Building Quantum-One-Way Functions from Block Ciphers: Davies-Meyer and Merkle-Damgård Constructions

Akinori Hosoyamada (NTT / Nagoya University) and Kan Yasuda(NTT)

2018.12.3 Asiacrypt 2018 @ Brisbane

Outline

- **Backgrounds**
  - Post-quantum security of sym-key schemes
  - Are hash functions post-quantum secure?
- **Our Results**
- **Summary**

Outline

- **Backgrounds**
  - Post-quantum security of sym-key schemes
  - Are hash functions post-quantum secure?
- **Our Results**
- **Summary**

Symmetric-key & quantum: backgrounds

“the security of symmetric key crypto will not be affected by quantum computers”

Known quantum attacks : ～２０１０

	Classical	Quantum
Exhaustive Key search	$O(2^n)$	$O(2^{n/2})$
Collision search	$O(2^{n/2})$	$O(2^{n/3})$

“It is sufficient to use 2n-bit keys instead of n-bit keys”

Known attacks : 2018

	Classical	Quantum
Exhaustive Key search	$O(2^n)$	$O(2^{n/2})$
Collision search	$O(2^{n/2})$	$O(2^{n/3})$
Key recovery attack against Even-Mansour	$O(2^{n/2})$	Poly-time
Forgery attack against CBC-like MACs	$O(2^{n/2})$	Poly-time

Note：We assume that quantum oracles are available

Symmetric-key & quantum: backgrounds

~~“the security of sy ic key crypto would not be affected b um computers”~~

Poly-time attack is possible !!

- The works by Kuwakado and Morii (ISIT 2010, ISITA 2012)
- The work by Kaplan et al. (CRYPTO 2016)

Symmetric-key & quantum: backgrounds

~~“the security of sy ic key crypto would not be affected b qu um computers”~~

Poly-time attack is possible !!

- The works by Kuwakado and Morii (ISIT 2010, ISITA 2012)
- The work by Kaplan et al. (CRYPTO 2016)

We should study post-quantum security of symmetric key crypto carefully

Outline

- **Backgrounds**
  - Post-quantum security of sym-key schemes
  - Are hash functions post-quantum secure?
- **Our Results**
- **Summary**

Outline

- **Backgrounds**
  - Post-quantum security of sym-key schemes
  - Are hash functions post-quantum secure?
- **Our Results**
- **Summary**

Post-quantum security requirement for hash

Hash functions should be secure against quantum superposition query attacks

- **Reason: Hash functions are public and used to instantiate QRO (Quantum Random Oracle)**
  - Many post-quantum public-key schemes are proven to be secure in the quantum random oracle model

