Goldreich, Oded; **Goldwasser, Shafi**; **Halevi, Shai**

Public-key cryptosystems from lattice reduction problems. (English) Zbl 0889.94011

Kaliski, Burton S. jun. (ed.), Advances in Cryptology - CRYPTO '97. 17th annual international cryptology conference. Santa Barbara, CA, USA. August 17–21, 1997. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 1294, 112-131 (1997).

A lattice $L(B)$ is defined as the integral combinations of basis vectors of the basis $B = \{b_1, \ldots, b_n\}$. There are two difficult problems related to lattices. The first one is the CVP (Closest Vector Problem), i.e. given a lattice $L(B)$ with basis B and an arbitrary vector v, find a vector in the lattice $L(B)$ that is closest to v in some norm. The second one is the SBP (Smallest Basis Problem), i.e. find a basis B' for a lattice $L(B)$ such that the orthogonality defect (i.e. $\prod |b_i| / |\det(B)|$) is the smallest.

The first problem is known to be NP-hard for any l_p-norm. For the second no known polynomial time solution is known.

The proposed cryptosystem makes use of two bases for the same lattice L.

The basis B has a small orthogonality defect (i.e. the orthogonality defect of the inverse matrix B^{-1}). The basis B' has a large one. The matrix B' is made public.

The observation now is that if v is a random vector and e is a random noise vector satisfying some properties then if $B'v + e$ is known, v can be reconstructed in a simple way if B is known, but it is difficult to reconstruct v if B is not known. The proposed cryptosystem makes use of this observation by embedding a message in a more or less random vector v and then calculating $B'v + e$ for some randomly chosen noise vector e satisfying some extra conditions. An attacker has to solve either the CVP or the SBP to obtain v and hence to find the message.

For the entire collection see [Zbl 0870.00047].

Reviewer: Herman J. Tiersma (Diemen)

MSC:

94A60 Cryptography
68W30 Symbolic computation and algebraic computation
11Y16 Number-theoretic algorithms; complexity

Keywords:

public-key cryptosystems; lattice reduction problems; closest vector problem; smallest basis problem; orthogonality defect