The Information Handed Over Each Round Stays at Zero While the Confidence Piles Up

— Where an impostor passes a single round with probability 0.5, the doubt remaining is 9.765625×10^{-4} after 10 rounds, 9.536743×10^{-7} after 20 and 9.313226×10^{-10} after 30 — the separator is that confidence and information are different quantities — [Paper 675]

Yuuki YAMAGISHI (山岸 勇輝)
Yamagishi Complexity Torus Lab, Japan
September 2026

— From thinking to syncing. —

Abstract

“Showing that one knows without teaching it” sounds like a contradiction. But what is handed over and what the other party comes to believe are different quantities.How confidence piles up while the information per round stays at zero is counted.No new theorem or law is claimed. First, the remaining doubt falls exponentially with the number of rounds——where an impostor passes one round with probability 0.5, the doubt is 9.765625×10^{-4} after 10 rounds, 9.536743×10^{-7} after 20 and 9.313226×10^{-10} after 30 (Section 2). **Second, the number of rounds is proportional to the digits demanded——9.965784 rounds for less than one in a thousand, 19.931569 for one in a million and 29.897353 for one in a billion (rounded up, 10, 20 and 30)** (Section 2). **Third, a different strength per round changes the count by orders——where an impostor passes with probability 0.999, the same confidence takes 20713 rounds, a factor of 692.800549** (Section 2). **Fourth, and this is the core. Through all of it, the information handed over stays at zero——if the distribution of exchanges the verifier sees does not depend on the secret, each round yields 0 bits about it, and n rounds yield $0 \times n = 0$ bits** (Section 3). **Fifth, showing the secret ends it in one ——revealing a secret that is one of a thousand leaks 9.965784 bits at once and brings confidence to 1 immediately. The same confidence costs 0 bits on one path and 9.965784 on the other** (Section 3). **Sixth, the separator is that confidence and information are different quantities——a quantity that does not grow when added and one that does live together inside one procedure** (Section 4). **Keywords**: zero-knowledge proof, interactive proof, soundness amplification, repetition, confidence, information content.

Scope of this paper (scope note): **No new theorem or law is claimed——interactive proofs, amplification of soundness by repetition and the notion of zero knowledge are all standard (Goldwasser, Micali and Rackoff 1989, Goldreich 2001).No scheme is named——which problem a scheme rests on, whether graph isomorphism, discrete logarithms or recent succinct systems, is not the subject.Zero knowledge is not proved——that the distribution of exchanges does not depend on the secret is assumed; no simulator is constructed.Complexity assumptions are not entered into——one-wayness, and the distinction between computational and perfect zero knowledge, are not treated.Implementation is not discussed——randomness, replay and side channels are not the subject.Relation to earlier papers**: **Paper 305 showed that "security" rests on three grounds and that the information-theoretic one, that what carries no information cannot be computed by any machine, is the strongest——this paper piles confidence on that ground.Paper 317 showed that a significance level is a promise per test and not per study——here too the promise is per round, and repetition changes the overall guarantee. The direction is opposite: in Paper 317 repetition thins the guarantee, and here it thickens the confidence.**What is added is **setting the remaining doubt and the required rounds side by side for two forms**, **showing that the same confidence costs 692.800549 times as many rounds in one of them**, **placing zero information beside growing confidence in one table**, **setting the outright disclosure (9.965784 bits) as a control**, and **placing the separator on confidence against information**.

1. Notation and the Question

Setting: **the proving side holds a secret and the verifying side does not know it. Let p be the probability that an impostor without the secret passes a single exchange. The probability of passing all n is**

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

where ε is the doubt one is willing to allow. Meanwhile, if the distribution of exchanges does not depend on the secret, each round gives the verifier 0 bits about it.

Question: **if confidence grows, must information not be growing too?**

2. Counting How Confidence Piles Up

Computation 2.1: **for the form in which an impostor passes with probability 0.5, the remaining doubt and the confidence were derived.**

rounds	remaining doubt	confidence
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

Reaching less than one in a billion takes 29.897353 rounds, rounded up to 30; one in a thousand takes 9.965784 and one in a million 19.931569, exactly in proportion to the digits demanded.

Computation 2.2: for the form in which an impostor passes with probability 0.999, one guess in a thousand, the same one in a billion takes 20712.9025 rounds, rounded up to 20713, a factor of 692.800549.

> **Observation 2.3**
>
> the strength per round sets the cost.In both forms the confidence grows exponentially; what differs is the base——the closer the base is to one, the more rounds the same confidence costs, by orders.

