Comunicado Técnico 119
ISSN 1677-8464
Dezembro, 2015
Campinas, SP

Sistema de criptografia simétrica via porta lógica quântica

Alexandre de Castro[1]
Jacomo Giovanetti Minto Neto[2]

Atualmente, a teoria relacionada à criptologia é fortemente baseada na hipótese de unidirecionalidade de caminhos computacionais. Esta conjectura matemática sustenta que deve haver uma função bijetora para a qual o cálculo em uma direção é fácil, enquanto reconstruir o estado de entrada a partir do estado de saída é difícil - “fácil” e “difícil” devem ser entendidas no sentido de complexidade computacional. Mais especificamente, esta proposição de complexidade computacional, essencialmente, requer a existência de uma permutação unidirecional.

Nos últimos anos, tem surgido a ideia de que uma operação unitária (permutação) unidirecional pode estar relacionada às limitações físicas, ao invés de limitações puramente matemática.

Recentemente foi mostrado que a porta controlled-NOT (CNOT) gate se torna irreversível com restrições adiabáticas (CASTRO, 2014) uma vez que o seu circuito quântico só pode ser completado se uma operação de disjunção exclusiva no seu qubit objeto ganhar informação extra igual a Log(2). Aqui, esse conceito de operação unitária irreversível é utilizado para mostrar que, se uma chave criptográfica for obtida por uma função quadrática módulo 2 da mensagem (plaintext), o resultado é um qubit objeto perfeitamente emaranhado, que produz um cifrador XOR com comportamento de um one-time pad (OTP).

O operador unitário U_{CNOT} pode ser escrito sobre dois qubits, operacionalmente, $|a\rangle$ e $|b\rangle \epsilon GF_2$, onde o primeiro é o qubit de controle, o último é o qubit objeto, e GF_2 é o campo de Galois (MULLEN; PANARIO,2013) de dois elementos, $F_2 = \{0,1\}$:

Assim, $U_{CNOT}\,[|a\rangle \otimes |b\rangle] = |a\rangle \otimes |a \oplus b\rangle$, onde $a \oplus b = (a + b)$ mod2. 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 representação matricial para esta transformação é:

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

[1] Físico, doutor em Biomatemática, pesquisador da Embrapa Informática Agropecuária, Campinas, SP
[2] Estudante, estagiário da Embrapa Informática Agropecuária, Campinas, SP

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

Para $U(0,1) = (1,1)$:

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

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

Logo,

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

Note-se que a transformação de estado $U_{CNOT}|1,0\rangle = |1,1\rangle$ pode ser substituída por $U_{CNOT}|1,b\rangle = |1,\mathrm{NOT}\,(b) \oplus b\rangle$, para $b = 0$.

Em GF_2, a porta NOT corresponde à representação polinomial $\mathrm{NOT}(b) = b \oplus 1$, e todo elemento b satisfaz a propriedade $b = b^2$. Assim, a negação lógica também pode ser representada pelo polinômio $\mathrm{NOT}(b) = b^2 \oplus 1$.

A disjunção exclusiva $\mathrm{NOT}(b) = b \oplus 1$, onde $\mathrm{NOT}(b)$ é a chave pública e b é cada bit da mensagem, corresponde à operação adição de campo (mod2) sobre o campo de Galois de dois elementos (NIELSEN; CHUANG, 2000).

As seguintes representações são equivalentes no campo finito de característica 2: $b^2 \oplus 1 \Rightarrow \{101\}$ e $b \Rightarrow \{010\}$.

Assim:

$$\begin{array}{ccccc} b^2 \oplus 1 & \oplus & b & = & b^2 \oplus b \oplus 1 \\ \{1\ 0\ 1\} & \mathrm{XOR} & \{0\ 1\ 0\} & = & \{1\ 1\ 1\} \end{array}$$

Portanto $\mathrm{NOT}(b) \oplus b = b^2 \oplus b \oplus 1$. Logo, $U_{CNOT}|1,b\rangle = |1,b^2 \oplus b \oplus 1\rangle$, onde o $b^2 \oplus b \oplus 1$ é a mensagem cifrada.

Considerando que a porta CNOT é unitária (permutação), a sua ação precisa ser desfeita se uma segunda CNOT é aplicada (ver aspectos termodinâmicos em CASTRO, 2014). Logo, essa transformação unitária deve ser uma função bijetora que é a sua própria inversa, de modo que exista uma involução. Contudo, o polinômio $b^2 \oplus b \oplus 1$ irredutível sobre um campo finito de dois elementos (ou seja, o polinômio não pode ser fatorado em um produto de dois polinômios de grau menor), uma vez que este sempre produz 1 para entradas 0 ou 1, tornando, assim, toda a operação unidirecional. A Figura 1 mostra o protótipo em funcionamento.

No esquema da Figura 1 a chave destrói a própria semente que a gerou, pois o seu estado inicial é definitivamente ignorado. O sistema apresentado aqui é um modelo de chaves verdadeiramente aleatórias que podem ser obtidas a partir da porta quântica denominada controlled-NOT (CNOT).

Conclusões

- O protocolo de criptografia simétrica via porta quântica CNOT apresentado neste trabalho, representa um modelo OTP seguro, pois a chave de criptografia não é obtida a partir de um gerador pseudo-randômico e, sim, através do próprio protocolo de criptografia.

