The one-way to hiding Lemma

Reprogramming in the Quantum Random Oracle Model

Kathrin Hövelmanns[1]

[1]Ei/Ψ, Eindhoven University of Technology, Netherlands

Quiques - Quantum Techniques for Provable Security
October 17, 2021

Eindhoven Institute for the Protection of Systems and Information

EINDHOVEN UNIVERSITY OF TECHNOLOGY

Intro: The one-way to hiding Lemma (OW2H)

Context: Quantum-resistant public-key primitives

OW2H: Replace classical reprogramming

Use cases:

- CCA conversions (e.g., as used in the NIST competition)
- Block ciphers
- MACs
- ZK proofs
- AKE

Outline and goal of this talk

1. Example: Typical reprogramming use case
2. Simple ('original') OW2H
3. Extensions and improvements of OW2H
4. Summary

Goal: Learn

- where/how OW2H can be used
- what the best known bounds are

Motivating example: Reprogramming use case

PKE transformation Derand

Transformative step in current CCA conversions

Encrypt-with-Hash: $\mathsf{PKE}^{\mathsf{G}} := \mathsf{Derand}[\mathsf{PKE}, \mathsf{G}]$

PKE transformation Derand

Transformative step in current CCA conversions

Encrypt-with-Hash: $\mathsf{PKE}^{\mathsf{G}} := \mathsf{Derand}[\mathsf{PKE}, \mathsf{G}]$

- $\mathsf{PKE}^{\mathsf{G}}$ uses Gen and Dec
- Encryption: $\mathsf{Enc}^{\mathsf{G}}(pk, m) := \mathsf{Enc}(pk, m; \mathsf{G}(m))$

Use $\mathsf{G}(m)$ as Enc's randomness

PKE transformation Derand

Transformative step in current CCA conversions

Encrypt-with-Hash: $\mathsf{PKE}^{\mathsf{G}} := \mathsf{Derand}[\mathsf{PKE}, \mathsf{G}]$

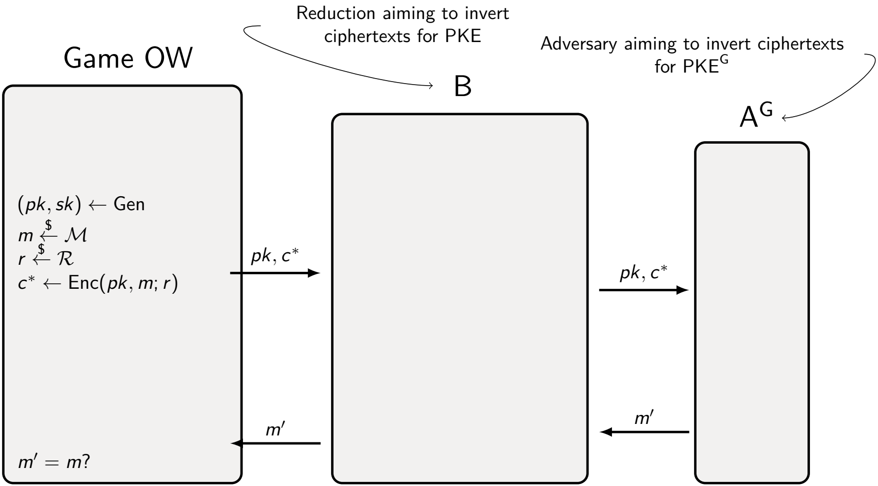
- $\mathsf{PKE}^{\mathsf{G}}$ uses Gen and Dec
- Encryption: $\mathsf{Enc}^{\mathsf{G}}(pk, m) := \mathsf{Enc}(pk, m; \mathsf{G}(m))$

Use $\mathsf{G}(m)$ as Enc's randomness

Theorem (ROM)

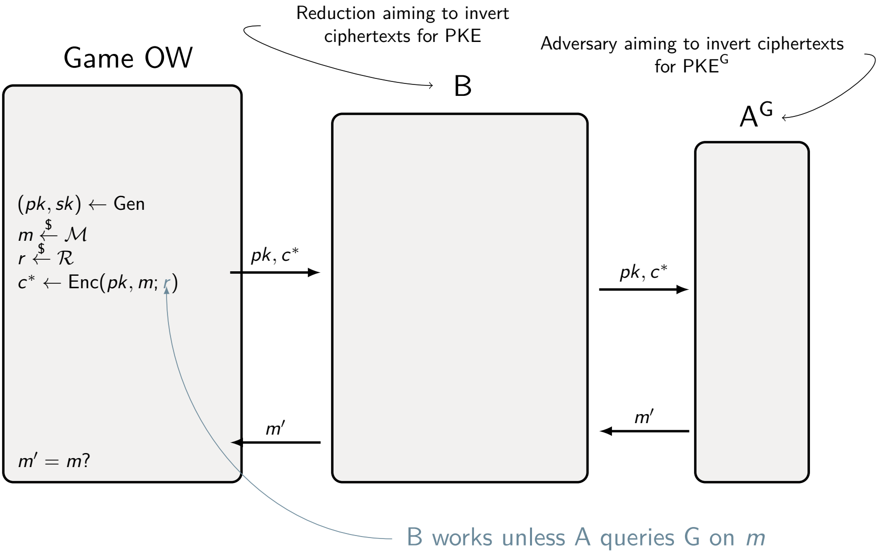
PKE OW secure $\Rightarrow$ $\mathsf{Derand}[\mathsf{PKE}, \mathsf{G}]$ OW secure

