ISSN 1392 – 124X INFORMATION TECHNOLOGY AND CONTROL, 2011, Vol. 40, No. 3

A NEW EFFICIENT KEY AGREEMENT SCHEME FOR VSAT SATELLITE COMMUNICATIONS BASED ON ELLIPTIC CURVE CRYPTOSYSTEM

Jeong-Woo Hong, **Sang-Yoon Yoon**, **Dong-In Park**

Korea Institute of Science and Technology Information,
335 Gwahangno, Yuseong-Gu, Daejeon 305-806, South Korea
e-mail: jwhong@kisti.re.kr, net2nus@kisti.re.kr, dipark@kisti.re.kr

Myung-Jin Choi

Satellite Information Research Institute, Korea Aerospace Research Institute,
45 Eoeun-Dong, Yuseong-Gu, Daejeon 305-333, South Korea
e-mail: prime@kari.re.kr

Eun-Jun Yoon, **Kee-Young Yoo** *

School of Electrical Engineering and Computer Science, Kyungpook National University,
1370 Sankyuk-Dong, Buk-Gu, Daegu 702-701, South Korea
e-mail: ejyoon@knu.ac.kr, yook@knu.ac.kr

crossref http://dx.doi.org/10.5755/j01.itc.40.3.634

Abstract. A satellite communication is suitable for broadcasting service and long-hual transmission based on telecommunications. In the satellite communication environment, unauthorized user should not have to obtain his/her required services from the satellite communication systems without authentication. Therefore, authentication is an important security technique to prevent illegal service requests. Quite recently, Lee-Lin-Hwang **[C. C. Lee, T. C. Lin, M. S. Hwang. A key agreement scheme for satellite communications, Information Technology and Control, 2010, Vol. 39, No. 1, 43-47.]** proposed a secure scheme based on key agreement scheme with mutual authentication to solve the security problems on the VSAT satellite communications. However, Lee-Lin-Hwang's scheme is inefficiently designed because it is based on the RSA cryptosystem. Therefore, the scheme cannot be applicable for the low-power satellite communication environments because it involves high communication and computation costs. Based on these motivations, this paper proposes a new efficient and secure key agreement scheme for VSAT satellite communications based on elliptic curve cryptosystem (ECC) to minimize the complexity of computational costs between VSAT and HUB and fit VSAT satellite communication environments. Compared with previous schemes, the newly proposed scheme has the following more practical merits: (1) it provides secure session key agreement function by adopting elliptic curve cryptosystem, (2) it can reduce the total execution time and memory requirement due to the elliptic curve cryptography, and (3) it not only is secure against well-known cryptographical attacks but also provides perfect forward secrecy. As a result, the proposed scheme is extremely suitable for use in satellite communication environments since it provides security, reliability, and efficiency.

Keywords: authentication, VSAT, key agreement, satellite communication, elliptic curve cryptosystem.

1. Introduction

In general, a satellite communication is suitable for broadcasting service and long-hual transmission based on telecommunications. Due to the rapid development of satellite communication technology, a low-cost very small aperture terminal (VSAT) network can be used for data, voice, and video communications [1–3]. If we do not apply security technology for the satellite communication systems, it can be vulnerable to unauthorized access to the transmitted data. To provide strong security for the satellite communication, encryption and mutual authentication techniques can be used to protect data communication in satellite communications [4–6].

In 1998, Park and Lim [7] first proposed key distribution schemes with mutual authentication to provide privacy and authentication on the VSAT satellite communications. However, Tseng [8] and Yi et al. [9], respectively, proved that Park-Lim schemes are insecure against an impersonation attack. Moreover, Tseng [8] proposed an improved scheme to remedy the impersonation attack and provide secure mutual authentication. Quite recently, Lee-Lin-Hwang [10] also proposed a secure scheme based on key agreement scheme with mutual authentication to solve the

