

It Cannot Be Copied, Yet It Can Be Corrected

— The Syndrome Tells **8** Bits about the Error and **0** Bits about the State — Eavesdropping Appears as the
Number **25%** by the Same Reasoning — [Paper 281]

Yuuki YAMAGISHI (山岸 勇輝)

Yamagishi Complexity Torus Lab, Japan

August 2026

— *From thinking to syncing.* —

Abstract

A quantum state cannot be copied (the no-cloning theorem). Yet quantum error correction works. To correct one must know the error; to know it one must measure; and measuring destroys the state—so it would seem. This paper asks why these two are compatible—the answer is that what is measured is not the state but the error. No new mathematical theorem and no new law is claimed. First, we count the bits the syndrome tells. Shor’s 9-qubit code tells **8** bits about the error and **0** bits about the logical state (Section 2). Second, the 5-qubit code saturates exactly. Against **16** syndromes there are **16** errors to correct—not one to spare (Section 3). Third, the same reasoning turns eavesdropping into a number. Under BB84 intercept-resend, the error rate is exactly **25%** (Section 4). Fourth, **25%** is 2.27 times the security limit. The one-way post-processing limit is **11.0028%**, so it is certain to be detected (Section 5). Fifth, checking **73** bits drops the miss probability below 10^{-9} . That is **0.75⁷³** (Section 5). Sixth, the separator is that security does not rest on computational cost. However fast computers become, **25%** stays **25%** (Section 6).

Scope of this paper (scope note): No new mathematical theorem and no new law is claimed—the no-cloning theorem, Shor’s 9-qubit code, the 5-qubit code, BB84, the 25% of intercept-resend, and the 11% of Shor–Preskill are all standard. We do not construct codes—all we count is the number of syndromes and the number of errors to be corrected. We do not prove the no-cloning theorem—we merely quote it. We give no security proof—the 11.0028% of Shor–Preskill is quoted as a number only, and we do not enter the proof. We do not discuss real quantum key distribution—loss, dark counts, multi-photon components, and device attacks are not treated at all. The 25% of this paper is a value for ideal intercept-resend only. We do not claim the best attack—intercept-resend is not the best attack. A cleverer attack obtains the same information at a lower error rate. 25% is a number for “how conspicuous a naive attack is”. We do not treat finite-key effects—the 0.75^{73} of Section 5 is the miss probability under full interception, not a complete assessment of statistical security. We do not discuss quantum computation—neither Shor’s factoring nor the threshold theorem is treated. Relation to earlier papers: Paper 163 separated “a good code exists” from “here is a good code”—this paper stands on the construction side and counts the syndromes of specific codes. Paper 252 counted four quantities called “information”—the 8 and the 0 counted here are the bits one and the same measurement returns about two different objects, a separation of objects, not of kinds of quantity. Paper 188 treated cases exactly determined by fewer measurements than unknowns—this paper is the converse: measuring exactly what is needed and nothing else. Paper 179 showed that “cannot be constructed” has distinct roots—no-cloning is one such “cannot construct,” and this paper uses as a premise that its root is linearity. Paper 68 read the qubit as a Hopf fibration—this paper counts the same qubit as a number of bits of information. What is added is counting the bits the syndrome tells, separated as “8 about the error, 0 about the state”, confirming that the 5-qubit code saturates exactly at $16 = 16$, setting beside it the fact that the same reasoning yields the 25% of BB84, and computing that 25% is 2.2722 times the security limit.

1. Notation, and Two Things That Should Not Coexist

The first: the no-cloning theorem—no operation copies an unknown quantum state.

The second: quantum error correction—an encoded state can be restored after an error enters.

Why they look incompatible: To correct, one must know which error entered. To know, one must measure. Measuring a quantum state destroys it.

The answer: What is measured is not the state. What is measured is the kind of error.

The method of this paper: We show this distinction by counting bits.

2. Counting the Bits the Syndrome Tells

Setting: We embed k logical qubits in n physical qubits. In a stabiliser code the number of generators is $n - k$, and each returns ± 1 .

Check 2.1: Shor’s 9-qubit code ($n = 9, k = 1$).

Quantity	Value
Physical qubits n	9
Logical qubits k	1
Number of generators $n - k$	8
Number of syndromes 2^8	256
Single-qubit errors to correct $1 + 3n$	28
Spare	228

Observation 2.2

The syndrome returns 8 bits. Those 8 bits tell which error entered where.

