Towards a better understanding of (post-)quantum security of symmetric key schemes

NTT Secure Platform Laboratories (and Nagoya University)

Akinori Hosoyamada

@ASK 2019 (2019.12.13)

Introduction

Quantum Attacks against Symmetric Cryptosystems?

It has been said that symmetric key schemes would not to be much affected by quantum computers

Known Quantum Attacks：～２０１０

NTT

	Classical	Quantum
Exhaustive Key Search	$O(2^n)$	$O(2^{n/2})$
Collision Finding	$O(2^{n/2})$	$O(2^{n/3})$

"2n-bit key suffices"

Known Quantum Attacks : Today

NTT

	Classical	Quantum
Exhaustive Key Search	$O(2^n)$	$O(2^{n/2})$
Collision Finding	$O(2^{n/2})$	$O(2^{n/3})$
Key Recovery on Even-Mansour	$O(2^{n/2})$	Polynomial time
Forgery against CBC-MAC	$O(2^{n/2})$	Polynomial time

Remark：The last two attacks assumes that quantum keyed oracles are available

Quantum Attacks against Symmetric Cryptosystems?

It has been said tha[illegible]metric key schemes
would not to be much [illegible] by quantum computers

Symmetric key schemes may be significantly affected !!

- Attacks by Kuwakado and Morii at ISIT2010, ISITA2012
- Attacks by Kaplan et al. at CRYPTO2016

Quantum Attacks against Symmetric Cryptosystems?

It has been said tha … mmetric key schemes
would not to be much … by quantum computers

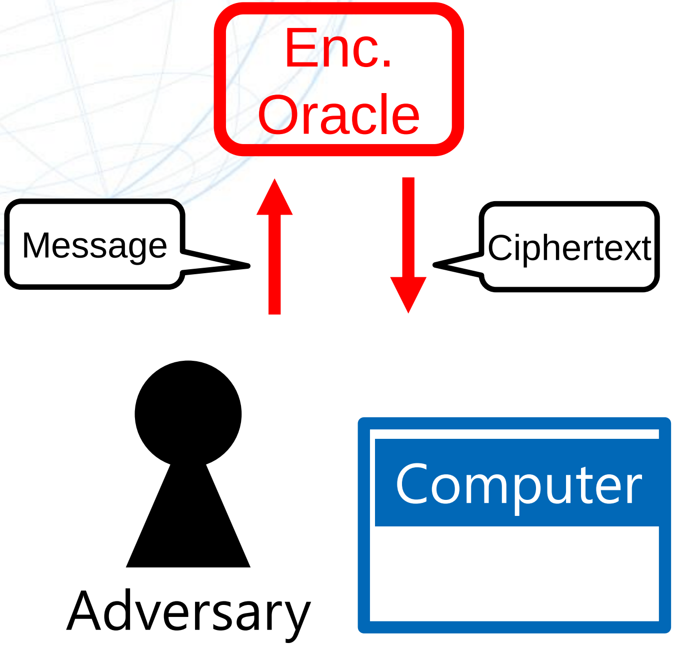
Symmetric key schemes may be significantly affected !!

- Attacks by Kuwakado and Morii at ISIT2010, ISITA2012
- Attacks by Kaplan et al. at CRYPTO2016

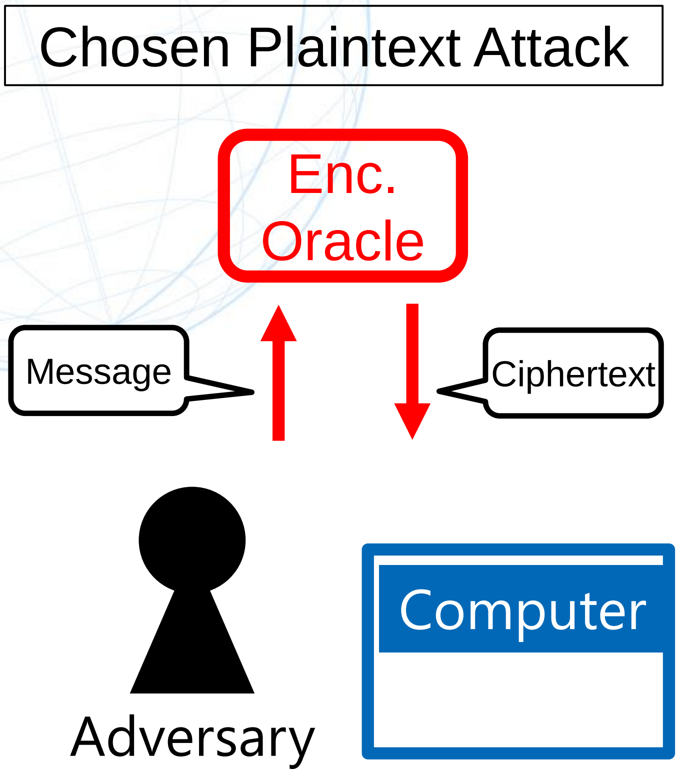
Post-quantum security of symmetric schemes should be analyzed more carefully

