Protocolo de criptografia simétrico baseado em permutações unidirecionais

Jacomo Giovanetti Minto Neto[1]
Alexandre de Castro[2]
Edgard Henrique dos Santos[3]
Adauto Mancini[4]

Resumo: Neste artigo, um protocolo de criptografia simétrica utilizando o conceito de permutação unidirecional é apresentado. Os resultados mostram que a probabilidade de inversão da primitiva criptográfica se aproxima de zero mais rápido que o recíproco de um polinômio positivo indicando que uma permutação unidirecional é um gerador eficaz de (pseudo) aleatoriedade e pode ser utilizada na construção de um sistema de criptografia seguro.

Palavras-chave: permutação unidirecional, probabilidade negligenciável, polinômio positivo.

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

[2] Físico, doutor em Ciências, pesquisador da Embrapa Informática Agropecuária, Campinas, SP.

[3] Bacharel em Ciência da Computação, analista da Embrapa Informática Agropecuária, Campinas, SP.

[4] Bacharel em Ciência da Computação, mestre em Ciência da Computação, pesquisador da Embrapa Informática Agropecuária, Campinas, SP.

Introdução

O conceito de permutações de sentido único (unidirecional) está diretamente relacionado à geração de (pseudo) aleatoriedade. Nesse sentido, uma permutação unidirecional pode ser vista como um gerador próprio de (pseudo) aleatoriedade (GOLDREICH; LEVIN, 1989). Neste artigo é apresentado um protocolo criptográfico que utiliza a técnica de permutação unidirecional para gerar (pseudo) aleatoriedade desenvolvida por um dos autores (CASTRO, 2016).

Materiais e Métodos

Nesta seção são apresentadas as definições utilizadas para mostrar uma permutação unidirecional.

Seja $g : \{0,1\}^* \rightarrow \{0,1\}^*$ uma função que preserva seu comprimento e é fácil de calcular para cada entrada, mas difícil de inverter dada a imagem de uma entrada aleatória (HEMASPAANDRA; ROTHE, 1999; RABI. SHERMAN, 1997). Uma função é chamada fortemente unidirecional se, e somente se, a probabilidade P de inversão é negligenciável, ou seja, aproxima-se de zero mais rapidamente do que o recíproco de qualquer polinômio positivo (GOLDREICH, 2004; LEVIN, 2003):

$$\mathcal{P}_{g^{-1}g \leftarrow g} \in O\left(1/poly\right).$$

Em outras palavras, um evento que ocorre com probabilidade negligenciável $\mathcal{P}_{g^{-1}g \leftarrow g} < \frac{1}{poly}$ seria altamente improvável de ocorrer mesmo se fosse repetido um número polinomial de vezes. Caso contrário, a função é chamada fracamente unidirecional se $\mathcal{P}_{g^{-1}g \leftarrow g} > \frac{1}{poly}$.

Considere as entradas de $g(a,x) = (a, f(x) + ax) \in GF_{2^{|x|}}$

i) A função f para todo $x \in \{0,1\}$ tem comprimento de entrada

igual ao comprimento da saída.

ii) A saída $f(x)+ax$ pode ser substituída por uma função *hash* de muitos bits para um bit.

Para entrada par, $a = x$ implica que $f(x)= x$.

Consequentemente, $g(a,x)=(a,x^2 \oplus x)$, pois $x = x^2$ sobre o corpo finito de característica 2. Este corpo finito é uma estrutura algébrica que suporta as operações lógicas x.AND.x' e x.XOR.x', com x, x' = 0, 1.

Para entrada ímpar, $a \neq x$ implica que $f(x)= x^2 \oplus 1$.

Consequentemente, $g(a,x)=(a,x^2 \oplus x \oplus 1)$, pois $x \oplus 1 = x^2 \oplus 1$ sobre o corpo finito de característica 2 (CASTRO, 2016).

Resultados e Discussão

Considere que $x^2 \oplus x \oplus 1 = NOT(x^2 \oplus x)$ para x=0,1, e que $|x^2 \oplus x \oplus 1| \leq 1$.

Logo, g é unidirecional, pois a probabilidade de inverter g, $\mathcal{P}_{g^{-1}g \leftarrow g}$, é negligenciável, pois $\mathcal{P}_{p(x)<1} < \frac{1}{(x^2+x+1)_{GF_2}}$. Pode-se observar que $\mathcal{P}_{g^{-1}g \leftarrow g}$ se aproxima de zero mais rapidamente do que $\frac{1}{(x^2+x+1)_{GF_2}}$, onde $x^2 \oplus x \oplus 1$ é o único polinômio positivo entre os $2^3 = 8$ polinômios sobre (CASTRO, 2016).

