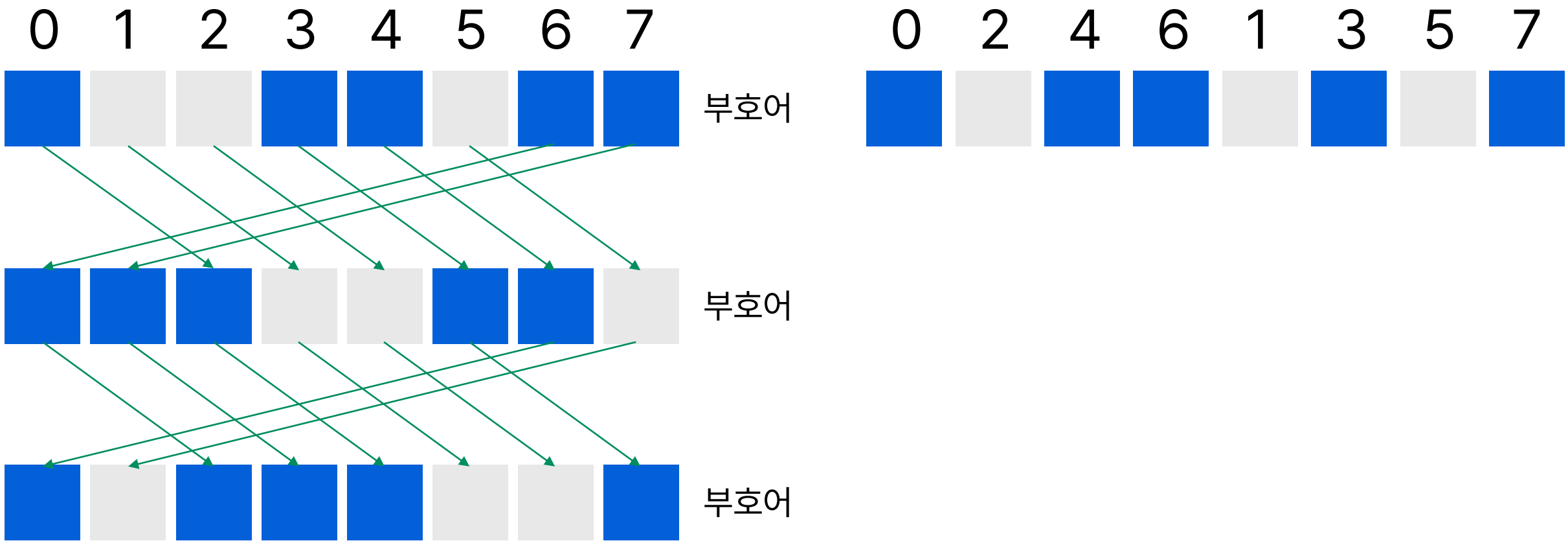


# Quasi-Cyclic 부호



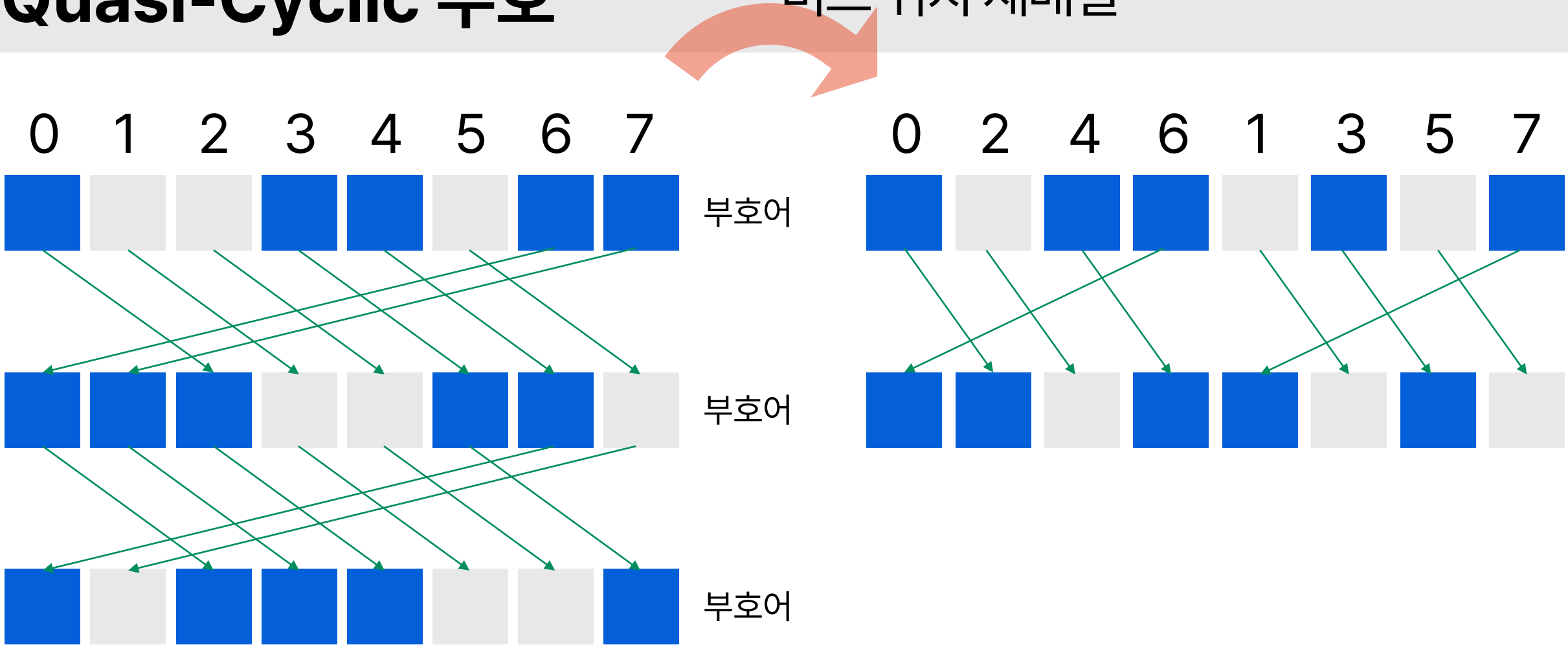

QC 부호는 $s$비트 단위 순환성을 가짐

# Quasi-Cyclic 부호



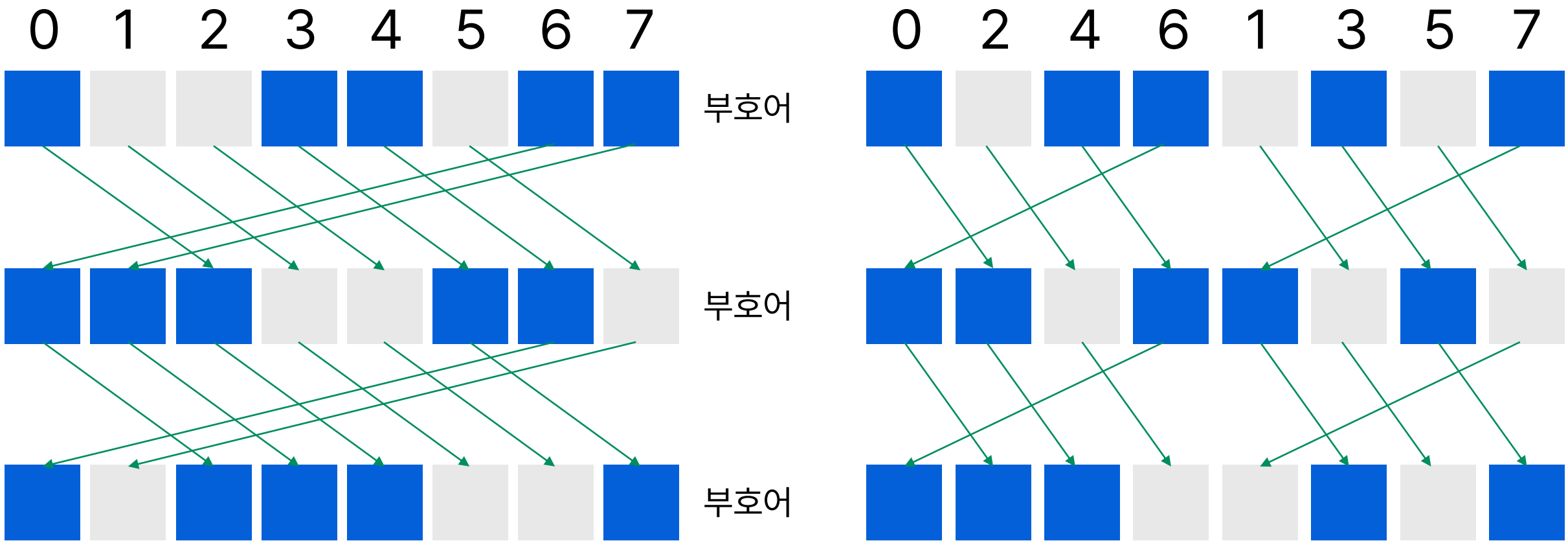

QC 부호는 $s$비트 단위 순환성을 가짐

# Quasi-Cyclic 부호




QC 부호는 $s$비트 단위 순환성을 가짐

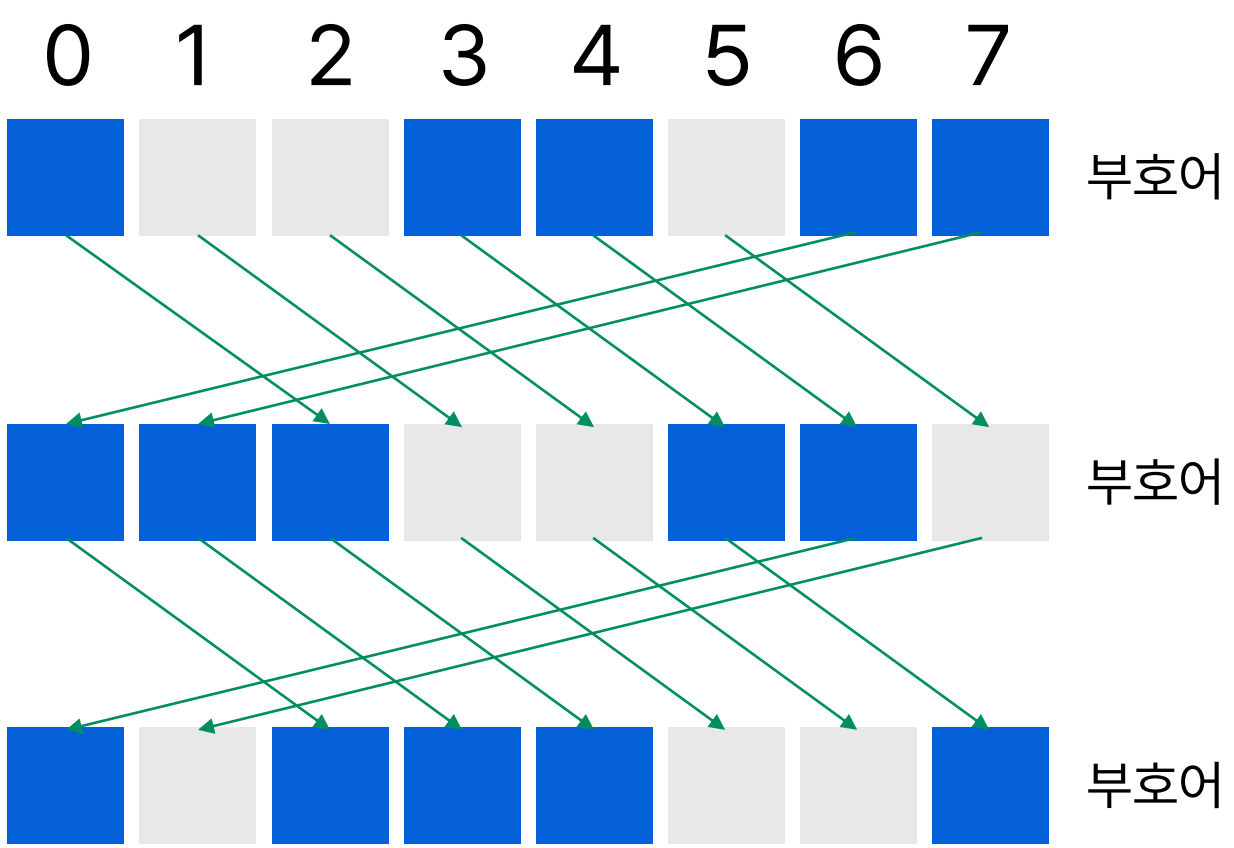
# Quasi-Cyclic 부호

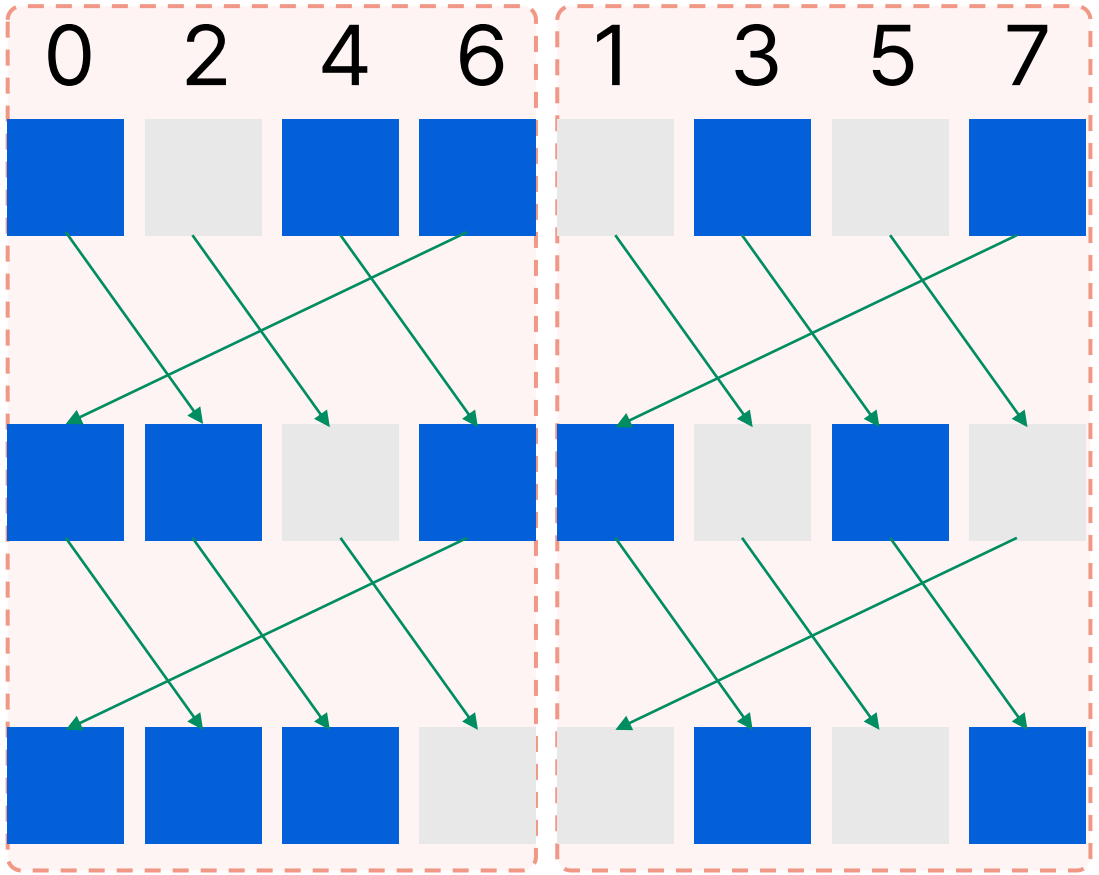



QC 부호는 $s$비트 단위 순환성을 가짐

# Quasi-Cyclic 부호

비트 위치 재배열



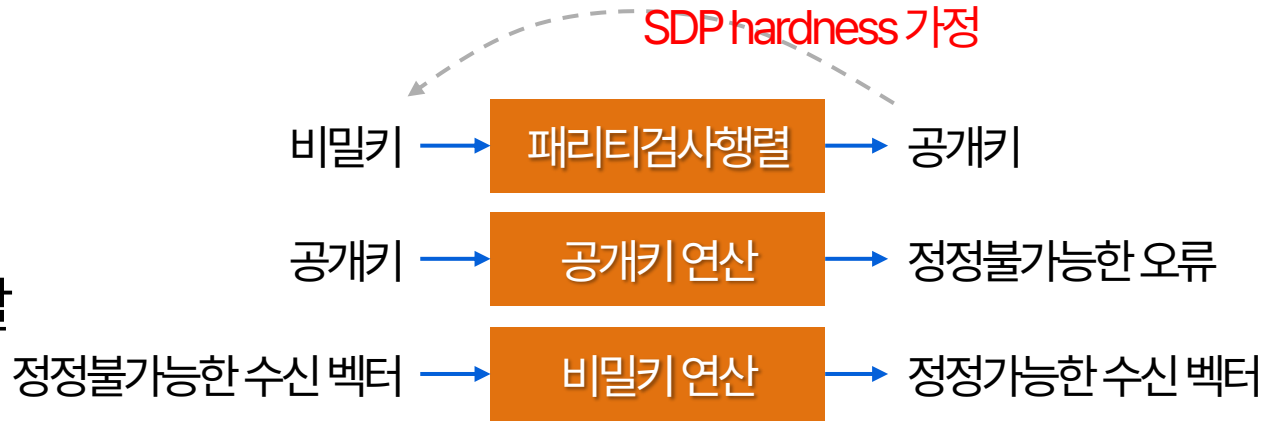

QC 부호는 $s$비트 단위 순환성을 가짐

QC 부호는 블록 단위 순환성을 가짐

# HQC가 사용하는 선형 부호

## Quasi-Cyclic 부호

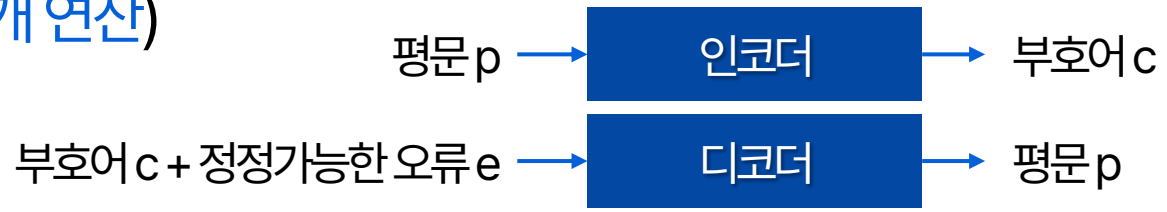
