Cryptanalysis of 'Quantum public key encryption scheme with four states key'

Nithik R

Independent Researcher

E-mail: nithikr@protonmail.com

Abstract. Liu *et al* (2022 *Phys. Scr.* **97** 045102) propose a quantum public key encryption scheme in which a qubit message is encrypted by a controlled-NOT gate driven by a four-state public key, followed by measurement of the message register, and claim information-theoretic security. I show that the encryption map reduces exactly to $|M\rangle \mapsto R_\theta X^m |M\rangle$, where the outcome m is published. R_θ is diagonal and the ciphertext reproduces the computational-basis distribution $(|\alpha|^2, |\beta|^2)$ of the plaintext, and the plaintexts $|0\rangle$ and $|1\rangle$ are perfectly distinguishable. The claim of information-theoretic security is therefore invalid.

Keywords: quantum cryptography, quantum public key encryption, cryptanalysis, information-theoretic security, dephasing channel

1. Introduction

Liu *et al* [1] propose a quantum public key encryption (QPKE) scheme in which the private key is a classical two-bit symbol, the public key is a single qubit drawn from the four eigenstates of the Pauli operators X and Y, and the plaintext is an arbitrary qubit $|M\rangle = \alpha|0\rangle + \beta|1\rangle$. Encryption consists of a controlled-NOT (CNOT) gate with the public key as control and the message as target, followed by a computational-basis measurement of the target whose outcome m is transmitted in the clear together with the residual control qubit. On the basis of the irreversibility of this measurement, the authors assert (theorem 2 and section 2.6.2 of [1]) that no information about the plaintext can be obtained from the ciphertext, and conclude that the scheme is information-theoretically secure in the sense of Shannon [2].

In this Comment I show that this conclusion does not hold. Writing the encryption stage as a single linear map, we obtain the closed form

$$|M\rangle \longmapsto |M_{en}\rangle = R_\theta X^m |M\rangle , \tag{1}$$

where $R_\theta = \mathrm{diag}(1, e^{i\theta})$ is a relative-phase rotation fixed by the private key and $m \in \{0, 1\}$ is the published measurement outcome. Because R_θ is diagonal and X is a known permutation of the computational basis, the ciphertext carries the computational-basis probability distribution of the plaintext without any loss. Equivalently, the encryption changes the relative phase of the plaintext while leaving the probabilities of measuring 0 and 1 unchanged, except for a possible interchange of the two probabilities. Since the value of the bit determining this interchange is publicly available, an adversary can determine the original measurement probabilities from the ciphertext. In particular, when the plaintext is a computational-basis state, these probabilities are either (1,0) or (0,1), so the plaintext can be determined exactly from a single copy of the ciphertext. Thus, the scheme provides no secrecy for classical messages encoded in the computational basis.

2. The scheme of Liu *et al*

I restate the relevant part of the protocol of [1] in the notation used there, restricted without loss of generality to a single message qubit; the scheme processes an n-qubit message qubit-wise with independently generated keys, so the single-qubit analysis extends componentwise.

The private key symbol K_p is classical and uniformly distributed over four values,

$$K_p \in \{k_0, k_1, k_2, k_3\}, \tag{2}$$

and therefore carries $\log_2 4 = 2$ bits. The corresponding public key is a single qubit of the form

$$|K_v\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right), \qquad \theta \in \left\{0, \pi, \frac{\pi}{2}, -\frac{\pi}{2}\right\}, \tag{3}$$

generated from K_p according to table 1 of [1], reproduced here as table 1. The four public keys are the eigenstates $|\pm\rangle$ and $|P_\pm\rangle$ of X and Y respectively; the state listed in [1] for k_1, namely $(i\,|0\rangle + |1\rangle)/\sqrt{2}$, equals $|P_-\rangle$ up to the physically irrelevant global phase i, so the parametrisation (3) covers all four cases.

Table 1. Public key generation rules of the scheme of [1], together with the phase θ of equation (3). States are specified up to a global phase.

