From: Doge Protocol <dogeprotocol1@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] New quantum algorithm proposing polynomial time attack on AES, too good to be real?
Date: Sunday, July 24, 2022 11:55:27 AM ET

Came accross this paper today and wanted to bring to attention of this community.

Can community verify the claims in the paper? If substantiated, this is a big development.

https://eprint.iacr.org/2022/948

Snippet from abstract:

We demonstrate how it can be used to search the keyspace of any block cipher that can be implemented on a quantum computer with the keyspace in superpositon. In particular we give a polynomial time attack on AES−128, AES−192 and AES−256. --

From: Tony Arcieri <bascule@gmail.com> via pqc-forum@list.nist.gov
To: Doge Protocol <dogeprotocol1@gmail.com>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] New quantum algorithm proposing polynomial time attack on AES, too good to be real?
Date: Sunday, July 24, 2022 12:00:45 PM ET

I've seen a number of criticisms of this paper, and ePrint has withdrawn it.
One criticism, if I understand correctly, is that it relies on an oracle which outputs if two bits of the key are correct, which if it existed could also break AES classically.

On Sun, Jul 24, 2022 at 9:54 AM Doge Protocol <dogeprotocol1@gmail.com> wrote:

> Came accross this paper today and wanted to bring to attention of this community.
>
> Can community verify the claims in the paper? If substantiated, this is a big development.
>
> https://eprint.iacr.org/2022/948
>
> Snippet from abstract:
>
> We demonstrate how it can be used to search the keyspace of any block cipher that can be implemented on a quantum computer with the keyspace in superpositon. In particular we give a polynomial time attack on AES−128, AES−192 and AES−256. --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/aa3c189e-8263-44dd-ae83-4fae718ba599n%40list.nist.gov.

--
Tony Arcieri

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CAHOTMVJwjE8Af2C6rfixmZAb4LA9w%3Dw4iGL%3Dsjv39Jz_tEDEdw%40mail.gmail.com.

From: Xavier Bonnetain <xavier.bonnetain@inria.fr> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] New quantum algorithm proposing polynomial time attack on AES, too good to be real?
Date: Sunday, July 24, 2022 12:44:05 PM ET

Hi all,

Indeed, the algorithm is flawed. Here's a quick summary of what the algorithm does and where the issue is.

The algorithm begins but doing many grover searches in the key space with the predicate "Does the encryption of M with K matches the expected encryption on bits (2i,2i+1)?"

Assuming the proportion of keys that fulfill this property is exactly 1/4, we obtain, in 1 grover iteration, the exact quantum superposition of all matching keys.

Now, the idea is that the correct key is the only one that appears in all the superpositions. The Hadamard product allows to get the interstection of 2 quantum superpositions.

Thus, by iterating Hadamard products, we can recover the key.

There are 2 main problems:

- in the algorithm, computing a Hadamard product is not efficient, here it would be exponential.

- The claimed result is not possible: this algorithm would efficiently break any block cipher (and probably, beyond that, almost all cryptography) in black box. This violates lower bounds on the quantum security of the ideal cipher.

To summarize, any attack, classical or quantum, against AES (or any cipher), must, at some point, leverage a specific property of the cipher. This is not the case here.

Cheers,

Xavier

> **De:** "Tony Arcieri" <bascule@gmail.com>
> **À:** "Doge Protocol" <dogeprotocol1@gmail.com>

Cc: "pqc-forum" <pqc-forum@list.nist.gov>
Envoyé: Dimanche 24 Juillet 2022 18:00:21
Objet: Re: [pqc-forum] New quantum algorithm proposing polynomial time attack on AES, too good to be real?

I've seen a number of criticisms of this paper, and ePrint has withdrawn it.
One criticism, if I understand correctly, is that it relies on an oracle which outputs if two bits of the key are correct, which if it existed could also break AES classically.

On Sun, Jul 24, 2022 at 9:54 AM Doge Protocol <dogeprotocol1@gmail.com> wrote:

> Came accross this paper today and wanted to bring to attention of this community.
>
> Can community verify the claims in the paper? If substantiated, this is a big development.
>
> https://eprint.iacr.org/2022/948
>
> Snippet from abstract:
>
> We demonstrate how it can be used to search the keyspace of any block cipher that can be implemented on a quantum computer with the keyspace in superpositon. In particular we give a polynomial time attack on AES−128, AES−192 and AES−256.
>
> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/aa3c189e-8263-44dd-ae83-4fae718ba599n%40list.nist.gov.

--
Tony Arcieri

> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CAHOTMVJwjE8Af2C6rfixmZAb4LA9w%3Dw4iGL%3Dsjv39Jz_tEDEdw%40mail.gmail.com.