Efficient Quantum Collision Search and Related Problems

André Schrottenloher, joint works with André Chailloux, Lorenzo Grassi and María Naya-Plasencia

Inria de Paris, SECRET

June 19, 2018

Outline

Cryptographic Context

Cryptography

Asymmetric

- No shared secret;
- Key exchange protocols, digital signature, public-key systems (RSA, ECC)...

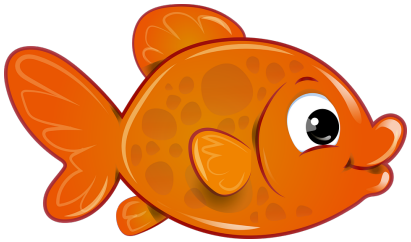
Symmetric

- Shared secret;
- Block ciphers, stream ciphers, hash functions...

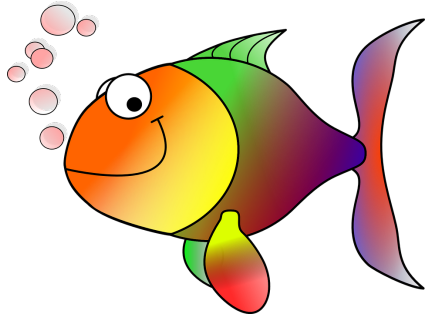
Symmetric cryptography

Alice and Bob share a secret key k and communicate with a block cipher $\mathrm{E}_k : \{0,1\}^n \to \{0,1\}^n$.

Typically $n = 128$.



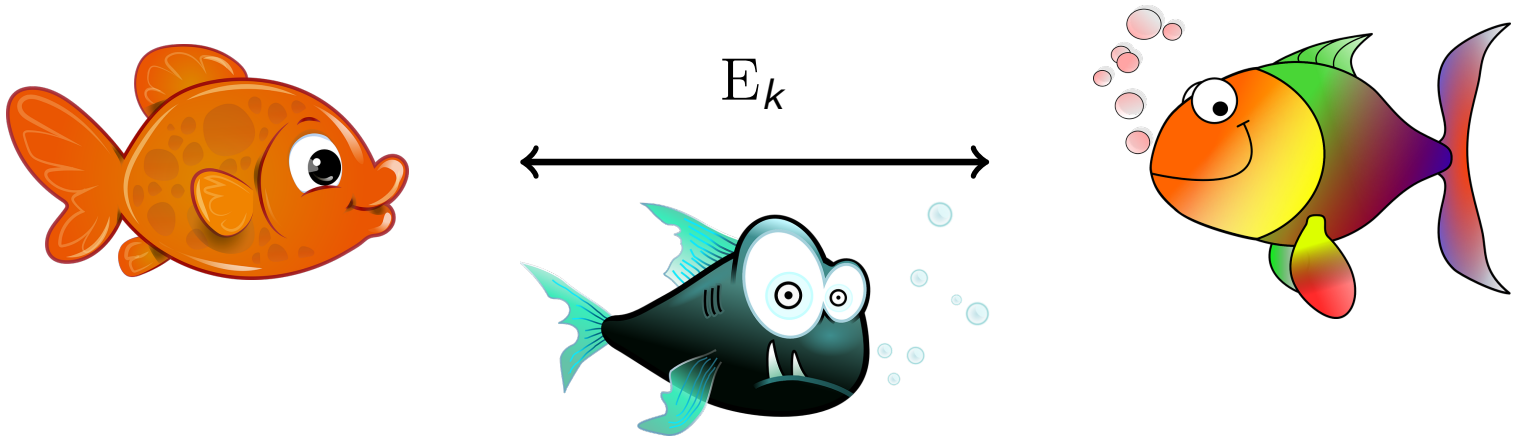
E_k



Symmetric cryptography

Alice and Bob share a secret key k and communicate with a block cipher $\mathrm{E}_k : \{0,1\}^n \to \{0,1\}^n$.

Typically $n = 128$.



An adversary attacks!

He wants to recover the key.

Generic attacks

An ideal cipher has its security defined by generic attacks.

