Saturday, July 12. 2008

Software crypto on CMT

Lawrence Spracklen wrote a really interesting article about cryptography done in software on CMT. This sounds counterintuitive at first, as cryptography is considered as a computational intensive task and thus considered as a tasks for fast superscalar cores. But according to the article from Lawrence this is a implementation issue. Take the strength of the CMT architecture, and the result is a little bit different: As a result, as the number of strands is increased, performance scales almost linearly. Indeed, for Niagara, per-core Kasumi performance is around 8 times the performance of a single strand, and per-chip Kasumi performance is close to 64X single-strand performance. Indeed, single-core Kasumi performance is around 1.3X the performance of a single-core of a 3GHz Xeon processor.

Posted by Joerg Moellenkamp in English, Oracle at 10:01