Na Figura 1, o quadro geral do protótipo criptográfico que utiliza o conceito de permutação unidirecional:

A Figura 1, mostra o procedimento para realizar a criptografia e descriptografia de um texto simples. Na primeira etapa o texto é inserido no sistema e a função matemática criptográfica é ativada, assim fornecendo o texto cifrado. A seguir, o texto cifrado é novamente inserido no sistema juntamente com a chave gerada na primeira etapa e o texto inicial é recuperado, mostrando que o modelo de permutação unidirecional apresentado neste trabalho representa um cifrador XOR (sistema simétrico) seguro.

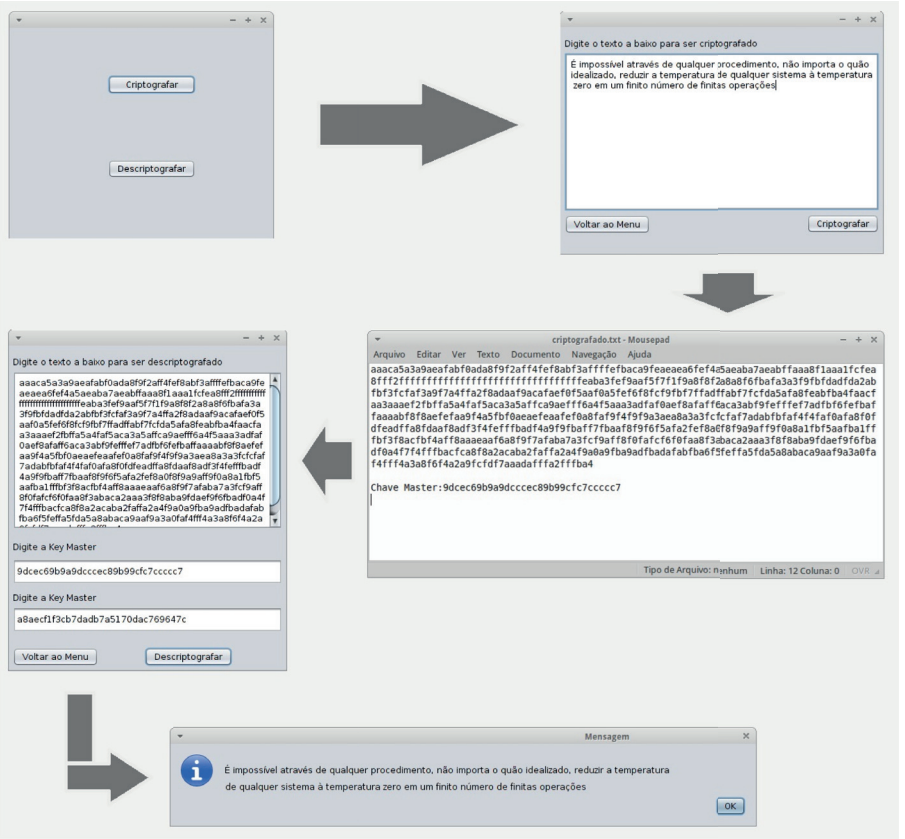

Figura 1. Protocolo de criptografia simétrica via modelo de permutação unidirecional.

Considerações Finais

Neste trabalho, apresentamos um protocolo criptográfico via permutação unidirecional, que representa um modelo seguro, pois a probabilidade de inverter a primitiva criptográfica é negligenciável.

Referências

CASTRO, A. de. **Quantum one-way permutation over the finite field of two elements**. Arxiv: 1609.01541. Disponível em: <https://arxiv.org/abs/1609.01541>. Acesso em: 10 ago. 2016.

GOLDREICH, O. **Foundations of cryptography**: basic tools. Cambridge: Cambridge Univiversity, 2004.

HEMASPAANDRA, L. A.; ROTHE, J. Creating strong, total, commutative, associative one-way functions from any one-way function in complexity theory. **Journal Computer and System Sciences**, v. 58, n. 3, p. 648–659, June 1999. DOI: 10.1006/jcss.1998.1613.

LEVIN, L. A. The tale of one-way functions. **Problems Information Transmission**, v. 39, n. 1, p. 92-103, Jan. 2003. DOI: 10.1023/A:1023634616182.

RABI, M.; SHERMAN, A. An observation on associative one-way functions in complexity theory. **Information Processing Letters**, v. 64, n. 5, p. 239-244, Dec. 1997.