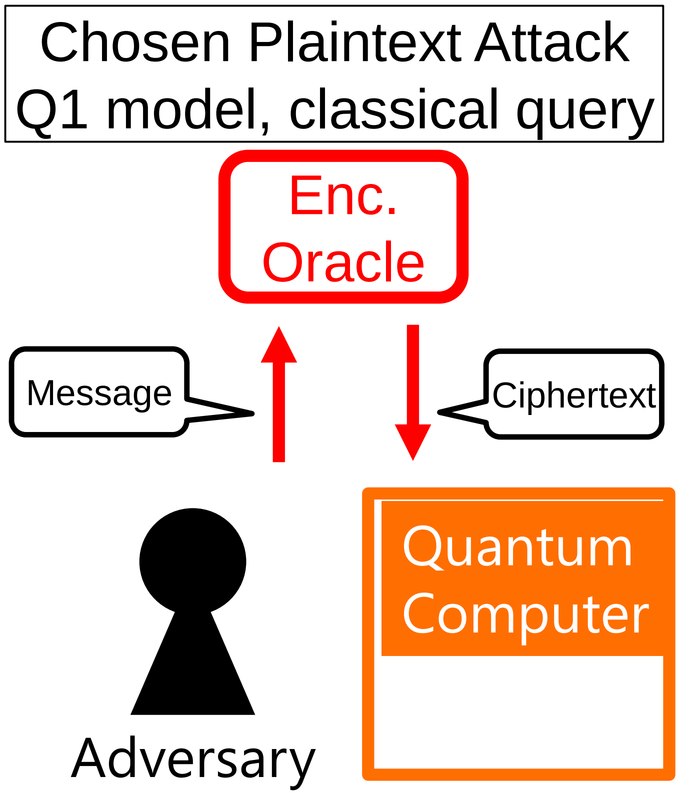
Attack Models

Chosen Plaintext Attack

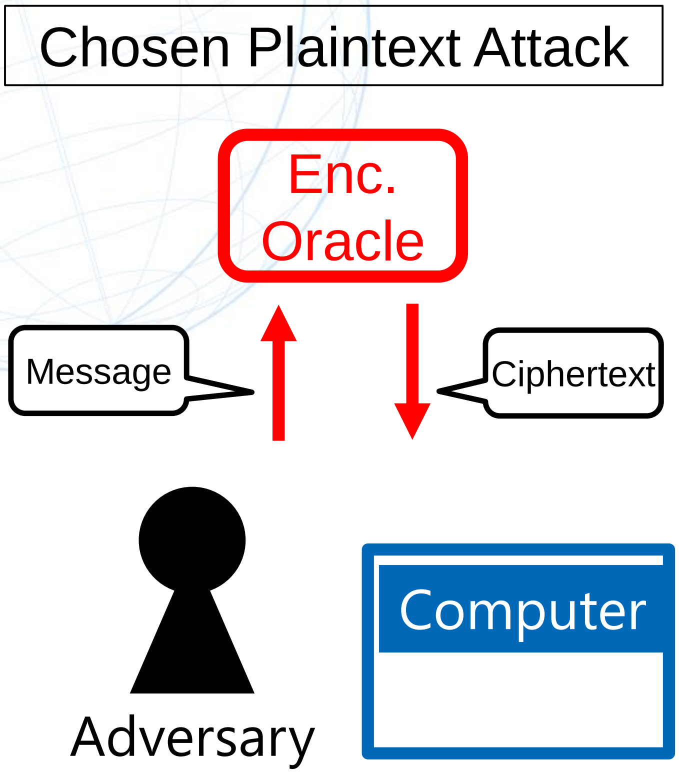


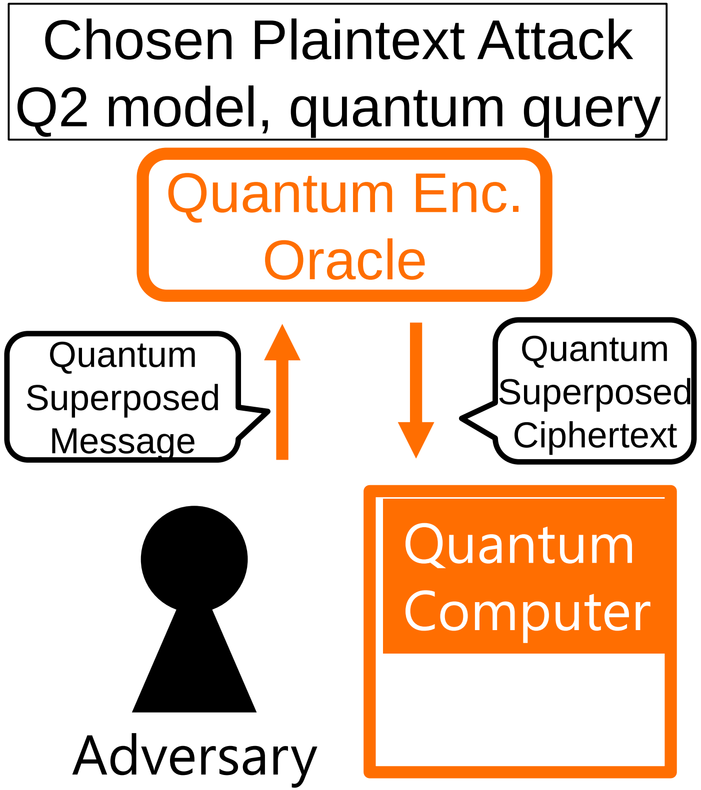
Attack Models





Attack Models





Question:
Why should we consider quantum query attacks?