비밀키를 사용하여 정정가능한 오류로 변환하는 역할

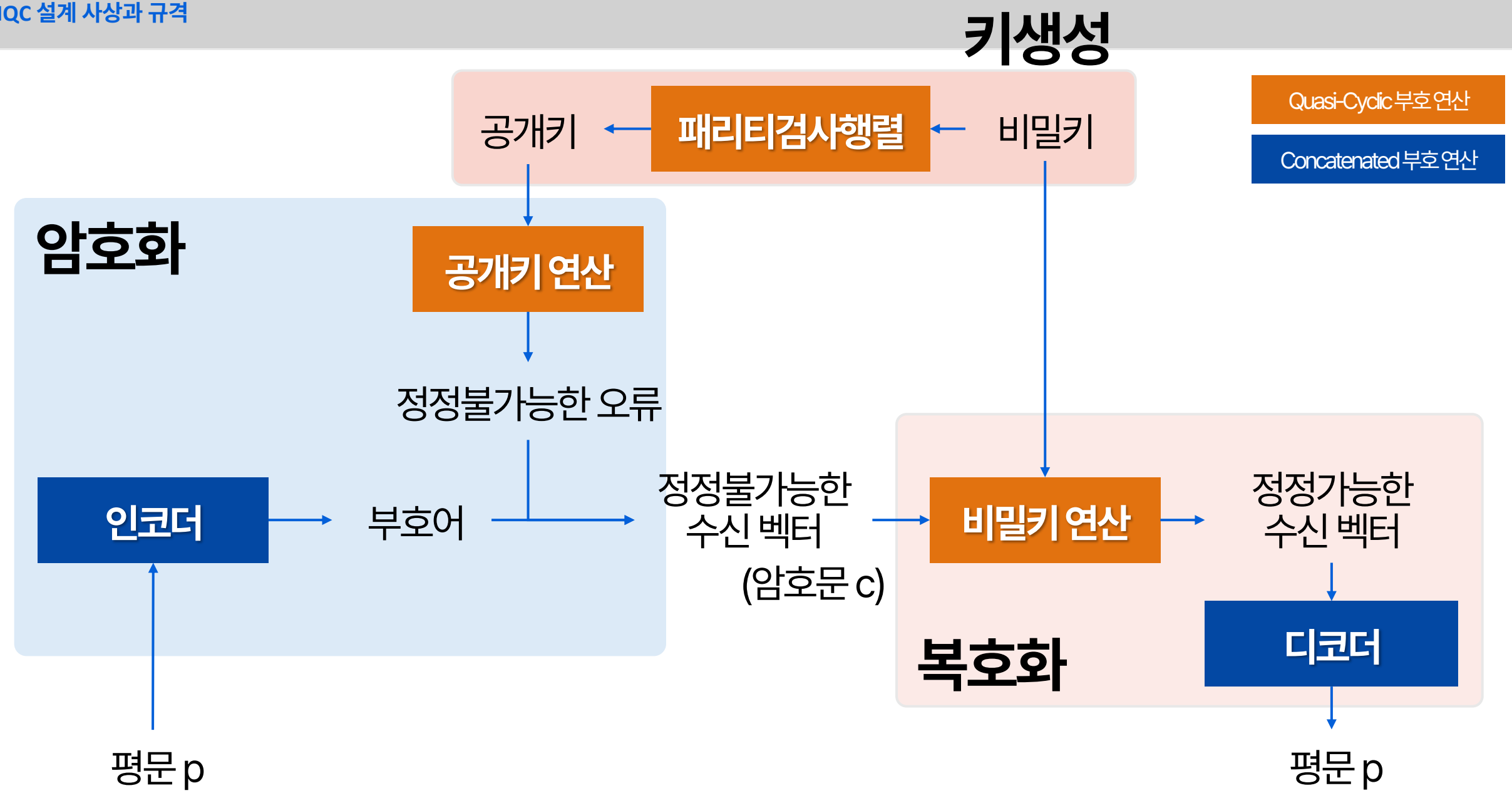



## Concatenated 부호

평문의 근삿값으로부터 평문을 복구하는 역할 (공개 연산)

(shortened RS + duplicated RM)




키생성
공개키
패리티검사행렬
비밀키
Quasi-Cyclic 부호 연산
Concatenated 부호 연산
암호화
공개키 연산
정정불가능한 오류
인코더
부호어
정정불가능한
수신 벡터
(암호문 c)
비밀키 연산
정정가능한
수신 벡터
복호화
디코더
평문 p
평문 p

# HQC.PKE

1: **procedure** GenKeyPair$^{PKE}$($param$)
2: $h \xleftarrow{\$} \{0,1\}^n$
3: $(x_1, x_2) \xleftarrow{\$} (\{0,1\}^n_{w_x})^2$
4: $s \leftarrow x_1 + h \cdot x_2 \in \{0,1\}^n$
7: **return** $pk^{PKE}, sk^{PKE}$
8: **end procedure**

Quasi-Cyclic 부호

비밀키 → 패리티검사행렬 → 공개키

1: **procedure** Encrypt($pk^{PKE}, m, \theta$)
3: $(r_1, r_2) \leftarrow (\{0,1\}^n_{w_r})^2$
4: $u \leftarrow r_1 + h \cdot r_2$
5: $t \leftarrow (s \cdot r_2 + e)$
6: $noise \leftarrow t_[$
7: $v \leftarrow$ Enco
8: $c \leftarrow (u, v)$

Quasi-Cyclic 부호

공개키 → 공개키 연산 → 정정불가능한 오류

평문 p → 인코더 → 부호어 c

1: **procedure** Decrypt($sk^{PKE}; c$)
$t \leftarrow u \cdot x_2$
$w \leftarrow t_{[0:n_1 n_2]}$
4: $p \leftarrow \text{Decode}_{\mathcal{C}}(v - w)$
5: **return** $p$
6: **end procedure**

