Criptografia de Voz em Tempo Real utilizando o Algoritmo de Exponenciação Modular de Montgomery

Renan Rizzatti Tochetto
Universidade de Passo Fundo – Curso de Engenharia Elétrica
99042 – 800, Campus São José, Passo Fundo, RS
E-mail: 63289@upf.br

Blanca R. Maquera Sosa
Universidade de Passo Fundo – Curso de Engenharia Elétrica
99042 – 800, Campus São José, Passo Fundo, RS
E-mail: blamaso@upf.br

RESUMO

Neste trabalho apresenta-se criptografia de voz em tempo real, utilizando os algoritmos de criptografia RSA juntamente com o algoritmo de Exponenciação Modular de Montgomery [1].

Com o avanço das telecomunicações e processadores digitais de sinais, os algoritmos de criptografia de texto, voz e imagens foram cada vez sendo mais eficientes e sofisticados devido à segurança dos dados. A base e a implementação destes algoritmos estão nas diversas áreas da Matemática Pura e Aplicada [2] e linguagens de programação respectivamente. A segurança do método RSA se baseia na dificuldade da fatoração de números inteiros extensos.

O código RSA é basicamente o resultado de dois cálculos matemáticos. Um para cifrar e outro para decifrar. O RSA utiliza duas chaves criptográficas, uma chave pública e uma privada. No caso da criptografia assimétrica tradicional, a chave pública é usada para criptografar a voz e a chave privada é usada para decriptografar a voz [3].

O algoritmo de exponenciação modular de Montgomery é composto de uma repetição de multiplicações modulares. Neste algoritmo é utilizado o método de exponenciação binária. A idéia básica do método binário é calcular uma exponenciação utilizando a expressão binária do expoente. A operação de exponenciação é desmembrada em uma série de quadrados e operações de multiplicação pelo uso do método binário. Estes parâmetros para uso de criptografia são muito eficientes para processamento de voz, uma vez que aceleram o cálculo da exponenciação [4].

Qualquer tipo de informação que necessite ser armazenada em um sistema computacional ou transmitida em um canal de transmissão necessita passar por um tratamento de sinal, ou seja, uma codificação de fonte. A codificação digital de voz utiliza a amostragem e a quantização do sinal para conseguir a menor taxa de codificação possível e a melhor qualidade do sinal sintetizado. A codificação de fonte utilizada neste artigo foi a modulação DPCM, cujo processo de codificação minimiza a redundância das amostras altamente correlacionadas, que são características de um sinal de voz [5].

Este sistema de criptografia de voz foi implementado no kit DSK TMS320c6711 da Texas Instruments [6], e obteve resultados satisfatórios no que respeita a velocidade de criptografia e qualidade da voz no receptor.

Palavras-chave*: Criptografia, Algoritmo de Montgomery, Modulação DCPM, Processamento digital de sinais.*

Referências

[1] WU, Chia-Long, Der-Chyuan LOU, Te-Jen CHANG, "An Efficient Montgomery Exponentiation Algorithm for Cryptographic Applications" Abril de 2005.

[2] Coutinho, S. S. Números *Inteiros e Criptografia RSA*- IMPA-SBM (1997).

[3] BARBOSA, Luis Alberto de Moraes, Luis Fernando B Braghetto, Marcelo Lotierso Brisqui, Sirlei Cristina da Silva, "RSA Criptografia Assimétrica e Assinatura Digital" Campinas, Julho de 2003.

[4] NBISSOLI, Marçal Luiz, Dr. Edward David Moreno Ordonez. “impacto da multiplicação e exponenciação modular em Hardware no algoritmo RSA”. Centro Universitário “Eurípides De Marília” – Univem.

[5] COUCH II, Leon W.. Modern communication systems: principles and applications. Englewood Cliffs: Prentice Hall, 1995. 598 p.

[6] http://www.ti.com/ww/br/