Protótipo de sistema de segurança criptográfica via porta lógica quântica

Jacomo Giovanetti Minto Neto[1]
Alexandre de Castro[2]
Adauto Luiz Mancini[3]

Resumo: O cifrador XOR não é considerado completamente seguro, pois não há chaves de criptografia verdadeiramente aleatórias, dado que as chaves são geradas em geradores de números pseudorrandômicos a partir de sementes que não podem ser negligenciadas. No entanto, uma chave que destrói a própria semente que a gerou, pode ser considerada verdadeiramente aleatória, pois o seu estado inicial é definitivamente ignorado. Neste trabalho, nós apresentamos um modelo de chaves verdadeiramente aleatórias que podem ser obtidas a partir da porta quântica denominada controlled-NOT (CNOT) usada para emaranhar estados EPR.

Palavras-chave: porta lógica quântica, criptografia, OTP, cifrador XOR, campo de galois.

Introdução

Em um trabalho anterior, Bayer (2006) sugeriu que a porta CNOT é assimétrica. Nesta mesma linha, recentemente mostramos que a porta CNOT se torna irreversível com restrições adiabáticas (CASTRO, 2014), uma vez que o seu circuito quântico só pode ser completado se uma operação de

[1] Estudante de Análise e Desenvolvimento de Sistemas da Faculdade de Tecnologia de Americana (Fatec, Americana, SP), estagiário da Embrapa Informática Agropecuária, Campinas, SP.

[2] Doutor em Ciências (Biomatemática), pesquisador da Embrapa Informática Agropecuária, Campinas, SP.

[3] Mestre em Ciência da Computação, pesquisador da Embrapa Informática Agropecuária, Campinas, SP.

disjunção exclusiva no seu qubit ancilla ganha uma informação extra igual a Log(2). Aqui, mostramos que, se a chave de criptografia é obtida por uma função quadrática módulo 2 da mensagem (plaintext), o resultado é um qubit ancilla perfeitamente emaranhado, que produz um cifrador XOR com comportamento de um one-time pad(OTP).

Materiais e Métodos

O operador unitário U_{CNOT} pode ser escrito sobre dois qubits, operacionalmente, $|a\rangle$ e $|b\rangle \in GF_2$, onde o primeiro é o qubit de controle que representa cada bit da chave criptográfica e o último é o qubit ancilla que representa cada bit da mensagem original, e GF_2 é o campo de Galois (MULLEN; PLANARIO, 2013) de dois elementos, $F_2 = \{0,1\}$:

$$U_{\text{CNOT}} |a \otimes b\rangle = |a\rangle \otimes |a \oplus b\rangle$$

onde $a \oplus b = (a+b) \text{mod} 2$ representa a mensagem cifrada. Na operação CNOT, o primeiro qubit é conservado, ao passo que o segundo qubit é o resultado de uma operação XOR entre o primeiro e o segundo qubit (NIELSEN; CHUANG, 2000).

A matricial para esta transformação é:

$$U(0,0) = (0,0) \Rightarrow \begin{pmatrix} U_{11} & U_{12} & U_{13} & U_{14} \\ U_{21} & U_{22} & U_{23} & U_{24} \\ U_{31} & U_{32} & U_{33} & U_{34} \\ U_{41} & U_{42} & U_{43} & U_{44} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \therefore \begin{pmatrix} U_{11} \\ U_{21} \\ U_{31} \\ U_{41} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\Rightarrow U_{11} = 1,\ U_{21} = U_{31} = U_{41} = 0$$

Da mesma forma, para $U(0,1) = (0,1)$: $U_{22} = 1,\ U_{12} = U_{32} = U_{42} = 0$

Para:

$$U(1,0) = (1,1) \Rightarrow \begin{pmatrix} 1 & 0 & U_{13} & U_{14} \\ 0 & 1 & U_{23} & U_{24} \\ 0 & 0 & U_{33} & U_{34} \\ 0 & 0 & U_{43} & U_{44} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \therefore \begin{pmatrix} U_{13} \\ U_{23} \\ U_{33} \\ U_{43} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$\Rightarrow U_{43} = 1,\ U_{13} = U_{23} = U_{33} = 0$$

Para , $U(1,1) = (1,0)$, $U_{34} = 1$, $U_{14} = U_{24} = U_{34} = 0$.

Logo,

$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$, onde $U^2 = I_d$ é uma permutação.

Note-se que na transformação:

	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	1	0	0	0
(0,1)	0	1	0	0
(1,0)	0	0	0	1
(1,1)	0	0	1	0

O estado $U_{\text{CNOT}}\ |1,0\rangle \rightarrow |1,1\rangle$ pode ser substituído por $U_{\text{CNOT}}\ |1,b\rangle \rightarrow |1, NOT(b) \oplus b\rangle$, onde $|NOT(b) \oplus b\rangle$ representa uma função irreversível.

Resultados e Discussão

A partir da construção acima, mesmo considerando a porta CNOT unitária (permutação), somente poderá ocorrer a decriptação se a chave gerada aleatoriamente por meio da função irreversível for aplicada, executando, assim, uma transformação unitária que é a sua própria inversa, de modo que exista uma involução. (ver aspectos termodinâmicos (CASTRO, 2014).

Considerações Finais

Neste trabalho, apresentamos um protocolo de criptografia via porta CNOT, que representa um modelo OTP seguro, pois a chave de criptografia não é obtida a partir de um gerador pseudorrandômico e, sim, através do próprio protocolo de criptografia.

Referências

BAYER, G. W. Quantum computation violates mirror symmetry. **Quantum Information Processing**, v. 5, n. 1, p. 25-30, Feb. 2006. DOI: 10.1007/s11128-005-0010-1.

CASTRO, A. One-way-ness in the input-saving (Turing) machine. **Physica A**: Statistical Mechanics and its Applications, v. 415, n.1, p. 473-478, Dec. 2014. DOI: 10.1016/j.physa.2014.08.021.

MULLEN, G. L.; PANARIO, D. **Handbook of finite fields**. Boca Raton: CRC Press, 2013. 1033 p.

NIELSEN, M. A.; CHUANG, I. L. **Quantum computation and quantum information**. Cambridge: New York: Cambridge University Press, 2000. 676 p. ill.