Nostradamus Goes Quantum

TECHNISCHE UNIVERSITÄT DARMSTADT

Barbara Jiabao Benedikt (✉), Marc Fischlin, and Moritz Huppert

Cryptoplexity, Technische Universität Darmstadt, Germany
{barbara_jiabao.benedikt, marc.fischlin}@tu-darmstadt.de
moritz.huppert@proton.me

ATHENE
National Research Center for Applied Cybersecurity

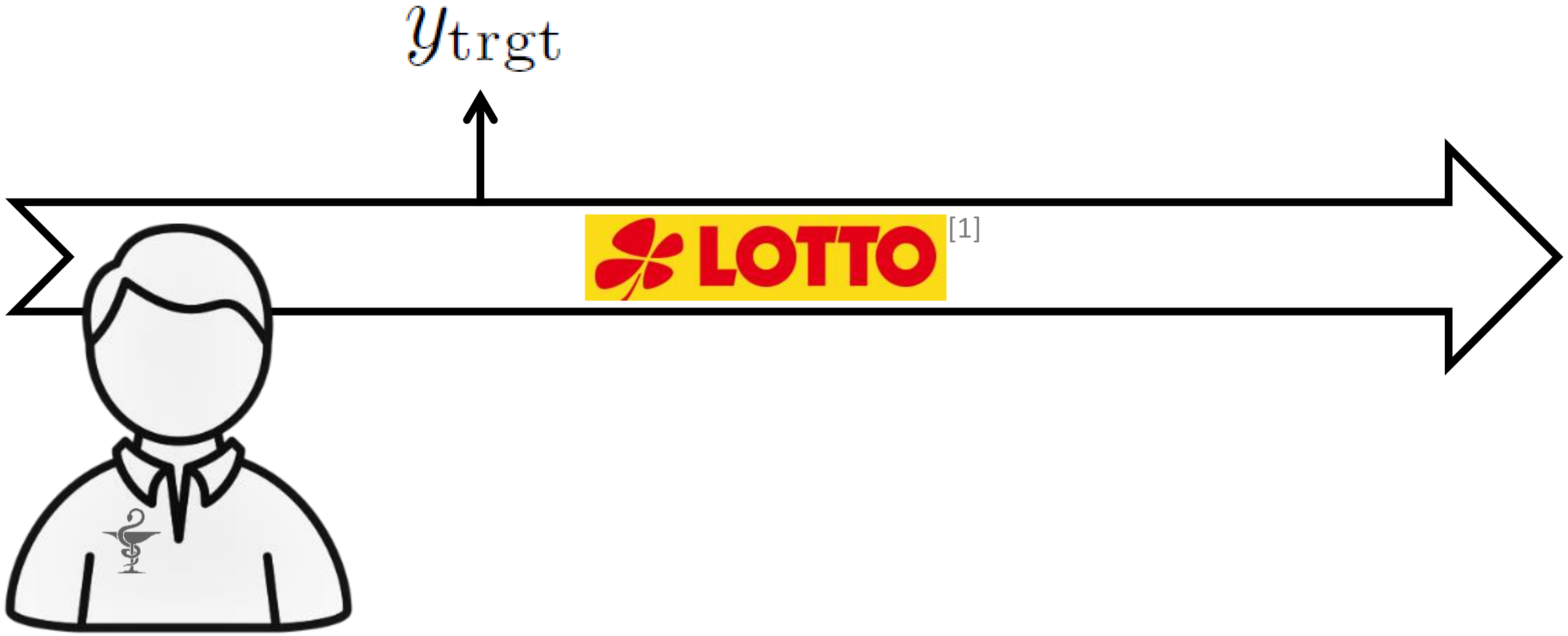
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

The Modern Nostradamus [KK06]

[KK06] Kelsey and Kohno. Herding Hash Functions and the Nostradamus Attack. Advances in Cryptology - EUROCRYPT 2006.

[1] www.lotto.de

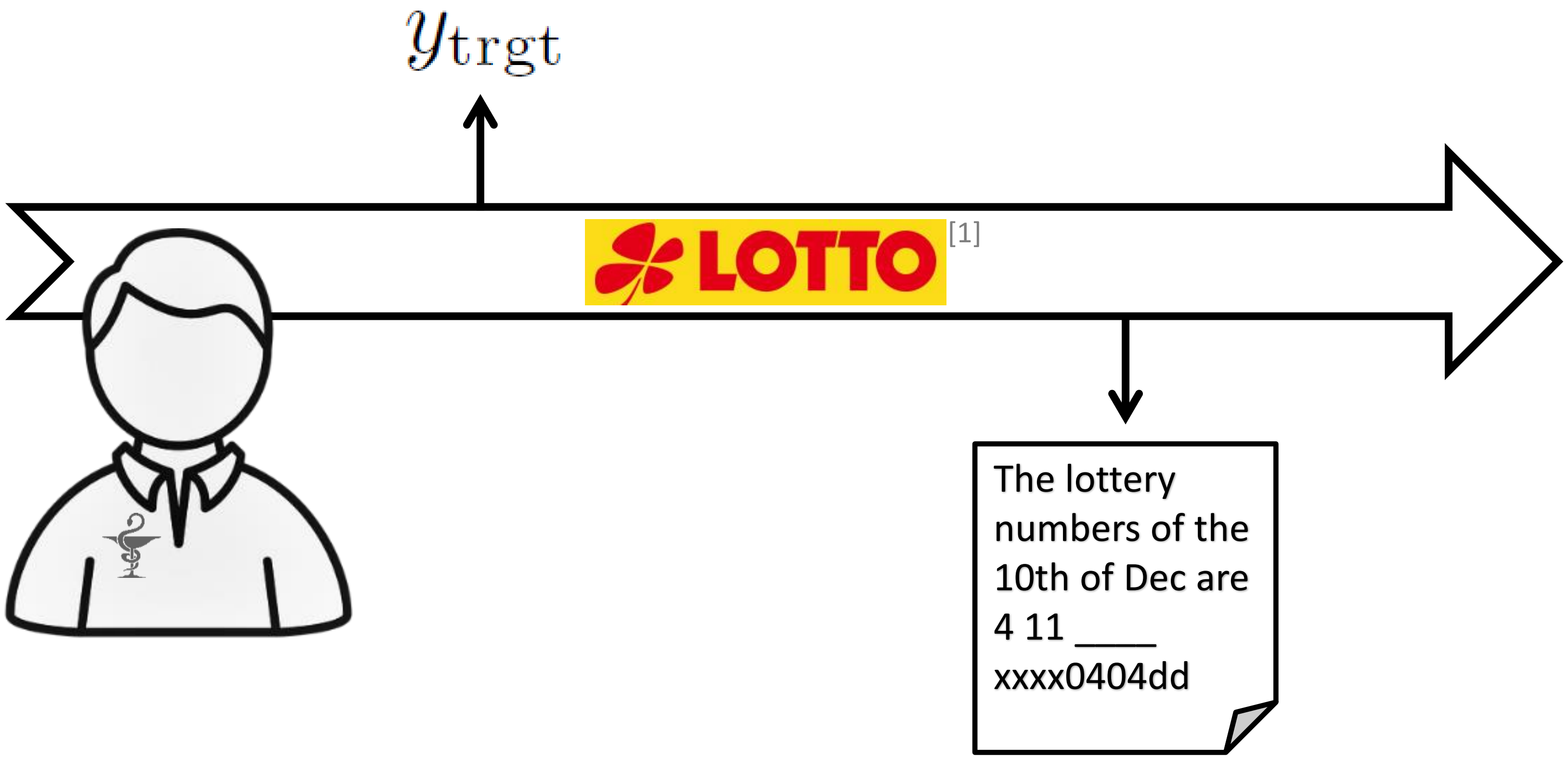
The Modern Nostradamus [KK06]



[KK06] Kelsey and Kohno. Herding Hash Functions and the Nostradamus Attack. Advances in Cryptology - EUROCRYPT 2006.

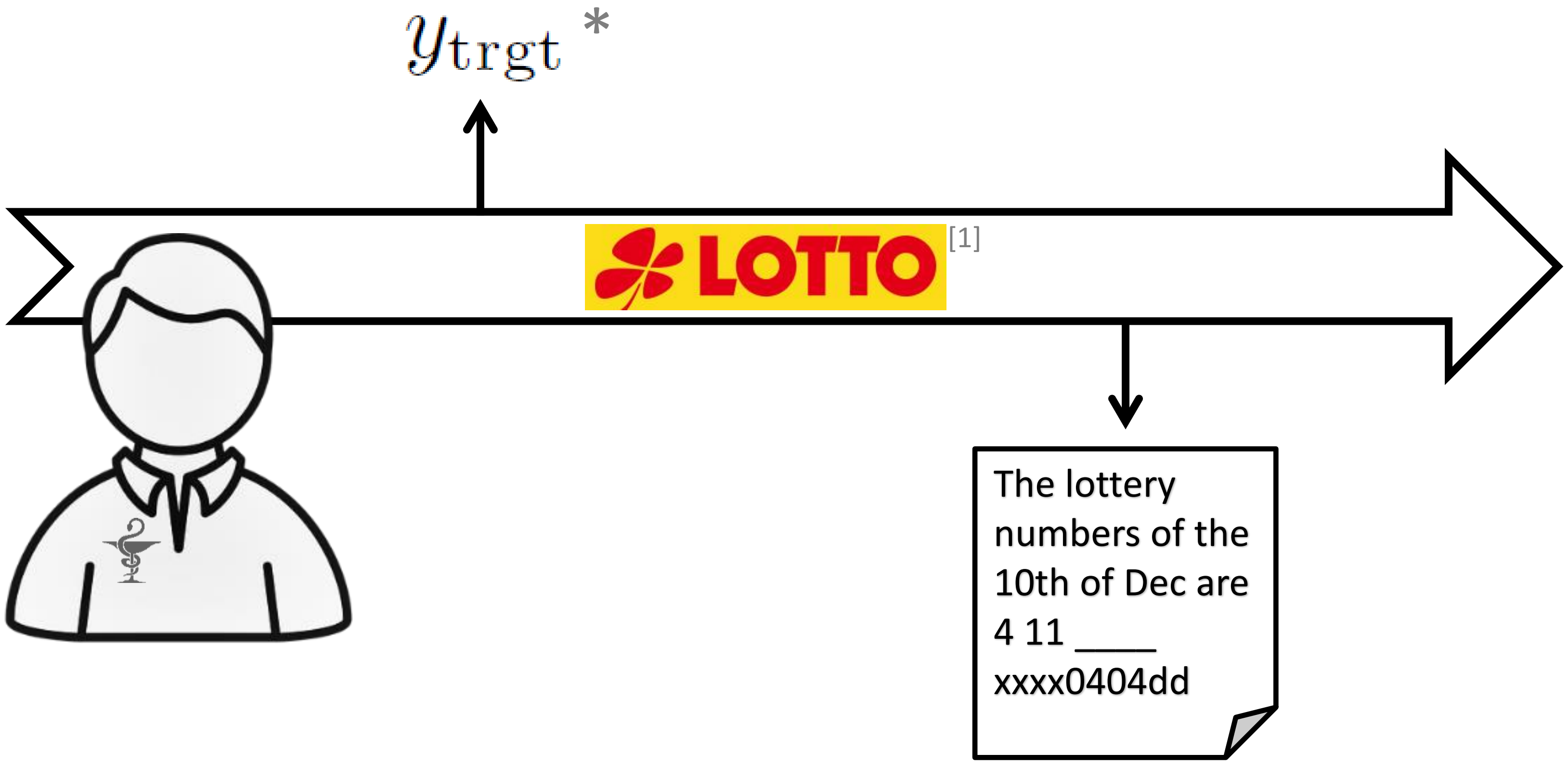
[1] www.lotto.de

The Modern Nostradamus [KK06]



[KK06] Kelsey and Kohno. Herding Hash Functions and the Nostradamus Attack. Advances in Cryptology - EUROCRYPT 2006.

The Modern Nostradamus [KK06]



* hash value of an iterated hash function

[KK06] Kelsey and Kohno. Herding Hash Functions and the Nostradamus Attack. Advances in Cryptology - EUROCRYPT 2006.

History of Nostradamus-Attacker

Legendary Nostradamus

↓

requires magic

Classical Nostradamus [KK06, BSU12]

↓

$$\mathcal{O}\left(\sqrt{n} \cdot 2^{\frac{2n}{3}}\right)$$

[BSU12] Blackburn, Stinson and Upadhyay. On the complexity of the herding attack and some related attacks on hash functions. Designs, Codes and Cryptography, 2012.

[KK06] Kelsey and Kohno. Herding Hash Functions and the Nostradamus Attack. Advances in Cryptology - EUROCRYPT 2006.

History of Nostradamus-Attacker

Legendary Nostradamus

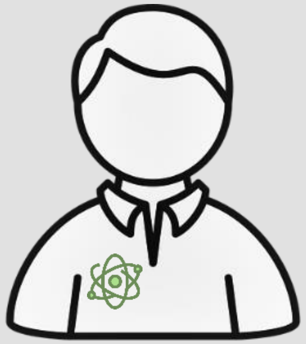
↓

requires magic

Classical Nostradamus [KK06, BSU12]

↓

$$\mathcal{O}\left(\sqrt{n}\cdot 2^{\frac{2n}{3}}\right)$$



Quantum Nostradamus [our work]

↓

$$\mathcal{O}\left(\sqrt[3]{n}\cdot 2^{\frac{3n}{7}}\right)$$

[BSU12] Blackburn, Stinson and Upadhyay. On the complexity of the herding attack and some related attacks on hash functions. Designs, Codes and Cryptography, 2012.

[KK06] Kelsey and Kohno. Herding Hash Functions and the Nostradamus Attack. Advances in Cryptology - EUROCRYPT 2006.

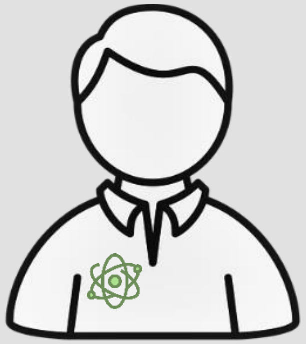
History of Nostradamus-Attacker

Legendary Nostradamus

requires magic

Classical Nostradamus [KK06, BSU12]

$$\mathcal{O}\left(\sqrt{n} \cdot 2^{\frac{2n}{3}}\right)$$



Quantum Nostradamus [our work]

$$\underline{\mathcal{O}\left(\sqrt[3]{n} \cdot 2^{\frac{3n}{7}}\right)}$$

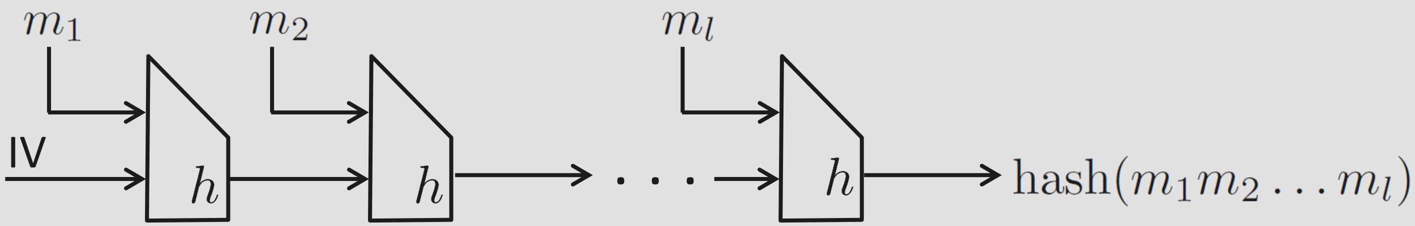
Essentially optimal!

[BSU12] Blackburn, Stinson and Upadhyay. On the complexity of the herding attack and some related attacks on hash functions. Designs, Codes and Cryptography, 2012.

[KK06] Kelsey and Kohno. Herding Hash Functions and the Nostradamus Attack. Advances in Cryptology - EUROCRYPT 2006.