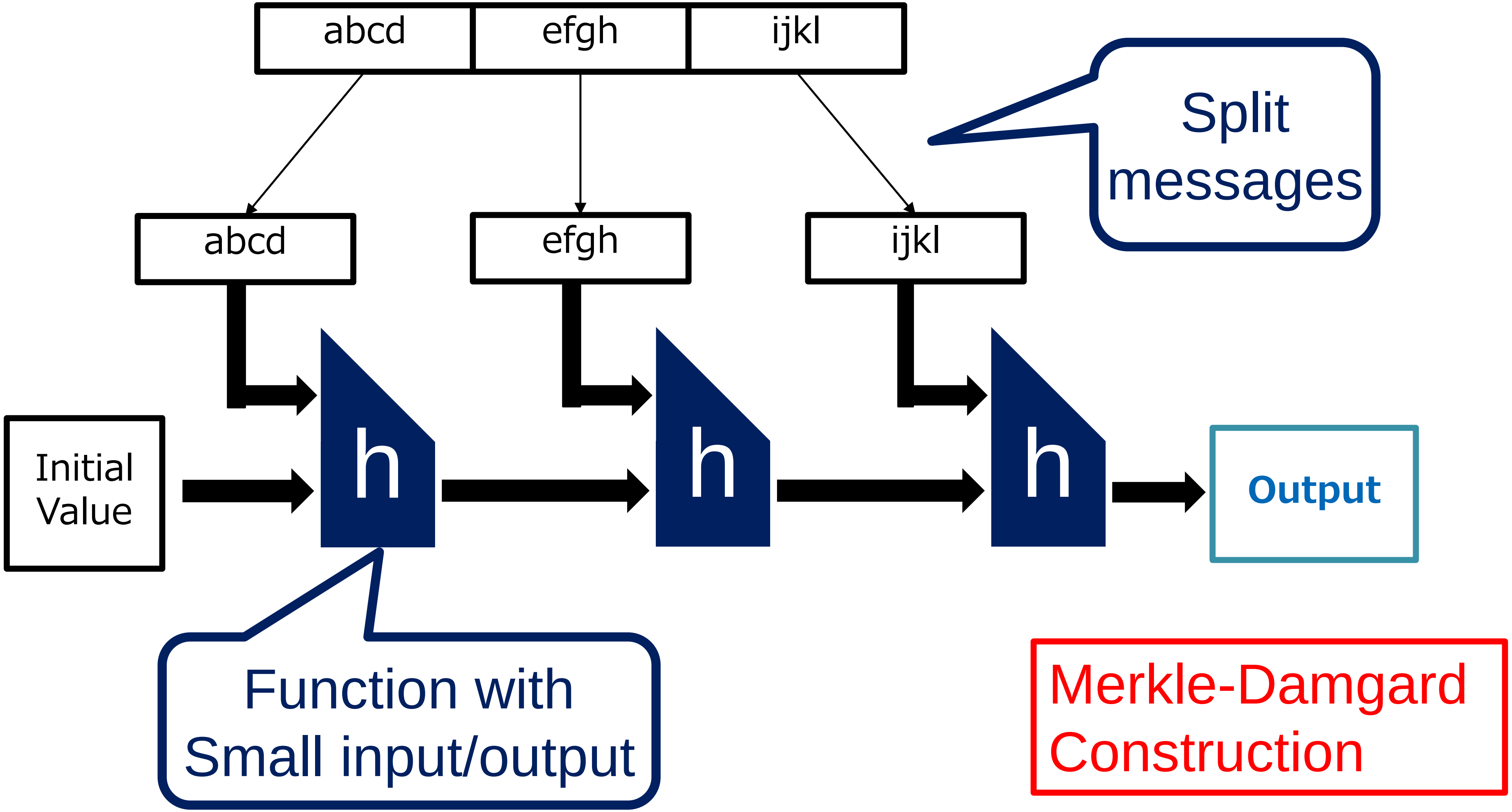
Hash-based signature, Key Exchange,…

Post-quantum security requirement for hash

Hash functions should be secure against quantum superposition query attacks

We study security of
typical hash constructions:
Merkle-Damgård with Davies-Meyer