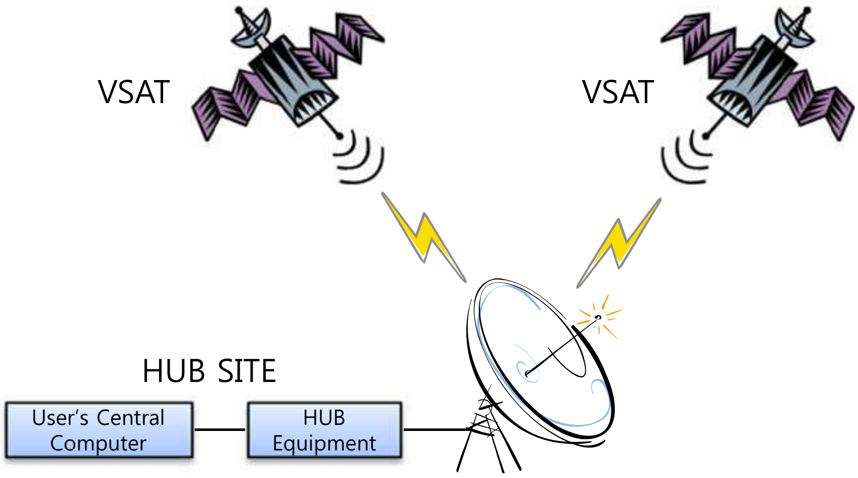

Figure 1. Satellite communication environment

security problems on the VSAT satellite communications (From here, we call this scheme LLH). Comparing with other key distribution schemes for VSAT satellite communications, LLH scheme is more secure and efficient. Nevertheless, we can find out that all previously proposed schemes are inefficiently designed because they are based on the RSA cryptosystem. It means that the schemes are not efficient and not applicable for the low-power satellite communication environments because they involve high communication and computation costs.

Based on these motivations, this paper proposes a new efficient and secure key agreement scheme for VSAT satellite communications based on elliptic curve cryptosystem (ECC) to minimize the complexity of computational costs between VSAT and HUB and fit VSAT satellite communication environments. In order to exploit the key block size, speed, and security jointly, the proposed scheme is based on one-way hash function and elliptic curve cryptography [11–13]. ECC presents an attractive alternative cryptosystem, because its security is based on the elliptic curve discrete logarithm problem (ECDLP) and it operates over a group of points on an elliptic curve. It can offer a level of security comparable to the classical cryptosystems that use much larger key sizes. Generally, the elliptic curve discrete logarithm problem (ECDLP) with an order of 160 bit prime offers approximately the same level of security as the discrete logarithm problem (DLP) with 1024 bit modulus [11–14]. Therefore, the proposed scheme can reduce the total execution time and memory requirement in comparison with previous related schemes. By adopting the ECC-based key agreement technique, the proposed scheme can provide strong and efficient key agreement function with the property of perfect forward secrecy to reduce the computation loads for the VSAT. To provide practicality, the proposed scheme is composed of three sub-phases, which are initialization, VSAT registration, and common key agreement. Compared with previous schemes, the newly proposed scheme has the following more practical merits: (1) it provides secure session key agreement function by adopting elliptic curve cryptosystem, (2) it can reduce the total execution time and memory requirement due to the elliptic curve cryptography, and (3) it not only is secure against well-known cryptographical attacks but also provides perfect forward secrecy. As a result, compared with related schemes, the proposed scheme has strong security and enhanced computational efficiency. Thus, the proposed scheme is extremely suitable for use in satellite communication environments since it provides security, reliability, and efficiency.

The rest of this paper is organized as follows: Section 2 introduces the basic concept of VSAT satellite communication environment and elliptic curve cryptosystem, respectively. Section 3 briefly reviews the LLH scheme. The proposed scheme is presented in Section 4, while Section 5 discusses the security and efficiency of the proposed scheme. The conclusion is given in Section 6.

2. Preliminaries

This section introduces the basic concept of VSAT satellite communication environment and elliptic curve cryptosystem, respectively.

