

ชื่อโครงการ (ภาษาไทย) การศึกษาและวิเคราะห์ประสิทธิภาพและความปลอดภัยและพัฒนการใช้งานฟังก์ชันทางเดียวหรือข้อผูกมัดแบบคลุมเครือที่รับความคลาดเคลื่อนได้เป็นค่า

ชื่อโครงการ(ภาษาอังกฤษ) The Study and Analysis of The Efficiency and Security of The Fuzzy Commitment with Value-Oriented Deviation

แหล่งเงิน เงินงบประมาณแผ่นดิน/เงินรายได้

ประจำปีงบประมาณ 2555 จำนวนเงินที่ได้รับการสนับสนุน 50,000 บาท

ระยะเวลาทำการวิจัย 1 ปี ตั้งแต่ ตุลาคม 2554 ถึง กันยายน 2555

ชื่อ-สกุล หัวหน้าโครงการ และผู้ร่วมโครงการวิจัย พร้อมระบุ หน่วยงานต้นสังกัดและ อีเมล

ก. นล เปรมชัยเจริญ หัวหน้าโครงการ คณะเทคโนโลยีสารสนเทศ สจล nol@it.kmitl.ac.th

คำสำคัญ ข้อผูกมัดแบบคลุมเครือ, การพิสูจน์ตัวตนแบบคลุมเครือ, การพิสูจน์เอกลักษณ์บุคคลแบบคลุมเครือ

(Keywords) fuzzy commitment, fuzzy authentication, fuzzy identity authentication

บทคัดย่อ

ฟังก์ชันทางเดียวแบบคลุมเครือเป็นส่วนสำคัญในระบบการพิสูจน์ตัวตนบุคคลด้วยการใช้ข้อมูลทางชีวภาพ โดยข้อมูลที่ใช้พิสูจน์สามารถมีค่าคลาดเคลื่อนได้ไม่เกินค่าที่กำหนด ความคลาดเคลื่อนที่มีได้อาจเป็นความคลาดเคลื่อนเป็นบิตหรือเป็นค่า ขึ้นกับฟังก์ชันที่ใช้ รายงานฉบับนี้ศึกษาประสิทธิภาพการใช้งานฟังก์ชันทางเดียวแบบคลุมเครือตัวหนึ่งที่ชื่อว่า ฟัชซีแมทชิง ซึ่งเป็นฟังก์ชันที่อนุญาตให้ความคลาดเคลื่อนเกิดขึ้นเป็นค่า และได้นำเสนอฟังก์ชันตัวใหม่ที่ใช้วิธีการมอดูเลชันและไม่ต้องการเข้ารหัสเพื่อแก้ไขความผิดพลาด และได้พัฒนาการใช้งานเบื้องต้นของฟังก์ชันดังกล่าวที่นำเสนอขึ้นใหม่

Abstract

Fuzzy commitment schemes are important components of a number of biometric authentication protocols. Inputs to the scheme can contain error up to some certain limit. The range of the error can be in the number of bits or value, depending on the scheme. This report studies the efficiency of one of such schemes, called fuzzy matching. This scheme allows an input to contain error by value. The study suggests a new scheme based on modulation and does not require the use of error correcting code. An demonstrative application is developed based on the new scheme.