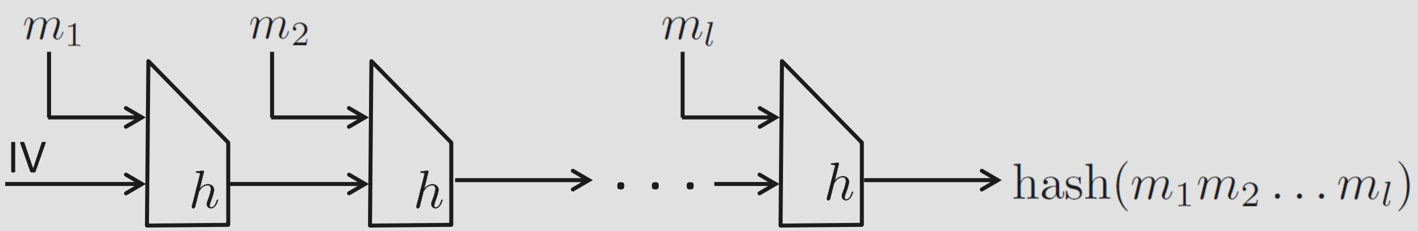
Preliminaries

$\text{hash} : \{0,1\}^* \rightarrow \{0,1\}^n$ **<u>iterated</u>** hash function, e.g.,



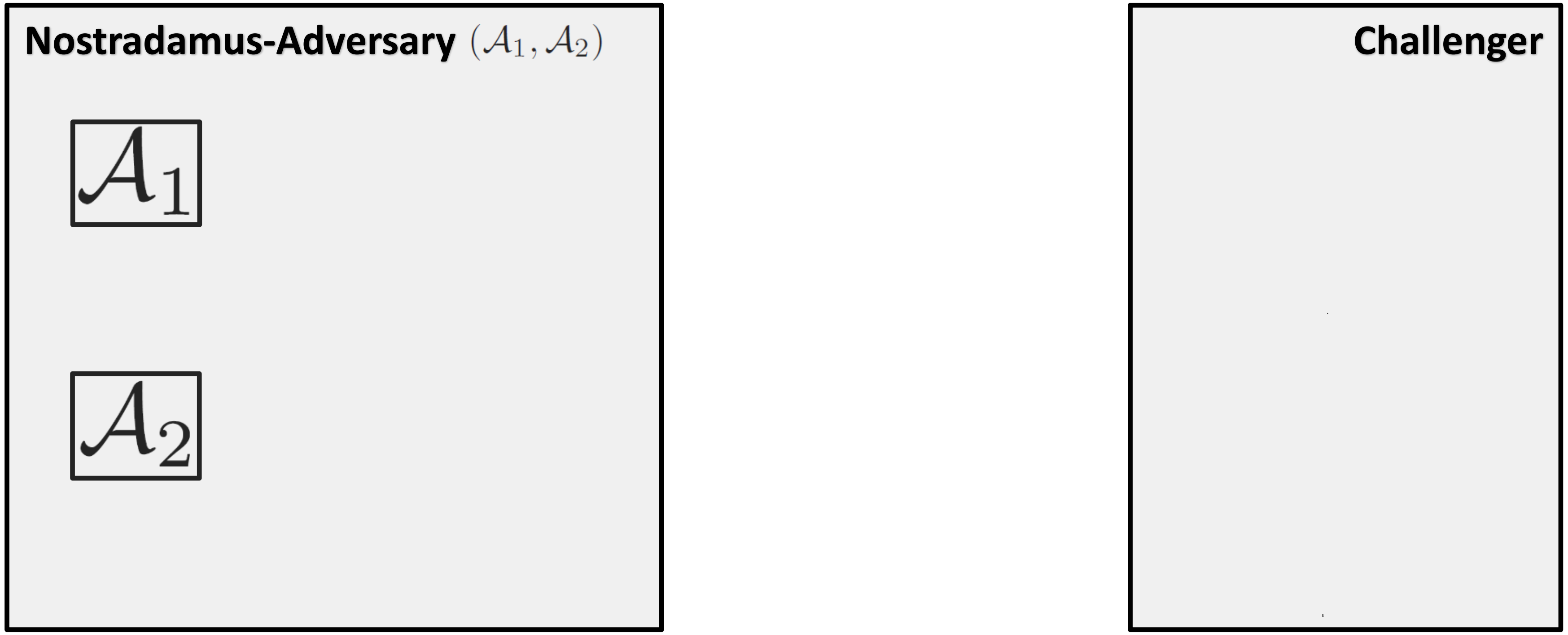
Preliminaries

$\text{hash}: \{0,1\}^* \rightarrow \{0,1\}^n$ **iterated** hash function, e.g.,*

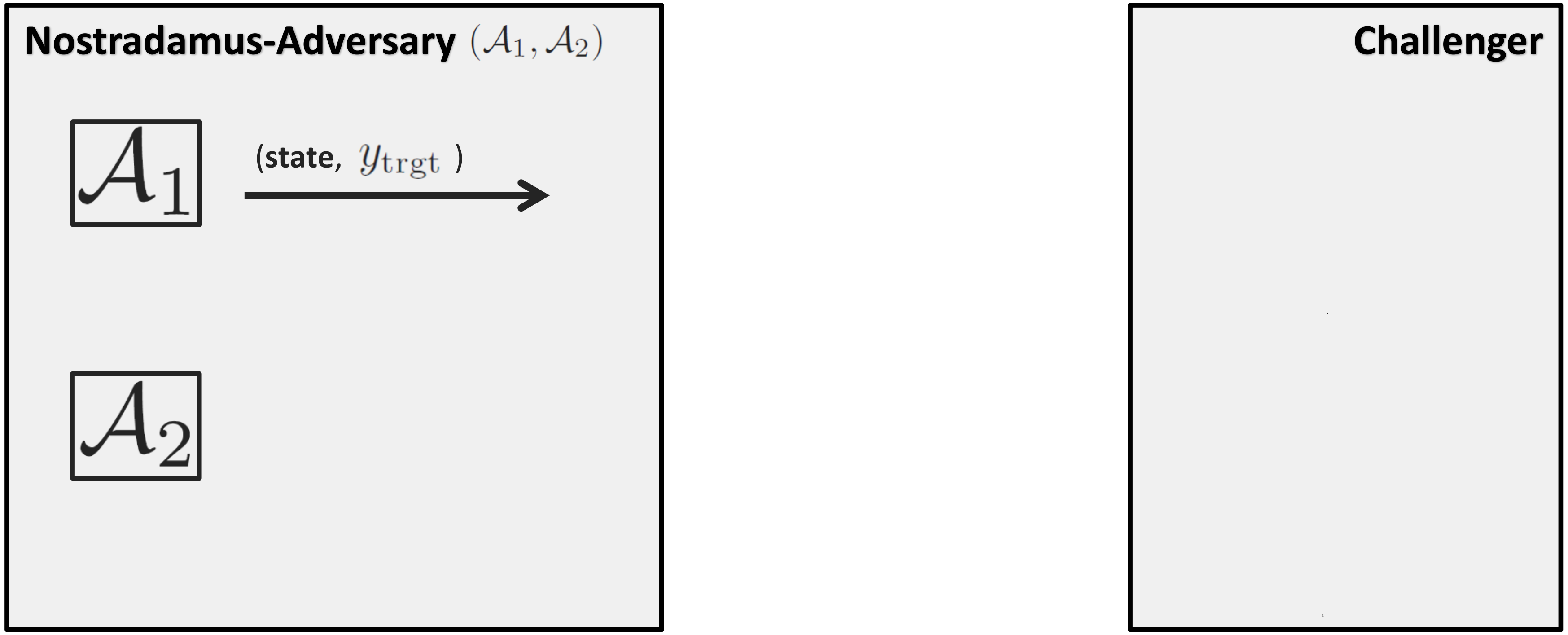


* Results also applicable to SHA-2, SHA-3 or SHAKE.

