Quantum Cryptanalysis of AES

Xavier Bonnetain, María Naya-Plasencia, André Schrottenloher

Inria de Paris, SECRET

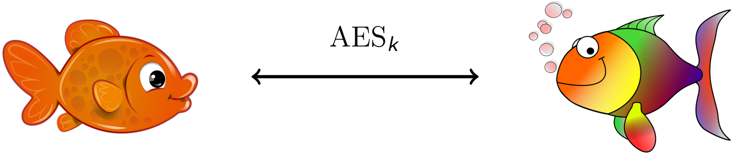
October 8, 2018

Outline

Cryptographic Context

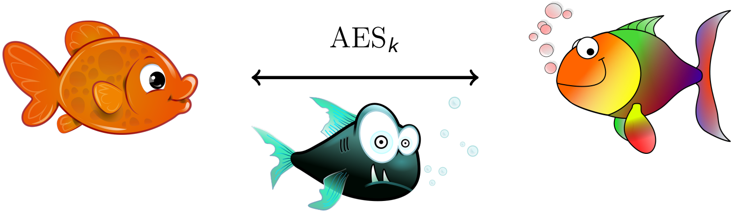
Our situation (symmetric)

Alice and Bob share a secret key k and communicate with a block cipher $\mathrm{AES}_k : \{0,1\}^n \to \{0,1\}^n$, $n = 128$.



Our situation (symmetric)

Alice and Bob share a secret key k and communicate with a block cipher $\mathrm{AES}_k : \{0,1\}^n \to \{0,1\}^n$, $n = 128$.



An adversary attacks!

He wants to recover the key.

Key-recovery attack on a block cipher

Generic (ideal cipher)

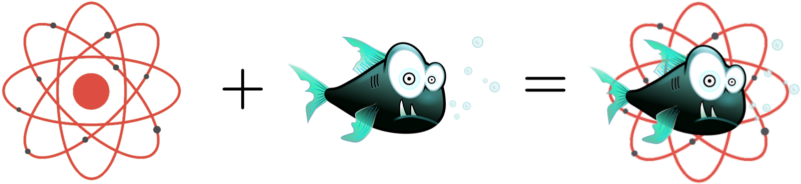
…try all keys!

Exhaustive search of k: costs $2^{|k|}$.

Cryptanalysis

- How to trust a cipher?
- If an attack is found, the cipher is **broken**!
- We try to **attack the highest number of rounds**.

The adversary becomes quantum



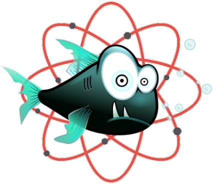
Grover's algorithm

- $f\ : \{0,1\}^n \rightarrow \{0,1\}$ 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 key-recovery attack on a block cipher

Generic (ideal cipher)

… Grover all keys!
Exhaustive quantum search of k: costs $2^{|k|/2}$.



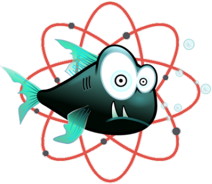
- Common security measure: double the key size.

Quantum key-recovery attack on a block cipher

Generic (ideal cipher)

. . . Grover all keys!

Exhaustive quantum search of k: costs $2^{|k|/2}$.



- Common security measure: double the key size.

Cryptanalysis

What about quantum cryptanalysis?

The AES

Blocks are 128 bits, divided in 4 × 4 bytes.