Question:
Why should we consider quantum query attacks?

A1. Classical algorithms can be converted into quantum algorithms

quantum query attacks on obfuscated implementations?

Question:
Why should we consider quantum query attacks?

A1. Classical algorithms can be converted into quantum algorithms

quantum query attacks on obfuscated implementations?

A2. Quantum query attacks lead to more realistic <u>[classical query + quantum computation]</u> attacks

Ex.) Offline Simon's algorithm at Asiacrypt 2019.

Question:
Why should we consider quantum query attacks?

A1. Classical algorithms can be converted into quantum algorithms

quantum query attacks on obfuscated implementations?

A2. Quantum query attacks lead to more realistic [classical query + quantum computation] attacks

Ex.) Offline Simon's algorithm at Asiacrypt 2019.

A3. For hash functions, quantum query attacks are natural

Question:
Why should we consider quantum query attacks?

NTT

A1. Classical algorithms can be converted into quantum algorithms

quantum query attacks on obfuscated implementations?

A2. Quantum query attacks lead to more realistic [classical query + quantum computation] attacks

Ex.) Offline Simon's algorithm at Asiacrypt 2019.

A3. For hash functions, quantum query attacks are natural

A4. If a scheme is secure against quantum query attacks, it can be used in cryptographic applications that run on quantum computers.

Quantum Query Attacks

Known Quantum Attacks : Today

NTT

	Classical	Quantum
Exhaustive Key Search	$O(2^n)$	$O(2^{n/2})$
Collision Finding	$O(2^{n/2})$	$O(2^{n/3})$
Key Recovery on Even-Mansour	$O(2^{n/2})$	Polynomial time
Forgery against CBC-MAC	$O(2^{n/2})$	Polynomial time

Remark：The last two attacks assumes that quantum keyed oracles are available

Known Quantum Attacks : Today

NTT

	Classical	Quantum
Exhaustive Key Search	$O(2^n)$	
Collision Finding	$O(2^{n/2})$	
Key Recovery on Even-Mansour	$O(2^{n/2})$	Polynomial time
Forgery against CBC-MAC	$O(2^{n/2})$	Polynomial time

Simon's algorithm

Remark : The last two attacks assumes that quantum keyed oracles are available

Simon's period finding algorithm

NTT

Problem

Suppose $f: \{0,1\}^n \to S$ and $s \in \{0,1\}^n$ satisfy

$$\forall x \in \{0,1\}^n \;\; f(x \oplus s) = f(x)$$

Given an oracle access to f, find s.

Classical algorithms: Exponential time

Simon's quantum algorithm: Polynomial time [Sim97]

[Sim97] Daniel R Simon. On the power of quantum computation. *SIAM journal on computing*, 26(5):1474–1483, 1997.

Simon's period finding algorithm

Problem

To mount poly-time attacks,
it is important to reduce
the target problem to Simon's problem

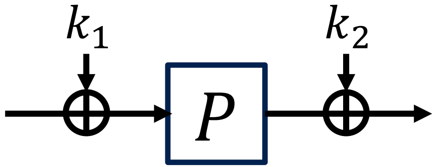
[Sim97] Daniel R Simon. On the power of quantum computation. *SIAM journal on computing*, 26(5):1474–1483, 1997.

Key-Recovery Attack on Even-Mansour

NTT

Even-Mansour cipher E_{k_1,k_2}

(P:public permutation)



Quantum CPA against Even-Mansour ciphers

$f(x) = E_{k_1,k_2}(x) \oplus P(x)$ **satisfies** $f(x \oplus k_1) = f(x)$

- **We <u>can recover k_1 in polynomial time</u> with Simon's algorithm**
- k_2 **can easily be recovered since we have**

$$E_{k_1,k_2}(x) \oplus P(x \oplus k_1) = k_2$$

[KM12] H. Kukakado and M. Morii: Security on the quantum-type Even-Mansour cipher. ISITA 2010.

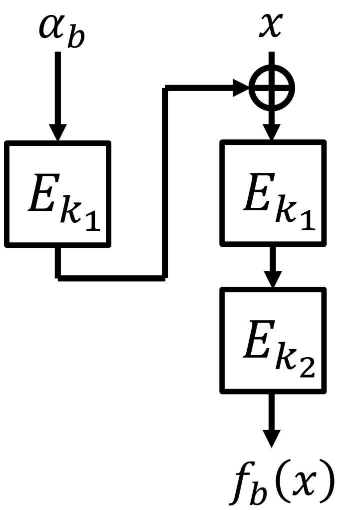
Various MACs/AEs are broken in poly-time…

NTT

If quantum queries are allowed, Simon's algorithm breaks

- CBC-MAC
- PMAC
- GMAC
- GCM
- OCB

…



In polynomial time !

M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia: Breaking symmetric cryptosystems using quantum period finding (CRYPTO 2016)

Luby-Rackoff (Feistel) Construction

NTT

Security in the classical setting

	PRP? (secure against CPA?)	SPRP? (secure against CCA?)
2-round	×	×
3-round	○	×
4-round	○	○
5-round	○	○

M. Luby, C. Rackoff: How to construct pseudo-random permutations from pseudorandom functions (CRYPTO '85)

Luby-Rackoff (Feistel) Construction

NTT

Security in the quantum setting

	PRP? (secure against CPA?)	SPRP? (secure against CCA?)
2-round	×	×
3-round	× [KM10]	×
4-round	O [HI19]	× [IHMSI19]
5-round	O [HI19]	?

