Post-Quantum Security of the Even-Mansour Cipher

Gorjan Alagic, Chen Bai, Jonathan Katz and **Christian Majenz**

Eurocrypt 2022, Trondheim

Outline

- Motivation
- Introduction
- Result
- Techniques, Technical Contributions

Motivation

Quantum attacks

Quantum attacks

Post-quantum attacks

Public-key cryptography: Shor's algorithm

Quantum attacks

Post-quantum attacks

Public-key cryptography: Shor's algorithm

- RSA

Quantum attacks

Post-quantum attacks

Public-key cryptography: Shor's algorithm

- RSA
- Discrete Log

Quantum attacks

Post-quantum attacks

Public-key cryptography: Shor's algorithm

- RSA
- Discrete Log

complete break!

Quantum attacks

Post-quantum attacks

Public-key cryptography: Shor's algorithm

- RSA
- Discrete Log

complete break!

Symmetric cryptography: Grover search&friends

Quantum attacks

Post-quantum attacks

Public-key cryptography: Shor's algorithm

- RSA
- Discrete Log

complete break!

Symmetric cryptography: Grover search&friends

- Block ciphers

Quantum attacks

Post-quantum attacks

Public-key cryptography: Shor's algorithm

- RSA
- Discrete Log

complete break!

Symmetric cryptography: Grover search&friends

- Block ciphers
- Hash functions

Quantum attacks

Post-quantum attacks

Public-key cryptography: Shor's algorithm

- RSA
- Discrete Log

complete break!

Symmetric cryptography: Grover search&friends

- Block ciphers
- Hash functions
- Quantum-aided differential&linear cryptanalysis

Quantum attacks

Post-quantum attacks

Public-key cryptography: Shor's algorithm

- RSA
- Discrete Log

complete break!

Symmetric cryptography: Grover search&friends

- Block ciphers
- Hash functions
- Quantum-aided differential&linear cryptanalysis

Degraded security… but by how much?

Quantum attacks

Post-quantum attacks

Public-key cryptography: Shor's algorithm

- RSA
- Discrete Log

complete break!

Symmetric cryptography: Grover search&friends

- Block ciphers
- Hash functions
- Quantum-aided differential&linear cryptanalysis

Degraded security… but by how much?

Beyond post-quantum attacks

Symmetric cryptography: Simon's algorithm

Quantum attacks

Post-quantum attacks

Public-key cryptography: Shor's algorithm

- RSA
- Discrete Log

complete break!

Symmetric cryptography: Grover search&friends

- Block ciphers
- Hash functions
- Quantum-aided differential&linear cryptanalysis

Degraded security… but by how much?

Beyond post-quantum attacks

Symmetric cryptography: Simon's algorithm

- Even-Mansour

Quantum attacks

Post-quantum attacks

Public-key cryptography: Shor's algorithm

- RSA
- Discrete Log

complete break!

Symmetric cryptography: Grover search&friends

- Block ciphers
- Hash functions
- Quantum-aided differential&linear cryptanalysis

Degraded security... but by how much?

Beyond post-quantum attacks

Symmetric cryptography: Simon's algorithm

- Even-Mansour
- Block cipher modes of operation

Quantum attacks

Post-quantum attacks

Public-key cryptography: Shor's algorithm

- RSA
- Discrete Log

complete break!

Symmetric cryptography: Grover search&friends

- Block ciphers
- Hash functions
- Quantum-aided differential&linear cryptanalysis

Degraded security… but by how much?

Beyond post-quantum attacks

Symmetric cryptography: Simon's algorithm

- Even-Mansour
- Block cipher modes of operation

complete break in unrealistic model…

Quantum attacks

Post-quantum attacks

Public-key cryptography: Shor's algorithm

- RSA
- Discrete Log

complete break!

Symmetric cryptography: Grover search&friends

- Block ciphers
- Hash functions
- Quantum-aided differential&linear cryptanalysis

Degraded security… but by how much?

Beyond post-quantum attacks

Symmetric cryptography: Simon's algorithm

- Even-Mansour
- Block cipher modes of operation

complete break in unrealistic model…

Post-quantum security for symmetric cryptography

Far less of a concern than for public-key crypto….

But we should prove post-quantum security where possible!

Introduction

Post-quantum security

Post-quantum security

Security against quantum attacks…

Post-quantum security

Security against quantum attacks…

But what *are* realistic quantum attacks?

Post-quantum security

Post-quantum attacks

Public-key cryptography: Shor's algorithm

- RSA
- Discrete Log

complete break!

Symmetric cryptography: Grover search&friends

- Block ciphers
- Hash functions
- Quantum-aided differential&linear cryptanalysis

Degraded security... but by how much?

Beyond post-quantum attacks

Symmetric cryptography: Simon's algorithm

- Even-Mansour
- Block cipher modes of operation

complete break in unrealistic model...

Post-quantum security

Post-quantum (Q1)

Beyond post-quantum (Q2)

Post-quantum security

Post-quantum (Q1)

- Quantum computation allowed

Beyond post-quantum (Q2)

- Quantum computation allowed

Post-quantum security

Post-quantum (Q1)

- Quantum computation allowed
- Quantum access to "offline primitives": QROM, Q-ideal permutation/ cipher etc.

Beyond post-quantum (Q2)

- Quantum computation allowed
- Quantum access to "offline primitives": QROM, Q-ideal permutation/ cipher etc.

Post-quantum security

Post-quantum (Q1)

- Quantum computation allowed
- Quantum access to “offline primitives”: QROM, Q-ideal permutation/cipher etc.

Beyond post-quantum (Q2)

- Quantum computation allowed
- Quantum access to “offline primitives”: QROM, Q-ideal permutation/cipher etc.
- **Quantum access** to online-primitives: **q**CPA, **q**CCA, **q**CMA…

Post-quantum security

Post-quantum (Q1)

- Quantum computation allowed
- Quantum access to "offline primitives": QROM, Q-ideal permutation/cipher etc.
- **Classical-only** access to online-primitives: CPA, CCA, CMA…

Beyond post-quantum (Q2)

- Quantum computation allowed
- Quantum access to "offline primitives": QROM, Q-ideal permutation/cipher etc.
- **Quantum access** to online-primitives: **q**CPA, **q**CCA, **q**CMA…

Post-quantum security

Post-quantum (Q1)

- Quantum computation allowed
- Quantum access to “offline primitives”: QROM, Q-ideal permutation/ cipher etc.
- **Classical-only** access to online-primitives: CPA, CCA, CMA…

Beyond post-quantum (Q2)

- Quantum computation allowed
- Quantum access to “offline primitives”: QROM, Q-ideal permutation/ cipher etc.
- **Quantum access** to online-primitives: **q**CPA, **q**CCA, **q**CMA…

Unrealistic

Post-quantum security

Post-quantum (Q1)

- Quantum computation allowed
- Quantum access to "offline primitives": QROM, Q-ideal permutation/cipher etc.
- **Classical-only** access to online-primitives: CPA, CCA, CMA…

Challenge: Mix of classical and quantum oracles!

Beyond post-quantum (Q2)

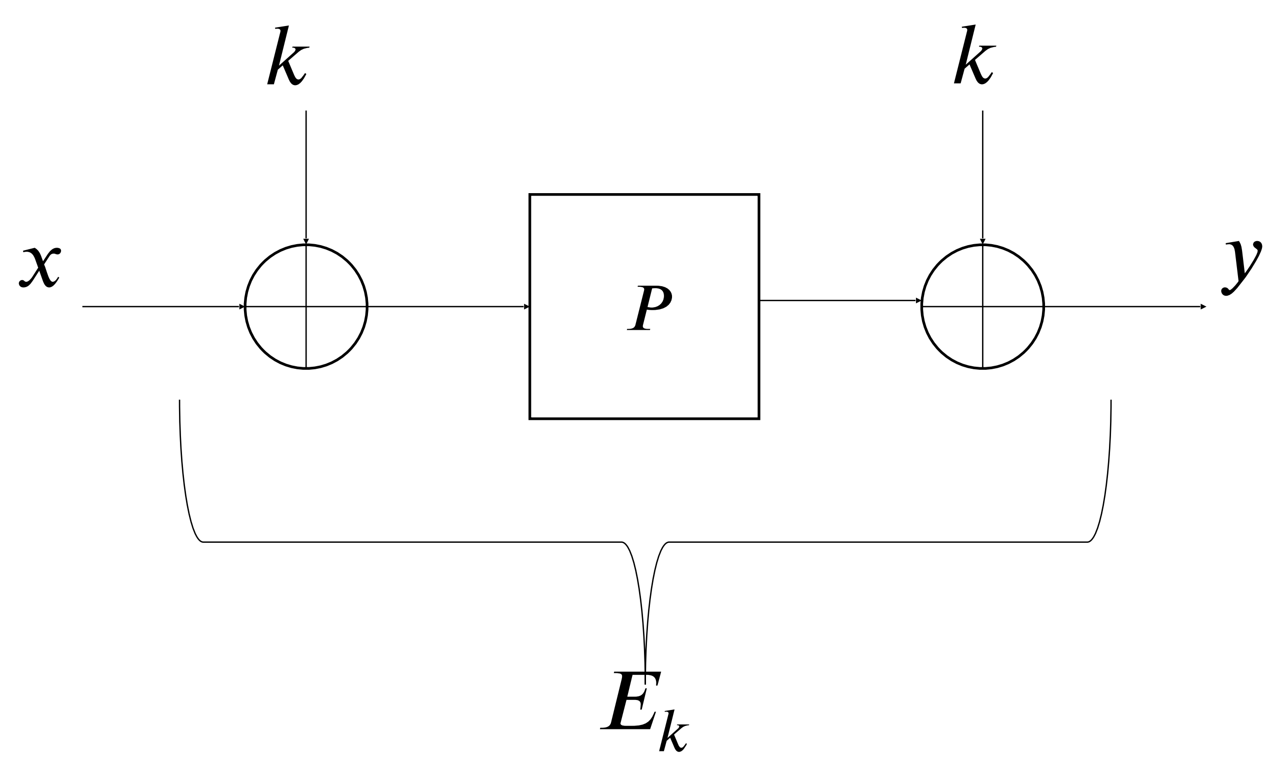
- Quantum computation allowed
- Quantum access to "offline primitives": QROM, Q-ideal permutation/cipher etc.
- **Quantum access** to online-primitives: **q**CPA, **q**CCA, **q**CMA…