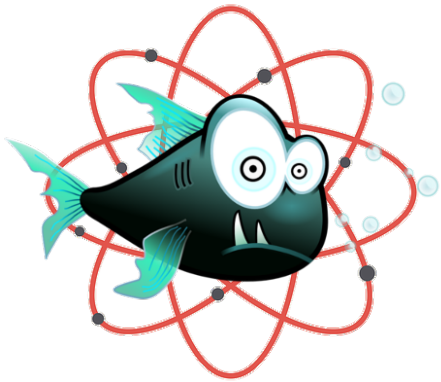
Example

- Generic key-recovery attack on $\mathrm{E}_k : \{0,1\}^n \to \{0,1\}^n$: given a few plaintext-ciphertext pairs, find k by exhaustive search. Costs $2^{|k|}$.
- $|k| = 128$: $2^{128} =$ approx. 10^{22} core-years.

Cryptanalysis

- The cipher is not ideal.
- The adversary tries very hard to find a better way of recovering the key.
- If there is a way, the cipher is broken.

A (wild) quantum adversary attacks!



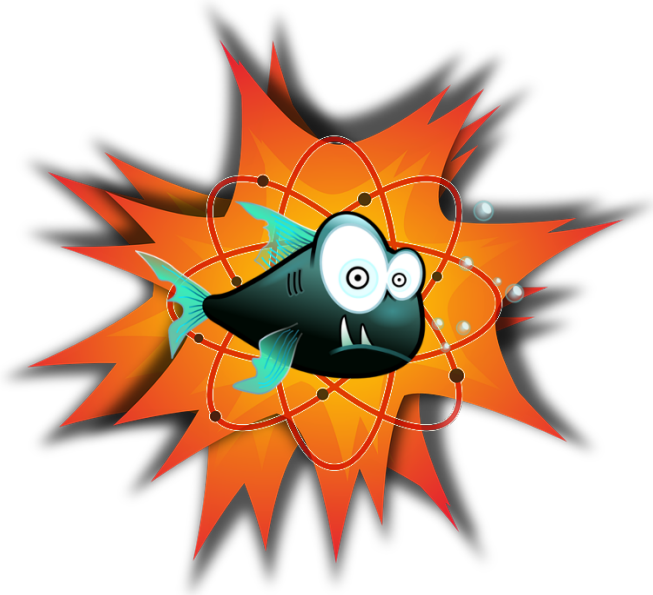
- He has a quantum computer.
- What happens?

Quantum principles

A quantum algorithm is a sequence of quantum gates applied to a pool of qubits. At each time step, the qubits are in a superposition of states (zeroes and ones).

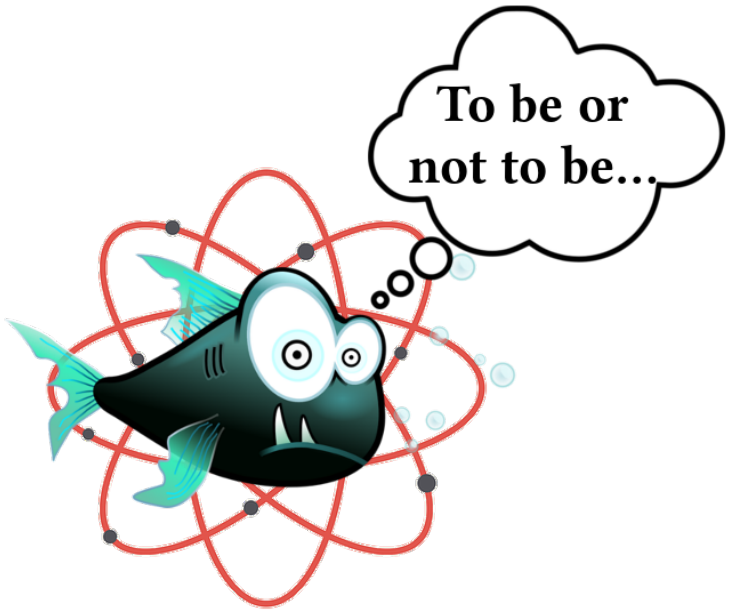
We are doomed

Since the computations are done in superposition, the quantum adversary can try all possibilities at once, hence breaking everything!



