一回ごとに渡す情報が零のままでも、確信だけは積み上がる

— 偽者が一回だけ通る確率が 0.5 の形では、残る疑いは 10 回で 9.765625×10^{-4}、20 回で 9.536743×10^{-7}、30 回で 9.313226×10^{-10} になる — 分離子は、確信度と情報量が別の量であることである — [論文675]

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

「知っていることを、教えずに示す」という言い方は、矛盾しているように聞こえる。だが渡す情報と、相手が得る確信は、別の量である。一回ごとの情報が零のまま、確信だけがどう積み上がるかを数える。新しい定理も法則も主張しない。 第一に、残る疑いは、回数とともに指数的に小さくなる——偽者が一回通る確率が 0.5 の形では、残る疑いは 10 回で 9.765625×10^{-4}、20 回で 9.536743×10^{-7}、30 回で 9.313226×10^{-10} である（第2節）。 第二に、要る回数は、目標の桁数に比例する——千分の一未満に 9.965784 回、百万分の一未満に 19.931569 回、十億分の一未満に 29.897353 回（切り上げてそれぞれ 10・20・30 回）である（第2節）。 第三に、一回あたりの強さが違えば、要る回数は桁で変わる——一回あたり 0.999 で通ってしまう形では、同じ確信に 20713 回が要り、比は 692.800549 倍である（第2節）。 第四に、これが本稿の芯である。それでも、渡している情報は零のままである——一回ごとに相手が見る受け答えの分布が秘密に依らなければ、そこから得られる情報は 0 ビットで、n 回繰り返しても $0 \times n = 0$ ビットである（第3節）。 第五に、秘密を見せれば、一回で終わる——千通りのうちの一つという秘密をそのまま見せると 9.965784 ビットが一度に漏れ、確信は一回で 1 になる。同じ確信に、片方は 0 ビット、片方は 9.965784 ビットを払う（第3節）。 第六に、分離子は、確信度と情報量が別の量であることである——足しても増えない量と、足すと増える量が、同じ手続きの中に同居している（第4節）。 キーワード：ゼロ知識証明、対話証明、健全性の増幅、繰り返し、確信度、情報量。

本稿の射程（射程注記）：新しい定理も法則も主張しない——対話による証明、繰り返しによる健全性の増幅、ゼロ知識という概念は、いずれも既知である（ゴールドワッサー、ミカリ＆ラコフ 1989、ゴールドライヒ 2001）。方式を名指さない——どの問題に基づく方式か（グラフの同型、離散対数、近年の簡潔な証明系）は主題ではない。零知識であることを証明しない——受け答えの分布が秘密に依らないことは前提として置く。証明（模擬器の構成）は行わない。計算量の仮定に立ち入らない——一方向性の仮定や、計算量的な零知識と完全な零知識の区別は扱わない。実装を論じない——乱数の質、再送、サイドチャネルは主題ではない。既刊との関係：論文305は「安全」の根拠が三つあり、そのうち情報理論的なもの（情報が無いものはどんな計算機でも計算できない）が最も強いことを示した——本稿はその根拠の上で、情報を渡さずに確信だけを渡す手続きを数える。論文317は有意水準が「一回あたり」の約束であって研究あたりではないことを示した——ここでも約束は一回あたりで、繰り返すことで全体の保証が変わる。向きは逆で、317では繰り返しが保証を薄め、本稿では繰り返しが確信を濃くする。加えたのは、残る疑いと要る回数を二つの形で並べたこと、同じ確信に要る回数が692.800549倍違うことを示したこと、情報量0と確信の増加を同じ表に置いたこと、秘密をそのまま見せる場合（9.965784ビット）を対照に置いたこと、分離子を「確信度と情報量は別の量」に置いたことである。

1. 記法と問い

設定：証明する側は秘密を持ち、検証する側はそれを知らない。一回の受け答えで、秘密を持たない偽者が通ってしまう確率を p とする。n 回すべてを通る確率は次になる。

$$p^n, \qquad n \geq \frac{\log \varepsilon}{\log p}$$

ε は許す疑いの大きさである。いっぽう、検証する側が一回ごとに得る情報は、受け答えの分布が秘密に依らなければ0ビットである。

問い：確信が増えるなら、情報も増えているのではないか。

2. 確信の積み上がりを数える

計算2.1：一回あたり0.5で通る形について、残る疑いと確信を出した。

回数	残る疑い	確信
1	5.000000×10^{-1}	0.500000000
10	9.765625×10^{-4}	0.999023438
20	9.536743×10^{-7}	0.999999046
30	9.313226×10^{-10}	0.999999999

十億分の一未満にするのに要る回数は 29.897353 で、切り上げて 30 回である。千分の一未満なら 9.965784、百万分の一未満なら 19.931569 で、目標の桁数にちょうど比例する。

計算 2.2：一回あたり 0.999 で通ってしまう形（千通りから一つを当てる形）では、同じ十億分の一未満に 20712.9025 回、切り上げて 20713 回が要る。比は 692.800549 倍である。

> **観察 2.3**
>
> 一回あたりの強さが、費用を決める。どちらの形でも、確信は指数的に増える。違うのは底である——底が 1 に近いほど、同じ確信に要る回数は桁で増える。

