Integer Factoring Utilizing PC Cluster

Kazumaro Aoki

NTT
1-1 Hikari-no-oka, Yokosuka-shi, Kanagawa-ken, 239-0847 Japan
maro@isl.ntt.co.jp

The integer factoring problem is one of the oldest and important problems and it is considered as hard, i.e., the problem cannot be solved in polynomial time for the worst case, because the security of RSA is heavily dependent on the difficulties of integer factoring. As is well known, hardware technology is progressing rapidly from year to year and it seems that the time is now ripe to factor 1024-bit integers. Recently, there have been many studies that have investigated the possibility of 1024-bit integer factoring.

Base on the progress in hardware, several studies claim that special purpose hardware for integer factoring can factor a 1024-bit integer in a year at a reasonable cost. However, there seems to be no published report that the world record for integer factoring was superseded by this kind of hardware. A supercomputer is a promising candidate for factoring large integers, but it is not cost effective. Considering a limited budget, a PC cluster seems to be the most cost effective hardware for factoring a large integer. Actually, recent world records were superseded using a PC cluster.

This presentation introduces the usage of a PC cluster for integer factoring. In particular, the experience of achieving the world record will be discussed. Our factoring team wrote several tens of thousands of lines of source code, and used hundreds of PCs. They spent several months to achieve the record. We did not expect any PC miscomputation, however, it is still of serious concern. It is hoped that this presentation provides a better understanding of what has been accomplished toward world-class integer factoring.

L. Goubin and M. Matsui (Eds.): CHES 2006, LNCS 4249, p. 60, 2006.