Superposition Meet-in-the-Middle Attacks: Updates on Fundamental Security of AES-like Ciphers Review

Josh Barber

Department of Physics and Computer Science

CP614: Applied Cryptography

Dr. Angèle Foley

April 17th, 2023

Superposition Meet-in-the-Middle Attacks: Updates on Fundamental Security of AES-like Ciphers Review

These are exciting times being in the digital age, where quantum computing is on the horizon. Quantum computing recently has proven to complete NP-complete problems in polynomial time (Traversa et al., 2015). This is groundbreaking on the technological front. Solving an NP-complete problem only means we can solve problems that were not solvable before. This could revolutionize scientific sectors and find discoveries that have never been discovered before. When it comes to climate, agriculture and business, quantum computing technology will positively impact us. Quantum computing will surely offer huge benefits and advancements in technology, however with great means of positive change also gives the potential to do the exact opposite.

In recent years from 2021 to 2022, cyberattacks have increased by 38% with education/research, government and healthcare being the primary targets. With the introduction of ChatGPT, it may only accelerate the number of cyberattacks in 2023 (Check Point Research, 2023). Cyberattacks could potentially disable the economy of a city, state, or our entire country and United States and Canada are shockingly unprepared for these types of devastating attacks (Cybersecurity Ventures, 2016). The amount of damages from cyberattacks is forecasted to be around $8 trillion USD alone for 2023, with an annual growth of damages of around 15 percent over the next two years (Cybersecurity Ventures, 2021). Cybersecurity is arguably behind conventional standards already, and with the introduction of quantum computing it may have a devastating impact on government sectors and companies that are unprepared. The World Economic Forum says that the action in preparing for cybersecurity on quantum computing attacks must be now as there is a risk of ‘harvest now, decrypt later’ attacks (World Economic Forum, 2022).

Since 2003, the United States government announced that AES could be used to protect classified information, and since then AES has become the default encryption algorithm approved by the NSA. Ever since 2003, it has been the most widely used symmetric key cryptographic algorithm (TechTarget, 2021). The task for the AES cryptographic algorithm to uphold attacks from quantum computing cyberattacks seems daunting. One of the most powerful cyptanalysis attacks for symmetric keys is the Meet-in-the-Middle (MITM) attack. The attacker divides the encryption process into two parts, an initial encryption phase and a decryption phase. The attacker then generates a table of all possible keys for the encryption phase and another table of all possible keys for the decryption phase. The attacker then matches the two tables to find the matching keys that generate the same output. If the AES encryption key size is 128 bits, the attacker must perform 2^{128} computations to successfully perform a MITM, which is not feasible with current classical computing resources.

Bao, Guo, and Shi introduce a new concept of a MITM attack on AES like hash functions called "superposition meet-in-the-middle" attack. This technique builds on previous meet-in-the-middle attacks, which involves finding two inputs that hash to the same output which is known as a “collision.” It is done so using superposition from quantum mechanics. As a side note, superposition in computer science is based on a fundamental concept in quantum mechanics, which allows quantum systems to be in multiple states or positions simultaneously. The superposition MITM attack involves superimposing multiple inputs or states to create a single output, which can then be used to find collisions more efficiently. Collisions in cryptography occur when two different inputs produce the same output value in a hash function mainly because of a fixed size. Creating a collision of hashes in this case confirms a correct key.

The attack involves three steps:

1. Precomputation: In this step, the attacker generates a large number of intermediate values by encrypting a set of plaintexts using the encryption algorithm being attacked. The attacker then stores these intermediate values in a lookup table.
2. Superposition: In this step, the attacker uses a quantum computer to create a superposition of all possible keys and plaintexts. This is done by applying a Hadamard transform to each qubit in the key and plaintext registers.
3. Meet-in-the-middle: In this step, the attacker performs a brute-force search on the superposition to find a matching pair of keys and plaintexts. The attacker uses the lookup table generated in the precomputation step to quickly determine whether a given intermediate value matches a key and plaintext pair.

The superposition MITM attack can reduce the time complexity of a regular meet-in-the-middle attack on an AES encryption key size of 128 bits, from 2^{128} computations to 2^{64}

computations. While this is still a substantial number of computations, it is within the range of feasibility for current and future quantum computers.

