Anonymity of NIST PQC Round 3 KEMs

Keita Xagawa (草川 恵太) NTT Social Informatics Laboratories

2022/06/04 EUROCRYPT 2022

Backgrounds

QC vs. PQC

Quantum Computers:

- Google: 54 qubits (2019)
- IBM Q53: 53 qubits (2019)
- USTC: 76 qubits (2020)

[Sho94] QC solves factoring/DL easily

[GE21] ERR 10^{-3}, 1ms/1cycle
20Mqubits QC solves RSA2048 in 8h.

→ Consider quantum  !

cf. https://en.wikipedia.org/wiki/List_of_quantum_processors

[Sho94] Shor (FOCS 1994)
[GE21] Gidney, Ekerå (Quantum 2021)

Countermeasures:

1. Looooooooong RSA/DL
2. Post-Quantum Cryptography (PQC)
3. Quantum Cryptography (e.g., QKD)

NIST PQC Round 3 (2020-07-22—)

4 Finalists: KEM

Classic McEliece (code)
CRYSTALS-Kyber (lattice)
NTRU (lattice)
SABER (lattice)

3 Finalists: Sig

CRYSTALS-Dilithium (lattice)
Falcon (lattice)
Rainbow (MQ)

5 Alternates: KEM

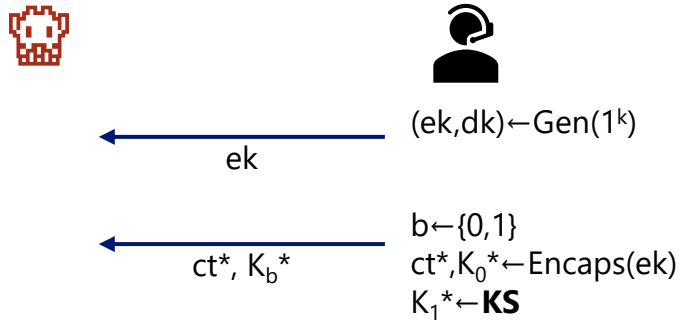
BIKE (code)
FrodoKEM (lattice)
HQC (code)
NTRU Prime (lattice)
SIKE (isogeny)

3 Alternates: Sig

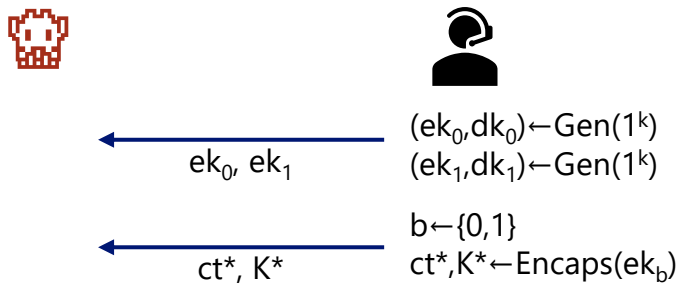
GeMSS (MQ)
Picnic (ZK)
SPHICS+ (Hash)

Anonymity of KEM

Indistinguishability (IND):



Anonymity (ANO):



Applications:

- Anonymous credential
- Auction
- Anonymous AKE, etc

Review of [GMP22]: ANON in QROM

NAME	KEM			PKE
	IND	ANO	CF	ANO
Classic McEliece	Y	**?**	**N**	**?**
Kyber	**?**	**?**	**?**	**?**
NTRU	Y	**?**	**?**	**?**
Saber	**?**	**?**	**?**	**?**
FrodoKEM (+Kyber'&Saber')	Y	**Y**	**Y**	**Y**

SPR=Strong Pseudorandomness, ANO=Anonymity
CF=Collision Freeness, ROB=Robustness

Show anonymity of FO$^{\not\perp}$

Problems:

1. Hard to simul. two dec. oracles
   - CME: not collision-free
   - NTRU: SXY uses H(m)
2. Need to avoid tweaks
   - Kyber/Saber: 'pre-key' and 'nest'

[GMP22] Grubbs, Maram, Paterson (EUROCYRPT 2022, https://eprint.iacr.org/2021/708)

Our result

Our Results – 1

1. Strong Pseudorandom (SPR) → Anonymous
2. KEM/DEM framework for SPR HPKE
    1. Smooth SPR-CCA KEM$^{\perp\!\!\!\perp}$ and SPR-otCCA DEM
    2. Sparse SPR-CCA KEM$^{\perp}$ and INT-CTXT, SPR-otCCA DEM
3. Strongly Disjoint-Simulatable PKE
   –(SXY etc.)→ Smooth/Sparse SPR-CCA KEM
4. Apply them to NIST PQC Round 3 KEM

