Comment on “An encryption protocol for NEQR images based on one-particle quantum walks on a circle”

Markus Grassl^{1,2}

Received: 27 October 2020 / Accepted: 1 April 2021
© The Author(s) 2023

Abstract

In [1], the authors propose a protocol to encrypt quantum images. Below we show that the protocol is incorrect.

Keywords Entanglement · Quantum circuits · Quantum image encryption

1 The main idea

The key idea of [1] is to apply a self-inverse operation to a quantum state $|I\rangle$ encoding a quantum image and a key state $|K\rangle$ which can be interpreted as a quantum image of the same format as well. The output of the proposed encryption operation is a quantum state $|X\rangle$ which again corresponds to a quantum image of the same format.

2 Discussion of the encryption operation

In Eq. (9) of [1], the authors define the NEQR model for a quantum image I of size $2^n \times 2^n$ as follows:

$$|I\rangle = \frac{1}{2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} |c_{i,j}\rangle |i\rangle |j\rangle. \quad (1)$$

The indices i and j encode the x and y coordinates of a pixel with color value $c_{i,j}$. The key K for the encryption is represented in the same way (see also Eqs. (22) and (23) of [1]) as

This comment refers to the article available online at <https://doi.org/10.1007/s11128-019-2386-3>.

✉ Markus Grassl
markus.grassl@ug.edu.pl

¹ International Centre for Theory of Quantum Technologies, University of Gdansk, Wita Stwosza 63, 80-308 Gdańsk, Poland

² Max Planck Institute for the Science of Light, Staudtstraße 2, 91058 Erlangen, Germany

$$|K\rangle = \frac{1}{2^n} \sum_{\mu=0}^{2^n-1} \sum_{v=0}^{2^n-1} |k_{\mu,v}\rangle |\mu\rangle |v\rangle. \quad (2)$$

For clarity, we use Roman indices i, j for the image state $|I\rangle$ and Greek indices μ, v for the key state $|K\rangle$.

The encryption operation is said to be given by Eq. (24) of [1] which we repeat literally here:

$$\begin{aligned} & |x_{i,j}^7, x_{i,j}^6, \dots, x_{i,j}^0\rangle \otimes |i\rangle |j\rangle \\ &= \hat{C}_{\text{not}}^{\otimes 8} |k_{i,j}^7, k_{i,j}^6, \dots, k_{i,j}^0\rangle |c_{i,j}^7, c_{i,j}^6, \dots, c_{i,j}^0\rangle \otimes |i\rangle |j\rangle \\ &= |C_{\text{not}}(k_{i,j}^7, c_{i,j}^7) C_{\text{not}}(k_{i,j}^6, c_{i,j}^6) \dots C_{\text{not}}(k_{i,j}^0, c_{i,j}^0)\rangle \otimes |i\rangle |j\rangle. \end{aligned} \quad (3)$$

Note that the second line of (3) includes the eight qubits specifying the “color” values $k_{i,j}^7 \dots k_{i,j}^0$ of the pixel at position (i, j) in the key state $|K\rangle$, while those qubits are missing from the first and last line.

In the following, we discuss two possible interpretations of the proposed encryption operation. The first is based on the quantum circuit for the encryption algorithm given in Figure 4 of [1] (reproduced here in Fig. 1), while the second is based on the explanation given by the authors around Eq. (24):

“...each entry $|x_{i,j}^7, x_{i,j}^6, \dots, x_{i,j}^0\rangle \otimes |i\rangle |j\rangle$ is computed according to Eq. (24) for each pair of indices $|i\rangle, |j\rangle$.”

2.1 Encryption following Fig. 4

Looking at the quantum circuit for the encryption algorithm given in Figure 4 of [1], one finds that the qubits related to the pixel positions, denoted $|X_u\rangle$ and $|Y_i\rangle$ in the figure, do not enter any operation. Furthermore, the qubits related to the pixel positions of the key state $|K\rangle$ are not shown at all. The qubits related to the color values in the key state $|K\rangle$ are drawn in magenta. The horizontal lines depicting them are not connected to any output. Related, the number of qubits of the right hand side of the first line of Eq. (24) is different from the left hand side of the first line.

When we apply the eight CNOT gates of Eq. (24) (also shown in the figure) to the tensor product of the image $|I\rangle$ and the key $|K\rangle$, we obtain

$$\begin{aligned} \hat{C}_{\text{not}}^{\otimes 8}(|K\rangle |I\rangle) &= \hat{C}_{\text{not}}^{\otimes 8} \left(\frac{1}{2^n} \sum_{\mu=0}^{2^n-1} \sum_{v=0}^{2^n-1} |k_{\mu,v}\rangle |\mu\rangle |v\rangle \otimes \frac{1}{2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} |c_{i,j}\rangle |i\rangle |j\rangle \right) \\ &= \frac{1}{2^n} \sum_{\mu=0}^{2^n-1} \sum_{v=0}^{2^n-1} |k_{\mu,v}\rangle |\mu\rangle |v\rangle \otimes \frac{1}{2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} |c_{i,j} \oplus k_{\mu,v}\rangle |i\rangle |j\rangle \\ &= \frac{1}{4^n} \sum_{\mu=0}^{2^n-1} \sum_{v=0}^{2^n-1} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} |k_{\mu,v}\rangle |\mu\rangle |v\rangle \otimes |c_{i,j} \oplus k_{\mu,v}\rangle |i\rangle |j\rangle. \end{aligned} \quad (4)$$