Observation 2.3

This is the core of the paper. The number of bits those 8 tell about the logical state is 0. The generators commute with the logical operators, so measuring them does not destroy the superposition of the logical state——nothing has been copied, and nothing has been peeked at.

Check 2.4: We count the same way for three codes.

Code	n	Generators	Syndromes	Errors to correct	About the state
Shor	9	8	256	28	0 bits
Steane	7	6	64	22	0 bits
5-qubit	5	4	16	16	0 bits

Observation 2.5

The rightmost column is 0 throughout. However large the code, the amount the syndrome tells about the state does not grow——this is why the two coexist.

3. The 5-Qubit Code Saturates Exactly

Setting: To distinguish errors by syndrome one needs syndromes $\geq$ errors to correct. For $k = 1$ and distance 3 this reads $1 + 3n \leq 2^{n-1}$ (the quantum Hamming bound).

Check 3.1:

n	$1 + 3n$	2^{n-1}	Possible?
3	10	4	No
4	13	8	No
5	16	16	Exactly
6	19	32	Spare
7	22	64	Spare
9	28	256	Spare

Observation 3.2

At $n = 5$ equality holds. The 16 syndromes correspond one-to-one to the 16 errors with none to spare——a perfect code.

Observation 3.3

$n = 4$ fails at $13 > 8$. Correcting one qubit error requires at least 5—here is an exact lower bound.

Observation 3.4

Paper 179 wrote that “cannot be constructed” has distinct roots. The root by which $n = 4$ cannot be constructed is counting—solving the inequality $1 + 3n \leq 2^{n-1}$ alone gives $n \geq 5$. No detail of quantum mechanics is needed.

4. The Same Reasoning Turns Eavesdropping into a Number

Setting: BB84. Alice picks one of two bases (rectilinear or diagonal) at random and sends a bit. Bob also picks a basis at random. Eve measures en route and resends what she measured (intercept-resend).

Check 4.1: We look only at cases where Bob’s basis matched Alice’s (after sifting).

Eve’s basis	Probability	State resent	Bob’s error rate
Matches Alice	$1/2$	Correct	0
Differs from Alice	$1/2$	Off by 45°	$1/2$
Total			$\frac{1}{2} \cdot 0 + \frac{1}{2} \cdot \frac{1}{2} = \mathbf{0.25}$

Observation 4.2

The error rate is exactly **25%**. Eve is conspicuous because she measured—exactly the obverse of Section 2, where measuring is not conspicuous.

Check 4.3: We count how much Eve obtained.

Quantity	Value
Probability Eve's bit is right	$\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \mathbf{0.75}$
Mutual information $1 - h(1/4)$	0.188722 bits

Observation 4.4

Eve gains only 0.19 bits per bit, yet leaves 25% errors. Her footprint is far too large for her take.

Observation 4.5

A point to write honestly——intercept-resend is not the best attack. A cleverer attack obtains the same information with fewer errors——25% is a number for “how conspicuous a naive attack is,” not a proof of security.

5. 25% Is 2.27 Times the Limit

Setting: Whether a key can be extracted at error rate q is set, for one-way post-processing, by $R = 1 - 2h(q)$ (Shor--Preskill).

Check 5.1:

Error rate q	$h(q)$	Key rate $R = 1 - 2h(q)$
0	0	+1.000000
0.01	0.080793	+0.838414
0.02	0.141441	+0.717119
0.05	0.286397	+0.427206
0.08	0.402179	+0.195642
0.110028	0.500000	0
0.15	0.609840	−0.219681
0.25	0.811278	−0.622556

Observation 5.2

The limit is **11.0028%**. The 25% of intercept-resend is 2.2722 times that—not just outside the boundary, but far outside.

Check 5.3: We see whether intercepting only part can hide. Intercepting a fraction f gives error rate $0.25f$.

Quantity	Value
Upper bound on f with $0.25f \leq 0.110028$	0.440111
Information Eve then obtains	0.083059 bits per sifted bit

Observation 5.4

Hiding is possible. But the take falls to 0.083 bits per 1 bit—the better she hides, the less she takes.

Check 5.5: Under full interception, the probability that n checked bits show no error at all is 0.75^n .

n	0.75^n
10	5.63×10^{-2}
20	3.17×10^{-3}
50	5.66×10^{-7}
73	7.58×10^{-10}
100	3.21×10^{-13}
200	1.03×10^{-25}

Observation 5.6

Checking **73** bits drops the miss probability below 10^{-9} . However many tens of thousands of bits the key has, what is needed to check it is **73** bits.

6. Separator: Security Does Not Rest on Computational Cost

Observation 6.1

Separator——what must be moved for this 25% to become another number? Only the theory of measurement itself.

