Group Action Key Encapsulation and Non-Interactive Key Exchange in the QROM

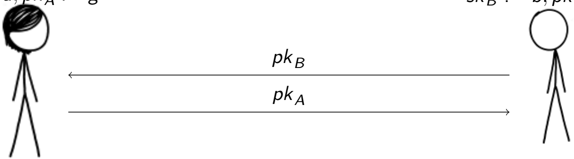
J. Duman, D. Hartmann, E. Kiltz, S. Kunzweiler, J. Lehmann, D. Riepel

Ruhr-University Bochum

6. December 2022

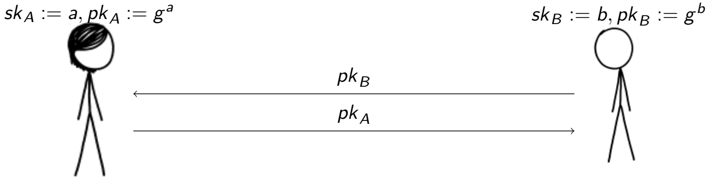
Non-Interactive Key Exchange [DH76]

$sk_A := a, pk_A := g^a$ $\quad$ $sk_B := b, pk_B := g^b$



$(pk_B)^a = (g^b)^a$ $\quad$ $(pk_A)^b = (g^a)^b$

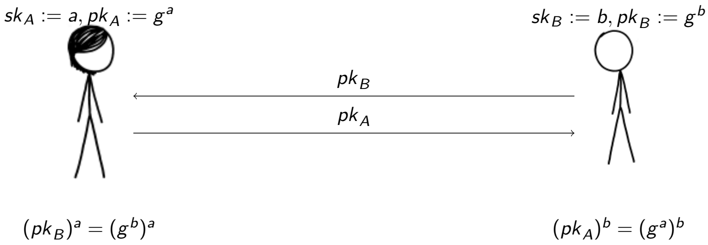
Non-Interactive Key Exchange [DH76]



$(pk_B)^a = (g^b)^a$ $\quad$ $(pk_A)^b = (g^a)^b$

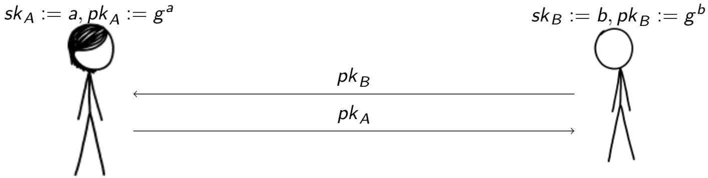
- passively secure under Decisional Diffie-Hellman assumption

Non-Interactive Key Exchange [DH76]



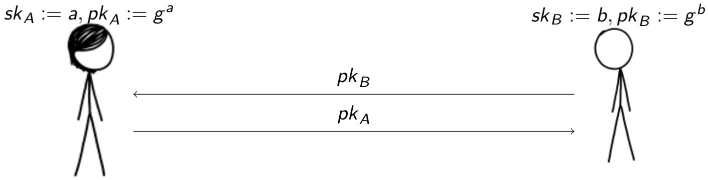
- passively secure under Decisional Diffie-Hellman assumption
- $(g^a, g^b, g^{ab}) \approx_c (g^a, g^b, g^u)$ for $a, b, u \leftarrow \mathbb{Z}_p$

Non-Interactive Key Exchange



$$H(g^a, g^b, g^{ab})$$

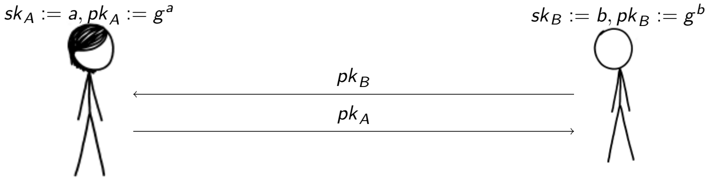
Non-Interactive Key Exchange



$$\mathsf{H}(g^a, g^b, g^{ab})$$

- actively secure under *Strong* Computational Diffie-Hellman assumption [ABR01] in the random oracle model