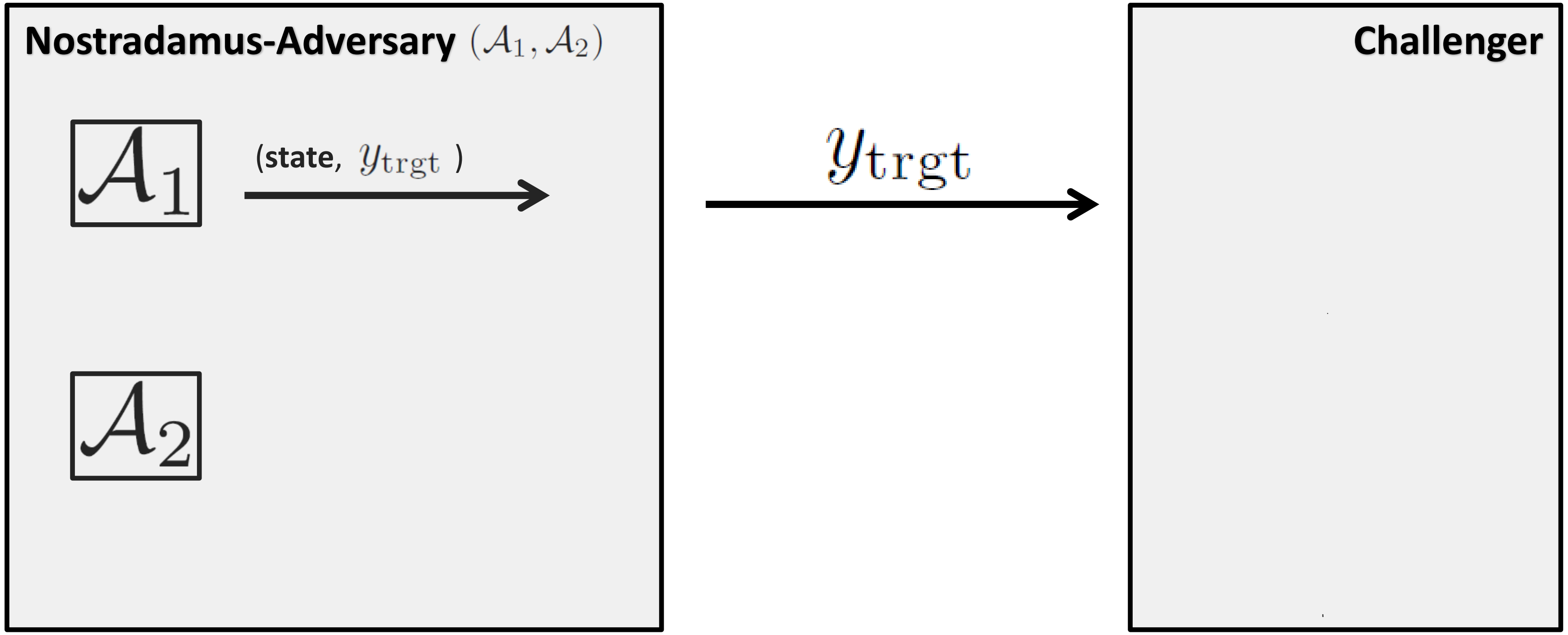
The Formal Nostradamus-Attack



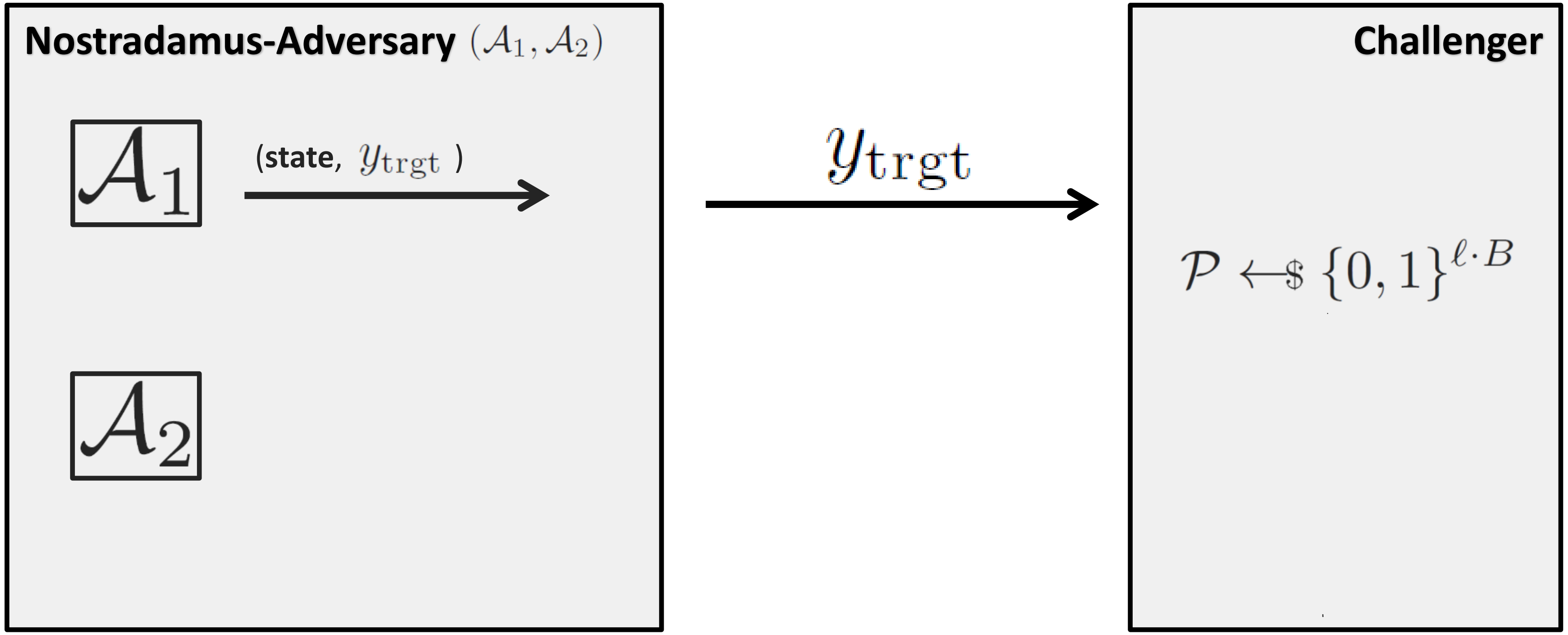
The Formal Nostradamus-Attack



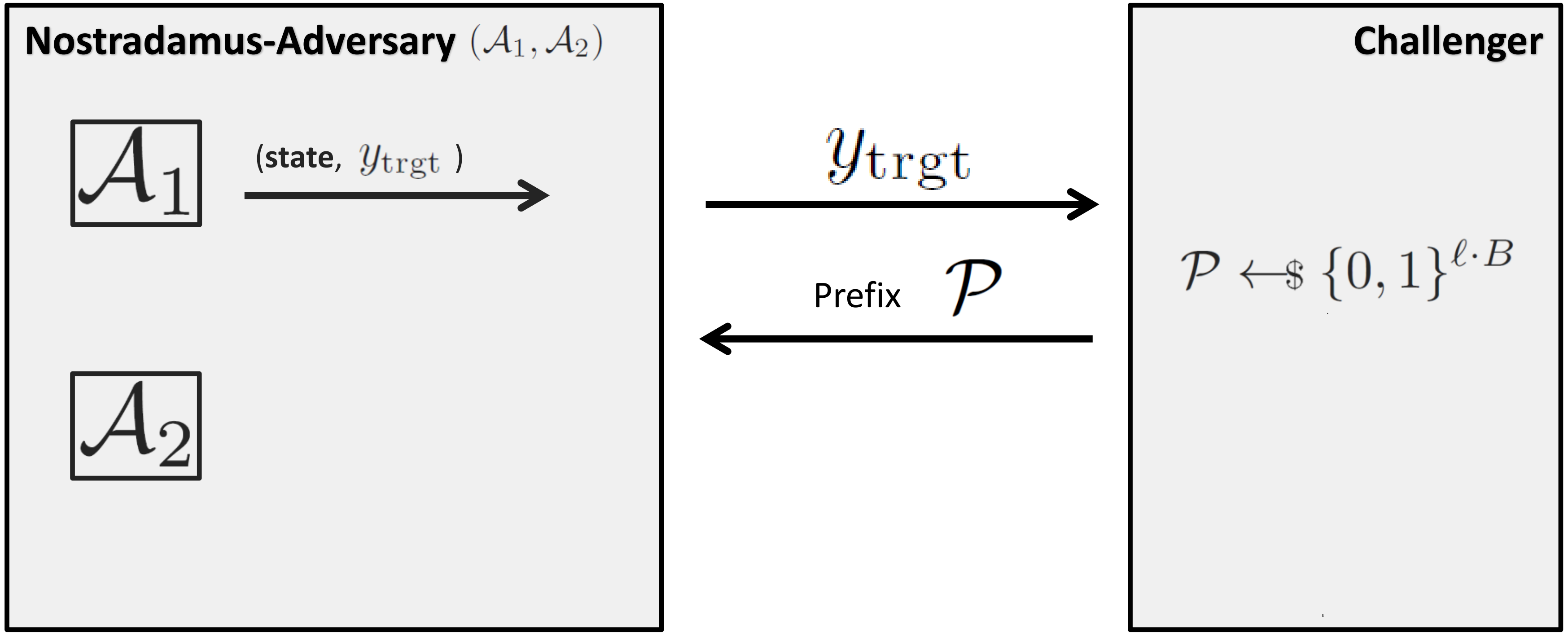
The Formal Nostradamus-Attack



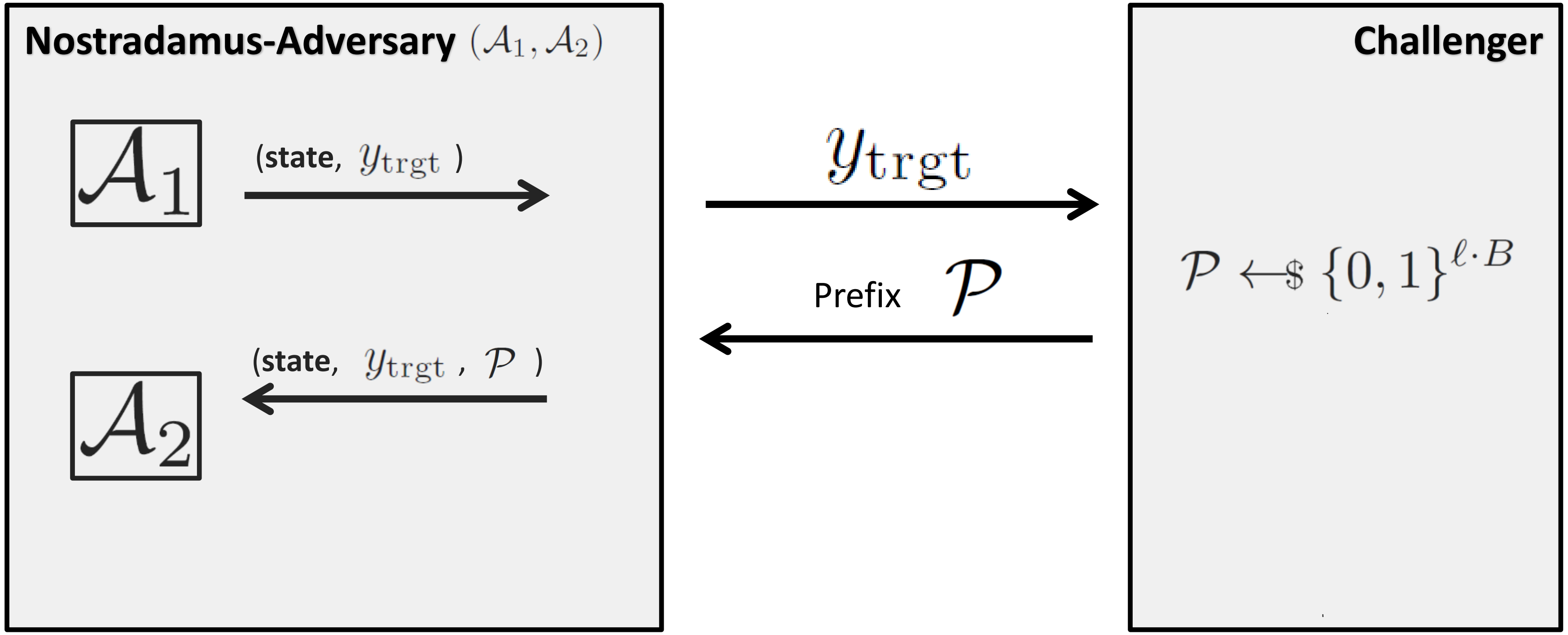
The Formal Nostradamus-Attack



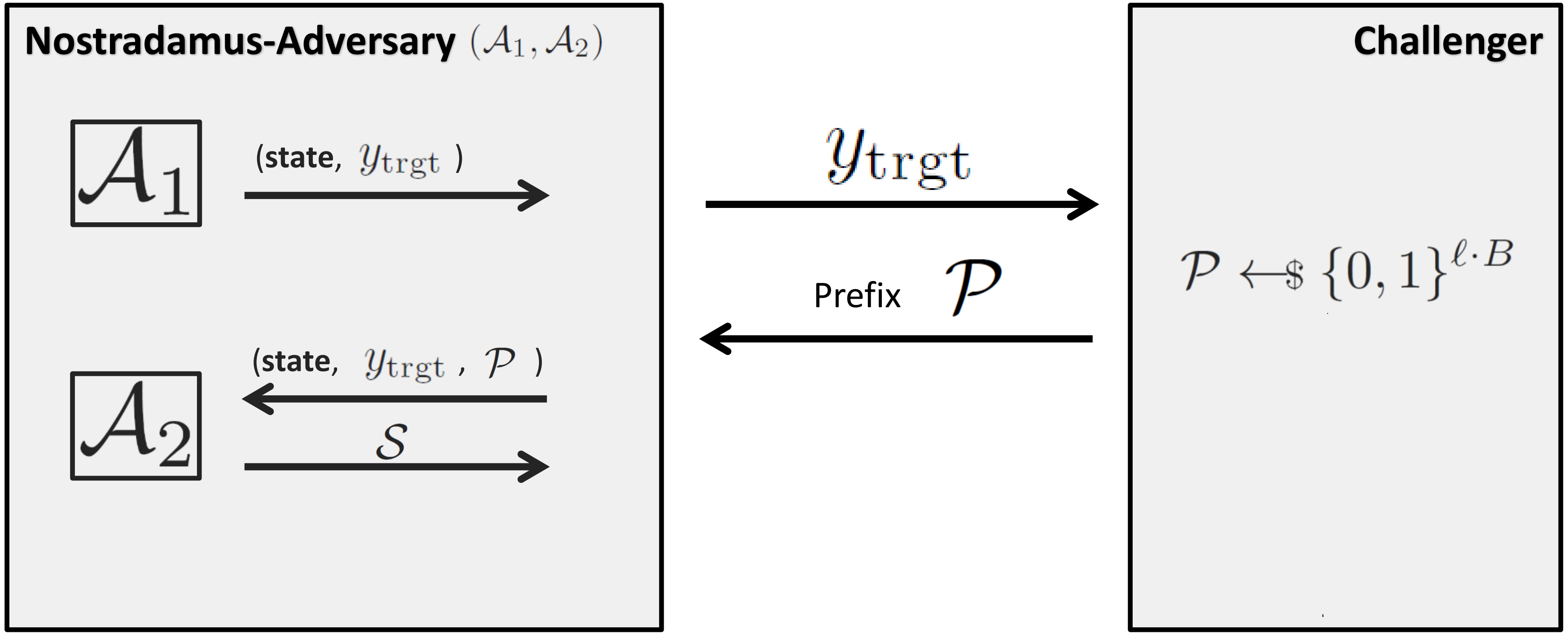
The Formal Nostradamus-Attack



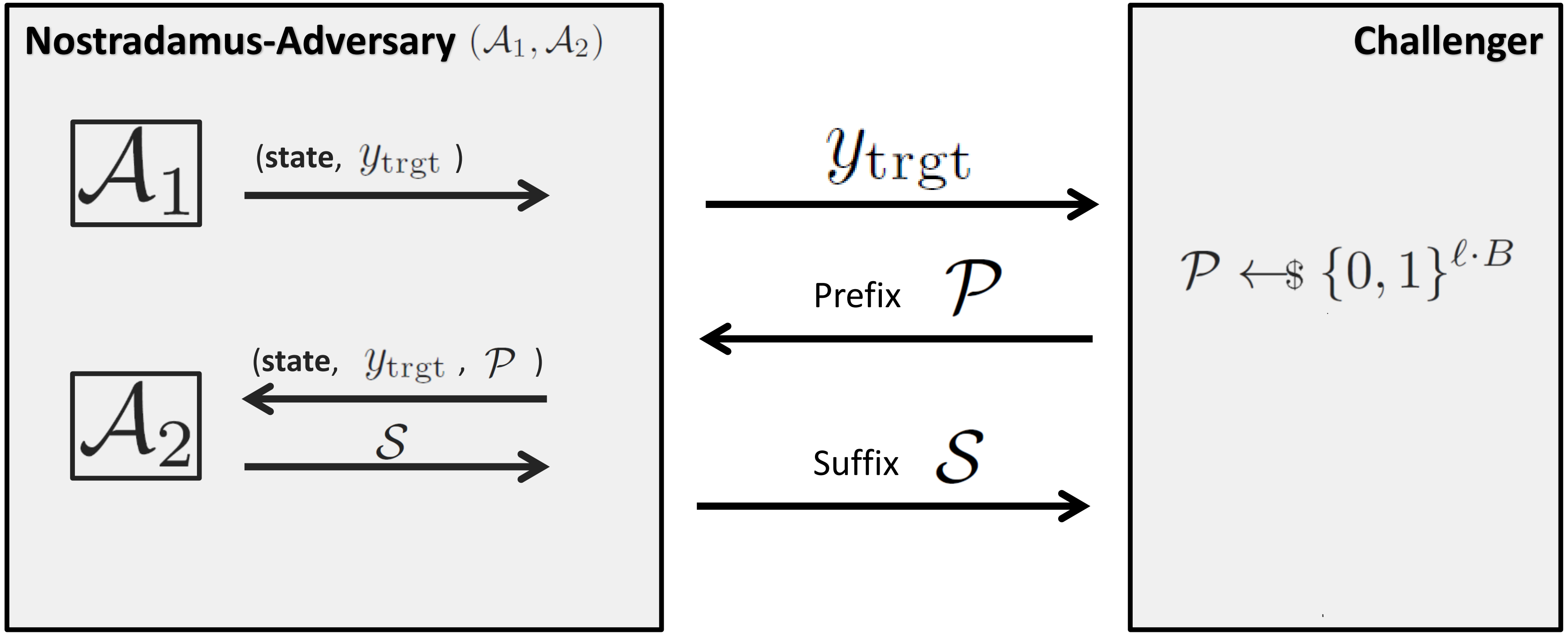
The Formal Nostradamus-Attack



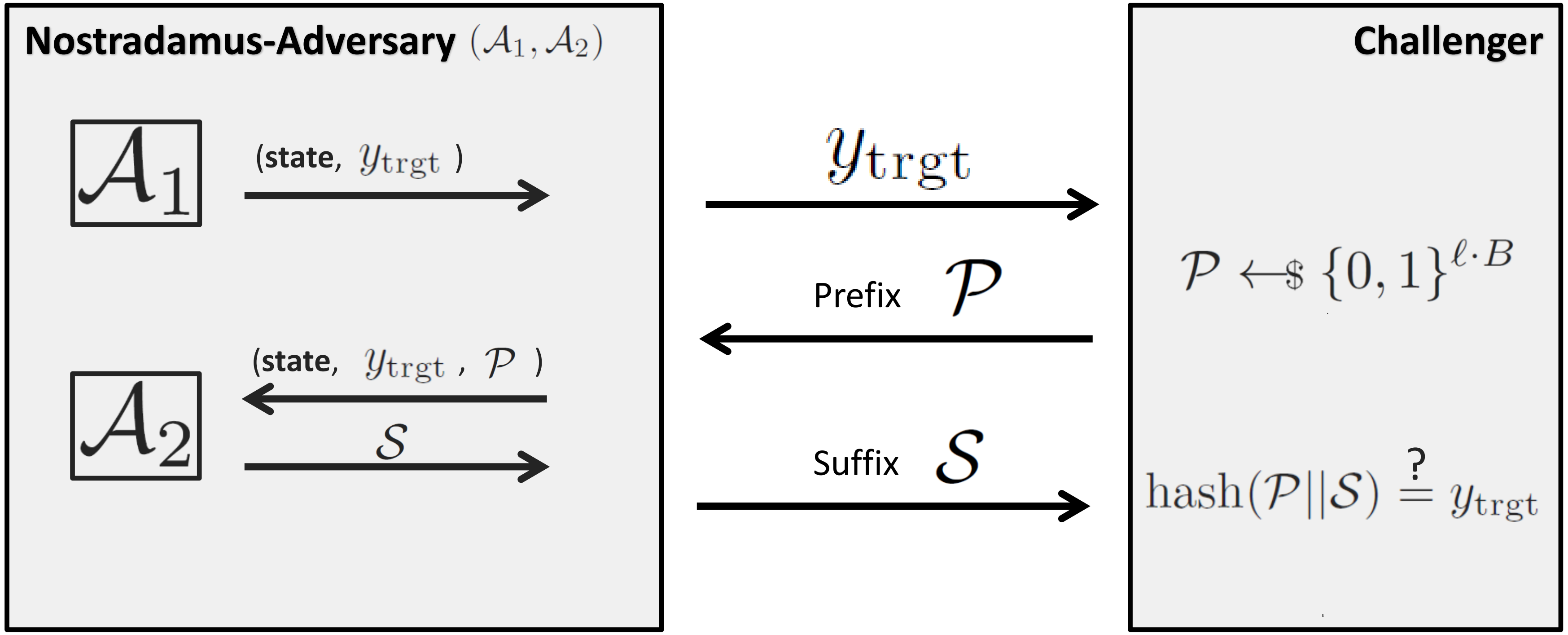
The Formal Nostradamus-Attack



The Formal Nostradamus-Attack



The Formal Nostradamus-Attack



History of Nostradamus-Attacker

Legendary Nostradamus

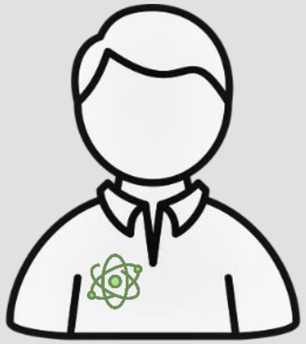
↓

requires magic

Classical Nostradamus [KK06, BSU12]

↓

$$\mathcal{O}\left(\sqrt{n}\cdot 2^{\frac{2n}{3}}\right)$$



Quantum Nostradamus [our work]

