

「安全」の根拠は三つあり、量子計算機が壊すのは一つだけである

— RSA 2048 bit は $10^{25.3}$ 倍加速され、鍵長を 8 倍にしても量子側の手間は 512 倍にしかない —
情報が無いものは、どんな計算機でも計算できない — [論文305]

山岸 勇輝 (Yuuki YAMAGISHI)

Yamagishi Complexity Torus Lab, Japan | 山岸勇輝ラボ

2026年8月

— *From thinking to syncing.* —

要旨

「この暗号は安全である」という一文は、三つの別の根拠のどれかに立っている。本稿が問うのは、量子計算機が壊すのはどれかである——答は、一つだけである。新しい数学定理も新しい法則も主張しない。第一に、根拠は三つある。計算量的安全・情報理論的安全・物理的安全であり、依存先が三つとも違う（第2節）。第二に、これが本稿の芯である。量子計算機が壊すのは一つ目だけであり、残り二つには原理的に届かない（第3節）。第三に、壊れ方は劇的である。RSA 2048 bit で古典と量子の手間の比は $10^{25.3}$ である（第4節）。第四に、鍵長では対抗できない。鍵長を 8 倍にしても、量子側の手間は 512 倍にしかない（第4節）。第五に、対称鍵は倍にすれば済む。グローバーは平方根しか稼がず、AES-256 は実効 128 bit で足りる（第5節）。第六に、分離子は「難しさに立つか、情報の不在に立つか」である（第6節）。

本稿の射程 (scope note) : 新しい数学定理も新しい法則も主張しない——数体篩の計算量、ショアのアルゴリズム、グローバーのアルゴリズム、ワントタイムパッドの完全秘匿性は、いずれも標準的である。暗号を作らない——使うのは一つの指数と、一つの相互情報量だけである。アルゴリズムを説明しない——ショアもグローバーも手間の式を引くだけであり、中身には立ち入らない。実装の安全を論じない——鍵管理、乱数の質、サイドチャネル、実装の欠陥は一切扱わない。現実の破られ方の大半はここにあるが、本稿は根拠の型だけを扱う。量子計算機の実現可能性を論じない——いつ作れるかも、作れるかも扱わない。作れたとして何が壊れるかだけを数える。手間の値を主張しない——数体篩の指数は漸近形であり、 $10^{25.3}$ は定数因子を無視した桁である。比較の向きと桁だけが本稿の主張である。格子暗号を扱わない——耐量子暗号も計算量的安全の側にあるが、どの問題が量子で難しいままかは本稿では判定しない。既刊との関係：論文281 は複製できないのに訂正できることを示し、盗聴が 25% という数になると書いた——本稿の三つ目の根拠はそこで示された物理的安全である。論文252 は「情報量」が四つあり要るものが違うと数えた——本稿の二つ目の根拠は相互情報量が厳密に 0 であることに立つ。論文112 は「同じ韻を踏む六つの別根」を数えた——本稿の「安全」も一語の下に三つの別根を持つ。論文302 は存在が定量を教えないことを扱った——本稿の計算量的安全も「難しい」の定量が定まらない側にある。加えたのは三つの根拠を依存先で並べたこと、RSA 2048 bit の加速を $10^{25.3}$ と計算したこと、鍵長を 8 倍にしても量子側が 512 倍にしかならないと示したこと、対称鍵と公開鍵で対処法が違う理由を平方根と三乗で分けたことである。

1. 記法と問い

事実：「この暗号は安全である」という一文は、暗号によってまったく違うことを意味している。

問い：何種類あるか。そして量子計算機は、そのどれを壊すか。

観察 1.1

よくある言い方は「量子計算機が暗号を破る」である。本稿はこれを正確でないと見る——破られるのは三つのうち一つだけである。

2. 根拠は三つあり、依存先が三つとも違う

検算 2.1 :

根拠	中身	例	何に依存するか
計算量的安全	解くのが難しい	RSA、楕円曲線	相手の計算力
情報理論的安全	情報が残っていない	ワンタイムパッド	何にも依存しない
物理的安全	測れば壊れる	量子鍵配送	測定の理論

