SISTEMA CRIPTOGRAFICO DE CHAVE SECRETA UTILIZANDO A TRANSFORMADA DE CAMPO DE GALOIS

F.M.R. Alencar
A.M.P. Léo
R.M. Campello de Souza
CODEC - Grupo de Comunicações
Departamento de Eletrônica e Sistemas - UFPE
CP. 7.800, 50.741, Recife-PE, Brasil

RESUMO

Neste trabalho é apresentado um novo cifrador de blocos de chave secreta baseado na Transformada de Campo de Galois. O sistema permite implementações com taxa de transmissão unitária, o que resulta em características modulares, possibilitando sua implementação de forma iterativa.

PALAVRAS CHAVE : Cifragem Privada; Cifragem de Bloco; Cifragem Múltipla; Transformada de Campo de Galois.

1. INTRODUÇÃO

Transformadas definidas em Campos de Galois [1] têm tido um papel relevante no contexto da engenharia de comunicações. Inicialmente, tais transformadas foram aplicadas na área de Processamento Digital de Sinais [2], tendo seu espectro de ação se estendido, posteriormente, à área de Codificação de Canal [3], [4]. Neste trabalho, a Transformada de Campo de Galois (GFT) é aplicada à área de Segurança de Dados para a construção de um cifrador de blocos de chave secreta.

Com o avanço tecnológico, a comunicação de dados através de canais inseguros tem se tornado uma prática habitual. Por razões de segurança, procura-se impedir que pessoas não autorizadas tenham acesso aos dados que transitam pela rede de comunicação, o que tem despertado a busca por sistemas de comunicação que garantam a privacidade e a autenticidade da informação transmitida e/ou armazenada. Neste trabalho, é apresentado um sistema criptográfico modularizado que permite garantir a segurança da informação, tornando-a não inteligível a usuários não autorizados, respeitando-se os princípios da difusão e confusão de Shannon [5]. O sistema pode ser utilizado iterativamente como forma de dificultar sua criptanálise, sendo possível estabelecer condições para se transmitir com uma taxa unitária.

Na seção 2 a seguir, são apresentados alguns conceitos básicos referentes à GFT. A descrição do sistema proposto é feita na seção 3, na seção 4 um exemplo ilustrativo é apresentado e na seção 5 são determinadas as condições para se ter um cifrador de taxa de transmissão unitária. Com base nas seções anteriores estabelecemos, na seção 6, algumas conclusões.

2. A TRANSFORMADA DE CAMPO DE GALOIS

O vetor $\{a_i\}$, formado por n elementos de um corpo GF(q) de característica p, e o vetor $\{A_j\}$, formado por n elementos de $GF(q^m)$, formam um par GFT, aqui denotado por $\{a_i\} \longleftrightarrow \{A_j\}$, se

$$A_j = \sum_{i=0}^{n-1} a_i \alpha^{ji} \qquad (1.1)$$

e

$$a_i = \frac{1}{n(\mathrm{mod}\ p)} \sum_{j=0}^{n-1} A_j \alpha^{-ji} \qquad (1.2)$$

onde α é um elemento de ordem n de $GF(q^m)$. Por analogia com a transformada clássica de Fourier, $\mathbf{a} = \{a_i\}$ é dito ser um vetor no domínio do tempo cujo espectro é $\mathbf{A} = \{A_j\}$. Sem perda de generalidade, será considerado o caso em que α é um elemento primitivo de $GF(q^m)$p. A definição do par GFT acima é inteiramente análoga àquela de um par da transformada discreta de Fourier (DFT) [6], onde o núcleo de transformação $e^{-j2\pi/n}$ é substituído por α, uma raiz n-ésima da unidade em $GF(q^m)$.

A GFT possui várias propriedades importantes, sendo de especial interesse no contexto deste trabalho o resultado apresentado a seguir [3].

Teorema 1

Se $\{a_i\} \longleftrightarrow \{A_j\}$, então, $a_i \in GF(q)$ se e só se

$$A_j^{\,q} = A_{((jq))} \tag{1.3}$$

onde $((x))$ denota $x(\mathrm{mod}\,n)$. Deste modo, se a componente espectral A_j é especificada, então as outras componentes espectrais cujos índices estão na classe ciclotômica de j devem ser uma potência de A_j, tal que apenas um membro da classe precisa ser diretamente calculado por (1.1).