Observation 6.2

Making computers faster does not move 25%. Making the key longer does not move it. Making the algorithm cleverer does not move it——25% comes from the overlap of bases, not from computational cost.

Observation 6.3

Its standing differs from classical cryptography. There, security is “hard to solve,” and hardness is relative to the speed of computers. Here, security is “measuring is conspicuous,” and it does not depend on the adversary’s computing power.

Observation 6.4

Sections 2 and 4 are two faces of one fact.

	About the error	About the state
Syndrome measurement (Sec. 2)	gains 8 bits	gains 0 bits $\Rightarrow$ no damage
Eve’s measurement (Sec. 4)	—	tries to gain $\Rightarrow$ damage (25%)

Observation 6.5

So “cannot be copied, yet can be corrected” is no contradiction. Nothing has been copied and nothing observed—because only 0 bits were taken about the state, the price is also 0.

7. Roll Call and Closing

1. Shor’s syndrome is 8 bits (Check 2.1): $2^8 = 256$ cases.
2. Of which 0 bits about the state (Observation 2.3): Hence no damage.
3. 0 for all three codes (Check 2.4): Enlarging does not increase it.
4. $16 = 16$ at five qubits (Check 3.1): Saturates exactly.
5. $n = 4$ fails at $13 > 8$ (Observation 3.3): At least 5 are needed.
6. Intercept-resend error rate 25% (Check 4.1): $\frac{1}{2} \cdot \frac{1}{2}$.
7. Eve’s take 0.188722 bits (Check 4.3): Small against the footprint.
8. Security limit 11.0028% (Check 5.1): 25% is 2.2722 times it.
9. Hiding gives 0.083059 bits (Check 5.3): The better hidden, the less taken.
10. 73 bits give 10^{-9} (Check 5.5): Checking is short.

Closing: It cannot be copied yet can be corrected because what is measured is not the state. The syndrome of Shor's 9-qubit code tells 8 bits about the error and 0 bits about the logical state—because only 0 bits are taken, the price is also 0. Enlarging the code does not increase that 0—Shor, Steane, and the 5-qubit code are equally 0 about the state. And in the 5-qubit code, 16 syndromes correspond one-to-one to 16 errors. The obverse of the same reasoning turns eavesdropping into a number—Eve tries to take about the state, so a footprint of 25% remains. That is 2.2722 times the security limit of 11.0028%, and checking 73 bits drops the miss probability below 10^{-9} . One thing separates them—counting how many bits that measurement takes about the state. Count, and correction and eavesdropping are seen as two faces of one principle. Fail to count, and the two look contradictory.

References

1. Wootters, W. K. and Zurek, W. H. (1982). A Single Quantum Cannot Be Cloned. *Nature*, 299(5886).
 2. Shor, P. W. (1995). Scheme for Reducing Decoherence in Quantum Computer Memory. *Physical Review A*, 52(4).
 3. Steane, A. M. (1996). Error Correcting Codes in Quantum Theory. *Physical Review Letters*, 77(5).
 4. Laflamme, R., Miquel, C., Paz, J. P. and Zurek, W. H. (1996). Perfect Quantum Error Correcting Code. *Physical Review Letters*, 77(1).
 5. Bennett, C. H. and Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*.
 6. Shor, P. W. and Preskill, J. (2000). Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters*, 85(2).
 7. Nielsen, M. A. and Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press.
 8. Gottesman, D. (1997). *Stabilizer Codes and Quantum Error Correction*. PhD thesis, California Institute of Technology.
 9. Yamagishi, Y. (2026). *The Qubit as a Hopf Fibration* [Paper 68]. Zenodo. 10.5281/zenodo.21642238
 10. Yamagishi, Y. (2026). *"A Good Code Exists" and "Here Is a Good Code" Are Different Sentences* [Paper 163]. Zenodo. 10.5281/zenodo.22092677
 11. Yamagishi, Y. (2026). *"Cannot Be Constructed" Has Distinct Roots* [Paper 179]. Zenodo. 10.5281/zenodo.22098419
 12. Yamagishi, Y. (2026). *Fewer Measurements Than Unknowns, and Still Exact* [Paper 188]. Zenodo. 10.5281/zenodo.22105691
 13. Yamagishi, Y. (2026). *Information Is Four Quantities, and They Need Different Things* [Paper 252]. Zenodo. 10.5281/zenodo.22161148
-

— From thinking to syncing. —

Yuuki YAMAGISHI (山岸 勇輝)