Quantum Symmetric-key Cryptanalysis: An Overview

Tianyu Zhang

Cryptanalysis Taskforce
Nanyang Technological University, Singapore

SGCRYPT 2026

Outline

Symmetric-key (SK) Cryptography

Examples:

- Block ciphers (e.g., AES)
- Hash functions (e.g., SHA-2, SHA-3, Whirlpool)
- Modes of operation (e.g., GCM)

These primitives can be further composed to build other SK constructions, for instance OWFs, MACs, AEADs, PRFs, PRGs, etc.

Symmetric-key (SK) Cryptography

Examples:

- Block ciphers (e.g., AES)
- Hash functions (e.g., SHA-2, SHA-3, Whirlpool)
- Modes of operation (e.g., GCM)

These primitives can be further composed to build other SK constructions, for instance OWFs, MACs, AEADs, PRFs, PRGs, etc.

- Core building blocks of cryptographic protocols and systems
- Security relies on *cryptanalysis*, rather than reduction to hardness assumptions

Generic v.s. Dedicated Attacks

Generic attack (or generic bound)

- defines the ideal security of a SK primitive
- e.g. for hash function with n-bit output, in the classical setting, generic preimage attack costs $O(2^n)$, generic collision attack costs $O(2^{n/2})$

Generic v.s. Dedicated Attacks

Generic attack (or generic bound)

- defines the ideal security of a SK primitive
- e.g. for hash function with n-bit output, in the classical setting, generic preimage attack costs $O(2^n)$, generic collision attack costs $O(2^{n/2})$

Dedicated attack (or simply attack)

- exploits structural weaknesses of a specific primitive to find an attack better than the generic attack on reduced/full rounds
- known cryptanalytic techniques: differential, linear, meet-in-the-middle, rebound, etc.

Generic v.s. Dedicated Attacks

Generic attack (or generic bound)

- defines the ideal security of a SK primitive
- e.g. for hash function with n-bit output, in the classical setting, generic preimage attack costs $O(2^n)$, generic collision attack costs $O(2^{n/2})$

Dedicated attack (or simply attack)

- exploits structural weaknesses of a specific primitive to find an attack better than the generic attack on reduced/full rounds
- known cryptanalytic techniques: differential, linear, meet-in-the-middle, rebound, etc.

Security margin

$$1 - \frac{\text{Number of rounds attacked}}{\text{Number of full rounds}}$$

Quantum Implications on SK Cryptanalysis

1. Generic attacks are accelerated by quantum algorithms
   - e.g., Grover's algorithm gives quadratic speed-up for brute-force key recovery on block ciphers $\Rightarrow$ double key sizes to maintain same security levels for PQ use

Quantum Implications on SK Cryptanalysis

1. Generic attacks are accelerated by quantum algorithms
   - e.g., Grover's algorithm gives quadratic speed-up for brute-force key recovery on block ciphers $\Rightarrow$ double key sizes to maintain same security levels for PQ use
2. Quantum adversary may better exploit structural weaknesses of SK primitives, lead to more powerful dedicated quantum attacks than the classic ones

Quantum Implications on SK Cryptanalysis

1. Generic attacks are accelerated by quantum algorithms
    - e.g., Grover's algorithm gives quadratic speed-up for brute-force key recovery on block ciphers $\Rightarrow$ double key sizes to maintain same security levels for PQ use
2. Quantum adversary may better exploit structural weaknesses of SK primitives, lead to more powerful dedicated quantum attacks than the classic ones
3. Different assumptions on quantum capabilities lead to different analysis

Quantum Implications on SK Cryptanalysis

1. Generic attacks are accelerated by quantum algorithms
   - e.g., Grover's algorithm gives quadratic speed-up for brute-force key recovery on block ciphers $\Rightarrow$ double key sizes to maintain same security levels for PQ use
2. Quantum adversary may better exploit structural weaknesses of SK primitives, lead to more powerful dedicated quantum attacks than the classic ones
3. Different assumptions on quantum capabilities lead to different analysis