Unrealistic

The Even-Mansour Cipher

Given a public permutation $P: \{0,1\}^n \to \{0,1\}^n$ and a key $k \in \{0,1\}^n$, the cipher $E: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is defined as:

$E_k[P](x) = P(x \oplus k) \oplus k$

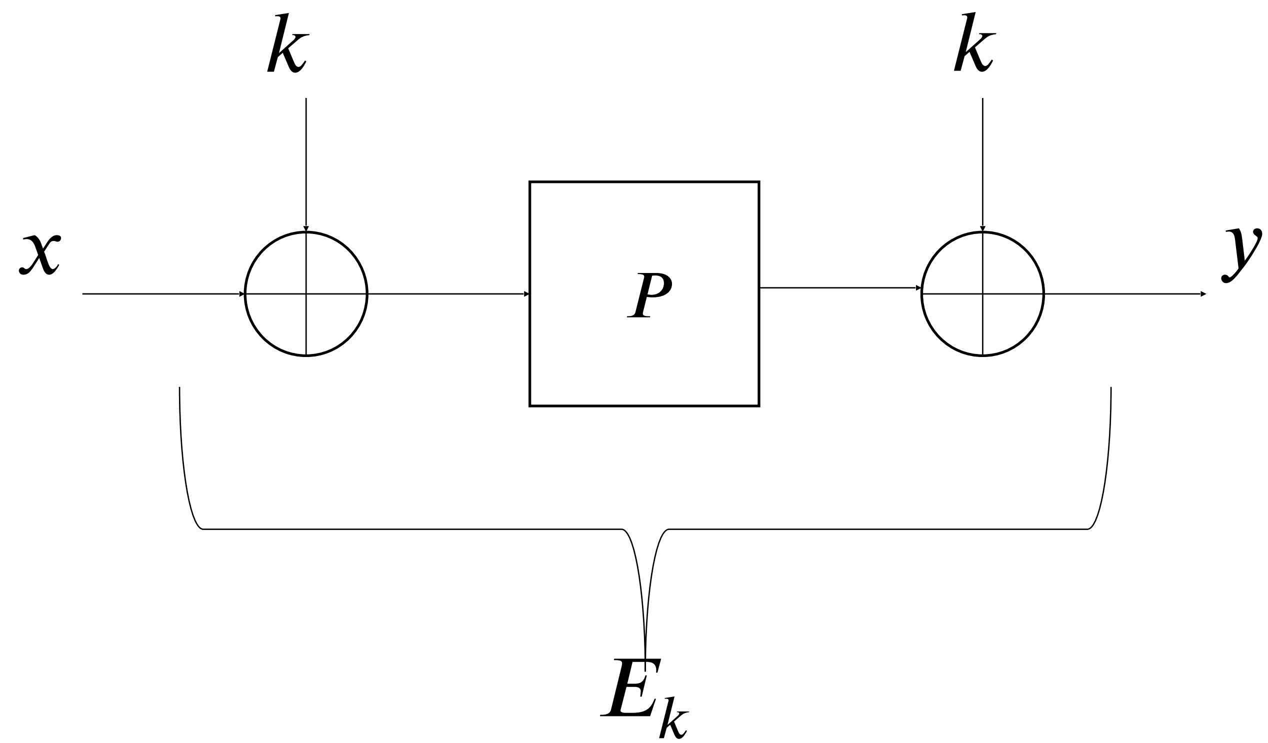


The Even-Mansour Cipher

Given a public permutation $P: \{0,1\}^n \rightarrow \{0,1\}^n$ and a key $k \in \{0,1\}^n$, the cipher $E: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ is defined as:

$$E_k[P](x) = P(x \oplus k) \oplus k$$

- Minimal Construction

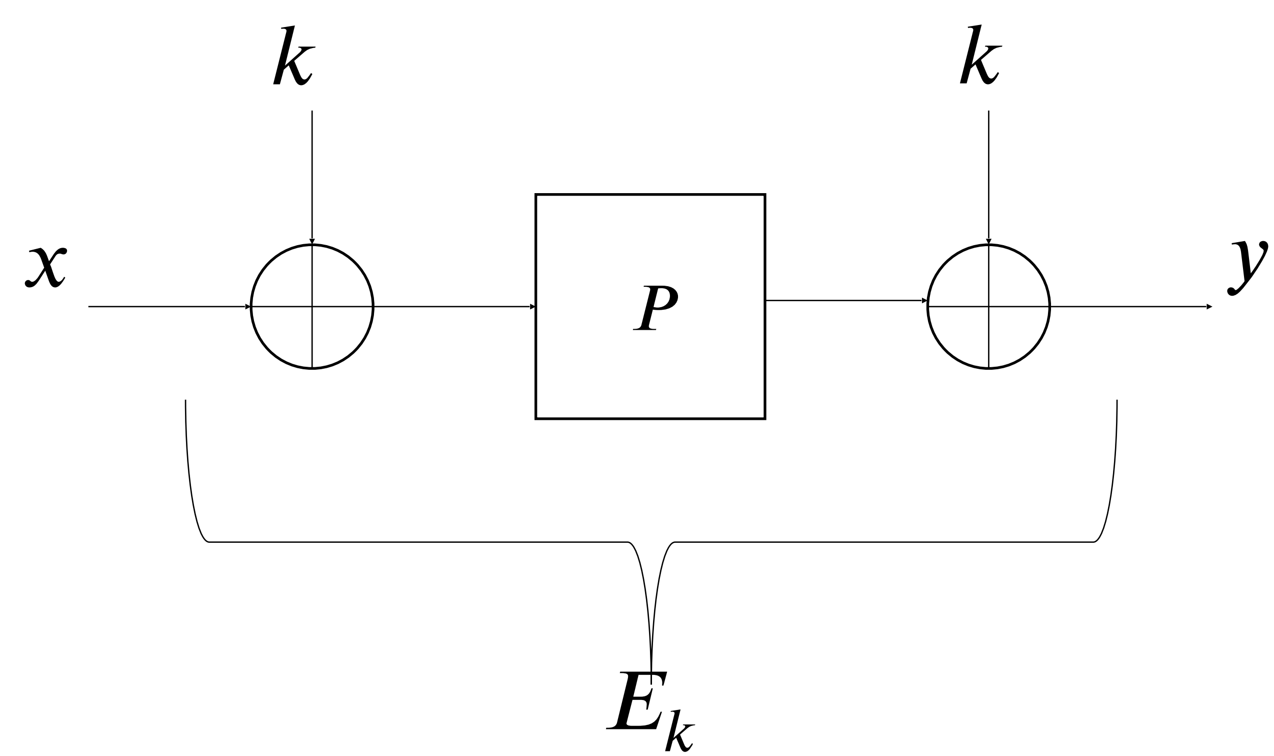


The Even-Mansour Cipher

Given a public permutation $P: \{0,1\}^n \rightarrow \{0,1\}^n$ and a key $k \in \{0,1\}^n$, the cipher $E: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ is defined as:

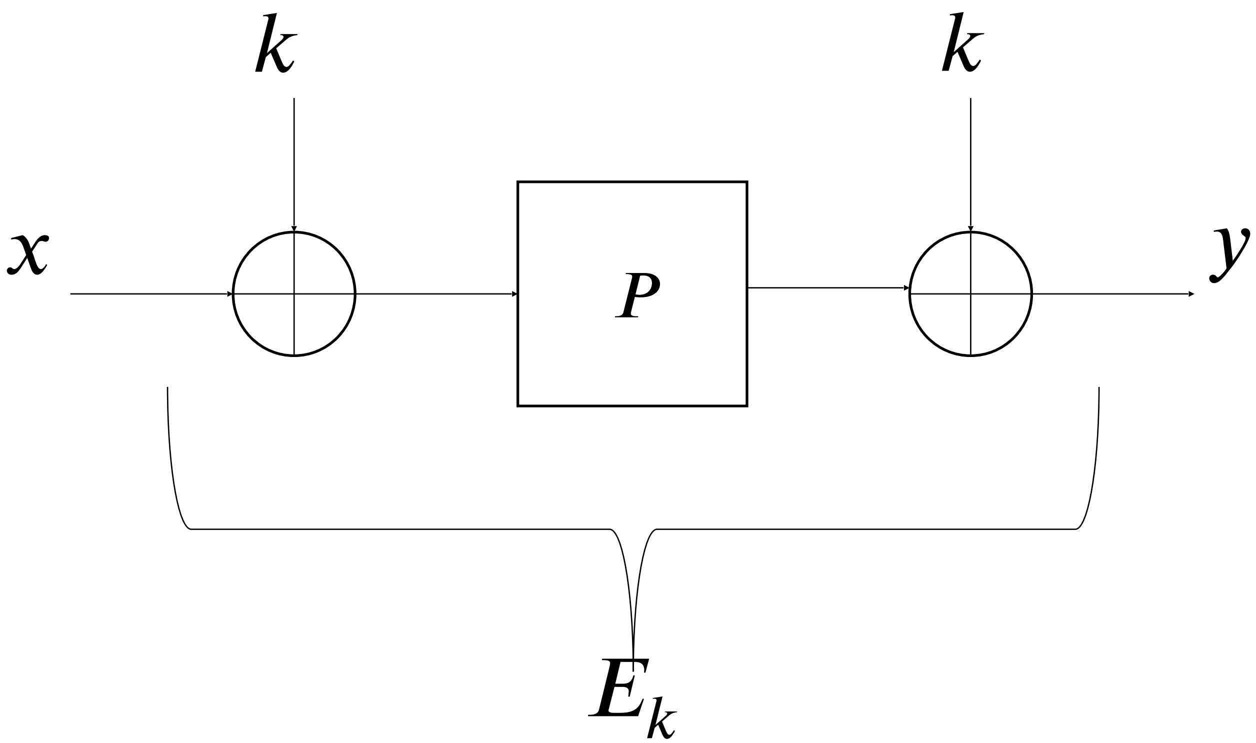
$$E_k[P](x) = P(x \oplus k) \oplus k$$

- Minimal Construction
- Key ingredient in many symmetric-key constructions, e.g. Elephant, Chaskey



Security of Even-Mansour

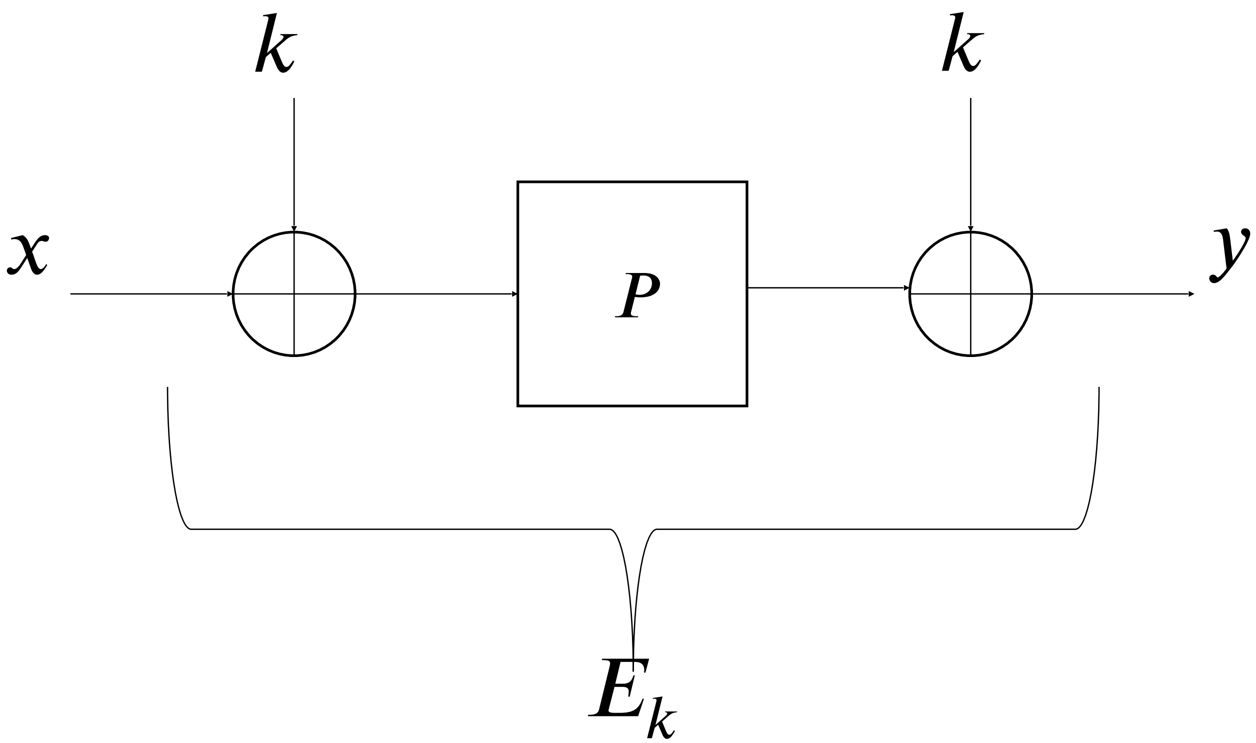
Suppose the adversary makes q_E queries to E_k and q_P queries to P:



Security of Even-Mansour

Suppose the adversary makes q_E queries to E_k and q_P queries to P:

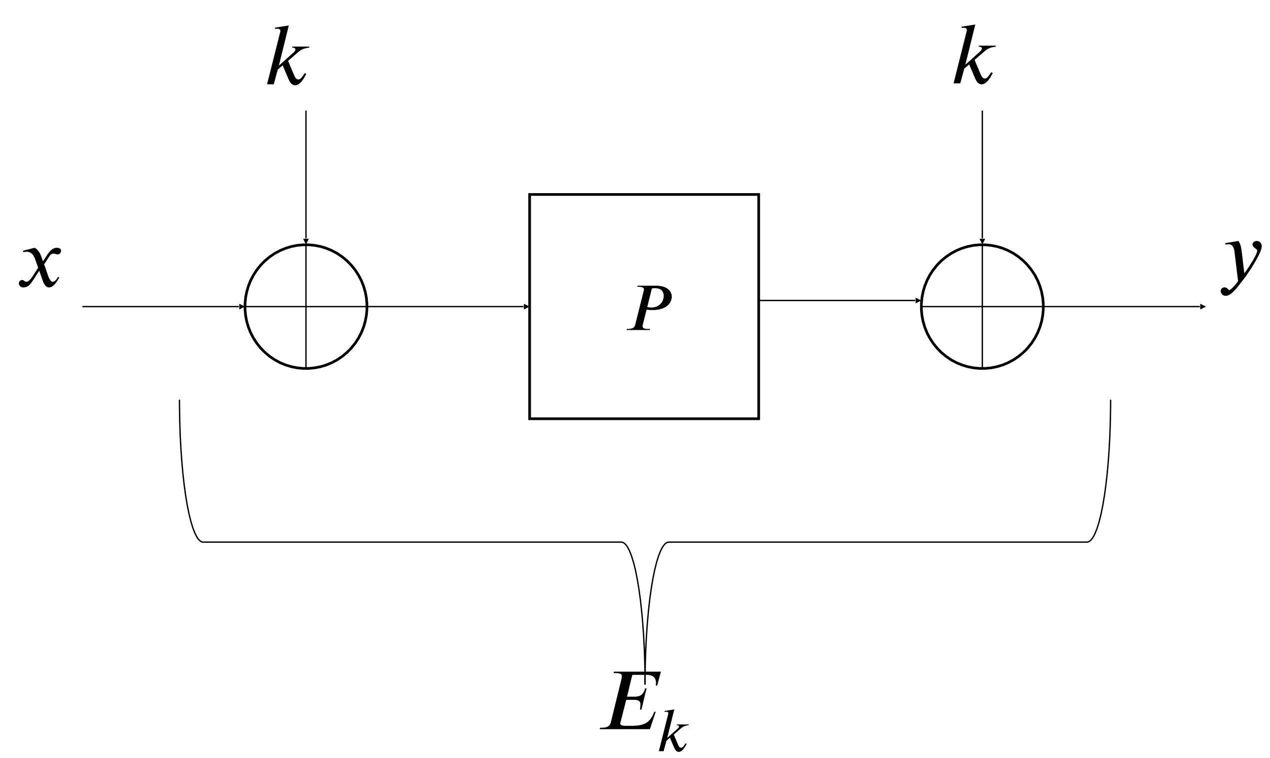
- Classical: $q_E \cdot q_P = \Omega(2^n)$. [EM97]



Security of Even-Mansour

Suppose the adversary makes q_E queries to E_k and q_P queries to P:

