School of Computer Science
Ph.D. Final Defense
by

YU-HSIN LI

FINDING MINIMUM GAPS AND DESIGNING KEY DERIVATION FUNCTIONS

ABSTRACT

"While the priest climbs a post, the devil climbs ten". The problem size gets larger as computers become faster. Using naive algorithms, even equipped with fast CPUs and large memories, computers still cannot handle many problems of certain size. Some searching tasks, however, can be answered with the help of the algorithmic technique, such as time and space trade-off.

Let n and k be positive integers, $n > k$. Define $r(n,k)$ to be the minimum value of

$$\left|\sqrt{a_1} + \cdots + \sqrt{a_k} - \sqrt{b_1} - \cdots - \sqrt{b_k}\right|$$

where $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k$ are positive integers no larger than n. It is important to find a tight bound for $r(n,k)$, in connection to the sum-of-square-roots problem, a famous open problem in computational geometry. The current best lower bound and upper bound are far apart. For exact values of $r(n,k)$, only a few simple cases have been reported so far, and they can be found easily using exhaustive search. The new algorithm is developed to find $r(n,k)$ *exactly* in $n^{k+o(k)}$ time and in $n^{\lceil k/2 \rceil + o(k)}$ space. Space usage is decreased dramatically along with little increase in time, compared to an intuitive trade-off method. Our algorithm reduces time for swap-in and swap-out, minimizing the total running time. The problem is solved in size that was infeasible for a naive trade-off scheme. We also present lots of numerical data.

The time and space trade-off technique has its limitation. For some problems, when space is reduced to a certain extent, time will be increased exponentially. The trade-off technique does not apply to this situation. We want to explore such a property to discourage trade-off attacks.

Key generation is an important part of symmetric-key encryption algorithms, such as AES. A key derivation function can be used to generate symmetric cipher session keys. As CPU technology advances, key derivation functions are more vulnerable to off-line brute force attacks. Based on the Memory Wall problem, we propose a simple number theoretic way to mitigate exhaustive search attacks. We also present a formal definition of memory bounded functions. On one hand, if attackers try to reduce memory usage, they are forced to spend dramatically more time. On the other hand, a memory-bound security scheme will minimize the difference between high-end and low-end computers. Trade-off attacks will hence be deterred.

Date: Wednesday, March 23, 2011
Time: 4:00 P.M.
Place: Devon Energy Hall (DEH) Forum room 320

Committee Members:
Dr. Qi Cheng, Chair
Dr. Sudarshan Dhall (CS)
Dr. Changwook Kim (CS)
Dr. Krishnaiyan Thulasiraman (CS)
Dr. Ralf Schmidt (MATH)

Reading Copy of dissertation available in the Computer Science office

For accommodations on the basis of disability, please call 325-4042.