HARDWARE/SOFTWARE CO-DESIGN: UM ESTUDO DE CASO USANDO CRIPTOGRAFIA DE CHAVE PÚBLICA

Gabriel Marchesan ALMEIDA[1] , Luciano Lores CAIMI[2], Daniel Gomes MESQUITA[3]
Universidade Regional Integrada do Alto Uruguai e das Missões
Departamento de Engenharias e Ciência da Computação
Av. Universidade das Missões 464
Santo Ângelo- RS -98802 470
{gmarchesan, caimi}@urisan.tche.br; mesquita@lirmm.fr

RESUMO

Algoritmos de criptografia estão evoluindo constantemente, no sentido de suprir as necessidades de segurança. A aritmética modular é parte integrante destes algoritmos, especialmente nos sistemas criptográficos de chave pública. Para obter melhor desempenho do sistema e também manter sua integridade física, é desejável implementar sistemas criptográficos em hardware. Contudo, muitos algoritmos criptográficos requerem a implementação de aritmética modular, especificamente multiplicação modular, para operandos com mais de 1024 bits de comprimento. Adicionalmente, o algoritmo deve ser flexível o bastante para suportar protocolos independentes, uma característica da maioria dos sistemas de criptografia modernos. Reconfigurabilidade, em especial reconfiguração em tempo de execução é uma questão crítica para possibilitar o balanceamento entre os algoritmos criptográficos requeridos para os algoritmos dos protocolos independentes. A reconfiguração dinâmica de FPGAs é uma alternativa viável para este objetivo. Além do emprego de técnicas de reconfiguração dinâmica, dada a complexidade de aplicações que envolvem criptografia. Outra questão de suma importância, dada a complexidade de um sistema criptografico, é o projeto integrado hardware/software do sistema (*co-design*). A implementação de sistemas digitais complexos implica o uso de uma grande quantidade de ferramentas de projeto, geralmente compondo um sistema de desenvolvimento integrado. Estes sistemas de desenvolvimento são formados por métodos e ferramentas que permitem a modelagem, validação e síntese dos componentes eletrônicos, através de um conjunto de modelos formais e/ou informais. Ferramentas de co-design devem ser capazes de dar suporte a diferentes técnicas de projeto para cada componente e permitir também especificar a forma de interação destes componentes. As ferramentas disponíveis hoje no mercado fornecem a equipes de projetistas experientes a capacidade de elaborar em poucas semanas, projetos de circuitos que equipes de projetistas há 10 anos atrás levavam meses desenvolvendo. Este poder não é e provavelmente nunca será suficiente para suprir a necessidade de desempenho requerida para o projeto de produtos tecnológicos no estado da arte. Assim, ferramentas e modelos estão sempre em constante evolução na busca de soluções mais rápidas e de mais baixo custo. Após a extensa automatização do nível físico de abstração, os esforços hoje apontam para a busca da automatização do nível sistêmico, onde as primitivas de projetos são objetos complexos tais como processadores, memórias, software, sistemas operacionais e acionadores de dispositivos de entrada e saída. A maioria dos sistemas digitais modernos são programáveis e configuráveis, consistindo de componentes de software e hardware. Pretende-se pois pesquisar e empregar sistemas, e eventualmente propor e desenvolver ferramenta(s) de apoio ao projeto integrado de hardware e software para sistemas criptográficos.

PALAVRAS-CHAVE: Criptografia de Chave Pública, RSA, FPGAs.

---

[1] Bolsista de IC (Graduando do Curso de Ciência da Computação – URI –Santo Ângelo)
[2] Orientador do Projeto (Mestre em Ciência da Computação – URI –Santo Ângelo)
[3] Co-Orientador do Projeto (Doutorando em Microeletrônica – LIRMM – França)