Private key K_p	Public key $\|K_v\rangle$	Notation	θ
k_0	$\frac{1}{\sqrt{2}}(\|0\rangle + i\,\|1\rangle)$	$\|P_+\rangle$	$\pi/2$
k_1	$\frac{1}{\sqrt{2}}(\|0\rangle - i\,\|1\rangle)$	$\|P_-\rangle$	$-\pi/2$
k_2	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|+\rangle$	0
k_3	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|-\rangle$	π

The plaintext is a qubit

$$|M\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \qquad |\alpha|^2 + |\beta|^2 = 1, \tag{4}$$

where $|\alpha|^2$ and $|\beta|^2$ are the probabilities of the outcomes 0 and 1 in a computational-basis (Z) measurement. Encryption proceeds in two steps: a CNOT gate is applied with $|K_v\rangle$ as control and $|M\rangle$ as target; the target is then measured in the Z basis, the outcome m is published, and the control register is transmitted as the ciphertext $|M_{en}\rangle$. Decryption is performed by the holder of K_p, who applies the key- and m-dependent correction listed in table 2 of [1]. The security claim of [1] rests on two statements: that K_p cannot be inferred from $|K_v\rangle$, and that the measurement performed during encryption destroys the plaintext irreversibly. The first statement is correct but concerns only key recovery; the second, as I now show, is false.

3. Closed form of the encryption map

Define the diagonal phase-rotation operator

$$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}, \tag{5}$$

so that the public key (3) is $|K_v\rangle = R_\theta\,|+\rangle$. The joint input state of the encryption circuit is

$$\begin{aligned} |K_v\rangle \otimes |M\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}\,|1\rangle\right) \otimes (\alpha\,|0\rangle + \beta\,|1\rangle) \\ &= \frac{1}{\sqrt{2}}\left(\alpha\,|00\rangle + \beta\,|01\rangle + \alpha e^{i\theta}\,|10\rangle + \beta e^{i\theta}\,|11\rangle\right). \end{aligned} \tag{6}$$

The CNOT gate exchanges $|10\rangle \leftrightarrow |11\rangle$, giving

$$\mathrm{CNOT}\,(|K_v\rangle \otimes |M\rangle) = \frac{1}{\sqrt{2}}\left(\alpha\,|00\rangle + \beta\,|01\rangle + \beta e^{i\theta}\,|10\rangle + \alpha e^{i\theta}\,|11\rangle\right). \tag{7}$$

Grouping equation (7) according to the state of the second (message) qubit yields

$$\mathrm{CNOT}\left(|K_v\rangle \otimes |M\rangle\right) = \frac{1}{\sqrt{2}}\Big[\left(\alpha\,|0\rangle + \beta e^{i\theta}\,|1\rangle\right) \otimes |0\rangle + \left(\beta\,|0\rangle + \alpha e^{i\theta}\,|1\rangle\right) \otimes |1\rangle\Big]. \tag{8}$$

The two branch states are precisely

$$\alpha\,|0\rangle + \beta e^{i\theta}\,|1\rangle = R_\theta\,|M\rangle\,, \qquad \beta\,|0\rangle + \alpha e^{i\theta}\,|1\rangle = R_\theta X\,|M\rangle\,, \tag{9}$$

with X the Pauli bit-flip operator, so that the encryption circuit acts as

$$|K_v\rangle \otimes |M\rangle \overset{\text{CNOT}}{\longrightarrow} \frac{1}{\sqrt{2}}\sum_{m=0}^{1}\left(R_\theta X^m\,|M\rangle\right) \otimes |m\rangle\,. \tag{10}$$

Measuring the message register in the Z basis therefore returns $m = 0$ and $m = 1$ with equal probability, independently of $|M\rangle$, and leaves the control register in the pure state

$$|M_{en}\rangle = R_\theta X^m\,|M\rangle\,, \tag{11}$$

which is equation (1). Equation (11) is exact and reproduces, case by case, the four decryption rules tabulated in [1]: since $R_\theta X^m$ is unitary and depends only on (K_p, m), the legitimate receiver inverts it, which is why the protocol is correct. It is also the reason why it is not secure.