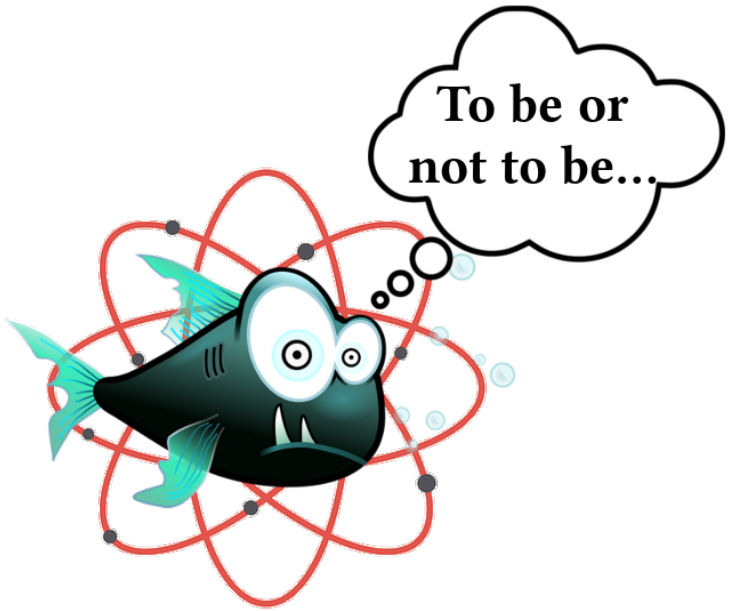
Entering the post-quantum era

Having broken all cryptography that ever existed, the adversary comes to reconsider his purpose in life.



Entering the post-quantum era

Having broken all cryptography that ever existed, the adversary comes to reconsider his purpose in life.



This is not true.

Entering (for real) the post-quantum era

- RSA (*factorization*) and ECC (*discrete logarithms*) become broken in polynomial time (Shor).
- We are looking for replacements (ongoing NIST call): codes, lattices, isogenies...

...but all of this concerns *asymmetric* cryptography...

In symmetric cryptography

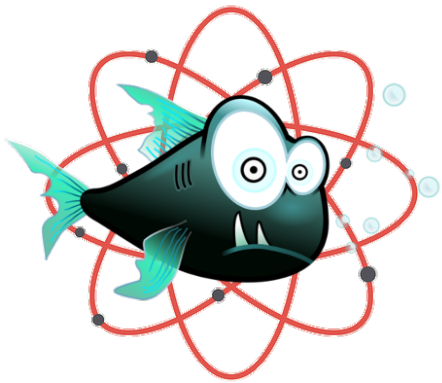
We know how to speed up some generic attacks.

Grover's algorithm

- $f : \{0,1\}^n \to \{0,1\}$ is a test function.
- We look for x such that $f(x) = 1$ (there are 2^t solutions).
- We implement f as a quantum circuit.
- With Grover: $O\left(2^{(n-t)/2}\right)$ calls to f instead of 2^{n-t} classically.

Quantum attacks on symmetric crypto

Quantum key-recovery on a block cipher:



- With $|k| = 128$: classically $2^{|k|} = 2^{128} = 10^{22}$ core-years;
- Quantumly $2^{|k|/2} = 2^{64} = 10^{3}$ core-years...

- Common belief: to reach the same security, "double the key size".
- Can we improve cryptanalysis?
- Can we improve other generic attacks?

Quantum Collision Search

Hash functions

A hash function $H : \{0,1\}^\star \to \{0,1\}^n$ behaves like a random function.

- If it does not, it is broken.
- Typically $n = 256$ or 512.

In this work: restriction to $H : \{0,1\}^n \to \{0,1\}^n$.

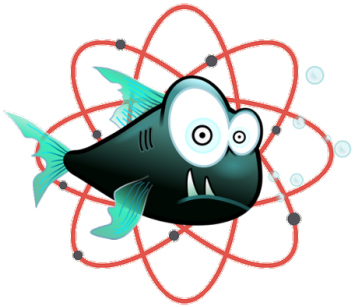
Classical collision search

Collision resistance

Finding a pair x, y with $H(x) = H(y)$ (a collision of H) takes time $O\left(2^{n/2}\right)$.

- Birthday paradox: among $2^{n/2}$ queries, there is a collision with constant probability ($2^{n/2}$ queries $\simeq 2^n$ pairs).
- Pollard's rho: $O\left(2^{n/2}\right)$ time and queries with $O(n)$ memory.
- This is a query lower bound.

