OTIMIZANDO PROCESSADORES EXTENSÍVEIS COM CONJUNTO DE INSTRUÇÕES EM RESTRIÇÕES DE DADOS DE LARGURA DE BANDA

Cláudio Roberto Ribeiro – RA 095387

Professor Paulo Cesar Centoducatte

(Instituto de Computação – Unicamp)

(Optimizing Instruction-set Extensible Processors under Data Bandwidth Constraints - Kubilay Atasu, Robert G. Dimond, Oskar Mencer, Wayne Luk, Can Ozturan e Gunhan Dundar - DATE 2007)

Objetivos

A presente pesquisa apresenta uma metodologia através da Programação Linear Inteira extraindo um conjunto mais rentável de extensões sobre instruções, criando arquiteturas otimizadas para processadores extensíveis com restrição de largura de banda. Diferente das abordagens anteriores aplicou-se uma diferenciação entre números de entradas e saídas por extensões de conjunto de instruções e número de registro de portas de arquivo de registros. Essa diferenciação torna a nossa abordagem aplicável a arquiteturas que incluem estado de registros arquitetonicamente visíveis e de canais dedicados a transferência de dados.

Metodologia

Utilizando um conjunto de instruções de extensão em código C através da arquitetura Tensilica Xtensa, com informações sobre banda de dados, tempo e latência de transferência, identificou-se um conjunto de instruções mais rentável baseada no ILP. Considerando a cobertura e overhead de transferência de dados, integrou-se a técnica dentro de um compilador, gerando implementações do processador ASIC personalizado a partir do código C. Considerando a área de silício como uma restrição primária, sendo explorado o impacto das diferentes áreas de restrições no número de ciclos de execução, foi aplicado o framework de Trimaran para a geração de controle de informação. Trabalhando com Elcor e depois de aplicar otimização clássicas, implementou-se algoritmos para identificar as extensões. Foi utilizado o CPLEX para resolver problemas da ILP.

Criou-se um modelo baseado na ILP, estruturando dentro de classes de isomorfismo, foi gerada uma máquina de alto nível (MDES) para as instruções selecionadas. Para cada instrução selecionada, foi substituído pelo código correspondente. Depois disso, foi aplicado o padrão Trimaran e finalmente criou-se o código assembly e foram coletadas as estatísticas de programação.

Resultados

Aplicou-se algoritmos nos quatro tipos de criptografias, AES, DES, SHA e Hash com blocos básicos bem grandes, para demonstrar a escalabilidade. Em contraste às extensões que nós criamos podem ter um número ilimitado de entradas e saídas. Otimizou-se a velocidade de 1.1x para 1.3x no SHA, de 1.5x para 1.9x no DES, de 3.4x para 4.3x de decriptografia no AES , e de 2.6x para 2.8x de Criptografia no AES. Com portas de arquivo de registro adicionais obteve-se a melhora de velocidade de 1.6x no SHA, 2.6x no DES, 5.9x de decriptografia no AES, e 3.8x para Criptografia no AES. Com um arquivo de registro com 2 portas de leitura e 1 de escrita, foi criado automaticamente uma CPU implementando as extensões selecionadas para cada restrição de área através da sintetização de cada núcleo UMC's 130nm usando Synopsys Design Compiler e Cadence SoC Encounter. O maior desempenho do processador de decriptografia AES gerado, ocorre com aumento de apenas 35% sob a área do processador não estendida, enquanto oferecida uma velocidade de 4.3x. Consequentemente ocorreu o pior caso com restrição de 200MHz e para evitar a diminuição do clock do relógio do processador, utilizou-se a técnica de conjunto de instruções de ciclos múltiplos, sendo esta a parte de maior consumo de tempo do algoritmo , foi criado um modelo de algoritmo, que repetidamente resolve os problemas ILP. As estatísticas da ILP, associadas com a primeira repetição da geração de modelo algoritmo no maior bloco básico de cada marca de referência dada a uma restrição de (4,4) nas entradas e saídas é o tempo de resolução de apenas poucos segundos. Entretanto, pode exceder uma hora como acontece para SHA. Observou-se um tempo de execução total de 13 segundos para criptografia AES, 20 segundos para decriptografia AES, 2.5 minutos para DES, e por volta de 21.5 horas para SHA. Obteve-se ótimos resultados na ILP em todos os casos.

Conclusões

Essa pesquisa demonstra que o processador com duas portas de leitura de registros e uma porta de escrita, gera 4.3x de velocidade com apenas 35% da área de cobertura, com potencial de acréscimo de portas de arquivos de registro, melhorando o desempenho acima de 6.6. Através de extensões com conjunto de instruções otimizadas com o modelo ILP e integrando as informações sobre largura de banda e custos de transferência, avalia-se o acesso usando as implementações ASIC atuais para demonstrar que nossos processadores automaticamente personalizados cumprem o cronograma dentro da área de silício.