↓

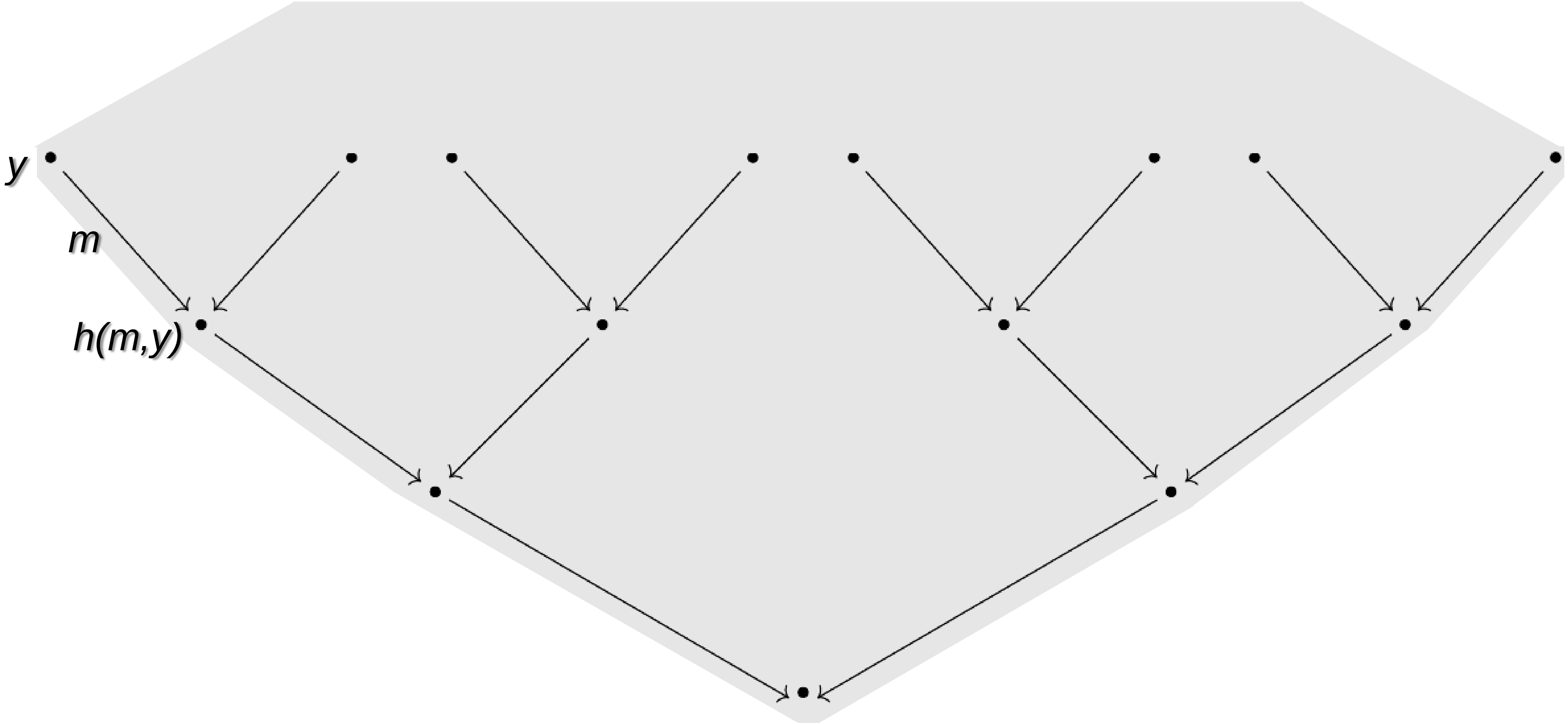
$$\mathcal{O}\left(\sqrt[3]{n}\cdot 2^{\frac{3n}{7}}\right)$$

Essentially optimal!

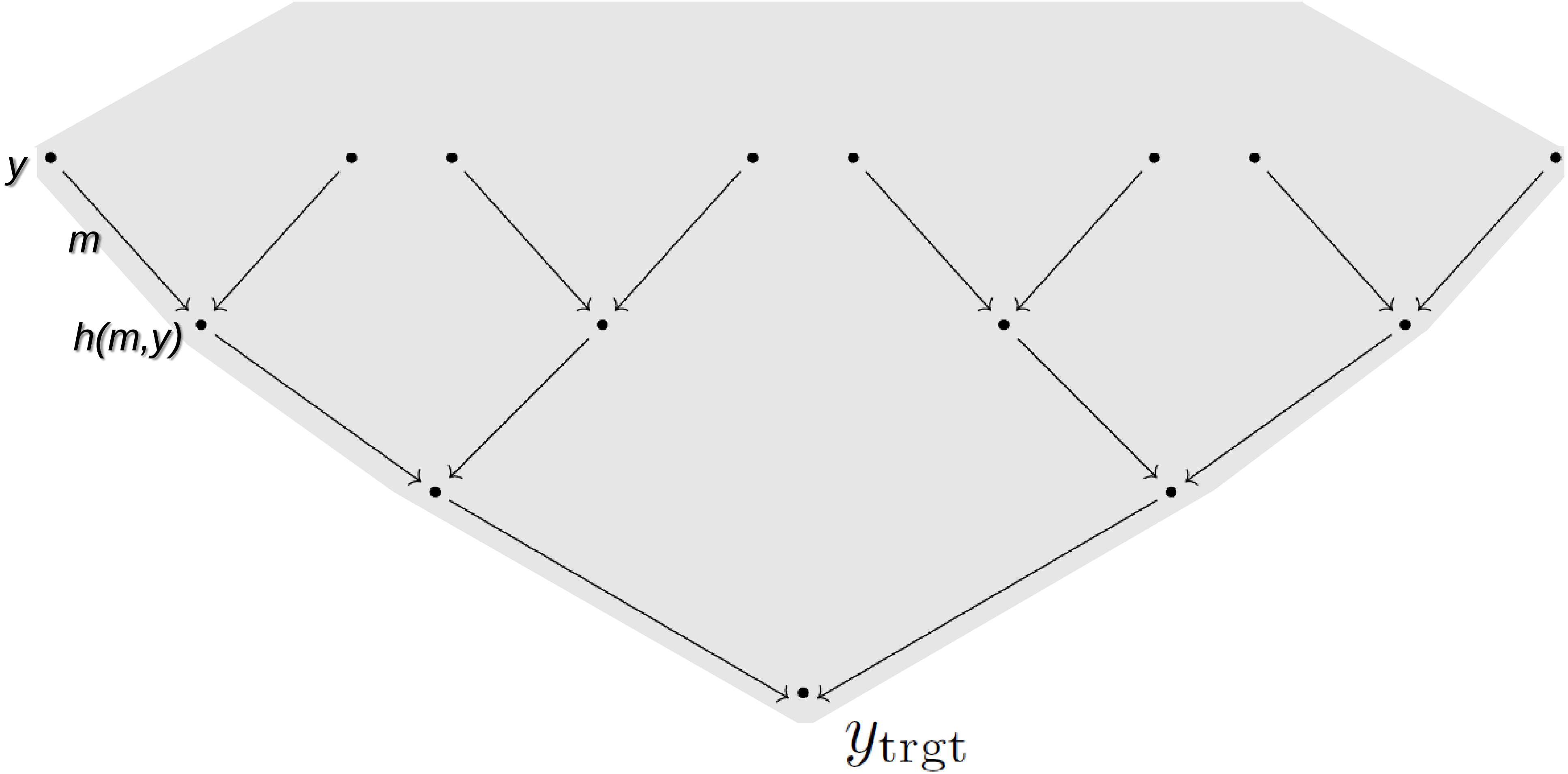
[BSU12] Blackburn, Stinson and Upadhyay. On the complexity of the herding attack and some related attacks on hash functions. Designs, Codes and Cryptography, 2012.

[KK06] Kelsey and Kohno. Herding Hash Functions and the Nostradamus Attack. Advances in Cryptology - EUROCRYPT 2006.

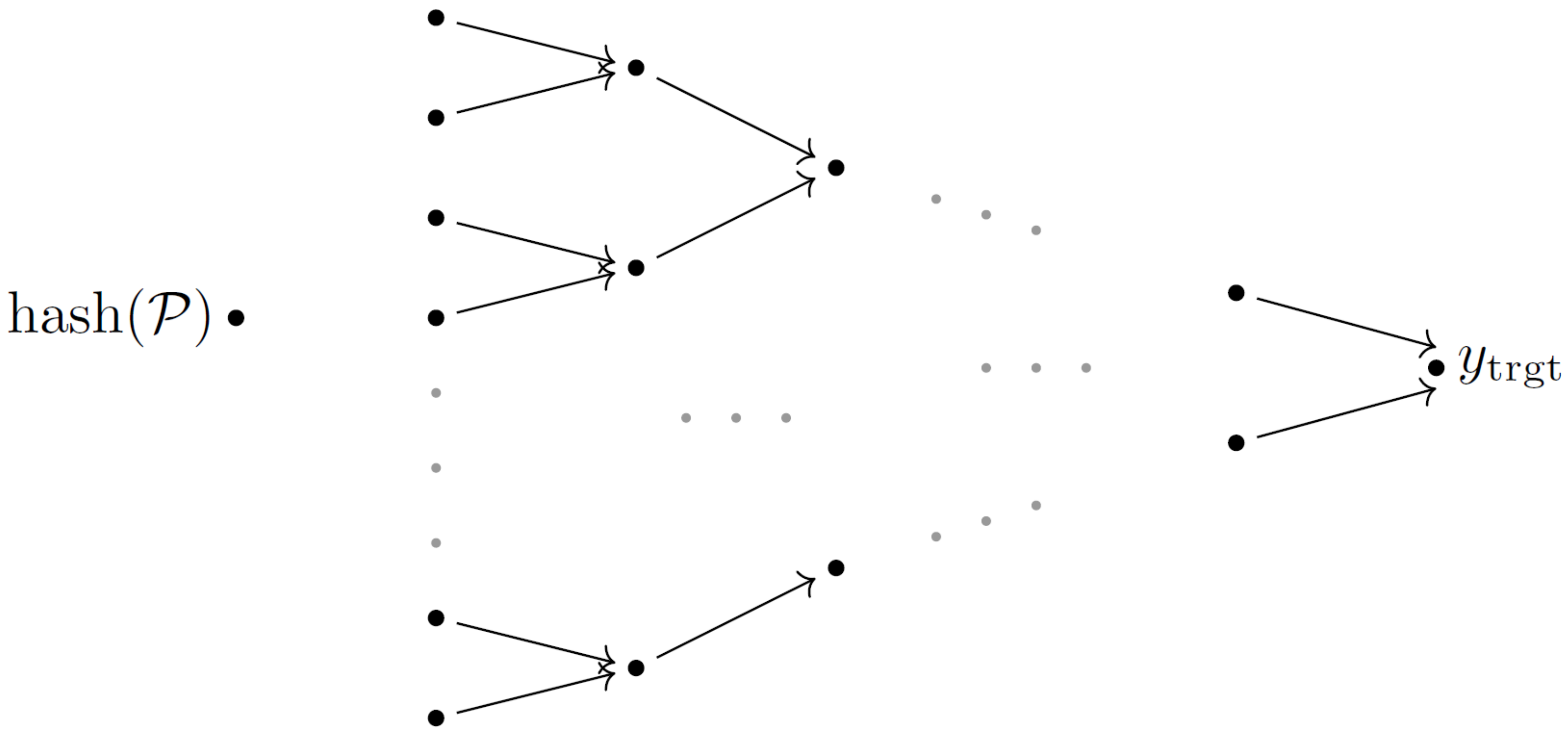
The First Phase



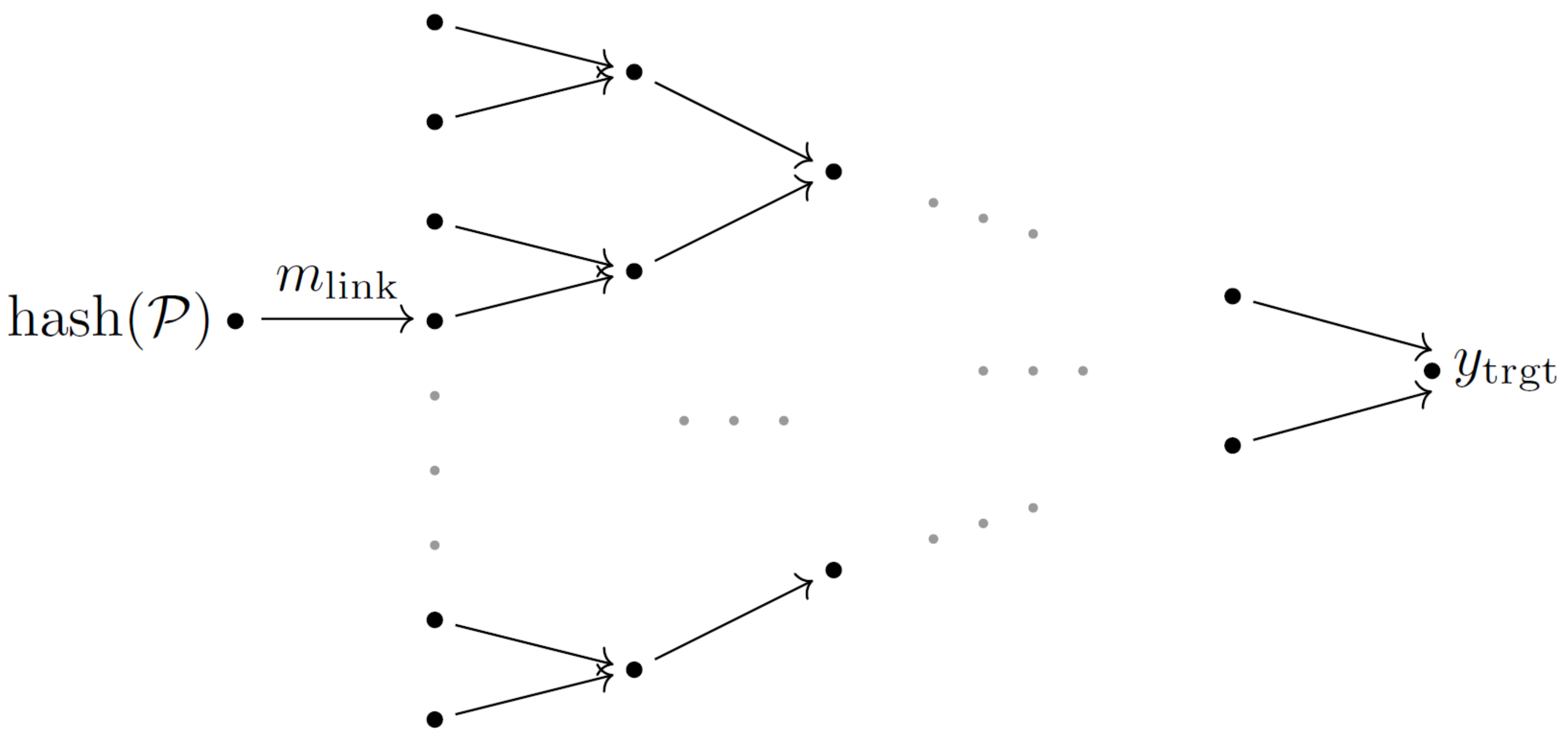
The First Phase



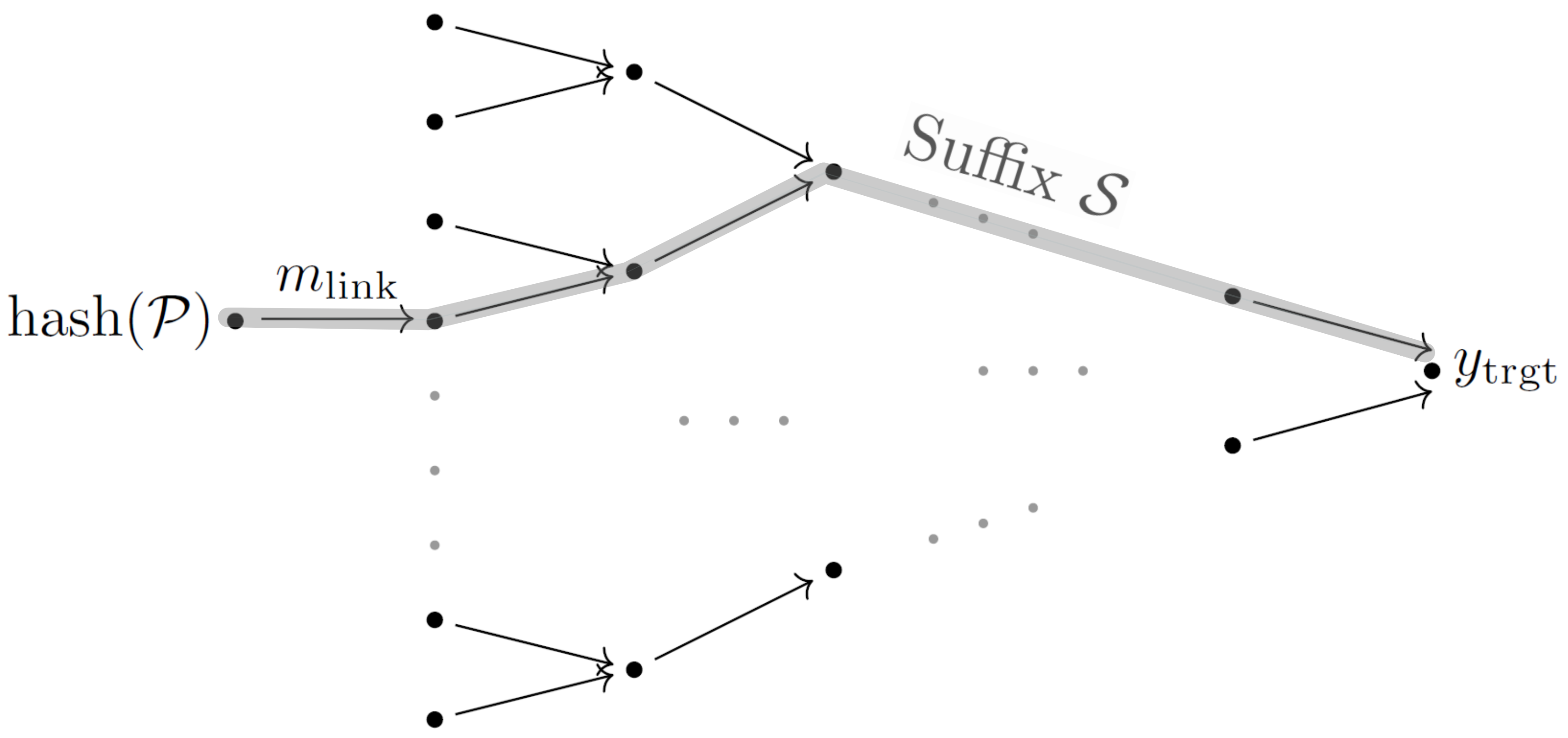
The Second Phase



The Second Phase



The Second Phase



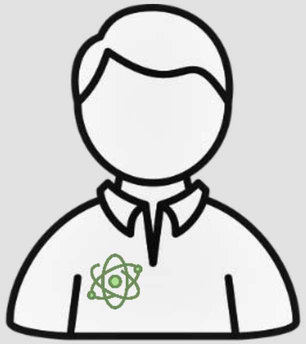
History of Nostradamus-Attacker

Legendary Nostradamus

requires magic

Classical Nostradamus [KK06, BSU12]