Non-Interactive Key Exchange

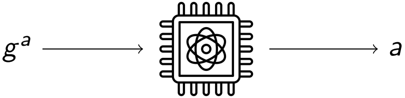


$\mathsf{H}(g^a, g^b, g^{ab})$

- actively secure under *Strong* Computational Diffie-Hellman assumption [ABR01] in the random oracle model
- Assumption: difficult to compute g^{ab} given g^a, g^b and oracle

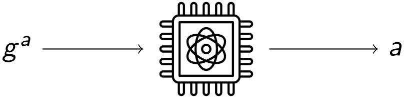
$$\text{GA-DDH}_{g^a}(g_1, g_2) := \begin{cases} 1 \text{ if } g_1^a = g_2 \\ 0 \text{ else} \end{cases} .$$

NIKE in a Quantum World



- Lattice and Code-based Crypto are popular alternatives for PKE and AKE, but efficient NIKE is an open research question
- Isogeny-based cryptography, like CSIDH [CLM+18], offer candidate for quantum-resistant NIKE

NIKE in a Quantum World



- Lattice and Code-based Crypto are popular alternatives for PKE and AKE, but efficient NIKE is an open research question
- Isogeny-based cryptography, like CSIDH [CLM$^+$18], offer candidate for quantum-resistant NIKE
- we use the group action abstraction

Cryptographic Group Actions [ADMP20]

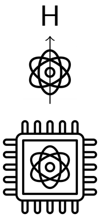
- Let $(\mathcal{G}, \cdot)$ be a group with identity element $e \in \mathcal{G}$, and $\mathcal{X}$ a set. The map $\star \colon \mathcal{G} \times \mathcal{X} \to \mathcal{X}$ is a group action if it satisfies the following properties:
- 1. Identity: $e \star x = x$ for all $x \in \mathcal{X}$.
- 2. Compatibility: $(g \cdot h) \star x = g \star (h \star x)$ for all $g, h \in \mathcal{G}$ and $x \in \mathcal{X}$.

Cryptographic Group Actions [ADMP20]

- Let $(\mathcal{G}, \cdot)$ be a group with identity element $e \in \mathcal{G}$, and $\mathcal{X}$ a set. The map $\star\colon \mathcal{G} \times \mathcal{X} \to \mathcal{X}$ is a group action if it satisfies the following properties:
- 1. Identity: $e \star x = x$ for all $x \in \mathcal{X}$.
- 2. Compatibility: $(g \cdot h) \star x = g \star (h \star x)$ for all $g, h \in \mathcal{G}$ and $x \in \mathcal{X}$.
- Additional assumptions:
- $\mathcal{G}$ and $\mathcal{X}$ are finite, $\mathcal{G}$ is commutative
- $\star\colon \mathcal{G} \times \mathcal{X} \to \mathcal{X}$ is regular
- distinguished element $\tilde{x} \in \mathcal{X}$ (" origin ")

Quantum Random Oracle Model [BDF+11]

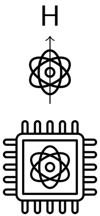
$$\mathsf{H}\left(\frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle\right)$$



- Quantum computers can execute hash functions in quantum superposition

Quantum Random Oracle Model [BDF+11]

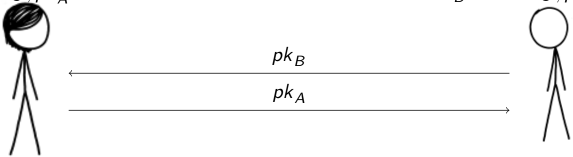
$$\mathsf{H}\left(\frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle\right)$$



- Quantum computers can execute hash functions in quantum superposition
- therefore need to extend this in the ROM by allowing quantum access

