Abstract

In this paper, we elaborate the security threats that exist on hybrid cryptosystem based on satisfiability problem. In such system the encryption is carried out by generating 3-SAT clauses by random insertion of literal in a given 2-SAT clause instance. The solution of 2-SAT clause instance gives the secret key and the placement of literal for conversion to 3-SAT gives the position vector. Two crucial parameter for encryption. Thus, the system seems to be robust. However, the security of such system is at stake, when we apply the polynomial solvability formulation of 3-SAT[2]. Here, we propose a chosen plain text attack on such system using polynomial solvability of 3-SAT as reported in[3]. We observe that the complexity of the attack is
Hybrid Cryptosystem based on 2-SAT & 3-SAT and the Implications of Polynomial Solvability of 3-SAT

O(3n), where n is the number of clauses.

**Reference**


**Index Terms**

Computer Science Communications
Hybrid Cryptosystem based on 2-SAT & 3-SAT and the Implications of Polynomial Solvability of 3-SAT

Key words

Public Key
Satisfiability

NP-complete

Secret key