$$\mathcal{O}\left(\sqrt{n}\cdot 2^{\frac{2n}{3}}\right)$$



Quantum Nostradamus [our work]

$$\underline{\mathcal{O}\left(\sqrt[3]{n}\cdot 2^{\frac{3n}{7}}\right)}$$

Essentially optimal!

[BSU12] Blackburn, Stinson and Upadhyay. On the complexity of the herding attack and some related attacks on hash functions. Designs, Codes and Cryptography, 2012.

[KK06] Kelsey and Kohno. Herding Hash Functions and the Nostradamus Attack. Advances in Cryptology - EUROCRYPT 2006.

Grover's Algorithm

Theorem [BBHT98, Gro96]. Let $M^* \subseteq \{0,1\}^B$ be a *non-empty* set of suitable message blocks. Then there is a quantum algorithm, which finds a suitable message block after

$$\mathcal{O}\left(\sqrt{p^{-1}}\right)$$

"valuations" of message blocks, where $p := |M^*| \cdot 2^{-B}$.

[BBHT98] Boyer, Brassard, Høyer and Tapp. Tight bounds on quantum searching. Progress of Physics, 1998.

[Gro96] Grover. A fast quantum mechanical algorithm for database search. Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing 1996.

Grover's Algorithm

Theorem [BBHT98, Gro96]. Let $M^* \subseteq \{0,1\}^B$ be a *non-empty* set of suitable message blocks. Then there is a quantum algorithm, which finds a suitable message block after

$$\mathcal{O}\left(\sqrt{p^{-1}}\right)$$

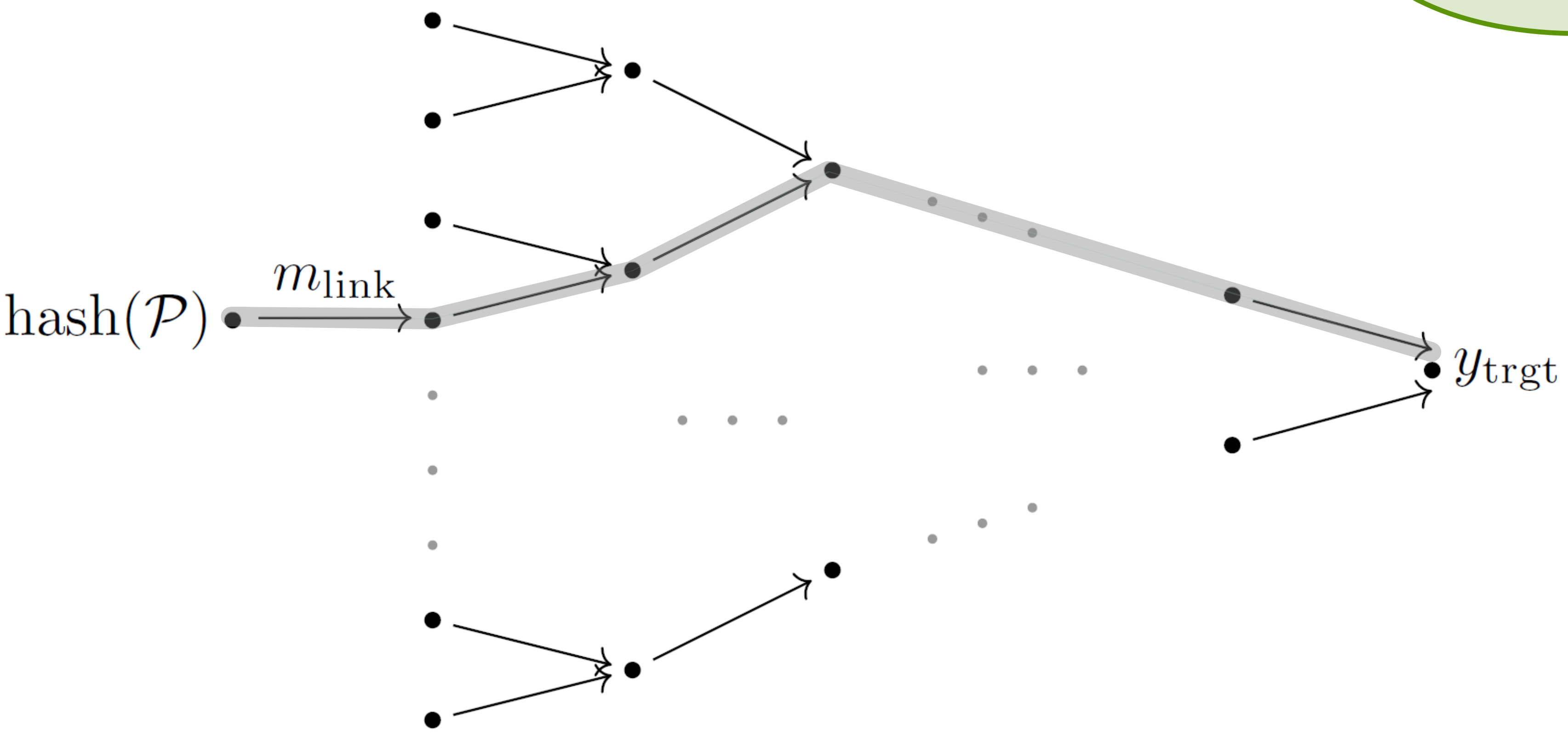
"valuations" of message blocks, where $p := |M^*| \cdot 2^{-B}$.

Check of Suitability

[BBHT98] Boyer, Brassard, Høyer and Tapp. Tight bounds on quantum searching. Progress of Physics, 1998.
[Gro96] Grover. A fast quantum mechanical algorithm for database search. Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing 1996.

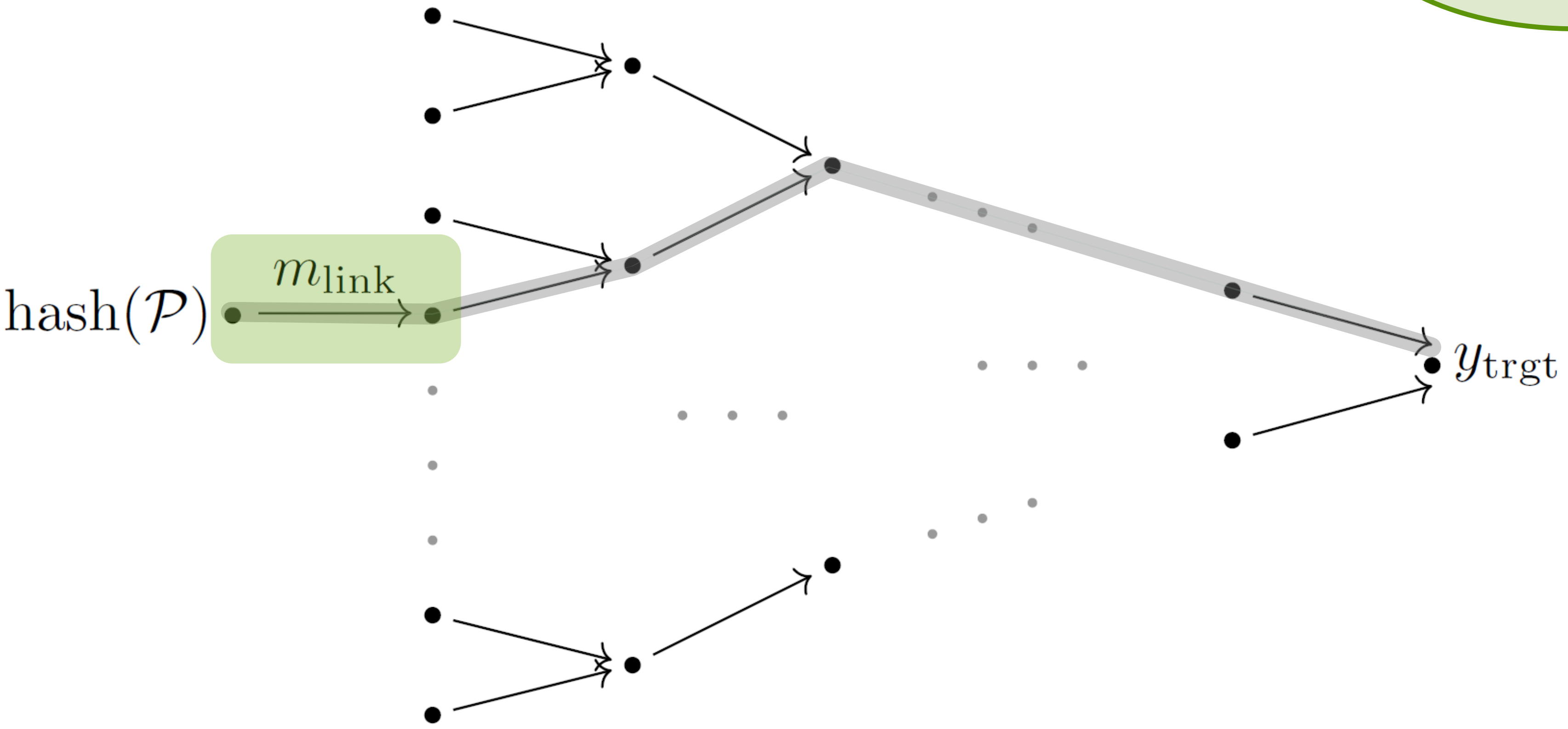
How to Apply Grover's Algorithm

Grover succeeds after $\mathcal{O}\left(\sqrt{p^{-1}}\right)$ evaluations of h.



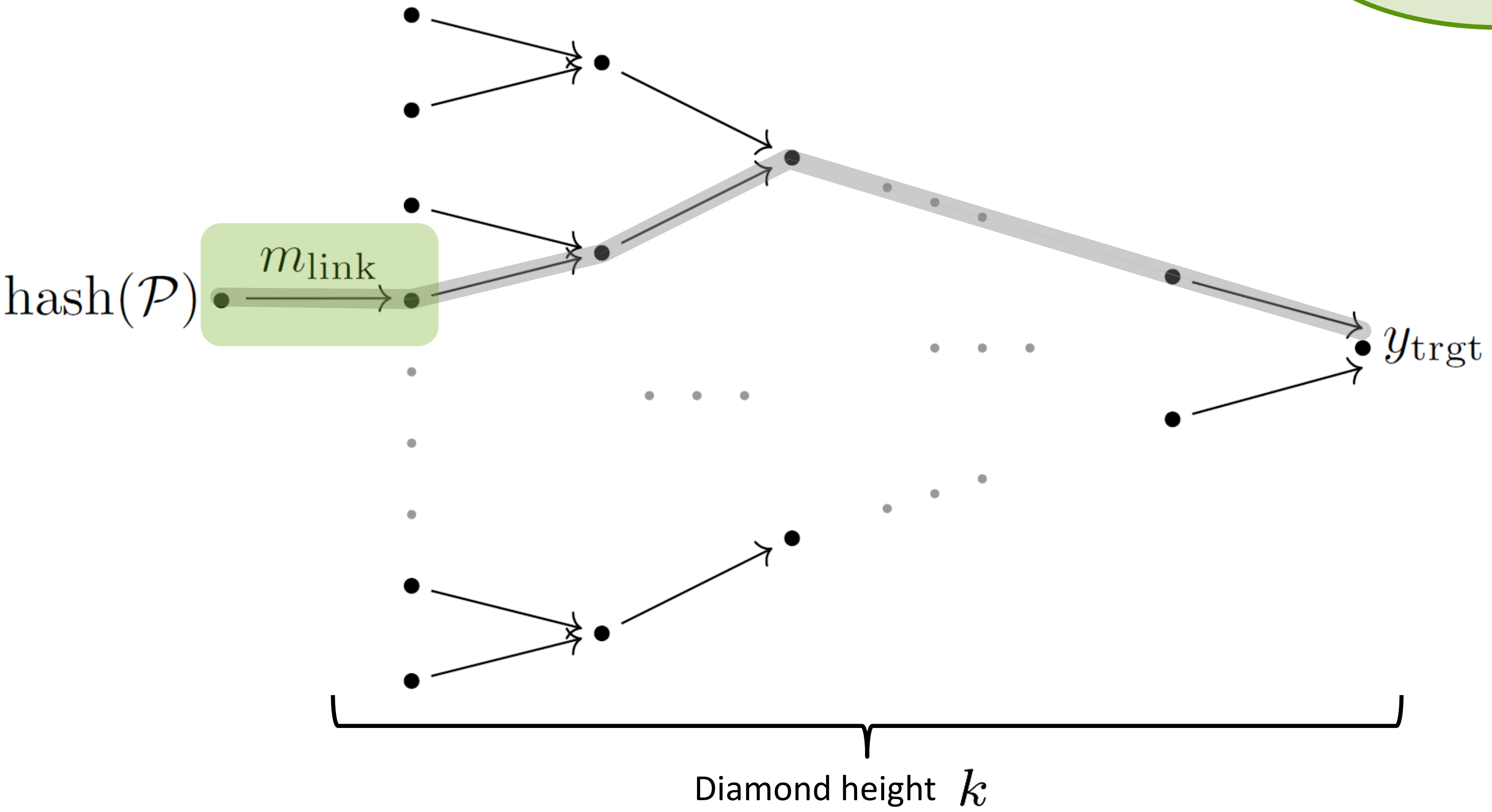
How to Apply Grover's Algorithm

Grover succeeds after $\mathcal{O}\left(\sqrt{p^{-1}}\right)$ evaluations of h.