Typical construction:
Merkle-Damgård with Davies Meyer



abcd efgh ijkl

abcd

efgh

ijkl

Split messages

Initial Value

h

h

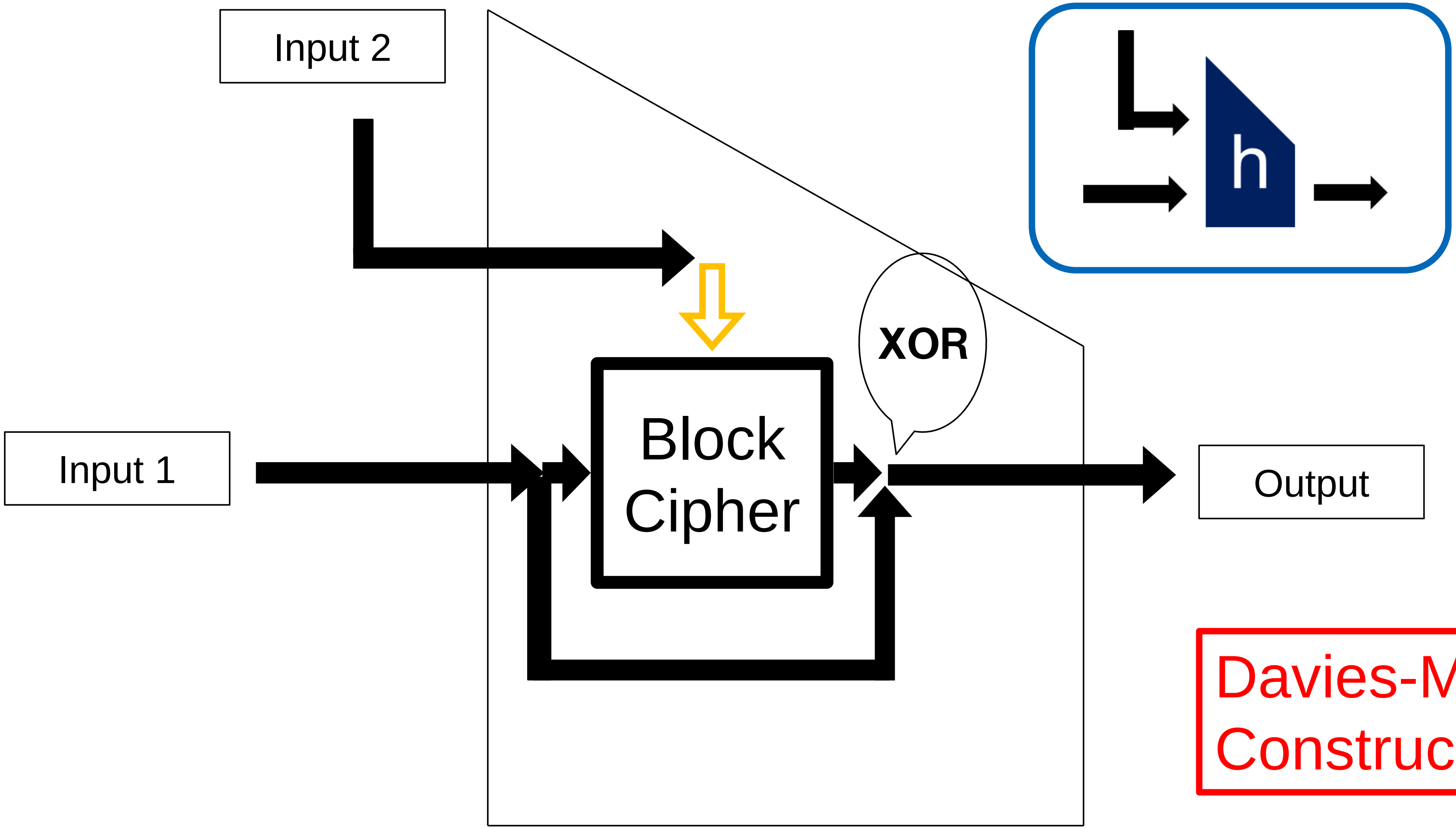
h

Output

Function with Small input/output

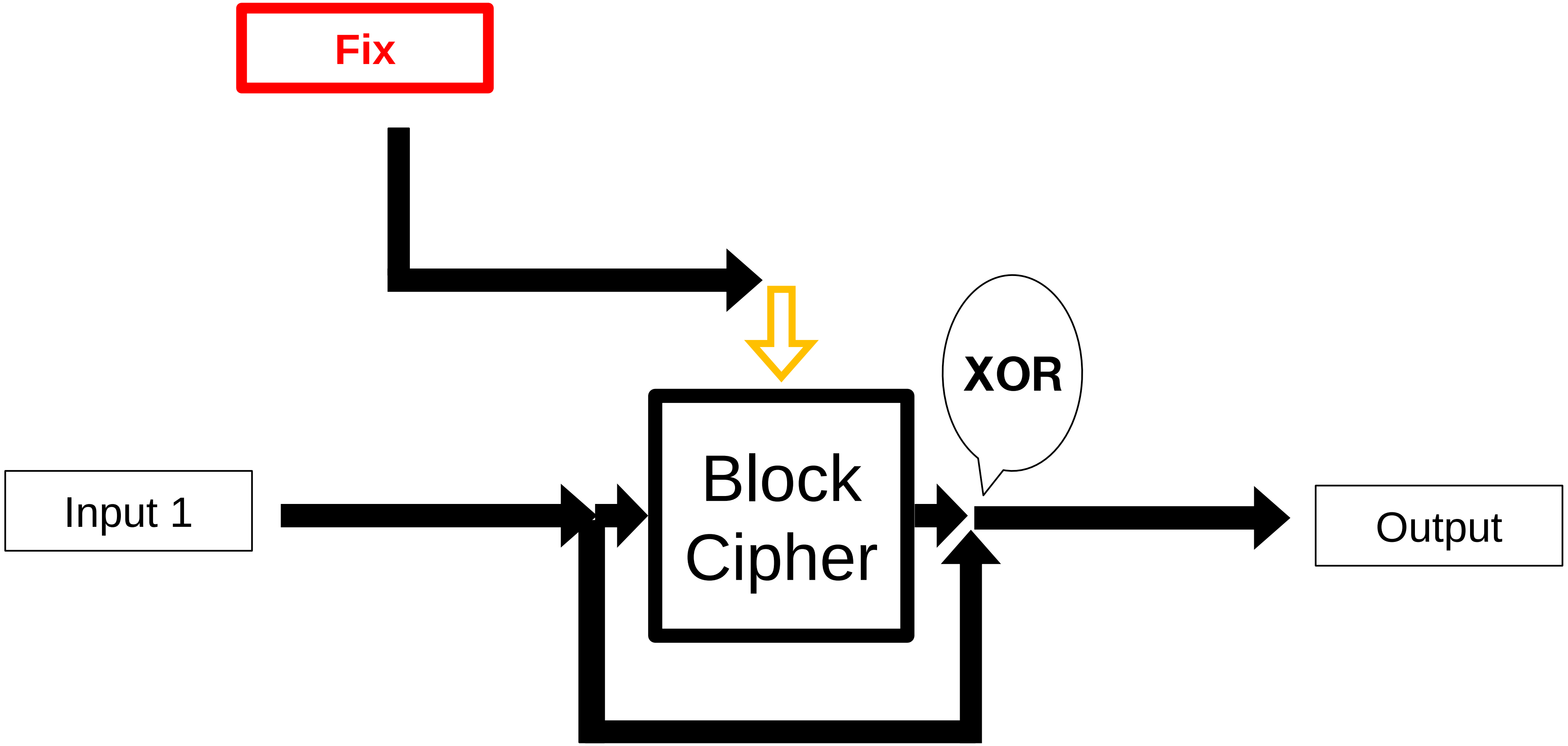
Merkle-Damgard Construction

Typical construction: Merkle-Damgård with Davies Meyer

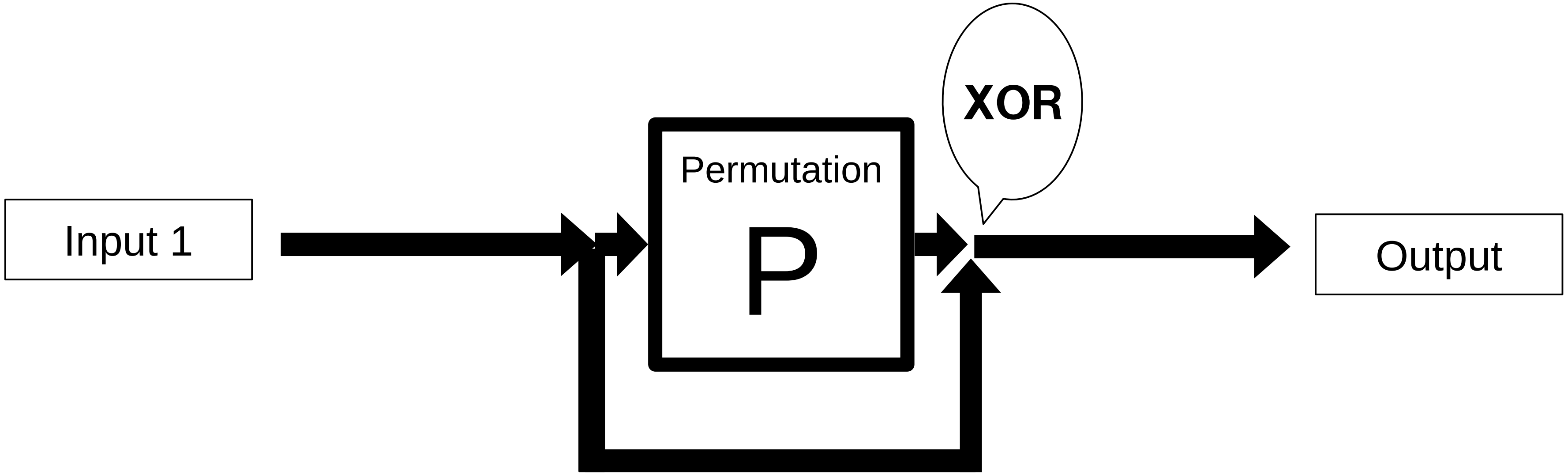


Davies-Meyer Construction

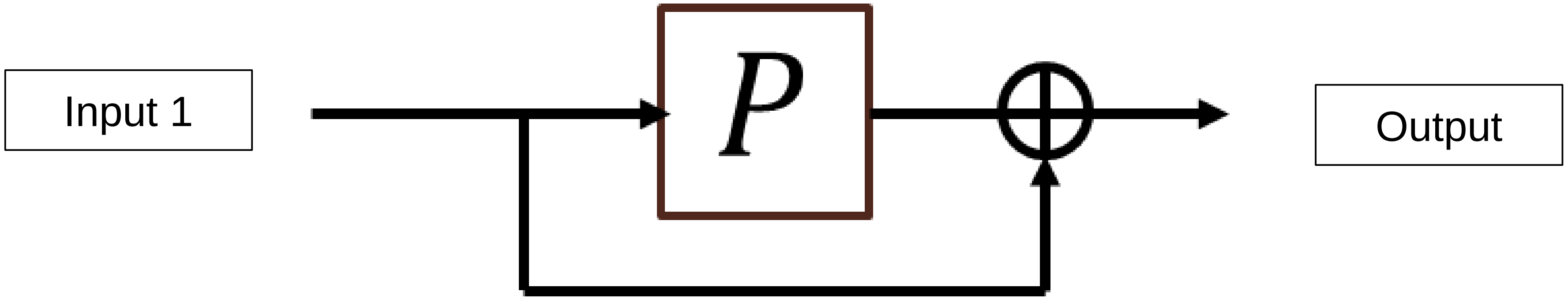
Typical construction: Merkle-Damgård with Davies Meyer