3. DESCRIÇÃO DO SISTEMA

A figura 1 abaixo, apresenta o diagrama de blocos do cifrador do sistema criptográfico proposto. A operação de cifragem, envolvendo os blocos mostrados na figura, é descrita a seguir.

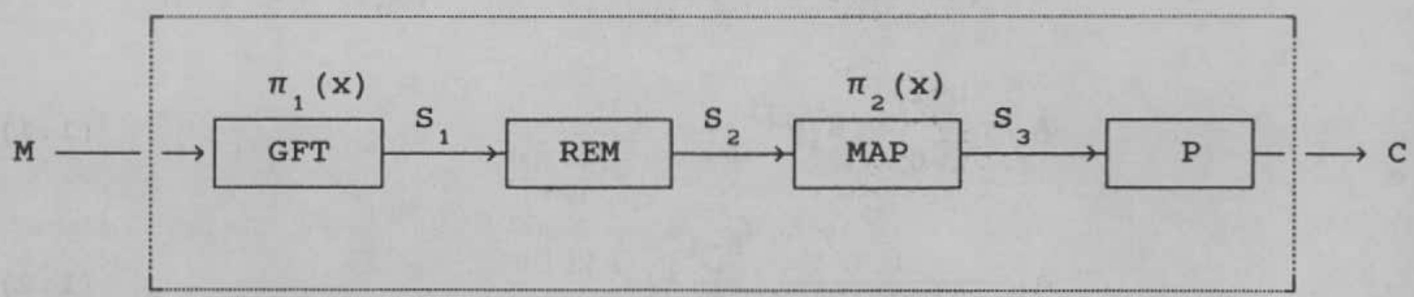

Fig. 1 - Sistema de Chave Privada baseado na GFT - Cifragem

Bloco GFT

Inicialmente, é aplicada a GFT a blocos de texto claro de comprimento n, $M = a_0 a_1 a_2 \ldots a_{n-1}$, com $a_i \in GF(q)$. O espectro de M é a sequência $S_1 = A_0 A_1 A_2 \ldots A_{n-1}$, de elementos de $GF(q^m)$, onde $n|(q^m - 1)$. Esta GFT é computada através de um algorítmo rápido (FFT) [2].

Bloco REM

Tendo em vista o teorema 1, a n-upla S_1 apresenta componentes redundantes, as quais precisam ser removidas. Dessa forma, a saída S_2 do bloco REM contém apenas um representante para cada classe ciclotômica. Além disso, a componente A_0 de S_1, dada pela soma módulo p dos elementos de mensagem, é suprimida neste bloco, sendo posteriormente justaposta à saída do bloco MAP. O comprimento L_2 da sequência S_2 é dada pelo número de polinômios irredutíveis $I_q(k)$ de grau k>1, sobre GF(q), onde k|m, isto é [7],

$$L_2 = \sum_{\substack{k|m \\ k>1}} I_q(k) = \sum_{\substack{k|m \\ k>1}} \left(\left(\frac{1}{k} \sum_{d|k} \mu(d)\, q^{k/d} \right) \right) \qquad (1.4)$$

onde $\mu(.)$ denota a função de Moebius [8]

Bloco MAP

Os elementos de $GF(q^m)$ remanescentes passam a ser representados como m-uplas q-árias, segundo um outro polinômio gerador de $GF(q^m)$, $\pi_2(x)$. Assim, o comprimento L_3 da saída desse bloco será

$$L_3 = mL_2 + 1 \qquad (1.5)$$

Bloco P

O texto cifrado C é então produzido aplicando-se uma permutação P sobre a saída do bloco MAP.

Neste cifrador, a chave secreta $k = (k_1, k_2, k_3, k_4)$ corresponde aos dois polinômios usados para gerar $GF(q^m)$, (k_1, k_2); às componentes A_j remanescentes de S_2, (k_3) e à permutação final P, (k_4). O processo de decifragem é feito como mostrado na figura 2.