[KM10] M. Luby, C. Rackoff: Quantum distinguisher between the 3-round Feistel cipher and the random permutation (ISIT 2010)
[IHMSI19] G. Ito, A. Hosoyamada, R. Matsumoto, Y. Sasaki, T. Iwata: quantum chosen-ciphertext attacks against Feistel ciphers? (CT-RSA 2019)
[HI19] A. Hosoyamada, T. Iwata: 4-Round Luby-Rackoff construction is a qPRP. (Asiacrypt 2019)

Other Quantum Query Attacks

NTT

- Speed-up for differential/linear cryptanalysis [KLLN16b]
- Key recovery attacks on Feistel by using the quantum distinguishers [HS18b,IHMSI19]
- The attack with Kuperberg's algorithm [BN18]
- The attack on the FX construction by Leander and May [LM17]
- Speed-up for Demiric-Secluk meet-in-the-middle attack [HS18b, BNS19]

[BN18] X. Bonnetain, M. Naya-Plasencia: Hidden Shift Quantum Cryptanalysis and Implications, Asiacrypt 2018.

[HS18b] A. Hosoyamada, Y. Sasaki: Quantum Demiric-Selçuk Meet-in-the-Middle Attacks: Applications to 6-Round Generic Feistel Constructions, SCN 2018.

[IHMSI19] G. Ito, A. Hosoyamada, R. Matsumoto, Y. Sasaki, T. Iwata: Quantum Chosen-Ciphertext Attacks Against Feistel Ciphers. CT-RSA 2019.

[KLLN16b] M. Kaplan, G. Leurent, A. Leverrier, M. Naya-Plasencia: Quantum Differential and Linear Cryptanalysis. IACR Trans. Symmetric Cryptol. 2016(1), pp. 71-94.

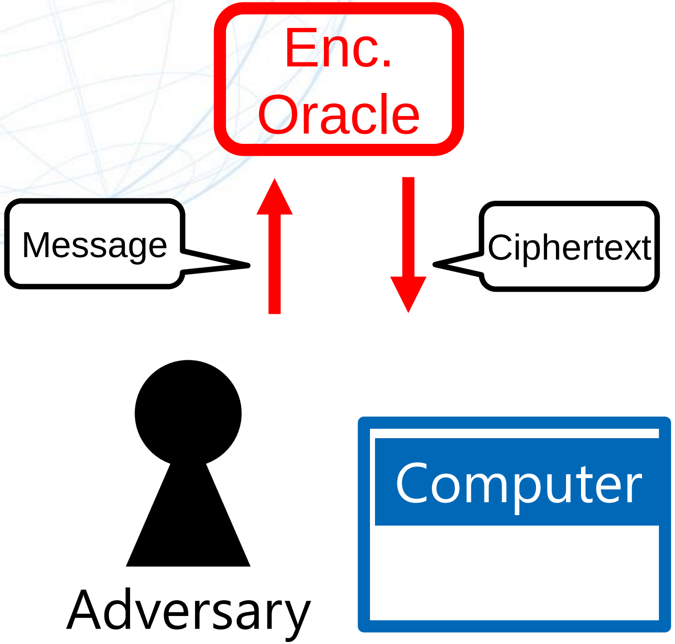
[LM17] G. Leander, A. May: Grover Meets Simon - Quantumly Attacking the FX-construction. Asiacrypt 2017.

[BNS19] X. Bonnetain, M. Naya-Plasencia, A. Schrottenloher: Quantum Security Analysis of AES. IACR Trans. Symmetric Cryptol. 2019(2), pp. 55-93.

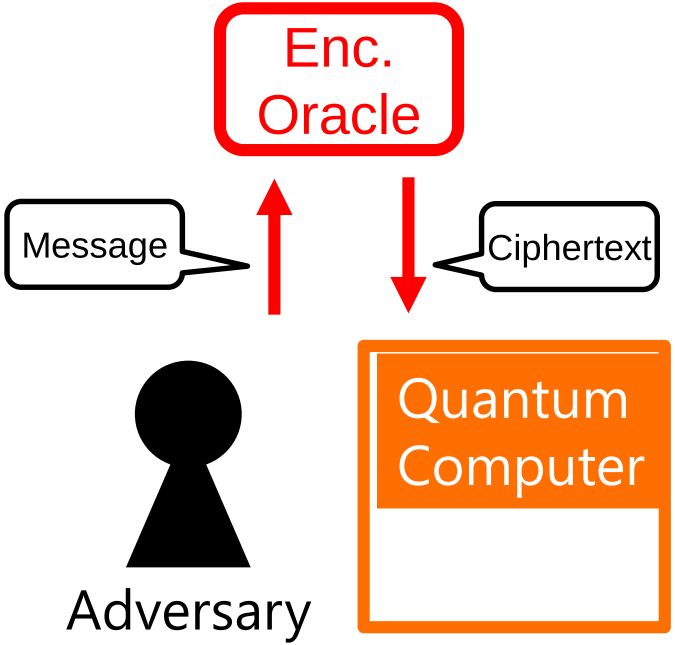
Attacks with Classical Query + Quantum Computation