NIKE from Group Actions

$sk_A := a \leftarrow \mathcal{G}, pk_A := a \star \tilde{x}$ $\qquad$ $sk_B := b \leftarrow \mathcal{G}, pk_B := b \star \tilde{x}$

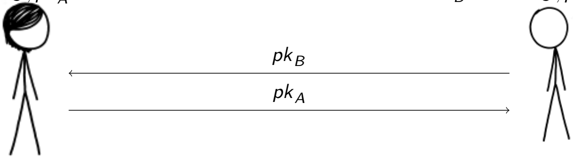


$\mathsf{H}(a \star \tilde{x}, b \star \tilde{x}, ab \star \tilde{x})$

- This work: necessity of a quantum-accessible version of the Strong CDH assumption in the group action setting for active security in the QROM
- proof from such an assumption

NIKE from Group Actions

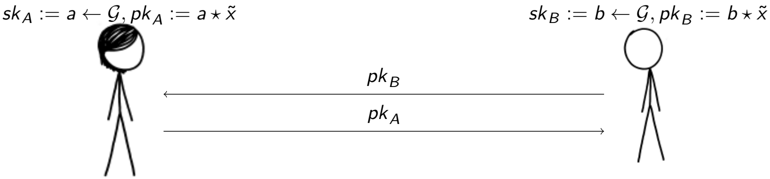
$sk_A := a \leftarrow \mathcal{G}, pk_A := a \star \tilde{x}$ $\qquad$ $sk_B := b \leftarrow \mathcal{G}, pk_B := b \star \tilde{x}$



$$\mathrm{H}(a \star \tilde{x}, b \star \tilde{x}, ab \star \tilde{x})$$

- This work: necessity of a quantum-accessible version of the Strong CDH assumption in the group action setting for active security in the QROM
- proof from such an assumption
- Constructions with weaker assumptions
- Security of the corresponding KEMs

NIKE from Group Actions



$\mathrm{H}(a \star \tilde{x}, b \star \tilde{x}, ab \star \tilde{x})$

- This work: necessity of a quantum-accessible version of the Strong CDH assumption in the group action setting for active security in the QROM
- proof from such an assumption
- Constructions with weaker assumptions
- Security of the corresponding KEMs
- in particular first construction and proof of NIKE from Group Action CDH assumption with active security in the QROM

Group Action Hashed ElGamal

<u>Gen</u>

$sk := g \leftarrow \mathcal{G}$
$pk := g \star \tilde{x}$
return (pk, sk)

<u>Encaps(pk)</u>

$r \leftarrow \mathcal{G}$
$\mathrm{ct} := r \star \tilde{x}$
$K := \mathrm{H}(\mathrm{ct}, r \star pk)$
return (ct, K)

<u>Decaps(sk, ct)</u>

$z := sk \star \mathrm{ct}$
$K := \mathrm{H}(\mathrm{ct}, z)$
return K

- CCA security of KEM $\approx$ active security of NIKE

Group Action Strong CDH assumption variants

- difficult to compute $gh \star \tilde{x}$ given $g \star \tilde{x}$, $h \star \tilde{x}$ and access to decision oracle

  $$\text{GA-DDH}_g(x_1, x_2) := \begin{cases} 1 \text{ if } g \star x_1 = x_2 \\ 0 \text{ else} \end{cases}$$

- GA-Fully-Quantum-Strong-CDH = both inputs x_1 and x_2 are quantum-accessible

Group Action Strong CDH assumption variants

- difficult to compute $gh \star \tilde{x}$ given $g \star \tilde{x}$, $h \star \tilde{x}$ and access to decision oracle
  $$\text{GA-DDH}_g(x_1, x_2) := \begin{cases} 1 \text{ if } g \star x_1 = x_2 \\ 0 \text{ else} \end{cases}$$
- GA-Fully-Quantum-Strong-CDH = both inputs x_1 and x_2 are quantum-accessible
- GA-Partially-Quantum-Strong-CDH = only second input x_2 is quantum-accessible

