Solving Generalized Small Inverse Problems

http://www.firstlight.cn 2010-04-21

We introduce a ``generalized small inverse problem (GSIP)" and present an algorithm for solving this problem. GSIP is formulated as finding small solutions of $f(x_0, x_1, \ldots , x_n)=x_0 h(x_1, \ldots , x_n)+C=0 (\bmod \; M)$ for an n-variate polynomial h, non-zero integers C and M. Our algorithm is based on lattice-based Coppersmith technique. We provide a strategy for construction of a lattice basis for solving $f=0$, which are systematically transformed from a lattice basis for solving $h=0$. Then, we derive an upper bound such that the target problem can be solved in polynomial time in $\log M$ in an explicit form. Since GSIPs include some RSA related problems, our algorithm is applicable to them. For example, the small key attacks by Boneh and Durfee are re-found automatically.

存档文本