Quasi-Cyclic 부호

Concatenated 부호

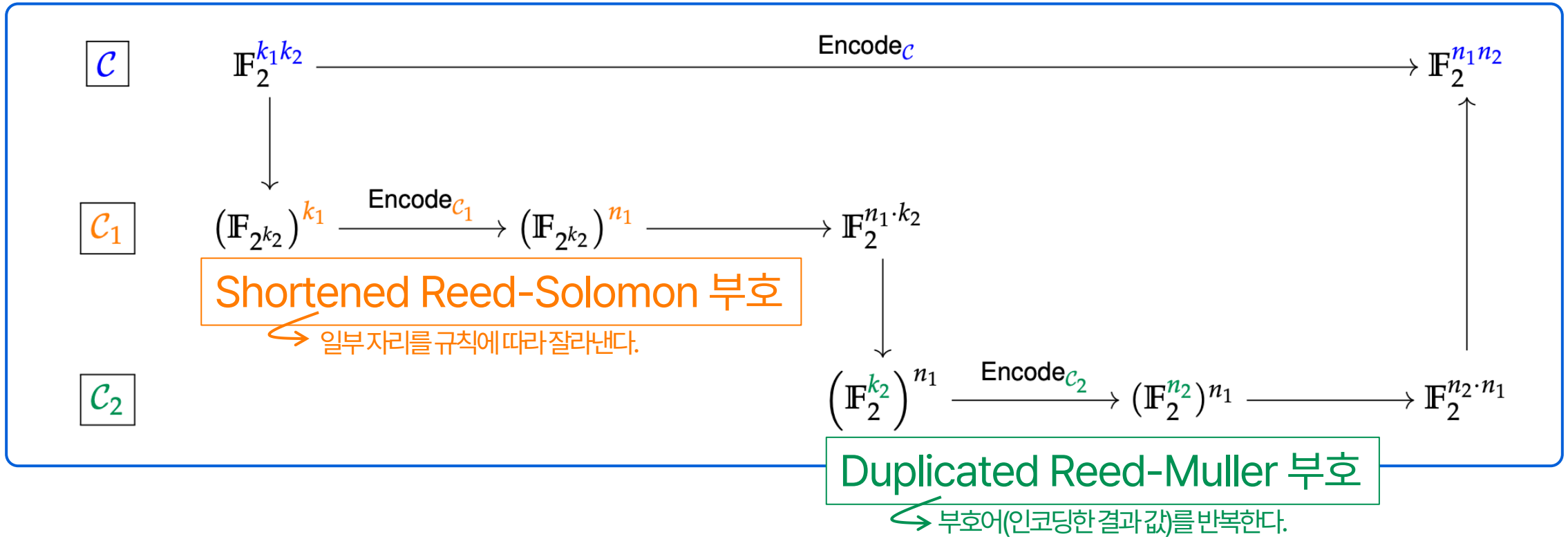
정정불가능한 수신 벡터 → 비밀키 연산 → 정정가능한 수신 벡터

부호어 c + 정정가능한 오류 e → 디코더 → 평문 p

Concatenated 부호

# Concatenated 부호

Concatenated 부호 $\mathcal{C}$의 인코딩



# Concatenated 부호

| Parameter | hqc-128 | hqc-192 | hqc-256 |
|---|---|---|---|
| $\mathcal{C}_1$ | $[46,16,31]_{256}$ (shortening of $[255,225,31]_{256}$) | $[56,24,33]_{256}$ (shortening of $[255,223,33]_{256}$) | $[90,32,59]_{256}$ (shortening of $[255,197,59]_{256}$) |
| $\mathcal{C}_2$ | $[384,8,192]_2$ ($[128,8,64]_2 \times 3$) | $[640,8,320]_2$ ($[128,8,64]_2 \times 5$) | $[640,8,320]_2$ ($[128,8,64]_2 \times 5$) |
| $\mathcal{C}$ | $[17664,128,\geq 5952]_2$ | $[35840,192,\geq 10560]_2$ | $[57600,256,\geq 15680]_2$ |

# HQC.KEM - GenKeyPair

**Input:** Parameter $param = (n, k, \delta, w_x, w_r, w_e)$
**Output:** Public key $pk^{\mathsf{KEM}} = (h, s) \in (\{0,1\}^n)^2$, secret key $sk^{\mathsf{KEM}} = ((x_1, x_2), \sigma) \in (\{0,1\}^n_{w_x})^2 \times \{0,1\}^k$

1: **procedure** $\mathsf{GenKeyPair}^{\mathsf{KEM}}(param)$
2: $pk^{\mathsf{PKE}}, sk^{\mathsf{PKE}} \leftarrow \mathsf{GenKeyPair}^{\mathsf{PKE}}(param)$
3: $\sigma \xleftarrow{\$} \{0,1\}^k$ ▷ $\sigma$ is used in cases of implicit rejection
4: $pk^{\mathsf{KEM}} \leftarrow pk^{\mathsf{PKE}}$
5: $sk^{\mathsf{KEM}} \leftarrow (sk^{\mathsf{PKE}}, \sigma)$
6: **return** $pk^{\mathsf{KEM}}, sk^{\mathsf{KEM}}$
7: **end procedure**

# HQC.KEM - Encap

**Input:** Public key $pk^{\mathsf{KEM}} = (\mathbf{h}, \mathbf{s}) \in \{0,1\}^n \times \{0,1\}^n$
**Output:** Shared secret $\kappa \in \{0,1\}^{512}$ and ciphertext $(c, salt)$

1: **procedure** Encap($pk$)
2: $m \xleftarrow{\$} \{0,1\}^k$
3: $salt \xleftarrow{\$} \{0,1\}^{128}$
4: $\theta \leftarrow G(m \| (pk^{\mathsf{KEM}})_{[0:256]} \| salt)$
5: $c \leftarrow \mathsf{Encrypt}(pk^{\mathsf{PKE}}, m, \theta)$
6: $\kappa \leftarrow K(m, c)$
7: **return** $\kappa$ and $(c, salt)$
8: **end procedure**

# HQC.KEM - Decap

**Input:** Ciphertext $(c, salt)$, public key $pk^{\mathsf{KEM}}$
and secret key $sk^{\mathsf{KEM}} = (\mathbf{x}_1, \mathbf{x}_2, \sigma) \in \left(\{0,1\}_w^n\right)^2 \times \{0,1\}^k$

**Output:** Session key $\kappa \in \{0,1\}^{512}$

**procedure** Decap($pk^{\mathsf{KEM}}, sk^{\mathsf{KEM}}, (c, salt)$)
  $m' \leftarrow \mathsf{Decrypt}(sk^{\mathsf{PKE}}, c)$
  $\theta' \leftarrow G(m' \| (pk^{\mathsf{KEM}})_{[0:256]} \| salt)$
  $c' \leftarrow \mathsf{Encrypt}(pk^{\mathsf{KEM}}, m', \theta')$
  **if** $m' = \perp$ or $c \neq c'$ **then**
    **return** $\kappa \leftarrow K(\sigma, c)$
  **else**
    **return** $\kappa \leftarrow K(m', c)$
  **end if**
**end procedure**

# 소개할 내용들

NIST PQC 공모전
4라운드 암호 평가 결과

SDP, IND-CCA2-secure KEM, DFR
**HQC 안전성**

HQC 설계 사상과 규격
QC 부호, Concatenated 부호

# Quasi-Cyclic 부호에서 정의하는 SDP

# QC 부호의 SDP

**가정**

**순환 구조의 QC 부호 디코딩**이 **랜덤 선형 부호 디코딩**과 **난이도가 비슷**할 것이다.

QC 부호의 SDP에서
오류벡터 $x_1, x_2, e, r_1, r_2$를 찾는 난이도

$\approx$

랜덤 부호의 SDP에서
오류벡터를 찾는 난이도

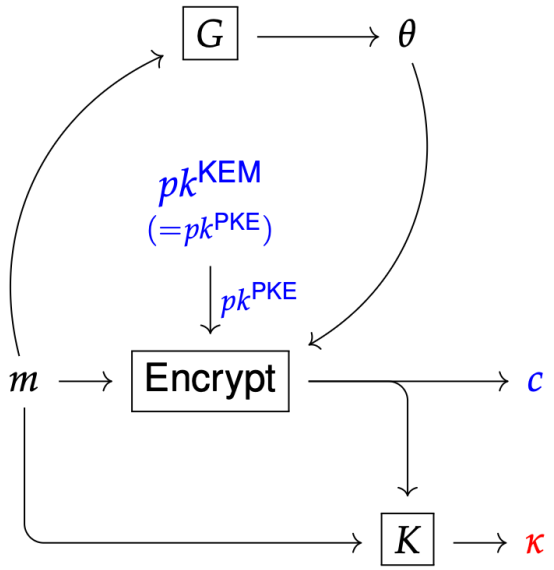
따라서 **ISD**Information Set Decoding를 HQC 기반 문제의 해를 찾는 가장 강력한 알고리듬으로 간주하고, 파라미터를 결정함.

# KEM 구조 안전성 증명

# KEM 구조 안전성

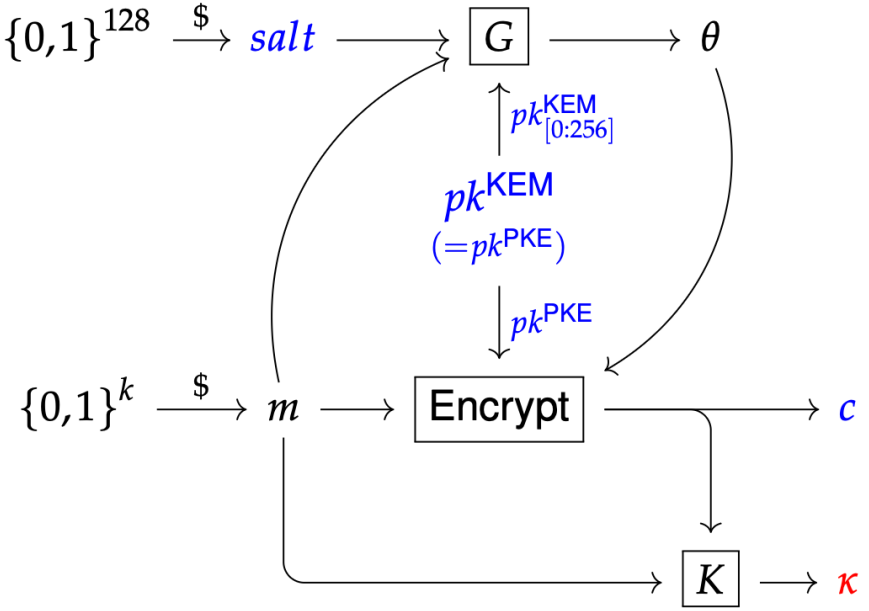
- HQC는 FO[Fujisaki-Okamoto] 변환으로 ROM에서의 IND-CCA2 안전성을 보장함

