A novel cache architecture with enhanced performance and security

WANG, ZHENGHONG; LEE, R.B. A novel cache architecture with enhanced performance and security. Proceedings of the 2008 41st IEEE/ACM International Symposium on Microarchitecture, p. 83-93, 2008.

Thomaz Eduardo de Figueiredo Oliveira - ra036272

Um cache ideal deve possuir quatro características fundamentais: baixa taxa de erros e baixo tempo de acesso, qualidades difíceis de se implementar simultaneamente; consumo eficiente de energia, devido ao superaquecimento e às limitações de bateria dos sistemas móveis; e garantia de segurança, principalmente contra os novos ataques *side-channel*, que se baseiam nas diferenças de tempo dos acertos e erros do cache.

O maior problema em propor uma solução à questão da segurança é a grande perda de performance. Desta forma, o artigo introduz uma nova arquitetura de cache, cujo objetivo é reunir as quatro características citadas acima.

A arquitetura se baseia em dois conceitos: o *Remapeamento dinâmico (Dynamic Re-mapping)* e o *Mapeamento lógico direto (LDM)*.

O *remapeamento dinâmico* consiste em mapear os endereços de memória para o cache de forma dinâmica. Por meio de uma *tabela de remapeamento (RMT)* os índices da memórias são mapeados às linhas reais do cache.

Ao trocar a *RMT*, um distinto mapeamento é feito.

Para diminuir a taxa de erros, propõe-se um maior índice de cache, porém, sem aumentá-lo fisicamente. Isto é feito por meio do *mapeamento lógico direto*.

A implementação física de *registros de número de linha (LNreg)* permite relacionar a linha real de um cache com um suposto cache lógico *(LDM cache)* com k bits de índice extras.

Assim, o *LNreg* é a representação física das *RMTs*. Seus campos conterão o ID da *RMT* e o número do índice.

Para isso o decodificador de endereços precisará ser modificado. Ao invés de buscar uma série de índices constantes, ele fará uma busca nos conteúdos do *LNreg*.

A outra mudança é o algorítmo de substituição de linhas *(SecRAND)*, que objetiva garantir a segurança da arquitetura. Os erros de tag são tratados como em um cache comum; porém com o *LDM*, os erros de índice precisam ter um tratamento especial.

Na ocorrência de um erro de índice, uma nova linha é escolhida aleatoriamente como vítima a ser substituida. Após a decisão, o *LNreg* é atualizado com os novos valores.

As comparações com os modelos atuais comprovam a eficiência e economia da nova arquitetura. O tempo de acesso ficou em média 1% maior e o o consumo energético apenas 2%. Além disso, o novo cache atingiu as menores taxas de erros.

Com o *SecRAND* o cache consegue evitar que atacante possa prever quais linhas do cache físico um processo está usando. Impedindo a concretização de ataques *side-channel*.