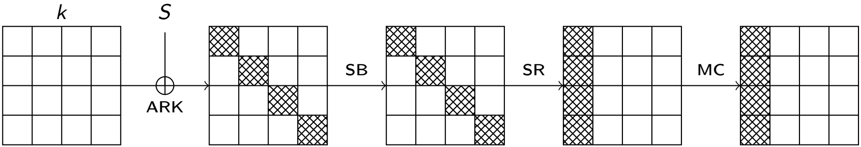
AES round function

AddRoundKey (ARK): XOR the round key;

SubBytes (SB): Apply the AES S-Box to each byte;

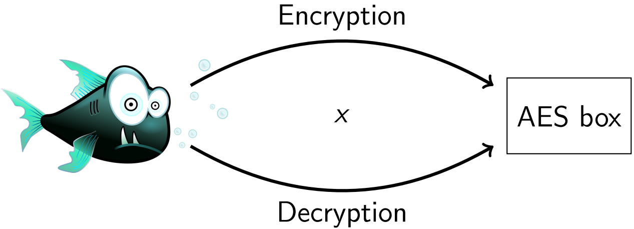
ShiftRows (SR): Shift the i-th row by i bytes left;

MixColumns (MC): Multiply each column by the AES MDS matrix.



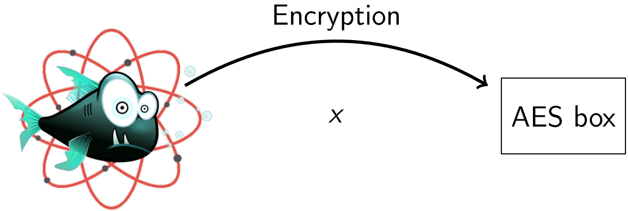
Classical cryptanalysis of AES (secret-key)

The adversary accesses an encryption and a decryption black-box and tries to guess the key.



Our quantum attacks

The adversary accesses classically an encryption black-box.



Our Results

We found quantum attacks on reduced-rounds AES: key-recovery below Grover's exhaustive search.

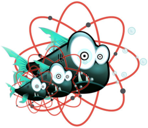
	Classical		Quantum	
Version	Rounds attacked	Method	Rounds attacked	Method
AES-128	7	ID or DS-MITM	6	Square
AES-192	8	DS-MITM	7	Square
AES-256	9	DS-MITM	8	DS-MITM

How to (Simply) Write a Quantum Attack

Correspondence principle

Classical exhaustive search ⇔ Quantum exhaustive search

Nested exhaustive search ⇔ Nested quantum exhaustive search

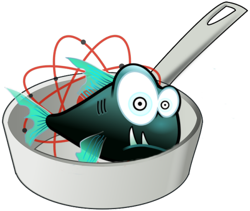


Example: find $x \in S_1$ such that P_1 (prob. p_1, cost cc_1) **and** (there exists $y \in S_2$ such that P_2 (prob. p_2, cost cc_2)).

$$\underbrace{\frac{1}{p_1}}_{\text{Outer search}} \left(\underbrace{\frac{1}{p_2}}_{\text{Inner search}} cc_2 + cc_1 \right) \qquad \underbrace{\frac{1}{\sqrt{p_1}}}_{\text{Outer search}} \left(\underbrace{\frac{1}{\sqrt{p_2}}}_{\text{Inner search}} cc_2 + cc_1 \right)$$

A quantum attack recipe

1. Write a search / nested search procedure
2. Compute the classical complexity (depending on success probabilities)
3. Replace all success probabilities by their square roots
4. You are (almost) done!



Grover's "soufflé" property

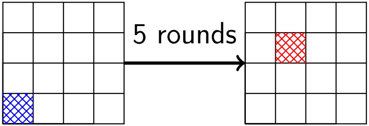
We get closer to the solutions. . . until we start moving away from it!

- The size of the solution space should be know at runtime (otherwise, the soufflé strikes back).
- This is not always the case with Grovers within Grovers. . .

Quantum DS-MITM attack on 8-round AES-256

The middle rounds

If a 🟦 → 🟥 differential is ensured, encryption of some differences in 🟦 produces a specific result in 🟥 .