PKE transformation Derand: security proof

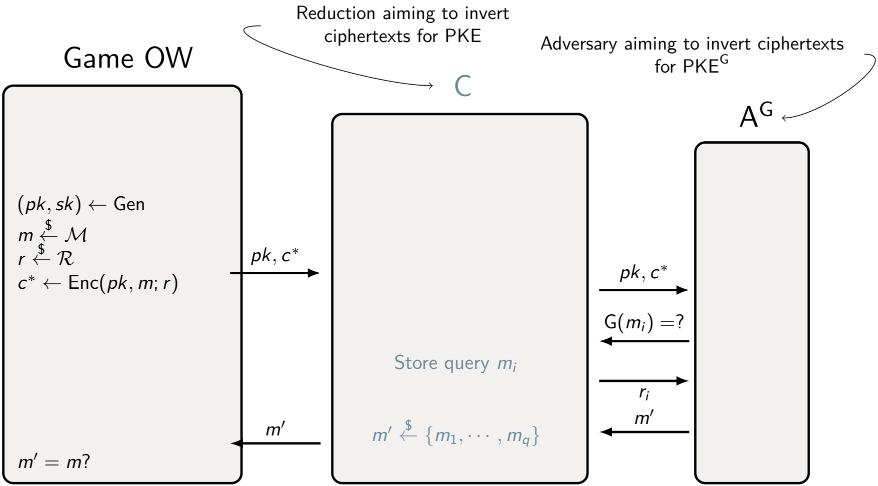


A wins ⇒ B wins

PKE transformation Derand: security proof

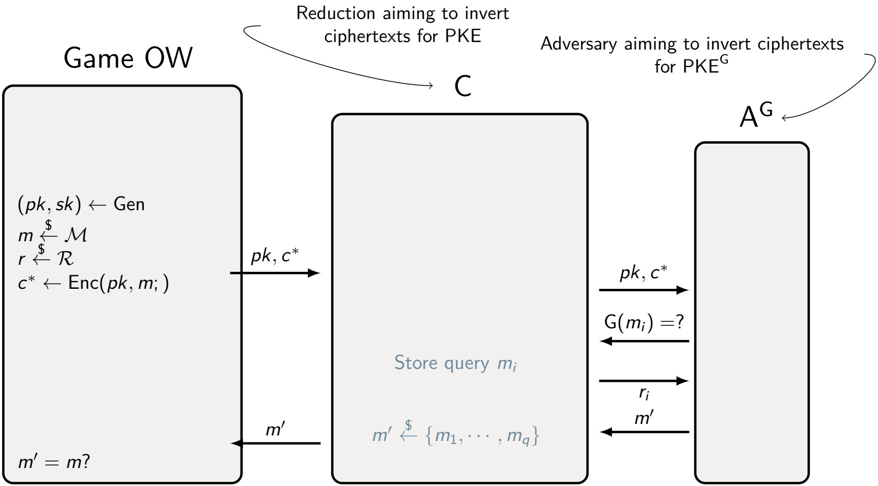


PKE transformation Derand: security proof



A queries G on $m \Rightarrow$ C wins with Pr $\frac{1}{q}$

PKE transformation Derand: security proof



$$\mathrm{Adv}(\mathsf{A}, \mathsf{PKE}^{\mathsf{G}}) \leq \mathrm{Adv}(\mathsf{B}, \mathsf{PKE}) + q \cdot \mathrm{Adv}(\mathsf{C}, \mathsf{PKE})$$

PKE transformation Derand: Takeaway

We used:

- $\mathsf{G}(m) \approx \$$ unless queried
- Queries can be memorised and used later by reduction

QROM:

- What does it mean to say that $\mathsf{G}(m)$ was queried?
- Bookkeeping isn't trivial

Simple ('original') OW2H

original OW2H [Unruh14]

Quantum counterpart of 'random-until-query':

$$\left|\Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}}(x, \mathsf{G}(x))\right] - \Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}}(x, \$)\right]\right|$$

original OW2H [Unruh14]

Quantum counterpart of 'random-until-query':

$$\left|\Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}}(x, \mathsf{G}(x))\right] - \Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}}(x, \$)\right]\right|$$

Extractor $\mathsf{Ext}^{\mathsf{G}}(x)$:

1. Picks random $i \in \{1, \cdots, q\}$
2. Runs $\mathsf{A}^{\mathsf{G}}(x, \$)$ only until i-th query to G
3. Measures input register of i-th query
4. Returns measurement result x'

original OW2H [Unruh14]

Quantum counterpart of 'random-until-query':

$$\left|\Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}}(x, \mathsf{G}(x))\right] - \Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}}(x, \$)\right]\right| \leq 2q \cdot \sqrt{\Pr\left[x \leftarrow \mathsf{Ext}^{\mathsf{G}}(x)\right]}$$

Extractor $\mathsf{Ext}^{\mathsf{G}}(x)$:

1. Picks random $i \in \{1, \cdots, q\}$
2. Runs $\mathsf{A}^{\mathsf{G}}(x, \$)$ only until i-th query to G
3. Measures input register of i-th query
4. Returns measurement result x'

original OW2H : Application to our example use case

$G_0 := \mathsf{OW}: \quad c^* := \mathsf{Enc}(pk, m; \mathsf{G}(m))$

G_0: OW advantage of A against $\mathsf{PKE}^{\mathsf{G}} = \mathsf{Derand}[\mathsf{PKE}, \mathsf{G}]$

original OW2H : Application to our example use case

$G_0 :=$ OW: $\quad c^* := \mathsf{Enc}(pk, m; \mathsf{G}(m))$

G_1: $\quad c^* := \mathsf{Enc}(pk, m; \$)$

G_0: OW advantage of A against $\mathsf{PKE}^{\mathsf{G}} = \mathsf{Derand}[\mathsf{PKE}, \mathsf{G}]$

G_1: OW advantage of reduction B against PKE (as in ROM)

original OW2H : Application to our example use case

$$G_0 := \mathsf{OW}: \quad c^* := \mathsf{Enc}(pk, m; \mathsf{G}(m))$$
$$G_1: \quad c^* := \mathsf{Enc}(pk, m; \$)$$

G_0: OW advantage of A against $\mathsf{PKE}^{\mathsf{G}} = \mathsf{Derand}[\mathsf{PKE}, \mathsf{G}]$