These observations motivates comprehensive quantum cryptanalysis of deployed SK primitives to evaluate their concrete security margins in the PQ era

Quantum Implications on SK Cryptanalysis

1. Generic attacks are accelerated by quantum algorithms
   - e.g., Grover's algorithm gives quadratic speed-up for brute-force key recovery on block ciphers $\Rightarrow$ double key sizes to maintain same security levels for PQ use
2. Quantum adversary may better exploit structural weaknesses of SK primitives, lead to more powerful dedicated quantum attacks than the classic ones
3. Different assumptions on quantum capabilities lead to different analysis

These observations motivates comprehensive quantum cryptanalysis of deployed SK primitives to evaluate their concrete security margins in the PQ era

In this talk, we will briefly introduce:

- Commonly used adversary modes in quantum SK cryptanalysis
- Simon's algorithm and its applications on Modes of Operations
- Grover's algorithm and its application on Hash Functions

Outline

Quantum Adversary Models

In quantum SK cryptanalysis, we usually consider two axes of assumptions:

Query access to cryptographic oracles: (keyed oracles are more concerned)

- **Model Q0**: classical queries to oracle, classical computation
- **Model Q1**: classical queries to oracle, access to a quantum computer
- **Model Q2**: superposition queries to oracle
- **Model Q3**: superposition related-key queries to oracle overly strong and mostly impractical

Quantum Adversary Models

In quantum SK cryptanalysis, we usually consider two axes of assumptions:

Query access to cryptographic oracles: (keyed oracles are more concerned)

- **Model Q0**: classical queries to oracle, classical computation
- **Model Q1**: classical queries to oracle, access to a quantum computer
- **Model Q2**: superposition queries to oracle
- **Model Q3**: superposition related-key queries to oracle overly strong and mostly impractical

Existence of qRAM:

- **Model QA**: No qRAM, consider quantum time-space trade-offs
- **Model QB**: No qRAM, consider quantum time complexity, with only polynomial-sized quantum computer, may use classical memory for storage
- **Model QC**: Arbitrary qRAM, consider quantum time complexity

Outline

Simon's Algorithm

Simon's Problem

Given oracle access to a function $f : \{0,1\}^n \to \{0,1\}^m$ such that

$$f(x) = f(x \oplus s)$$

for a secret $s \neq 0$, recover s.

- Classical query complexity: $O(2^{n/2})$
- Quantum query complexity [Sim94]: $O(n)$
- Requires **Q2 model**: superposition oracle access
- Core idea: Each query of the Simon's algorithm recovers one linear relation on s. $O(n)$ queries to recover full s.

Impact on SK Modes and Constructions

Simon's algorithm enables **polynomial-time** key-recovery attacks on many modes and constructions in the Q2 model:

- On Modes of Operation [KLLN16, Bon17]:
  - MACs: CBC–MAC, PMAC, GMAC
  - AEAD: GCM, OCB
  - Many CAESAR candidates (e.g., AEZ, CLOC, COPA, OTR)
- On Constructions:
  - 3–round Feistel [KM10]
  - Even–Mansour [KM12]
  - FX construction [LM17]

Impact on SK Modes and Constructions

Simon's algorithm enables **polynomial-time** key-recovery attacks on many modes and constructions in the Q2 model:

- On Modes of Operation [KLLN16, Bon17]:
  - MACs: CBC–MAC, PMAC, GMAC
  - AEAD: GCM, OCB
  - Many CAESAR candidates (e.g., AEZ, CLOC, COPA, OTR)
- On Constructions:
  - 3–round Feistel [KM10]
  - Even–Mansour [KM12]
  - FX construction [LM17]

Remarks:

- Q2 attacks assumes the adversary has quantum access to the keyed primitives.
- Need to be extra careful when implementing those primitives on quantum computers.

Outline

Grover's Algorithm

Unstructured Search

Given oracle access to $f : \{0,1\}^n \to \{0,1\}$, find x such that $f(x) = 1$.

