

A Key Halves for Two Different Reasons, and One of Them Is Not Waiting for a Quantum Computer

— Twenty-Three People Share a Birthday with Probability **0.507297** — A **64**-Bit Hash Collides at **5.06×10^9**

Inputs — [Paper 318]

Yuuki YAMAGISHI (山岸 勇輝)

Yamagishi Complexity Torus Lab, Japan

August 2026

— *From thinking to syncing.* —

Abstract

Paper 305 showed that a quantum computer halves the effective length of a symmetric key (Grover). This paper asks whether that is the only road to halving—the answer is there is another, and it needs only a classical machine. No new mathematical theorem and no new law is claimed. First, twenty-three people pass one half. The chance of a shared birthday is **0.507297** (Section 2). Second, this is the core of the paper. The count needed goes as $\sqrt{N}$, not N — $1.1774\sqrt{N}$ (Section 3). Third, a **64**-bit hash collides at **5.06×10^9** inputs (Section 3). Fourth, this is not waiting for a quantum computer. It is happening now, on classical machines (Section 4). Fifth, the two halvings are distinct roots. Grover halves search, the birthday bound halves collision (Section 5). Sixth, the separator is whether one target is named or any two must merely agree (Section 6).

Scope of this paper (scope note): No new mathematical theorem and no new law is claimed—the birthday paradox, the birthday bound, collision resistance being half the output length, and Grover’s quadratic speed-up are all standard. We do not build cryptography—all we use is one product and one square root. We do not discuss hash design—which functions are sound is not treated. Only the limit that follows from the output length. We do not assess existing attacks—the actual breaks of MD5 and SHA-1 (differential attacks) are not entered. The birthday bound is a floor, and real attacks are sometimes faster. We do not discuss whether quantum computers will be built—Paper 305 treated that; here it is quoted for comparison. We do not build probability theory—the derivation of $1.1774\sqrt{N}$ is not entered. Relation to earlier papers: Paper 305 showed that security rests on three grounds and a quantum computer breaks one, tabulating Grover halving symmetric key lengths ($128 \rightarrow 64$, $256 \rightarrow 128$)—this paper shows the same halving arriving by a second road that has nothing to do with quantum mechanics. 305 stands on the search side; this paper on the collision side. Paper 281 showed that what cannot be copied can still be corrected—the same cryptographic family, with this paper on the hashing side. Paper 190 showed that “rare” is measured on a logarithmic scale—the $\sqrt{N}$ here is that scale’s word for halving. Paper 300 showed that whether two things share a root is decidable—this paper applies those criteria to the two halvings. Paper 316 showed three counts returning one integer—this paper shows two mechanisms returning one halving, the same form. What is added is computing the coincidence probability by group size, giving 0.507297 at twenty-three, tabulating the needed count as $1.1774\sqrt{N}$ by output length, and adjudicating Grover’s halving and the birthday halving as distinct roots by Paper 300’s criteria.

1. Notation and the Question

Fact (Paper 305): Grover’s search turns 2^n into $2^{n/2}$. So a 256-bit symmetric key has an effective length of 128 bits—and a quantum computer is required.

Question: Is that the only road to halving?

Observation 1.1

The answer is there is another—and it is not waiting for a quantum computer.

2. Twenty-Three People Pass One Half

Setting: Take n birthdays, independent and uniform over 365 days. The chance that all differ is $\prod_{i=0}^{n-1} (365 - i)/365$.

Check 2.1:

People	Chance that some pair shares a birthday
10	0.116948
20	0.411438
23	0.507297
30	0.706316
50	0.970374
70	0.999160

Observation 2.2

Twenty-three pass one half. There are 365 days and only 23 people are needed——intuition answers around 180, and by then it is long over.

Observation 2.3

The gap comes from counting the wrong thing. What acts is the number of pairs, not of people——23 people give $\binom{23}{2} = 253$ pairs, the same order as 365.

Observation 2.4

“Does anyone share MY birthday” is a different question. That one grows as n , and needs 253 people to pass one half——one phrase, “a shared birthday”, covering two questions.

3. The Core: It Goes as $\sqrt{N}$

Setting: Feed M random inputs to a hash with N possible outputs. The number of pairs is $\binom{M}{2} \simeq M^2/2$, so the chance of a collision reaches about one half at $M \simeq 1.1774\sqrt{N}$.

Check 3.1:

Output length	$N = 2^n$	Inputs for a 50% collision, $1.1774\sqrt{N}$
32 bits	4.295×10^9	7.716×10^4
64 bits	1.845×10^{19}	5.057×10^9
128 bits	3.403×10^{38}	2.172×10^{19}
256 bits	1.158×10^{77}	4.007×10^{38}

Observation 3.2

This is the core of the paper. The count goes as $\sqrt{N}$ and not N —the exponent halves.

Observation 3.3

32 bits collide at 77 thousand. On any modern machine that is instantaneous—four billion possibilities, and 77 thousand suffice.

Observation 3.4

Even 64 bits need only 5.06×10^9 . Five billion is an amount one can actually assemble—a 64-bit hash is unusable as collision resistance.

Observation 3.5

A point to write honestly—the birthday bound is a floor. Real attacks exploit the function’s structure and are sometimes faster—this paper gives the limit that follows from output length alone, not the strength of any particular function.

4. This Is Not Waiting for a Quantum Computer

Check 4.1: The two halvings side by side.

