THE DESIGN AND IMPLEMENTATION OF THE CONDITIONAL ACCESS SYSTEM FOR CABLE TV SUBSCRIPTION USING FIXED CONTROL WORD SCRAMBLE

WITCHA BURIRAK

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE (COMPUTER SCIENCE) FACULTY OF GRADUATE STUDIES MAHIDOL UNIVERSITY 2014

THE DESIGN AND IMPLEMENTATION OF THE CONDITIONAL ACCESS SYSTEM FOR CABLE TV SUBSCRIPTION USING FIXED CONTROL WORD SCRAMBLE

WITCHA BURIRAK 5338170 ITCS / M

M.Sc. (COMPUTER SCIENCE)

RESEARCH PROJECT ADVISORY COMMITTEE: DAMRAS WONGSAWANG, Ph.D., CHOMTIP PORNPANOMCHAI, Ph.D.

ABSTRACT

This research developed a Digital Video Broadcasting (DVB) Conditional Access system (CAS) that allows using fixed Control Word (CW). Actually, the CW used to scramble the video and audio channel is changed in seconds. The only complied Conditional Access Set-Top-Box (CAS-STB) can be used to watch the channel but the Basic Interoperable Scrambling System Set-Top-Box (CAS-STB) can not. In order to allow both CAS-STB and BISS-STB to be used to watch from the same encrypted channel, the CW within the Entitlement Control Message (ECM) should be modified.

This research project has developed the system called "Conditional Access System Using Fixed Control Word (CASFCW)". In CASFFCW, the signal encryption structure has been changed. We create the conditional access on cable TV signal by using a fixed key encryption system. The CASFCW has been examined and tested in the actual applications for many situations. There are five types of STB selected for the experiment in this research, 1) Set-Top-Box support only BISS brand PSI 2) Set-Top-Box support only Conditional Access System brand SUN Box (ABV-CAS) 3) STB support only Conditional Access System brand HUMAX (Irdeto-CAS) 4) STB support only Conditional Access System brand GMMz (Novel-CAS) and 5) Set-Top-Box support only BISS brand D-Khoom. The experimental results show that, the BISS-STB cannot be used to watch any channels that are encrypted by using any CAS. A channel is encrypted by ABV-CAS and allows only their STB to be used to watch the channel. The STB that support both BISS and Irdeto-CAS or Novel-CAS are not able to be used to watch the encrypted channel by ABV-CAS. Finally, for the channel encrypted by using CASFCW, both types of CAS-STB and BISS-STB allow people to watch the channel.

KEY WORDS: DIGITAL VIDEO ENCRYPTION/ CONDITIONAL ACCESS SYSTEM/ / FIXED CONTROL WORD SCRAMBLE/ DIGITAL VIDEO BROADCASTING

61 pages

การออกแบบและการทำให้เกิดผลของระบบการเข้าถึงแบบมีเงื่อนไขสำหรับโทรทัศน์แบบบอกรับเป็นสมาชิกโดยใช้การเข้ารหัสด้วยคำควบคุมแบบคงที่

THE DESIGN AND IMPLEMENTATION OF THE CONDITIONAL ACCESS SYSTEM FOR CABLE TV SUBSCRIPTION USING FIXED CONTROL WORD SCRAMBLE

วิชชา บุรีรักษ์ 5338170 ITCS/M

วท.ม. (วิทยาการคอมพิวเตอร์)

คณะกรรมการที่ปรึกษาโครงการวิจัย : ดำรัส วงศ์สว่าง, Ph.D. ชมทิพ พรพนมชัย, Ph.D.

บทคัดย่อ

วัตถุประสงค์ของงานวิจัยนี้เพื่อพัฒนาและออกแบบระบบการเข้าถึงแบบมีเงื่อนไข สำหรับโทรทัศน์แบบบอกรับเป็นสมาชิกโดยใช้การเข้ารหัสด้วยคำควบคุมแบบคงที่ ซึ่งอุปกรณ์รับสัญญานดาวเทียมที่รองรับการใช้งานระบบเข้ารหัสสัญญานแบบบอกรับเป็นสมาชิกด้วยคำควบคุมแบบไม่คงที่เท่านั้น ที่สามารถถอดรหัสและรับสัญญาณช่องรายการที่เข้ารหัสด้วยคำควบคุมแบบไม่คงที่ได้ แต่อุปกรณ์รับสัญญานดาวเทียมที่รองรับการใช้งานระบบเข้ารหัสสัญญานด้วยคำควบคุมแบบคงที่จะไม่สามารถถอดรหัสได้ เพื่อให้อุปกรณ์รับสัญญานดาวเทียมที่รอรับการใช้งานทั้งระบบเข้ารหัสด้วยคำควบคุมแบบไม่คงที่และคงที่ให้สามารถรับชมช่องรายการเดียวกันและเวลาเดียวกันได้นั้น การเข้ารหัสสัญญานวิดีโอและออดิโอแบบบอกรับเป็นสมาชิกควรใช้คำควบคุมแบบคงที่

งานวิจัยนี้ได้ทำการทดลองกับการเข้ารหัสสัญญาณทั้งแบบคงที่และไม่คงที่จำนวน 5 ช่องทีวี โดยใช้อุปกรณ์รับสัญญานดาวเทียมจำนวน 5 ชนิดคือ1) อุปกรณ์รับสัญญานดาวเทียมที่รองรับการเข้ารหัสคำควบคุมแบบคงที่ยี่ห้อพีเอสไอ และ ดีคุ้ม, 2) อุปกรณ์รับสัญญานดาวเทียมที่รองรับการเข้ารหัสคำควบคุมแบบไม่คงที่ยี่ห้อซันบล๊อก, ฮิวแม็ก และจีเอ็มเอ็ม หลังจากที่มีการทดสอบกับอุปกรณ์รับสัญญานดาวเทียมที่รองรับการเข้ารหัสด้วยคำควบคุมแบบคงที่จะไม่สามารถรับชมช่องการที่เข้ารหัสแบบบอกรับเป็นสมาชิกที่ใช้คำควบคุมที่ไม่คงที่ได้ และอุปกรณ์รับสัญญานดาวเทียมที่รองรับการเข้ารหัสบอกรับเป็นสมาชิกด้วยคำควบคุมแบบไม่คงที่นั้น จะไม่สามารถรับชมช่องการที่เข้ารหัสแบบคำควบคุมแบบคงที่ได้ ส่วนช่องรายการที่เข้ารหัสแบบบอกรับเป็นสมาชิกที่ใช้คำควมคุมแบบคงที่นั้น อุปกรณ์รับสัญญานดาวเทียมทั้งสองชนิดสามารถถอดรหัสและรับชมได้

61 หน้า