4. Failure of information-theoretic security

Theorem 1 (Preservation of computational-basis populations) *Let* $|M\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ *be the plaintext and let* $(|M_{en}\rangle\,, m)$ *be the ciphertext produced by the scheme of [1], with* m *published. Then the ciphertext determines the computational-basis distribution* $(|\alpha|^2, |\beta|^2)$ *of the plaintext, for every value of the private key.*

Proof. By equation (11), $|M_{en}\rangle = R_\theta X^m\,|M\rangle$. The operator R_θ of equation (5) is diagonal in the computational basis and thus alters only the relative phase of the $|1\rangle$ component, leaving the moduli of the amplitudes unchanged.
For $m = 0$,

$$|M_{en}\rangle = R_\theta\,|M\rangle = \alpha\,|0\rangle + \beta e^{i\theta}\,|1\rangle\,, \tag{12}$$

so a Z measurement of the ciphertext yields $P(0) = |\alpha|^2$ and $P(1) = |\beta|^2$.
For $m = 1$,

$$|M_{en}\rangle = R_\theta X\,|M\rangle = \beta\,|0\rangle + \alpha e^{i\theta}\,|1\rangle\,, \tag{13}$$

so $P(0) = |\beta|^2$ and $P(1) = |\alpha|^2$. Since m is published as part of the ciphertext, an adversary knows whether the interchange has occurred and can undo it by applying X^m. In both cases the distribution $(|\alpha|^2, |\beta|^2)$ is recovered without any knowledge of K_p. ∎

Since the ciphertext uniquely determines the computational-basis probability distribution of the plaintext, an adversary can extract non-trivial information about the message without knowing the private key. An information-theoretically secure encryption scheme must reveal no information whatsoever about the plaintext from the ciphertext alone. This scheme therefore fails to achieve information-theoretic security.

5. Origin of the error

The proof of theorem 2 in [1] argues that "after the implementation of CNOT gate, the plaintext of message qubits will be measured ... This process cannot be reversed." The premise is correct and the conclusion does not follow. Irreversibility of the measurement on the target register says nothing about the register that is actually transmitted. In a CNOT gate whose control is prepared in a balanced superposition, the amplitudes of the target are transplanted onto the control, as equation (8) shows explicitly: the two branches of the post-CNOT state differ only by the operator X acting on the *control*. The measurement of the target therefore does not destroy the message; it merely selects which of the two unitary images of the message, $R_\theta |M\rangle$ or $R_\theta X |M\rangle$, is handed to the channel. Destroying a copy of the plaintext is not the same as destroying the plaintext.

6. Conclusion

The encryption stage of the QPKE scheme of Liu *et al* [1] reduces to the single-qubit map $|M\rangle \mapsto R_\theta X^m |M\rangle$ with m publicly announced. Because R_θ is diagonal in the computational basis, the ciphertext carries the plaintext distribution $(|\alpha|^2, |\beta|^2)$ intact; averaged over the key, the protocol is exactly a completely dephasing channel followed by a publicly known bit flip. Plaintexts drawn from the computational basis are recovered with certainty from a single ciphertext, so the scheme leaks up to one full bit per transmitted qubit and the claim of information-theoretic security in [1] is invalid. The mechanism responsible is not a numerical oversight but the structure of the circuit: the sole source of randomness capable of hiding the populations is the measurement outcome, which the protocol publishes. Reducing a protocol to its minimal algebraic form before assessing its security, as done in equation (11), exposes this immediately.

Acknowledgements

An earlier version of this analysis was publicly posted by the author on 7 August 2026 [6]. The author declares no conflict of interest and received no funding for this work. The author used a large language model for LaTeX document formatting and language editing assistance.

Data availability statement

No new data were created or analysed in this study. All results are analytical and are derived in full within the article.

References

[1] Liu Z, Xie Q, Zha Y and Dong Y 2022 Quantum public key encryption scheme with four states key *Phys. Scr.* **97** 045102

[2] Shannon C E 1949 Communication theory of secrecy systems *Bell Syst. Tech. J.* **28** 656–715

[3] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* (Bangalore, India) pp 175–179

[4] Nikolopoulos G M and Ioannou L M 2009 Deterministic quantum-public-key encryption: forward search attack and randomization *Phys. Rev. A* **79** 042327

[5] Okamoto T, Tanaka K and Uchiyama S 2000 Quantum public-key cryptosystems *Advances in Cryptology — CRYPTO 2000 (Lecture Notes in Computer Science vol 1880)* (Berlin: Springer) pp 147–165

[6] Nithik R 2026 Cryptanalysis of a Quantum Public-Key Encryption Scheme *Recu Blog* (7 August 2026) https://recu.blog/posts/cryptanalysis-of-a-quantum-public-key-encryption-scheme/