Nostradamus Goes Quantum

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
The Modern Nostradamus [KK06]

The Modern Nostradamus [KK06]

The Modern Nostradamus [KK06]

The lottery numbers of the 10th of Dec are 4 11 ____ xxxx0404dd

The Modern Nostradamus [KK06]

The lottery numbers of the 10th of Dec are 4 11 _____ xxxx0404dd

* hash value of an iterated hash function


[1] www.lotto.de
History of Nostradamus-Attacker

Legendary Nostradamus

requires magic

Classical Nostradamus

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


History of Nostradamus-Attacker

- **Legendary Nostradamus**: requires magic
- **Classical Nostradamus [KK06, BSU12]**: $O\left(\sqrt{n} \cdot 2^{\frac{2n}{3}}\right)$
- **Quantum Nostradamus [our work]**: $O\left(\sqrt[3]{n} \cdot 2^{\frac{3n}{7}}\right)$


History of Nostradamus-Attacker

**Legendary Nostradamus**
- Requires magic

**Classical Nostradamus [KK06, BSU12]**
- $O\left(\sqrt{n} \cdot 2^{\frac{2n}{3}}\right)$

**Quantum Nostradamus [our work]**
- $O\left(\frac{3}{7} \sqrt{n} \cdot 2^{\frac{3n}{7}}\right)$

Essentially optimal!


Preliminaries

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

\[ m_1 \rightarrow h \rightarrow m_2 \rightarrow h \rightarrow \cdots \rightarrow h \rightarrow \text{hash}(m_1m_2 \cdots m_l) \]
Preliminaries

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

\[
\text{hash}(m_1 m_2 \ldots m_l)
\]

* Results also applicable to SHA-2, SHA-3 or SHAKE.
The Formal Nostradamus-Attack

Nostradamus-Adversary \((A_1, A_2)\)

Challenger
The Formal Nostradamus-Attack
The Formal Nostradamus-Attack

**Nostradamus-Adversary** $(A_1, A_2)$

$A_1$ (state, $y_{trgt}$) → $y_{trgt}$ → Challenger

$A_2$
The Formal Nostradamus-Attack
The Formal Nostradamus-Attack

Nostradamus-Adversary \((A_1, A_2)\)

\[ A_1 \xrightarrow{(\text{state, } y_{\text{trgt}})} A_2 \]

Challenger

\[ P \leftarrow \$ \{0, 1\}^{\ell \cdot B} \]
The Formal Nostradamus-Attack

Nostradamus-Adversary $(A_1, A_2)$

- $A_1$ gets $(\text{state}, y_{\text{trgt}})$
- $A_2$ gets $(\text{state}, y_{\text{trgt}}, P)$

Challenger

- $y_{\text{trgt}}$ sent to $A_1$
- $P \leftarrow \$ \{0, 1\}^{\ell \cdot B}$

Prefix $P$
The Formal Nostradamus-Attack

Nostradamus-Adversary \((A_1, A_2)\)

- \(A_1\) (state, \(y_{\text{trgt}}\))
- \(A_2\) (state, \(y_{\text{trgt}}, \mathcal{P}\))

Challenger

- \(y_{\text{trgt}}\) → Prefix \(\mathcal{P}\) ← \(\mathcal{P} \leftarrow \{0, 1\}^{\ell\cdot B}\)
The Formal Nostradamus-Attack

Nostradamus-Adversary \((A_1, A_2)\):

- \(A_1\): \((\text{state}, y_{\text{trgt}})\)
- \(A_2\): \((\text{state}, y_{\text{trgt}}, \mathcal{P})\)

Challenger:

- \(\mathcal{P} \leftarrow \$ \{0, 1\}^\ell \cdot B\)

Prefix: \(\mathcal{P}\)

Suffix: \(s\)
The Formal Nostradamus-Attack

**Nostradamus-Adversary** \((A_1, A_2)\)

- \(A_1\) returns \((\text{state}, y_{\text{trgt}})\)
- \(A_2\) returns \((\text{state}, y_{\text{trgt}}, \mathcal{P})\)

**Challenger**

1. \(\mathcal{P} \leftarrow \$ \{0, 1\}^\ell \cdot B\)
2. \(\text{hash}(\mathcal{P} || S) = y_{\text{trgt}}\)
History of Nostradamus-Attacker

Legendary Nostradamus

requires magic

Classical Nostradamus

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

Quantum Nostradamus

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

Essentially optimal!


The First Phase

\[ y \quad m \quad h(m,y) \]
The First Phase

\[ y \\ m \Rightarrow h(m,y) \Rightarrow y_{\text{trgt}} \]
The Second Phase

\[ \text{hash}(P) \]
The Second Phase

\[ \text{hash}(\mathcal{P}) \xrightarrow{m_{\text{link}}} \ldots \xrightarrow{y_{\text{target}}} \]
The Second Phase
History of Nostradamus-Attacker

**Legendary Nostradamus**
- Requires magic

**Classical Nostradamus**
- $\mathcal{O}(\sqrt{n} \cdot 2^{2n/3})$

**Quantum Nostradamus**
- [our work]
- $\mathcal{O}(\sqrt[3]{n} \cdot 2^{3n/7})$
- Essentially optimal!

---


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 $O\left(\sqrt{p^{-1}}\right)$ “valuations” of message blocks, where $p := |M^*| \cdot 2^{-B}$.

**References**


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 $O\left(\sqrt{p^{-1}}\right)$ “valuations” of message blocks, where $p := |M^*| \cdot 2^{-B}$.

Check of Suitability

How to Apply Grover’s Algorithm

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

$\text{hash}(P) \xrightarrow{m_{\text{link}}} \cdots \xrightarrow{\cdots} \cdots \xrightarrow{y_{\text{trgt}}}$
How to Apply Grover’s Algorithm

Grover succeeds after $O\left(\sqrt{p^{-1}}\right)$ evaluations of $h$. 
How to Apply Grover’s Algorithm

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

Diamond height $\delta$
How to Apply Grover’s Algorithm

Grover succeeds after $O\left(\sqrt{p^{-1}}\right)$ evaluations of $h$. 
How to Apply Grover’s Algorithm

Grover succeeds after $\mathcal{O}(\sqrt{p^{-1}})$ evaluations of $h$. 
Naïve Approach [BHT98]

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

Grover succeeds after $O\left(\sqrt{p^{-1}}\right)$ evaluations of $h$. 
Naïve Approach [BHT98]

Naïve Approach [BHT98]


Grover succeeds after $O\left(\sqrt{p^{-1}}\right)$ evaluations of $h$. 
Naïve Approach [BHT98]

Problem: Needs a lot of evaluations for each pair!


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

Enhanced Approach

upper

lower

\[\ldots\]
Enhanced Approach

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

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

Advantage: Needs fewer evaluations on average for each pair!

Grover succeeds after $O\left(\sqrt{p^{-1}}\right)$ evaluations of $h$. 
<table>
<thead>
<tr>
<th></th>
<th>Classical [KK06]</th>
<th>Naïve [our work]</th>
<th>Enhanced [our work]</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_1$</td>
<td>$O\left(\sqrt{k} \cdot 2^{\frac{n+k}{2}}\right)$</td>
<td>$O\left(2^{\frac{n}{3}+k}\right)$</td>
<td>$O\left(\frac{3}{\sqrt{k}} \cdot 2^{\frac{n+2k}{3}}\right)$</td>
</tr>
<tr>
<td>$A_2$</td>
<td>$O\left(2^{n-k}\right)$</td>
<td>$O\left(2^{\frac{n-k}{2}}\right)$</td>
<td>$O\left(2^{\frac{n-k}{2}}\right)$</td>
</tr>
<tr>
<td>The Attack ($A_1, A_2$)</td>
<td>$O\left(\sqrt{n} \cdot 2^{\frac{2n}{3}}\right)$</td>
<td>$O\left(2^{\frac{4n}{9}}\right)$</td>
<td>$O\left(\frac{3}{\sqrt{n}} \cdot 2^{\frac{2n}{7}}\right)$</td>
</tr>
</tbody>
</table>

$n = \text{hash size} \quad k = \text{diamond height}$

<table>
<thead>
<tr>
<th></th>
<th>Classical [KK06]</th>
<th>Naïve [our work]</th>
<th>Enhanced [our work]</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_1$</td>
<td>$O\left(\sqrt{k} \cdot 2^{\frac{n+k}{2}}\right)$</td>
<td>$O\left(2^\frac{n}{3} + k\right)$</td>
<td>$O\left(\frac{3}{\sqrt{k}} \cdot 2^{\frac{n+2k}{3}}\right)$</td>
</tr>
<tr>
<td>$A_2$</td>
<td>$O(2^{n-k})$</td>
<td>$O\left(2^{\frac{n-k}{2}}\right)$</td>
<td>$O\left(2^{\frac{n-k}{2}}\right)$</td>
</tr>
<tr>
<td>The Attack ($A_1, A_2$)</td>
<td>$O\left(\sqrt{n} \cdot 2^{\frac{2n}{3}}\right)$</td>
<td>$O\left(2^{\frac{4n}{9}}\right)$</td>
<td>$O\left(\frac{3}{\sqrt{n}} \cdot 2^{\frac{2n}{7}}\right)$</td>
</tr>
</tbody>
</table>

Essentially optimal!

About Lower Bounds
Lower Bound of c-Collision Finder [LZ19]

**Theorem.** Given a random function \( f : X \rightarrow Y \) any quantum algorithm needs at least 
\[
\Omega \left( 2^{\frac{1}{2c-1}} \cdot \frac{n}{2} \right)
\]
evaluations of function \( f \) to find a \textbf{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.

How to derive a Lower Bound for \((A_1, A_2)\)?
## How to derive a Lower Bound for $(A_1, A_2)$?

<table>
<thead>
<tr>
<th></th>
<th>Classical [KK06]</th>
<th>Naïve [our work]</th>
<th>Enhanced [our work]</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_1$</td>
<td>$O\left(\sqrt{k} \cdot 2^{\frac{n+k}{2}}\right)$</td>
<td>$O\left(2^{\frac{n}{3}+k}\right)$</td>
<td>$O\left(\frac{3}{\sqrt{k}} \cdot 2^{\frac{n+2k}{3}}\right)$</td>
</tr>
<tr>
<td>$A_2$</td>
<td>$O\left(2^{n-k}\right)$</td>
<td>$O\left(2^{\frac{n-k}{2}}\right)$</td>
<td>$O\left(2^{\frac{2n-k}{2}}\right)$</td>
</tr>
<tr>
<td>The Attack ($A_1, A_2$)</td>
<td>$O\left(\sqrt{n} \cdot 2^{\frac{2n}{3}}\right)$</td>
<td>$O\left(2^{\frac{4n}{9}}\right)$</td>
<td>$O\left(\frac{3}{\sqrt{n}} \cdot 2^{\frac{2n}{7}}\right)$</td>
</tr>
</tbody>
</table>

$n = \text{hash size}$

$k = \text{diamond height}$

How to derive a Lower Bound for \((A_1, A_2)\)?

| \(A_1\) \n| Classical \([\text{KK06]}\) \n| Naïve \([\text{our work]}\) \n| Enhanced \([\text{our work]}\) \n| \(A_2\) \n| \(O(\sqrt{k} \cdot 2^{\frac{n+k}{2}})\) \n| \(O(2^{\frac{n}{3}} + k)\) \n| \(O\left(\frac{3}{k} \cdot 2^{\frac{n+2k}{3}}\right)\) \n| The Attack \((A_1, A_2)\) \n| \(O\left(\sqrt{n} \cdot 2^{\frac{2n}{3}}\right)\) \n| \(O\left(2^{\frac{4n}{9}}\right)\) \n| \(O\left(\frac{3}{n} \cdot 2^{\frac{2n}{7}}\right)\) \n

Doesn’t matter, if k or k+1!

n = hash size
k = diamond height
How to derive a Lower Bound for $(A_1, A_2)$?
How to derive a Lower Bound for \((A_1, A_2)\)?
How to derive a Lower Bound for \((\mathcal{A}_1, \mathcal{A}_2)\)?

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

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 $S$. 
To Sum Up:

- *Quantum Nostradamus Attack*, which needs $O\left(\sqrt[3]{n} \cdot 2^{\frac{3n}{7}}\right)$ 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 $\mathcal{O}\left(\sqrt[3]{n} \cdot 2^{3n/7}\right)$ h-evaluations

• There are *Lower Bounds*:
  
  • $\Omega\left(2^{3n/7}\right)$ with Diamond Structure
  
  • $\Omega\left(2^{3n/7 - s}\right)$ 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