American Journal of Applied Sciences 6 (9): 1714-1717, 2009

ISSN 1546-9239

© 2009 Science Publications

**Group Re-keying Protocol Based on Modular Polynomial Arithmetic Over Galois Field GF(2n)**

 1 1 2

Sundaram Sudha, Azman Samsudin and Mohammad Ahmad Alia

1

School of Computer Sciences, University Sains Malaysia, Malaysia

2

Department of Computer Information System, Al-Zaytoonah University of Jordan, Jordan

**Abstract: Problem statement:** In this study we propose a group re-keying protocol based on modular polynomial arithmetic over Galois Field GF(2n). Common secure group communications requires encryption/decryption for group re-keying process, especially when a group member is leaving the group. **Approach:** This study proposes secret keys multiplication protocol based on modular polynomial arithmetic (SKMP), which eliminates the need for the encryption/decryption during the group re-keying. **Results:** The implementation based on modular polynomial arithmetic over Galois Field GF(2n) offers fast re-keying process (about 50% faster than Secret Keys Multiplication Protocol (SKM) for 128 bit key) and compact key size representation against other secret keys multiplication protocols. With SKMP group re-keying is handled more efficiently through modular polynomial arithmetic manipulation rather than the expensive encryption/encryption which need to be done on every membership change.

**Key words**: Multicast, group re-keying, public-key, Polynomial arithmetic, Galois Field GF(2n)