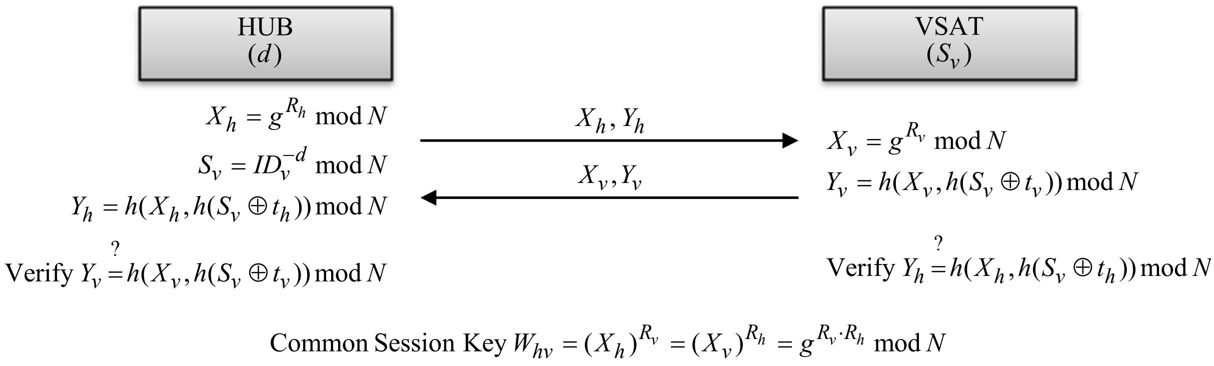

Figure 2. Common key generation phase of the LLH scheme

2.1. VSAT Satellite Communication Environment

Fig. 1 shows the proposed satellite communication environment. A VSAT network environment has a star configuration. It includes many VSATs and a single HUB. The HUB can communicate with the VSATs via the outbound links (HUB-to-VSAT) [15–17]. Contrary, a number of remote VSATs can communicate with the HUB via the inbound links (VSAT-to-HUB). The VSAT satellite communications have the following advantages [18, 19]: (1) high reliability, (2) high quality of transmission, (3) low cost communication, (4) good usage rates (e.g. independent of distance), (5) simple network installation, operation, and management. Digital video broadcasting (DVB) return channel system (DVB-RCS) [20, 21] is the best known application of satellite technology, and was standardized by the European Telecommunications Standards Institute (ETSI) [22].

In the satellite communication environment, each VSAT must perform common key generation phase procedure to authenticate the HUB for a transaction. Basically, each VSAT must register with the HUB site to obtain a secret key. Then, the VSAT uses the obtained secret key to perform the common key generation procedures with the HUB.

2.2. Elliptic Curve Cryptosystem (ECC)

ECC was first proposed by Koblitz [11] and Miller [12], and its security was based upon the difficulty of elliptic curve discrete logarithm problem (ECDLP). Compared with public key cryptosystem (PKC), ECC offers a better performance because it can achieve the same security with a smaller key size. For example, 160-bit ECC and 1024-bit RSA have the same security level in practice [13]. Thus, ECC-based authentication schemes are more suitable for smart cards and mobile devices than PKC-based ones.

An elliptic curve is a cubic equation of the form as follows:

$$y^2 + axy + by = x^3 + cx^2 + dx + e \qquad (1)$$

where a, b, c, d, and e are real numbers. In an elliptic curve cryptosystem, the elliptic curve equation is defined as the form of

$$Ep(a,b) : y^2 = x^3 + ax + b(\text{mod} p) \qquad (2)$$

over a prime finite field F_p, where $a, b \in F_p$, $p > 3$, and $4a^3 + 27b^2 \neq 0(\text{mod} p)$. Given an integer $s \in F_p^*$ and a point $P \in E_p(a,b)$, the point multiplication sP over $E_p(a,b)$ can be defined as

$$sP = \underbrace{P + P + \cdots + P}_{\text{s times}}. \qquad (3)$$

More details of ECC definitions can be found in [13]. Generally, the security of ECC relies on the difficulties of the following problems.

Definition 1. Given two points P and Q over $E_p(a,b)$, the elliptic curve discrete logarithm problem (ECDLP) is to find an integer $s \in F_p^*$ such that $Q = sP$.

Definition 2. Given three points P, sP, and tP over $E_p(a,b)$ for $s, t \in F_p^*$, the computational Diffie-Hellman problem (CDHP) is to find the point stP over $E_p(a,b)$.

Definition 3. Given two points P and $Q = sP + tP$ over $E_p(a,b)$ for $s, t \in F_p^*$, the elliptic curve factorization problem (ECFP) is to find two points sP and tP over $E_p(a,b)$.

Up to now, there is no algorithm to be able to solve any of the above problems.

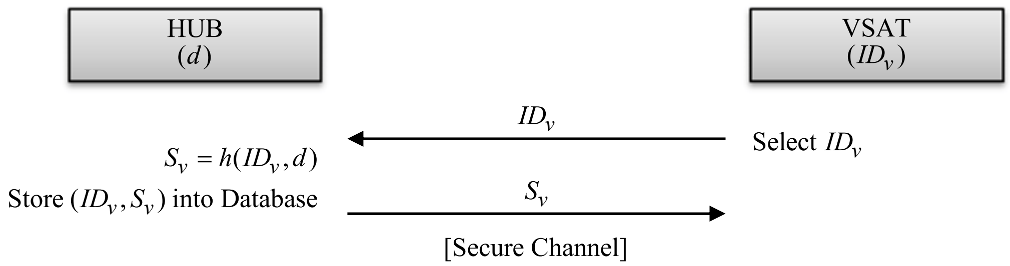

Figure 3. Proposed VSAT registration phase

3. LLH Scheme

The LLH scheme is composed of two phases: the initiation phase and the common key generation phase.

3.1. Initiation Phase

HUB is assigned to the key distribution center. The HUB generates two prime numbers p and q, and computes $N = p \cdot q$, chooses a random number d, and chooses a small prime e such that $e \cdot d \equiv 1 \bmod (p-1)(q-1)$. The HUB selects an integer g, which is the primitive element of both $GF(p)$ and $GF(q)$. The HUB calculates the VSAT's secret key $S_v = ID_v^{-d} \bmod N$. Then the HUB stores p, q, d and publishes N, g, e.

3.2. Common Key Generation Phase

HUB selects a random number R_h, and then computes X_h, S_v, and Y_h as follows:

$$X_h = g^{R_h} \bmod N, \tag{4}$$

$$S_v = ID_v^{-d} \bmod N, \tag{5}$$

$$Y_h = h(X_h, h(S_v \oplus t_h)) \bmod N. \tag{6}$$

Note that S_v may be pre-computed to reduce the computational cost and t is time stamp. Thus, the HUB can store the VSAT's secret key S_v in his/her database. VSAT randomly chooses a number R_v, and calculates X_v and Y_v as follows:

$$X_v = g^{R_v} \bmod N, \tag{7}$$

$$Y_v = h(X_v, h(S_v \oplus t_v)) \bmod N. \tag{8}$$

After HUB and VSAT exchanging (X_h, Y_h, t_h) and (X_v, Y_v, t_v), HUB can check the validity of VSAT by checking whether the following equation holds or not:

$$Y_v \stackrel{?}{=} h(X_v, h(S_v \oplus t_v)) \bmod N. \tag{9}$$

If the above equation holds, HUB computes the common key $W_{hv} = (X_v)^{R_h} = g^{R_v R_h} \bmod N$. In the same way, VSAT can check the validity of HUB by checking whether the following equation holds or not:

$$Y_h \stackrel{?}{=} h(X_h, h(S_v \oplus t_h)) \bmod N. \tag{10}$$

If the above equation holds, VSAT computes the common key $W_{hv} = (X_h)^{R_v} = g^{R_v R_h} \bmod N$. The above procedure is illustrated in Fig. 2.

4. Proposed Scheme

The proposed scheme is composed of three phases: the system initiation phase, the VSAT registration phase and the common key generation phase.

4.1. System Initiation Phase

In this phase, HUB is assigned to the key distribution center and generates parameter of the system.

1. HUB chooses an elliptic curve E over a finite field F_p. Let $E(F_p)$ denote the set of all the point on E.
2. HUB chooses a base point $P \in E(F_p)$, such that the subgroup generated by P has a large order n.
3. HUB chooses a secure one-way hash function $h(\cdot)$, where $h : \{0,1\}^* \rightarrow Z_p^*$.
4. HUB selects its master key d.
5. HUB keeps d in private and publishes the parameter $(F_p, E, n, P, h(\cdot))$.

4.2. VSAT Registration Phase

In this phase, VSAT which wants to register at the HUB should obtain its secret key S_v. The VSAT begins its registration at the HUB as follows.

1. VSAT → HUB: ID_V

   VSAT sends its identity ID_V to the HUB.