Typical construction: Merkle-Damgård with Davies Meyer

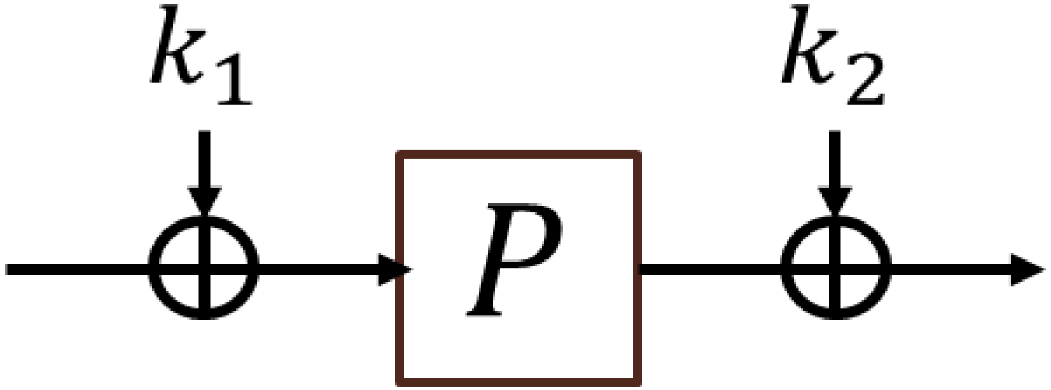


Typical construction:
Merkle-Damgård with Davies Meyer



Quantum insecure construction: Even-Mansour cipher

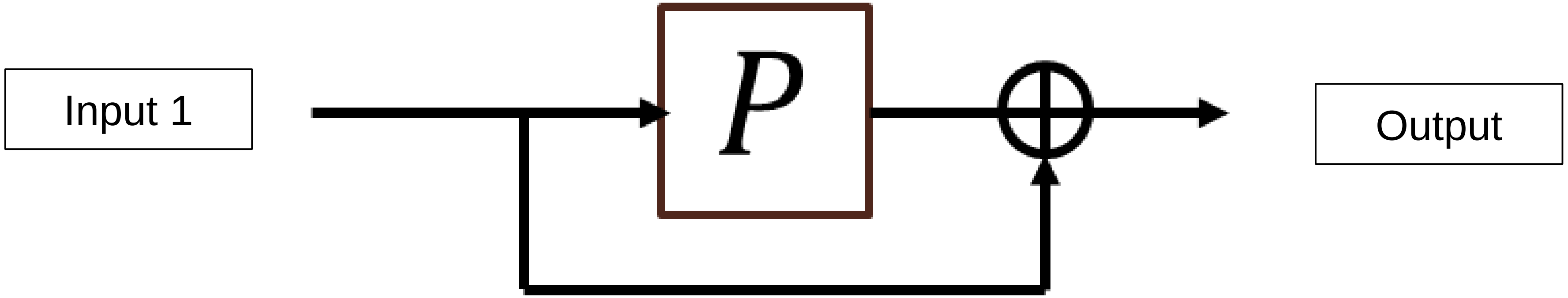
Quantum insecure



Permutation & XOR

Typical construction:
Merkle-Damgård with Davies Meyer

Simplified Hash function

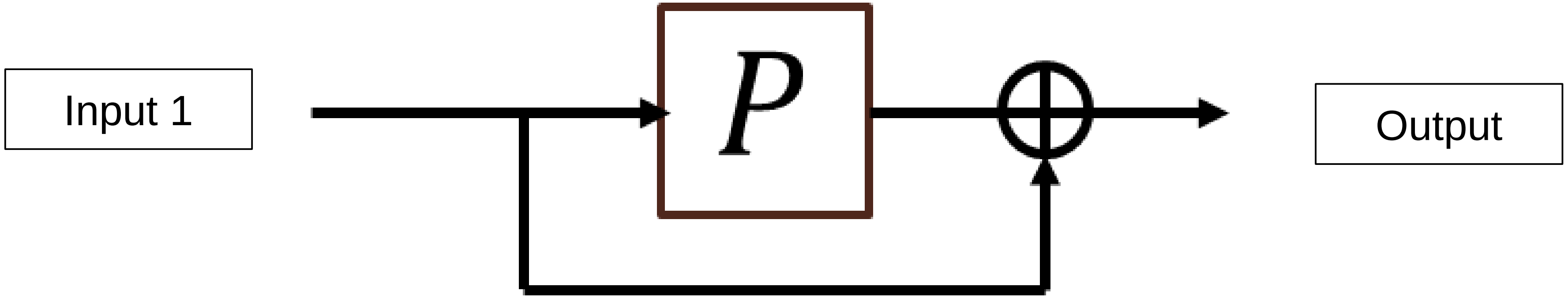


Permutation & XOR

Typical construction:
Merkle-Damgård with Davies Meyer

Is this secure????