Quantum collision search



The quantum adversary strikes again!
Doesn't he?

He implements $H : \{0,1\}^n \to \{0,1\}^n$ as a quantum circuit.

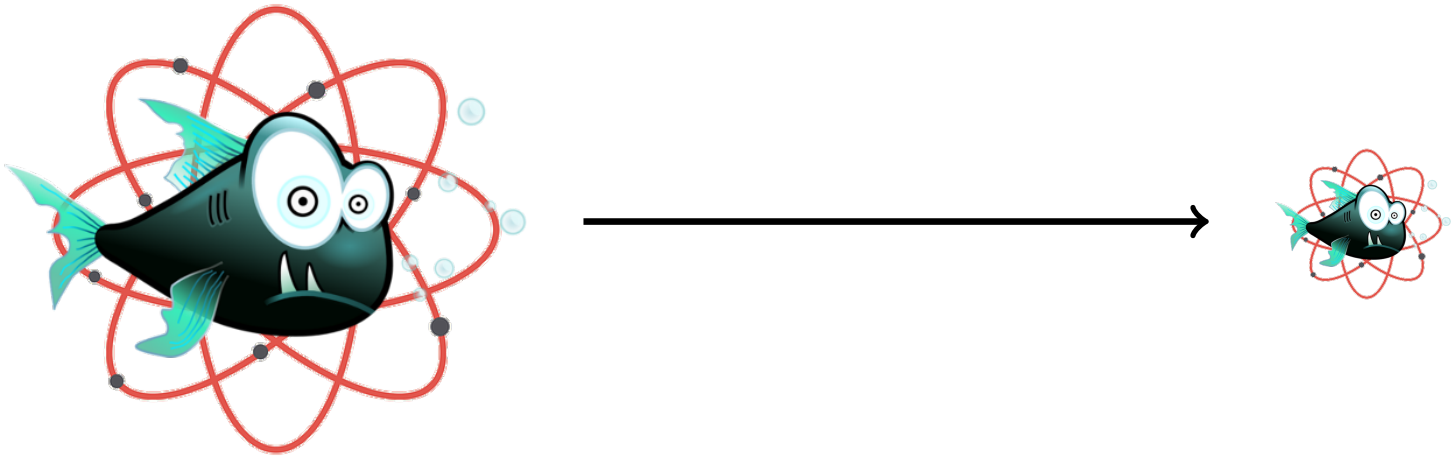
- Using Grover: $O(2^{n/2})$ time and queries...
- Brassard, Høyer and Tapp, 1998: $\widetilde{O}(2^{n/3})$ time, $O(2^{n/3})$ queries, and using $\widetilde{O}(2^{n/3})$ qubits.
- $\Omega(2^{n/3})$ is the quantum query lower bound.

Too many qubits is not "reasonable"

The quantum memory problem

Quantum computing seems even more difficult with too many qubits (Grover and Rudolph, 2004).

What happens if we reduce the number of qubits to $O(n)$?



Collision search with few qubits

The quantum query lower bound ($2^{n/3}$ instead of $2^{n/2}$) has been reached.

But...

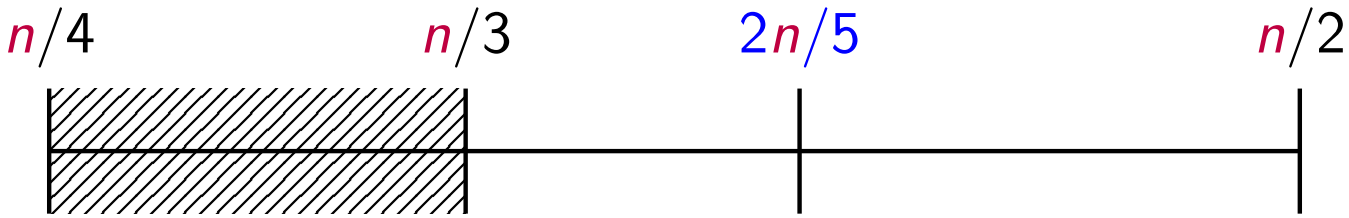
With $O(n)$ qubits, no quantum speedup for collision search!

Challenge (Grover and Rudolph, 2004)

Find an algorithm for collision [...] which gives a searching speedup greater than merely a square-root factor over the number of available processing qubits.

In what follows

	Time	Queries	Qubits	*Classical* memory
Grover	$O(2^{n/2})$	$O(2^{n/2})$	$O(n)$	0
BHT[a]	$O(2^{n/3})$	$O(2^{n/3})$	$O(2^{n/3})$	0
BHT variant	$O\left(2^{2n/3}\right)$	$O\left(2^{n/3}\right)$	$O(n)$	$O(2^{n/3})$
Our result[b]	$O(2^{2n/5})$	$O(2^{2n/5})$	$O(n)$	$O(2^{n/5})$



And more significant quantum speedups on other problems.

[a] Brassard, Høyer, and Tapp, 1998

[b] Chailloux, Naya-Plasencia, S., ASIACRYPT 2017

Efficient Quantum Collision Search

Generalizing Grover

Grover's algorithm

- Search space of size 2^n, 2^t solutions, an efficient test function;
- Time and queries $O\left(2^{(n-t)/2}\right)$ instead of 2^{n-t};
- Returns the superposition of all solutions.

Amplitude amplification (Brassard et al., 2002)

- Building the search space in time T_1;
- Testing in time T_2;
- 2^t solutions among 2^n;
- Time $O\left(2^{(n-t)/2}\left(T_1 + T_2\right)\right)$.

BHT algorithm (Brassard, Høyer, Tapp, 1998)

Classical:

- Perform ℓ arbitrary classical queries to H : $H(x_1), \ldots, H(x_\ell)$.
- Search $x \in \{0,1\}^n$ such that $H(x) \in \{H(x_1), \ldots, H(x_\ell)\}$.

Optimal $\ell = 2^{n/2}$:

$$2^{n/2} + \frac{2^n}{2^{n/2}}$$

BHT algorithm (Brassard, Høyer, Tapp, 1998)

Classical:

- Perform ℓ arbitrary classical queries to H : $H(x_1), \ldots, H(x_\ell)$.
- Search $x \in \{0,1\}^n$ such that $H(x) \in \{H(x_1), \ldots, H(x_\ell)\}$.

Optimal $\ell = 2^{n/2}$:

$$2^{n/2} + \frac{2^n}{2^{n/2}}$$

Quantum (BHT):

- Perform ℓ arbitrary classical queries to H : $H(x_1), \ldots, H(x_\ell)$.
- With Grover, search $x \in \{0,1\}^n$ such that $H(x) \in \{H(x_1), \ldots, H(x_\ell)\}$.

Optimal $\ell = 2^{n/3}$:

$$\underbrace{2^{\frac{n}{3}}}_{\text{Initial list}} + \underbrace{\sqrt{\frac{2^n}{2^{n/3}}}}_{2^{n/3} \text{ solutions among } 2^n}$$

BHT without quantum memory

Membership query:
We must test whether $H(x) \in \{H(x_1), \ldots, H(x_\ell)\}$.

With a quantum data structure:
This is done in $O(n)$.

Without:
There is a way... sequentially in time $O(\ell)$.

Queries:

$$2^{n/3} + \sqrt{2^n/2^{n/3}}\,(1+0)$$

Time:

$$2^{n/3} + 2^{n/3}\left(1 + 2^{n/3}\right)$$

BHT without quantum memory

Membership query:
We must test whether $H(x) \in \{H(x_1), \ldots, H(x_\ell)\}$.

With a quantum data structure:
This is done in $O(n)$.

Without:
There is a way... sequentially in time $O(\ell)$.

Queries:

$$2^{n/3} + \sqrt{2^n/2^{n/3}}(1+0)$$

Time:

$$2^{n/3} + 2^{n/3}\left(1 + 2^{n/3}\right)$$

Improving

$$\underbrace{2^{\frac{n}{3}}}_{\text{Initial list}} + \underbrace{2^{\frac{n}{3}}}_{2^{n/3} \text{ solutions among } 2^n} \left(\underbrace{1}_{\text{Querying } H} + \underbrace{2^{\frac{n}{3}}}_{\text{Membership}} \right)$$

Ideas

- Use the same method!
- Replace quantum memory by classical storage.
- Define distinguished points.

Step 1: distinguished points

Definition (Distinguished points)

All the x whose image starts with u zeroes.

