同じ演算が、順は多項式・逆は指数である——ただし比が大きいだけでは足りない

— 法 $2^{127}-1$ で鍵交換を実際に行い、両側が同じ共有秘密に達することを確かめた — 分離子は、逆問題が易しいか難しいかである — [論文676]

山岸 勇輝 (Yuuki YAMAGISHI)
Yamagishi Complexity Torus Lab, Japan｜山岸勇輝ラボ
2026年9月

— From thinking to syncing. —

要旨

公開の場で数を交換するだけで、二人だけが知る秘密を作れる。同じ演算が、順方向は易しく逆方向は難しいからである。その易しさと難しさを実際に数え、比がどれだけあれば安全と言えるのかを見る。新しい定理も法則も主張しない。 第一に、手続きは実際に動く——法 $2^{127}-1$ で鍵交換を行い、両側がそれぞれの計算から同じ共有秘密に達することを確かめた（第2節）。 第二に、順と逆の手間は桁で違う——作る側は約 **254** 回の乗算、破る側（平方根の攻撃）は約 1.304382×10^{19} 回で、比は 5.135361×10^{16} 倍である（第2節）。 第三に、これが本稿の芯である。比が大きいだけでは足りない——その 5.135361×10^{16} 倍という比があっても、毎秒 **1** 兆回の機械なら **0.413334** 年で破れてしまう（第3節）。 第四に、桁を **2** 倍にすると、二つの側の効き方が違う——作る手間は **2.000000** 倍にしかならないのに、破る手間は 1.304382×10^{19} 倍になり、破るのに要る時間は 5.391449×10^{18} 年になる（第3節）。 第五に、だから鍵長は「比」ではなく「絶対の大きさ」で決める——比は **127 bit** でも **254 bit** でも同じ形で効くが、破るのに要る時間は **0.413334** 年と 5.391449×10^{18} 年に分かれる（第3節）。 第六に、分離子は、逆問題が易しいか難しいかである——難しさに賭けているのであって、不可能性に賭けているのではない（第4節）。 キーワード：鍵交換、離散対数、一方向性、計算量、公開鍵暗号、鍵長。

本稿の射程（射程注記）：新しい定理も法則も主張しない——公開の場での鍵交換（ディフィー＆ヘルマン 1976）、離散対数の難しさ、平方根の手間で解く攻撃は、いずれも既知である（メネゼス、ヴァン・オールショット＆ヴァンストーン 1996）。方式を評価しない——どの群を使うべきか、楕円曲線か有限体かは主題ではない。具体的な製品や規格も名指さない。認証を扱わない——中間者攻撃と、それを防ぐ認証の仕組みは主題ではない。鍵交換そのものの数だけを見る。量子計算機を扱わない——量子による加速は論文305 の側であり、本稿は古典の手間だけを数える。実装を論じない——乱数の質、サイドチャネル、実装の誤りは主題ではない。手間の見積もりは代表値である——作る側を 2 桁ぶんの乗算、破る側を群の大きさの平方根とするのは標準的な見積もりであり、実際の攻撃はこれより速い場合も遅い場合もある。既刊との関係：論文305 は「安全」の根拠が三つ（情報理論的・計算量的・物理的）あり、量子計算機が壊すのは一つだけであることを示した——本稿はそのうち計算量的な根拠の内側に入り、順と逆の手間を一つの手続きで数える。論文304 は「容量」が無限長でしか達成できない数であることを示した——そこでも「達成できる」と「いくらでも近づける」が分かれた。ここでは「破れない」と「破るのに時間がかかる」が分かれる。加えたのは、実際に共有秘密を計算して一致を確かめたこと、順と逆の手間の比を数にしたこと、比が大きくても 127 bit では 0.413334 年で破れることを示したこと、桁を倍にしたときの二つの側の効き方を並べたこと、分離子を「逆問題が易しいか難しいか」に置いたことである。

1. 記法と問い

設定：素数 p と生成元 g を公開する。二人はそれぞれ秘密の数 a、b を選び、g^a、g^b を公開する。共有秘密は次で一致する。

$$(g^b)^a \bmod p = (g^a)^b \bmod p$$

作るのは繰り返し二乗で、乗算の回数は桁数に比例する。破るには g^a から a を求める（離散対数）必要がある。

問い：安全性は何に賭けているのか——不可能性か、それとも手間の差か。

2. 順と逆を数える

計算 2.1：法 $2^{127}-1$ で鍵交換を行った。両側の計算はそれぞれ別の秘密から出発し、同じ共有秘密に達した。

計算 2.2：手間を数えた。

法の桁	作る側（乗算の回数）	破る側（回数）
127 bit	**254**	1.304382×10^{19}
254 bit	**508**	1.701412×10^{38}
508 bit	**1016**	2.894802×10^{76}