3. The Information Handed Over Stays at Zero

> **Observation 3.1**
>
> this is the core.What the verifier sees is the exchange each round. If its distribution does not depend on the secret, one round yields 0 bits about the secret——and 0 bits collected n times is $0 \times n = 0$ bits, which does not grow. The confidence nevertheless grows as $1 - p^{n}$.

Computation 3.2: as a control, revealing the secret outright, one of a thousand, leaks 9.965784 bits and brings the confidence to 1 in a single step.

Observation 3.3

the same confidence has two ways of being paid for.One is 30 exchanges and 0 bits; the other is one disclosure and 9.965784 bits——buying confidence does not require paying in information. What is paid is rounds.

Observation 3.4

the same numbers appear elsewhere.Paper 629 gave 9.965784, 19.931569 and 29.897353 as the number of tosses at which a bank limited to 10^k caps a game of infinite expectation. Paper 298 gave 9.536743×10^{-7} and 9.313226×10^{-10} as ruin probabilities under doubling——both are the same constants, $\log_2 10^k$ and 0.5^n, in different subjects. Sharing a number does not make it the same story.

4. The Separator

Observation 4.1

the separator is that confidence and information are different quantities.Information is a quantity that grows by addition, and is 0 per round when the exchanges do not depend on the secret. Confidence is a quantity that grows by multiplication, the doubt falling by a factor p each round——one that does not grow when added and one that grows when multiplied, inside a single procedure.

Observation 4.2

beside Paper 305.Paper 305 placed, as the strongest of three grounds, that what carries no information cannot be computed by any machine——the procedure here builds confidence on that strongest ground: however much faster computation becomes, nothing comes out of 0 bits.

Observation 4.3

beside Paper 317.Paper 317 showed that a significance level is a promise per test and not per study——here too the promise is per round, but the direction is reversed: there repetition thins the guarantee, and here it thickens the confidence. The same phrase, “per round”, works both ways.

Observation 4.4

what is not said.Neither a proof of zero knowledge, nor the choice of scheme, nor any complexity assumption is treated——what is shown is that the growth of confidence and the growth of information can be counted separately.

5. Roll Call and Closing

1. $\mathbf{9.765625 \times 10^{-4}}$ **after 10** (Computation 2.1): **the remaining doubt.**
2. $\mathbf{9.313226 \times 10^{-10}}$ **after 30** (Computation 2.1): **below one in a billion.**
3. **29.897353 rounds** (Computation 2.1): **in proportion to digits.**
4. **20713 rounds in the other form** (Computation 2.2): **a base close to one.**
5. **a factor of 692.800549** (Computation 2.2): **strength per round.**
6. **information stays at 0 bits** (Observation 3.1): **the core.**
7. **disclosure leaks 9.965784 bits** (Computation 3.2): **confidence 1 in one step.**
8. **two ways to pay** (Observation 3.3): **rounds or information.**
9. **the same numbers elsewhere** (Observation 3.4): **Papers 629 and 298.**
10. **confidence against information** (Observation 4.1): **the separator; Papers 305 and 317.**

Closing: **Showing without teaching is not a contradiction.Where an impostor passes with probability 0.5, the doubt falls to 9.765625×10^{-4} in 10 rounds and 9.313226×10^{-10} in 30, and less than one in a billion takes 29.897353 rounds.Where the impostor passes with 0.999, the same confidence takes 20713 rounds, 692.800549 times as many ——confidence grows by multiplication, and its base sets the cost.Throughout, the information handed over stays at 0 bits——revealing the secret would settle it in one step at 9.965784 bits, but the payment is of a different kind.The separator is that confidence and information are different quantities.Placed among the earlier papers——confidence is built on the information-theoretic ground Paper 305 called strongest, and the “per round” promise of Paper 317 is shown working in the opposite direction.To be honest——zero knowledge is assumed here and not proved.**

References

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. Yamagishi, Y. (2026). *A Strategy That Wins* $\mathbf{99.9999\%}$ *of the Time Has Expectation Exactly* $\mathbf{0}$ [Paper 298]. Zenodo. 10.5281/zenodo.22171857
4. Yamagishi, Y. (2026). *Security Rests on Three Grounds, and a Quantum Computer Breaks Only One* [Paper 305]. Zenodo. 10.5281/zenodo.22172118
5. Yamagishi, Y. (2026). *A Significance Level Is a Promise per Test, Not per Study* [Paper 317]. Zenodo. 10.5281/zenodo.22208819
6. Yamagishi, Y. (2026). *A Game with Infinite Expectation Has an Expectation of About* $\mathbf{41}$ *Once the Bank Is Limited to* $\mathbf{10^{12}}$ [Paper 629]. Zenodo. 10.5281/zenodo.23014552

— 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)