## FO 변환의 Encap




(a) $\kappa, c \leftarrow \mathsf{Encap}(pk^{\mathsf{KEM}})$

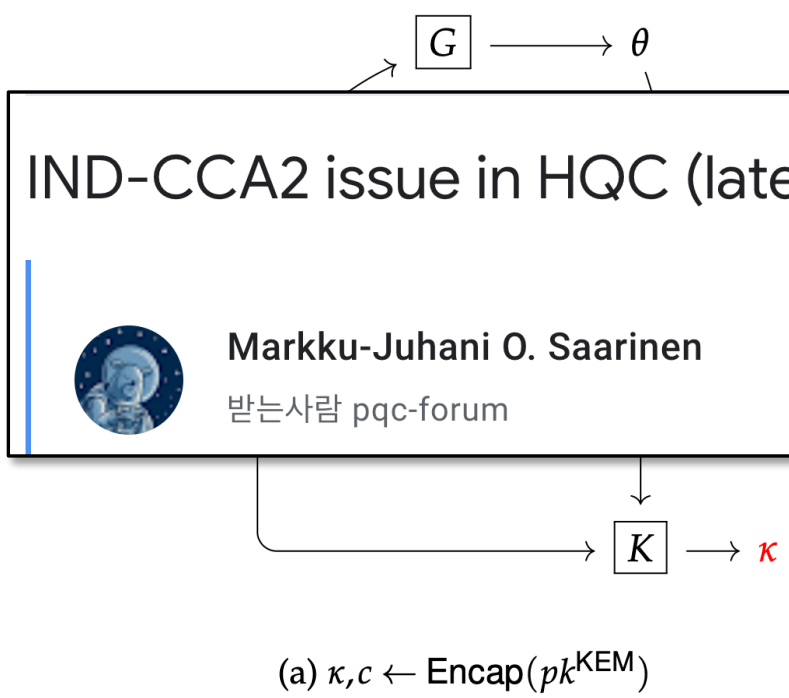
## HQC의 Encap




(a) $\kappa, (c, salt) \leftarrow \mathsf{Encap}(pk^{\mathsf{KEM}})$

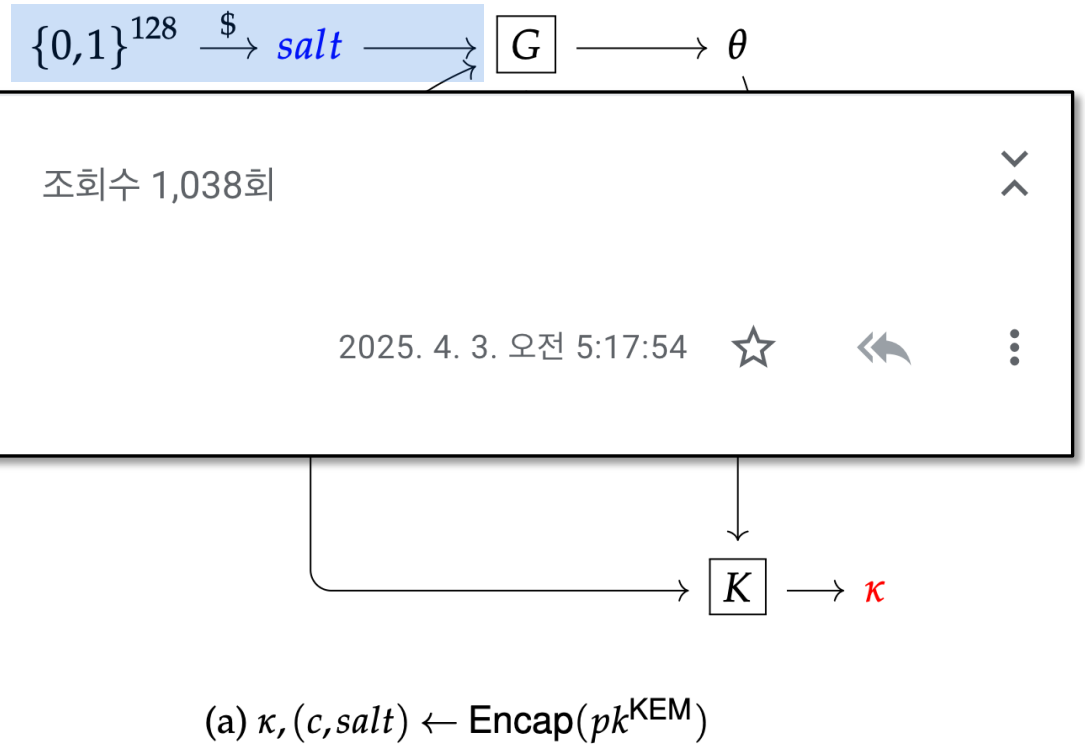
# KEM 구조 안전성

## FO 변환의 Encap




(a) $\kappa, c \leftarrow \mathsf{Encap}(pk^{\mathsf{KEM}})$

## HQC의 Encap




(a) $\kappa, (c, salt) \leftarrow \mathsf{Encap}(pk^{\mathsf{KEM}})$

IND-CCA2 issue in HQC (latest version) 조회수 1,038회

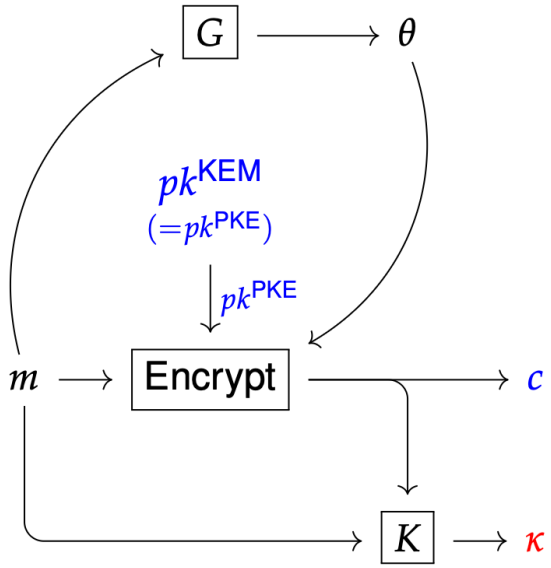
Markku-Juhani O. Saarinen

받는사람 pqc-forum

2025. 4. 3. 오전 5:17:54

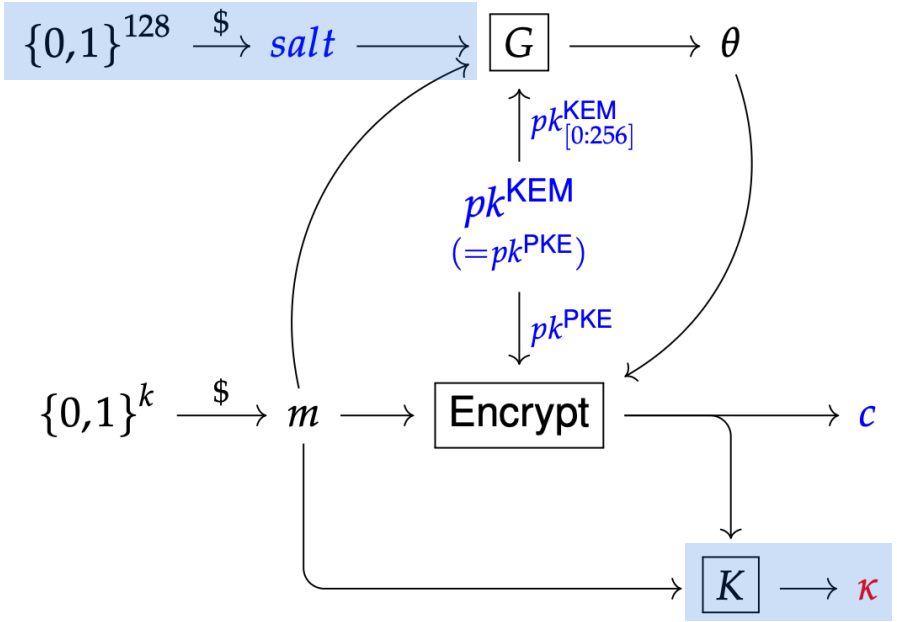
# KEM 구조 안전성

## FO 변환의 Encap



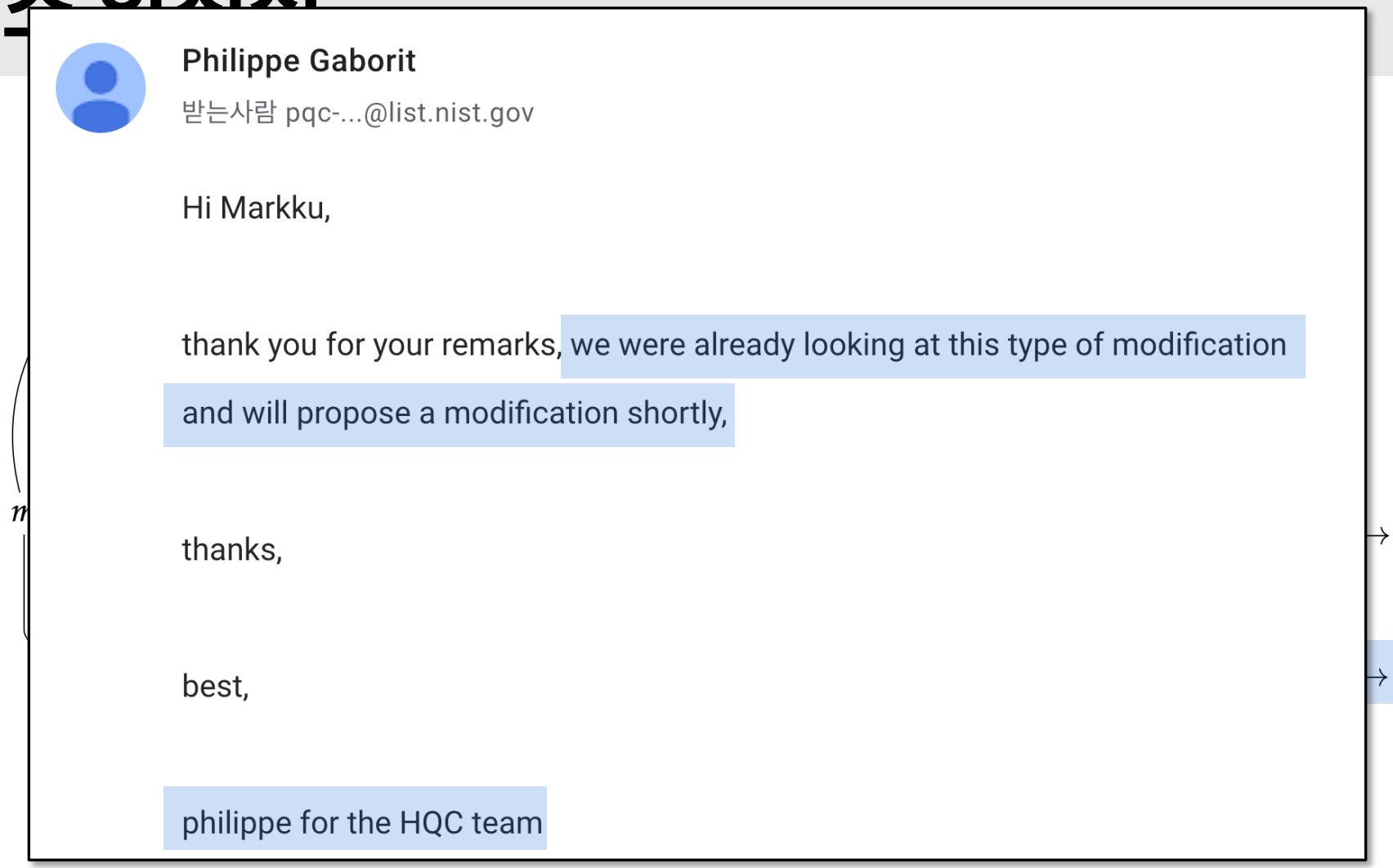

(a) $\kappa, c \leftarrow \mathsf{Encap}(pk^{\mathsf{KEM}})$

## HQC의 Encap




(a) $\kappa, (c, salt) \leftarrow \mathsf{Encap}(pk^{\mathsf{KEM}})$

# KEM 구조 안전성



**Philippe Gaborit**

받는사람 pqc-...@list.nist.gov

Hi Markku,

thank you for your remarks, we were already looking at this type of modification and will propose a modification shortly,