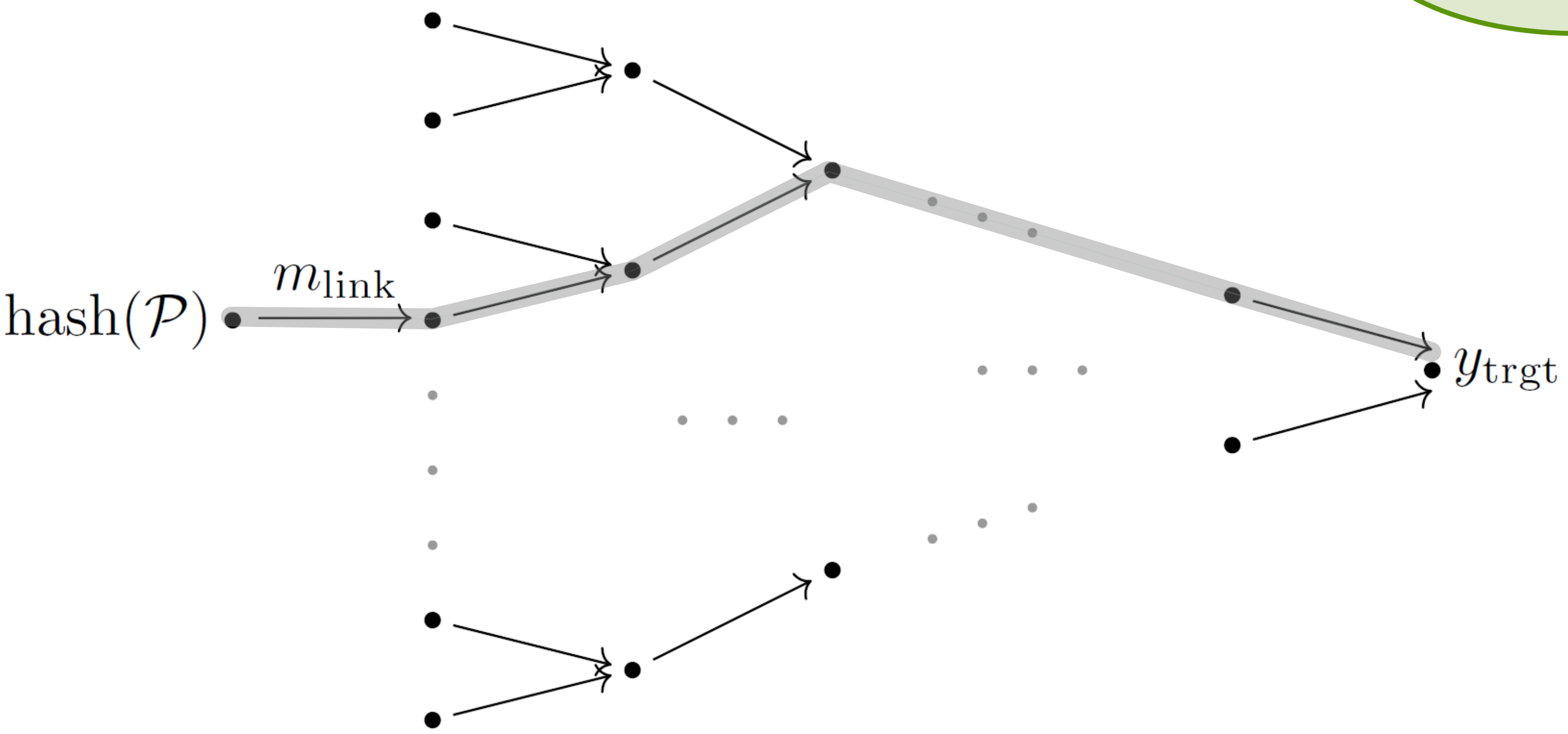
How to Apply Grover's Algorithm

Grover succeeds after $\mathcal{O}\left(\sqrt{p^{-1}}\right)$ evaluations of h.



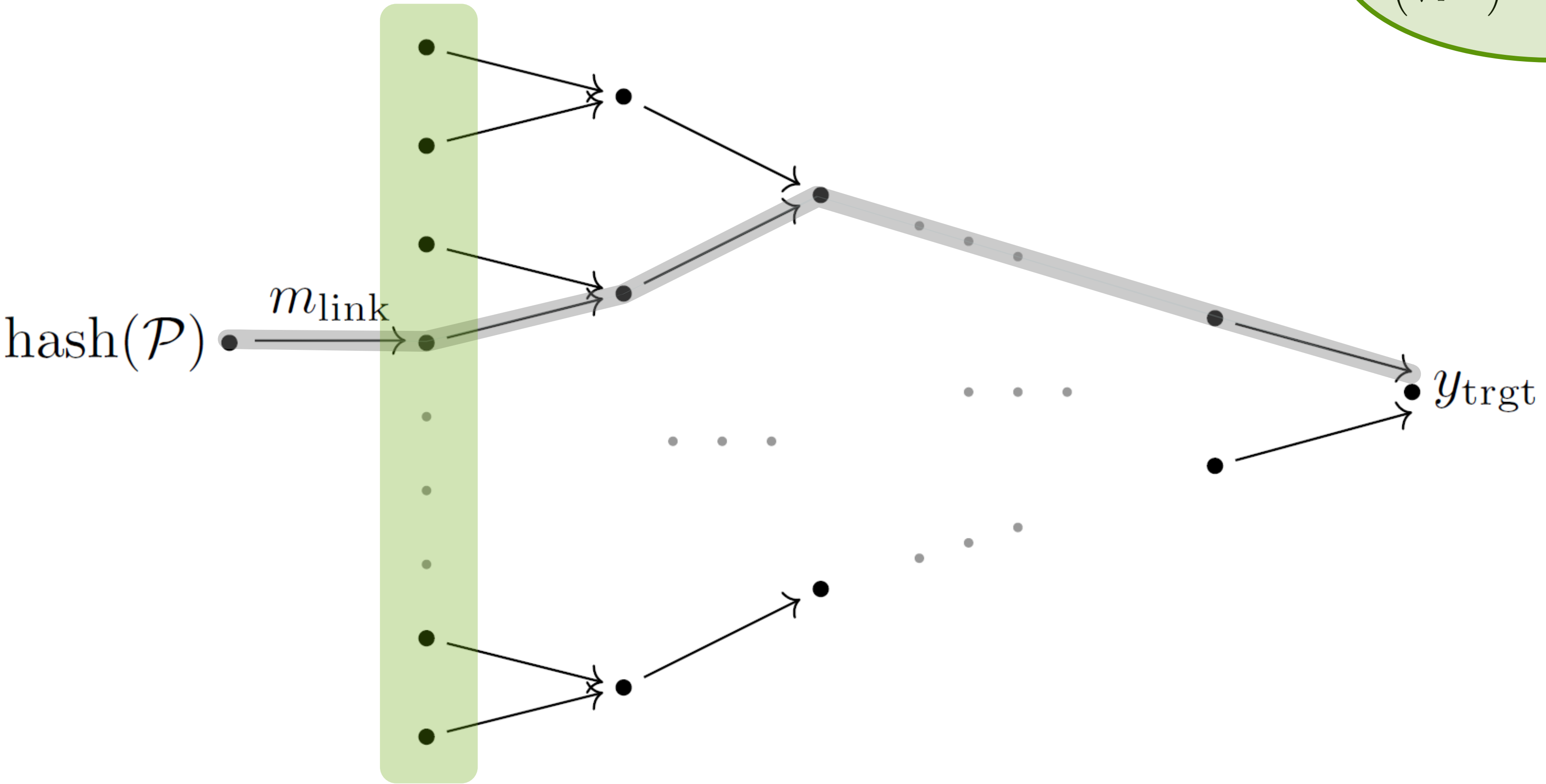
How to Apply Grover's Algorithm

Grover succeeds after $\mathcal{O}\left(\sqrt{p^{-1}}\right)$ evaluations of h.



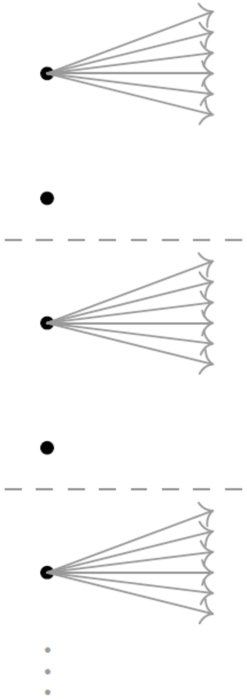
How to Apply Grover's Algorithm

Grover succeeds after $\mathcal{O}\left(\sqrt{p^{-1}}\right)$ evaluations of h.



Naïve Approach [BHT98]

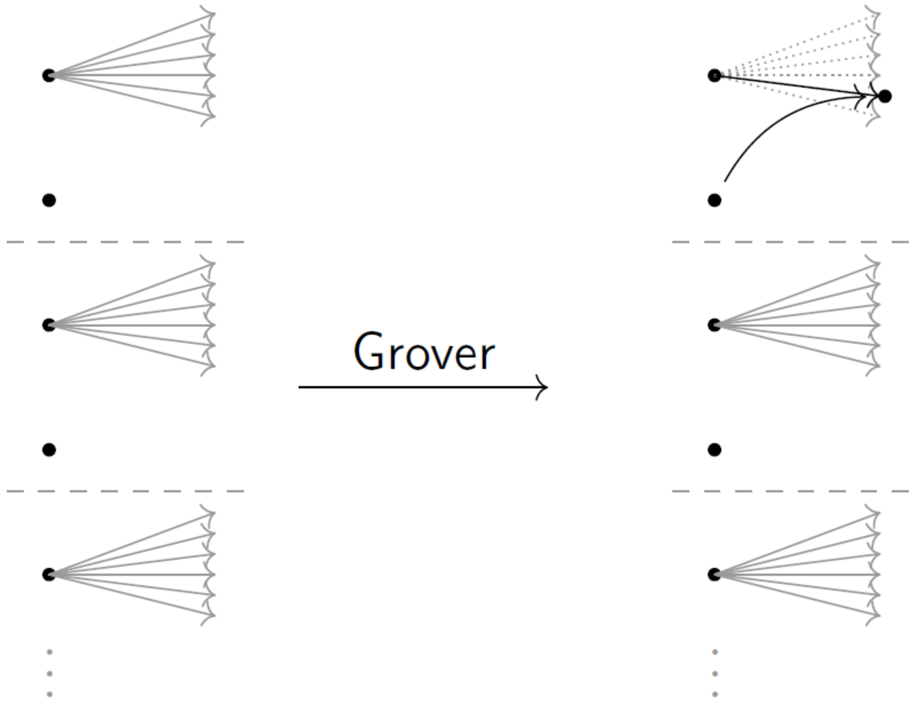
Grover succeeds after $\mathcal{O}\left(\sqrt{p^{-1}}\right)$ evaluations of h.



[BHT98] Brassard, Høyer and Tapp. Quantum cryptanalysis of hash and claw-free Functions. LATIN '98: Theoretical Informatics, Third Latin American Symposium.

Naïve Approach [BHT98]

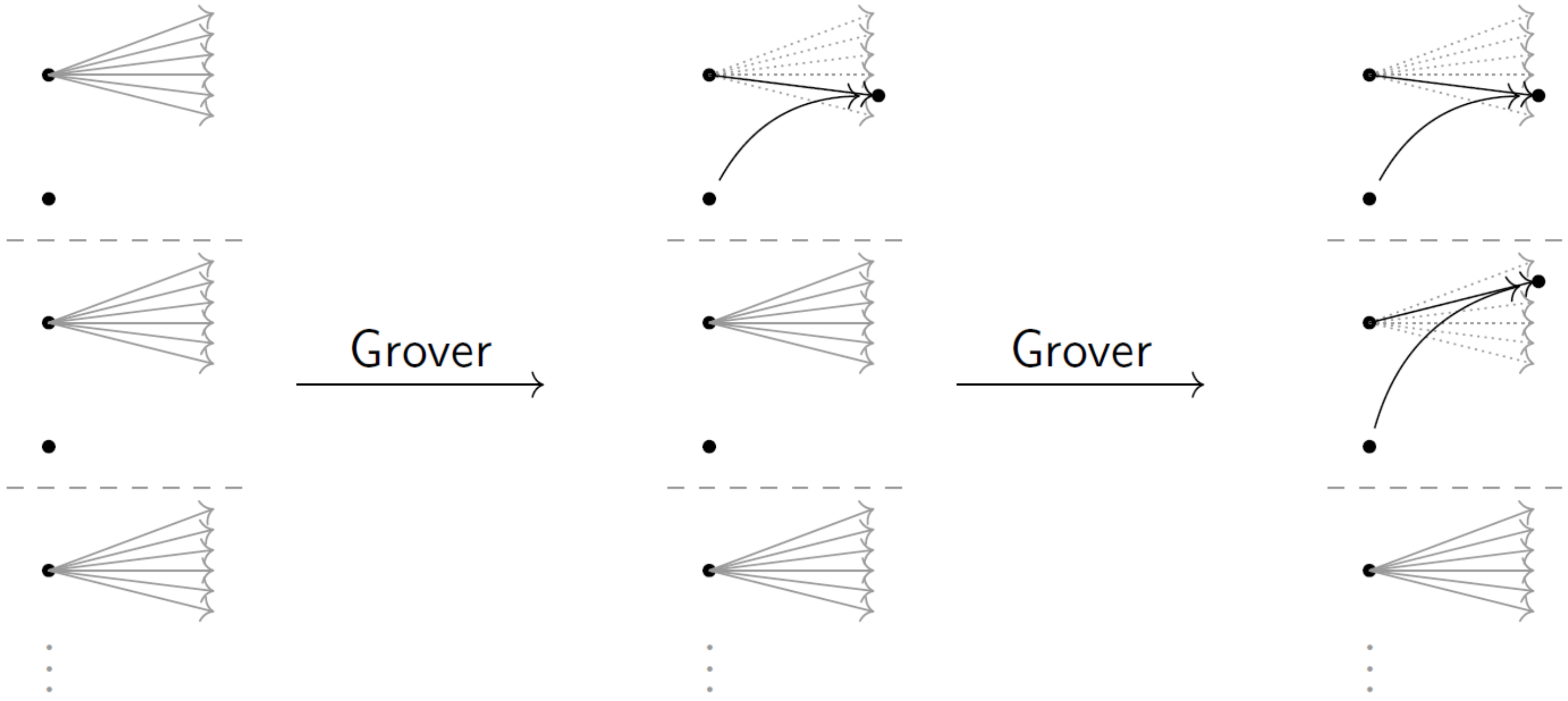
Grover succeeds after $\mathcal{O}\left(\sqrt{p^{-1}}\right)$ evaluations of h.



[BHT98] Brassard, Høyer and Tapp. Quantum cryptanalysis of hash and claw-free Functions. LATIN '98: Theoretical Informatics, Third Latin American Symposium.

