Quantum security on a colour imagine

Gabriela Mogos
Al.I.Cuza University, Computer Science Department
Iasi, Romania
gabi.mogos@gmail.com

March 9, 2008

1 Introduction

The digital signature - is a compulsory attribute of the electronic document, obtained after its cryptographic transformation by using the private key, on the purpose of confirming the authenticity of the electronic document. The digital signature for the electronic documents is equivalent to an olograph signature for the printed documents. The signature is a sample of data which demonstrates that a certain person wrote or agreed on the document to which a signature was attached. In fact, a digital signature provides a much higher level of security than the olograph signature. The receiver of the message signed digitally can check both the fact that the original message belongs to the person whose signature was attached, and the fact that the message wasn't altered, intentionally or by accident, from the moment in which it was signed. Further more, the digital signature cannot be denied, and the one who signed the document cannot exonerate him later by declaring that it had been forged. In other words, the digital signatures allow the authentication of the digital messages, assuring the receiver of the identity of the sender, and of the integrity of the message. This work has the purpose to apply a digital signature on a message made of plenty of quantum bits (qutrits). The message under study is a image file.

2 Pixel vs qubit

We can say that the concept of information represents a matter of maximum generality, meaning a piece of news, a message, a signal, etc., about events, facts, states, objects, etc., in general about forms of manifestation of the reality surrounding us. Shannon defines the entropy as a function measuring the quantity of information. In the theory of the sending of the information, the informational entropy is defined as the quantity of information reported to an element of the message that was sent. In general, the quantity of information related to the realization of an elementary event i from the field of events is defined as the logarithm (negative) base two from the probability of the realization of that elementary event:

$$H_i = -log_2 p(_i). \qquad (1)$$

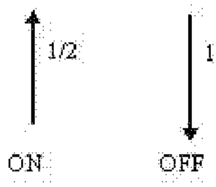
As we know, the digital image is made of a finite number of pixels. The pixel, considered as the basic unit of the image (element of the sent message), can be seen as an object limited by a closed surface, and bearing information.

Conventionally, we take two independent events (states) ON and OFF of a pixel. The information obtained when two independent events appear with the probability of p_1 and p_2 is equal to the sum of the information obtained by each event. Consequently, writing p_1 the probability of obtaining the event (state) ON and p_2 the probability of obtaining the event (state) OFF, the entropy is minimum when we obtain the state ON (for $p_1 = 1$ and $p_2 = 0$) or when we obtain the state OFF (for $p_1 = 0$ and $p_2 = 1$) and maximum when the two states are equiprobable (determined by their combination).

We can notice that the pixel can be associated with a two-level system, i.e. like a spin.

Spin networks are mathematical entities; they do not contain any information, because the information is a physical value. In order to create the information, they must intersect a transversal surface, each "intersection" being quantified with a unit of information.

Thus, the image can be seen as a closed transversal surface, intersected by a spin network, and the resulted unit of information is the pixel.



Thus, the pixel in the state ON can be associated to the spin $\frac{1}{2}$ (with a representation in SU(2) by the state $|\frac{1}{2}\rangle$), and the pixel in the state OFF can be associated with the spin $-\frac{1}{2}$ (with a representation in SU(2) by the state $|\frac{-1}{2}\rangle$).

The existence of the pixel in an equiprobable state of ON and OFF is translated by the fact that the spin is in a superposition of quantum states, as it follows:

$$\frac{1}{\sqrt{2}}[|\frac{1}{2}\rangle \pm | -\frac{1}{2}\rangle] \tag{2}$$

The states $|\frac{1}{2}\rangle$ and $| -\frac{1}{2}\rangle$ are written:

$$|\frac{1}{2}\rangle \doteq \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{3}$$

$$| -\frac{1}{2}\rangle \doteq \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{4}$$

The image is characterized by an entropy equal to the sum of the entropy of the pixels it contains.

$$H = \sum_{i=1}^{n} H(i) \tag{5}$$

3 Qubit representation in coordinates RGB

A pixel belonging to an image can be represented in three dimensions using the coordinates (R,G,B), its colour being obtained by the linear combination of the three. In the same time, using the Bloch sphere, we can represent the state of a qubit. If we associate the 3-D representation to a qubit with the representation of the pixel in the coordinates (R,G,B), we can write the state of such a qubit as a linear combination of the projections on the three axes of coordinates (R,G,B). The qubit thus represented is a three-level system, called also qutrit.

$$|\Psi\rangle = r|R\rangle + g|G\rangle + b|B\rangle \tag{6}$$

or:

$$|\Psi\rangle = \sum_{r,g,b} c_{r,g,b}|RGB\rangle \tag{7}$$

4 Quantum signature

The quantum signature is a succession of qutrits - i.e. a set of data in the electronic format, serving as identification data.

Similar to the classical digital signature, the quantum signature observes all these conditions:
- it is uniquely linked with the person who signed
- it assures the identification of the person who signed
- it is created by exclusive means, controlled by the person who signed
- any of their afterwards changes can be identified.

Starting with the scheme Quantum Secret Sharing (QSS), this work proposes a procedure of application of the quantum signature on a colour imagine, made of qutrits.