G_1: OW advantage of reduction B against PKE (as in ROM)

$$\mathrm{Adv}(\mathsf{A}, \mathsf{PKE}^{\mathsf{G}}) \leq \mathrm{Adv}(\mathsf{B}, \mathsf{PKE}) + \left|\Pr\left[G_0^{\mathsf{A}} \Rightarrow 1\right] - \Pr\left[G_1^{\mathsf{A}} \Rightarrow 1\right]\right|$$

original OW2H : Application to our example use case

$G_0 :=$ OW: $\quad c^* := \mathsf{Enc}(pk, m; \mathsf{G}(m))$

G_1: $\quad c^* := \mathsf{Enc}(pk, m; \$)$

G_0: OW advantage of A against $\mathsf{PKE}^{\mathsf{G}} = \mathsf{Derand}[\mathsf{PKE}, \mathsf{G}]$

G_1: OW advantage of reduction B against PKE (as in ROM)

$$\mathrm{Adv}(\mathsf{A}, \mathsf{PKE}^{\mathsf{G}}) \leq \mathrm{Adv}(\mathsf{B}, \mathsf{PKE}) + \left| \Pr\left[G_0^{\mathsf{A}} \Rightarrow 1\right] - \Pr\left[G_1^{\mathsf{A}} \Rightarrow 1\right] \right|$$

OW2H Extractor $\mathsf{Ext}^{\mathsf{G}}(x) =$ Reduction $\mathsf{C}'(pk, c^*)$:

1. Pick random $i \in \{1, \cdots, q\}$
2. Run $\mathsf{A}^{\mathsf{G}}(pk, c^*)$ until i-th query to G
3. Measures input register of i-th query
4. Returns measurement result m'

original OW2H : Application to our example use case

$G_0 :=$ OW: $\quad c^* := \mathsf{Enc}(pk, m; \mathsf{G}(m))$

G_1: $\quad c^* := \mathsf{Enc}(pk, m; \$)$

G_0: OW advantage of A against $\mathsf{PKE}^\mathsf{G} = \mathsf{Derand}[\mathsf{PKE}, \mathsf{G}]$

G_1: OW advantage of reduction B against PKE (as in ROM)

$$\mathrm{Adv}(\mathsf{A}, \mathsf{PKE}^\mathsf{G}) \leq \mathrm{Adv}(\mathsf{B}, \mathsf{PKE}) + \left|\Pr\left[G_0^\mathsf{A} \Rightarrow 1\right] - \Pr\left[G_1^\mathsf{A} \Rightarrow 1\right]\right|$$

OW2H Extractor $\mathsf{Ext}^\mathsf{G}(x) =$ Reduction $\mathsf{C}'(pk, c^*)$:

1. Pick random $i \in \{1, \cdots, q\}$
2. Run $\mathsf{A}^\mathsf{G}(pk, c^*)$ until i-th query to G
3. Measures input register of i-th query
4. Returns measurement result m'

$$\left|\Pr\left[G_0^\mathsf{A} \Rightarrow 1\right] - \Pr\left[G_1^\mathsf{A} \Rightarrow 1\right]\right| \leq 2q \cdot \sqrt{\mathrm{Adv}(\mathsf{C}', \mathsf{PKE})}$$

original OW2H : Limitations

Quantum counterpart of 'random-until-query':

$$\left|\Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}}(x, \mathsf{G}(x))\right] - \Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}}(x, \$)\right]\right| \leq 2q \cdot \sqrt{\Pr\left[x \leftarrow \mathsf{Ext}^{\mathsf{G}}(x)\right]}$$

Limitations:

- Non-tightness (q and $\sqrt{..}$) $\rightarrow$ Modular proofs less attractive
- Reprogramming N positions $\rightarrow$ Bound $\cdot N$
- Game must know positions a-priori $\rightarrow$ Inapplicable when positions partially depend on A

Extensions of OW2H

Extensions of OW2H

Tighter & several positions at once: AHU19 ('semi-classical' OW2H)

Tightness improvements via 'smarter' extractors:

- BHH+19 ('double-sided' OW2H)
- KSS+20 ('MRM')

Generalisations:

- Compressed oracles: CMSZ19
- Adaptively chosen positions: GHHM21

semi-classical OW2H [AHU19]

Still counterpart of 'random-until-query', but more general:

$G_1, G_2 : X \to Y$

$S \subset X$ s. th. $G_1(x) = G_2(x)$ for all $x \notin S$

z: input to A

Goal: Upper bound for

$\left|\Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}_1}(z)\right] - \Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}_2}(z)\right]\right|$

semi-classical OW2H : semi-classical oracles

Semi-classical oracle O_S^{SC} for $S \subset X$:

Applied to $|\psi\rangle_{X,\{0,1\}}$

(e.g., $|x, 0\rangle$ for some $x \in X$)

semi-classical OW2H : semi-classical oracles

Semi-classical oracle O_S^{SC} for $S \subset X$:

Applied to $|\psi\rangle_{X,\{0,1\}}$

(e.g., $|x, 0\rangle$ for some $x \in X$)

Intuition: 'Flattening' of $|\psi\rangle$ to state $|\psi'\rangle$

$|\psi'\rangle$ contains only elements of S or only elements of $X \setminus S$

semi-classical OW2H : semi-classical oracles

Semi-classical oracle O_S^{SC} for $S \subset X$:

Applied to $|\psi\rangle_{X,\{0,1\}}$

(e.g., $|x, 0\rangle$ for some $x \in X$)

Formally: O_S^{SC} acts on $|x, b\rangle$ by

- mapping $|x, b\rangle$ to $|x, b \oplus b'\rangle$, where $b' = 1$ iff $x \in S$
- measuring the $\{0, 1\}$-register

semi-classical OW2H : semi-classical oracles

Semi-classical oracle O_S^{SC} for $S \subset X$:

Applied to $|\psi\rangle_{X,\{0,1\}}$

(e.g., $|x, 0\rangle$ for some $x \in X$)

Example:

$X := \{0, 1\}$, $S := \{1\}$

$|\psi\rangle_{X,\{0,1\}} := (\frac{1}{\sqrt{3}}|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|1\rangle) \otimes |0\rangle$

semi-classical OW2H : semi-classical oracles

Semi-classical oracle O_S^{SC} for $S \subset X$:

Applied to $|\psi\rangle_{X,\{0,1\}}$

(e.g., $|x, 0\rangle$ for some $x \in X$)

Example:

$X := \{0,1\}$, $S := \{1\}$

$$|\psi\rangle_{X,\{0,1\}} := \left(\frac{1}{\sqrt{3}}|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|1\rangle\right) \otimes |0\rangle$$

$$\mathsf{O}_S^{SC}|\psi\rangle = \begin{cases} |00\rangle & \text{with prob } \frac{1}{3} \\ |11\rangle & \text{with prob } \frac{2}{3} \end{cases}$$

semi-classical OW2H : 'punctured' oracles

O_S^{SC} 'flattens' $|\psi, 0\rangle$ to

$$\begin{cases} |\psi'_S, 1\rangle & \text{s. th. } |\psi'_S\rangle \text{ only contains elements of } S \\ |\psi'_{X\setminus S}, 0\rangle & \text{s. th. } |\psi'_{X\setminus S}\rangle \text{ only contains elements of } X \setminus S \end{cases}$$

semi-classical OW2H : 'punctured' oracles

O_S^{SC} 'flattens' $|\psi, 0\rangle$ to

$$\begin{cases} |\psi'_S, 1\rangle & \text{s. th. } |\psi'_S\rangle \text{ only contains elements of } S \\ |\psi'_{X\setminus S}, 0\rangle & \text{s. th. } |\psi'_{X\setminus S}\rangle \text{ only contains elements of } X \setminus S \end{cases}$$

'Punctured' oracle $\mathrm{G} \setminus S$:

Before applying oracle unitary U_{G}, first apply O_S^{SC}

semi-classical OW2H : 'punctured' oracles

O_S^{SC} 'flattens' $|\psi, 0\rangle$ to

$$\begin{cases} |\psi'_S, 1\rangle & \text{s. th. } |\psi'_S\rangle \text{ only contains elements of } S \\ |\psi'_{X\setminus S}, 0\rangle & \text{s. th. } |\psi'_{X\setminus S}\rangle \text{ only contains elements of } X \setminus S \end{cases}$$

'Punctured' oracle $\mathrm{G} \setminus S$:

Before applying oracle unitary U_{G}, first apply O_S^{SC}

FIND := 'second register switched to 1'

FIND $\rightarrow$ measuring $|\psi'_S, 1\rangle$ yields $x \in S$

semi-classical OW2H : (Simpl.) Theorems from [AHU19]

Want to bound dist. advant. between G_1 and G_2

$G_1(x) = G_2(x)$ for all $x \notin S$

semi-classical OW2H : (Simpl.) Theorems from [AHU19]

Want to bound dist. advant. between G_1 and G_2

$G_1(x) = G_2(x)$ for all $x \notin S$

Th.1:

$$\left|\Pr\left[1 \leftarrow \mathsf{A}^{G_1}(z)\right] - \Pr\left[1 \leftarrow \mathsf{A}^{G_2}(z)\right]\right| \leq 2\sqrt{(q+1) \cdot \Pr[\mathsf{FIND} : \mathsf{A}^{G_2 \setminus S}(z)]}$$

semi-classical OW2H : (Simpl.) Theorems from [AHU19]

Want to bound dist. advant. between G_1 and G_2

$G_1(x) = G_2(x)$ for all $x \notin S$

Th.1:

$$\left|\Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}_1}(z)\right] - \Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}_2}(z)\right]\right| \leq 2\sqrt{(q+1) \cdot \Pr[\mathsf{FIND} : \mathsf{A}^{\mathsf{G}_2 \setminus \mathsf{S}}(z)]}$$

... but

- a reduction might not know S
- how can we use FIND to extract?

semi-classical OW2H : (Simpl.) Theorems from [AHU19]

Want to bound dist. advant. between G_1 and G_2

$G_1(x) = G_2(x)$ for all $x \notin S$

Th.1:

$$\left|\Pr\left[1 \leftarrow \mathsf{A}^{G_1}(z)\right] - \Pr\left[1 \leftarrow \mathsf{A}^{G_2}(z)\right]\right| \leq 2\sqrt{(q+1) \cdot \Pr[\mathsf{FIND} : \mathsf{A}^{G_2 \setminus S}(z)]}$$

Th.2:

$$\Pr[\mathsf{FIND} : \mathsf{A}^{G_2 \setminus S}(z)] \leq 4q \cdot \Pr\left[x \in S : x \leftarrow \mathsf{Ext}^{G}(x)\right]$$

semi-classical OW2H : (Simpl.) Theorems from [AHU19]

Want to bound dist. advant. between G_1 and G_2

$G_1(x) = G_2(x)$ for all $x \notin S$

Th.1:

$$\left|\Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}_1}(z)\right] - \Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}_2}(z)\right]\right| \leq 2\sqrt{(q+1)\cdot \Pr[\mathsf{FIND} : \mathsf{A}^{\mathsf{G}_2\setminus\mathsf{S}}(z)]}$$

Th.2:

$$\Pr[\mathsf{FIND} : \mathsf{A}^{\mathsf{G}_2\setminus\mathsf{S}}(z)] \leq 4q \cdot \Pr\left[x \in S : x \leftarrow \mathsf{Ext}^{\mathsf{G}}(x)\right]$$