- Este protocolo quântico gera uma chave verdadeiramente aleatória, pois se a chave é negligenciada, ela não poderá ser gerada novamente, uma vez que a mensagem é totalmente destruída no processo de criptografia.

- Este protocolo também pode ser utilizado em conjunto com um protocolo de criptografia assimétrica para a transmissão da chave.

Referências

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.

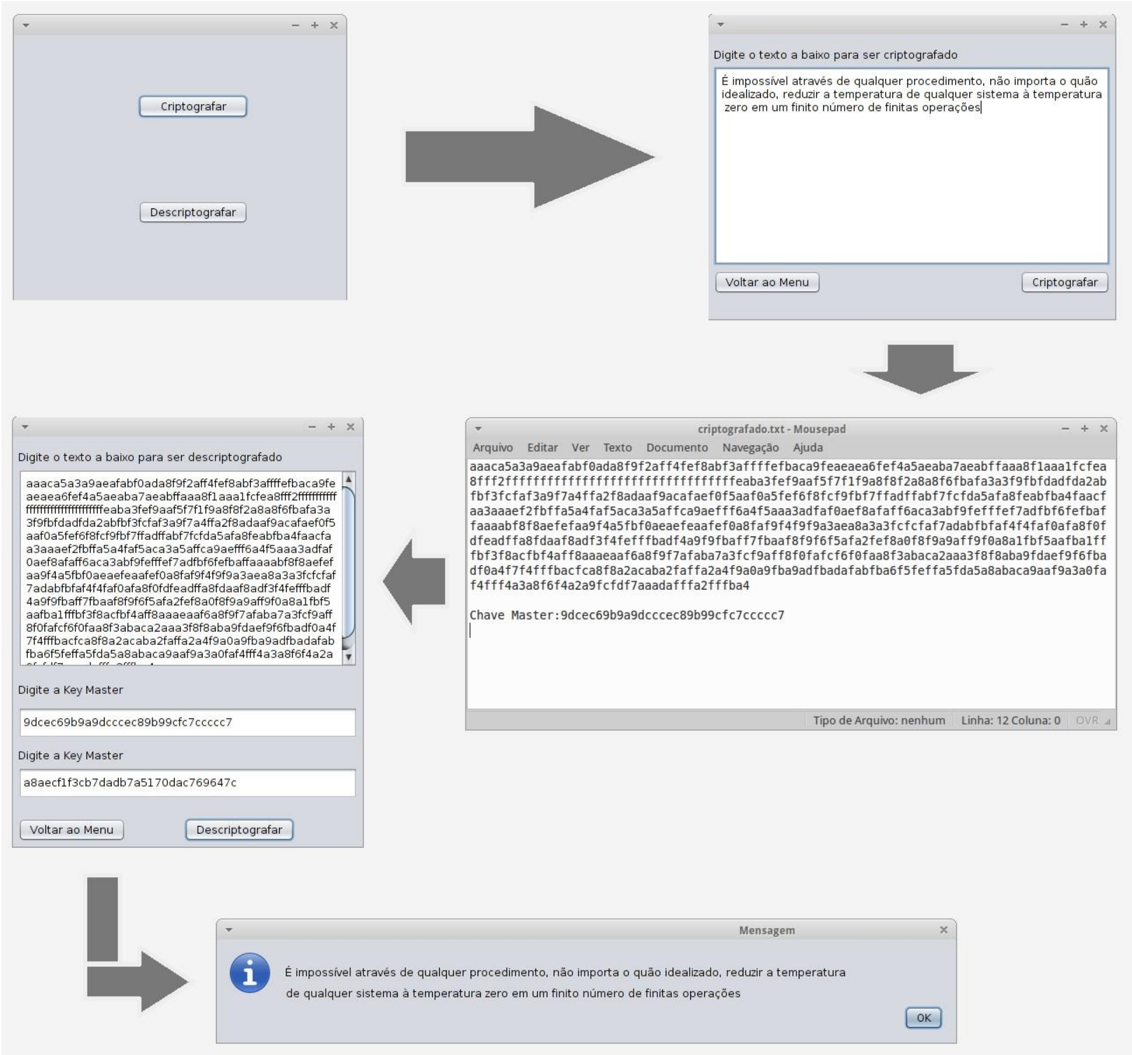

Figura 1. Funcionamento do protótipo de criptografia simétrica via porta lógica CNOT.

Comunicado Técnico, 119

Embrapa Informática Agropecuária
Endereço: Caixa Postal 6041 - Barão Geraldo
13083-886 - Campinas, SP
Fone: (19) 3211-5700
www.embrapa.br/informatica-agropecuaria
sac: www.embrapa.br/fale-conosco/sac/

Ministério da Agricultura, Pecuária e Abastecimento

1ª edição publicação digital - 2015

Expediente

Supervisão editorial: *Stanley Robson de Medeiros Oliveira, Neide Makiko Furukawa*

Normalização bibliográfica: *Maria Goretti Gurgel Praxedes*

Revisão de texto: *Adriana Farah Gonzalez*

Editoração eletrônica: *Neide Makiko Furukawa*

CGPE 12475