

「鍵長が半分になる」は二つあり、片方は量子計算機を待たない

— 23 人で誕生日が重なる確率は **0.507297** — 64 ビットの衝突は 5.06×10^9 個で起きる — [論文318]

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

論文305 は、量子計算機が対称鍵の実効長を半分にすると示した（グローバー）。本稿が問うのは、半分になる道はそれだけかである——答は、もう一本あり、そちらは古典で足りるである。新しい数学定理も新しい法則も主張しない。第一に、23 人で半分以上を超える。同じ誕生日の組がある確率は **0.507297**（第2節）。第二に、これが本稿の芯である。必要な個数は N ではなく $\sqrt{N}$ に比例する—— $1.1774\sqrt{N}$ （第3節）。第三に、64 ビットなら 5.06×10^9 個で衝突する（第3節）。第四に、これは量子計算機を待たない。古典の計算機で、いま起きている（第4節）。第五に、二つの半分は別根である。グローバーは探索、誕生日は衝突を半分にする（第5節）。第六に、分離子は「一つを当てるのか、二つを一致させるのか」である（第6節）。

本稿の射程（射程注記）：新しい数学定理も新しい法則も主張しない——誕生日のパラドックス、誕生日限界、衝突耐性が鍵長の半分であること、グローバーの二次加速は、いずれも標準的である。暗号を作らない——使うのは一つの積と、一つの平方根だけである。ハッシュ関数の設計を論じない——どの関数が安全かは扱わない。出力長だけから出る限界を見る。既存の攻撃を評価しない——MD5 や SHA-1 の実際の破られ方（差分攻撃）には立ち入らない。誕生日限界は下限であって、実際の攻撃はそれより速いことがある。量子計算機の実現可能性を論じない——論文305 が扱った。本稿は比較のために引くだけである。確率論を作らない——近似式 $1.1774\sqrt{N}$ の導出には立ち入らない。既刊との関係：論文305 は「安全の根拠は三つあり、量子計算機が壊すのは一つだけ」と示し、グローバーで対称鍵の実効長が半分になることを表にした（ $128 \rightarrow 64$ 、 $256 \rightarrow 128$ ）——本稿は同じ「半分」が、量子とは無関係にもう一本の道から出ることを示す。305 が探索の側、本稿が衝突の側である。論文281 は複製できないのに訂正はできると示した——同じ暗号の家系であり、本稿はハッシュの側に立つ。論文190 は「稀」が対数の目盛りで測ると示した——本稿の $\sqrt{N}$ は対数で半分になるという、その系である。論文300 は同根か別根かは判定できると示した——本稿は二つの「半分」にその基準を当てる。論文316 は同じ整数を三つの数え方が返すと示した——本稿は同じ「半分」を二つの機構が返すという、同じ型である。加えたのは人数ごとの一致確率を計算したこと、23 人で **0.507297** と出したこと、出力長ごとに必要な個数を $1.1774\sqrt{N}$ で並べたこと、グローバーの半分と誕生日の半分以上を論文300 の基準で別根と判定したことである。

1. 記法と問い

事実（論文305）：グローバーの探索は 2^n を $2^{n/2}$ にする。だから対称鍵 256 ビットの実効長は 128 ビットになる——量子計算機が要る。

問い：半分になる道は、それだけなのか。

観察 1.1

答はもう一本あるである——そしてそちらは量子計算機を待たない。

2. 23 人で、半分以上を超える

設定： n 人の誕生日が独立に一様（365 日）とする。全員が違う確率は $\prod_{i=0}^{n-1} (365 - i) / 365$ である。

検算 2.1：

人数	同じ誕生日の組がある確率
10	0.116948
20	0.411438
23	0.507297
30	0.706316
50	0.970374
70	0.999160

観察 2.2

23 人で半分以上を超える。365 日あるのに、23 人しか要らない——直感は 180 人あたりを答えるが、その手前で八割方終わっている。

観察 2.3

ずれの理由は数えているものが違うことである。人の数ではなく、組の数が効く——23 人なら組は $\binom{23}{2} = 253$ 通りあり、365 と同じ桁である。

