Summary on the Vulnerability of the Knapsack Encryption Algorithm

Xiaoxiao Jiang > xjiang3@scu.edu | Weihao Liu > wliu4@scu.edu

Introduction of The Knapsack Encryption Algorithm

At its core, the Knapsack Encryption Algorithm relies on the difficulty of the subset-sum problem in combinatorial mathematics, where the goal is to find a subset of numbers that add up to a given total. In the context of encryption, these numbers are used to create a public key, with a corresponding private key known only to the receiver.

Vulnerabilities Discovered

In 1984 Adi Shamir published an attack on the Merkle-Hellman cryptosystem which can decrypt encrypted messages in polynomial time without using the private key. Researchers discovered that the algorithm's reliance on the subset-sum problem was its Achilles' heel. The specific vulnerabilities identified include:

- Lattice-Based Attacks (1982): Discovered by Adi Shamir, these attacks leverage the LLL (Lenstra–Lenstra–Lovász) lattice reduction algorithm to break the knapsack-based cryptosystems. Shamir demonstrated that most knapsack problems could be transformed into lattice problems, which the LLL algorithm could then solve efficiently, rendering the encryption ineffective.
- Low-Density Attacks (1988): J.C. Lagarias and A.M. Odlyzko introduced the concept of low-density attacks, which specifically target knapsack problems with low-density sums. They proved that when the sum density is low, it becomes computationally feasible to find solutions, compromising the encryption's integrity.
- Structural Weaknesses: Further research revealed that the Knapsack Algorithm had inherent structural weaknesses. If attackers can determine the subset of the super-increasing sequence used to generate the public key, they may be able to crack the encryption system. Additionally, the use of weaker random number generators or poor code implementation can also make the knapsack cryptosystem more susceptible to being broken

Reference

[1] https://www.tutorialspoint.com/knapsack-encryption-algorithm-in-cryptography

[2] https://en.wikipedia.org/wiki/Merkle%E2%80%93Hellman_knapsack_cryptosystem#Cryptanalysis

[3] Shamir, Adi. "A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem." IEEE Transactions on Information Theory 30, no. 5 (1984): 699-704.

[4] Lagarias, J.C., and A.M. Odlyzko. "Solving Low-Density Subset Sum Problems." Journal of the ACM (JACM) 32, no. 1 (1985): 229-246.