Simplified Hash function



Permutation & XOR

Typical construction: Merkle-Damgård with Davies Meyer

Is

sec

Let’s try to come up with a Poly-time attack !!

☺

Permutation & XOR

Typical construction:
Merkle-Damgård with Davies Meyer

Is th

sec

Let’s try to co

oly-time attack !!

P

mutation &

OR

Typical construction:
Merkle-Damgård with Davies Meyer

Is thi

sec

Let’s try to co oly-time attack !!

It seems impossible

Pe mutation & XOR

It is hard to make poly-time attacks…

Why impossible?

It is hard to make poly-time attacks…

Why impossible?

- **Strategy of quantum poly-time attacks:**
  1. Make a periodic function with a secret period
  2. Apply Simon’s period finding algorithm

Hash functions have no secret information!!

It is hard to make poly-time attacks…

Why impossible?

•S

If attack is impossible,
let’s give a security proof

od

Hash functions have no secret information!!

Security notions for hash functions

1. Preimage resistance (One-wayness)
2. Second preimage resistance
3. Collision resistance

"Post-quantum secure" hash functions must satisfy all of them *against quantum superposition attackers*

Security notions for hash functions

1. **Preimage resistance (One-wayness)**
2. Second
image resistance
3. Col

Our focus

“Post-quantum secure” hash functions must satisfy all of them *against quantum superposition attackers*

Outline

- **Backgrounds**
  - Post-quantum security of sym-key schemes
  - Are hash functions post-quantum secure?
- **Our Results**
- **Summary**

Outline

- Backgrounds
  - Post-quantum security of sym-key schemes
  - Are hash functions post-quantum secure?
- **Our Results**
- Summary

Our results

Results

1. **Proposal of a quantum version of the ideal cipher model**

2. **Proof of optimal one-wayness** ($2^{n/2}$ quantum queries are required to break one-wayness) **of the combination of Merkle-Damgård with Davies-Meyer (fixed block length, with a specific padding)**

3. **A proof technique to show quantum oracle indistinguishability**

Our results

Results

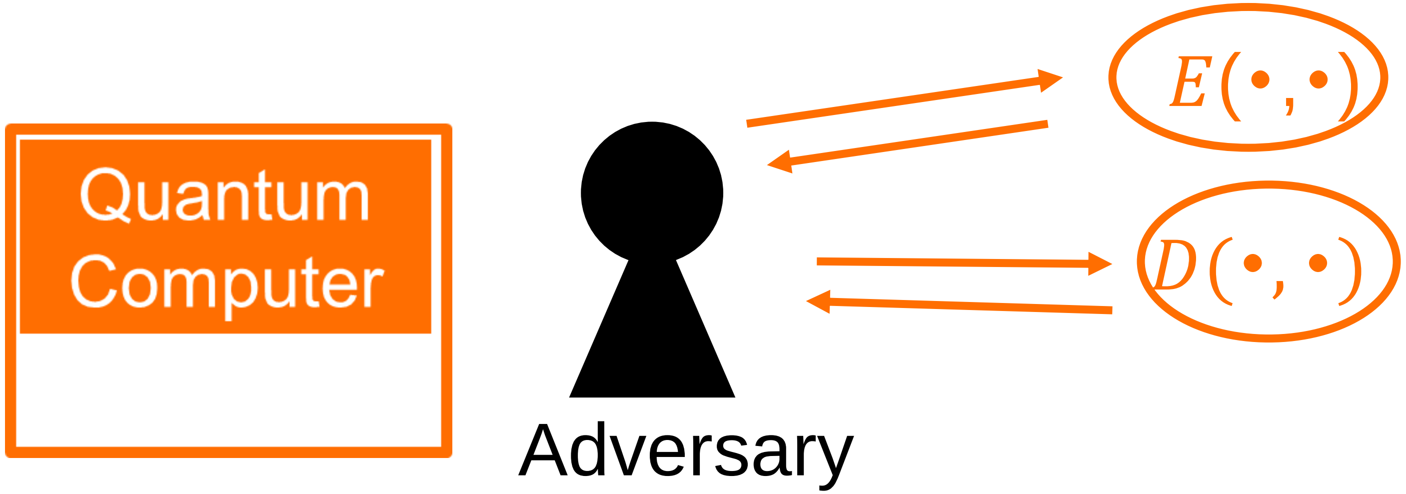
1. **Proposal of a quantum version of the ideal cipher model**

2. **Proof of optimal one-wayness** ($2^{n/2}$ quantum queries are required to break one-wayness) **of the combination of Merkle-Damgård with Davies-Meyer** **(fixed block length, with a specific padding)**

3. **A proof technique to show quantum oracle indistinguishability**

Quantum ideal cipher model

- **Quantum ideal cipher model**
  - Permutation $\boxed{E_K}$ is chosen at random for each key K, and given to the adversary as a quantum black-box oracle
  - Adversary can make quantum superposition queries to both Enc oracle and Dec oracle



Quantum oracles

Quantum ideal cipher model

$$E_K \xleftarrow{\$} \mathrm{Perm}(\{0,1\}^n) \text{ for each } K$$

Oracle O_E :

$$|0\rangle|k\rangle|x\rangle|y\rangle \mapsto |0\rangle|x\rangle|k\rangle|y \oplus E_k(x)\rangle$$

$$|1\rangle|k\rangle|x\rangle|y\rangle \mapsto |1\rangle|k\rangle|x\rangle|y \oplus D_k(x)\rangle$$