[CS03] Cramer, Shoup (SIAM J. Comput. 33(1), 2003)
[Moh10] Mohassel (ASIACRYPT 2010)
[GRP22] Grubbs, Maram, Paterson (EUROCRYPT 2022)

Our Results – 2

NAME	KEM			PKE
	IND	ANO	CF	ANO
Classic McEliece	Y	**Y**	N	**Y**
Kyber	?	?	?	?
NTRU	Y	**Y**	**Y**	**Y**
Saber	?	?	?	?
FrodoKEM (+Kyber'&Saber')	Y	Y	Y	Y

SPR=Strong Pseudorandomness, ANO=Anonymity
CF=Collision Freeness, ROB=Robustness

NAME	KEM			PKE
	IND	ANO	CF	ANO
BIKE	Y	**Y**	**Y**	**Y**
HQC-128/196	Y	**Y**	**Y**	**Y**
HQC-256	Y	**N**	**Y**	**N**
sntrupr of NTRU Prime	**?**	**?**	**?**	**?**
ntrulpr of NTRU Prime	Y	**Y**	**Y**	**Y**
SIKE	Y	**Y**	**Y**	**Y**

SXY: SDS ⇝ SPR-CCA → ANO-CCA

SXY [SXY18]

Deterministic PKE

Gen$(1^k) \to$ (ek,dk)
Enc(ek,m)$\to$ct
Dec(dk,ct)$\to$m/$\perp$

PKE is Strongly Disjoint-Siml.

1. **Enc**(ek,U(M)) $\approx_c$ Sim(1^k)

2. Pr[c$\leftarrow$Sim(1^k): c$\in$**Enc**(ek,M)] is negl.

KEM = SXY[PKE,H,H′]

Gen(1^k)
(ek,dk)$\leftarrow$**Gen**(1^k), seed$\leftarrow\{0,1\}^k$
return ek and (dk,ek,seed)

Encaps(ek;m)
ct$\leftarrow$**Enc**(ek,m), K$\leftarrow$H(m)
return ct and K

Decaps((dk,ek,seed),ct)
m′ $\leftarrow$**Dec**(dk,ct)
If ct=**Enc**(ek,m′) then K$\leftarrow$H(m′)
Else K$\leftarrow$H′(seed,ct)
return K

[SXY18] Saito, Xagawa, Yamakawa (EUROCRYPT 2018)

SDS ⇝ IND-CCA [SXY18]

PKE is SDS

1. **Enc**(ek,U(M)) $\approx_c$ Sim(1^k)
2. Pr[c←Sim(1^k): c∈**Enc**(ek,M)] is negl.

KEM = SXY[PKE,H,H']

Gen(1^k):
(ek,dk)←**Gen**(1^k)
seed←{0,1}^{k}

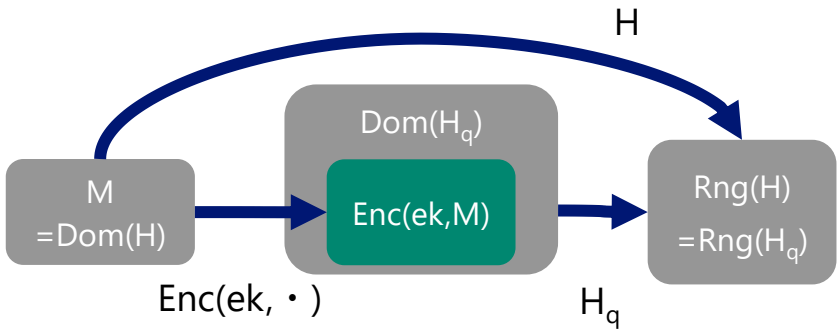
Encaps(ek;m)
ct←**Enc**(ek,m)
K←H(m)

Decaps(dk,ct)
m'←**Dec**(dk,ct)
If ct=**Enc**(ek,m')
 then K←H(m')
else K←H'(seed,ct)

Simulate Decaps w/ H

Let H(m) := H_q(**Enc**(ek,m))

- **Decaps**(ct) = H_q(ct)
- Dom(H_q) \ Enc(ek,M) is inaccessible
  → H_q(Sim(1^k)) looks random



SDS ⇝ IND-CCA [SXY18]

NTT

PKE is SDS

1. **Enc**(ek,U(M)) $\approx_c$ Sim(1^k)
2. Pr[c←Sim(1^k): c∈**Enc**(ek,M)] is negl.