thanks,

best,

philippe for the HQC team

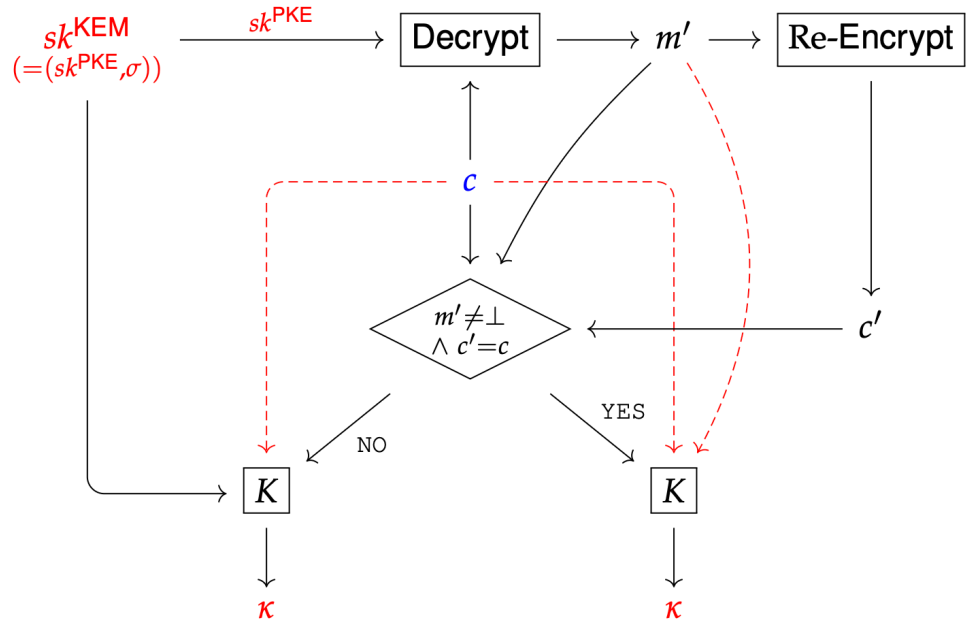
$m$

$\rightarrow c$

$\rightarrow \kappa$

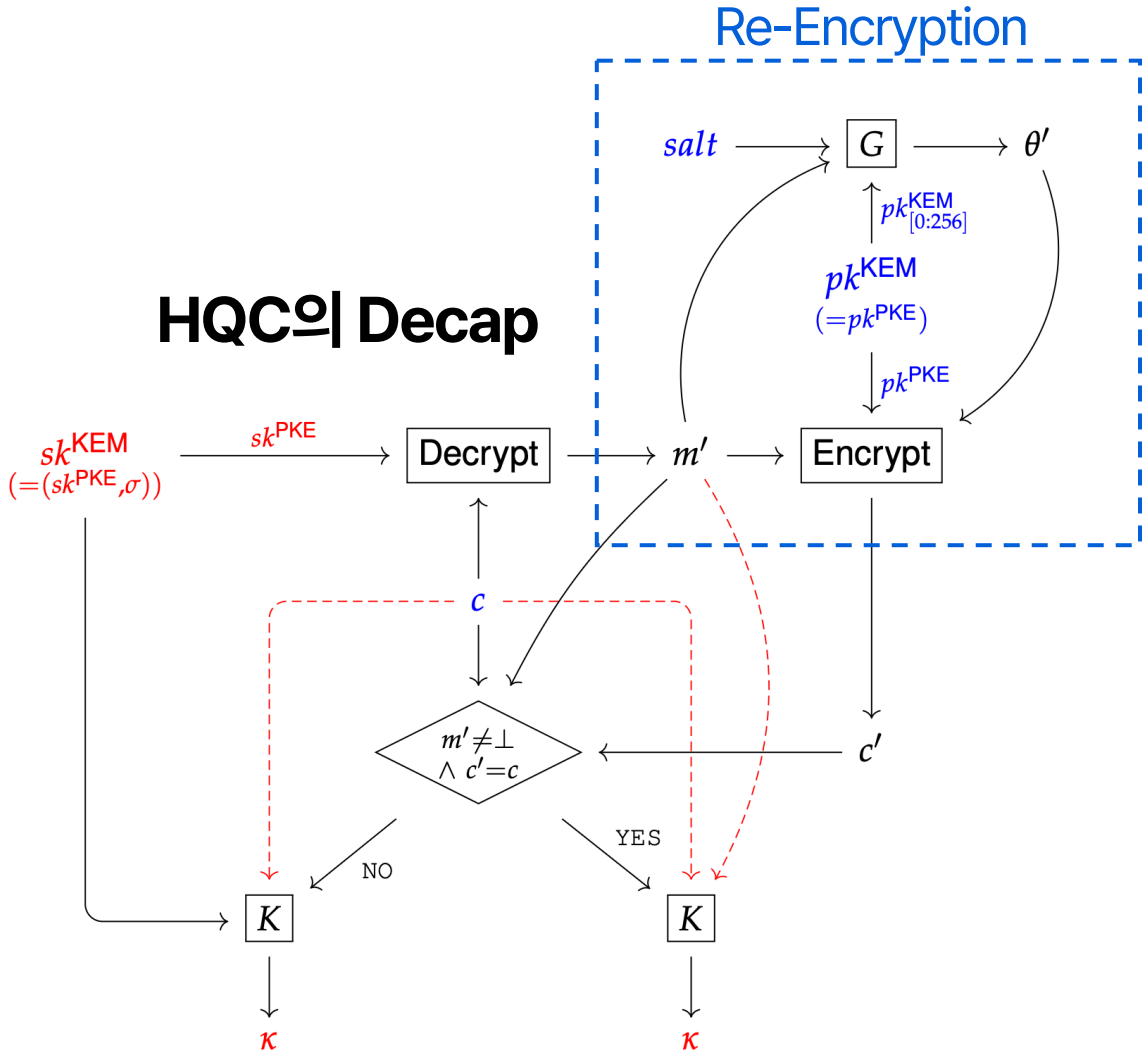
# KEM 구조 안전성

## FO 변환의 Decap




(b) $\kappa \leftarrow \mathrm{Decap}(pk^{KEM}, sk^{KEM}; c)$

## HQC의 Decap




(b) $\kappa \leftarrow \mathrm{Decap}(pk^{KEM}, sk^{KEM}; (c, salt))$

# DFR

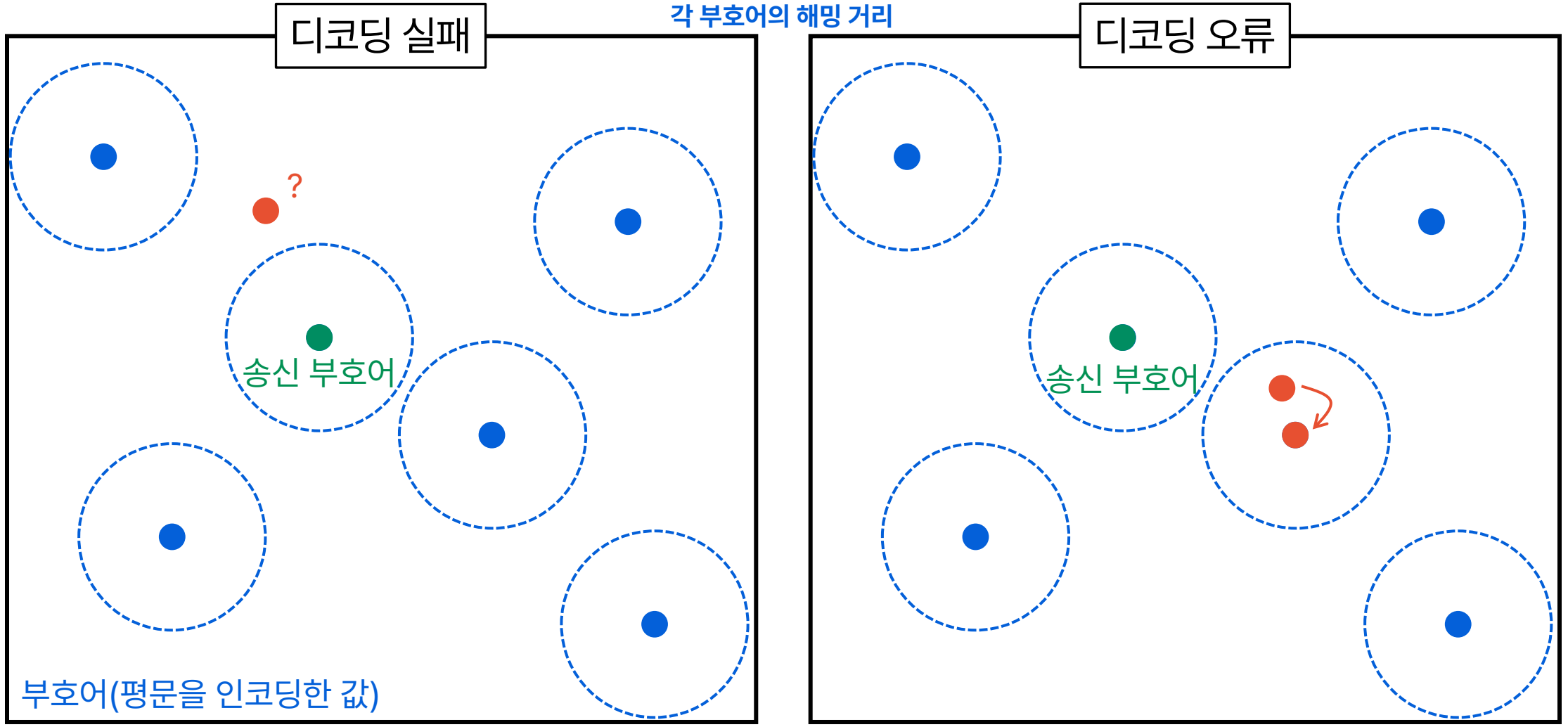
## (Decryption Failure Rate)

# DFR의 정의

$$DFR \coloneqq \Pr\left[\begin{array}{c} pk^{\mathrm{PKE}}, sk^{\mathrm{PKE}} \leftarrow \mathrm{GenKeyPair}^{\mathrm{PKE}}(1^{\lambda}), \\ p \xleftarrow{\$} \{0,1\}^{k}, \\ (u,v) \leftarrow \mathrm{Encrypt}(pk^{\mathrm{PKE}}; p) \end{array} : \mathrm{Decrypt}(sk^{\mathrm{PKE}}; (u,v)) \neq p \right]$$

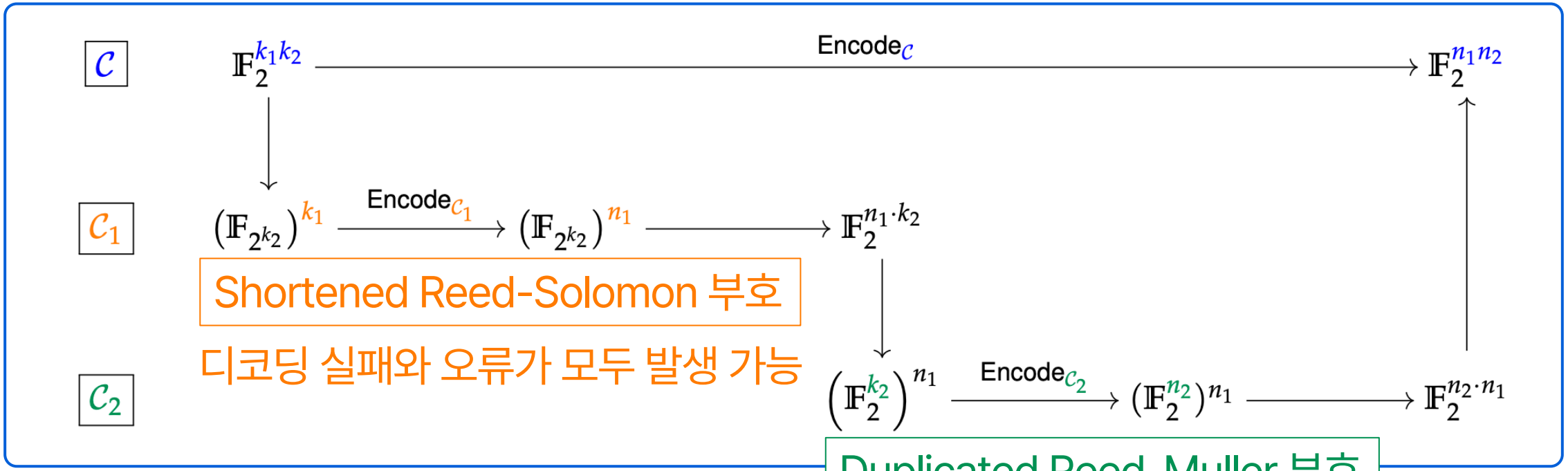
$$= \Pr\left[\begin{array}{c} h \xleftarrow{\$} \{0,1\}^{n}, \\ (x_1, x_2) \xleftarrow{\$} \left(\{0,1\}^{n}_{w_x}\right)^2, \\ e \xleftarrow{\$} \{0,1\}^{n}_{w_e}, \\ p \xleftarrow{\$} \{0,1\}^{k}, \\ e' \leftarrow e + x_1 r_2 + x_2 r_1 \end{array} : \mathrm{Decode}_{\mathcal{C}}\left(\mathrm{Encode}_{\mathcal{C}}(p) + e'_{[0:n_1 n_2]}\right) \neq p \right]$$