Attack Models

Chosen Plaintext Attack



Chosen Plaintext Attack
Q1 model, classical query



Offline Simon’s algorithm (AC 2019)

NTT

Quantum query attack with Simon’s algorithm is applicable

+

Simple On-Off MITM attack is applicable in the classical setting

⇓

Even if quantum queries are not allowed and just a small quantum computer is available, by using Simon’s algorithm we can mount a memory-efficient attack

X. Bonnetain, A. Hosoyamada, M. Naya-Plasencia, Y. Sasaki, A. Schrottenloher: Quantum Attacks without Superposition Queries: the Offline Simon’s Algorithm (Asiacrypt 2019)

Offline Simon's algorithm (AC 2019)

NTT

(Q1 / Classical query) attacks on Even-Mansour

	Time	Query	Q. Mem	C. Mem
Kuwakado & Morii [KM12]	$2^{n/3}$	$2^{n/3}$	$2^{n/3}$	$2^{n/3}$
Hosoyamada & Sasaki [HS18a]	$2^{3n/7}$	$2^{3n/7}$	Poly(n)	$2^{n/7}$
Offline Simon	$2^{n/3}$ $(< 2^{3n/7})$	$2^{n/3}$	**poly(n)**	**poly(n)**

Note: Polynomial factors are ignored. Only classical queries are allowed to keyed oracles.
No parallelized computations.

[KM12] H. Kukakado and M. Morii: Security on the quantum-type Even-Mansour cipher. ISITA 2010.
[HS18a] A. Hosoyamada, Y. Sasaki: Cryptanalysis Against Symmetric-Key Schemes with Online Classical Queries and Offline Quantum Computations, CT-RSA 2018.

Other classical query attacks

NTT

- Differential / Linear Cryptanalysis [KLLN16b]
- Online-Offline meet-in-the-middle attacks [HS18a]
- Demiric-Selçuk meet-in-the-middle attacks [BNH19,HS18b]

and more…

[KLLN16b] M. Kaplan, G. Leurent, A. Leverrier, M. Naya-Plasencia: Quantum Differential and Linear Cryptanalysis. IACR Trans. Symmetric Cryptol. 2016(1), pp. 71-94.

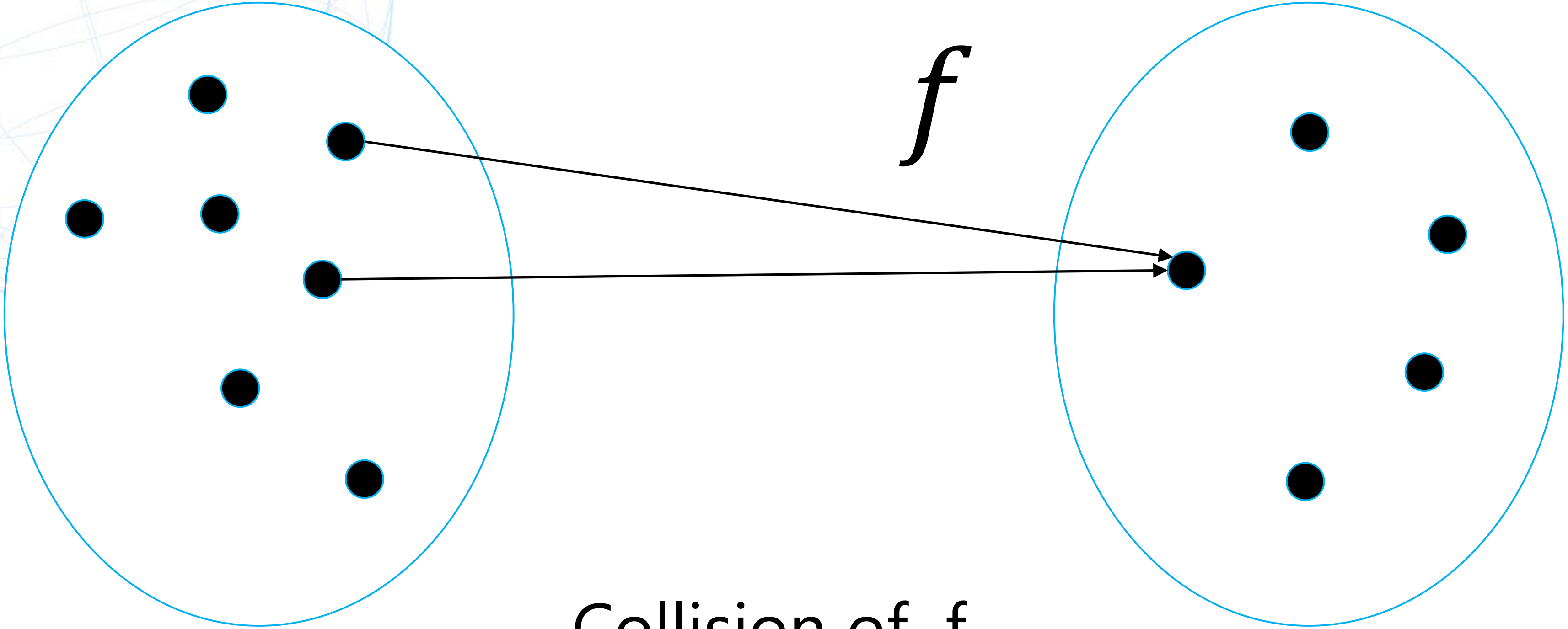
[BNS19] X. Bonnetain, M. Maya-Plasencia, A. Schrottenloher: Quantum Security Analyais of AES. IACR Toransactoins on Symmetric Cryptology, 2019(2).

[HS18a] A. Hosoyamada, Y. Sasaki: Cryptanalysis Against Symmetric-Key Schemes with Online Classical Queries and Offline Quantum Computations, CT-RSA 2018.

[HS18b] A. Hosoyamada, Y. Sasaki: Quantum Demiric-Selçuk Meet-in-the-Middle Attacks: Applications to 6-Round Generic Feistel Constructions, SCN 2018.

Generic Attacks on Hash

Collision Attack on Hash



Collision of f

Collision Attack on Hash

The number of queries required to find a collison

Classical : $\Theta(N^{1/2})$

Quantum : $\Theta(N^{1/3})$

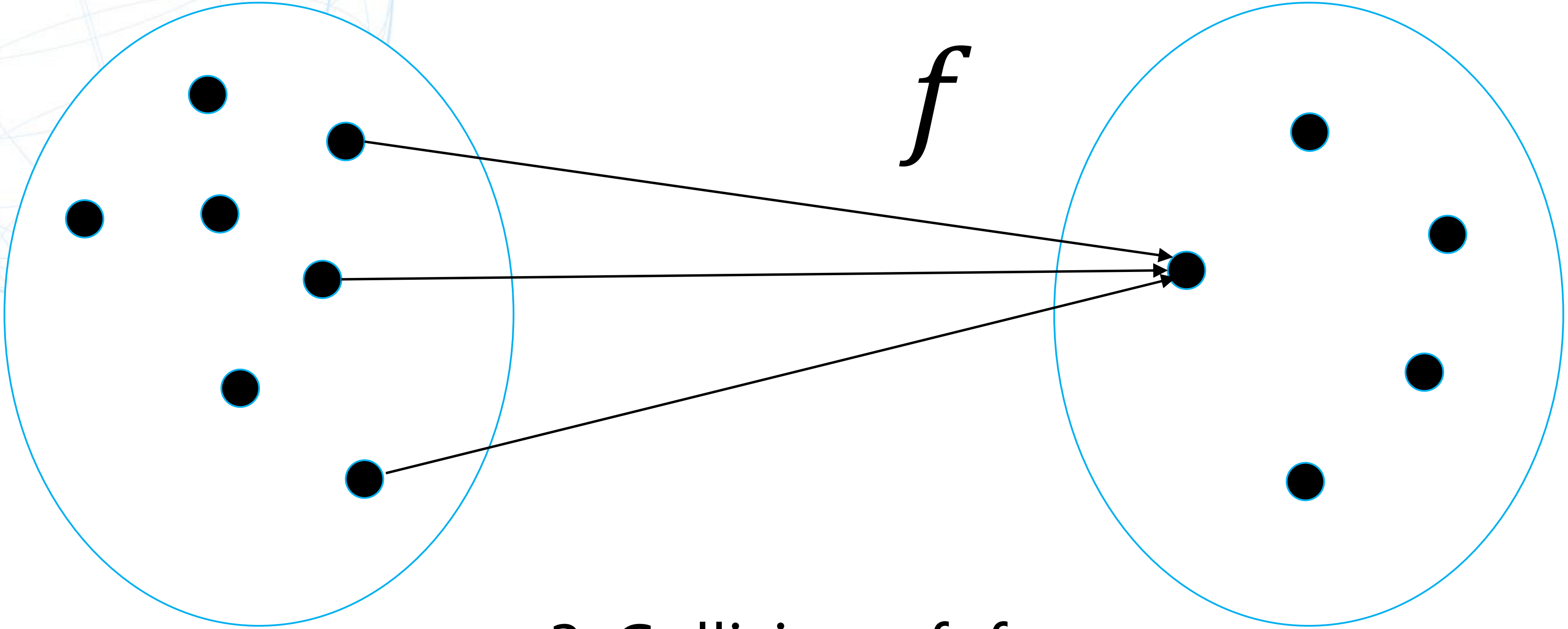
[BHT97,Zha15]

The BHT Algorithm

[BHT97] G. Brassard, P. Hoyer, A. Tapp: Quantum cryptanalysis of hash and claw-free functions. ACM Sigact News, 28(2), pp. 14-17 (1997).

[Zha15] M. Zhandry: A note on the quantum collision and set equality problems. Quantum Information & Computation 15(7&8): pp. 557-567 (2015)

MultiCollision Attack on Hash



3-Collision of f

MultiCollision Attack on Hash

NTT

The number of queries required to find an ℓ-collison

Classical : $\Theta(N^{(\ell-1)/\ell})$ [STKT08]

Quantum : $\Theta\left(N^{\frac{2^{\ell-1}-1}{2^{\ell}-1}}\right)$

[HSX17, HSTX19,LZ19]

[STKT08] K. Suzuki, D. Tonien, K. Kurosawa, K. Toyota : Birthday paradox for multi-collisions. IEICE Transactions, 91-A(1):39–45, 2008

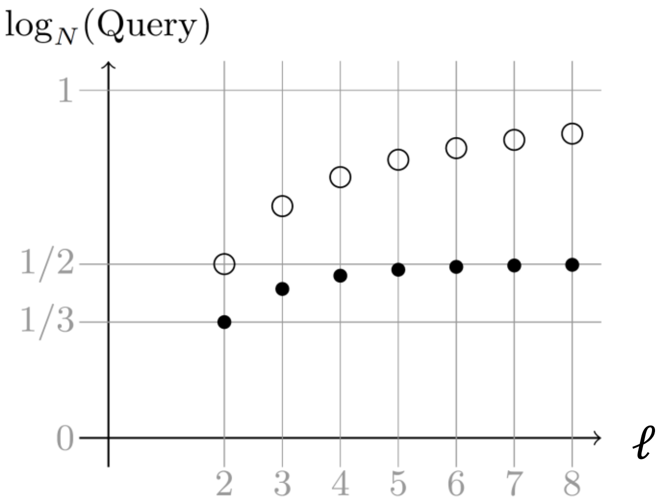
[HSX17] A. Hosoyamada, Yu Sasaki, K. Xagawa: Quantum Multicollision-Finding Algorithm. Asiacrypt 2017.

[HSTX19] A. Hosoyamada, Yu Sasaki, S. Tani, K. Xagawa: Improved Quantum Multicollision-Finding Algorithm. PQCrypto 2019.

[LZ19] Q. Liu, M. Zhandry: On Finding Quantum Multi-collisions, Eurocrypt 2019.

MultiCollision Attack on Hash

ℓ (multiplicity)	2	3	4	5
Classical (○)	$N^{\frac{1}{2}}$	$N^{\frac{2}{3}}$	$(N^{\frac{3}{4}})$	$(N^{\frac{4}{5}})$
Quantum (●)	$N^{\frac{1}{3}}$	$N^{\frac{3}{7}}$	$N^{\frac{15}{31}}$	$N^{\frac{31}{63}}$



Other generic attacks on hash

NTT

- Collision finding with polynomial number of qubits[CNS17]
  - The BHT algorithm finds a collision in time $\boldsymbol{N^{1/3}}$ but requires $\boldsymbol{N^{1/3}}$ qubits…
  - Even if only poly-qubits are available, collision can be found in time $\boldsymbol{N^{2/5}}$ $(< \boldsymbol{N^{1/2}})$
- Acceleration for the k-xor problem[Amb07, GNS18]
- Multi-target preimage search [BB17, CNS17]
  - Applicable to key recovery in multi-key/user setting

[Amb07] Quantum walk algorithm for element distinctness. SIAM J. Comput. 37(1), 210-239 (2007).
[BB17] G. Banegas, D. Bernstein: Low-Communication Parallel Quantum Multi-Target Preimage Search. SAC 2017.
[CNS17] A. Chailloux, M. Naya-Plasencia, A. Schrottenloher: An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography. Asiacrypt 2017.
[GNS18] L. Grassi, M. Naya-Plasencia, A. Schrottenloher: Quantum Algorithms for the k-xor Problem. Asiacrypt 2018.

Challenges for the future in cryptanalysis

Attacks on keyed primitives

NTT

- More attacks on concrete primitives
- Applications of quantum algorithms other than Simon (period finding), Grover, Quantum-walk-search
- New quantum algorithms (attacks) that are specific to concrete symmetric key schemes
- Other applications of quantum algorithms in the classical query model

and more…

Generic attacks on hash

- New Time-Memory tradeoff for inverting functions that is better than the classical tradeoff?

Time-Memory tradeoff for inverting function

- f: random function/permutation (n-bit to n-bit) / $\mathcal{A}$: adversary

1. $\mathcal{A}$ runs precomputation with h and store (classical/quantum) data of size S
2. $\mathcal{A}$ receives a randomly chosen y
3. $\mathcal{A}$ tries to find x s.t. f(x) = y in time T by using the stored data

Time-Memory tradeoff for inverting function

- f: random function/permutation (n-bit to n-bit) / $\mathcal{A}$: adversary

1. $\mathcal{A}$ runs precomputation with h and store (classical/quantum) data of size S
2. $\mathcal{A}$ receives a randomly chosen y
3. $\mathcal{A}$ tries to find x s.t. f(x) = y in time T by using the stored data

Classical tradeoff between T and S:

$T = 2^n/S$ (if f is a random permutation)

Time-Memory tradeoff for inverting function

NTT

- f: random function/permutation (n-bit to n-bit) / $\mathcal{A}$: adversary

1. $\mathcal{A}$ runs precomputation with h and store (classical/quantum) data of size S
2. $\mathcal{A}$ receives a randomly chosen y
3. $\mathcal{A}$ tries to find x s.t. f(x) = y in time T by using the stored data

<u>Classical tradeoff between T and S</u>:

$T = 2^n/S$ (if f is a random permutation)

<u>Quantum tradeoff between T and S</u>:

So far, there does not exist any tradeoff that is better than $T = 2^n/S$

Grover search achieves $T = 2^{n/2}$ when S=1 but it is not clear what kind of trade-off is possible when S > 1…

Security Proofs / Lower bounds

What has already been done?

