**Malaysian Journal of Mathematical Sciences**

Journal homepage: https://einspem.upm.edu.my/journal

# A Chronological Review of Key Establishment Models and Protocols

Yap, E. Y. Y.*[1], Chin, J. J.[2,3], and Goh, A.[3]

[1]*Faculty of Engineering, Multimedia University, Malaysia*
[2]*Faculty of Computing and Informatics, Multimedia University, Malaysia*
[3]*Information Security Lab, MIMOS Berhad, Malaysia*

*E-mail: ernestyyy0306@gmail.com*
**Corresponding author*

*Received: 15 June 2021*
*Accepted: 8 October 2021*

## Abstract

This work is a review on existing authenticated key exchange (AKE) security models and protocols mainly based on Diffie-Hellman Key Exchange (DHKE). We provide a discussion on the various security models of AKEs, such as the Bellare Rogaway (BR) model, Canetti Krawczyk (CK) model and their variants. Then we provide a review covering over ninety protocols in chronological order. The security models' security features and protocol examples that fit in those security models are exhibited.

**Keywords:** security models; Bellare-Rogaway; Canetti-Krawczyk; authenticated key exchange; protocols; review.