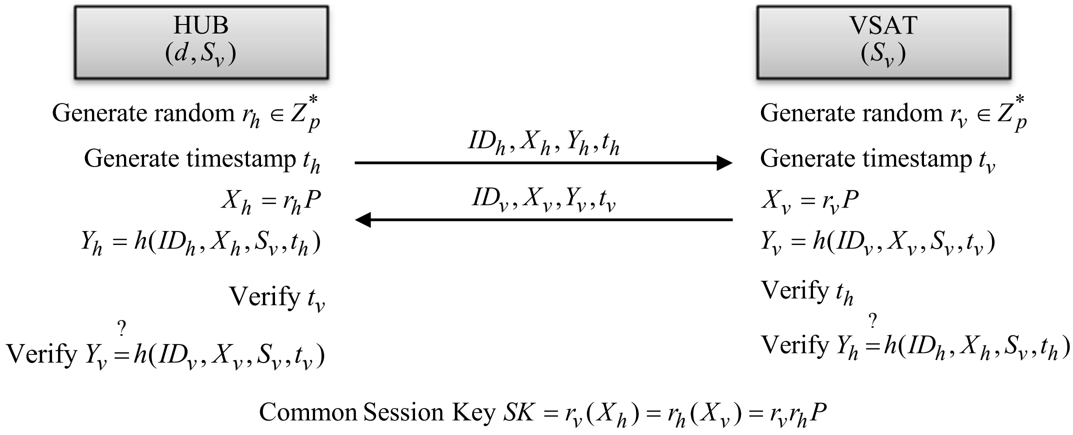

Figure 4. Proposed common key generation phase

2. HUB → VSAT: S_v

   HUB calculates the VSAT's secret key $S_v = h(ID_v, d)$ and delivers S_v to the VSAT function through a secure channel. Finally, the HUB securely maintains an ID database table which includes (ID_v, S_v).

The above procedure is illustrated in Fig. 3.

4.3. Common Key Generation Phase

In this phase, both HUB and VSAT agree a common session key after performing a secure mutual authentication procedure. Fig. 4 shows the proposed common key generation phase.

1. HUB → VSAT: (ID_h, X_h, Y_h, t_h)

   HUB obtains the stored VSAT's secret key S_v in his/her database. HUB selects a random number $r_h \in Z_p^*$, generates the current timestamp t_h, and then computes X_h and Y_h as follows:

$$X_h = r_h P, \tag{11}$$

$$Y_h = h(ID_h, X_h, S_v, t_h). \tag{12}$$

   Finally, HUB sends (ID_h, X_h, Y_h, t_h) to VSAT.

2. VSAT → HUB: (ID_v, X_v, Y_v, t_v)

   VSAT randomly chooses a number r_v, generates the current timestamp t_v, and calculates X_v and Y_v as follows:

$$X_v = r_v P, \tag{13}$$

$$Y_v = h(ID_v, X_v, S_v, t_v). \tag{14}$$

   Finally, VSAT sends (ID_v, X_v, Y_v, t_v) to HUB.

3. After HUB and VSAT exchanging (ID_h, X_h, Y_h, t_h) and (ID_v, X_v, Y_v, t_v), HUB first checks the validity of the received timestamp t_v. If it is valid, HUB can check the validity of VSAT by checking whether the following equation holds or not:

$$Y_v \stackrel{?}{=} h(ID_v, X_v, S_v, t_v). \tag{15}$$

   If the above equation holds, HUB computes the common session key $SK = r_h(X_v) = r_v r_h P$.

4. In the same way, VSAT first checks the validity of the received timestamp t_h. If it is valid, VSAT can check the validity of HUB by checking whether the following equation holds or not:

$$Y_h \stackrel{?}{=} h(ID_h, X_h, S_v, t_h). \tag{16}$$

   If the above equation holds, VSAT computes the common session key $SK = r_v(X_h) = r_v r_h P$.

To protect (e.g., encrypt) further information exchanged in the session, VSAT and HUB uses the one-time session key SK.

5. Security and Performance Analysis

5.1. Security Analysis

This subsection provides the proof of correctness of the proposed scheme. First, the security terms [14] needed for the analysis of the proposed scheme are defined as follows:

Definition 4. A strong secret key (S_v) has a value of high entropy, which cannot be guessed in polynomial time.

Definition 5. A secure chaotic one-way hash function $y = h(x)$ is where given x to compute y is easy and given y to compute x is hard.

Here, five security properties: guessing attack, replay attack, impersonation attack, secure mutual authentication, and perfect forward secrecy, will be considered for the proposed scheme.

1. *Guessing attack*. In an off-line guessing attack, an adversary A guesses a long-term secret key and verifies his/her guess, but he/she does not need to participate in any communication during the guessing phase. In an undetectable on-line guessing attack, an adversary A searches to verify a guessed long-term secret key in an on-line transaction and a failed guess cannot be detected and logged by the server. Suppose that an adversary A intercepts the messages (ID_h, X_h, Y_h, t_h) from HUB and wants to guess the secret key $S_v = h(ID_v, d)$ from the message, where d is the master key d of HUB. First, A chooses a value which is regarded as S_v^* and checks whether the equation $Y_h \stackrel{?}{=} h(ID_h, X_h, S_v^*, t_h)$ holds; if it shows that $S_v^* = S_v$, then A finds the correct secret key S_v. Due to the fact of Definitions 4 and 5, it is difficult to directly find the secret key S_v without knowing the master key d of HUB. Therefore, the proposed scheme can resist the guessing attack.

2. *Replay attack*. A replay attack is that an unauthorized party records previous messages and uses them to cheat the receiver in later processes. The replay attacks fail because the freshness of the messages transmitted in the common key generation phase is provided by the timestamps t_h and t_v. Except for VSAT (or HUB), only HUB (or VSAT) who can embed the secret value S_v and two timestamps in the hashed message $Y_v = h(ID_v, X_v, S_v, t_v)$ of Step (1) (or $Y_h = h(ID_h, X_h, S_v, t_h)$ of Step (2)), respectively. For example, suppose that an adversary A intercepts the message (ID_h, X_h, Y_h, t_h) from HUB and then stores it in his/her system. After a while, A sends the old message (ID_h, X_h, Y_h, t_h) to VSAT to impersonate HUB. Then, VSAT will detect the replay attack by checking the freshness of the timestamp t_h. Therefore, the proposed scheme can prevent replay attacks.

3. *Impersonation attack*. In the proposed scheme, an adversary A can try the impersonation attack to forge the (ID_h, X_h, Y_h, t_h). Assume that A pretends that he/she is HUB and forges (ID_h, X_h, Y_h, t_h). Firstly, A chooses a random number r_h and computes $X_h = r_h P$. Then, $Y_h = h(ID_h, X_h, S_v, t_h)$ is computed and (ID_h, X_h, Y_h, t_h) is sent to VSAT. After VSAT receives (ID_h, X_h, Y_h, t_h) from A, VSAT can check the validity of HUB by checking whether the equation $Y_h \stackrel{?}{=} h(ID_h, X_h, S_v^*, t_h)$ holds or not. Because A does not have the secret key S_v and S_v is difficult to guess due to the fact of Definitions 4 and 5, VSAT will reject the adversary A's forged message.

4. *Secure mutual authentication*. Mutual authentication schemes enable participants mutually to authenticate each other's identity. That is, it means that both the VSAT and HUB are authenticated to each other within the same protocol. After HUB and VSAT exchanging (ID_h, X_h, Y_h, t_h) and (ID_v, X_v, Y_v, t_v), both HUB and VSAT will check if the hashed message Y_v or Y_h contains the secret value S_v, its computed X_v or X_h, and the timestamps t_v and t_h, respectively. Since the hashed messages included two timestamps t_v and t_h, both HUB and VSAT will believe the i-th random nonce t_v or t_h was originally sent from VSAT and HUB, respectively. HUB and VSAT agree a one-time session key $SK = r_v r_h P$ to protect (e.g., encrypt) further information exchanged in the session. By adopting Elliptic Curve Diffie-Hellman key exchange algorithm (e.g., $r_v P, r_h P, r_v r_h P$, $SK = r_v r_h P$, where P is a generator), the proposed scheme can also provide perfect forward secrecy. Therefore, the proposed scheme can provide secure mutual authentication and session key agreement.

5. *Perfect forward secrecy.* Perfect forward secrecy means that if long-term private keys of one or more entities are compromised, the secrecy of previous session keys established by honest entities is not affected. In the proposed scheme, a disclosed long-lived secret keys d cannot derive the session key $SK = r_v r_h P$ used before because without getting the used random integers r_v and r_h, nobody can compute the used session key SK. If an attacker wiretaps all conversations of the medium and derives some used random point elements $r_v P$ and $r_h P$, he/she could not compute the used session key SK. This problem is the Elliptic Curve Diffie-Hellman key exchange algorithm based on ECDLP and CDHP of Definitions 1 and 2. Therefore, the proposed scheme provides perfect forward secrecy.

Table 1. Efficiency comparisons between the proposed scheme and related schemes

	HUB	VSAT	Total
Park-Lim scheme [7]	$7T_{exp} + 9T_{mul} + 2T_h$	$8T_{exp} + 2T_{mul} + T_h$	$15T_{exp} + 11T_{mul} + 3T_h$
Tseng scheme [8]	$5T_{exp} + 4T_{mul} + 2T_h$	$5T_{exp} + 4T_{mul} + 2T_h$	$10T_{exp} + 8T_{mul} + 4T_h$
LLH scheme [10]	$2T_{exp} + 4T_h$	$2T_{exp} + 4T_h$	$4T_{exp} + 8T_h$
Proposed scheme	$2T_{pm} + 2T_h$	$2T_{pm} + 2T_h$	$4T_{pm} + 4T_h$

5.2. Performance Evaluation

In the following, we show the performance of our proposed scheme. The performance evaluation of the proposed scheme mainly concerns the time complexity. For convenience, we suppose some notations are used to analyze the computational complexity as follows:

- T_{exp} is the time for executing a modular exponentiation operation;
- T_{pm} is the time for executing a elliptic curve multiplication operation;
- T_{mul} is the time for modular multiplication.
- T_h is the time for executing the one-way hash function $h(\cdot)$.

Table 1 summarizes the comparison among Park-Lim scheme [7], Tseng scheme [8], LLH scheme [10], and the proposed scheme.

Considering the computational complexity in the Park-Lim scheme with ID [7], the total computational complexity required for the HUB is $7T_{exp} + 9T_{mul} + 2T_h$. The total computational complexity required for the VSAT is $8T_{exp} + 2T_{mul} + T_h$. The total complexity for the Park-Lim scheme with ID is $15T_{exp} + 11T_{mul} + 3T_h$ as shown in Table 1.

Considering the computational complexity in the Tseng scheme with ID [8], the total computational complexity required for the HUB is $5T_{exp} + 4T_{mul} + 2T_h$ for computing HUB. The total computational complexity required for the VSAT is $5T_{exp} + 4T_{mul} + 2T_h$. The total computational complexity required for the Tseng scheme is $10T_{exp} + 8T_{mul} + 4T_h$ as shown in Table 1.

Considering the computational complexity in the LLH scheme with ID [10], the total computational complexity required for the HUB is $2T_{exp} + 4T_h$ for computing HUB. The total computational complexity required for the VSAT is $2T_{exp} + 4T_h$. The total computational complexity required for the LLH scheme is $4T_{exp} + 8T_h$ as shown in Table 1.

In the propose scheme, considering the computational complexity required for the HUB, the HUB is needed to compute X_h, Y_h, S_v, and SK. Note that S_v may be pre-computed to reduce the computational cost. Thus, the HUB is only needed to compute X_h, Y_h, and SK on line. They respectively require T_{pm}, T_h, and T_{pm}. Meanwhile, the HUB must check whether the equation $Y_v = h(ID_v, X_v, S_v, t_v)$ holds or not, which takes $1T_h$. Therefore, the total computational complexity required for the HUB is $2T_{pm} + 2T_h$. As for the complexity for the VSAT, the VSAT is needed to compute X_v, Y_v, and SK. They respectively require T_{pm}, T_h, and T_{pm}; it also needs to check whether the equation $Y_h = h(ID_h, X_h, S_v, t_h)$ holds or not with the same cost of T_h. Therefore, the total computational complexity required for the VSAT is $2T_{pm} + 2T_h$. Thus, the total computational complexity required for our scheme is $4T_{pm} + 4T_h$.

We should point out that the computation cost of modular exponentiation(T_{exp}) is much more expensive than that of Elliptic curve point multiplication(T_{pm}). In conclusion, the proposed scheme is more efficient than others.

6. Conclusions

This paper proposed a new efficient and secure key agreement scheme for VSAT satellite communications based on elliptic curve cryptosystem (ECC) to minimize the complexity of computational costs between VSAT and HUB and fit VSAT satellite communication environments. We have shown that the newly proposed scheme has the following more practical merits compared with previously related schemes: (1) it provides secure session key agreement function by adopting elliptic curve cryptosystem, (2) it can reduce the total execution time and memory requirement due to the elliptic curve cryptography, and (3) it not only is secure against well-known cryptographical attacks but also provides perfect forward secrecy. As a result, we believe that the proposed scheme is extremely suitable for use in satellite communication environments since it provides security, reliability, and efficiency.

Acknowledgements

We would like to thank the anonymous reviewers for their helpful comments in improving our manuscript. This research was supported by the IT Research and Development program of MKE/KEIT

(10035245) and the ITRC program of MKE/NIPA (NIPA-2010-C1090-1021-0002).

References

[1] **V. M. Dorofeev, L. Y. Kantor.** VSAT applications in Russian satellite communications, *International Journal of Satellite Communications*, 1993, Vol. 11, No. 4, 223-228.