It should be noted that the superposition MITM attacks on AES-like hashing functions are not applicable to all the types of AES-like hash functions. This is because the superposition MITM attack relies on specific properties of the hash function. Some hash functions use a simple, iterative compression function that cannot be represented as a combination of multiple rounds. Furthermore, the effectiveness of the superposition MITM attack also depends on the number of rounds in the compression function and the size of the message blocks. Hash functions with larger message blocks and more rounds in the compression function would be less vulnerable to these attacks, as they increase the complexity of the attack and make it more difficult to find a collision.

With superposition MITM attacks exposing many AES-like hash functions, allowed the authors to propose a new security notion called "strong superposition resistance" (SSR). This measure assesses a hash function's resistance to the superposition meet-in-the-middle attack. The authors prove that if a hash function is SSR-secure, then it is also secure against other known attacks (Bao et al., 2022). A proposed method to enforce SSR-secure compliancy is a lattice-based cryptography, which involves problems related to the shortest vector problem, which is believed to be hard for quantum computers to solve (Micciancio & Regev, 2008).

Although the quantum threat is still looming over AES-like hash functions, NIST is still finding candidates to the next successor of the AES cryptography encryption algorithm that would be preventative to post-quantum cyberattacks. There is a list of candidates that focus on lattice-based cryptography. Some of the known candidates of the lattice-based cryptography scheme are NTRU, Kyber, Saber, and NewHope. There are other variants using different cryptography schemes, but there is a high probability a lattice-based cryptography scheme will be the new standard (NIST, 2022). While going through the candidate process, it is a race against time as quantum computing will eventually become mainstream within 10-20 years from now. In the meantime, it is proven that AES 256-bit key is resistant enough to fight off quantum attacks that are using brute force, which is exactly what the superposition MITM attack is. To successfully brute force the AES-like hash function with 256-bit key, it would require a quantum computer with a qubit size of 6,600, whereas the largest quantum computer right now only has 1,121 qubits, created by IBM (Fierce Electronics, 2022). Regardless of the AES resistance, it is imperative to understand that the AES-like hash functions are not going to hold secure for much longer, unless it is upgraded to uphold strong superposition resistance standards. Hopefully, the candidate selection process will be concluded before the quantum computing technology has caught up. In the meantime, increasing the AES key size or making the AES-like hash function SSR compliant, may be the only solutions for the time being.

References

Bao, Z., Guo, J., Shi, D., & Tu, Y. (2022, October 12). Superposition meet-in-the-middle attacks: Updates on fundamental security of AES-like hashing. SpringerLink. Retrieved April 17, 2023, from https://link.springer.com/chapter/10.1007/978-3-031-15802-5_3

Micciancio, D., & Regev, O. (2008, July 22). Lattice-based cryptography - New York University. Retrieved April 17, 2023, from https://cims.nyu.edu/~regev/papers/pqc.pdf

Traversa, F. L., Ramella, C., Bonani, F., & Di Ventra, M. (2015, July 3). Memcomputing NP-complete problems in polynomial time using polynomial resources and collective states. Science Advances. Retrieved April 17, 2023, from https://www.science.org/doi/10.1126/sciadv.1500031

Fierce Electronics. (2022, January 11). AES-256 joins quantum resistance. Fierce Electronics. https://www.fierceelectronics.com/electronics/aes-256-joins-quantum-resistance

Check Point Research. (2023, January 5). 38% increase in 2022 global cyberattacks. Check Point Software Technologies Ltd. https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/

Cybersecurity Ventures. (2021, November 9). Cybercrime to cost the world $8 trillion annually in 2023. Cybersecurity Ventures. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

Cybersecurity Ventures. (2016, May 29). Hackerpocalypse: A cybercrime report. Cybersecurity Ventures. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Science Magazine. (2015, November 6). Quantum computing. Science. https://www.science.org/doi/10.1126/sciadv.1500031

TechTarget. (2021, September). Advanced Encryption Standard (AES). TechTarget. Retrieved April 17, 2023, from https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard

World Economic Forum. (2022, September 26). Organizations must prepare for quantum computing threat to cybersecurity now. World Economic Forum. https://www.weforum.org/agenda/2022/09/organizations-protect-quantum-computing-threat-cybersecurity/

National Institute of Standards and Technology. (2022). Post-Quantum Cryptography Standardization - Round 3 Submissions. Retrieved April 17, 2023, from https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions