

Security Rests on Three Grounds, and a Quantum Computer Breaks Only One

— RSA at **2048** Bits Is Accelerated by **$10^{25.3}$** , Yet Multiplying the Key Length by **8** Raises the Quantum Effort Only **512**-fold — What Holds No Information Cannot Be Computed by Any Machine — [Paper 305]

Yuuki YAMAGISHI (山岸 勇輝)
Yamagishi Complexity Torus Lab, Japan
August 2026

— *From thinking to syncing.* —

Abstract

The sentence “this cipher is secure” rests on one of three different grounds. This paper asks which of them a quantum computer breaks—the answer is one. No new mathematical theorem and no new law is claimed. First, there are three grounds. Computational, information-theoretic, and physical security, and all three depend on different things (Section 2). Second, this is the core of the paper. A quantum computer breaks only the first, and cannot in principle reach the other two (Section 3). Third, the breaking is dramatic. At RSA 2048 bits the ratio of classical to quantum effort is **$10^{25.3}$** (Section 4). Fourth, key length cannot answer it. Multiplying the key length by 8 raises the quantum effort only **512**-fold (Section 4). Fifth, symmetric keys need only be doubled. Grover gains only a square root, and AES-256 retains an effective **128** bits (Section 5). Sixth, the separator is resting on difficulty against resting on the absence of information (Section 6).

Scope of this paper (scope note): No new mathematical theorem and no new law is claimed—the complexity of the number field sieve, Shor’s algorithm, Grover’s algorithm, and the perfect secrecy of the one-time pad are all standard. We do not build cryptography—all we use is one exponent and one mutual information. We do not explain the algorithms—Shor and Grover are quoted by their cost formulas, and we do not enter their workings. We do not discuss implementation security—key management, randomness quality, side channels, and implementation flaws are not treated at all. Most real breaks live there, but this paper treats only the type of ground. We do not discuss the feasibility of quantum computers—neither when nor whether they can be built is treated. Only what would break if they were. We assert no values for the effort—the sieve’s exponent is asymptotic, and $10^{25.3}$ is an order with constants dropped. Only the direction and the order are claimed. We do not treat lattice cryptography—post-quantum schemes also sit on the computational ground, and which problems stay hard under quantum attack is not adjudicated here. Relation to earlier papers: Paper 281 showed that what cannot be copied can still be corrected, and that eavesdropping becomes the number 25%—the third ground here is the physical security shown there. Paper 252 counted four quantities called “information,” needing different things—the second ground here rests on a mutual information that is exactly 0. Paper 112 counted “six distinct roots sharing one rhyme”—“security” here likewise has three distinct roots under one word. Paper 302 treated how existence does not give quantity—computational security likewise sits where “hard” has no settled quantity. What is added is lining up the three grounds by what they depend on, computing the RSA-2048 acceleration as $10^{25.3}$, showing that an eightfold key length raises the quantum effort only 512-fold, and separating symmetric from public key by square root against cube.

1. Notation and the Question

Fact: The sentence “this cipher is secure” means quite different things for different ciphers.

Question: How many kinds are there? And which of them does a quantum computer break?

Observation 1.1

The common phrasing is “quantum computers will break cryptography.” This paper regards that as imprecise—only one of three is broken.

2. Three Grounds, All Depending on Different Things

Check 2.1:

Ground	Content	Example	Depends on
Computational	it is hard to solve	RSA, elliptic curves	the adversary's power
Information-theoretic	no information remains	one-time pad	nothing at all
Physical	measuring destroys	quantum key distribution	the theory of measurement

Observation 2.2

The rightmost column holds three different things. The first is relative (to the adversary), the second absolute, the third relative to physical law—one word “secure” covering three standings.

Observation 2.3

Only the first weakens with time. As computers get faster the same key gets weaker—the second and third do not weaken with time.

Observation 2.4

Paper 112 counted “six distinct roots sharing one rhyme.” “Security” here has three distinct roots—and different roots break differently.

3. The Core: A Quantum Computer Breaks Only the First

Check 3.1: We apply a quantum computer to all three.

