A Modular Exponentiation Based Batch Rekeying Scheme for Multicast and Broadcast in Mobile WiMAX

Hung-Min Sun[1], Shih-Ying Chang[1], and Chien-Chien Chiu[2]
[1]*Dept. of Computer Science, National Tsing Hua University, Taiwan, R.O.C.*
[2]*WiMAX Center of Networks & Multimedia Institute, Institute for Information Industry, Taipei, Taiwan, R.O.C.*
hmsun@cs.nthu.edu.tw, godspeed@is.cs.nthu.edu.tw, and vittorio@nmi.iii.org.tw

Abstract*-Mobile WiMAX (IEEE 802.16e) is an emerging wireless technology. It supports wider converge and higher bandwidth than conventional wireless technologies. Multicast and Broadcast (M&B) is a usable service provided by WiMAX. Many applications, such as Pay-TV system, can be more efficiently distributed by using M&B service. Although 802.16e defines M&B Rekeying Algorithm (MBRA) to protect M&B communication, MBRA does not consider forward and backward secrecy. More precisely, the key update procedure is triggered periodically without reflecting group membership change. In this paper, we propose a new modular exponentiation based periodical batch rekeying scheme applicable to WiMAX because MBRA has the property of periodical trigger. Security analysis and performance evaluation show that our scheme is secure and efficient, respectively. Regarding efficiency, our scheme requires O(1) messages to update keys.*

Keywords: Batch Rekeying, mobile WiMAX, Multicast and Broadcast (M&B), multicast security.

1. Introduction

In IEEE 802.16 family, the recent standard for mobile communication, 802.16e (802.16-2005) [1], is an important milestone in wireless communication technology. Worldwide Interoperability for Microwave Access (WiMAX) [2] is a forum responsible for certifying the products of IEEE 802.16. IEEE 802.16e is also called mobile WiMAX due to its mobility. WiMAX provides wider converge and higher bandwidth than conventional wireless technologies such as WiFi (IEEE 802.11) [3] and thus will largely enhance the quality of wireless access networks and be helpful for spreading associated wireless applications. Multicast/Broadcast (M&B) in WiMAX is especially suitable for multimedia applications such as Pay-TV system because multimedia providers can efficiently distribute the same contents to the users within a M&B group.

IEEE 802.16e [1] defines Multicast and Broadcast Rekeying Algorithm (MBRA) to protect M&B group communication; however, Xu *et al.* [4][5][6] shows that MBRA lacks forward and backward secrecy. This is because the key update procedures in MBRA are periodically triggered without reflecting the changes in group membership.

Most group key management schemes [7][8][9][10][11] supporting forward and backward secrecy are categorized into individual rekeying, which processes a request at a time. Individual rekeying is not suitable for MBRA since the key update procedures are periodically triggered. Comparing with individual rekeying, batch rekeying [12][13][14], which processes a batch of leave or join requests at a time, is more applicable to mobile WiMAX; however, current approaches [12][13][14] are not applicable to large dynamic group, such as mobile WiMAX networks.

In this paper, we propose a new batch rekeying scheme basing on modular exponentiation for M&B group communication. Our scheme requires less communication and storage complexity than those in conventional rekeying schemes. Besides that, our proposed scheme has forward secrecy and backward secrecy so it addresses the security problem of MBRA. Moreover, our proposed scheme is compatible with current design of MBRA because our scheme can be periodically triggered.

This paper is organized as follows. Background and related work are described in Section 2 and Section 3. In Section 4, we present our scheme. In Section 5, security analysis and performance evaluation are given. We also discuss the related performance and security issues in this section. Finally, we conclude in Section 6.