3. 渡している情報は、零のままである

> **観察 3.1**
>
> これが本稿の芯である。検証する側が見るのは、毎回の受け答えである。その分布が秘密に依らないなら、一回の受け答えから秘密について得られる情報は 0 ビットである——0 ビットを n 回集めても $0 \times n = 0$ ビットで、増えない。それでも確信は $1 - p^n$ で増える。

計算 3.2：対照として、秘密（千通りのうちの一つ）をそのまま見せる場合を置いた。漏れる情報は 9.965784 ビットで、確信は一回で 1 になる。

観察 3.3

同じ確信に、二つの払い方がある。一方は 30 回の受け答えと 0 ビットの情報、他方は 1 回の提示と 9.965784 ビットの情報である——確信を買うのに、情報を払う必要はない。払っているのは回数である。

観察 3.4

同じ数が、別の場所にも出る。論文629 は、期待値が無限の賭けで胴元の資金を 10^k 円に限ったときの回数として $9.965784 \cdot 19.931569 \cdot 29.897353$ を出した。論文298 は、倍賭けの破産確率として $9.536743 \times 10^{-7} \cdot 9.313226 \times 10^{-10}$ を出した——どちらも $\log_2 10^k$ と 0.5^n という同じ定数であり、主題は別である。数が同じことは、同じ話であることを意味しない。

4. 分離子

観察 4.1

分離子は、確信度と情報量が別の量であることである。情報量は足し算で増える量で、受け答えが秘密に依らなければ一回あたり 0 である。確信は掛け算で増える量で、一回あたり p 倍ずつ疑いが減る——足しても増えない量と、掛けて増える量が、同じ手続きに同居している。

観察 4.2

論文305 と並べる。305 は、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、安全の三つの根拠のうち最も強いものとして置いた——本稿の手続きは、その最も強い根拠の上に確信を積む。計算の速さがどれだけ上がっても、0 ビットからは何も出てこない。

観察 4.3

論文317 と並べる。317 は、有意水準が一回あたりの約束であって研究あたりではないことを示した——ここでも約束は一回あたりである。ただし向きが逆で、317 では繰り返しが保証を薄め、本稿では繰り返しが確信を濃くする。同じ「一回あたり」という言葉が、二つの向きに働く。

> **観察 4.4**
>
> 言わないこと。零知識であることの証明も、方式の選択も、計算量の仮定も扱っていない——示したのは、確信の増え方と情報の増え方が別々に数えられることである。

5. 点呼と結び

1. 10 回で $\mathbf{9.765625 \times 10^{-4}}$（計算 2.1）：残る疑い。
2. 30 回で $\mathbf{9.313226 \times 10^{-10}}$（計算 2.1）：十億分の一未満。
3. 要る回数 **29.897353**（計算 2.1）：桁数に比例。
4. 0.999 の形では 20713 回（計算 2.2）：底が 1 に近い。
5. 比は **692.800549** 倍（計算 2.2）：一回あたりの強さ。
6. 情報は 0 ビットのまま（観察 3.1）：本稿の芯。
7. 秘密を見せれば **9.965784** ビット（計算 3.2）：一回で確信 1。
8. 同じ確信に二つの払い方（観察 3.3）：回数か情報か。
9. 同じ数が別の主題にも出る（観察 4.1）：論文629・論文298。
10. 確信度と情報量（観察 4.1）：分離子・論文305・論文317。

結び：教えずに示すことは、矛盾ではない。一回あたり 0.5 で通る形では、残る疑いは 10 回で 9.765625×10^{-4}、30 回で 9.313226×10^{-10} になり、十億分の一未満にするのに要る回数は 29.897353 である。一回あたり 0.999 の形なら同じ確信に 20713 回、692.800549 倍が要る——確信は掛け算で増え、その底が費用を決める。そのあいだ、渡している情報は 0 ビットのままである——秘密をそのまま見せれば 9.965784 ビットで一回で済むが、払っているものが違う。分離子は、確信度と情報量が別の量であることである。既刊との位置——論文305 が最も強いとした情報理論的な根拠の上に確信を積み、論文317 の「一回あたりの約束」が逆向きに働く場合を示した。正直に言えば——零知識であることは前提として置いており、その証明は行っていない。

参考文献

1. Goldreich, O. (2001). *Foundations of Cryptography: Basic Tools*. Cambridge University Press.
2. Goldwasser, S., Micali, S., & Rackoff, C. (1989). The Knowledge Complexity of Interactive Proof Systems. SIAM Journal on Computing.
3. 山岸勇輝 (2026).『勝率 99.9999% の戦略の期待値は、ちょうど 0 である』[論文298]. Zenodo. 10.5281/zenodo.22171857

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

5. 山岸勇輝 (2026). 『有意水準は「一回あたり」の約束であって、研究あたりではない』[論文317]. Zenodo. 10.5281/zenodo.22208819

6. 山岸勇輝 (2026). 『期待値が無限の賭けも、胴元の資金を 10^{12} 円に限れば約 **41** 円になる』[論文629]. Zenodo. 10.5281/zenodo.23014552

— 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)