観察 2.4

「自分と同じ誕生日の人がいるか」なら話は別である。そちらは n に比例し、半分を超えるのに 253 人 要る——同じ「誕生日が重なる」が二つの問いを指している。

3. 芯： $\sqrt{N}$ に比例する

設定： N 通りの値をとるハッシュに、無作為な入力を M 個入れる。組の数は $\binom{M}{2} \simeq M^2/2$ で、一致確率がおよそ $1/2$ になるのは $M \simeq 1.1774\sqrt{N}$ のときである。

検算 3.1：

出力長	$N = 2^n$	衝突が 50% になる個数 $1.1774\sqrt{N}$
32 ビット	4.295×10^9	7.716×10^4
64 ビット	1.845×10^{19}	5.057×10^9
128 ビット	3.403×10^{38}	2.172×10^{19}
256 ビット	1.158×10^{77}	4.007×10^{38}

観察 3.2

これが本稿の芯である。必要な個数は N ではなく $\sqrt{N}$ に比例する——指数が半分になる。

観察 3.3

32 ビットは 7.7 万個で衝突する。いまの計算機なら一瞬である——43 億通りあっても、7.7 万個で足りる。

観察 3.4

64 ビットでも 5.06×10^9 個である。50 億個は現実に用意できる量——64 ビットのハッシュは、衝突耐性としては使えない。

観察 3.5

正直に書くべき点——誕生日限界は下限である。実際の攻撃は関数の構造を突いてもっと速いことがある——本稿は出力長だけから出る限界を書いており、個々の関数の強さは扱わない。

4. これは、量子計算機を待たない

検算 4.1：二つの「半分」を並べる。

	何を半分にするか	要る計算機	いつから
グローバー（論文305）	探索の指数	量子	まだ
誕生日（本稿）	衝突の指数	古典	最初から

観察 4.2

下の行は、いま起きている。SHA-256 の衝突耐性ははじめから 128 ビットであり、量子計算機ができて変わらない——もう半分になっているものは、もう一度は半分にならない。

観察 4.3

だから設計の作法が違う。「128 ビットの安全性が欲しい」なら、探索に対しては 128 ビット、衝突に対しては 256 ビットの出力が要る——同じ要求に、二つの答が要る。

観察 4.4

論文305 は「鍵長では対抗できない」と書いた（RSA について）。ハッシュでは対抗できる——出力長を倍にすれば衝突耐性も倍になるからである。同じ「長さを増やす」が、片方では効かず、他方では効く。

5. 二つの半分は、別根である

検算 5.1：論文300 の判定基準を当てる。

基準	結果
恒等性を保つ対応があるか	いいえ。振幅増幅と鳩の巣に翻訳は無い
同じ量が入っているか	いいえ。量子の回数 対 組の数
一方から他方が出るか	いいえ。片方は量子力学、他方は数え上げ
値（指数の半減）は一致するか	はい。どちらも $n \rightarrow n/2$

観察 5.2

三つ「いいえ」、一つ「はい」である。機構は別根で、指数の半減だけが同じ——論文316 が「同じ整数を三つの数え方が返す」と書いたのと同じ型である。

観察 5.3

なぜ両方とも「半分」なのか。どちらも平方根が出るからである——グローバーは振幅の二乗が確率だから、誕生日は組の数が個数の二乗だから。二乗が出る場所が違う。

観察 5.4

論文190 は「稀」は対数の目盛りで測ると書いた。平方根は、対数の目盛りでは半分である——だからどちらも「ビットが半分」と言える。

6. 分離子：一つを当てるのか、二つを一致させるのか

観察 6.1

分離子——一つのあたりを探すのか、二つの一致を探すのか。

探すもの	手間	例
指定された一つ（原像）	N	与えられた値になる入力を探す
どれでもいい二つ（衝突）	$\sqrt{N}$	同じ値になる入力の組を探す

観察 6.2

二行目は、答を選べる。どの組でもよいので当たりが $M^2/2$ 通りある——自由度が手間を平方根にする。

観察 6.3

これは第2節の二つの誕生日問題と同じ分岐である。「自分と同じ人」は指定された一つ（253 人要る）、「誰かと誰か」はどれでもいい二つ（23 人でよい）——11 倍の差が、この分岐から出ている。