- We generate a list of distinguished points.
- We are now searching only among the distinguished points (2^{n-u}) for the same number of solutions ($2^{n/3}$).

Total time:

$$\underbrace{\underbrace{2^{\frac{n}{3}}}_{\text{List size}} \times \underbrace{2^{\frac{u}{2}}}_{\substack{\text{Grover search} \\ \text{of a DP}}}}_{\text{First step: constructing the list}} + \underbrace{\underbrace{2^{\frac{n}{3}-\frac{u}{2}}}_{\text{Fewer queries}} \left(\underbrace{2^{\frac{u}{2}}}_{\substack{\text{Building} \\ \text{all the DPs}}} + \underbrace{2^{\frac{n}{3}}}_{\text{Membership}} \right)}_{\text{Second step: searching a collision}}$$

Step 2: optimize the list size

The list now contains 2^v distinguished points.

Total time:

$$\underbrace{\underbrace{2^v}_{\text{List size}} \times \underbrace{2^{\frac{u}{2}}}_{\substack{\text{Grover search} \\ \text{of a DP}}}}_{\text{First step: constructing the list}} + \underbrace{\underbrace{2^{\frac{n-v-u}{2}}}_{\text{Fewer queries}} \left(\underbrace{2^{\frac{u}{2}}}_{\substack{\text{Building} \\ \text{all the DPs}}} + \underbrace{2^v}_{\text{Membership}} \right)}_{\text{Second step: searching a collision}}$$

Balancing the computing time

Total time:

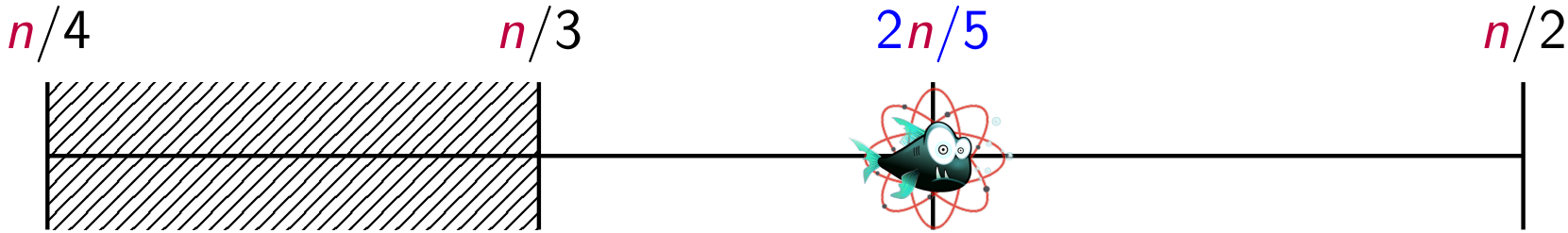
$$\underbrace{\underbrace{2^{v}}_{\text{List size}} \times \underbrace{2^{\frac{u}{2}}}_{\text{Grover search of a DP}}}_{\text{First step: constructing the list}} + \underbrace{\underbrace{2^{\frac{n-v-u}{2}}}_{\text{Fewer queries}} \left(\underbrace{2^{\frac{u}{2}}}_{\text{Building all the DPs}} + \underbrace{2^{v}}_{\text{Membership}} \right)}_{\text{Second step: searching a collision}}$$

Optimized as:

- $v = \frac{n}{5}, u = \frac{2n}{5}$;
- Time: $\widetilde{O}(2^{2n/5})$;
- Qubits: $O(n)$ (running Grover instances);
- *Classical* memory: $2^{n/5}$.

Consequences

We trade quantum memory for classical storage.



n	C. time	Q. time	*Classical* memory
128	2^{64}	$2^{51.2}$	$2^{25.6} \leq 1GB$
160	2^{80}	2^{64}	$2^{32} \leq 86GB$
256	2^{128}	$2^{102.4}$	$2^{51.2} \leq 83PB$