Fig. 1 Quantum circuit for the encryption algorithm (reproduced from [1, Fig. 4])

Note that the state on the right of the tensor product sign in (4) depends on both the indices i, j and μ, v , i.e., the state is in general entangled with respect to the bipartition indicated by the tensor product sign.

When we discard the qubits of the key state $|K\rangle$, the state corresponding to the encrypted image will be a mixed state, i.e., a state involving some randomness. An alternative description is to perform a measurement of the qubits related to the key state $|K\rangle$ with respect to the computational bases. This will yield a random, uniformly distributed pixel position (μ_0, v_0) with corresponding color value k_{μ_0, v_0} . (As the CNOT gates do not depend on the variables μ, v , it is actually sufficient to consider the color value k_{μ_0, v_0} .) Then, the state of the encrypted image will be

$$|X(\mu_0, v_0, k_{\mu_0, v_0})\rangle = \frac{1}{2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} |c_{i,j} \oplus k_{\mu_0, v_0}\rangle |i\rangle |j\rangle. \quad (5)$$

Note that all pixels will be modified in the very same way. More severely, the random value k_{μ_0, ν_0} is unknown and cannot be deterministically reproduced in the decryption step.

The state in eq. (5) is clearly different from the state

$$|\tilde{X}\rangle = \frac{1}{2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} |c_{i,j} \oplus k_{i,j}\rangle |i\rangle |j\rangle. \quad (6)$$

which one would obtain taking the uniform superposition of the states on the right hand side of Eq. (24) for all values of i, j .

2.2 Encryption conditioned on the pixel position

As already mentioned, the authors add the explanation that the encrypted image should be computed “for each pair of indices $|i\rangle, |j\rangle$.” Recall that the pixel indices i, j in the original image and the pixel indices μ, ν in the image used as key are independent of each other.

One attempt in that direction could be to condition the CNOT operations on the indices i, j and μ, ν being equal. In this case, the state of the whole systems reads

$$\frac{1}{4^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} |k_{i,j}\rangle |i\rangle |j\rangle |c_{i,j} \oplus k_{i,j}\rangle |i\rangle |j\rangle \quad (7)$$

$$+ \frac{1}{4^n} \sum_{\mu, \nu=0}^{2^n-1} \sum_{\substack{i, j=0 \\ (i,j) \neq (\mu, \nu)}}^{2^n-1} |k_{\mu, \nu}\rangle |\mu\rangle |\nu\rangle |c_{i,j}\rangle |i\rangle |j\rangle. \quad (8)$$

While the summand in (7) somehow resembles the desired state (6), the pixel position i, j occurs in the qubits related to the key $|K\rangle$ as well. Ignoring those register would be equivalent to measuring the pixel position. Moreover, the whole state is a superposition of the states (7) and (8), again different from the intended result.

3 Concluding remarks

More generally, the authors aim at a reversible quantum operation U_{enc} that acts on a quantum image $|I\rangle$ and a key $|K\rangle$ in order to produce an encoded quantum image $|X(K)\rangle$ of the same format as the original image. At the same time, the encoded image $|X\rangle$ should not be entangled with the rest of the output of the operation, i.e.,

$$U_{\text{enc}}(|K\rangle \otimes |I\rangle) = |K'\rangle \otimes |X(K)\rangle. \quad (9)$$

In the proposed encryption protocol, the modification of the image $|I\rangle$ is controlled by the basis states of the Hilbert space related to the key $|K\rangle$. In general, the key

$|K\rangle$ is a superposition with respect to that basis, and hence any nontrivial encoding operation necessarily creates entanglement between the Hilbert space of the key and the Hilbert space of the image. Ignoring the key after the encryption operation (partial trace) results in a mixed state of the output, and decryption is not possible in general.

Acknowledgements The 'International Centre for Theory of Quantum Technologies' project (contract no. 2018/MAB/5) is carried out within the International Research Agendas Programme of the Foundation for Polish Science co-financed by the European Union from the funds of the Smart Growth Operational Programme, axis IV: Increasing the research potential (Measure 4.3).

Funding Open Access funding enabled and organized by Projekt DEAL.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

Reference

1. Abd-El-AttyAhmed, B., Abd El-Latif, A.A., Venegas-Andraca, S.E.: An encryption protocol for NEQR images based on one-particle quantum walks on a circle. *Quantum Information Processing* **18**, 272 (2019). <https://doi.org/10.1007/s11128-019-2386-3>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.