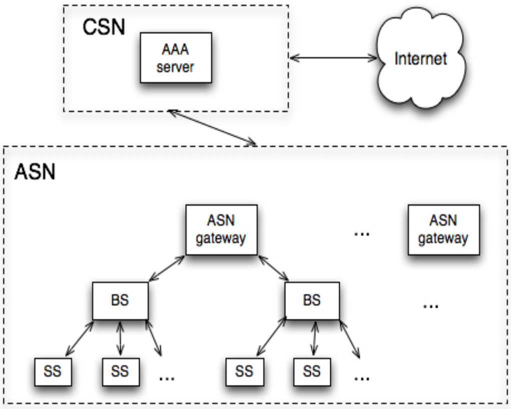

Figure 1 WiMAX network architecture

2. Background

2.1 Network model of WiMAX

WiMAX networks [2] are controlled by different network providers, Network Access Provider (NAP) and Network Service Provider (NSP). NAP builds one or more Access Service Networks (ASN), which provide WiMAX radio access infrastructure for one or more NSPs and also provide radio access functions for Subscriber Station (SS) we also called Mobile Station (MS) due to its mobility. NSP constructs Connectivity Service Network (CSN), which supplies IP connectivity and WiMAX bandwidth services to MS. Logically, ASN can be separated into two parts, one or more Base Stations (BS) and one or more ASN Gateways (ASN-GW). BS is in charge of wireless access for SS and ASN-GW is responsible for connections with CSN. CSN comprises AAA server to execute authentication, access control and accounting functions for users, devices and services. Fig. 1 illustrates WiMAX network architecture.

Before accessing WiMAX network, SS must authenticate to AAA server through Privacy Key Management version 2 (PKM$_{v2}$) authentication [2]. After successful authentication, each SS and the serving BS will individually share secret keys, such as Authentication Key (AK), Traffic Encryption Key (TEK) and Key Encryption Key (KEK). After that, two keys, Group Traffic Encryption Key (GTEK) and Group Key Encryption Key (GKEK), which protect M&B communications, are securely sent to SS.

A M&B group could comprise one or several BSs. So, a M&B group could have hundreds of SSs. This means the rekeying overhead may be large for MBRA since this overhead linearly increases with the group size.

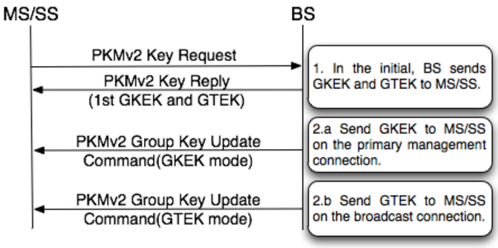
MS/SS
BS
PKMv2 Key Request
PKMv2 Key Reply
(1st GKEK and GTEK)
1. In the initial, BS sends GKEK and GTEK to MS/SS.
PKMv2 Group Key Update Command(GKEK mode)
2.a Send GKEK to MS/SS on the primary management connection.
PKMv2 Group Key Update Command(GTEK mode)
2.b Send GTEK to MS/SS on the broadcast connection.

Figure 2 Multicast and Broadcast Rekeying Algorithm

2.2 Multicast and Broadcast Rekeying Algorithm (MBRA)

MBRA defined by 802.16e is used to update GTEK and GKEK. The group key update commands of MBRA have two modes, GKEK mode and GTEK mode as shown in Fig. 2. In GKEK mode, GKEK encrypted by the associated KEK is unicasted to SS on primary management connection. In GTEK mode, GTEK encrypted by associated GKEK is broadcasted to SSs. In addition, the time period of updating TEK is 30 minutes to 7 days [1]. We consider that the time periods of updating GTEK and GKEK are also close to that of updating TEK.

2.3 Security requirements

The security requirements of M&B are listed as follows.

- **Group confidentiality**
  The messages exchanged within M&B groups can not be sniffed by attackers. Only authorized group members can obtain multicast and broadcast messages.
- **Forward secrecy**
  If an attacker compromises any subset of old group keys, he still can not obtain any subsequent group keys. This property means that a leaving user can not know any group key that will be used in later sessions.
- **Backward secrecy**
  If an attacker compromises a set of group keys, he can not obtain preceding group keys. This property means that a new joining user can not know the group key used in previous sessions.

2.4 Batch Rekeying

Comparing with individual rekeying, batch rekeying supports multiple membership changes. Regarding individual rekeying, the cost of updating keys linearly grows with the number of members involved membership changes. However, the cost of processing multiple membership change in batch rekeying is close to that of processing single membership change. For a dynamic group, batch rekeying is hard to be applied since members are hard to leave or join together. In this case, batch rekeying is often periodically triggered to make more applicable.

In this paper, we propose a new batch rekeying algorithm for MBRA. The major reason is that MBRA are periodically triggered. For compatible design, a batch rekeying scheme is more suitable for MBRA since batch rekeying schemes are often periodically triggered.

3. Related Work

Some research [4][5][6] has been proposed to address the security problem in MBRA. Unfortunately, none of these proposed schemes completely solves the problem. Xu *et al.* [4][5] proposed an improved MBRA to ensure forward and backward secrecy, but they did not consider scalability issue. Although they have mentioned the possibility to adopt schemes like LKH [7] to enhance performance, they did not have detailed description about that. On the other hand, Deininger *et al.* [6] concentrated on the broadcast authentication and storage issue in MBRA.

Most tree-based rekeying schemes [7][8][9][10][11] require $O(log(n))$ messages where n is size of a group to update keys for forward and backward secrecy; however, these tree-based schemes are not suitable for large dynamic group such as M&B group. These algorithms will incur large cost to maintain key tree since balanced tree construction in large dynamic group is more complicated. Besides that, the cost of $O(log(n))$ can not be ignored when n is large. Besides that, the performance of these schemes can not be optimized when these schemes are employed in the case of periodic rekeying. In this case, these schemes have to handle a batch of requests one by one. The cost often linearly grows with the number of processed requests since these schemes are optimized for processing a single request.

Batch rekeying [12][13][14], which processes a batch of join and leave requests in a group, is majorly designed for mitigating inefficiency problem in individual rekeying, which processes a request at a time. To optimize the communication cost, the cost of processing multiple requests can be close to that of processing a single request. Our previous research [14] can optimize that by using exclusive key set but this scheme is impractical for large dynamic group because each leaf node of key tree should assign to the same user. On the other hand, Zheng *et al.* [13] use Chinese Remainder Theorem (CRT) to optimize the communication cost, but the message length will linearly increase with the number of group members. In short, batch rekeying is more applicable to mobile WiMAX due to periodical rekeying; however, none of batch rekeying schemes is applicable to large dynamic group.

In view of this, we propose a new batch rekeying algorithm applicable to mobile WiMAX.

4. Proposed Scheme

Without loss of generality, we assume that a M&B group has n SSs. A Key Distribution Center (KDC), which is responsible for key assignment, will update keys whenever group membership changes. In mobile WiMAX networks, the functionality of KDC can be constructed in BS or ASN-GW. Let $\{text\}_{key}$ be the encryption of *text* using *key*.

- **Key assignment**

In the beginning, KDC generates $N = pq$ where p and q are two distinct large prime numbers, randomly selects a secret $g \in Z_N^*$, selects a distinct prime number for each user u_i and computes

$$K_i = g^{p_i} \bmod N \qquad (1)$$

as the secret key of u_i. After computing these parameters, KDC publishes (N, p_1, p_2,…,p_n) and keeps (g, p, q) as secret. Finally, KDC securely sends K_i to u_i as follows.

$$\text{KDC} \rightarrow u_i, \{K_i\}_{\text{KEK}_i},$$

where KEK_i is generated in PKM_{v2} authentication and known by only u_i and serving BS. In addition, we call the computational operation defined in Eqa. (1) modular exponentiation.

- **Join operation**

When a new user u_i joins a M&B group at the session t+1, KDC should update current GTEK so as to ensure backward secrecy. KDC updates GTEK for current users by using broadcasting as follows.

$$\text{KDC} \rightarrow \text{G}, \{\text{GTEK}^{t+1}\}_{\text{GTEK}_t}$$

where GTEK^{t+1} is the key used in session t+1.

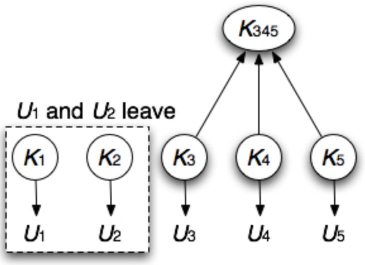

Figure 3 A concrete example of key update when U_1 and U_2 leave the group.

After that, KDC selects a new prime number p_i which is not currently used, computes the corresponding individual secret key K_i, and securely sends K_i to u_i as follows.

$$\text{KDC} \rightarrow u_i, \{K_i||\text{GTEK}^{t+1}\}_{\text{KEK}_i}$$

where || denotes concatenation. By this way, the newly joining user can not know the previous GTEK^t so backward secrecy can be ensured.

- **Leave operation**

When a user leaves the group, the key update is more complicated than that in join operation. We assume that U^t is a set of users who is allowed to access session t. Then, we assume that some users leave the group at session t. KDC computes $K_{U^{t+1}}$ as follows.

$$K_{U^{t+1}} = g^{e_{t+1}} \bmod N \tag{2}$$

where

$$e_{t+1} = \prod_{\{i:i\in U^{t+1}\}} p_i \ . \tag{3}$$

After that, KDC broadcasts new GTEK as follows.

$$\text{KDC} \rightarrow \text{G}, U^{t+1}||\{\text{GTEK}^{t+1}\}_{K_{U^{t+1}}}$$

After receiving this message, each user $u_i \in U^{t+1}$ can compute $K_{U^{t+1}}$ from K_i because $K_{U^{t+1}}$ is the power of K_i as follows.

$$K_{U^{t+1}} = (K_i)^{e_{t+1}/p_i} \tag{4}$$

Since p_j ,j = [1, n] have been published, all users can compute e_{t+1}/p_i where $p_i \mid e_{t+1}$. That is, $\frac{e_{t+1}}{p_i}$ is an integer. On the contrary, any user $u_j \notin U^{t+1}$ can not derive $K_{U^{t+1}}$ from self K_j since $\frac{e_{t+1}}{p_j}$ is not an integer. More detailed analysis is given in Section 5.1. In short, only authorized users can decrypt this broadcast message and obtain GTEK^{t+1}.

Obviously, our proposed scheme can conduct a batch of leaving requests. Fig. 3 illustrates an example processing multiple leaving requests. In this example, $K_{345} = g^{p_3p_4p_5} \bmod N$ can be computed by only u_3, u_4, and u_5.

In modular exponentiation, big prime numbers will increase the computation cost. Therefore, KDC assigns small prime numbers to all users can reduce computation cost. In order to reuse the small prime numbers, we should update g periodically. If we reuse the prime number without updating g, a re-joining user can compute g. KDC can send a randomly generated r to update g at session t as follows.

$$\text{KDC} \rightarrow \text{G}, \{r\}_{\text{GTEK}_\text{t}}, r \in Z_N^*$$

After receiving r, each user can update g to g^r by using following equation.

$$(K_i)^r = g^{p_i{}^r} \bmod N = g'^{p_i} \bmod N \tag{5}$$

Besides that, our proposed scheme requires only two messages to process multiple requests no matter how many users leave. In other words, the communication complexity is $O(1)$. It is more efficient than that in the previous schemes.

- **Periodical batch rekeying**

We have discussed how to process the single leave and join request. Then, we describe how our scheme applies to WiMAX. We assume that the time period is from session t to session t+1 and we describe how KDC processes a batch of requests in this time period.

When a user joins the group at session t, KDC will compute the individual secret key of this user, obtain pre-computed next group key GTEK^{t+1}, and securely send these keys to each user as follows.

$$\text{KDC} \rightarrow u_i, \{K_i||\text{GTEK}^{t+1}\}_{\text{KEK}_i},$$

where u_i is newly joining user. Note that join requests are processed one by one because batch processing can not reduce communication cost.

For the leave requests, KDC will process these requests at the end of session t at a time. At that time, KDC will firstly compute $K_{U^{t+1}}$ where e_{t+1} is computed as follows.

$$e_{t+1} = \prod_{\{i:i\in U^t\cap U^{t+1}\}} p_i \tag{6}$$

Since the newly joining users have known GTEK^{t+1}, it is unnecessary to let these users be able to compute $K_{U^{t+1}}$. On the other hand, this approach can reduce the computation overhead required for modular exponentiation. Then, KDC broadcasts GTEK^{t+1} as follows.

$$\text{KDC} \rightarrow \text{G}, \text{U}^t \cap \text{U}^{t+1}||\{\text{GTEK}^{t+1}\}_{K_{U^{t+1}}}$$

Finally, all users $\in U^{t+1}$ can obtain GTEK^{t+1}.

5. Analysis of Proposed Scheme

5.1 Security Analysis

We show our scheme secure by using following two propositions.

Proposition 1 *Only authorized user $u_i \in U^{t+1}$ can compute $K_{U^{t+1}}$ from K_i via Eqa. (4).*

Proof. Since $p_i \mid e_{t+1}$ for all authorized user $u_i \in U^{t+1}$, these users can compute correct $K_{U^{t+1}}$ via Eqa. (4). In other words, when $\frac{e_{t+1}}{p_i}$ is an integer, $K_{U^{t+1}}$ can be easily computed. For other user $u_j \notin U^{t+1}$, p_j does not divide e_{t+1} so u_j can not compute correct $K_{U^{t+1}}$ via Eqa. (4). Thus, only $u_i \in U^{t+1}$ can compute $K_{U^{t+1}}$. □

Some research [15][16] has proven Proposition 1 correct and design secure protocols on the basis of Proposition 1. Therefore, this also confirms the correctness of Proposition 1.

Proposition 2 *Let p_i, K_i, g, and N be defined in Eqa. (1). It is infeasible to obtain g from p_i, K_i, and N.*

Proof. We can show Proposition 2 correct by using Proposition 1. If a user u_i can compute g, this means that Eqa. (7) can be computed.

$$g = (K_i)^{1/p_i} \quad (7)$$

This obviously yields a contradiction with Proposition 1 since $\frac{1}{p_i}$ is not an integer. □

According Proposition 1 and Proposition 2, our proposed scheme is secure without illegal collusion.

The weakness of the proposed scheme is vulnerable to collusion attack, which means two or more users exchange their secret information in order to obtain some information they are not allowed to access. In our scheme, attackers can compute g so as to break the security of our scheme by using this attack. However, this seems to be a tradeoff between efficiency and collusion resistance since none of $O(1)$ batch rekeying schemes [13][14] can also has the capabaility of collusion resistance. The research of Micciancio *et al.* [17] also showed the same result.

To reduce the impact of collusion attack, KDC can periodically update K by using unicast. In this case, attackers should re-join the WiMAX networks and collude again so this method increases the cost to launch this attack.

5.2 Performance Evaluation

We compare our scheme with other individual rekeying schemes as shown in Table 1 and Table 2. The result shows that our scheme has smaller computation and storage complexity. Note that our scheme has the communication complexity of processing a batch of requests which is same to that for processing a single request.

Comparing with other batch rekeying schemes, our scheme neither requires maintaining a balanced key tree [7][12] nor linearly increases communication overhead with the growth of the group size [13]. More importantly, our scheme is more scalable, since our scheme has fixed communication cost when the group size increases.

5.3 Discussion

5.3.1 Reducing the computation cost

The major bottleneck of our proposed scheme is large computation cost of modular exponentiation. When the size of M&B group gets larger, the computation cost will exponentially increase. This cost will cause communication delay. To address this problem, we propose several approaches to reduce computational time.

First, since our implementation is not optimized, we can use some optimized algorithms [18][19] to accelerate the computation of modular exponentiation.

Second, we can use hardware to accelerate the computation. Since RSA [17], which has many hardware implementations [21], also requires modular exponentiation operation, we can use the hardware to accelerate computation.

Third, SS will hold two contiguous GTEKs in mobile WiMAX [1] so the key update procedures cause less delay in communication. Since GTEK^{t+1} has been obtained in the tth session, the communication delay made by computing $K_{U^{t+1}}$ can be tolerant. In other words, the delay of computing $K_{U^{t+1}}$ will not affect the protection of session t+1.

Besides that, the computation cost gets smaller when the group membership frequently changes according to Eqa (6). Therefore, our scheme is more suitable for a dynamic group. Consequently, the problem is solvable in the proposed scheme.

5.3.2 Tradeoff between efficiency and secrecy

Periodical rekeying will affect forward and backward secrecy because leaving and joining users still can access current session before the start of the next session. However, this tradeoff is acceptable for a large dynamic group since immediate rekeying triggered by membership change will cause large cost.

6. Conclusions

In this paper, we propose that batch rekeying is more applicable to M&B in mobile WiMAX because of the property of periodical rekeying. In addition, we propose a new $O(1)$ batch rekeying scheme which is especially applicable to a large

Table 1
Comparison of bandwidth consumption

	Join	
Scheme	multicast	unicast
LKH[7]	2*log*(*n*)-1	*log*(*n*)+1
LKH+[9]	2*log*(*n*)-1	*log*(*n*)+1
OFT[8]	*log*(*n*)+1	*log*(*n*)+1
OFCT[10]	*log*(*n*)	*log*(*n*)+1
TSEK[11]	2	*log*(*n*)+1
Our scheme	1	1

Table 2
Comparison of storage overhead

	Leave	Storage	
Scheme	Multicast	MS	BS
LKH[7]	2*log*(*n*)	*log*(*n*)+1	2*n*-1
LKH+[9]	0	*log*(*n*)+1	2*n*-1
OFT[8]	*log*(*n*)+1	*log*(*n*)+1	2*n*-1
OFCT[10]	*log*(*n*)+1	*log*(*n*)+1	2*n*-1
TSEK[11]	2	*log*(*n*)+1	2
Our scheme	2	2	*n*+1

dynamic group. We also show this scheme secure and efficient. By the proposed scheme, MBRA can reduce large communication and storage overhead so the bandwidth utilization can largely increase. In the future, we want to reduce the computation cost of modular exponentiation since the performance of our proposed scheme is decided by modular-exponentiation computation.