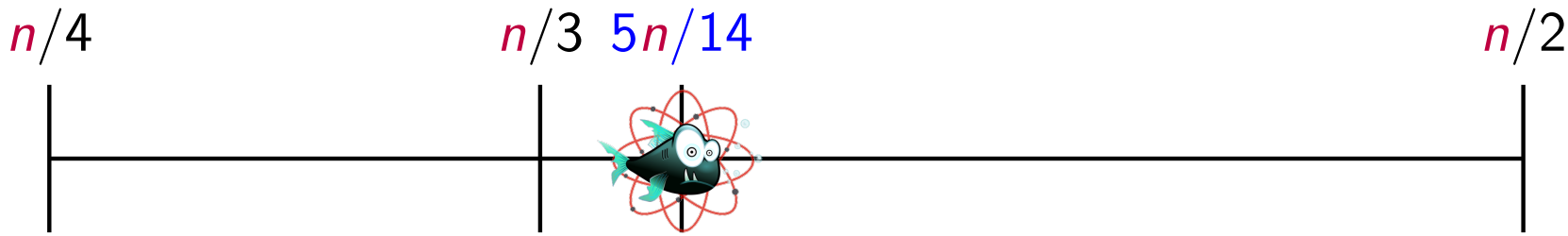
More recent results

Further low-qubits results

3-xor problem

Find x, y, z such that $H(x) \oplus H(y) \oplus H(z) = 0$.

- Classically (up to log factors) it is as hard as collision search ($O(2^{n/2})$).
- Now $O(2^{5n/14})$ quantum time and $O(2^{n/7})$ classical memory.[c]



Also available for multicollision search, 5-xor, 6-xor, 7-xor.
Parallelization speedups are better than Grover.[d]

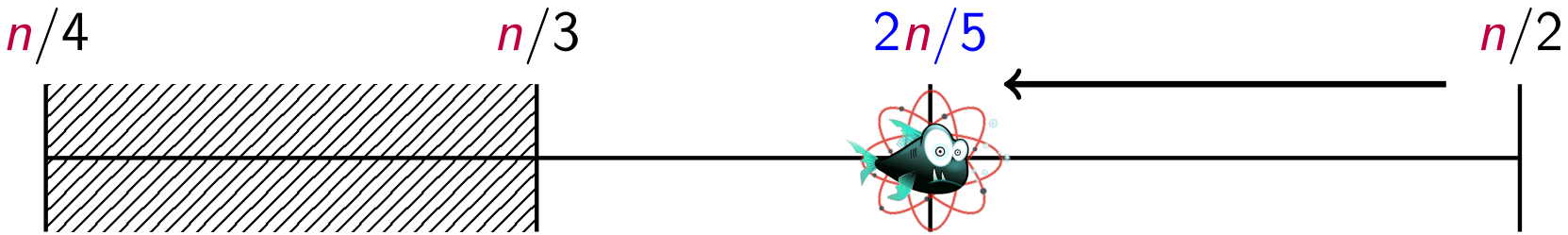
[c] Joint work with Lorenzo Grassi and María Naya-Plasencia, under submission.

[d] Work under submission.

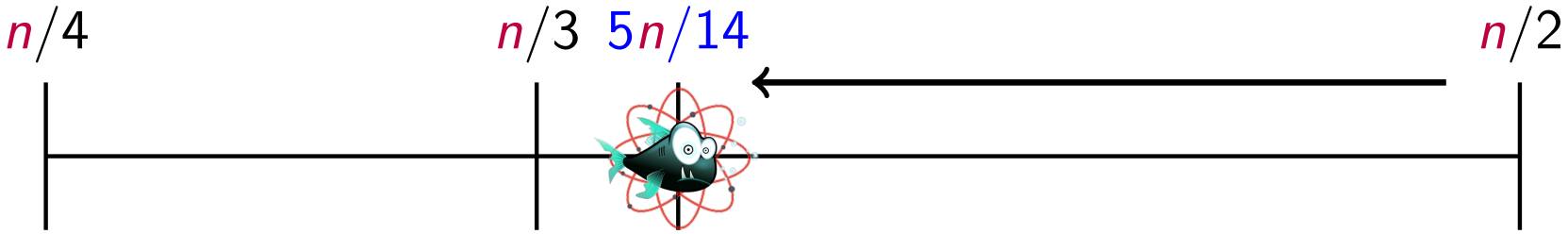
Conclusion

Conclusion

- Quantum collision search speedup with few qubits:



- Problems such as 3-xor behave even better:



- Many applications in cryptanalysis.
- Doubling the key size is not enough: one should also have a look at the state sizes.
- Can we bring the complexity down to the optimal?

Thank you.