Our results

Results

1. Proposal of a quantum version of the ideal cipher model

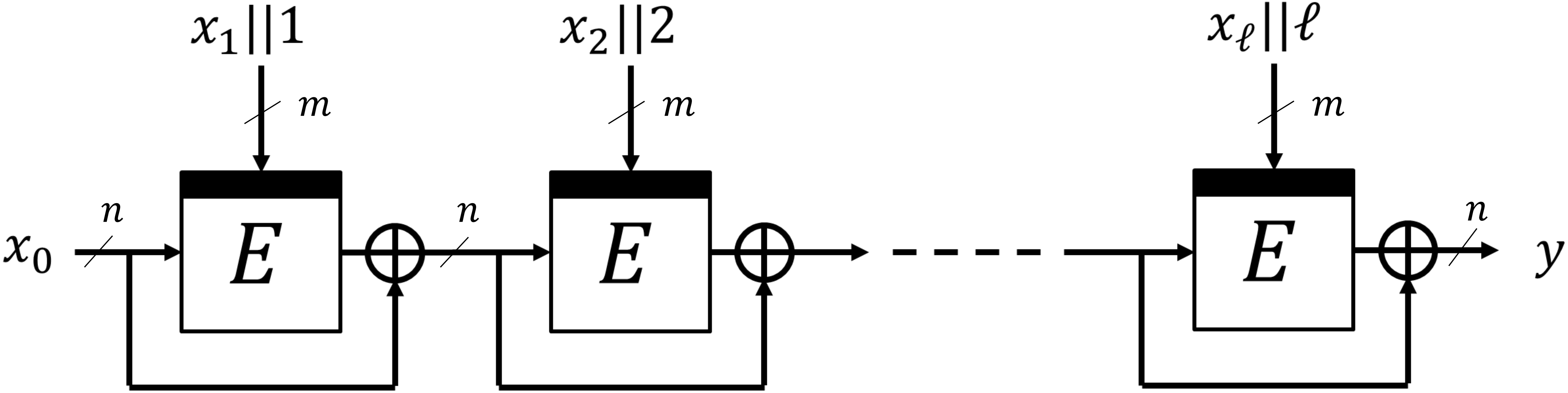
2. **Proof of optimal one-wayness** ($2^{n/2}$ quantum queries are required to break one-wayness) **of the combination of Merkle-Damgård with Davies-Meyer (fixed block length, with a specific padding)**

3. A proof technique to show quantum oracle indistinguishability

Our Construction:Merkle-Damgård with Davies-Meyer
(fixed block-length, with a specific padding)

Input: $x = x_0 || x_1 || \cdots || x_\ell$ ($x_0 \in \{0,1\}^n$ and $x_1, \ldots, x_\ell \in \{0,1\}^{n'}$, $n' < n$)

Output: $y \in \{0,1\}^n$



Our second result

Theorem 5.2

For any quantum q-query adversary A,

$$\mathrm{Adv}^{\mathrm{ow}}_{H^E}(A) \leq O\left(q/2^{n/2}\right) + \text{small terms}$$

holds.

H^E is Merkle-Damgård with Davies-Meyer
(fixed block length and specific padding)

Our second result

Theorem 5.2

For any quantum q-query adversary A,

$$\mathrm{Adv}^{\mathrm{ow}}_{H^E}(A) \leq O\left(q/2^{n/2}\right) + \text{small terms}$$

holds.

H^E is Merkle-Damgård with Davies-Meyer
(fixed block length and specific padding)

Giving a proof
= giving a quantum query lower bound

Remarks on query lower bound

Area [Model]	Problems	Backward query?
Quantum computation	Worst case	×
Cryptography [(Q)ROM] (Quantum) Random Oracle Model	Average case (randomized)	×
Cryptography [(Q)ICM] (Quantum) Ideal Cipher Model	Average case (randomized)	○

Our theorem is the first result on quantum query lower bound that takes backward queries to public permutations / BCs into account without any algebraic assumptions

Remarks on query lower bound

Area [Model]	Problems	Backward query?
Quantum computation	*Worst case*	×
Cryptography [(Q)ROM] (Quantum) Random Oracle Model	Average case (randomized)	×
Cryptography [(Q)ICM] (Quantum) Ideal Cipher Model	Average case (randomized)	○

Our theorem is the first result on quantum query lower bound that takes backward queries to public permutations / BCs into account without any algebraic assumptions

Remarks on query lower bound

Area [Model]	Problems	Backward query?
Quantum computation	Worst case	×
Cryptography [(Q)ROM] (Quantum) Random Oracle Model	*Average case (randomized)*	×
Cryptography [(Q)ICM] (Quantum) Ideal Cipher Model	*Average case (randomized)*	○

Our theorem is the first result on quantum query lower bound that takes <u>backward queries to public permutations / BCs</u> into account without any algebraic assumptions

Remarks on query lower bound

Area [Model]	Problems	Backward query?
Quantum computation	Worst case	×
Cryptography *[(Q)ROM]* *(Quantum) Random Oracle Model*	Average case (randomized)	×
Cryptography [(Q)ICM] (Quantum) Ideal Cipher Model	Average case (randomized)	○

Our theorem is the first result on quantum query lower bound that takes backward queries to public permutations / BCs into account without any algebraic assumptions