4. EXEMPLO

Como exemplo, consideremos o corpo de extensão $GF(2^3)$, onde $q = 2$, $m = 3$ e blocos de mensagem de comprimento $n = q^m - 1 = 7$

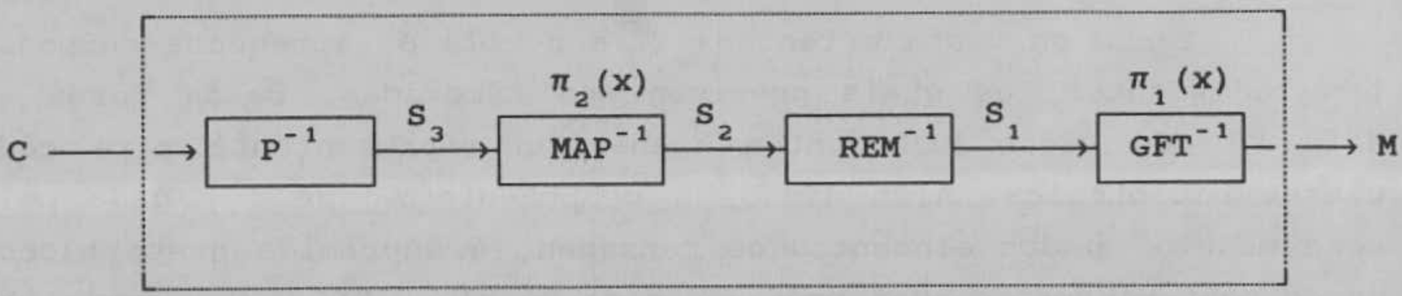

Fig.2 - Sistema de Chave Privada baseado na GFT - Decifragem

são cifrados. Para o corpo escolhido só existem dois polinômios geradores, $\pi_1(x) = x^3 + x + 1$ (k_1) e $\pi_2(x) = x^3 + x^2 + 1$ (k_2). A tabela 1 abaixo mostra os elementos de $GF(2^3)$.

GF(8)	$\pi_1(x) = x^3 + x + 1$	$\pi_2(x) = x^3 + x^2 + 1$
0	000	000
1	001	001
α	010	010
α^2	100	100
α^3	011	101
α^4	110	111
α^5	111	011
α^6	101	110

Tab. 1 - Elementos de $GF(2^3)$

Seja $M = (a_0 a_1 a_2 a_3 a_4 a_5 a_6) = (1011001)$ a mensagem que se deseja cifrar. Conforme a figura 2, após aplicarmos a GFT, determina-se a n-upla S_1

$$S_1 = (A_o A_1 A_2 A_3 A_4 A_5 A_6) = (0\ \alpha^3\ \alpha^6\ \alpha^4\ \alpha^5\ \alpha^2\ \alpha)$$

Da expressão (1.4), concluimos que apenas $[(2^3-2)/3] = 2$ componentes do vetor S_1, correspondentes às classes ciclotômicas mod 7 sobre GF(2), são suficientes para a determinação das demais. Usando-se a chave secreta k (k_3= 4, 6), obtém-se

$$S_2 = (A_4 A_6) = (\alpha^5\ \alpha)$$

Cada componente A_j de S_2 será mapeada numa tripla binária segundo a representação dos elementos de GF(2^3), considerando-se como polinômio gerador o polinômio $\pi_2(x)$, conforme indica a tabela 1. Assim,

$$S_3 = (011\ 010)$$

Neste ponto, faz-se necessário acrescentar, por justaposição, um bit que corresponderá à componente A_0 retirada. Desse modo,

$$S_4 = (0\ 011\ 010)$$

Finalmente, à mensagem S_4 é aplicada a permutação final P, escolhida previamente pelas partes, segundo a chave secreta k (k_4), obtendo-se o criptograma C = ($c_0 c_1 c_2 c_3 c_4 c_5 c_6$).

5. CIFRADOR DE TAXA UNITÁRIA

Nesta seção é considerado que o sistema criptográfico proposto utiliza blocos de texto claro de comprimento $n = q^m - 1$ primo. O interesse em se ter n primo reside no fato de, neste caso, ser possível enviar informações com uma taxa de transmissão unitária.