Naïve Approach [BHT98]

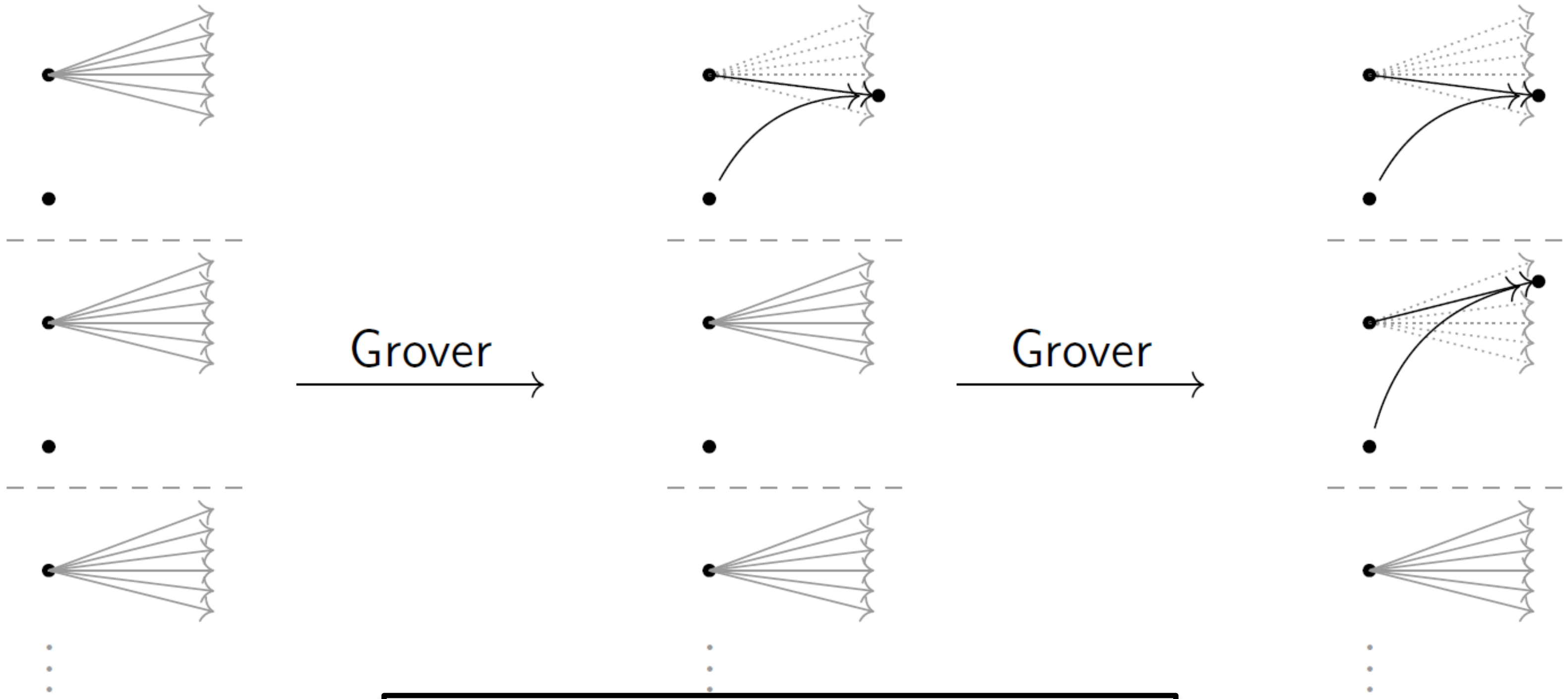
Grover succeeds after $\mathcal{O}\left(\sqrt{p^{-1}}\right)$ evaluations of h.



[BHT98] Brassard, Høyer and Tapp. Quantum cryptanalysis of hash and claw-free Functions. LATIN '98: Theoretical Informatics, Third Latin American Symposium.

Naïve Approach [BHT98]

Grover succeeds after $\mathcal{O}\left(\sqrt{p^{-1}}\right)$ evaluations of h.

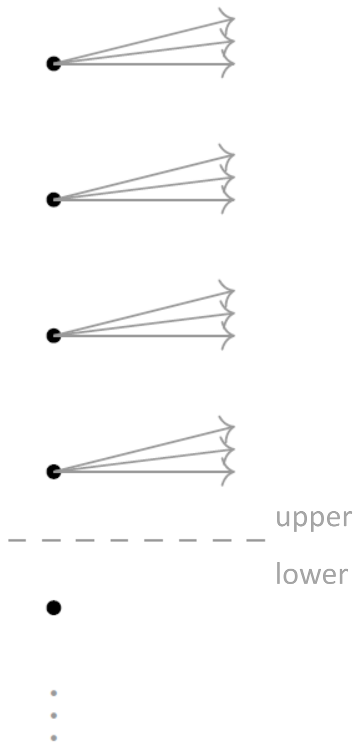


Problem: Needs a lot of evaluations for each pair!

[BHT98] Brassard, Høyer and Tapp. Quantum cryptanalysis of hash and claw-free Functions. LATIN ’98: Theoretical Informatics, Third Latin American Symposium.

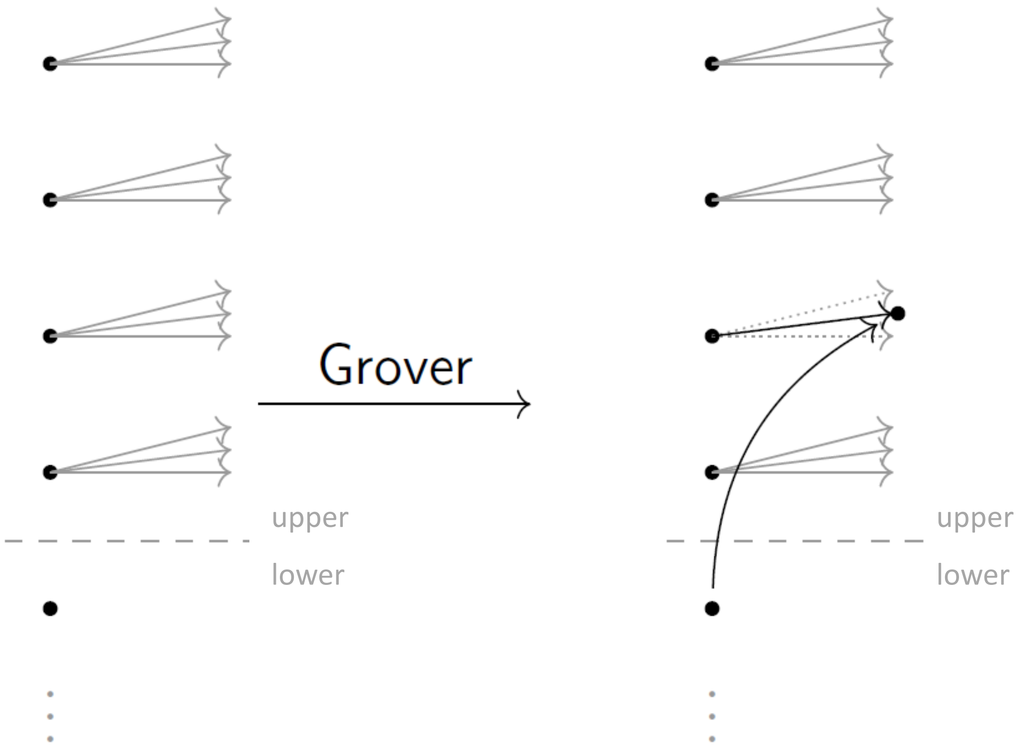
Enhanced Approach

Grover succeeds after $\mathcal{O}\left(\sqrt{p^{-1}}\right)$ evaluations of h.



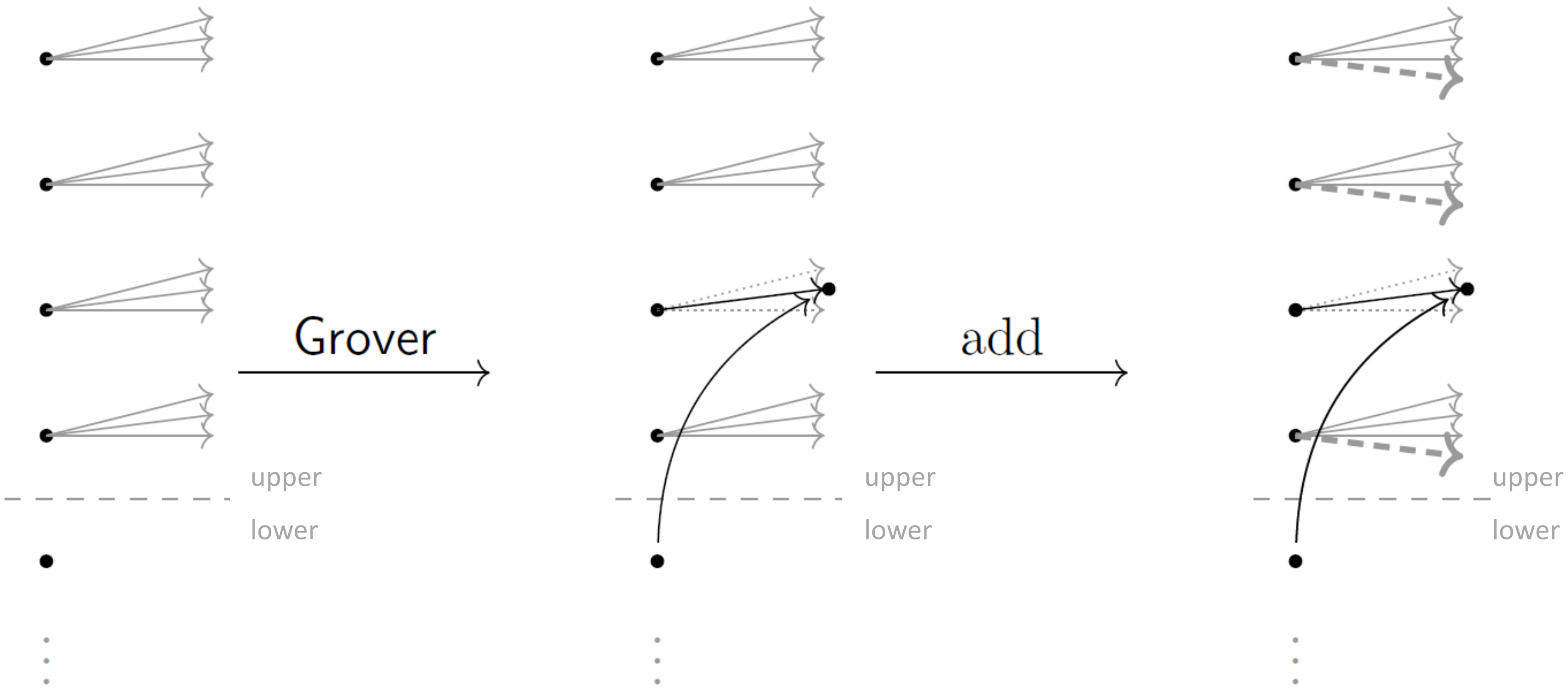
Enhanced Approach

Grover succeeds after $\mathcal{O}\left(\sqrt{p^{-1}}\right)$ evaluations of h.



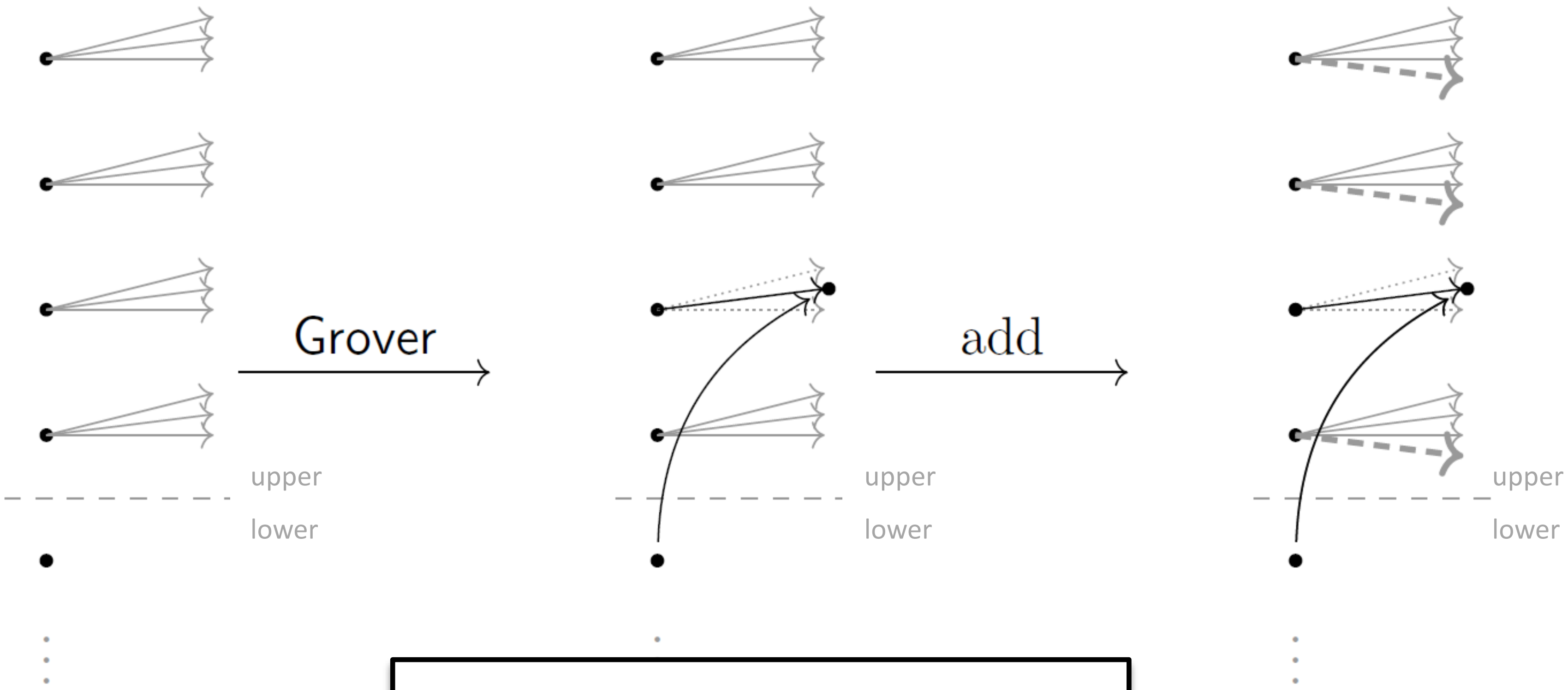
Enhanced Approach

Grover succeeds after $\mathcal{O}\left(\sqrt{p^{-1}}\right)$ evaluations of h.



Enhanced Approach

Grover succeeds after $\mathcal{O}\left(\sqrt{p^{-1}}\right)$ evaluations of h.



Advantage: Needs fewer evaluations on average for each pair!

	Classical [KK06]	Naïve **[our work]**	Enhanced **[our work]**
$\mathcal{A}_1$	$\mathcal{O}\left(\sqrt{k} \cdot 2^{\frac{n+k}{2}}\right)$	$\mathcal{O}(2^{\frac{n}{3}+k})$	$\mathcal{O}\left(\sqrt[3]{k} \cdot 2^{\frac{n+2k}{3}}\right)$
$\mathcal{A}_2$	$\mathcal{O}(2^{n-k})$	$\mathcal{O}\left(2^{\frac{n-k}{2}}\right)$	$\mathcal{O}\left(2^{\frac{n-k}{2}}\right)$
The Attack $(\mathcal{A}_1, \mathcal{A}_2)$	$\mathcal{O}\left(\sqrt{n} \cdot 2^{\frac{2n}{3}}\right)$	$\mathcal{O}\left(2^{\frac{4n}{9}}\right)$	$\mathcal{O}\left(\sqrt[3]{n} \cdot 2^{\frac{3n}{7}}\right)$

n = hash size
k = diamond height

[KK06] Kelsey and Kohno. Herding Hash Functions and the Nostradamus Attack. Advances in Cryptology - EUROCRYPT 2006.

	Classical [KK06]	Naïve **[our work]**	Enhanced **[our work]**
$\mathcal{A}_1$	$\mathcal{O}\left(\sqrt{k} \cdot 2^{\frac{n+k}{2}}\right)$	$\mathcal{O}(2^{\frac{n}{3}+k})$	$\mathcal{O}\left(\sqrt[3]{k} \cdot 2^{\frac{n+2k}{3}}\right)$
$\mathcal{A}_2$	$\mathcal{O}(2^{n-k})$	$\mathcal{O}\left(2^{\frac{n-k}{2}}\right)$	$\mathcal{O}\left(2^{\frac{n-k}{2}}\right)$
The Attack $(\mathcal{A}_1, \mathcal{A}_2)$	$\mathcal{O}\left(\sqrt{n} \cdot 2^{\frac{2n}{3}}\right)$	$\mathcal{O}\left(2^{\frac{4n}{9}}\right)$	$\mathcal{O}\left(\sqrt[3]{n} \cdot 2^{\frac{3n}{7}}\right)$

Essentially optimal!

n = hash size
k = diamond height

[KK06] Kelsey and Kohno. Herding Hash Functions and the Nostradamus Attack. Advances in Cryptology - EUROCRYPT 2006.