Ground	A quantum computer	Why
Computational (RSA, discrete log)	breaks it	Shor solves it in polynomial time
Information-theoretic (one-time pad)	cannot	what holds no information cannot be computed
Physical (QKD)	cannot	it rests on the theory of measurement itself

Observation 3.2

This is the core of the paper. Only one of the three breaks——“quantum computers will break cryptography” is one third right.

Check 3.3: We show why the second cannot break, in units of information. Plaintext M , uniform single-use key K , ciphertext $C = M \oplus K$.

Plaintext length [bit]	$H(M)$	$H(M C)$	Mutual information $I(M; C)$
8	8	8	0
128	128	128	0
1024	1024	1024	0

Observation 3.4

Seeing C does not change the distribution of M at all, so $H(M | C) = H(M)$ and $I(M; C) = 0$. Exactly zero, not approximately——there is no information to extract.

Observation 3.5

Hence no machine whatever can solve it. Exhaust the keys and every plaintext comes out equally likely——it is not “hard” but “absent”.

Observation 3.6

A point to write honestly——the one-time pad’s premises are heavy. The key must be as long as the plaintext, uniformly random, and never reused——the problem of distributing the key becomes as large as the problem of encryption. That is what the third ground fills (Paper 281).

4. The Breaking Is Dramatic, and Key Length Cannot Answer It

Setting: The classical effort (number field sieve) is $\exp(c(\ln N)^{1/3}(\ln \ln N)^{2/3})$ with $c = (64/9)^{1/3} = 1.922999$. Shor is $O((\log N)^3)$.

Check 4.1:

Key length [bit]	Classical [10^x]	Quantum [10^x]	Ratio [10^x]
512	19.24	8.13	11.12
1024	26.12	9.03	17.09
2048	35.19	9.93	25.25
4096	47.11	10.84	36.27

Observation 4.2

At RSA 2048 bits the ratio is $10^{25.3}$. And the longer the key, the wider the ratio——at 4096 bits it is $10^{36.3}$.

Check 4.3: Against the classical attack, longer keys do answer.

To reach 2^n classically	RSA key length
2^{80}	about 850 bits
2^{112}	about 1853 bits
2^{128}	about 2538 bits
2^{256}	about 13547 bits

Check 4.4: Against the quantum attack they do not. Shor is $(\log N)^3$, so the effort goes only as the cube of the key length.

n [bit]	Effort $\sim n^3$	Times that at $n = 2048$
2048	8.590×10^9	1.0
4096	6.872×10^{10}	8.0
8192	5.498×10^{11}	64.0
16384	4.398×10^{12}	512.0

Observation 4.5

An eightfold key length raises the quantum effort only **512**-fold. On the classical side the same change takes 10^{35} to 10^{47} , a factor of 10^{12} —one and the same move works on one side and not on the other.

Observation 4.6

The reason is the shape of the cost. Classical is sub-exponential, quantum polynomial—lengthening the key acts strongly inside an exponent and weakly inside a polynomial.

5. Symmetric Keys Need Only Be Doubled

Setting: The quantum attack on symmetric keys is Grover's, which gains only a square root.

Check 5.1:

Key length	Classical 2^n	Quantum $2^{n/2}$	Effective bits
128	3.403×10^{38}	1.845×10^{19}	64
192	6.277×10^{57}	7.923×10^{28}	96
256	1.158×10^{77}	3.403×10^{38}	128

Observation 5.2

AES-128 falls to an effective 64 bits. But AES-256 retains an effective 128—doubling the key suffices.

Observation 5.3

The same phrase “weakened against quantum computers” carries very different weights.

	Quantum speedup	Remedy
Symmetric (AES)	$\sqrt{}$ (Grover)	double the key
Public key (RSA)	sub-exponential $\rightarrow$ polynomial (Shor)	key length cannot

Observation 5.4

A square root is filled by key length; a collapsed exponent is not. The square-root price Paper 294 measured (the square of the improvement) is here a help—doubling recovers it.

6. Separator: Difficulty against the Absence of Information

Observation 6.1

Separator—what must move for the security to be lost?