Assim, considerando que ($q^m - 1$) é primo, pode-se afirmar que m é primo e q = 2 [8]. Portanto, todos os polinômios irredutíveis sobre GF(q) terão grau k = m, obtendo-se na saída do bloco REM, segundo a expressão (1.4), uma sequência de comprimento

$$L_2 = \frac{1}{m} \sum_{d|m} \mu(d)\ q^{m/d} \tag{1.6}$$

ou

$$L_2 = \frac{1}{m} \left(2^m - 2 \right) \tag{1.7}$$

Desta forma, o comprimento da saída do bloco MAP segundo a expressão (1.5) e, consequentemente, o comprimento do criptograma C, será

$$L_3 = m \left[\frac{1}{m} (2^m - 2) + 1 \right]$$

$$\therefore$$

$$L_3 = 2^m - 1 = n$$

Portanto, o comprimento da sequência de entrada será igual ao comprimento da sequência de saída, o que indica taxa de transmissão unitária. Nestas condições o sistema passa a apresentar características modulares que permitem sua implementação de forma iterativa. O número de iterações a serem realizadas, bem como a diversidade com respeito às chaves a ser empregadas em cada módulo, é função do nível de segurança desejado.

Considerando o caso de maior interesse prático mencionado, o fator de trabalho W relativo à uma busca exaustiva da chave para um único módulo do sistema, pode ser determinado examinando-se cada um dos blocos da figura 1:

<u>Blocos GFT e MAP</u> - Como todos os polinômios são primitivos [7], tem-se $(n - 1)/m$ possibilidades para cada bloco.

<u>Bloco REM</u> - Cada uma das $(n - 1)/m$ classes ciclotômicas tem m elementos. Considerando que as mesmas podem ser escolhidas em qualquer ordem, tem-se $(m)^{(n-1)/m} . [(n - 1)/m]!$ possibilidades.

<u>Bloco P</u> - Existem n! permutações de grau n.

Portanto, o fator de trabalho é

$$W = \left(\frac{n-1}{m} \right)^2 (m)^{\frac{n-1}{m}} \left(\frac{n-1}{m} \right)! \; n! \qquad (1.8)$$

Como uma situação de interesse prático é sugerido o valor de comprimento de bloco n = 127, que apresenta um fator de trabalho da ordem de 2^{700}. Uma busca exaustiva sobre o espaço de mensagens, objetivando a determinação da mensagem M que produziu um dado texto cifrado C conhecido, representa um fator de trabalho de $2^{127} - 1$ (a mensagem $a_i = 0$, $0 \leq i \leq (n-1)$, não é utilizado). A criptanálise do sistema através de pares de texto claro e texto cifrado, conhecido ou escolhido, aparentemente, não produz nenhuma redução significativa nestes valores.

6. CONCLUSÕES

Neste trabalho foi introduzido um sistema criptográfico de chave privada visando preservar o sigilo dos dados transmitidos por canais de comunicação inseguros, que tem por base a aplicação da Transformada Discreta de Fourier definida em um Campo de Galois. Foram utilizados os princípios da confusão e difusão propostos por Shannon de forma a fortalecer o sistema contra possíveis ataques. Para aumentar a velocidade de operação do sistema (cifragem e decifragem), as transformadas direta e inversa são computadas através de um algorítmo FFT. Foram estabelecidas as condições para que o sistema apresente uma taxa de transmissão unitária, fato esse que possibilita sua implementação de forma iterativa. O valor de comprimento de bloco n = 127 é proposto como padrão, uma vez que apresenta uma alta resistência aos ataques tipicamente aplicados a este tipo de sistema.

AGRADECIMENTOS

Este trabalho recebeu apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e do Banco do Brasil S.A.

7. REFERÊNCIAS

[1] J.M. Pollard, "The Fast Fourier Transform in a Finite Field", Mathematics of Computation, vol. 25, pp. 365-374, Abril 1971.

[2] R.E. Blahut, "Fast Algorithms for Digital Signal Processing", Addison-Wesley, 1985.

[3] R.E. Blahut, "Transform Techniques for Error Control Codes", IBM Journal of Research and Development, vol. 23, pp. 229-315, Maio 1979.

[4] R.M. Campello de Souza, "A Transform Based Decoding Algorithm for Cyclic Codes via Non Preserving Permutations", IEEE Int. Symposium on Information Theory, San Diego, USA, Janeiro 1990.

[5] C.E. Shannon, "Communication Theory of Secrecy Systems", Bell System Technical Journal, vol. 28, pp. 656-715, Outubro 1949.

[6] D.G. Myers, "Digital Signal Processing: Efficient Convolution and Fourier Transform Techniques", Prentice Hall, 1990.

[7] R.J. McEliece, "Finite Fields for Computer Scientists and Engineers", Kluwer, 1987.

[8] D.M. Burton, "Elementary Number Theory", Allyn and Bacon, 1976.