

หัวข้อวิทยานิพนธ์	ระบบการจ่ายเงินผ่านอุปกรณ์อิเล็กทรอนิกส์แบบออฟไลน์ที่ให้ความเป็นส่วนตัวในด้านข้อมูล
หน่วยกิตของวิทยานิพนธ์	12 หน่วย
โดย	นางสาวสุภาววรรณ บุญช่วยดี
อาจารย์ที่ปรึกษา	ดร.ประเสริฐ ถันธมานนท์
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
ปีการศึกษา	2542

บทคัดย่อ

วิทยานิพนธ์ฉบับนี้นำเสนอ โพรโตคอลแบบใหม่สำหรับระบบการจ่ายเงินผ่านอุปกรณ์อิเล็กทรอนิกส์แบบออฟไลน์ที่ให้ความเป็นส่วนตัวในด้านข้อมูลรวม 2 โพรโตคอล โดยโพรโตคอลที่นำเสนอสามารถแก้ปัญหาการใช้ข้อมูลอิเล็กทรอนิกส์ซ้ำในการชำระเงิน ซึ่งเป็นปัญหาที่สำคัญสำหรับระบบการจ่ายเงินผ่านอุปกรณ์อิเล็กทรอนิกส์ โดยโพรโตคอลทั้ง 2 มีคุณสมบัติที่แตกต่างกันคือ โพรโตคอลแรกสามารถช่วยแก้ปัญหาการใช้ข้อมูลอิเล็กทรอนิกส์ซ้ำหลังเกิดปัญหา แต่สามารถระบุตัวผู้ซื้อที่กระทำผิดดังกล่าวได้ ส่วนโพรโตคอลแบบที่สองมีกลไกที่สามารถป้องกันไม่ให้เกิดปัญหาการใช้ข้อมูลอิเล็กทรอนิกส์ซ้ำ

โพรโตคอลที่นำเสนอเป็นโพรโตคอลที่มีประสิทธิภาพดีขึ้นกว่าโพรโตคอลที่มีการนำเสนอมาก่อนหน้านี้ โดยเปรียบเทียบจากจำนวนครั้งของการส่งข้อมูล จำนวนข้อมูลที่ใช้ในการส่งข้อมูล และพื้นที่หน่วยความจำที่ใช้ในการจัดเก็บข้อมูล อีกทั้งยังคงไว้ซึ่งความมั่นคงในการรักษาความลับของข้อมูล ซึ่งได้รับมาจากการนำเทคนิคลายเซ็นดิจิทัลที่ดัดแปลงมาจาก DSA (Digital Signature Algorithm) และ บลายซิกเนเจอร์ที่ดัดแปลงมาจาก Modified DSA มาใช้

คำสำคัญ (Keywords) : ระบบการจ่ายเงินผ่านอุปกรณ์อิเล็กทรอนิกส์แบบออฟไลน์ที่ให้ความเป็นส่วนตัวในด้านข้อมูล / ลายเซ็นดิจิทัล / บลายซิกเนเจอร์/ การใช้ข้อมูลอิเล็กทรอนิกส์ซ้ำ