If z and S are independent, then

$$\Pr[\mathsf{FIND} : \mathsf{A}^{\mathsf{G}_2\setminus\mathsf{S}}(z)] \leq 4q \cdot \max_x \Pr\left[x \in S\right]$$

e.g., $\frac{4q}{|X|}$ for $S = \{x^*\}$, $x^* \overset{\$}{\leftarrow} X$

semi-classical OW2H : Application to our example

$G_0 :=$ OW: $\quad c^* := \mathsf{Enc}(pk, m; \mathsf{G}(m))$

G_1: $\quad c^* := \mathsf{Enc}(pk, m; \$)$

G_0: OW advantage of A against $\mathsf{PKE}^{\mathsf{G}} = \mathsf{Derand}[\mathsf{PKE}, \mathsf{G}]$

G_1: OW advantage of reduction B against PKE (as in ROM)

semi-classical OW2H : Application to our example

$G_0 :=$ OW: $\quad c^* := \mathsf{Enc}(pk, m; \mathsf{G}(m))$

G_1: $\quad c^* := \mathsf{Enc}(pk, m; \$)$

$$\mathrm{Adv}(\mathsf{A}, \mathsf{PKE}^{\mathsf{G}}) \leq \mathrm{Adv}(\mathsf{B}, \mathsf{PKE}) + \left| \Pr\left[G_0^{\mathsf{A}} \Rightarrow 1\right] - \Pr\left[G_1^{\mathsf{A}} \Rightarrow 1\right] \right|$$

semi-classical OW2H : Application to our example

$G_0 := \mathsf{OW}$: $\quad c^* := \mathsf{Enc}(pk, m; \mathsf{G}(m))$

G_1: $\quad c^* := \mathsf{Enc}(pk, m; \$)$

$$\mathrm{Adv}(\mathsf{A}, \mathsf{PKE}^{\mathsf{G}}) \leq \mathrm{Adv}(\mathsf{B}, \mathsf{PKE}) + \left|\Pr\left[G_0^{\mathsf{A}} \Rightarrow 1\right] - \Pr\left[G_1^{\mathsf{A}} \Rightarrow 1\right]\right|$$

$$\left|\Pr\left[G_0^{\mathsf{A}} \Rightarrow 1\right] - \Pr\left[G_1^{\mathsf{A}} \Rightarrow 1\right]\right| \leq 2\sqrt{(q+1)\cdot \Pr[\mathsf{FIND}]}$$

$$\Pr[\mathsf{FIND}] = \Pr[\mathsf{FIND} : m' \leftarrow \mathsf{A}^{\mathsf{G}_2 \setminus \{\mathsf{m}\}}(pk, \mathsf{Enc}(pk, m; \$))]$$

semi-classical OW2H : Application to our example

$G_0 :=$ OW: $c^* := \mathsf{Enc}(pk, m; \mathsf{G}(m))$

G_1: $c^* := \mathsf{Enc}(pk, m; \$)$

$$\mathrm{Adv}(\mathsf{A}, \mathsf{PKE}^{\mathsf{G}}) \leq \mathrm{Adv}(\mathsf{B}, \mathsf{PKE}) + \left|\Pr\left[G_0^{\mathsf{A}} \Rightarrow 1\right] - \Pr\left[G_1^{\mathsf{A}} \Rightarrow 1\right]\right|$$

$$\left|\Pr\left[G_0^{\mathsf{A}} \Rightarrow 1\right] - \Pr\left[G_1^{\mathsf{A}} \Rightarrow 1\right]\right| \leq 2\sqrt{(q+1) \cdot \Pr[\mathsf{FIND}]}$$

$$\Pr[\mathsf{FIND}] = \Pr[\mathsf{FIND} : m' \leftarrow \mathsf{A}^{\mathsf{G}_2 \setminus \{\mathsf{m}\}}(pk, \mathsf{Enc}(pk, m; \$))]$$

Upper bound Pr[FIND]:

Use query extractor as before (OW reduction C')

$\Rightarrow \Pr[\mathsf{FIND}] \leq 4q \cdot \mathrm{Adv}(\mathsf{C}', \mathsf{PKE})$ ...

semi-classical OW2H : Application to our example

$G_0 :=$ OW: $\quad c^* := \mathsf{Enc}(pk, m; \mathsf{G}(m))$

G_1: $\quad c^* := \mathsf{Enc}(pk, m; \$)$

$$\mathrm{Adv}(\mathsf{A}, \mathsf{PKE}^{\mathsf{G}}) \leq \mathrm{Adv}(\mathsf{B}, \mathsf{PKE}) + \left| \Pr\left[G_0^{\mathsf{A}} \Rightarrow 1\right] - \Pr\left[G_1^{\mathsf{A}} \Rightarrow 1\right] \right|$$

$$\left| \Pr\left[G_0^{\mathsf{A}} \Rightarrow 1\right] - \Pr\left[G_1^{\mathsf{A}} \Rightarrow 1\right] \right| \leq 2\sqrt{(q+1) \cdot \Pr[\mathsf{FIND}]}$$

$$\Pr[\mathsf{FIND}] = \Pr[\mathsf{FIND} : m' \leftarrow \mathsf{A}^{\mathsf{G}_2 \setminus \{\mathsf{m}\}}(pk, \mathsf{Enc}(pk, m; \$))]$$

Upper bound Pr[FIND]:

... or get better bounds via IND-CPA:

$$\Pr[\mathsf{FIND}'] = \Pr[\mathsf{FIND} : m' \leftarrow \mathsf{A}^{\mathsf{G}_2 \setminus \{\mathsf{m}''\}}(pk, \mathsf{Enc}(pk, m; \$))]$$

semi-classical OW2H : Application to our example

$G_0 :=$ OW: $c^* := \mathsf{Enc}(pk, m; \mathsf{G}(m))$

G_1: $c^* := \mathsf{Enc}(pk, m; \$)$

$$\mathrm{Adv}(\mathsf{A}, \mathsf{PKE}^{\mathsf{G}}) \leq \mathrm{Adv}(\mathsf{B}, \mathsf{PKE}) + \left|\Pr\left[G_0^{\mathsf{A}} \Rightarrow 1\right] - \Pr\left[G_1^{\mathsf{A}} \Rightarrow 1\right]\right|$$

$$\left|\Pr\left[G_0^{\mathsf{A}} \Rightarrow 1\right] - \Pr\left[G_1^{\mathsf{A}} \Rightarrow 1\right]\right| \leq 2\sqrt{(q+1) \cdot \Pr[\mathsf{FIND}]}$$

$$\Pr[\mathsf{FIND}] = \Pr[\mathsf{FIND} : m' \leftarrow \mathsf{A}^{\mathsf{G}_2 \setminus \{\mathsf{m}\}}(pk, \mathsf{Enc}(pk, m; \$))]$$