- Classical complexity: $O(2^n)$
- Quantum complexity: $O(2^{n/2})$ [Gro96]
- Key generalization: Quantum Amplitude Amplification (QAA) [BHMT02]
- Quadratic speed-up for brute-force key recovery for block ciphers and preimage search for hash functions, i.e., from $O(2^n)$ to $O(2^{n/2})$.
- How about collision search?

Application to Quantum Collision Search

Collision Search

Given a random function $H : \{0,1\}^n \to \{0,1\}^n$, find $x \neq y$ such that $H(x) = H(y)$.

- Best classical attack: Parallel Collision Search (PCS) [OW99]
  - Time complexity: $O(2^{n/2}/S)$ with S processors;
  - Time-space complexity: $O(2^{n/2})$
- Quantum Parallel Collision Search (QPCS) [Ber09]
  - Quantum time-space complexity $O(2^{n/2})$
  - Current best attack in terms of quantum time-space trade-offs
- How about in terms of time complexity?

Comparison of Quantum Generic Collision Attacks

	Time	Queries	Qubits	cMem	qRAM
QPCS	$2^{n/2}$	$2^{n/2}$	$\mathrm{poly}(n)$	/	/
BHT	$2^{n/3}$	$2^{n/3}$	/	/	$2^{n/3}$
CNS	$2^{2n/5}$	$2^{2n/5}$	$\mathrm{poly}(n)$	$2^{n/5}$	/

Generic bounds under different quantum adversary models:

- BHT algorithm achieve the lowest time complexity, but with exponential qRAM
- CNS algorithm is the best attack under the (*realistic*) assumption of polynomial qubits and no qRAM

Application 1: Differential-based Attacks

Differential Probability

Let $F : \{0,1\}^n \to \{0,1\}^n$ be a function. The **differential probability** of a pair of input/output differences $(\Delta_{in}, \Delta_{out})$ is

$$\Pr_{x \leftarrow \{0,1\}^n}\left[F(x) \oplus F(x \oplus \Delta_{in}) = \Delta_{out}\right].$$

A differential trail with probability p defines the cost of finding a valid pair

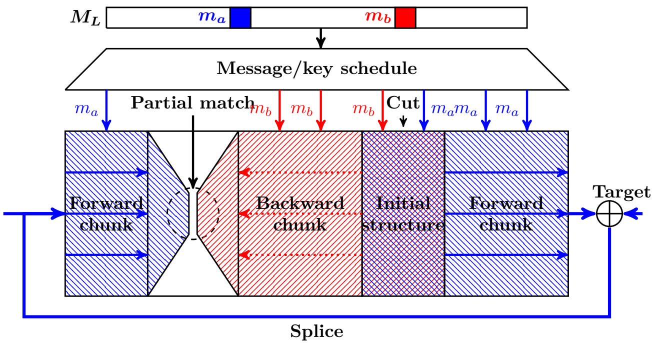
- **Classical setting:** Requires $\approx 1/p$ evaluations
- **Quantum setting:** QAA finds a valid pair in time $\approx \sqrt{1/p}$
  $\Rightarrow$ able to exploit differentials that are unusable in the classical setting!
- Enable quantum attacks on higher rounds than classical attacks!

Results on Classical/Quantum Collision Attacks

Attack	Rounds	Time	cMem	qRAM	Setting	Technique	Source
AES-128-MMO							
Collision	6	2^{56}	2^{32}	–	C	Rebound	[LMRRS09; GP10]
Collision	7	2^{60}	2^{60}	–	C	MITM	**Asiacrypt'25***
Chosen-prefix	5	2^{52}	2^{32}	–	C	Rebound, CPC	**FSE'25***
Collision	7	$2^{59.5}$	–	–	QA	Rebound, Grover	[HS20]
Collision	8	$2^{55.53}$	–	–	QA	Rebound, Grover, TA	**Crypto'22***
Chosen-prefix	6	$2^{61.5}$	–	–	QA	Rebound, Grover, CPC	**FSE'25***
Whirlpool							
Collision	5	2^{120}	2^{64}	–	C	Rebound	[GP10; LMRRS09]
Collision	6	2^{240}	2^{240}	–	C	MITM	**Eurocrypt'24***
Collision	6	2^{228}	–	–	QA	Rebound, QAA	[HS20]
Collision	6	$2^{201.4}$	–	–	QA/QB	Rebound, QAA	**FSE'25***
Chosen-prefix	6	$2^{205.4}$	–	–	QA	Rebound, QAA, CPC	**FSE'25***

