修了年月： 2006 年 3 月
専攻名 ： 基盤情報学専攻
氏名 ： TONGPRASIT BENJAMAS
学生証番号： 46328
論文題目：Tamper Resistant VLSI Technology Based on Floating-Gate-MOS Logic Circuit
(フローティング・ゲート・MOS に基づいたセキュリティ攻撃に強い VLSI 回路設計)
キーワード：
指導教員氏名： 柴田 直
指導教員役職： 教授

Abstract

The smartcard technologies play an essential role in various areas. The cryptographic algorithms have been developed to protect the sensitive data from being retrieved by other parties. A key using in cryptographic algorithm becomes an attractive target for the security attack.

This paper presents two solutions to prevent the circuit from being tampered. The first solution against power analysis attack is “power-balanced reconfigurable circuit”. The power consumption of proposed reconfigurable circuit has no correlation to the circuit’s internal state. Another solution proposed in this paper is “physical key generation circuit”. There is no binary data stored in the circuit. This circuit produces key by making use of the capacitors’ variation due to the properties variation during manufacturing process.