# 디코딩 실패Failure와 오류Error

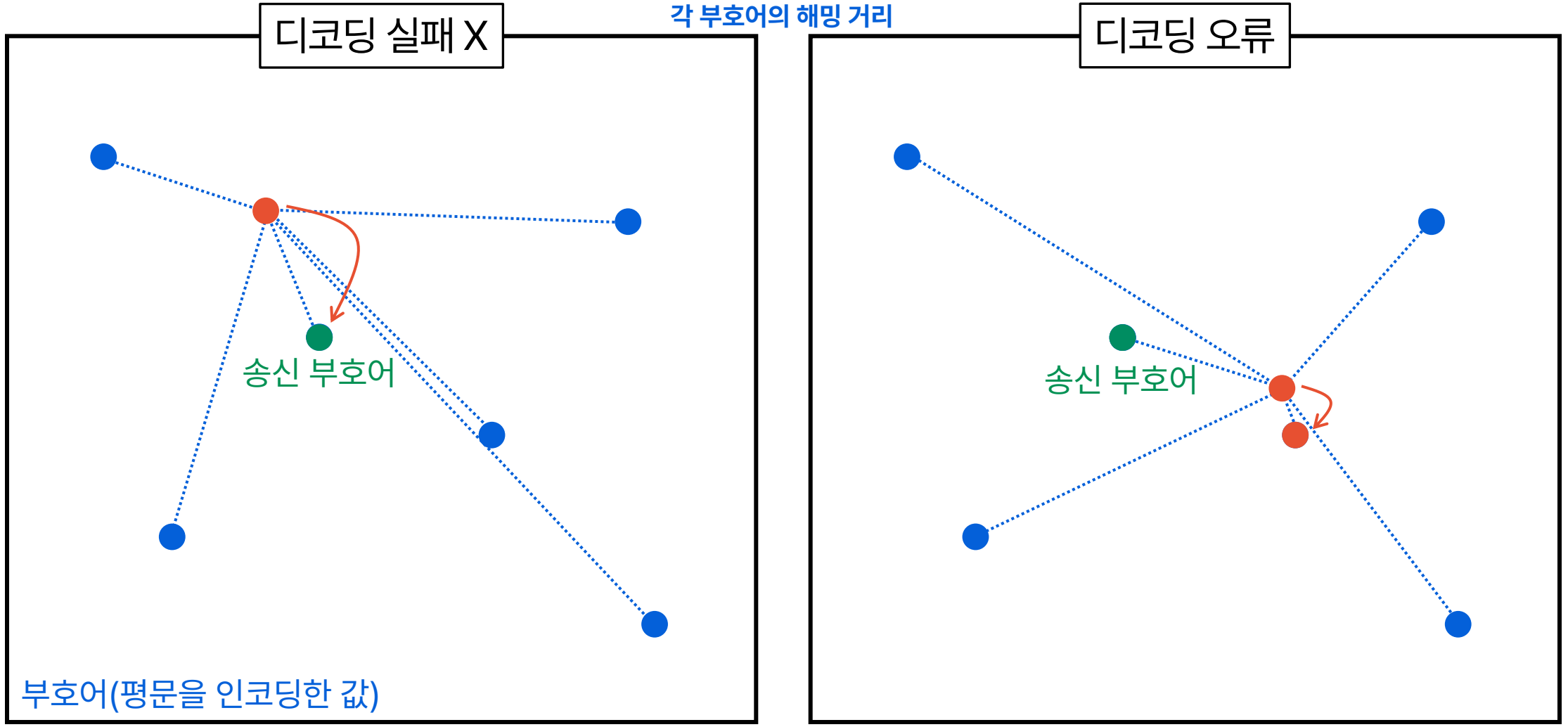


# Concatenated 부호의 DFR

Concatenated 부호 $\mathcal{C}$의 인코딩



# Duplicated Reed-Muller 부호의 디코딩



# DFR

| Parameter | $n_1$ | $n_2$ | $n_1 n_2$ | $n$ | $w$ | $w_r = w_e$ | DFR |
|---|---|---|---|---|---|---|---|
| hqc-128 | 46 | 384 | 17,664 | 17,669 | 66 | 75 | $< 2^{-128}$ |
| hqc-192 | 56 | 640 | 35,840 | 35,851 | 100 | 114 | $< 2^{-192}$ |
| hqc-256 | 90 | 640 | 57,600 | 57,637 | 131 | 149 | $< 2^{-256}$ |

# 마무리

## 오늘 소개한 것들

- NIST PQC 공모전 4라운드 암호 평가 결과
- HQC 설계 사상과 규격 (QC 부호, concatenated 부호)
- HQC 안전성 (QC 부호의 SDP, IND-CCA2-secure KEM, DFR)

## 현재 진행 중인 연구들

- HQC의 DFR을 엄밀히 분석
- HQC의 KEM 구조 안전성 엄밀히 증명

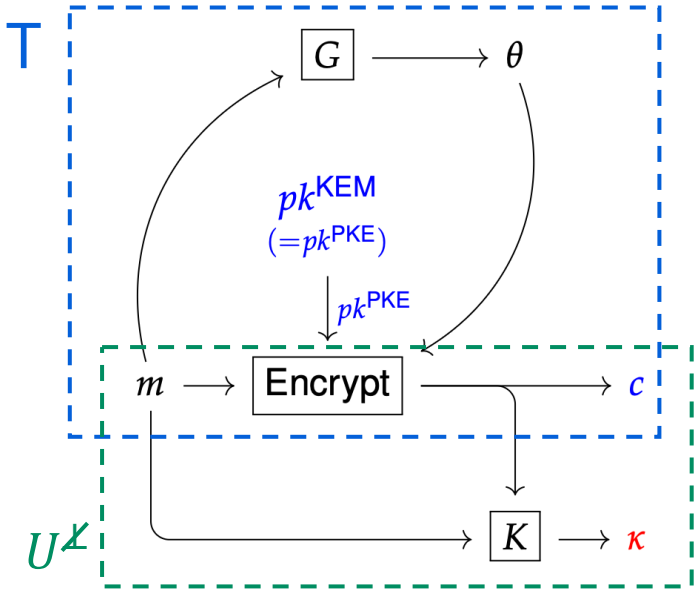
# HQC 파라미터

| | 평문 비트 길이 | Quasi-Cyclic 부호 정보 | Concatenated 부호 정보 |
|---|---|---|---|
| **Parameter** | $k$ | $n, (w_x, w_r, w_e)$ | $n_1 n_2$ |
| hqc–128 | 128 | $17{,}669, (66{,}75{,}75)$ | $17{,}664 (= 46 \times 384)$ |
| hqc–192 | 192 | $35{,}851, (100{,}114{,}114)$ | $35{,}840 (= 56 \times 640)$ |
| hqc–256 | 256 | $57{,}637, (131{,}149{,}149)$ | $57{,}600 (= 90 \times 640)$ |

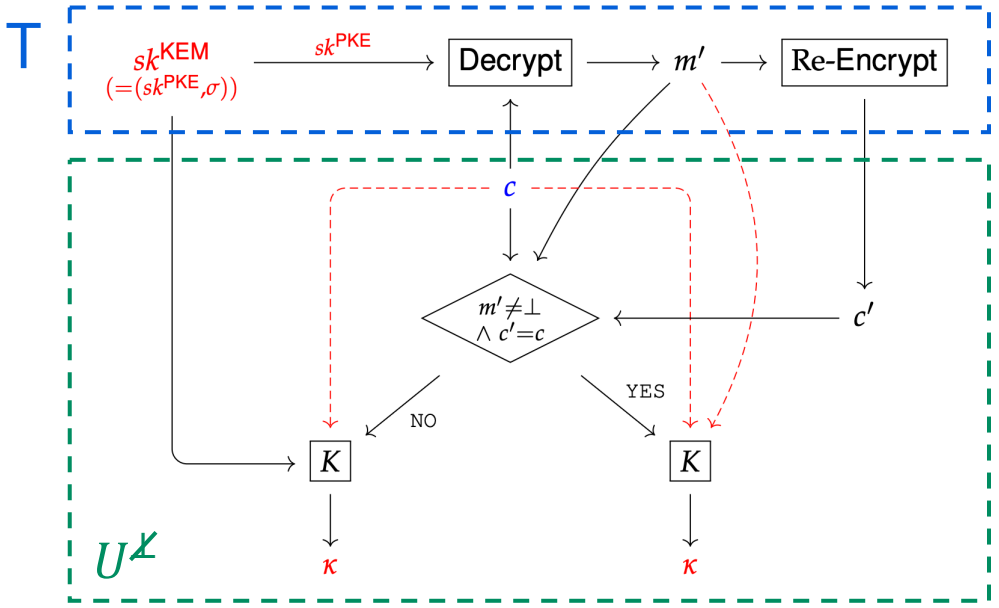
# KEM 구조 안전성

- HQC는 FO[Fujisaki-Okamoto] 변환으로 ROM에서의 IND-CCA2 안전성을 보장함

IND-CPA-secure PKE $\overset{\mathsf{T}}{\Rightarrow}$ OW-PCVA-secure $\mathrm{PKE}_1$ $\overset{\mathsf{U}^{\not\perp}}{\Longrightarrow}$ IND-CCA2-secure KEM.




(a) $\kappa, c \leftarrow \mathsf{Encap}(pk^{\mathsf{KEM}})$




(b) $\kappa \leftarrow \mathsf{Decap}(pk^{\mathsf{KEM}}, sk^{\mathsf{KEM}}; c)$