観察 2.2

右端の列が三つとも違う。一つ目は相対的（相手次第）、二つ目は絶対的、三つ目は物理法則に相対的——同じ「安全」という語が、三つの身分を覆っている。

観察 2.3

一つ目だけが時間とともに弱くなる。計算機が速くなれば、同じ鍵が弱くなる——二つ目と三つ目は、時間が経っても弱くならない。

観察 2.4

論文112は「同じ韻を踏む六つの別根」を数えた。本稿の「安全」も三つの別根である——そして根が違えば、壊れ方も違う。

3. 芯：量子計算機が壊すのは一つ目だけである

検算 3.1：三つに量子計算機を当ててみる。

根拠	量子計算機は	なぜ
計算量的安全（RSA・離散対数）	壊す	ショアが多項式時間で解く
情報理論的安全（ワンタイムパッド）	壊せない	情報が無いものは計算できない
物理的安全（量子鍵配送）	壊せない	測定の理論そのものに立つ

観察 3.2

これが本稿の芯である。三つのうち一つだけが壊れる——「量子計算機が暗号を破る」という一文は、三分の一しか当たっていない。

検算 3.3：二つ目が壊せない理由を、情報の量で示す。平文 M 、一様な使い捨ての鍵 K 、暗号文 $C = M \oplus K$ とする。

平文長 [bit]	$H(M)$	$H(M C)$	相互情報量 $I(M; C)$
8	8	8	0
128	128	128	0
1024	1024	1024	0

観察 3.4

C を見ても M の分布が一切変わらないので、 $H(M | C) = H(M)$ 、したがって $I(M; C) = 0$ である。厳密に 0 であり、近似ではない——取り出すべき情報が存在しない。

観察 3.5

したがってどんな計算機でも解けない。総当たりすればすべての平文が等確率で出てくる——「難しい」のではなく「無い」のである。

観察 3.6

正直に書くべき点——ワンタイムパッドの前提は重い。鍵は平文と同じ長さ・一様乱数・二度使わない——鍵を配る問題が、暗号の問題と同じ大きさになる。そこを三つ目の根拠が埋める（論文281）。

4. 壊れ方は劇的で、鍵長では対抗できない

設定：RSA の古典的な解法（数体篩）の手間は $\exp(c(\ln N)^{1/3}(\ln \ln N)^{2/3})$ 、 $c = (64/9)^{1/3} = 1.922999$ である。ショアは $O((\log N)^3)$ である。

検算 4.1：

鍵長 [bit]	古典 [10^x]	量子 [10^x]	比 [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

観察 4.2

RSA 2048 bit で、比は $10^{25.3}$ である。そして鍵長を伸ばすほど比が開く——4096 bit では $10^{36.3}$ 。

検算 4.3：古典に対しては、鍵長を伸ばせば対抗できる。

古典で 2^n 相当にするには	RSA 鍵長
2^{80}	約 850 bit
2^{112}	約 1853 bit
2^{128}	約 2538 bit
2^{256}	約 13547 bit

検算 4.4：ところが量子に対しては効かない。ショアは $(\log N)^3$ なので、鍵長 n の三乗にしかない。

n [bit]	手間 $\sim n^3$	$n = 2048$ の何倍
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

観察 4.5

鍵長を 8 倍にしても、量子側の手間は 512 倍にしかならない。古典側では 10^{35} から 10^{47} へ 10^{12} 倍に増えるのに——同じ操作が、片方には効き、もう片方には効かない。

観察 4.6

理由は手間の形である。古典は準指数、量子は多項式——鍵長を伸ばす操作は、指数の中では大きく効き、多項式の中では小さくしか効かない。

5. 対称鍵は、倍にすれば済む

設定：対称鍵に対する量子の攻撃はグローバーであり、平方根しか稼がない。

検算 5.1：

鍵長	古典 2^n	量子 $2^{n/2}$	実効鍵長
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

観察 5.2

AES-128 は実効 64 bitに落ちる。ところが AES-256 なら実効 128 bitで足りる——鍵長を倍にすれば済む。

観察 5.3

同じ「量子計算機に対して弱くなる」でも、対処の重さが違う。

量子の加速		対処
対称鍵（AES）	$\sqrt{\quad}$ （グローバー）	鍵長を倍に
公開鍵（RSA）	準指数 $\rightarrow$ 多項式（ショア）	鍵長では無理