Upper bound Pr[FIND]:

... or get better bounds via IND-CPA:

$$\Pr[\mathsf{FIND}'] = \Pr[\mathsf{FIND} : m' \leftarrow \mathsf{A}^{\mathsf{G}_2 \setminus \{\mathsf{m}''\}}(pk, \mathsf{Enc}(pk, m; \$))]$$

$$\Pr[\mathsf{FIND}'] \leq \frac{4q}{|\mathcal{M}|}$$

semi-classical OW2H : Application to our example

$G_0 :=$ OW: $c^* := \mathsf{Enc}(pk, m; \mathsf{G}(m))$

G_1: $c^* := \mathsf{Enc}(pk, m; \$)$

$$\mathrm{Adv}(\mathsf{A}, \mathsf{PKE}^{\mathsf{G}}) \leq \mathrm{Adv}(\mathsf{B}, \mathsf{PKE}) + \left|\Pr\left[G_0^{\mathsf{A}} \Rightarrow 1\right] - \Pr\left[G_1^{\mathsf{A}} \Rightarrow 1\right]\right|$$

$$\left|\Pr\left[G_0^{\mathsf{A}} \Rightarrow 1\right] - \Pr\left[G_1^{\mathsf{A}} \Rightarrow 1\right]\right| \leq 2\sqrt{(q+1) \cdot \Pr[\mathsf{FIND}]}$$

$$\Pr[\mathsf{FIND}] = \Pr[\mathsf{FIND} : m' \leftarrow \mathsf{A}^{\mathsf{G}_2 \setminus \{\mathsf{m}\}}(pk, \mathsf{Enc}(pk, m; \$))]$$

Upper bound Pr[FIND]:

... or get better bounds via IND-CPA:

$$\Pr[\mathsf{FIND}'] = \Pr[\mathsf{FIND} : m' \leftarrow \mathsf{A}^{\mathsf{G}_2 \setminus \{\mathsf{m}''\}}(pk, \mathsf{Enc}(pk, m; \$))]$$

$\Pr[\mathsf{FIND}'] \leq \frac{4q}{|\mathcal{M}|}$ $\quad |\Pr[\mathsf{FIND}'] - \Pr[\mathsf{FIND}]|$: IND-CPA reduction D

semi-classical OW2H : Application to our example

G_0 := OW: $c^* := \mathsf{Enc}(pk, m; \mathsf{G}(m))$

G_1: $c^* := \mathsf{Enc}(pk, m; \$)$

$$\mathrm{Adv}(\mathsf{A}, \mathsf{PKE}^{\mathsf{G}}) \leq \mathrm{Adv}(\mathsf{B}, \mathsf{PKE}) + \left| \Pr\left[G_0^{\mathsf{A}} \Rightarrow 1\right] - \Pr\left[G_1^{\mathsf{A}} \Rightarrow 1\right] \right|$$

$$\left| \Pr\left[G_0^{\mathsf{A}} \Rightarrow 1\right] - \Pr\left[G_1^{\mathsf{A}} \Rightarrow 1\right] \right| \leq 2\sqrt{(q+1) \cdot \Pr[\mathsf{FIND}]}$$

$$\Pr[\mathsf{FIND}] = \Pr[\mathsf{FIND} : m' \leftarrow \mathsf{A}^{\mathsf{G}_2 \setminus \{\mathsf{m}\}}(pk, \mathsf{Enc}(pk, m; \$))]$$

Upper bound Pr[FIND]:

... or get better bounds via IND-CPA:

$$\Pr[\mathsf{FIND}'] = \Pr[\mathsf{FIND} : m' \leftarrow \mathsf{A}^{\mathsf{G}_2 \setminus \{\mathsf{m}''\}}(pk, \mathsf{Enc}(pk, m; \$))]$$

$\Pr[\mathsf{FIND}'] \leq \frac{4q}{|\mathcal{M}|}$ $\quad |\Pr[\mathsf{FIND}'] - \Pr[\mathsf{FIND}]|$: IND-CPA reduction D

$$\Pr[\mathsf{FIND}] \leq \frac{4q}{|\mathcal{M}|} + \mathrm{Adv}(\mathsf{D}, \mathsf{PKE})$$

semi-classical OW2H : Conclusion

More general counterpart of 'random-until-query':

$$\left|\Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}_1}(z)\right] - \Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}_2}(z)\right]\right| \leq 2\sqrt{(q+1)\cdot \Pr[\mathsf{FIND} : \mathsf{A}^{\mathsf{G}_2 \setminus \mathsf{S}}(z)]}$$

Advantages:

Arbitrary many positions

Tighter bound if

- reduction knows how to puncture
- we can upper bound Pr[FIND], tightly

(Simpl.) double-sided OW2H [BHH+19]

$G_1, G_2 : X \to Y$

$S = \{x^*\}$ s. th. $G_1(x) = G_2(x)$ for all $x \neq x^*$

z: input to A

(Simpl.) double-sided OW2H [BHH+19]