According to this scheme, a secret is divided in n parts which will be distributed, any k, $(k \leq n)$ of these parts can reconstruct the secret, and $k-1$ or less parts cannot reconstruct it. In this work, we take into account the case when the signature is divided by three parts $n = 3$.

4.1 The scheme for $n = 3$

We will presume that the signature, made of three qutrits, will be divided among three parts (Alice, Bob and John). In order to get it, two of the three parts will be involved. Alice realizes the entanglement of the states of the signature qutrits, and combines the result with a qutrit belonging to the image.

The $|\Psi\rangle_{123}$ is the quantum state of the signature (the qutrits are maximally entangled) and the $|\Psi\rangle_4$ is the quantum state of the qutrit belonging to the image. Combining the state of the four particles we obtain:

$$|\Psi\rangle_{1234} = |\Psi\rangle_{123} \otimes |\Psi\rangle_4 \tag{8}$$

where

$$|\Psi\rangle_{123} = \alpha(|RRR\rangle_{123} + \beta|GGG\rangle_{123} + \gamma|BBB\rangle_{123})$$

and

$$|\Psi\rangle_4 = |R\rangle_4 + |G\rangle_4 + |B\rangle_4$$

Replacing the expressions $|\Psi\rangle_{123}$ and $|\Psi\rangle_4$ in the equation (8), we obtain:

$$|\Psi\rangle_{1234} = [\alpha(|RRR\rangle_{123} + \beta|GGG\rangle_{123} + \gamma|BBB\rangle_{123})] \otimes (|R\rangle_4 + |G\rangle_4 + |B\rangle_4)$$

4.1.1 Checking the identity of the person who signed

After receiving the image, if Bob wants to check the identity of the person who signed the image, he will need Alice. It is important that John, the third person in the diagram, can reconstitute the signature with Bob's help. Alice will realize a Bell projective measurement for the pair (1,4). There are $3^2 = 9$ possible states obtained, defined as it follows:

$$|\Psi_{nm}\rangle = \sum_j e^{\frac{2\pi ijn}{3}} |j\rangle \otimes |j + m \mod 3\rangle/\sqrt{3} \tag{9}$$

where $n \in \{0, 1, 2\}$, $m \in \{0, 1, 2\}$ and $j \in \{0, 1, 2\}$ are the three dimensions (R,G,B) numbered $(0, 1, 2)$ to simplify the calculus.

For a system made of three qutrits:

$$|\Psi^k_{nm}\rangle = \sum_j e^{\frac{2\pi ijk}{3}} |j\rangle \otimes |j + n \mod 3\rangle \otimes |j + m \mod 3\rangle/\sqrt{3} \tag{10}$$

After the measurement, the system will evolve in one of the states:

$$\begin{gathered}
\tfrac{1}{3}|\Psi_{RR}\rangle_{14}(\alpha|RR\rangle_{23} + \beta|GG\rangle_{23} + \gamma|BB\rangle_{23})\\
\tfrac{1}{3}|\Psi_{RG}\rangle_{14}(\alpha|GG\rangle_{23} + \beta|BB\rangle_{23} + \gamma|RR\rangle_{23})\\
\tfrac{1}{3}|\Psi_{RB}\rangle_{14}(\alpha|GG\rangle_{23} + \beta|RR\rangle_{23} + \gamma|GG\rangle_{23})\\
\tfrac{1}{3}|\Psi_{GR}\rangle_{14}(\alpha|RR\rangle_{23} + e^{\frac{-2\pi i}{3}}\beta|GG\rangle_{23} + e^{\frac{-4\pi i}{3}}\gamma|BB\rangle_{23})\\
\tfrac{1}{3}|\Psi_{BR}\rangle_{14}(\alpha|RR\rangle_{3} + e^{\frac{-4\pi i}{3}}\beta|GG\rangle_{23} + e^{\frac{-8\pi i}{3}}\gamma|BB\rangle_{23})\\
\tfrac{1}{3}|\Psi_{GG}\rangle_{14}(\alpha|GG\rangle_{23} + e^{\frac{-2\pi i}{3}}\beta|BB\rangle_{23} + e^{\frac{-4\pi i}{3}}\gamma|RR\rangle_{23})\\
\tfrac{1}{3}|\Psi_{BG}\rangle_{14}(\alpha|GG\rangle_{23} + e^{\frac{-4\pi i}{3}}\beta|BB\rangle_{23} + e^{\frac{-8\pi i}{3}}\gamma|RR\rangle_{23})\\
\tfrac{1}{3}|\Psi_{GB}\rangle_{14}(\alpha|BB\rangle_{23} + e^{\frac{-2\pi i}{3}}\beta|RR\rangle_{23} + e^{\frac{-4\pi i}{3}}\gamma|GG\rangle_{23})\\
\tfrac{1}{3}|\Psi_{BB}\rangle_{14}(\alpha|BB\rangle_{23} + e^{\frac{-4\pi i}{3}}\beta|RR\rangle_{23} + e^{\frac{-8\pi i}{3}}\gamma|GG\rangle_{23})
\end{gathered}$$