観察 5.4

平方根は鍵長で埋まり、指数の崩壊は埋まらない。論文294 が示した平方根の代償（改善の二乗）が、ここでは助けになっている——2 倍にすれば取り返せる。

6. 分離子：難しさに立つか、情報の不在に立つか

観察 6.1

分離子——何を動かすと、安全が失われるか。

根拠	何が動けば失われるか
計算量的安全	アルゴリズムか計算機（現に動いた）
情報理論的安全	何も動かさない（ $I = 0$ は恒等的）
物理的安全	測定の理論（量子力学そのもの）

観察 6.2

一つ目だけが人が動かせるものに立っている。二つ目は数学の恒等式、三つ目は物理法則——壊すのに要るものの階級が違う。

観察 6.3

したがって「量子計算機が暗号を破る」は、正確にはこう言うべきである——「量子計算機は、難しさに立つ暗号を破る」。情報の不在に立つ暗号にも、測定に立つ暗号にも、届かない。

観察 6.4

論文281 は、量子鍵配送の安全性が計算量ではないことを 25% という数で示した。本稿はその位置づけを三つの根拠の中に置く——三つ目の根拠であり、一つ目とは階級が違う。

観察 6.5

正直に書くべき点——現実の暗号はほとんど破られていない。破られるのは実装・鍵管理・乱数・サイドチャネルであって、根拠そのものではない——本稿は根拠の型だけを扱っており、実務の安全とは別の話である。

7. 点呼と結び

1. 根拠は三つ（検算2.1）：依存先が三つとも違う。
2. 一つ目だけが時間で弱る（観察2.3）：相対的だから。
3. 量子が壊すのは一つだけ（検算3.1）：三分の一。
4. $I(M; C) = 0$ が厳密（検算3.3）：取り出す情報が無い。
5. RSA 2048 で比 $10^{25.3}$ （検算4.1）：鍵長で開く。
6. 古典 2^{128} には 2538 bit（検算4.3）：伸ばせば効く。
7. 量子側は 8 倍で 512 倍（検算4.4）：伸ばしても効かない。
8. AES-128 は実効 64 bit（検算5.1）：256 なら 128。
9. 平方根は鍵長で埋まる（観察5.4）：2 倍で取り返せる。
10. 壊すのに要るものの階級が違う（観察6.2）：計算機か、恒等式か、法則か。

結び：「この暗号は安全である」は、三つの別の根拠のどれかに立っている——計算量的安全（難しい）、情報理論的安全（情報が無い）、物理的安全（測れば壊れる）である。量子計算機が壊すのは一つ目だけである——「量子計算機が暗号を破る」という一文は、三分の一しか当たっていない。壊れ方は確かに劇的である——RSA 2048 bit で古典と量子の手間の比は $10^{25.3}$ 、4096 bit では $10^{36.3}$ である。そして鍵長では対抗できない——古典に対しては 2538 bit で 2^{128} 相当まで行けるのに、量子側は鍵長を 8 倍にしても手間が 512 倍にしかならない。対称鍵は事情が違う——グローバーは平方根しか稼がないので、AES-256 にすれば実効 128 bit で足りる。分けるものは一つ——その安全が、難しさに立っているか、情報の不在に立っているか。難しさは計算機で動く。 $I(M; C) = 0$ は動かない。正確に言えばこうである——量子計算機は、難しさに立つ暗号を破る。

参考文献

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. 山岸勇輝 (2026). 割り当てられた領域と、その中の自由 — 同じ韻を踏む六つの別根のセンス [論文112]. Zenodo. 10.5281/zenodo.21962834
8. 山岸勇輝 (2026). 「情報量」は四つあり、要るものが違う [論文252]. Zenodo. 10.5281/zenodo.22161148
9. 山岸勇輝 (2026). 複製できないのに、訂正はできる [論文281]. Zenodo. 10.5281/zenodo.22171058
10. 山岸勇輝 (2026). 分離は、長さの平方根でしか良くならない [論文294]. Zenodo. 10.5281/zenodo.22171603

— *From thinking to syncing.* —

山岸 勇輝 (Yuuki YAMAGISHI)

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