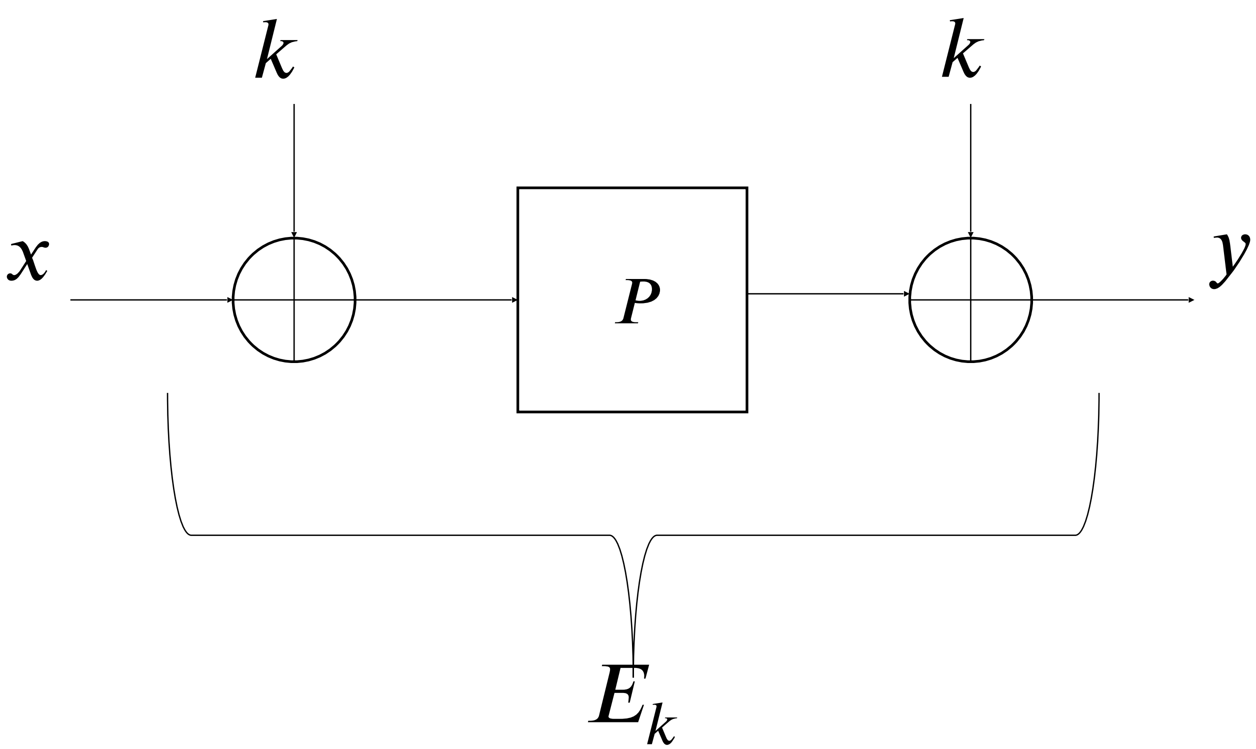
- Classical: $q_E \cdot q_P = \Omega(2^n)$. [EM97]
- Q2 (beyond post-quantum): Apply Simon's algorithm to give an attack using only $\mathcal{O}(n)$ queries. [KM12]



Security of Even-Mansour

Suppose the adversary makes q_E queries to E_k and q_P queries to P:

- Classical: $q_E \cdot q_P = \Omega(2^n)$. [EM97]
- Q2 (beyond post-quantum): Apply Simon's algorithm to give an attack using only $\mathcal{O}(n)$ queries. [KM12]
- **Q1 (post-quantum)?**



Result

Main Result

Theorem (Alagic, Bai, Katz, M):

Let P and R be a random permutations and E_k the Even-Mansour cipher using P. Any quantum adversary making at most q_P quantum queries to P and q_E classical queries to an oracle O has distinguishing advantage between $O = E_k$ and $O = R$ at most

$$10 \cdot 2^{-\frac{n}{2}} \left(q_P \sqrt{q_E} + q_E \sqrt{q_P} \right)$$

Main Result

Theorem (Alagic, Bai, Katz, M):
Let P and R be a random permutations and E_k the Even-Mansour cipher using P. Any quantum adversary making at most q_P quantum queries to P and q_E classical queries to an oracle O has distinguishing advantage between $O = E_k$ and $O = R$ at most

$$10 \cdot 2^{-\frac{n}{2}} \left(q_P \sqrt{q_E} + q_E \sqrt{q_P} \right)$$

- Shown by Jaeger, Song and Tessaro (TCC 21) for non-adaptive adversaries

Main Result

Theorem (Alagic, Bai, Katz, M):

Let P and R be a random permutations and E_k the Even-Mansour cipher using P. Any quantum adversary making at most q_P quantum queries to P and q_E classical queries to an oracle O has distinguishing advantage between $O = E_k$ and $O = R$ at most

$$10 \cdot 2^{-\frac{n}{2}} \left(q_P \sqrt{q_E} + q_E \sqrt{q_P} \right)$$

- Shown by Jaeger, Song and Tessaro (TCC 21) for non-adaptive adversaries
- Tight characterization of query complexity assuming $q_E \ll q_P$ (matching attacks: BHT/offline Simon's)

Techniques, Technical Contributions

General approach

General approach

- Classical security proofs of Even-Mansour use *global* techniques.
  Examples:

General approach

- Classical security proofs of Even-Mansour use *global* techniques. Examples:
    - Characterize the probability of bad events defined in terms of query transcripts

General approach

- Classical security proofs of Even-Mansour use *global* techniques. Examples:
  - Characterize the probability of bad events defined in terms of query transcripts
  - H-coefficient technique

General approach

- Classical security proofs of Even-Mansour use *global* techniques. Examples:
  - Characterize the probability of bad events defined in terms of query transcripts
  - H-coefficient technique
- Quantum queries $\Rightarrow$ no transcript!

General approach

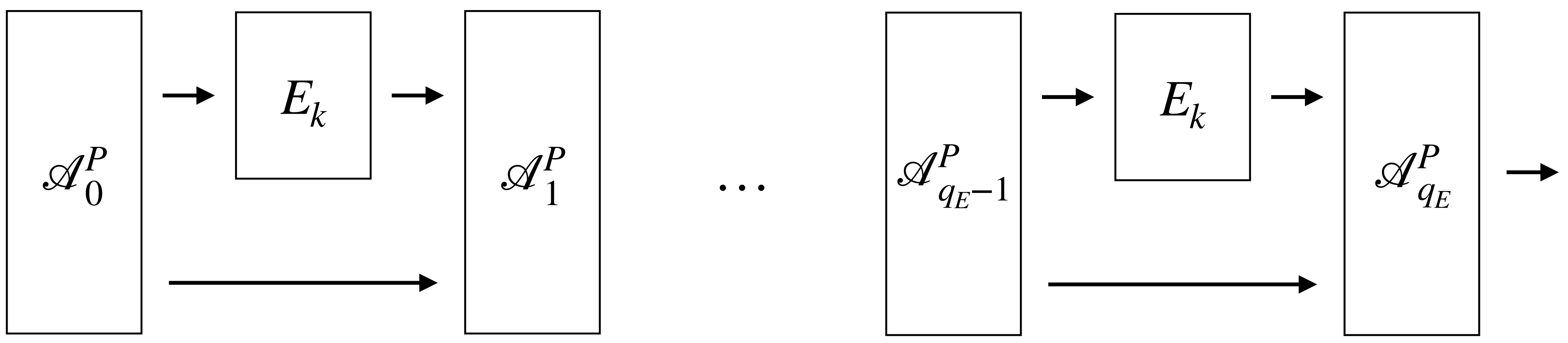
- Classical security proofs of Even-Mansour use *global* techniques. Examples:
  - Characterize the probability of bad events defined in terms of query transcripts
  - H-coefficient technique
- Quantum queries $\Rightarrow$ no transcript!
- Resort to “more primitive” technique: hybrid argument

The hybrid argument

- Think of adversary having $q_E + 1$ stages:

The hybrid argument

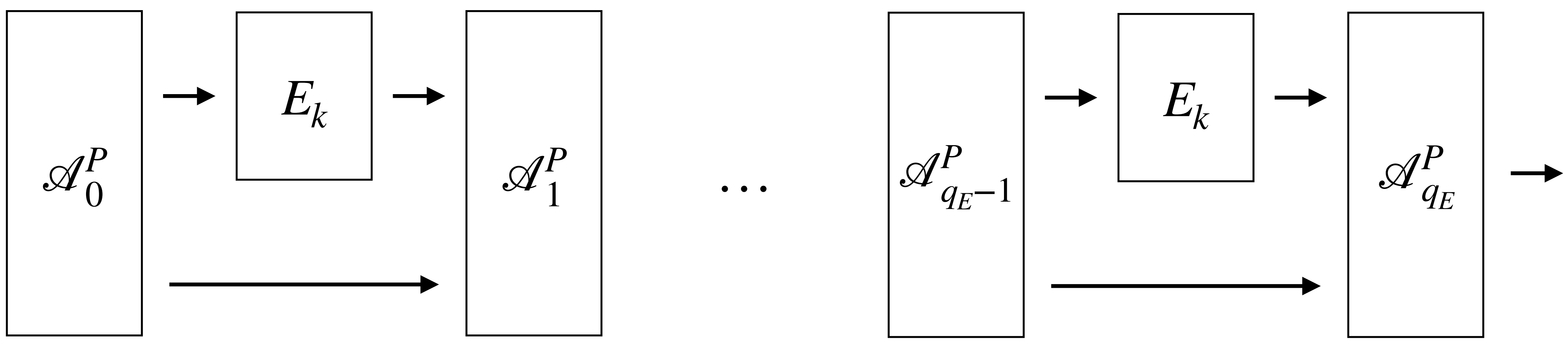
- Think of adversary having $q_E + 1$ stages:



- Each $\mathscr{A}_i^P$ makes arbitrary number of quantum queries to P, sum $\leq q_P$