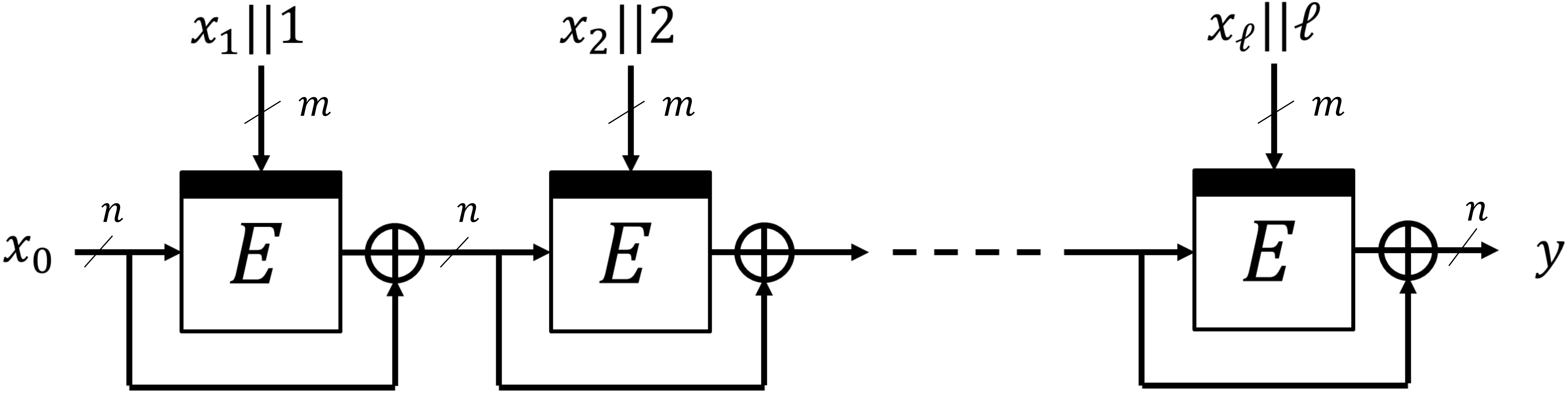
Remarks on query lower bound

Area [Model]	**Problems**	**Backward query?**
Quantum computation	Worst case	×
Cryptography [(Q)ROM] (Quantum) Random Oracle Model	Average case (randomized)	×
Cryptography *[(Q)ICM]* *(Quantum) Ideal Cipher Model*	Average case (randomized)	○

Our theorem is the first result on quantum query lower bound that takes backward queries to public permutations / BCs into account without any algebraic assumptions

Our Construction:Merkle-Damgård with Davies-Meyer

(fixed block-length, with a specific padding)

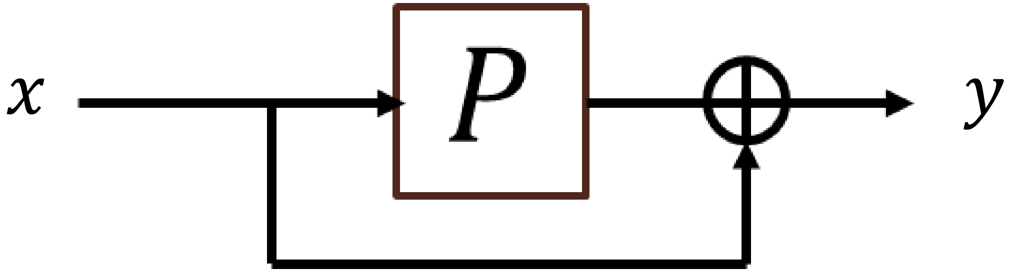


Somewhat complex…

Merkle-Damgård with Davies-Meyer

(with a specific padding)

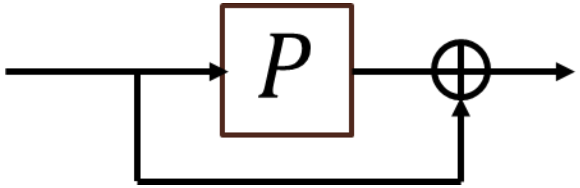
Lets' show this simplified function is one-way



One-wayness: proof strategy

It can be easily shown that:

Breaking one-wayness of

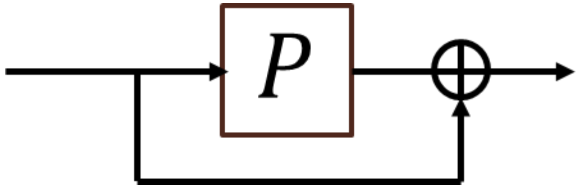


is almost as hard as

One-wayness: proof strategy

It can be easily shown that:

Breaking one-wayness of



is almost as hard as

Finding a <u>fixed point</u> of $\boxed{P}$

(An element x s.t. P(x)=x)

One-wayness: proof strategy

Next: I want to reduce

Finding a fixed point of $\boxed{P}$

to

One-wayness: proof strategy

Next: I want to reduce

Finding a fixed point of $\boxed{P}$

to

Distinguishing two distributions D_1, D_2 on $\mathrm{Func}(\{0,1\}^{\mathrm{n}}, \{0,1\})$

Since Boolean functions are much simpler than permutations

distributions D_1, D_2 on the set of boolean functions

- **Define D_1 on $\mathrm{Func}(\{0,1\}^\mathrm{n}, \{0,1\})$ as the distribution which corresponds to the following sampling:**

1. $P \leftarrow^{\$} \mathrm{Perm}(\{0,1\}^n)$
2. Define $f: \{0,1\}^n \rightarrow \{0,1\}$ by $f(x) = 1$ iff $P(x) = x$
3. Return f