Ground	What must move
Computational	an algorithm or a machine (and one did)
Information-theoretic	nothing can ($I = 0$ is identical)
Physical	the theory of measurement (quantum mechanics itself)

Observation 6.2

Only the first rests on something people can move. The second on a mathematical identity, the third on physical law—what it would take to break them is of a different class.

Observation 6.3

So “quantum computers will break cryptography” should be put exactly——“a quantum computer breaks the ciphers that rest on difficulty.”It reaches neither those resting on the absence of information nor those resting on measurement.

Observation 6.4

Paper 281 showed with the number 25% that quantum key distribution’s security is not computational.This paper places that within the three grounds——it is the third, of a different class from the first.

Observation 6.5

A point to write honestly——real ciphers are almost never broken.What is broken is implementation, key management, randomness, side channels, not the ground itself——this paper treats only the type of ground, which is a different matter from practical security.

7. Roll Call and Closing

1. Three grounds (Check 2.1): **All depending on different things.**
2. **Only the first weakens with time** (Observation 2.3): **Because it is relative.**
3. **Quantum breaks only one** (Check 3.1): **One third.**
4. $I(M; C) = 0$ exactly (Check 3.3): **No information to extract.**
5. **Ratio $10^{25.3}$ at RSA 2048** (Check 4.1): **Widening with key length.**
6. **2538 bits for classical 2^{128}** (Check 4.3): **Lengthening works there.**
7. **Eightfold gives 512-fold** (Check 4.4): **Lengthening does not work here.**
8. **AES-128 falls to 64 effective** (Check 5.1): **AES-256 gives 128.**
9. **A square root is filled by key length** (Observation 5.4): **Doubling recovers it.**
10. **Different classes of what must move** (Observation 6.2): **Machine, identity, or law.**

Closing: “This cipher is secure” rests on one of three different grounds——computational (it is hard), information-theoretic (there is no information), and physical (measuring destroys).A quantum computer breaks only the first——“quantum computers will break cryptography” is one third right.The breaking is indeed dramatic——at RSA

2048 bits the ratio of classical to quantum effort is $10^{25.3}$, and at 4096 bits $10^{36.3}$. And key length cannot answer it —against the classical attack 2538 bits reaches 2^{128} , while on the quantum side an eightfold key raises the effort only 512-fold. Symmetric keys are another matter—Grover gains only a square root, so AES-256 retains an effective 128 bits. One thing separates them—whether the security rests on difficulty or on the absence of information. Difficulty moves with machines. $I(M; C) = 0$ does not move. Put exactly—a quantum computer breaks the ciphers that rest on difficulty.

References

1. Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4).
 2. Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5).
 3. Grover, L. K. (1996). A Fast Quantum Mechanical Algorithm for Database Search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*.
 4. Lenstra, A. K. and Lenstra, H. W. (eds.) (1993). *The Development of the Number Field Sieve*. Berlin: Springer.
 5. Bennett, C. H. and Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*.
 6. Vernam, G. S. (1926). Cipher Printing Telegraph Systems. *Transactions of the American Institute of Electrical Engineers*, 45.
 7. Yamagishi, Y. (2026). *The Allotted Region and the Freedom Within* [Paper 112]. Zenodo. 10.5281/zenodo.21962834
 8. Yamagishi, Y. (2026). *Information Is Four Quantities, and They Need Different Things* [Paper 252]. Zenodo. 10.5281/zenodo.22161148
 9. Yamagishi, Y. (2026). *It Cannot Be Copied, Yet It Can Be Corrected* [Paper 281]. Zenodo. 10.5281/zenodo.22171058
 10. Yamagishi, Y. (2026). *Separation Improves Only as the Square Root of the Length* [Paper 294]. Zenodo. 10.5281/zenodo.22171603
-

— *From thinking to syncing.* —

Yuuki YAMAGISHI (山岸 勇輝)

© 2026 Yamagishi Complexity Torus Lab, Japan · Licensed under Creative Commons Attribution 4.0 International (CC BY 4.0)