The hybrid argument

- Think of adversary having $q_E + 1$ stages:



- Each $\mathscr{A}_i^P$ makes arbitrary number of quantum queries to P, sum $\leq q_P$
- Naive hybrids: replace E_k with R for first i calls

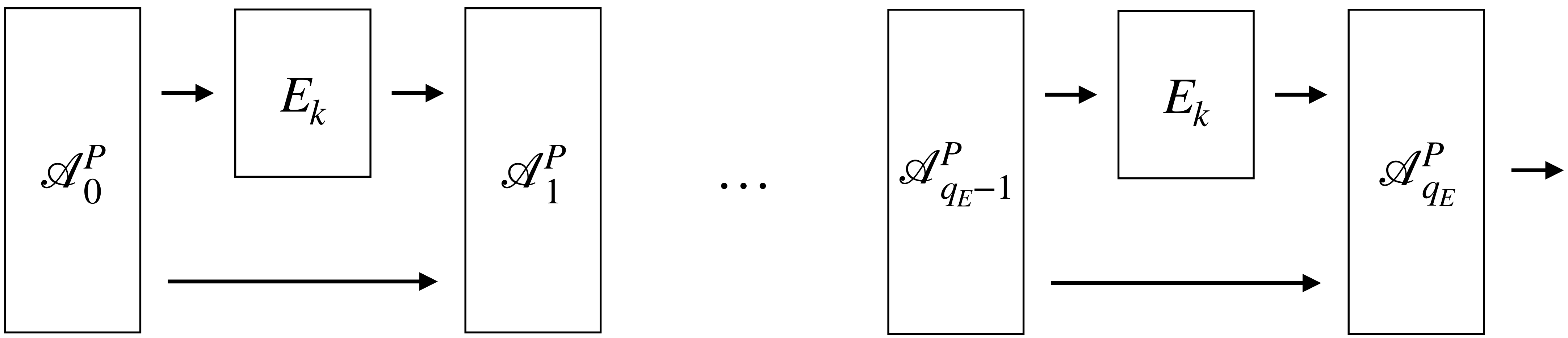
The hybrid argument

- Think of adversary having $q_E + 1$ stages:

- Each $\mathscr{A}_i^P$ makes arbitrary number of quantum queries to P, sum $\leq q_P$
- Naive hybrids: replace E_k with R for first i calls
- Consistency of the oracles?

The hybrid argument

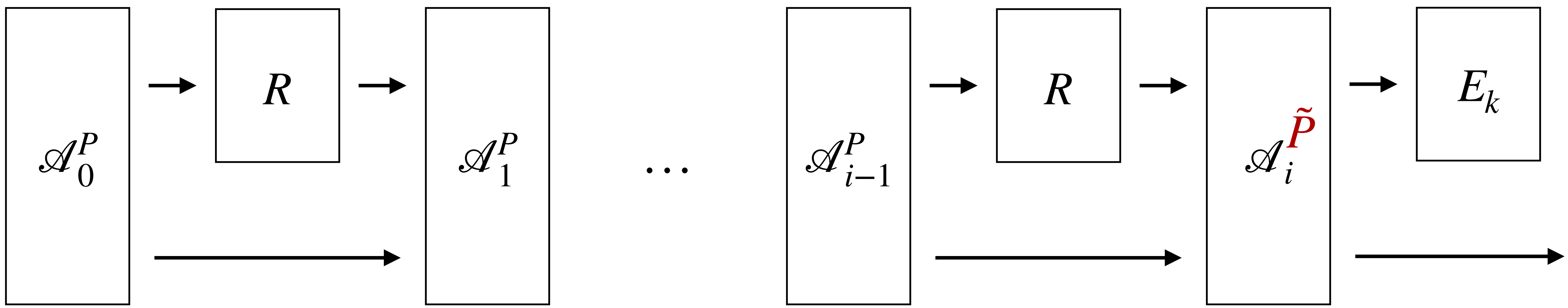
- Think of adversary having $q_E + 1$ stages:

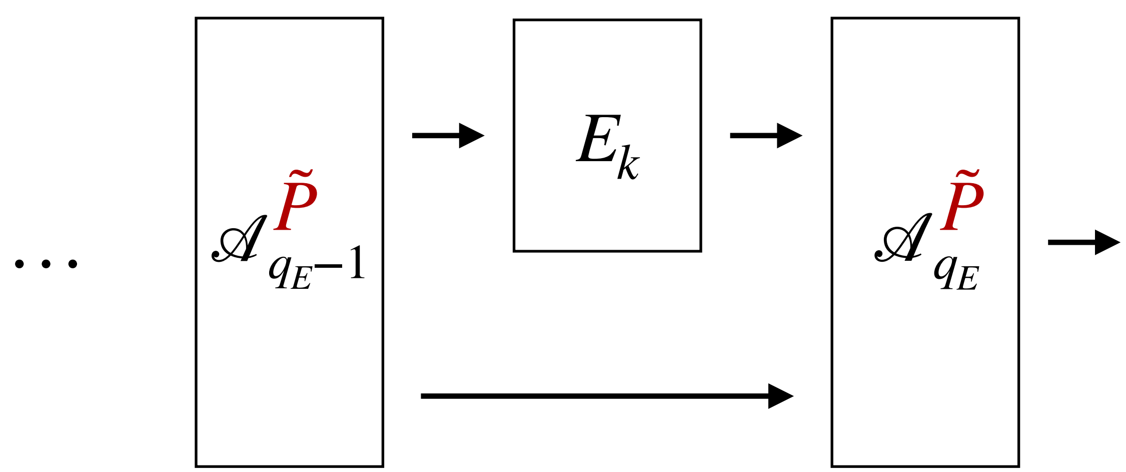


- Each $\mathscr{A}_i^P$ makes arbitrary number of quantum queries to P, sum $\leq q_P$
- Naive hybrids: replace E_k with R for first i calls
- Consistency of the oracles? Postpone problem until it goes away

The hybrids

H_i:

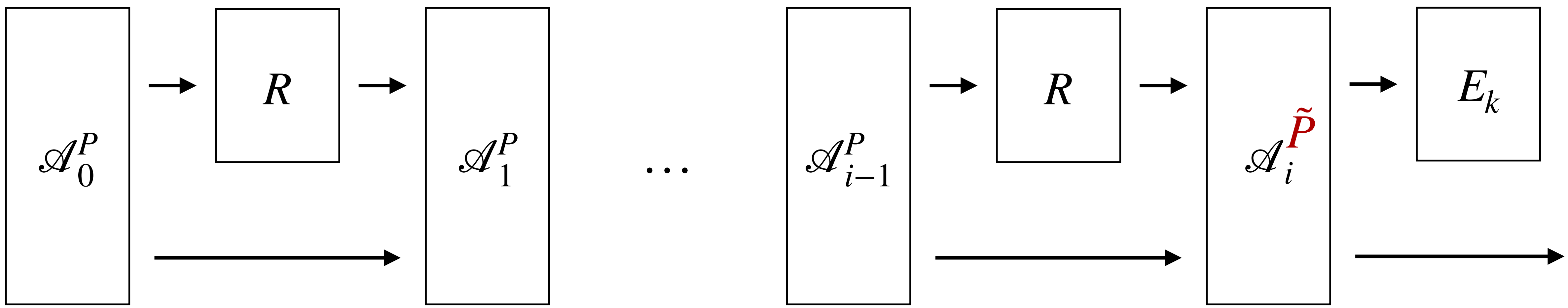


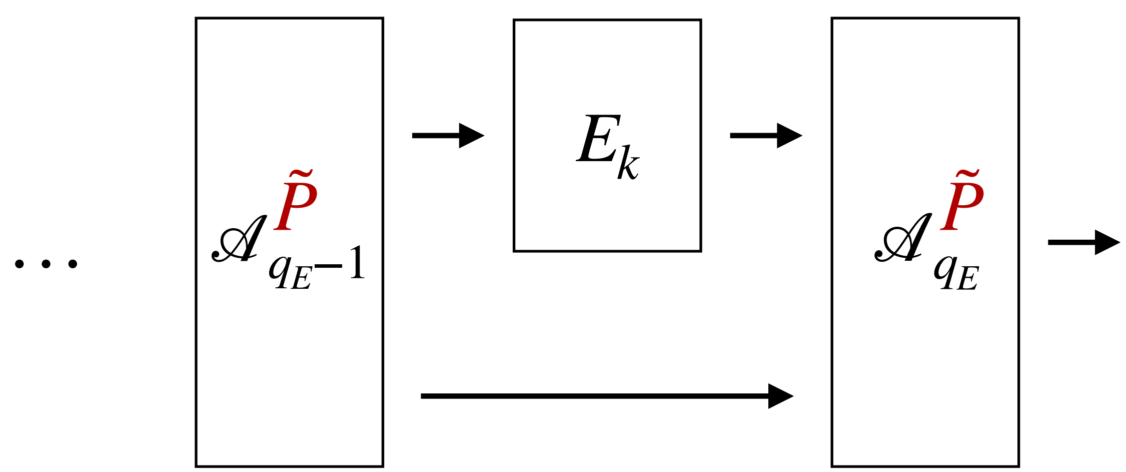


$\tilde{P}$: P with necessary modifications to ensure consistency of E_k and R

The hybrids

H_i:

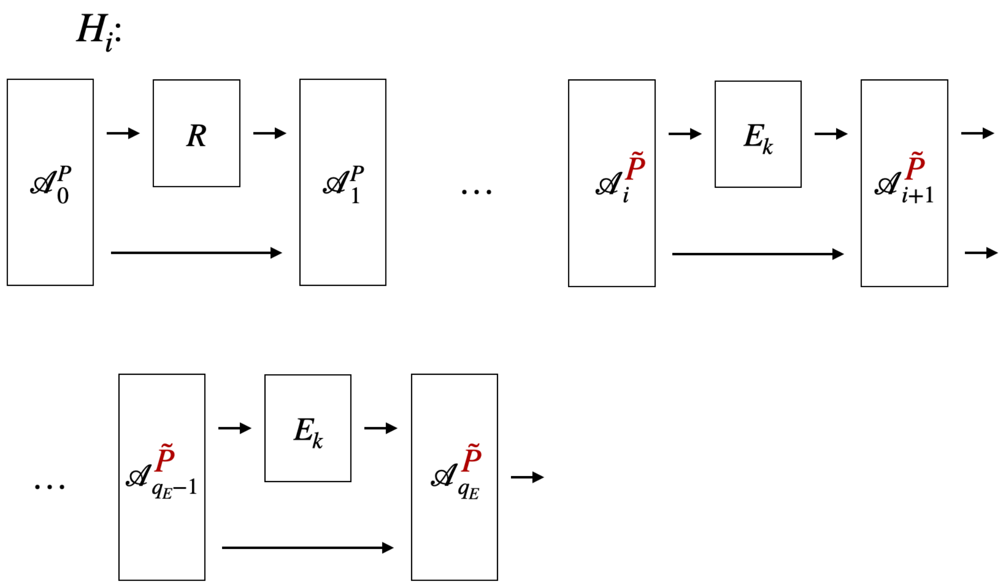




$\tilde{P}$: P with necessary modifications to ensure consistency of E_k and R

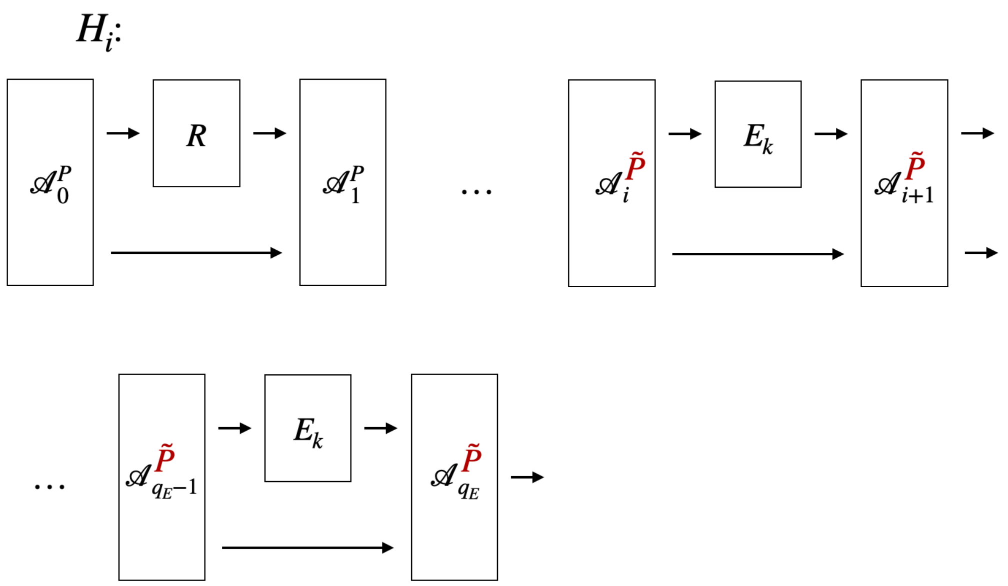
So $\tilde{P}$ gets messed up more and more as i grows… but in the end it's gone!

Technical Lemmas



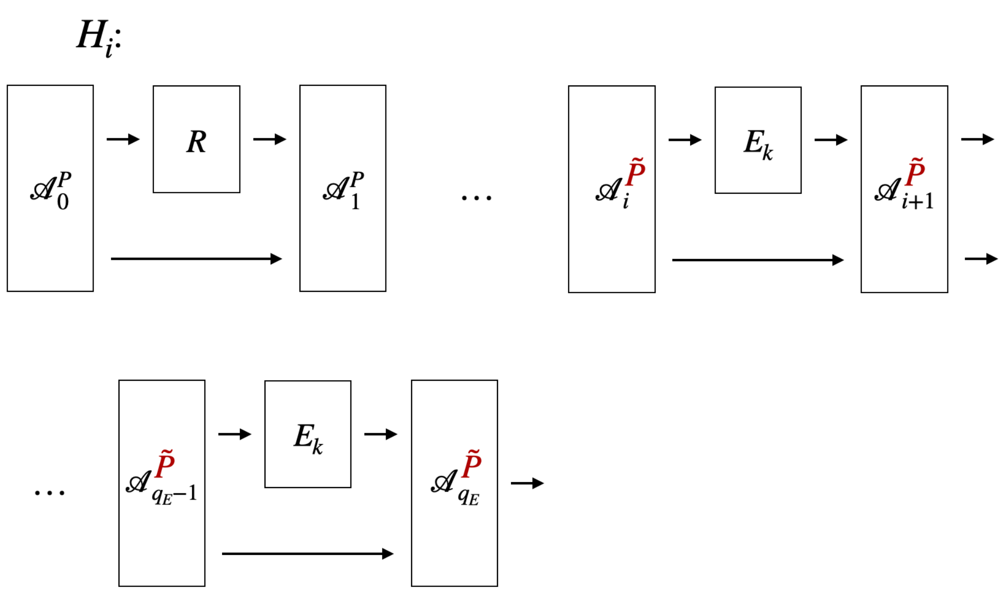
- Two steps in hybrid transition:

Technical Lemmas



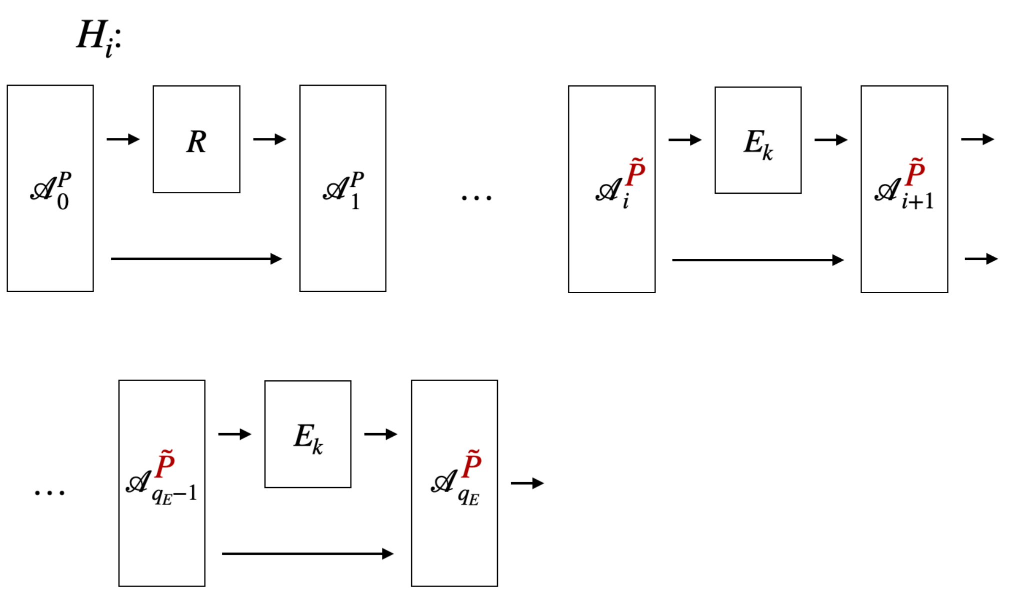
- Two steps in hybrid transition:
    1. Replace E_k with R and "repair" $\tilde{P}$

Technical Lemmas



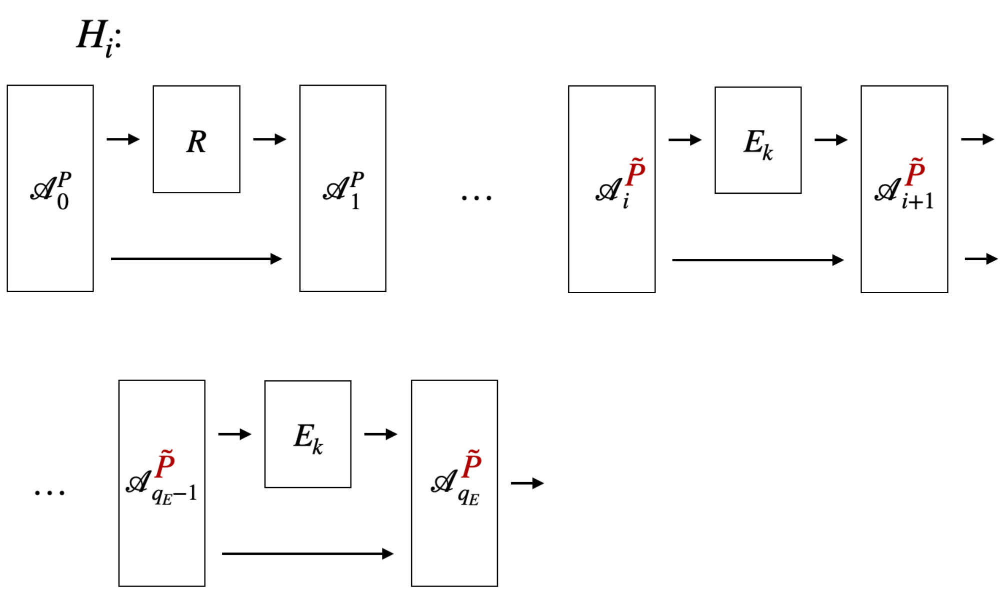
- Two steps in hybrid transition:
  1. Replace E_k with R and "repair" $\tilde{P}$
  2. Replace the first $\tilde{P}$ with P