	What halves	Machine needed	Since when
Grover (Paper 305)	the search exponent	quantum	not yet
Birthday (this paper)	the collision exponent	classical	always

Observation 4.2

The second row is happening now. SHA-256’s collision resistance has always been 128 bits, and a quantum computer will not change it——what is already halved is not halved again.

Observation 4.3

So the design rule differs. To want “128 bits of security” is to want 128 bits of output against search and 256 against collision——one requirement, two answers.

Observation 4.4

Paper 305 wrote that key length cannot keep up (for RSA). For hashes it can——double the output and the collision resistance doubles. The same “make it longer” fails in one place and works in the other.

5. The Two Halvings Are Distinct Roots

Check 5.1: Applying Paper 300’s criteria.

Criterion	Result
Is there a correspondence preserving identities?	no. Amplitude amplification does not translate into pigeonholes
Do the same quantities appear?	no. Quantum iterations against a count of pairs
Does one follow from the other?	no. One is quantum mechanics, the other counting
Do the values agree?	yes. Both give $n \rightarrow n/2$

Observation 5.2

Three noes and one yes. Distinct mechanisms, with only the halved exponent shared—the same form as Paper 316’s three counts returning one integer.

Observation 5.3

Why is it a half in both cases? Because a square root appears in both—for Grover because probability is the square of an amplitude, for the birthday bound because the number of pairs is the square of the count. The squaring happens in different places.

Observation 5.4

Paper 190 wrote that “rare” is measured on a logarithmic scale. On that scale a square root is a half—which is why both can be phrased as “half the bits”.

6. Separator: One Named Target, or Any Two Agreeing

Observation 6.1

Separator—whether a single named target is sought, or any two must merely agree.

What is sought	Work	Example
one named value (preimage)	N	find an input hashing to a given value
any two that agree (collision)	$\sqrt{N}$	find any pair with the same value

Observation 6.2

The second row gets to choose its answer. Any pair will do, so there are $M^2/2$ ways to win—that freedom is what takes the square root.

Observation 6.3

This is the same branch as the two birthday questions of Section 2. “Anyone sharing mine” names a target (253 people); “any two of us” does not (23 suffice)—the factor of 11 comes from this branch.

Observation 6.4

One last thing—“how many bits” is not one number. The same 256 is 256 against preimage, 128 against collision, 128 against quantum search—until one says what it is strong against, a bit count carries no number. The same place as Paper 306’s “how many base units there are is a promise”: the standing of a number is fixed by its context.

7. Roll Call and Closing

1. **0.507297** at twenty-three (Check 2.1): **With 365 days available.**
2. Pairs are what act (Observation 2.3): $\binom{23}{2} = 253$.
3. “Mine” needs **253 people** (Observation 2.4): **A factor of 11.**
4. The count is $1.1774\sqrt{N}$ (Check 3.1): **The exponent halves.**
5. **32 bits at 77 thousand** (Observation 3.3): **Instantaneous.**
6. **64 bits at 5.06×10^9** (Observation 3.4): **An assemblable amount.**
7. **The bound is a floor** (Observation 3.5): **Real attacks can be faster.**
8. **Classical suffices** (Check 4.1): **Not waiting for quantum.**
9. **Three noes, one yes** (Check 5.1): **Distinct mechanisms.**
10. **A bit count is not one number** (Observation 6.4): **Strong against what?**

Closing: Paper 305 showed Grover halving the effective length of a symmetric key ($256 \rightarrow 128$). There is a second road to that halving, and it is not waiting for a quantum computer. With 365 days available, twenty-three people share a birthday with probability **0.507297**—what acts is not the number of people but the number of pairs: 23 people give $\binom{23}{2} = 253$, the same order as 365. And the count needed goes as $\sqrt{N}$, not N — $1.1774\sqrt{N}$, so 32 bits collide at 77 thousand inputs and 64 bits at 5.06×10^9 . Five billion is an amount one can actually assemble. This happens on classical machines and always has—SHA-256’s collision resistance has always been 128 bits, and what is already halved is not halved again. The two halvings are distinct roots—Paper 300’s criteria give three noes and one yes. A square root appears in both, but the squaring happens in different places: an amplitude for Grover, a count of pairs for the birthday bound. One thing separates them—whether a single named target is sought, or any

two must merely agree. The freedom to choose the answer is what takes the square root. One last thing——“how many bits” is not one number. The same 256 is 256 against preimage, 128 against collision and 128 against quantum search; until one says what it is strong against, a bit count carries no number.

References

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. Yamagishi, Y. (2026). “Rare” Is Measured on a Logarithmic Scale [Paper 190]. Zenodo. 10.5281/zenodo.22106182
 7. Yamagishi, Y. (2026). It Cannot Be Copied, Yet It Can Be Corrected [Paper 281]. Zenodo. 10.5281/zenodo.22171058
 8. Yamagishi, Y. (2026). The Three Hundredth Census: Whether Two Things Share a Root Is Decidable [Paper 300]. Zenodo. 10.5281/zenodo.22171914
 9. Yamagishi, Y. (2026). Security Rests on Three Grounds, and a Quantum Computer Breaks Only One [Paper 305]. Zenodo. 10.5281/zenodo.22172118
 10. Yamagishi, Y. (2026). How Many “Base” Units There Are Is a Promise [Paper 306]. Zenodo. 10.5281/zenodo.22172149
 11. Yamagishi, Y. (2026). The Same Integer Comes Back from Three Different Counts [Paper 316]. Zenodo. 10.5281/zenodo.22208229
-

— 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)