196 **IMPLEMENTAÇÃO DO ALGORITMO RIJNDAEL EM LINGUAGEM VHDL PARA SÍNTESE EM LÓGICA PROGRAMÁVEL.** *Alex Fragoso Panato, Marcelo Boeira de Barcelos, Ricardo Augusto da Luz Reis* (Instituto de Informática UFRGS).

A criptografia é uma necessidade atual nos sistemas de comunições modernos. Para seu funcionamento, é necessário que o algoritmo de encriptação e decriptação seja implementado em software ou em hardware. O presente trabalho procura adequar o algoritmo Rijndael (novo padrão) em um hardware programável da família Altera, viabilizando aplicações que necessitem alto desempenho para processamento em massa de criptografia, como servidores web. Tendo em vista que há alguns estudos da implementação deste algoritmo elaborados, mas não usando sua plena potencialidade, este trabalho visa a construção de abordagens ao problema, enfocando o desempenho de processamento e a economia de custos de fabricação ou implementação. Para o seu desenvolvimento, foi escolhida a plataforma FLEX10k da Altera, por esta ser um padrão de mercado e possuir trabalhos para comparação. Por este mesmo motivo, foi escolhida a linguagem VHDL para especificação do circuito. Foram utilizadas as ferramentas de software Leonardo Spectrum para a escrita de códigos e o Max+Plus2 da Altera. Procurou-se desenvolver o dispositivo por blocos, testando e aferindo o desempenho e custo de cada bloco individualmente e, posteriormente, em conjunto. Na primeira etapa procurou-se desenvolver a versão de alto desempenho para, posteriromente, iniciar-se o estudo da verão de baixo custo. Os resultados preliminares indicam um alto desempenho da verão performance, comparada a outros trabalhos publicados. Para tal dispositivo, os recursos do componente programável utilizado ficam perto de seu limite. O desempenho de uma impelmentação em hardware programável é muito superior às inplementações em softwares, logo, tende a ser uma alternativa economicamente viável de tratamento de dados criptografados. Uma vez tendo a ampliado as comparações de desempenho com os trabalhos publicados, parece válido, também, que se procure opções de implementação em novos componentes programáveis, pois suas novas versões tem características mais robustas.