127 bit では、破る側は作る側の 5.135361×10^{16} 倍である。

> **観察 2.3**
>
> 同じ演算の二つの向きが、桁で分かれている。べき乗を計算するのは桁数に比例する仕事だが、そこから指数を取り出すのは群の大きさの平方根に比例する仕事である——一つの演算の中に、多項式と指数が同居している。

3. 比が大きいだけでは足りない

計算 3.1：毎秒 **1** 兆回を試せる機械で、破るのに要る時間を出した。

法の桁	破るのに要る時間
127 bit	**0.413334** 年
254 bit	5.391449×10^{18} 年
508 bit	9.173075×10^{56} 年

> **観察 3.2**
>
> これが本稿の芯である。比は同じでも、答は分かれる。**127 bit** でも比は 5.135361×10^{16} 倍あり、「作るのは易しく破るのは難しい」という形は保たれている。それでも **0.413334** 年で破れる——安全であるためには、比が大きいことに加えて、破る側の絶対の回数が大きくなければならない。

計算 3.3：桁を **2** 倍にすると、作る手間は **2.000000** 倍にしかならないのに、破る手間は 1.304382×10^{19} 倍になる。

観察 3.4

守る側が有利なのは、ここである。桁を増やす費用は線形で、攻める側の費用は指数的に増える——だから「もう少し長くする」という同じ一手が、二つの側で桁違いの意味を持つ。

4. 分離子

観察 4.1

分離子は、逆問題が易しいか難しいかである。本稿が数えたのは手間であって、不可能性ではない。逆を解く方法が一つ見つかれば、比はそのぶん小さくなる——安全性は「難しさ」に賭けており、その賭けの大きさは数で言える。

観察 4.2

論文305 と並べる。**305** は安全の根拠を三つに分け、情報が無いものはどんな計算機でも計算できないことを最も強い根拠として置いた——本稿はその隣の、計算量に賭ける側を数えた。**0.413334** 年という数は、その賭けが桁の選び方に依ることを示している。

観察 4.3

論文304 と並べる。**304** は「容量」が無限長でしか達成できない数であることを示した——そこでは「達成」と「近づく」が分かれた。ここでは「破れない」と「破るのに時間がかかる」が分かれる。どちらも、極限の語と有限の実務の間にある段差である。

観察 4.4

言わないこと。中間者攻撃も、群の選び方も、量子計算機も扱っていない。破る側の手間は標準的な見積もりである——示したのは、同じ演算の二つの向きの手間の差と、その差だけでは安全が決まらないことである。

5. 点呼と結び

1. 両側が同じ秘密に達する（計算 2.1）：手続きが動く。
2. 作る **254** 回（計算 2.2）：桁数に比例。
3. 破る $\mathbf{1.304382 \times 10^{19}}$ 回（計算 2.2）：平方根の手間。
4. 比は $\mathbf{5.135361 \times 10^{16}}$ 倍（計算 2.2）：多項式と指数の同居。
5. **127 bit** は **0.413334** 年（計算 3.1）：本稿の芯。
6. **254 bit** は $\mathbf{5.391449 \times 10^{18}}$ 年（計算 3.1）：同じ比でも分かれる。
7. **508 bit** は $\mathbf{9.173075 \times 10^{56}}$ 年（計算 3.1）：桁の効き。
8. 作る手間は **2.000000** 倍（計算 3.3）：線形。
9. 破る手間は $\mathbf{1.304382 \times 10^{19}}$ 倍（計算 3.3）：指数。
10. 易しいか難しいか（観察 4.1）：分離子・論文305・論文304。

結び：鍵交換が成り立つのは、同じ演算の順方向が多項式で、逆方向が指数だからである。法 $2^{127} - 1$ で実際に共有秘密の一致を確かめ、作る側 **254** 回に対し破る側 1.304382×10^{19} 回、比 5.135361×10^{16} 倍を数えた。それでも毎秒 1 兆回の機械なら **0.413334** 年で破れる——比が大きいことは必要だが、足りない。要るのは破る側の絶対の大きさである。桁を **2** 倍にすると、作る手間は **2.000000** 倍のままで、破るのに要る時間は 5.391449×10^{18} 年になる——同じ一手が、二つの側で桁違いの意味を持つ。分離子は、逆問題が易しいか難しいかである。既刊との位置——論文305 が分けた三つの根拠のうち、計算量に賭ける側を数えた。論文304 と同じく、極限の語と有限の実務の間の段差である。正直に言えば——破る側の手間は標準的な見積もりであり、より速い方法が見つかれば比は縮む。

参考文献

1. Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory.
2. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.
3. 山岸勇輝 (2026). 『「容量」は、無限長でしか達成できない数である』[論文304]. Zenodo. 10.5281/zenodo.22172081
4. 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

— 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)