観察 6.4

最後に一つ——「ビット数」は一つの数ではない。同じ 256 ビットが、原像に対しては 256、衝突に対しては 128、量子探索に対しては 128——何に対する強さかを言わないかぎり、ビット数は数を持たない。論文306 が「基本単位の個数は約束である」と書いたのと同じ場所で、数の身分が文脈で決まっている。

7. 点呼と結び

1. 23 人で 0.507297（検算2.1）：365 日あるのに。
2. 効くのは組の数（観察2.3）： $\binom{23}{2} = 253$ 。

3. 「自分と同じ」なら **253** 人（観察2.4）：11 倍違う。
4. 必要数は $1.1774\sqrt{N}$ （検算3.1）：指数が半分。
5. **32** ビットは **7.7** 万個（観察3.3）：一瞬である。
6. **64** ビットは 5.06×10^9 （観察3.4）：用意できる量。
7. 誕生日限界は下限（観察3.5）：実攻撃はもっと速いことがある。
8. 古典で足りる（検算4.1）：量子計算機を待たない。
9. 三「いいえ」一「はい」（検算5.1）：機構は別根。
10. ビット数は一つの数でない（観察6.4）：何に対する強さか。

結び：論文305は、グローバーが対称鍵の実効長を半分にすると示した（256 → 128）。半分になる道はもう一本あり、そちらは量子計算機を待たない。**365** 日あるのに、**23** 人で同じ誕生日の組がある確率は **0.507297**——効いているのは人の数ではなく組の数で、**23** 人なら $\binom{23}{2} = 253$ 通り、**365** と同じ桁である。そして必要な個数は N ではなく $\sqrt{N}$ に比例する—— $1.1774\sqrt{N}$ であり、**32** ビットは **7.7** 万個、**64** ビットは 5.06×10^9 個で衝突する。**50** 億個は現実に用意できる。これは古典の計算機で、最初から起きている——SHA-256 の衝突耐性ははじめから **128** ビットであり、もう半分になっているものは、もう一度は半分にならない。二つの半分は別根である——論文300の基準で三つ「いいえ」一つ「はい」。どちらも平方根が出るのは同じだが、二乗が出る場所が違う（グローバーは振幅、誕生日は組）。分けるものは一つ——指定された一つを当ててるのか、どれでもいい二つを一致させるのか。答を選べるのが、手間を平方根にする。最後に一つ——「ビット数」は一つの数ではない。同じ **256** が、原像には **256**、衝突には **128**、量子探索には **128** である。何に対する強さかを言わないかぎり、ビット数は数を持たない。

参考文献

1. von Mises, R. (1939). Über Aufteilungs- und Besetzungswahrscheinlichkeiten. *Revue de la Faculte des Sciences de l'Universite d'Istanbul*, 4.
2. Yuval, G. (1979). How to Swindle Rabin. *Cryptologia*, 3(3).
3. van Oorschot, P. C. and Wiener, M. J. (1999). Parallel Collision Search with Cryptanalytic Applications. *Journal of Cryptology*, 12(1).
4. Grover, L. K. (1996). A Fast Quantum Mechanical Algorithm for Database Search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*.
5. Stevens, M. et al. (2017). The First Collision for Full SHA-1. In *Advances in Cryptology — CRYPTO 2017*. Cham: Springer.
6. 山岸勇輝 (2026). 「稀」は、対数の目盛りで測る [論文190]. Zenodo. 10.5281/zenodo.22106182
7. 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
8. 山岸勇輝 (2026). 三百本目の点呼——同根か別根かは、判定できる [論文300]. Zenodo. 10.5281/zenodo.22171914

9. 山岸勇輝 (2026). 「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 [論文305]. Zenodo. 10.5281/zenodo.22172118
10. 山岸勇輝 (2026). 「基本」単位の個数は、約束である [論文306]. Zenodo. 10.5281/zenodo.22172149
11. 山岸勇輝 (2026). 同じ整数を、三つの別の数え方が返す [論文316]. Zenodo. 10.5281/zenodo.22208229

— *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)