About Lower Bounds

Lower Bound of c-Collision Finder [LZ19]

Theorem. Given a *random* function $f : X \to Y$ any quantum algorithm needs at least

$$\Omega\left(2^{\left(1-\frac{1}{2^c-1}\right)\cdot\frac{n}{2}}\right)$$

evaluations of function f to find a **c-collision**, i.e., c different elements $x_1, x_2, \ldots, x_c \in X$ such that $f(x_1) = f(x_2) = \cdots = f(x_c)$ with constant probability.

[LZ19] Liu and Zhandry. On Finding Quantum Multi-Collisions. Advances in Cryptology – EUROCRYPT 2019.

How to derive a Lower Bound for $(\mathcal{A}_1, \mathcal{A}_2)$?

How to derive a Lower Bound for $(\mathcal{A}_1, \mathcal{A}_2)$?

	Classical [KK06]	Naïve **[our work]**	Enhanced **[our work]**
$\mathcal{A}_1$	$\mathcal{O}\left(\sqrt{k} \cdot 2^{\frac{n+k}{2}}\right)$	$\mathcal{O}(2^{\frac{n}{3}+k})$	$\mathcal{O}\left(\sqrt[3]{k} \cdot 2^{\frac{n+2k}{3}}\right)$
$\mathcal{A}_2$	$\mathcal{O}(2^{n-k})$	$\mathcal{O}\left(2^{\frac{n-k}{2}}\right)$	$\mathcal{O}\left(2^{\frac{n-k}{2}}\right)$
The Attack $(\mathcal{A}_1, \mathcal{A}_2)$	$\mathcal{O}\left(\sqrt{n} \cdot 2^{\frac{2n}{3}}\right)$	$\mathcal{O}\left(2^{\frac{4n}{9}}\right)$	$\mathcal{O}\left(\sqrt[3]{n} \cdot 2^{\frac{3n}{7}}\right)$

n = hash size
k = diamond height

[KK06] Kelsey and Kohno. Herding Hash Functions and the Nostradamus Attack. Advances in Cryptology - EUROCRYPT 2006.

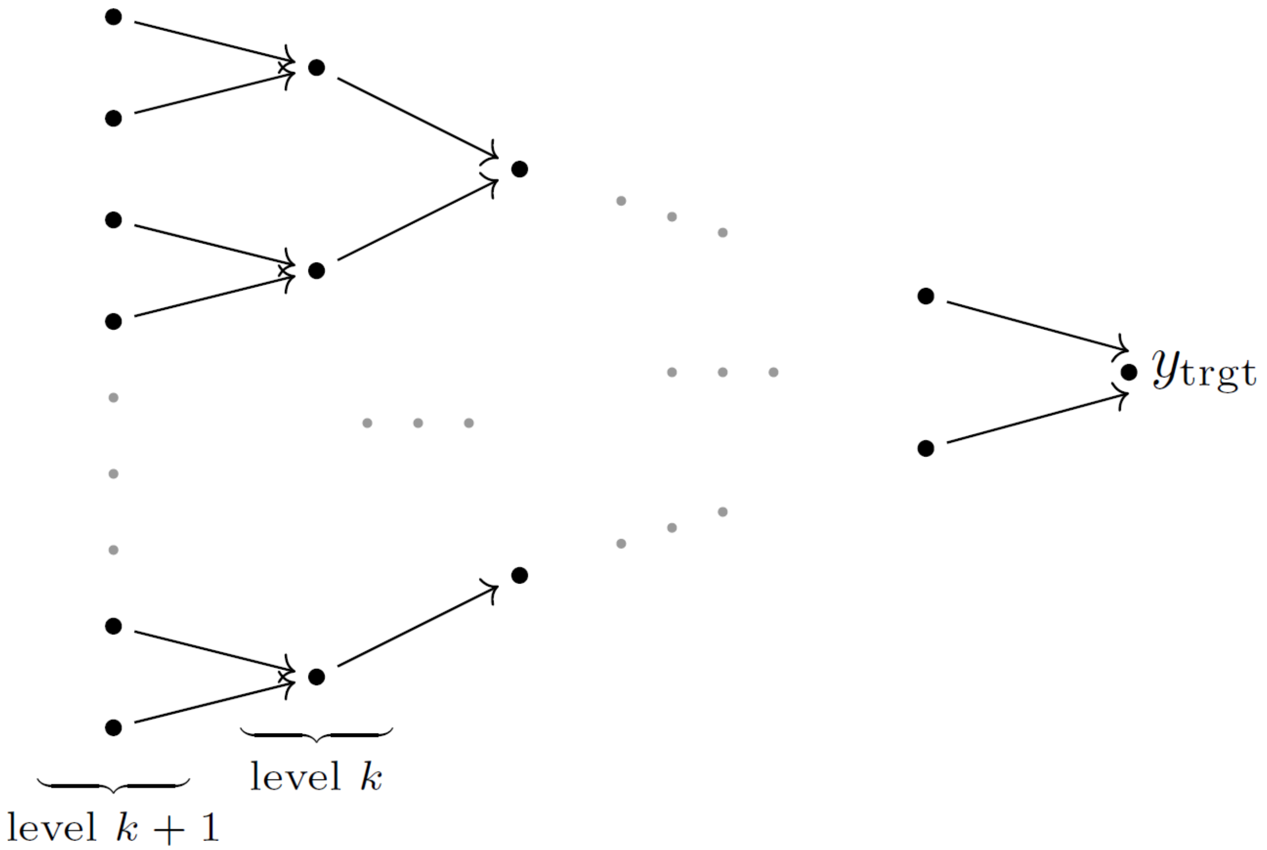
How to derive a Lower Bound for $(\mathcal{A}_1, \mathcal{A}_2)$?

	Classical [KK06]	Naïve **[our work]**	Enhanced **[our work]**
$\mathcal{A}_1$	$\mathcal{O}\left(\sqrt{k} \cdot 2^{\frac{n+k}{2}}\right)$	$\mathcal{O}(2^{\frac{n}{3}+k})$	$\mathcal{O}\left(\sqrt[3]{k} \cdot 2^{\frac{n+2k}{3}}\right)$ Doesn't matter, if k or k+1!
$\mathcal{A}_2$	$\mathcal{O}(2^{n-k})$	$\mathcal{O}\left(2^{\frac{n-k}{2}}\right)$	$\mathcal{O}\left(2^{\frac{n-k}{2}}\right)$
The Attack $(\mathcal{A}_1, \mathcal{A}_2)$	$\mathcal{O}\left(\sqrt{n} \cdot 2^{\frac{2n}{3}}\right)$	$\mathcal{O}\left(2^{\frac{4n}{9}}\right)$	$\mathcal{O}\left(\sqrt[3]{n} \cdot 2^{\frac{3n}{7}}\right)$

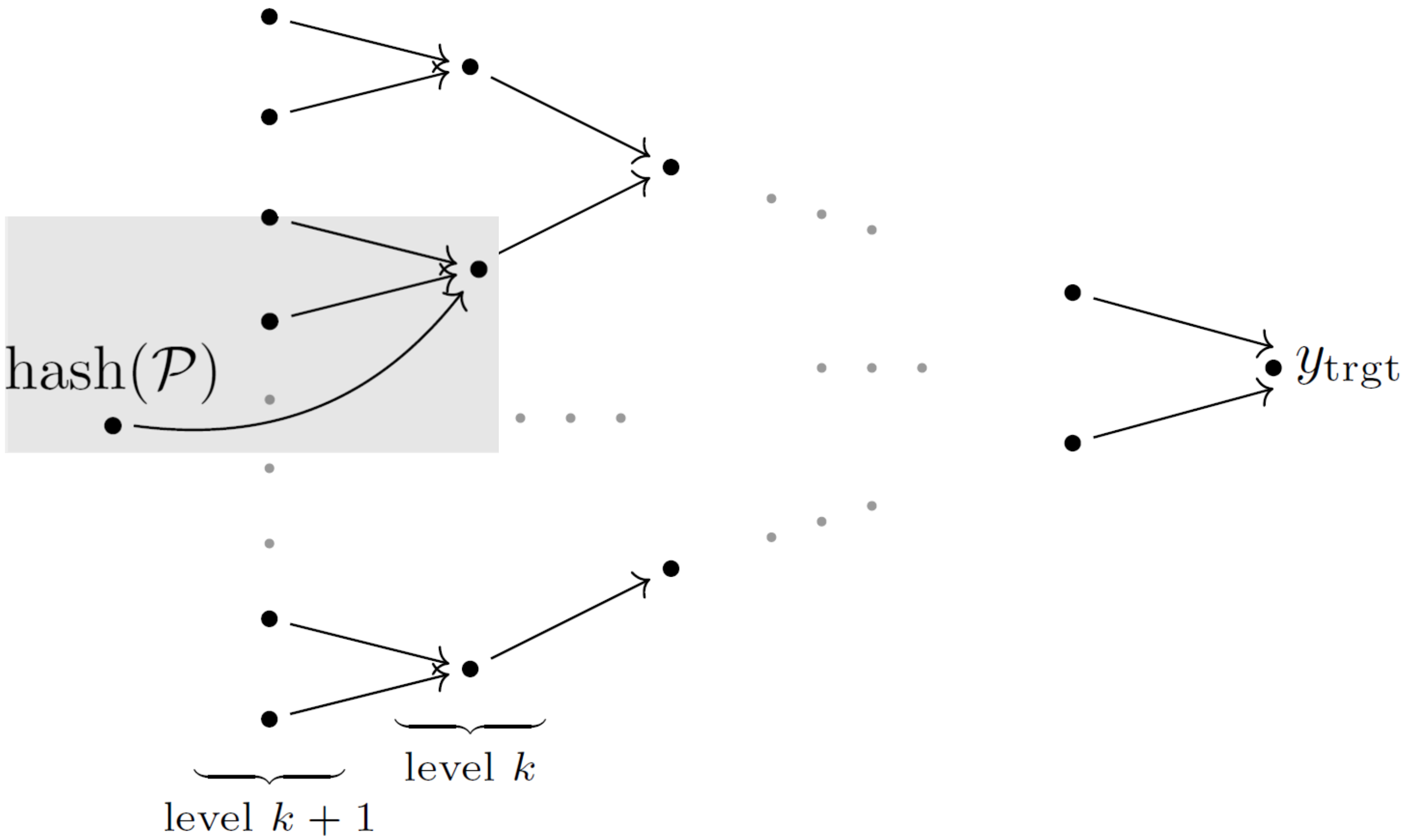
n = hash size
k = diamond height

[KK06] Kelsey and Kohno. Herding Hash Functions and the Nostradamus Attack. Advances in Cryptology - EUROCRYPT 2006.

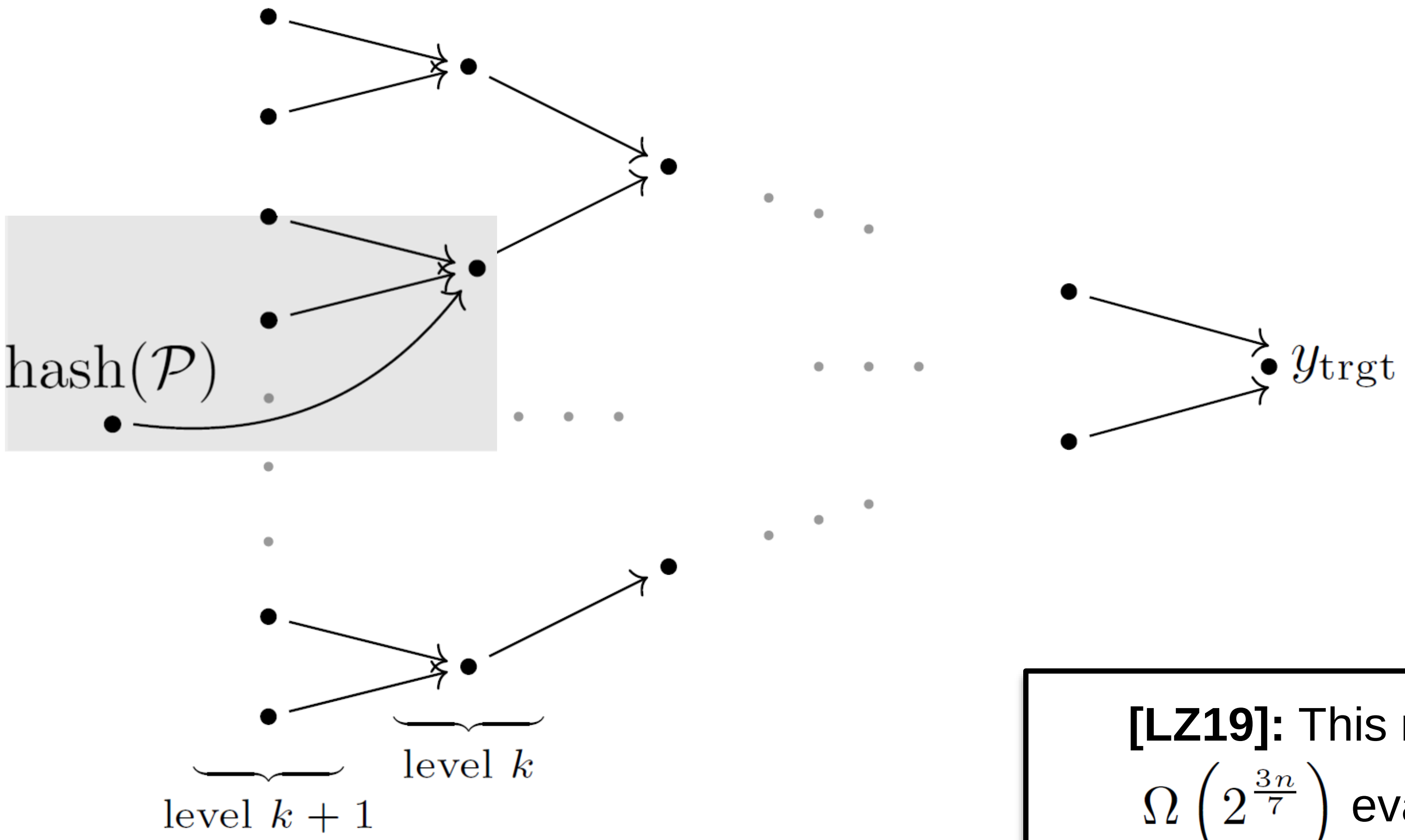
How to derive a Lower Bound for $(\mathcal{A}_1, \mathcal{A}_2)$?



How to derive a Lower Bound for $(\mathcal{A}_1, \mathcal{A}_2)$?



How to derive a Lower Bound for $(\mathcal{A}_1, \mathcal{A}_2)$?



[LZ19]: This needs at least $\Omega\left(2^{\frac{3n}{7}}\right)$ evaluations of h.

[LZ19] Liu and Zhandry. On Finding Quantum Multi-Collisions. Advances in Cryptology – EUROCRYPT 2019.

General Lower Bound

General Lower Bound

Theorem [our work]. Any Nostradamus Attacker $\mathcal{A}$ needs at least

$$\Omega\left(2^{\frac{3n}{7}-s}\right)$$

evaluations of h, where s is the maximal block length of suffix $\mathcal{S}$.

To Sum Up:

- *Quantum Nostradamus Attack*, which needs $\mathcal{O}\left(\sqrt[3]{n} \cdot 2^{\frac{3n}{7}}\right)$ h-evaluations
- There are *Lower Bounds*:
  - $\Omega\left(2^{\frac{3n}{7}}\right)$ with Diamond Structure
  - $\Omega\left(2^{\frac{3n}{7}-s}\right)$ in General

To Sum Up:

- *Quantum Nostradamus Attack*, which needs $\mathcal{O}\left(\sqrt[3]{n} \cdot 2^{\frac{3n}{7}}\right)$ h-evaluations
- There are *Lower Bounds*:
  - $\Omega\left(2^{\frac{3n}{7}}\right)$ with Diamond Structure
  - $\Omega\left(2^{\frac{3n}{7}-s}\right)$ in General

Thanks for the Attention!

Our full version: eprint.iacr.org/2022/1213
Our Qiskit-Experiments: git.rwth-aachen.de/marc.fischlin/quantum-nostradamus