KEM = SXY[PKE,H,H']

Gen(1^k):
(ek,dk)←**Gen**(1^k)
seed←{0,1}^{k}

Encaps(ek;m)
ct←**Enc**(ek,m)
K←H(m)

Decaps(dk,ct)
m'←**Dec**(dk,ct)
If ct=**Enc**(ek,m')
 then K←H(m')
else K←H'(seed,ct)

Simulate Decaps w/ H

H(m) := H_q(**Enc**(ek,m))
Decaps(ct) = H_q(ct)
Dom(H_q) \ Enc(ek,M) is inaccessible
→ H_q(Sim(1^k)) looks random

SDS ⇝ IND-CCA

{(ek,ct,K): ct←**Enc**(ek,m),K←H(m)} w/ dk
$\approx_s$ {(ek,ct,K): ct←**Enc**(ek,m),K←H_q(ct)} w/ H_q
$\approx_c$ {(ek,ct,K): ct←Sim,K←H_q(ct)} w/ H_q
$\approx_s$ {(ek,ct,K): ct←Sim,K←U} w/ H_q
… $\approx_c$ {(ek,ct,K): ct←**Enc**(ek,m),K←U} w/ dk

Attempt: SDS ⇝ ANON-CCA

NTT

PKE is SDS

1. **Enc**(ek,U(M)) $\approx_c$ Sim(1^k)
2. Pr[c←Sim(1^k): c∈**Enc**(ek,M)] is negl.

KEM = SXY[PKE,H,H']

Gen(1^k):
(ek,dk)←**Gen**(1^k)
seed←{0,1}^{k}

Encaps(ek;m)
ct←**Enc**(ek,m)
K←H(m)

Decaps(dk,ct)
m'←**Dec**(dk,ct)
If ct=**Enc**(ek,m')
 then K←H(m')
else K←H'(seed,ct)

Need to simul. two Decaps

Let H(m) := H_q(**Enc**(ek,m)) ?

[GRM21] Use H(m,c)

H(m,c) := H_i(c) if **Enc**(ek_i,m)=c or H_q(c)
Decaps0(ct) = H_0(ct)
Decaps1(ct) = H_1(ct)

Problem:

- Require collision-freeness
- Need to modify H

SPR-CCA → ANO-CCA [folklore]

NTT

KEM is Strongly PR.

$\{(ek,ct,K): (ct,K) \leftarrow \mathbf{Encaps}(ek)\}$

$\approx_c \{(ek,ct,K): ct \leftarrow Sim(1^k), K \leftarrow U\}$

KEM is Anonymous

$\{(ek_0,ek_1,ct_0,K_0): (ct_0,K_0) \leftarrow \mathbf{Encaps}(ek_0)\}$

$\approx_c \{(ek_0,ek_1,ct_1,K_1): (ct_1,K_1) \leftarrow \mathbf{Encaps}(ek_1)\}$

SPR-CCA → ANO-CCA

$\{(ek_0,ek_1,ct_0,K_0): (ct_0,K_0) \leftarrow \mathbf{Encaps}(ek_0)\}$

$\approx_c \{(ek_0,ek_1,ct,K): ct \leftarrow Sim(1^k), K \leftarrow U\}$

☜ reduced to SPR-CCA on ek_0

$\approx_s \{(ek_0,ek_1,ct,K): ct \leftarrow Sim(1^k), K \leftarrow U\}$

$\approx_c \{(ek_0,ek_1,ct_1,K_1): (ct_1,K_1) \leftarrow \mathbf{Encaps}(ek_1)\}$

☜ reduced to SPR-CCA on ek_1

SDS ⇝ IND-CCA [SXY18]

NTT

PKE is Strongly Disjoint-Siml.

1. **Enc**(ek,U(M)) $\approx_c$ Sim(1^k)
2. Pr[c←Sim(1^k): c∈**Enc**(ek,M)] is negl.