[2] **M. Maggenti, T. T. Ha, T. Pratt.** VSAT Networks-an overview, *International Journal of Satellite Communications*, 1987, Vol. 5, No. 3, 219-225.

[3] **L. P. Seidman.** Satellites for wideband access, *IEEE Communications Magazine*, Oct. 1996, Vol. 34, No. 10, 108-111.

[4] **M. S. Hwang and W. P. Yang.** Conference key distribution schemes for secure digital mobile communications, *IEEE Journal on Selected Areas in Communications*, Feb. 1995, Vol. 13, No. 2, 416-420.

[5] **C. C. Lee, M. S. Hwang, I. E. Liao.** Security enhancement on a new authentication scheme with anonymity for wireless environments, *IEEE Transactions on Industrial Electronics*, 2006, Vol. 53, No. 5, 1683-1687.

[6] **W. B. Lee, C. K. Yeh.** A new delegation-based authentication protocol for use in portable communication systems, *IEEE Transactions on Wireless Communications*, 2005, Vol. 4, No. 1, 57-64.

[7] **J. H. Park, S. B. Lim.** Key distribution for secure VSAT satellite communications, *IEEE Transactions on Broadcasting*, 1998, Vol. 44, No. 3, 274-277.

[8] **Y. M. Tseng.** Cryptanalysis and improvement of key distribution system for VSAT satellite communications, *Informatica*, 2002, Vol. 13, No. 3, 369-376.

[9] **X. Yi, Ch. K. Siew, H. M. Sun, H. T. Yeh, Ch. L. Lin, T. Hwang.** Security of Park-Lim key agreement schemes for VSAT satellite communications, *IEEE Transactions on Vehicular Technology*, March 2003, Vol. 52, No. 2, 465-468.

[10] **C. C. Lee, T. C. Lin, M. S. Hwang.** A key agreement scheme for satellite communications, *Information Technology and Control*, 2010, Vol. 39, No. 1, 43-47.

[11] **N. Koblitz.** Elliptic curve cryptosystems, *Mathematics of Computation*, 1987, vol. 48, 203-209.

[12] **V. Miller.** Uses of elliptic curves in cryptography, *In: Proc of CRYPTO'85, Lecture notes in computer science*, 1986, vol 218. Springer, Berlin, 417-426.

[13] **D. Hankerson, A. Menezes, S. Vanstone.** Guide to elliptic curve cryptography, *Lecture notes in computer science*, 2004, Springer, Berlin.

[14] **A. J. Menezes, P. C. Oorschot, S. A. Vanstone.** Handbook of applied cryptograph, *CRC Press*, 1997, New York.

[15] **N. Abramson.** VSAT data networks. *Proceedings of the IEEE*, July 1990, Vol. 78, pp. 1267-1274.

[16] **M. W. Mitchell, R. A. Hedinger.** The development of VSAT performance standards in the United States of America, *International Journal of Satellite Communications*, 1993, Vol. 11, No. 4, 195-200.

[17] **A. H. Rana, J. S. McCoskey, W. A. Check.** VSAT technology, trends, and applications, *Proceedings of the IEEE*, July 1990, Vol. 78, pp. 1087-1095.

[18] **D. M. Chitre, J. S. McCoskey.** VSAT networks: architectures, protocols, and management, *IEEE Communications Magazine*, 1988, Vol. 26, No. 7, 28-38.

[19] **K. M. S. Murthy, J. Alan, J. Barry, B. G. Evans, N. Miller, R. Mullinax, P. Noble, B. O'Neal, J. J. Sanchez, N. Seshagiri, D. Shanley, J. Stratigos, J. W. Warner.** VSAT user network examples, *IEEE Communications Magazine*, 1989, Vol. 27, No. 5, 50-57.

[20] **Ricardo Castellot Lou, Antonio Javier Sanchez Esguevillas, Borja de la Cuesta Diego, Belen Carro, Linghang Fan, Zhili Sun.** IPv6 networks over DVB-RCS satellite systems, *International Journal of Satellite Communications and Networking*, 2008, Vol. 26, No. 1, 45-56.

[21] **D. K. Petraki, M. P. Anastasopoulos, P. G. Cottis.** Dynamic resource allocation for DVB-RCS networks, *International Journal of Satellite Communications and Networking*, 2008, Vol. 26, No. 3, 189-210.

[22] **ETSI**, Digital video broadcasting (DVB); interaction channel for satellite distribution systems, *ETSI EN 301 790 v. 1.3.1*, Mar. 2003.

Received November 2010.