Group Action Strong CDH assumption variants

- difficult to compute $gh \star \tilde{x}$ given $g \star \tilde{x}$, $h \star \tilde{x}$ and access to decision oracle

  $$\text{GA-DDH}_g(x_1, x_2) := \begin{cases} 1 \text{ if } g \star x_1 = x_2 \\ 0 \text{ else} \end{cases}$$

- GA-Fully-Quantum-Strong-CDH = both inputs x_1 and x_2 are quantum-accessible
- GA-Partially-Quantum-Strong-CDH = only second input x_2 is quantum-accessible
- GA-Strong-CDH = only classical access to x_1 and x_2

Group Action Strong CDH assumption variants

- difficult to compute $gh \star \tilde{x}$ given $g \star \tilde{x}$, $h \star \tilde{x}$ and access to decision oracle

  $$\text{GA-DDH}_g(x_1, x_2) := \begin{cases} 1 \text{ if } g \star x_1 = x_2 \\ 0 \text{ else} \end{cases}$$

- GA-Fully-Quantum-Strong-CDH = both inputs x_1 and x_2 are quantum-accessible
- GA-Partially-Quantum-Strong-CDH = only second input x_2 is quantum-accessible
- GA-Strong-CDH = only classical access to x_1 and x_2
- GA-CDH = no oracle access

Necessity of the GA Partially Quantum Strong CDH assumption

$\underline{\mathcal{B}^{\mathsf{Decaps},\mathsf{H}}(pk, c^*, K)}$	$\underline{\mathsf{GA\text{-}DDH}_g(x_1, x_2)}$
$\hat{g} \leftarrow \mathcal{G} \setminus \{e\}$	**if** $x_1 = c^*$
$z \leftarrow \mathcal{A}^{\mathsf{GA\text{-}DDH}_g(\cdot,\lvert\cdot\rangle)}(pk, c^*)$	**return** $[[\mathsf{Decaps}(\hat{g}\star x_1) = \mathsf{H}(\hat{g}\star x_1, \hat{g}\star x_2)]]$
return $[[K \neq \mathsf{H}(c^*, z)]]$	**return** $[[\mathsf{Decaps}(x_1) = \mathsf{H}(x_1, x_2)]]$

- $\mathsf{Decaps}(x_1)$ evaluates to $\mathsf{H}(x_1, g \star x_1) \implies$ inputs of H are valid DH tuple
- challenge c^* can't be queried on Decaps $\implies$ shift by $\hat{g}$

Necessity of the GA Partially Quantum Strong CDH assumption

$\underline{\mathcal{B}^{\mathsf{Decaps},\mathsf{H}}(pk, c^*, K)}$	$\underline{\mathsf{GA\text{-}DDH}_g(x_1, x_2)}$
$\hat{g} \leftarrow \mathcal{G} \setminus \{e\}$	**if** $x_1 = c^*$
$z \leftarrow \mathcal{A}^{\mathsf{GA\text{-}DDH}_g(\cdot, \vert\cdot\rangle)}(pk, c^*)$	**return** $[[\mathsf{Decaps}(\hat{g} \star x_1) = \mathsf{H}(\hat{g} \star x_1, \hat{g} \star x_2)]]$
return $[[K \neq \mathsf{H}(c^*, z)]]$	**return** $[[\mathsf{Decaps}(x_1) = \mathsf{H}(x_1, x_2)]]$

- $\mathsf{Decaps}(x_1)$ evaluates to $\mathsf{H}(x_1, g \star x_1) \implies$ inputs of H are valid DH tuple
- challenge c^* can't be queried on Decaps $\implies$ shift by $\hat{g}$
- x_1 is used in Decaps $\implies$ needs to be classical

