1. 修了年月　：2018 年 3 月
2. 専攻名　　：複雑理工学専攻
3. 氏名　　：Yun Sheng
4. 学生証番号：47-166100

5. 論文題目：Security Analysis of BLISS

6. キーワード：BLISS, cache-attack, LLL algorithm

7. 指導教員氏名：國廣　昇
8. 指導教員役職：准教授

Abstract:

Cache attack is a kind of side-channel attack method that can extract target devices' cache memory data. Using those leaked data, attacker can recover secret key used in encryption algorithm or sign algorithm. Cache attack is a serious threat to devices using cache memory. At CHES 2016, Bruinderink presented a cache attack algorithm[**?**] that recover signature secret key from Bimodal lattice signature scheme(BLISS). In the recovery algorithm, attacker uses LLL algorithm as short vector oracle. Attacker can test each row vector of unimodular matrix until find the signature secret key. In this paper, we simulate the cache attack process by program and do an analysis on this cache attack algorithm. We also give an improvement to this cache attack method by using 52.57% signatures (compared to original attack method) to recover the secret key, at the cost of more searching time.