KEM = SXY[PKE,H,H']

Gen(1^k):
(ek,dk)←**Gen**(1^k)
seed←{0,1}^{k}

Encaps(ek;m)
ct←**Enc**(ek,m)
K←H(m)

Decaps(dk,ct)
m'←**Dec**(dk,ct)
If ct=**Enc**(ek,m')
 then K←H(m')
else K←H'(seed,ct)

Simulate Decaps w/ H

H(m) := H_q(**Enc**(ek,m))
Decaps(ct) = H_q(ct)
Dom(H_q) \ Enc(ek,M) is inaccessible
→ H_q(Sim(1^k)) looks random

SDS ⇝ IND-CCA

{(ek,ct,K): ct←**Enc**(ek,m),K←H(m)} w/ dk
$\approx_s$ {(ek,ct,K): ct←**Enc**(ek,m),K←H_q(ct)} w/ H_q
$\approx_c$ {(ek,ct,K): ct←Sim,K←H_q(ct)} w/ H_q
$\approx_s$ {(ek,ct,K): ct←Sim,K←U} w/ H_q
… $\approx_c$ {(ek,ct,K): ct←**Enc**(ek,m),K←U} w/ dk

SDS ⇝ SPR-CCA ~~IND-CCA~~ a la [SXY18]

NTT

PKE is Strongly Disjoint-Siml.

1. **Enc**(ek,U(M)) $\approx_c$ Sim(1^k)
2. Pr[c←Sim(1^k): c∈**Enc**(ek,M)] is negl.

KEM = SXY[PKE,H,H']

Gen(1^k):
(ek,dk)←**Gen**(1^k)
seed←{0,1}^{k}

Encaps(ek;m)
ct←**Enc**(ek,m)
K←H(m)

Decaps(dk,ct)
m'←**Dec**(dk,ct)
If ct=**Enc**(ek,m')
 then K←H(m')
else K←H'(seed,ct)

Simulate Decaps w/ H

H(m) := H_q(**Enc**(ek,m))
Decaps(ct) = H_q(ct)
Dom(H_q) \ Enc(ek,M) is inaccessible
→ H_q(Sim(1^k)) looks random

SDS ⇝ SPR-CCA ~~IND-CCA~~

{(ek,ct,K): ct←**Enc**(ek,m),K←H(m)} w/ dk
$\approx_s$ {(ek,ct,K): ct←**Enc**(ek,m),K←H_q(ct)} w/ H_q
$\approx_c$ {(ek,ct,K): ct←Sim,K←H_q(ct)} w/ H_q
$\approx_s$ {(ek,ct,K): ct←Sim,K←U} w/ H_q
$\approx_s$ {(ek,ct,K): ct←Sim,K←U} w/ dk
~~$\approx_\epsilon$ {(ek,ct,K): ct←**Enc**(ek,m),K←U} w/ dk~~

Summary

Summary – 1

1. Strong Pseudorandom (SPR) → Anonymous
2. KEM/DEM framework for SPR HPKE
    1. Smooth SPR-CCA KEM$^{\perp\!\!\!\perp}$ and SPR-otCCA DEM
    2. Sparse SPR-CCA KEM$^{\perp}$ and INT-CTXT, SPR-otCCA DEM
3. Strongly Disjoint-Simulatable PKE
   –(SXY etc.)→ Smooth/Sparse SPR-CCA KEM
4. Apply them to NIST PQC Round 3 KEM

[CS03] Cramer, Shoup (SIAM J. Comput. 33(1), 2003)
[Moh10] Mohassel (ASIACRYPT 2010)
[GRP22] Grubbs, Maram, Paterson (EUROCRYPT 2022)

Summary – 2

NAME	KEM			PKE
	IND	ANO	CF	ANO
Classic McEliece	Y	**Y**	N	**Y**
Kyber	?	?	?	?
NTRU	Y	**Y**	**Y**	**Y**
Saber	?	?	?	?
FrodoKEM (+Kyber'&Saber')	Y	Y	Y	Y

SPR=Strong Pseudorandomness, ANO=Anonymity
CF=Collision Freeness, ROB=Robustness

NAME	KEM			PKE
	IND	ANO	CF	ANO
BIKE	Y	**Y**	**Y**	**Y**
HQC-128/196	Y	**Y**	**Y**	**Y**
HQC-256	Y	**N**	**Y**	**N**
sntrupr of NTRU Prime	**?**	**?**	**?**	**?**
ntrulpr of NTRU Prime	Y	**Y**	**Y**	**Y**
SIKE	Y	**Y**	**Y**	**Y**

Open Problems:
1. Show SPR/ANO of Kyber/Saber/sntrupr of NTRU Prime w/o quantum indiff.
2. Show SPR/ANO of FO$^{\not\perp}$ *tightly* as IND [BHHHP19]+[KSSSS20]