Technical Lemmas



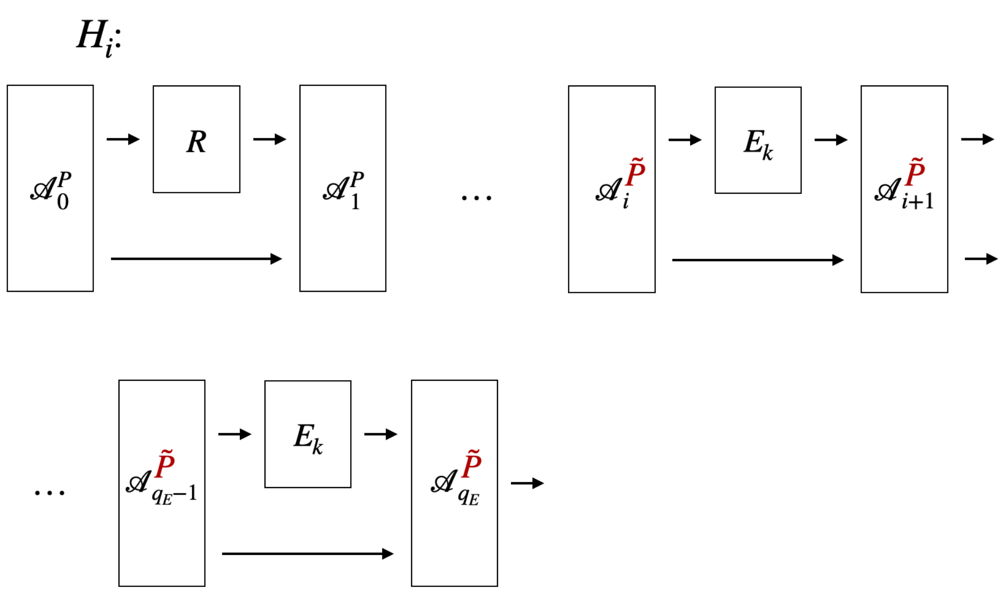
- Two steps in hybrid transition:
  1. Replace E_k with R and “repair” $\tilde{P}$
  2. Replace the first $\tilde{P}$ with P
- $\Rightarrow$ 2 Technical lemmas:

Technical Lemmas



- Two steps in hybrid transition:
  1. Replace E_k with R and "repair" $\tilde{P}$
  2. Replace the first $\tilde{P}$ with P
- $\Rightarrow$ 2 Technical lemmas:
  1. A resampling lemma for random permutations

Technical Lemmas



- Two steps in hybrid transition:
  1. Replace E_k with R and "repair" $\tilde{P}$
  2. Replace the first $\tilde{P}$ with P
- $\Rightarrow$ 2 Technical lemmas:
  1. A resampling lemma for random permutations
  2. A reprogramming lemma in terms of expected number of queries

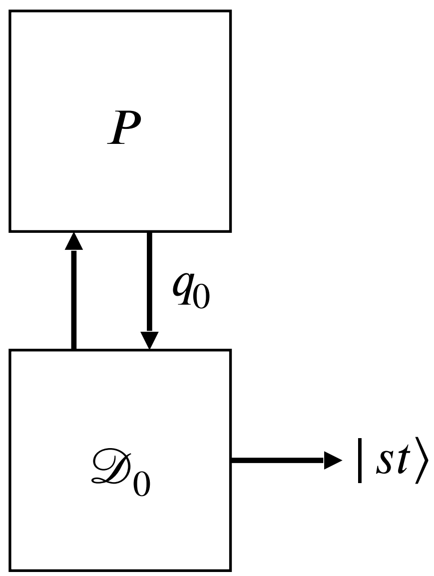
Resampling Lemma

Permutation version of “adaptive reprogramming lemma” (Grilo, Hövelmanns, Hülsing and Majenz, AC ’21)

Resampling Lemma

Permutation version of “adaptive reprogramming lemma” (Grilo, Hövelmanns, Hülsing and Majenz, AC ’21)

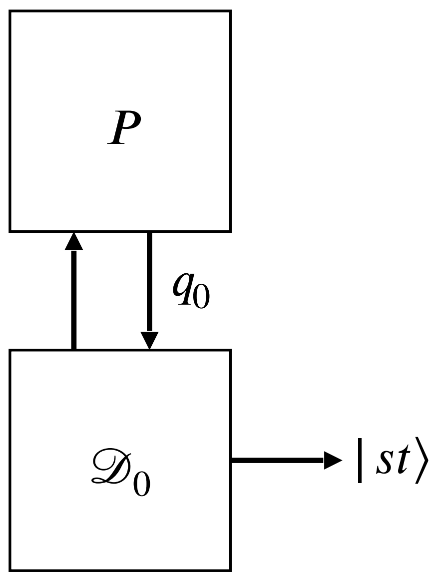
Phase 1:



Resampling Lemma

Permutation version of "adaptive reprogramming lemma" (Grilo, Hövelmanns, Hülsing and Majenz, AC '21)

Phase 1:

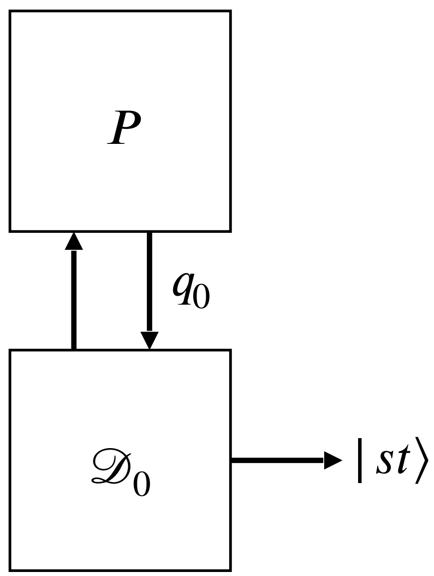


$$b \xleftarrow{\$} \{0,1\}$$
$$s_0 \xleftarrow{\$} \{0,1\}^n$$
$$s_1 \xleftarrow{\$} \{0,1\}^n$$

Resampling Lemma

Permutation version of "adaptive reprogramming lemma" (Grilo, Hövelmanns, Hülsing and Majenz, AC '21)

Phase 1:

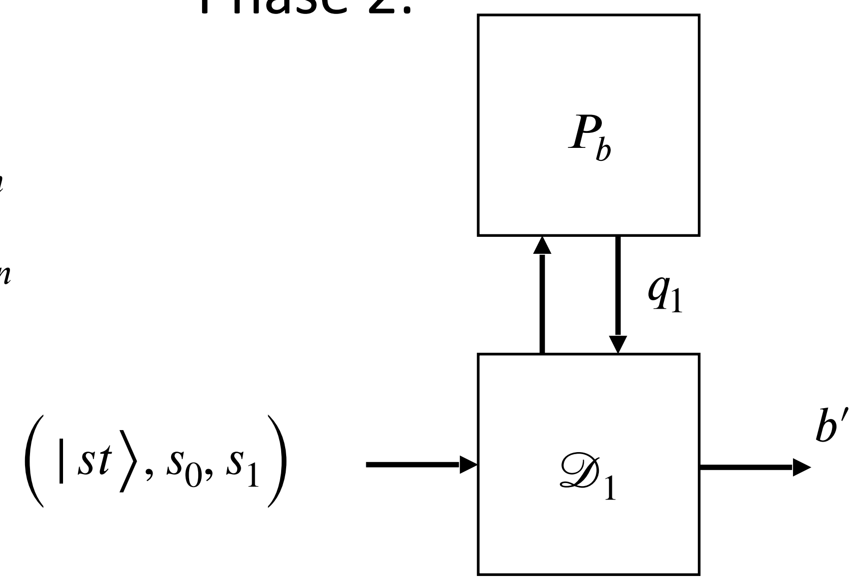


$b \xleftarrow{\$} \{0,1\}$

$s_0 \xleftarrow{\$} \{0,1\}^n$

$s_1 \xleftarrow{\$} \{0,1\}^n$

Phase 2:

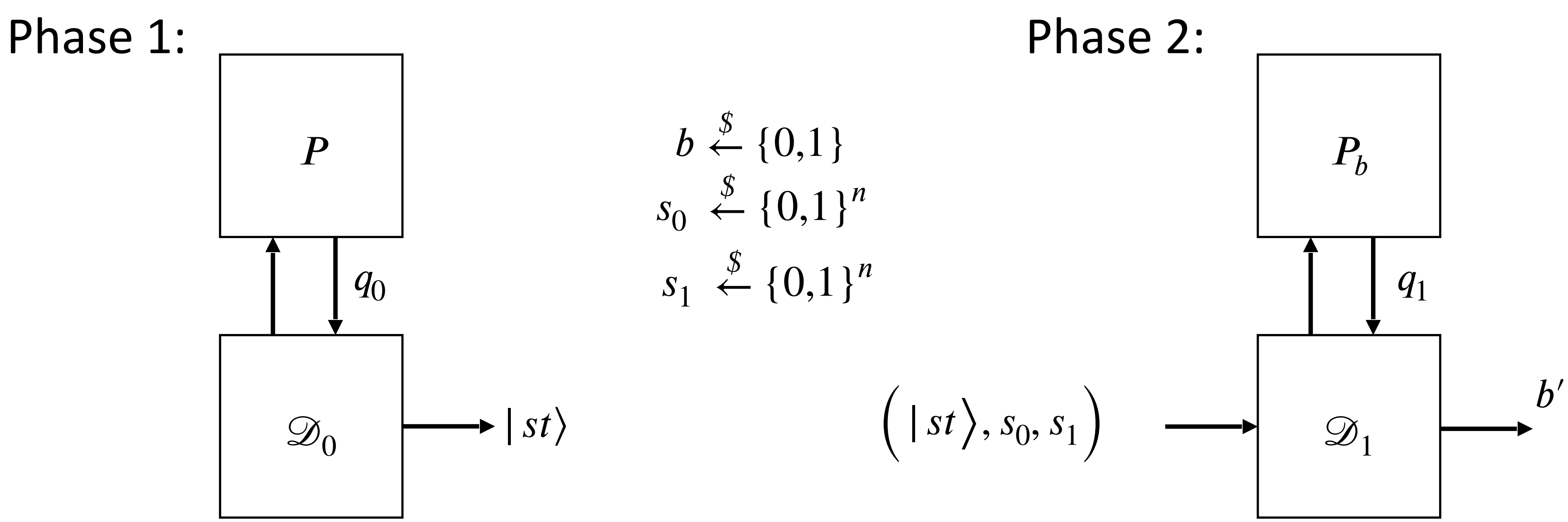


$P_0 = P$

$$P_1 = P \circ swap_{s_0,s_1} = \begin{cases} P(s_0) & if\ x = s_1 \\ P(s_1) & if\ x = s_0 \\ P(x) & otherwise \end{cases}$$

Resampling Lemma

Permutation version of "adaptive reprogramming lemma" (Grilo, Hövelmanns, Hülsing and Majenz, AC '21)



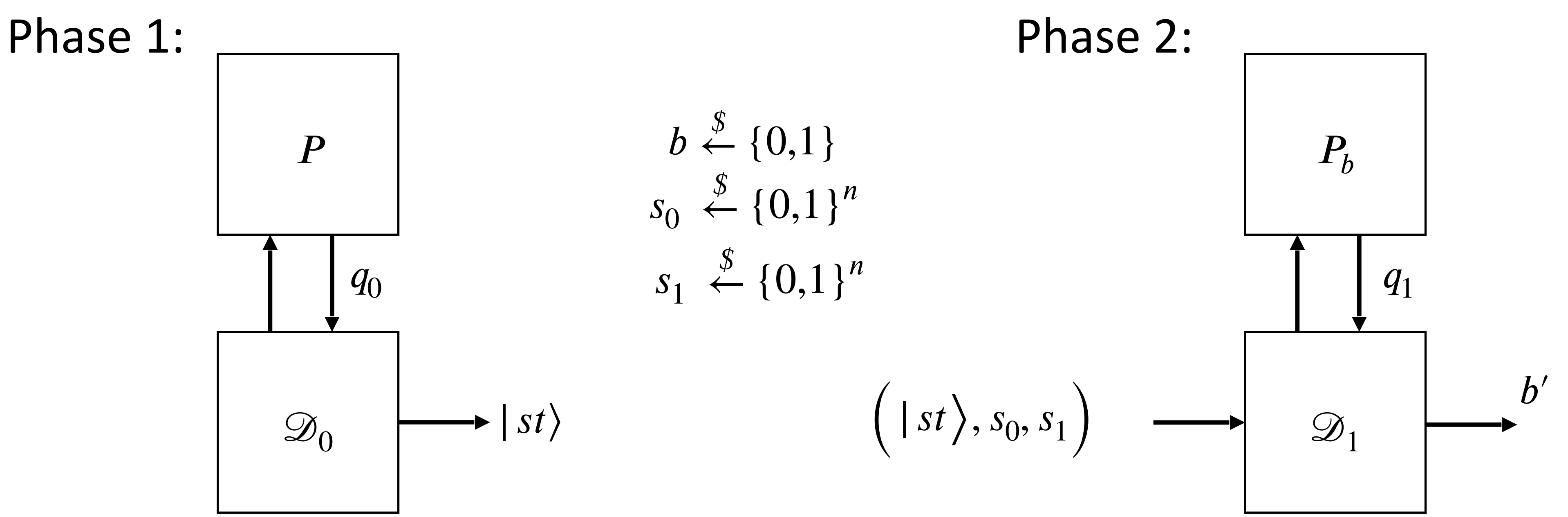
$\mathscr{D}$ wins if $b = b'$

$P_0 = P$

$$P_1 = P \circ swap_{s_0,s_1} = \begin{cases} P(s_0) & if\ x = s_1 \\ P(s_1) & if\ x = s_0 \\ P(x) & otherwise \end{cases}$$

Resampling Lemma

Permutation version of "adaptive reprogramming lemma" (Grilo, Hövelmanns, Hülsing and Majenz, AC '21)



$\mathscr{D}$ wins if $b = b'$

$P_0 = P$

$$P_1 = P \circ swap_{s_0,s_1} = \begin{cases} P(s_0) & if\ x = s_1 \\ P(s_1) & if\ x = s_0 \\ P(x) & otherwise \end{cases}$$

Lemma: Advantage $\leq O\left(\sqrt{q \cdot 2^{-n}}\right)$

Reprogramming Lemma

Expected # of queries version of “blinding lemma” (Alagic, Majenz, Russell, Song, EC ’20)

Reprogramming Lemma

Expected # of queries version of “blinding lemma” (Alagic, Majenz, Russell, Song, EC ’20)

Reprogramming game:

Reprogramming Lemma

Expected # of queries version of “blinding lemma” (Alagic, Majenz, Russell, Song, EC ’20)

Reprogramming game:

1. Distinguisher $\mathscr{D}$ supplies function F and specifies randomized reprogramming routine

Reprogramming Lemma

Expected # of queries version of “blinding lemma” (Alagic, Majenz, Russell, Song, EC ’20)

Reprogramming game:

1. Distinguisher $\mathscr{D}$ supplies function F and specifies randomized reprogramming routine
2. For random bit b, $\mathscr{D}$ receives oracle F_b ($F_0 = F$ and F_1 is reprogrammed)

Reprogramming Lemma

Expected # of queries version of "blinding lemma" (Alagic, Majenz, Russell, Song, EC '20)

Reprogramming game:

1. Distinguisher $\mathscr{D}$ supplies function F and specifies randomized reprogramming routine
2. For random bit b, $\mathscr{D}$ receives oracle F_b ($F_0 = F$ and F_1 is reprogrammed)
3. $\mathscr{D}$ loses access to F_b, receives description of F_1, outputs b'

Reprogramming Lemma

Expected # of queries version of "blinding lemma" (Alagic, Majenz, Russell, Song, EC '20)

Reprogramming game:

1. Distinguisher $\mathscr{D}$ supplies function F and specifies randomized reprogramming routine
2. For random bit b, $\mathscr{D}$ receives oracle F_b ($F_0 = F$ and F_1 is reprogrammed)
3. $\mathscr{D}$ loses access to F_b, receives description of F_1, outputs b'

$\mathscr{D}$ wins if $b = b'$

Reprogramming Lemma

Expected # of queries version of "blinding lemma" (Alagic, Majenz, Russell, Song, EC '20)

Reprogramming game:

1. Distinguisher $\mathscr{D}$ supplies function F and specifies randomized reprogramming routine
2. For random bit b, $\mathscr{D}$ receives oracle F_b ($F_0 = F$ and F_1 is reprogrammed)
3. $\mathscr{D}$ loses access to F_b, receives description of F_1, outputs b'

$\mathscr{D}$ wins if $b = b'$

Lemma: Advantage $\leq O\left(q\sqrt{2^{-n}}\right)$

Summary

- We proved post-quantum security of the Even-Mansour cipher
- Applications? Elephant and Chaskey use generlized versions of Even-Mansour. Also Jaeger et al. can actually do FX! $\Rightarrow$ Follow-up work (us+Patrick Struck), on eprint "soon" :)

Summary

- We proved post-quantum security of the Even-Mansour cipher
- Applications? Elephant and Chaskey use generlized versions of Even-Mansour. Also Jaeger et al. can actually do FX! ⇒ Follow-up work (us+Patrick Struck), on eprint "soon" :)

Coming soon: PhD position in provable post-quantum security @DTU (Copenhagen area)

Thank you for your attention!