* Results from CATF

Application 2: Quantum MITM Preimage Attacks



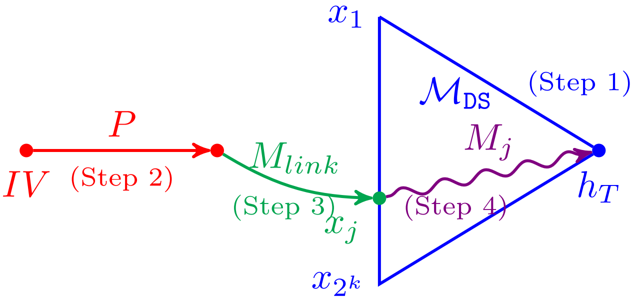
- Classical MITM Attacks: partition the function to two independently computable chunks, which meet in the middle and filtered by partial-match
- Quantum Variant: Nested Grover's search [SS22], storing one chunk into qRAM, and search for partial-matched candidates
- Need stronger conditions than classical attack!

Results on Classical/Quantum Preimage Attacks

Attack	Rounds	Time	cMem	qRAM	Setting	Technique	Source
AES-128-MMO							
Preimage	8/10	2^{120}	2^{32}	–	C	MITM	**Eurocrypt'21***
Preimage	7/10	2^{60}	–	2^{8}	QC	MITM, QAA	[SS23]
Preimage	7/10	2^{56}	–	2^{16}	QC	MITM, QAA	[DDS25]
AES-192-MMO							
Preimage	9/12	2^{112}	–	–	C	MITM	**Crypto'22***
Preimage	10/12	2^{124}	2^{124}	–	C	MITM	**Eurocrypt'24***
Preimage	9/12	2^{60}	–	2^{24}	QC	MITM, QAA	[DDS25]
AES-256-MMO							
Preimage	10/14	2^{120}	2^{56}	–	C	MITM	[DHS+21]
Preimage	9/14	2^{60}	–	2^{8}	QC	MITM, QAA	[DDS25]
Whirlpool							
Preimage	7/10	2^{480}	2^{128}	–	C	MITM	**Crypto'22***
Preimage	7.75/10	2^{480}	2^{256}	–	C	MITM	**Eurocrypt'24***
Preimage	6/10	2^{232}	–	2^{128}	QC	MITM, QAA	[DDS25]

* Results from CATF

Application 3: Quantum Nostradamus Attacks



- Nostradamus attack [KK06]: commit a hash value, then for any message given by the user, append a suffix to force the resulted message hash to the commitment
- Offline phase: builds a diamond structure
- Online phase: finds a link from initial hash value to any leaf of the diamond structure
- Both phases can be accelerated by quantum algorithms (offline: CNS/BHT, online: quantum MITM)

Results on Classical/Quantum Nostradamus Attacks

Attack	Rounds	Time	cMem	qRAM	Setting	Technique	Source
AES-128-MMO							
Nostradamus	6	$2^{82.7}$	$2^{82.2}$	–	C	MITM, Diamond	[ZSWH23]
Nostradamus	7	2^{83}	2^{82}	–	C	MITM, Diamond	**FSE'24***
Nostradamus	7	2^{58}	2^{30}	2^{8}	QC	MITM, Diamond, QAA	**FSE'24***
Whirlpool							
Nostradamus	4	2^{320}	2^{192}	–	C	MITM, Diamond	[ZSWH23]
Nostradamus	6	2^{334}	2^{333}	–	C	MITM, Diamond	**FSE'24***
Nostradamus	6	2^{230}	2^{117}	2^{24}	QC	MITM, Diamond, QAA	**FSE'24***

* Results from CATF

Thank You For Listening!

Questions?