Necessity of the GA Partially Quantum Strong CDH assumption

$\underline{\mathcal{B}^{\text{Decaps},\mathsf{H}}(pk, c^*, K)}$	$\underline{\text{GA-DDH}_g(x_1, x_2)}$
$\hat{g} \leftarrow \mathcal{G} \setminus \{e\}$	**if** $x_1 = c^*$
$z \leftarrow \mathcal{A}^{\text{GA-DDH}_g(\cdot, \lvert\cdot\rangle)}(pk, c^*)$	**return** $[[\text{Decaps}(\hat{g} \star x_1) = \mathsf{H}(\hat{g} \star x_1, \hat{g} \star x_2)]]$
return $[[K \neq \mathsf{H}(c^*, z)]]$	**return** $[[\text{Decaps}(x_1) = \mathsf{H}(x_1, x_2)]]$

- $\text{Decaps}(x_1)$ evaluates to $\mathsf{H}(x_1, g \star x_1)$ $\implies$ inputs of H are valid DH tuple
- challenge c^* can't be queried on Decaps $\implies$ shift by $\hat{g}$
- x_1 is used in Decaps $\implies$ needs to be classical
- x_2 used in the quantum-accessible random oracle $\implies$ can be quantum

Oneway-to-hiding [Unr14]

- $\mathsf{H}(x^*)$ look random to the adversary, if it doesn't query H on x^* in the ROM
- in the QROM an adversary can query every element by a single superposition query
- O2H still allows to reprogram the quantum random oracle on x^* if weight on x^* is negligible.

Oneway-to-hiding [Unr14]

- $\mathsf{H}(x^*)$ look random to the adversary, if it doesn't query H on x^* in the ROM
- in the QROM an adversary can query every element by a single superposition query
- O2H still allows to reprogram the quantum random oracle on x^* if weight on x^* is negligible.
- Intuition: for adversary to notice the reprogramming it needs to have enough weight on x^*. If the weight is noticeable, measuring a random query will give x^* with noticeable probability
- several improved variants exist

Proof Sketch Group Action Hashed ElGamal

$\underline{\mathsf{Decaps}(sk, c \neq c^*)}$	$\underline{\mathsf{H}(x_1, x_2)}$
return $\mathsf{H}(c, sk \star c)$	**if** $\mathsf{GA\text{-}DDH}_g(x_1, x_2)$
	return $\mathsf{H}_1(x_1)$
	return $\mathsf{H}_2(x_1, x_2)$

Proof Sketch Group Action Hashed ElGamal

Decaps$(sk, c \neq c^*)$	$\mathsf{H}(x_1, x_2)$
return $\mathsf{H}(c, sk \star c)$	**if** GA-DDH$_g(x_1, x_2)$ **return** $\mathsf{H}_1(x_1)$ **return** $\mathsf{H}_2(x_1, x_2)$

- Decaps simulation: secret-key is used on $x_2 \implies$ use separate hash function for valid DH tuples without second input $\implies$ simulate Decaps without sk

Proof Sketch Group Action Hashed ElGamal

$\underline{\mathrm{Decaps}(sk, c \neq c^*)}$	$\underline{\mathrm{H}(x_1, x_2)}$
return $\mathrm{H}_1(c)$	**if** $\text{GA-DDH}_g(x_1, x_2)$ **return** $\mathrm{H}_1(x_1)$ **return** $\mathrm{H}_2(x_1, x_2)$

- Decaps simulation: secret-key is used on x_2 $\implies$ use separate hash function for valid DH tuples without second input $\implies$ simulate Decaps without *sk*

Proof Sketch Group Action Hashed ElGamal

$\underline{\mathrm{Decaps}(sk, c \neq c^*)}$	$\underline{\mathrm{H}(x_1, x_2)}$
return $\mathrm{H}_1(c)$	**if** $\text{GA-DDH}_g(x_1, x_2)$ **return** $\mathrm{H}_1(x_1)$ **return** $\mathrm{H}_2(x_1, x_2)$