NTT

Generic bounds on random functions (query complexity)

- Preimages of random functions: $\Theta(N) \rightarrow \Theta\left(N^{1/2}\right)$
- RP-RF switch: $\Theta\left(N^{1/2}\right) \rightarrow \Theta\left(N^{1/3}\right)$
- Multicollision-Finding problem: $\Theta\left(N^{\frac{(\ell-1)}{\ell}}\right) \rightarrow \Theta\left(N^{\frac{2^{\ell-1}-1}{2^{\ell}-1}}\right)$
- k-xor: $\Theta\left(N^{\frac{1}{k}}\right) \rightarrow \Theta\left(N^{\frac{1}{k+1}}\right)$

Red: Classical Bound

Blue: Quantum Bound

What has already been done?

Security proofs for specific schemes

(against quantum query attacks, w/o algebraic assumptions)

- CPA security of encryption modes (CTR, CBC, OFB,…) (@PQCrypto2016)
- Generic composition for AE (@PQCrypto2016)
- PRF security of NMAC/HMAC (@CRYPTO2017)
- Sponge-like construction
  - PRF security of sponge with keyed (secret) permutation (@CRYPTO2017)
  - Collision-resistance (collapsing) of sponge with public function (@PQCrypto2018)
- Indifferentiability of (fixed-length) Merkle-Damgaard (@CRYPTO2019)
- PRP security of 4-Round Luby-Rackoff (Feistel) (@Asiacrypt 2019)

What is difficult in the quantum setting?

NTT

1. It is not trivial how to record queries
   - Copying the values of queries disturbs the adversary's quantum states, which leads to changing its behavior significantly

2. "Lazy Sampling" is not available
   - In classical proofs, the value F(x) of a random function F is randomly chosen on the fly when the adversary queries x to F
   - At most one value is fixed per each classical query
   - In the quantum setting, the adversary may query a superposition of all possible x at the same time…

The Compressed Oracle Technique

Compressed Oracle Technique [Zha19]

- It enables us to do "Lazy sampling" to some extent for random functions in the quantum setting
- The important observation: Sometimes recorded information should be "forgotten"
- Many applications:

  Quantum Indifferentiability of Merkle-Damgaard[Zha19]

  Lower bound for multicollision finding problem[LZ19]

  quantum PRP security of 4-round Luby-Rackoff[IH19]

  etc···

[Zha19] M. Zhandry: How to record quantum queries, and applications to quantum indifferentiability. Crypto 2019.

[LZ19] Q. Liu, M. Zhandry: On Finding Quantum Multi-collisions, Eurocrypt 2019.

[IH19] A. Hosoyamada, T. Iwata: 4-round Luby-Rackoff Construction is a qPRP. Asiacrypt 2019.

The Compressed Oracle Technique

One remark:

Zhandry's compressed oracle technique cannot be applied to permutations

Remarks on query lower bound

Research Area	Problems	Backward query?
Quantum computation	Worst case	×
Public key crypto	Average case (randomized)	×
Symmetric key crypto	Average case (randomized)	○

Remarks on query lower bound

Research Area	Problems	Backward query?
Quantum computation	Worst case	×
Public key crypto	Average case (randomized)	×
Symmetric key crypto	Average case (randomized)	○

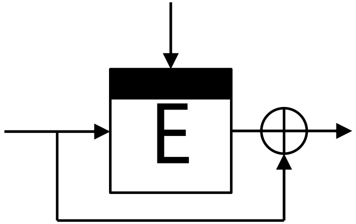
It is hard to treat permutations…

- So far there is no published results on quantum proof techniques for public random permutation or ideal cipher

- Exception: One-wayness of Davies-Meyer Compression function

  [HY18]

  - Giving security proofs by computing statistical distance
  - (so far & as far as I know) the only published results on quantum proofs for schemes in ideal permutation model / ideal cipher model w/o algebraic assumptions



[HY18] A. Hosoyamada, K. Yasuda: Building quantum one-way functions from block ciphers: Davies-Meyer and Merkle-Damgaard constructions. Asiacrypt 2018.

Challenges for the future

NTT

- Generic and strong proof technique to treat random permutations / ideal ciphers
  - The compressed oracle technique: Since F is a random function, F(x) and F(y) are independent, which means that the quantum registers for F(x) and F(y) are not entangled
  - If we try to apply the compressed oracle technique to a random permutation P, P(x) and P(y) are ***not*** independent, which means that the quantum registers for P(x) and P(y) will be ***entangled***

Quantum entanglement always make things extremely difficult…

Challenges for the future

NTT

- Generic and strong proof technique to treat random permutations / ideal ciphers
  - The compressed oracle technique: Since F is a random function, F(x) and F(y) are independent, which means that the quantum registers for F(x) and F(y) are not entangled
  - If we try to apply the compressed oracle technique to a random permutation P, P(x) and P(y) are ***not*** independent, which means that the quantum registers for P(x) and P(y) will be ***entangled***

Quantum entanglement always make things extremely difficult…

Solved??

Czajkowski, Majenz, Schaffner, Zur: Quantum lazy sampling and game-playing proofs for quantum indifferentiability. (ePrint 2019/428)

Summary

Summary

NTT

- Recent results show many unexpected attacks are possible in the quantum setting
  - Many schemes are broken in poly-time with quantum queries
  - Simon's algorithm is applicable even if only classical queries are allowed
  - Various new tradeoffs
- There are lots of challenging but interesting topics to study
  - Time-memory tradeoffs for inverting functions?
  - Proof techniques for permutations?
  - AES can be broken with quantum algorithms?

Thank you!