International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **8**, August **2010**

ICIC International ©2010 ISSN 1349-4198
pp. **3621–3630**

PARALLEL MULTI-RECIPIENT SIGNCRYPTION FOR IMBALANCED WIRELESS NETWORKS

Yiliang Han[1,2], Xiaolin Gui[1] and Xuguang Wu[2]

[1]Shannxi Key Laboratory of Computer Networks
Department of Computer Science and Technology
Xi'an Jiaotong University
Xi'an 710049, P. R. China
yilianghan@hotmail.com; xlgui@mail.xjtu.edu.cn

[2]Department of Electronic Technology
Engineering College of Armed Police Force
Xi'an 710086, P. R. China

Received February 2009; revised August 2009

Abstract. *A new paradigm called parallel multi-recipient signcryption is proposed, which enhances the performance sharply when a sender sends distinct messages to multiple recipients in imbalanced wireless networks. The framework including syntax, architecture and security model is presented. Randomness reusing and cipher text aggregation are used to reduce the computation and transmission overheads on the sender node. A parallel multi-recipient scheme called ParaSC-GDH is proposed also, which is semantic secure. When n messages are processed with ParaSC-GDH on the N cores (threads) system, the theoretic speedup is up to N and the communication overheads is (4n+3)/7n of traditional ways. An experiment result shows that, the improvement of CPU time and cipher text size are 48.6% and 42.8% when it processes 1,000 distinct messages. As the number of recipients growing, the improvements increase also.*
Keywords: Signcryption, Secure group communication, Multi-recipient cryptosystem

1. **Introduction.** Secure group communication is one of the major applications in wireless and mobile computing. Besides secure multicast/broadcast services, it is also the crucial component of other protocols, such as secure routing, data aggregation. To transmit messages to multiple receivers, two paradigms are employed to secure them at present. The direct way is that the sender node encrypts (signs) and transmits several messages for each receiver in sequence. The example is that using the Internet Protocol Security (IPsec) to establish a point-to-point link [1]. The sender replicates the packet on each of the secure connections. It is not an ideal resolution for the uncertain security and the heavy overheads. In public key cryptosystems, some algorithm may leak messages using the same modular [2]. For the broadcast nature of wireless networks, the packet is received by all of the nodes within the communication range even if they are not the potential receivers, and the idle nodes are awaked frequently and exhausted quickly. At the same time, the sender is occupied by the expensive computation and transmission jobs. The second way is encrypting the message with a shared key, which is generated by the group key agreement [3]. Though it is a simplified way to broadcast an encrypted message and adapted broadly including Multicast Security framework [4,5], it also has the fatal handicap, the whole system is compromised if one of users leaks the shared key. Thus, rekeying, backward and forward secrecy are obstacles.

On the other hand, privacy, integrity and data source authentication are fundamental secure requirements for the group communication. Except for classical cryptographic