$G_1, G_2 : X \to Y$

$S = \{x^*\}$ s. th. $G_1(x) = G_2(x)$ for all $x \neq x^*$

z: input to A

'double-sided' OW2H doesn't lose q:

$$\left|\Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}_1}(z)\right] - \Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}_2}(z)\right]\right| \leq 2 \cdot \sqrt{\Pr\left[x \leftarrow \mathsf{Ext}^{\mathsf{G}_1,\mathsf{G}_2}(z)\right]}$$

(Simpl.) double-sided OW2H [BHH+19]

$G_1, G_2 : X \to Y$

$S = \{x^*\}$ s. th. $G_1(x) = G_2(x)$ for all $x \neq x^*$

z: input to A

'double-sided' OW2H doesn't lose q:

$$\left|\Pr\left[1 \leftarrow \mathsf{A}^{G_1}(z)\right] - \Pr\left[1 \leftarrow \mathsf{A}^{G_2}(z)\right]\right| \leq 2 \cdot \sqrt{\Pr\left[x \leftarrow \mathsf{Ext}^{G_1,G_2}(z)\right]}$$

Intuition: Ext^{G_1,G_2} runs A on G_1, G_2 in superposition

double-sided OW2H : The extractor

Running A on G_1, G_2 in superposition:

double-sided OW2H : The extractor

Running A on G_1, G_2 in superposition:

$U^{sup}_{G_1,G_2}$ = 'superposition evaluation' of G_1, G_2:

- map $|x, y, +\rangle$ to $|x, y \oplus G_1(x), +\rangle$
- map $|x, y, -\rangle$ to $|x, y \oplus G_2(x), -\rangle$

double-sided OW2H : The extractor

Running A on G_1, G_2 in superposition:

$U^{\mathrm{sup}}_{G_1,G_2}$ = 'superposition evaluation' of G_1, G_2:

- map $|x, y, +\rangle$ to $|x, y \oplus G_1(x), +\rangle$
- map $|x, y, -\rangle$ to $|x, y \oplus G_2(x), -\rangle$

'swapping' unitary S: map $|x, y, b, x'\rangle$ to $|x, y, b, x' \oplus b \cdot x\rangle$

double-sided OW2H : The extractor

Running A on G_1, G_2 in superposition:

$U^{sup}_{G_1,G_2}$ = 'superposition evaluation' of G_1, G_2:

- map $|x, y, +\rangle$ to $|x, y \oplus G_1(x), +\rangle$
- map $|x, y, -\rangle$ to $|x, y \oplus G_2(x), -\rangle$

'swapping' unitary S: map $|x, y, b, x'\rangle$ to $|x, y, b, x' \oplus b \cdot x\rangle$

Evaluate-and-swap:

$\tilde{U}_{G_1,G_2} = S \circ U^{sup}_{G_1,G_2} \circ S^\dagger$

double-sided OW2H : The extractor

Running A on G_1, G_2 in superposition:

$U^{sup}_{G_1,G_2}$ = 'superposition evaluation' of G_1, G_2:

- map $|x, y, +\rangle$ to $|x, y \oplus G_1(x), +\rangle$
- map $|x, y, -\rangle$ to $|x, y \oplus G_2(x), -\rangle$

'swapping' unitary S: map $|x, y, b, x'\rangle$ to $|x, y, b, x' \oplus b \cdot x\rangle$

Evaluate-and-swap:

$\tilde{U}_{G_1,G_2} = S \circ U^{sup}_{G_1,G_2} \circ S^\dagger$

- $\tilde{U}_{G_1,G_2}|x, y, 0, 0\rangle = U_{G_1}|x, y\rangle \otimes |0, 0\rangle$ for $x \neq x^*$, but
- $\tilde{U}_{G_1,G_2}|x^*, y, 0, 0\rangle$ contains $\frac{1}{2} \cdot |1, x^*\rangle$ in last two reg.

double-sided OW2H : The extractor

Running A on G_1, G_2 in superposition:

Evaluate-and-swap:

$\tilde{U}_{G_1,G_2} = S \circ U^{sup}_{G_1,G_2} \circ S^\dagger$

double-sided OW2H : The extractor

Running A on G_1, G_2 in superposition:

Evaluate-and-swap:

$$\tilde{U}_{G_1,G_2} = S \circ U^{sup}_{G_1,G_2} \circ S^\dagger$$

$$A^G = U^A_q \circ U_G \circ U^A_{q-1} \circ U_G \circ \cdots \circ U_G \circ U^A_1$$

double-sided OW2H : The extractor

Running A on G_1, G_2 in superposition:

Evaluate-and-swap:

$\tilde{U}_{G_1,G_2} = S \circ U^{sup}_{G_1,G_2} \circ S^\dagger$

$A^G = U^A_q \circ U_G \circ U^A_{q-1} \circ U_G \circ \cdots \circ U_G \circ U^A_1$

Ext^{G_1,G_2}:

- Prepare registers for A and additionally $|0, 0_X\rangle$
- Apply $U^A_q \circ \tilde{U}_{G_1,G_2} \circ U^A_{q-1} \circ \tilde{U}_{G_1,G_2} \circ \cdots \circ \tilde{U}_{G_1,G_2} \circ U^A_1$
- Measure last register and output the result

double-sided OW2H : Conclusion

'double-sided' OW2H doesn't lose q:

$$\left|\Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}_1}(z)\right] - \Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}_2}(z)\right]\right| \leq 2 \cdot \sqrt{\Pr\left[x \leftarrow \mathsf{Ext}^{\mathsf{G}_1,\mathsf{G}_2}(z)\right]}$$

Tighter bound if reduction knows how to simulate both oracles

(Simpl.) MRM-OW2H [KSS+20]

$G_1, G_2 : X \to Y$

$S \subset X$ s. th. $G_1(x) = G_2(x)$ for all $x \notin S$

z: input to A

No square-root loss:

(Simpl.) MRM-OW2H [KSS+20]

$G_1, G_2 : X \to Y$

$S \subset X$ s. th. $G_1(x) = G_2(x)$ for all $x \notin S$

z: input to A

No square-root loss:

$$\left|\Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}_1}(z)\right] - \Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}_2}(z)\right]\right|$$

$$\leq 4q \cdot \Pr\left[S' \cap S \neq \emptyset : S' \leftarrow \mathsf{Ext}^{\mathsf{G}_1,\mathsf{G}_2}(z)\right]$$

(Simpl.) MRM-OW2H [KSS+20]

$G_1, G_2 : X \to Y$

$S \subset X$ s. th. $G_1(x) = G_2(x)$ for all $x \notin S$

z: input to A

No square-root loss:

$$\left|\Pr\left[1 \leftarrow \mathsf{A}^{G_1}(z)\right] - \Pr\left[1 \leftarrow \mathsf{A}^{G_2}(z)\right]\right|$$

$$\leq 4q \cdot \Pr\left[S' \cap S \neq \emptyset : S' \leftarrow \mathsf{Ext}^{G_1,G_2}(z)\right]$$

Intuition: Extraction from query or distinguishing measurement

MRM-OW2H : The extractor

Ext^{G_1,G_2}:

- Pick random $i \in \{1, \cdots, q\}$

MRM-OW2H : The extractor

$\mathsf{Ext}^{\mathsf{G}_1,\mathsf{G}_2}$:

- Pick random $i \in \{1, \cdots, q\}$
- x': Extract from i-th query, using $\mathsf{U}^{\mathsf{sup}}_{\mathsf{G}_1,\mathsf{G}_2}$

MRM-OW2H : The extractor

Ext^{G_1,G_2}:

- Pick random $i \in \{1, \cdots, q\}$
- x': Extract from i-th query, using $U^{sup}_{G_1,G_2}$
- x'': Run A with switching oracles, rewind, measure:

MRM-OW2H : The extractor

$\mathsf{Ext}^{\mathsf{G}_1,\mathsf{G}_2}$:

- Pick random $i \in \{1, \cdots, q\}$
- x': Extract from i-th query, using $\mathsf{U}^{\mathsf{sup}}_{\mathsf{G}_1,\mathsf{G}_2}$
- x'': Run A with switching oracles, rewind, measure:
  - Use G_1 until i-th query
  - Handle i-th query with $\mathsf{U}^{\mathsf{sup}}_{\mathsf{G}_1,\mathsf{G}_2}$
  - Switch to G_2 after i-th query
  - Let A finish and rewind until i-th query
  - Measure input resister

MRM-OW2H : The extractor

$\mathsf{Ext}^{\mathsf{G}_1,\mathsf{G}_2}$:

- Pick random $i \in \{1, \cdots, q\}$
- x': Extract from i-th query, using $\mathsf{U}^{\mathsf{sup}}_{\mathsf{G}_1,\mathsf{G}_2}$
- x'': Run A with switching oracles, rewind, measure:
  - Use G_1 until i-th query
  - Handle i-th query with $\mathsf{U}^{\mathsf{sup}}_{\mathsf{G}_1,\mathsf{G}_2}$
  - Switch to G_2 after i-th query
  - Let A finish and rewind until i-th query
  - Measure input resister
- return $S' := \{x', x''\}$

double-sided OW2H : Conclusion

'double-sided' OW2H doesn't lose q:

$$\left|\Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}_1}(z)\right] - \Pr\left[1 \leftarrow \mathsf{A}^{\mathsf{G}_2}(z)\right]\right|$$

$$\leq 4q \cdot \Pr\left[S' \cap S \neq \emptyset : S' \leftarrow \mathsf{Ext}^{\mathsf{G}_1,\mathsf{G}_2}(z)\right]$$

Tighter bound if reduction knows how to simulate both oracles

Further extensions of OW2H

Compressed oracles: [CMSZ19]

- puncture oracle database wrt relation
- Bound: $\sqrt{q \cdot \mathsf{FIND}}$
- reduction must know the relation

Further extensions of OW2H

Compressed oracles: [CMSZ19]

- puncture oracle database wrt relation
- Bound: $\sqrt{q \cdot \mathrm{FIND}}$
- reduction must know the relation

Adaptively chosen positions: GHHM21

- Oracle gets reprogrammed on (x_1, x_2)
- A chooses x_1, game chooses x_2
- Bound: $\frac{3}{2}\sqrt{q \cdot \max \Pr[x_2]}$

Summary

Comparison of OW2H variants

OW2H variant	Bound	# points	Reduction must know
Original	$q \cdot \sqrt{\mathsf{EXTRACT}}$	1	
Semi-classical 1	$\sqrt{q \cdot \mathsf{FIND}}$	arb	S
Semi-classical 2	$q \cdot \sqrt{\mathsf{EXTRACT}}$	arb	
Double-sided	$\sqrt{\mathsf{EXTRACT}}$	1	$\mathsf{G}_1, \mathsf{G}_2$
MRM	$q \cdot \mathsf{EXTRACT}$	arb	$\mathsf{G}_1, \mathsf{G}_2$
Compr oracle	$\sqrt{q \cdot \mathsf{FIND}}$	arb	Puncturing relation
Adaptive	$\frac{3R}{2}\sqrt{q \cdot \max \Pr[x_2]}$	R	How to sample x_2

EXTRACT: Probability of extracting a repr. position

FIND: Probability of measuring repr. position in query/database

Thanks for listening!

quantum_bat

[Unruh14]: D. Unruh. Revocable quantum timed-release encryption

[AHU19]: Ambainis et al. Quantum security proofs using semi-classical oracles

[BHH+20]: Bindel et al. Tighter proofs of CCA security in the quantum random oracle model

[KSS+20]: Kuchta et al. Measure-Rewind-Measure: Tighter Quantum Random Oracle Model Proofs for One-Way to Hiding and CCA Security

[CMSZ19]: Czajkowski et al. Quantum Lazy Sampling and Game-Playing Proofs for Quantum Indifferentiability

[GHHM21] Grilo et al. Tight adaptive reprogramming in the QROM