- **D_1 is the “distribution of fixed points of RP”**

- **Define D_2 as the degenerate distribution on the zero function**

One-wayness: proof strategy

Intuitively,

Finding a fixed point of $\boxed{P}$

is almost as hard as

Distinguishing two distributions D_1, D_2 on $\mathrm{Func}(\{0,1\}^n, \{0,1\})$

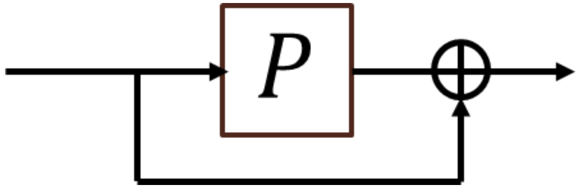
One-wayness: proof strategy

It is sufficient to show that

Distinguishing two distributions D_1, D_2 on $\mathrm{Func}(\{0,1\}^{\mathrm{n}}, \{0,1\})$ is hard

to show

Breaking one-wayness of



is hard

One-wayness: proof strategy

It is sufficient to show that

Distinguishing two distributions D_1, D_2 on $\mathrm{Func}(\{0,1\}^{\mathrm{n}}, \{0,1\})$ is hard

Brea

How to show it is hard?
→our third result

Our results

Results

1. **Proposal of a quantum version of the ideal cipher model**

2. **Proof of optimal one-wayness** ($2^{n/2}$ quantum queries are required to break one-wayness) **of the combination of Merkle-Damgård with Davies-Meyer** **(fixed block length, with a specific padding)**

3. **A proof technique to show quantum oracle indistinguishability**

Our third result

Proposition 3.2

Let D_1 be arbitrary distribution on $\mathrm{Func}(\{0,1\}^n, \{0,1\})$, and D_2 be the degenerate distribution on the zero function. Then

$$\mathrm{Adv}^{\mathrm{dist}}_{D_1,D_2}(A) \leq 2q \sum_{\alpha} p_1^{\mathrm{good}_\alpha} \sqrt{p_1^{f|\mathrm{good}_\alpha} \max_x |\{f \in \mathrm{good}_\alpha | f(x) = 1\}|}$$

$$+ \Pr_{F \sim D_1}[F \in \mathrm{bad}]$$ holds.

$\{\mathrm{good}_\alpha\}_\alpha \cdots$ a set of subsets of $\mathrm{Func}(\{0,1\}^n, \{0,1\})$

$\mathrm{bad} \coloneqq \mathrm{Func}(\{0,1\}^n, \{0,1\}) \setminus (\cup_\alpha \mathrm{good}_\alpha)$

$p_1^{\mathrm{good}_\alpha} \coloneqq \Pr_{\mathrm{F} \sim D_1}[F \in \mathrm{good}_\alpha], p_1^{f|\mathrm{good}_\alpha} \coloneqq \Pr_{\mathrm{F} \sim D_1}[F = f | F \in \mathrm{good}_\alpha]$

Condition: $\mathrm{good}_\alpha \cap \mathrm{good}_\beta = \emptyset$,and $p_1^{f|\mathrm{good}_\alpha}$is independendet of f

Our third result

Proposition 3.2

Let D_1 be arbitrary distribution on $\mathrm{Func}(\{0,1\}^n, \{0,1\})$, and D_2 be the degenerate distribution on the zero function. Then

$$\mathrm{Adv}^{\mathrm{dist}}_{D_1,D_2}(A) \leq 2q \sum_{\alpha} p_1^{\mathrm{good}_\alpha} \sqrt{p_1^{f|\mathrm{good}_\alpha} \max_x |\{f \in \mathrm{good}_\alpha | f(x) = 1\}|} + \Pr_{F \sim D_1}[F \in \mathrm{bad}]$$

holds.

We can give an upper bound of the advantage with only calculations of ***classical*** probabilities, if we can choose some “good” subsets of $\mathrm{Func}(\{0,1\}^n, \{0,1\})$

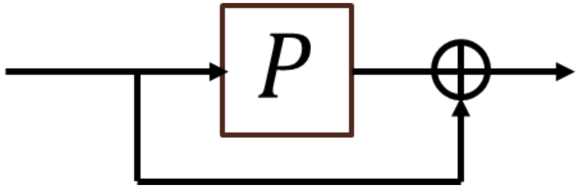
Recall arguments on our second result…

It is sufficient to show that

Distinguishing two distributions D_1, D_2 on $\mathrm{Func}(\{0,1\}^{\mathrm{n}}, \{0,1\})$ is hard

to show

Breaking one-wayness of



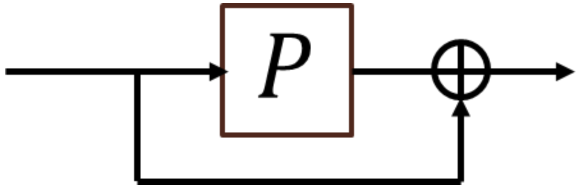
is hard

Recall arguments on our second result…

With our third result, we can show

$O(2^{n/2})$ queries are required to distinguish D_1, D_2 with a constant probability

Breaking one-wayness of



is hard

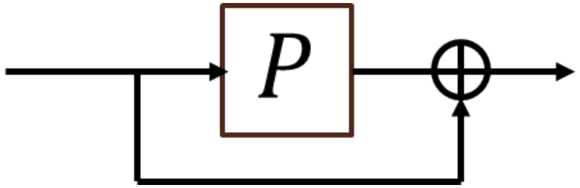
Recall arguments on our second result…

With our third result, we can show

$O(2^{n/2})$ queries are required to distinguish D_1, D_2 with a constant probability

thus

○ Breaking one-wayness of



is hard

Outline

- Backgrounds
  - Post-quantum security of sym-key schemes
  - Are hash functions post-quantum secure?
- Our Results
- Summary

Summary

- The combination of Merkle-Damgård with Davies-Meyer is one-way in "quantum ideal cipher model" (fixed block-length, with specific padding)
- The first result on quantum query lower bound that takes backward queries to public permutations or block ciphers into account w/o any algebraic assumptions
- A technique to show quantum oracle indistinguishability

Thank you!