- Decaps simulation: secret-key is used on $x_2 \implies$ use separate hash function for valid DH tuples without second input $\implies$ simulate Decaps without *sk*
- Caveat: quantum-access to H $\implies$ simulator needs quantum access to GA-DDH_g

Proof Sketch Group Action Hashed ElGamal

$\underline{\mathrm{Decaps}(sk, c \neq c^*)}$	$\underline{\mathrm{H}(x_1, x_2)}$
return $\mathrm{H}_1(c)$	**if** $\text{GA-DDH}_g(x_1, x_2)$ **return** $\mathrm{H}_1(x_1)$ **return** $\mathrm{H}_2(x_1, x_2)$

- Decaps simulation: secret-key is used on $x_2 \implies$ use separate hash function for valid DH tuples without second input $\implies$ simulate Decaps without sk
- Caveat: quantum-access to H $\implies$ simulator needs quantum access to GA-DDH_g
- use oneway-to-hiding to reprogram H on challenge input

Weaker assumptions

- Can we do better regarding assumptions?

Weaker assumptions

- Can we do better regarding assumptions?
- 1) key-confirmation hash removes the quantum-access from the decision oracle, KEM only (security based on GA-Strong-CDH assumption)

Weaker assumptions

- Can we do better regarding assumptions?
- 1) key-confirmation hash removes the quantum-access from the decision oracle, KEM only (security based on GA-Strong-CDH assumption)
- 2) generalize twinning to group actions, both NIKE and KEM (security based on GA-CDH assumption)

Key-Confirmation

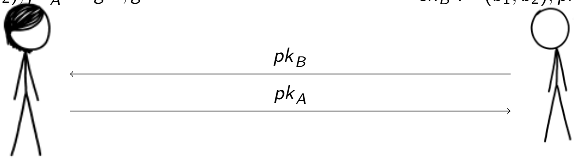
- add key-confirmation hash $\mathsf{H}'(ab \star \tilde{x})$ to encapsulation c for independent hash function H'
- since access to Decaps is classical $\implies$ $\mathsf{H}'(ab \star \tilde{x})$ is classical

Key-Confirmation

- add key-confirmation hash $\mathsf{H}'(ab \star \tilde{x})$ to encapsulation c for independent hash function H'
- since access to Decaps is classical $\implies$ $\mathsf{H}'(ab \star \tilde{x})$ is classical
- simulator can extract $ab \star \tilde{x}$ from key-confirmation hash and use *classical* DDH oracle to check for validity (GA-Strong-CDH assumption) of the DDH tuple
- Caveat: KEM only

Twinning [CKS08]

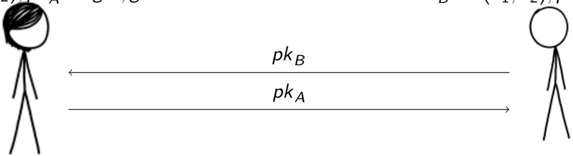
$sk_A := (a_1, a_2), pk_A := g^{a_1}, g^{a_2}$ $sk_B := (b_1, b_2), pk_B := g^{b_1}, g^{b_2}$



$$\mathsf{H}(g^a, g^b, g^{a_1 b_1}, g^{a_1 b_2}, g^{a_2 b_1}, g^{a_2 b_2})$$

Twinning [CKS08]

