ขั้นตอนวิธีสำหรับการเข้ารหัสข้อมูลบนฐานข้อมูลแบบกระจาย

ธัญพร ศรีดอกไม้[1*] สมชาย ปราการเจริญ[2] และ นลินภัสร์ ปรวัฒน์ปรียกร[3]

บทคัดย่อ

งานวิจัยฉบับนี้ได้ทำการพัฒนาขั้นตอนวิธีสำหรับการเข้ารหัสข้อมูลบนฐานข้อมูลแบบกระจายเพื่อแก้ไขปัญหาการรั่วไหลของข้อมูลอันเกิดจาก DBA ทุจริตได้ โดยจะนำมาใช้เทคนิคการเข้ารหัสแบบ Homomorphic Polynomials Ring ร่วมกับSecret Sharing เพื่อแยกและกระจายชิ้นส่วนของข้อมูล ประโยชน์ที่จะได้รับจากงานวิจัยชิ้นนี้คือ การลดความเสี่ยงและความเสียหายที่อาจเกิดจากการขโมยและการใช้งานระบบในทางที่ผิด ทำให้ผู้ใช้มั่นใจในระบบรักษาความมั่นคงของข้อมูลมากขึ้นว่าสามารถปกป้องข้อมูลของตนจากภัยทั้งภายในและภายนอกองค์กร ส่งผลให้ทำงานได้อย่างมีประสิทธิภาพดีขึ้นกว่าเดิม

คำสำคัญ: การเข้ารหัส, การเข้ารหัสโฮโมมอร์ฟิค, การเข้ารหัสโฮโมมอร์ฟิคแบบแพริเออร์, การแบ่งปันความลับ, การแปลงค่า

[1] นักศึกหลักสูตรปรัชญาดุษฎีบัณฑิต ภาควิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยี พระจอมเกล้าพระนครเหนือ
[2] รองศาสตราจารย์ ภาควิชาวิทยาการคอมพิวเตอร์และสารสนเทศ คณะวิทยาศาสตร์ประยุกต์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
[3] ผู้ช่วยศาสตราจารย์ ภาควิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
[*] ผู้นิพนธ์ประสานงาน โทร. 08-5244-3764 อีเมล: ladytanyaorm@gmail.com.

ACDD for Protecting Information leakage

Tanyaporn Sridokmai[1*] Somchai Prakancharoen[2] and Nalinpat Porrawatpreyakorn[3]

Abstract

The objective of research was to develop analgorithm for cryptic distribute databases (ACDD) for distributed database management of the encrypted data to solve the problem of information leakage caused by fraud DBAs. The used techniques were Paillier homomorphic Polynomials ring, Shamir's Secret Sharing scheme and transformation graph. The Advantages of this algorithm were that it can solve the problem of dishonest dealers and dishonest participants who try to deceive other participants data and enables perform calculations on encrypted data without decryption on which the calculation was carried out, with respect of the data confidentiality.

Keywords: Cryptosystem, Paillier encryption, Homomorphic encryption, Secret sharing, Transformations

[1] Doctoral Degree Student, Department of Information Technology, Faculty of Information Technology, King Mongkut's University of Technology North Bangkok

[2] Associate Professor, Department of Computer science Faculty of applied science, King Mongkut's University of Technology North Bangkok

[3] Assistant Professor, Department of Information Technology, Faculty of Information Technology King Mongkut's University of Technology North Bangkok

* Corresponding Author Tel. 08-5244-3764 e-mail: ladytanyaorm@gmail.com.