Acknowledgements

This study is conducted under the "III Innovative and Wireless Broadband Communications Technology and Application Project" of the Institute for Information Industry which is subsidized by the Ministry of Economy Affairs of the Republic of China.

References

[1] IEEE std. 802.16e-2005, IEEE standard for local and metropolitan area networks, part 16, air interface for fixed and mobile broadband wireless access systems, IEEE Press, Piscataway, NJ, Tech. Rep. 802.16e, 2005.

[2] Wimax end-to-end network systems architecture stage 2-3 release 1.1.0." WiMAX forum, Tech. Rep., 2007.

[3] Wireless LAN medium access control (MAC) and physical layer (PHY) specification," IEEE Press, Piscataway, NJ, Tech. Rep. 802.11, 1997.

[4] S. Xu, C. Huang, and M. Matthews, "Secure multicast in various scenarios of WirelessMAN," *SoutheastCon, 2007. IEEE*, pp. 709–714, 2007.

[5] S. Xu, C.T. Huang, and M. Matthews, "Secure Multicast in WiMAX," JOURNAL OF NETWORKS, Vol 3, pp. 48-57, 2008.

[6] A. Deininger, S. Kiyomoto, J. Kurihara, T. Tanaka, O. Min, S. Park, S. Kang, T. Kwon, S. Kumar, A. Kumar *et al.*, "Security Vulnerabilities and Solutions in Mobile WiMAX," *IJCSNS*, vol. 7, no. 11, p. 7, 2007.

[7] C. Wong, M. Gouda, and S. Lam, "Secure group communications using key graphs," *IEEE/ACM Transactions on Networking (TON)*, vol. 8, no. 1, pp. 16–30, 2000.

[8] D. McGrew and A. Sherman, "Key establishment in large dynamic groups using one-way function trees," *Manuscript*, vol. 474, 1998.

[9] M. Waldvogel, G. Caronni, D. Sun, N. Weiler, and B. Plattner, "The VersaKey Framework: Versatile Group Key Management," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, vol. 17, no. 9, 1999.

[10] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast security: a taxonomy and some efficient constructions," *INFOCOM' 99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 2, 1999.

[11] H. Kim, S. Hong, H. Yoon, and J. Cho, "Secure Group Communication with Multiplicative One-way Functions," *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05)-Volume I-Volume 01*, pp. 685–690, 2005.

[12] X. S. Li, Y. R. Yang, M. G. Gouda and S. S. Lam, "Batch Rekeying for Secure Group Communications," *ACM WWW10,* pp. 525-534, May 2001.

[13] X. Zheng, C. T. Huang, and M. Matthews, "Chinese Remainder Theorem Based Group Key Management," *ACM Southeast Regional Conference (ACMSE 2007)*, pp. 266-271, 2007.

[14] H.M. Sun, C.M. Chen, and C.Z. Shieh, " Flexible-Pay-Per-Channel: A New Model for Content Access Control in Pay-TV Broadcasting Systems, " IEEE Transactions on Multimedia, accepted, ready to publish, 2008.

[15] S. G. Akl and P. D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy," *ACM Transactions on Computer Systems (TOCS)*, pp. 239-248, 1983.

[16] S. Y. Wang and C. S. Laih, "Merging: An Efficient Solution for a Time-Bound Hierarchical Key Assignment Scheme," *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*, pp. 91-100, 2006.

[17] D. Micciancio and S. Panjwani, "Optimal communication complexity of generic multicast key distribution," *Advances in cryptology-EUROCRYPT*, vol. 3027, 2004.

[18] H. Wang and Q. Li, "Efficient Implementation of Public Key Cryptosystems on Mote Sensors (Short Paper)," *LECTURE NOTES IN COMPUTER SCIENCE, ICICS06,* pp. 519-528, 2006.

[19] S. M. Hong, S. Y. Ho, and H. Yoon, "New Modular Multiplication Algorithms for Fast Modular Exponentiation," *Advances in Cryptology - EUROCRYPT '96, LNCS 1070*, pp. 166-177, 1996.

[20] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[21] S. H. Tang, K. S. Tsui, and P. H. W. Leong, "Modular exponentiation using parallel multipliers," *IEEE International Conference on Field-Programmable Technology (FPT)*, pp. 52-59, 2003.