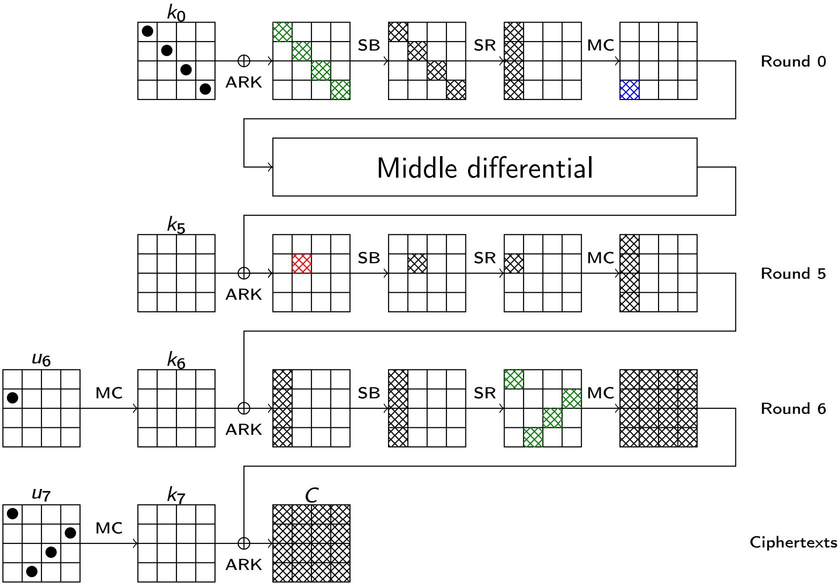
Input difference (any byte)

Output difference (any byte)

Main Property

If we make the difference in 🟦 take some arbitrary values (δ-sequence) and collect the sequence of output differences in 🟥 , there are only 2^{192} (24 byte-conditions) possibilities.

The classical attack tabulates the middle rounds. . . we don't.


k_0
ARK
SB
SR
MC
Round 0
Middle differential
k_5
ARK
SB
SR
MC
Round 5
u_6
MC
k_6
ARK
SB
SR
MC
Round 6
u_7
MC
k_7
ARK
C
Ciphertexts

Attack layout

1. Query the AES black-box and find enough (2^{48}) input-output pairs satisfying the 🟩 conditions
2. First search level: 10 key bytes

Testing a guess of key bytes

- Find a pair which gives 🟦 → 🟥
- Using some queries, compute the output sequence in 🟥
- Check the middle property: find if the sequence in 🟥 is possible

A classical attack

The number of "degrees of freedom" to search through:

$$\underbrace{10}_{\text{Key bytes}} + \underbrace{24}_{\text{Middle state bytes}} - \underbrace{4}_{\text{Key schedule relations}} = 30$$

- A middle-rounds encryption of a sequence is approx. 5 times an AES encryption
- We have $2^{30\times 8} = 2^{240}$ such sequences to evaluate
- Only $2^{250.3}$ S-Boxes against $2^{263.8}$ for exhaustive search
- Now for a quantum attack: "take the square root"

Working out the details

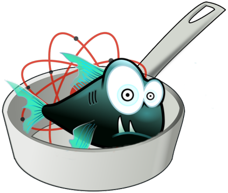
- We need 3 Grover levels: uncomputation factors;
- Grover's soufflé strikes back: S-Box differential equations give some errors.

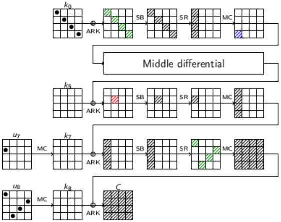
- We lose some bits but still win: $2^{136.3}$ S-Boxes against Grover's $2^{137.45}$.

Conclusion

Conclusion

- We analyzed existing attacks and found some quantum ones (Square, DS-MITM)
- We wrote our attacks in a unifying framework
- We showed how to quantumly exploit the S-Box
- We reached an 8-round attack on AES-256
- We found new trade-offs for classical DS-MITM attacks (9 rounds of AES-256 in data 2^{113}, time 2^{210} and memory 2^{194}).





Thank you.