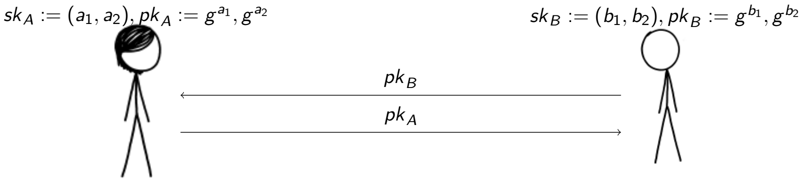
$sk_A := (a_1, a_2), pk_A := g^{a_1}, g^{a_2}$ $\qquad$ $sk_B := (b_1, b_2), pk_B := g^{b_1}, g^{b_2}$



$$\mathsf{H}(g^a, g^b, g^{a_1 b_1}, g^{a_1 b_2}, g^{a_2 b_1}, g^{a_2 b_2})$$

- actively secure under *standard* Computational Diffie-Hellman assumption in the random oracle model

Twinning [CKS08]



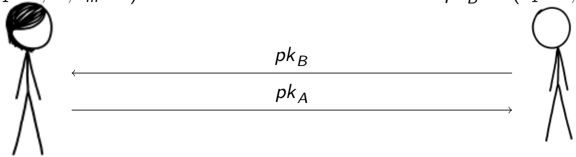
$$\mathsf{H}(g^a, g^b, g^{a_1 b_1}, g^{a_1 b_2}, g^{a_2 b_1}, g^{a_2 b_2})$$

- actively secure under *standard* Computational Diffie-Hellman assumption in the random oracle model
- Intuition: trapdoor test allows to simulate the decision oracle

Twinning with Group Actions

$sk_A := (a_1, ..., a_m) \leftarrow \mathcal{G}^m$
$pk_A := (a_1 \star \tilde{x}, ..., a_m \star \tilde{x})$

$sk_B := (b_1, ..., b_m) \leftarrow \mathcal{G}^m$
$pk_B := (b_1 \star \tilde{x}, ..., b_m \star \tilde{x})$



$$\mathrm{H}(pk_A, pk_B, a_1 b_1 \star \tilde{x}, \ldots, a_1 b_m \star \tilde{x}, \ldots, a_m b_1 \star \tilde{x}, \ldots, a_m b_m \star \tilde{x})$$

- proof similar to Hashed DH proof, but use trapdoor test instead of decision oracle
- for 128 bits security, $m = 85$
- actively secure under GA-CDH assumption

Summary

showed, in the QROM,

- necessity of GA-Quantum-Strong-CDH assumption for GA-Hashed-DH
- active security of GA-Hashed-DH based on GA-Quantum-Strong-CDH assumption
- alternative constructions using twinning (from GA-CDH) and key-confirmation (from GA-Strong-CDH) using weaker assumptions
- corresponding KEMs secure

Thank you! Full version: eprint 2022/1230

Michel Abdalla, Mihir Bellare, and Phillip Rogaway.
The oracle Diffie-Hellman assumptions and an analysis of DHIES.
In David Naccache, editor, *CT-RSA 2001*, volume 2020 of *LNCS*, pages 143–158. Springer, Heidelberg, April 2001.

Navid Alamati, Luca De Feo, Hart Montgomery, and Sikhar Patranabis.
Cryptographic group actions and applications.
In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 411–439. Springer, Heidelberg, December 2020.

Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry.
Random oracles in a quantum world.
In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 41–69. Springer, Heidelberg, December 2011.

David Cash, Eike Kiltz, and Victor Shoup.
The twin Diffie-Hellman problem and applications.
In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 127–145. Springer, Heidelberg, April 2008.

Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes.
CSIDH: An efficient post-quantum commutative group action.
In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 395–427. Springer, Heidelberg, December 2018.

Whitfield Diffie and Martin E. Hellman.
New directions in cryptography.
IEEE Transactions on Information Theory, 22(6):644–654, 1976.

Ehsan Ebrahimi Targhi and Dominique Unruh.
Post-quantum security of the Fujisaki-Okamoto and OAEP transforms.
In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B, Part II*, volume 9986 of *LNCS*, pages 192–216. Springer, Heidelberg, October / November 2016.

Dominique Unruh.
Revocable quantum timed-release encryption.
In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 129–146. Springer, Heidelberg, May 2014.