Checking the authenticity is similar for each of the results. If we consider that Alice is measuring the pair $(1, 4)$ and she will get as a result $|\Psi_{RR}\rangle_{14}$. In this case, the state of the pair $(2, 3)$ will collapse in:

$$\alpha|RR\rangle_{23}+\beta|GG\rangle_{23}+\gamma|BB\rangle_{23} = \frac{1}{3}[(|R\rangle_2+|B\rangle_2+|G\rangle)_2)(\alpha|R\rangle_3+\beta|G\rangle_3+\gamma|B\rangle_3)+(|R\rangle_2+e^{\frac{2\pi i}{3}}|G\rangle_2+e^{\frac{4\pi i}{3}}|B\rangle_2)$$

$$(\alpha|R\rangle_3+e^{\frac{-2\pi i}{3}}|G\rangle_3+e^{\frac{-4\pi i}{3}}|B\rangle_3)+(|R\rangle_2+e^{\frac{4\pi i}{3}}|G\rangle_2+e^{\frac{2\pi i}{3}}|B\rangle_2)(\alpha|R\rangle_3+e^{\frac{-4\pi i}{3}}\beta|G\rangle_3+e^{\frac{-2\pi i}{3}}\gamma|B\rangle_3)].$$

If Bob will measure the state of the qutrit $|R\rangle_2 + |B\rangle_2 + |G\rangle)_2$ he will determine the collapsing of the John's qutrit in the state $\alpha|R\rangle_3 + \beta|G\rangle_3 + \gamma|B\rangle)_3$, which is in fact the signature.

If Bob will measure the state of the qutrit $|R\rangle_2 + e^{\frac{2\pi i}{3}}|G\rangle_2 + e^{\frac{4\pi i}{3}}|B\rangle_2$, John can reconstruct the signature by applying the unitary operator $O_1 = \sum_{k=R,G,B} e^{\frac{2\pi ij}{3}}|k\rangle\langle k|$ over the state of the qutrit $\alpha|R\rangle_3 + e^{\frac{-2\pi i}{3}}|G\rangle_3 + e^{\frac{-4\pi i}{3}}|B\rangle_3$.

If Bob will measure the state of the qutrit $|R\rangle_2 + e^{\frac{4\pi i}{3}}|G\rangle_2 + e^{\frac{2\pi i}{3}}|B\rangle_2$, John will reconstruct the state of his qutrit by applying the unitary operator $O_2 = \sum_{k=R,G,B} e^{\frac{4\pi ij}{3}}|k\rangle\langle k|$.

This scheme is based on the fact that Bob can check the authenticity of the signature and the integrity of the image, being helped by John to reconstruct the signature.

The two schemes can be also used for the distribution of some private keys, used afterwards at the encrypting.

4.1.2 The attack over the signature

We can take two cases:

1. the case in which the eavesdropper acts from outside;
2. the case in which the eavesdropper acts from inside.

1. *The eavesdropper acts from outside.*

We can take the existence of an external intruder who acts over the communication channel. He will try to forge the signature using a complementary qutrit (ancilla) with which he "hooks" on the image in the moment of its transmission through the quantum communication channel. After Alice communicates the result of her measurement and the base she used, Bob and John will use the same base for their own qutrits. As the results of their measurements must be strongly correlated, the appearance of some disturbance determined by the existence of the intruder determines qutrits errors. When checking the results, we can notice the existence of some non-correlations, which strengthens the belief of an intruder's existence.

2. *The eavesdropper acts from inside*

We presume that we have an intruder inside the process, in the person of Bob. He will wish to forge the signature or to prove that the image broke during the transmission. As a result, after Alice announces publicly the result of the measurement and of the base used, Bob will communicate to John another result (which was prepared on purpose), which will determine the obtaining of an erroneous piece of information. If Alice and John will compare the two results, they will clearly notice the intervention of an intruder. Here, John will play a very important role in authenticating the signature

References

[1] Mark Hillery, Vladimir Buzek, Andre Berthiaume, *Quantum Secret Sharing*, quant-ph/9806063 v2, 1998.

[2] Feyman, *Lecture on Physics*, Vol. 3,1964.

[3] P. A. Zizzi., *Holography, Quantum Geometry, and, Quantum Information Theory*, Entropy, 2000, pp. 39-69.

[4] Carlton M. Caves, Gerard J. Milburn, *Qutrit entanglement*, quant-ph/9910001v2, 1999.

[5] Ye Yeo, *Quantum teleportation using three-particle entanglement*, quant-ph/0302030v1, 2003.

[6] Arti Chamoli, C. M. Bhandari, *Entanglement teleportation by Qutrits*, quant-ph/0702223, 2007.

[7] Sudhir Kumar Singh and R. Srikanth, *Generalized quantum secret sharing*, Physical Review A 71, 012328, 2005.

[8] Christian Schmid, Pavel Trojek, Mohamed Bourennane *et al.*, *Experimental Single Qubit Quantum Secret Sharing*, Physical Review Letters , 95, 230505, 2005.

[9] Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, *Reviews of Modern Physics - Quantum cryptography*, Vol. 74, January 2002.