An Efficient and Secure, ID-based Authenticated, Asymmetric Group Key Agreement Protocol for Ubiquitous Pay-TV Networks

Shaheena Khatoon[1], Sk Md Mizanur Rahman[2], Raylin Tso[3], Mohammed F. Alhamid[4]

[1] School of Studies in Mathematics, Pt. Ravishankar Shukla University, India
[2] Information and Communication Engineering Technology (ICET), Centennial College, Canada
[3] Department of Computer Science, National Chengchi University, Taiwan
[4] Department of Software Engineering, King Saud University, Saudi Arabia
shaheenataj.28@gmail.com, SRahman@centennialcollege.ca, raylin@cs.nccu.edu.tw, mohalhamid@ksu.edu.sa

Abstract

Internet-of-Things (IoT) based applications are rapidly gaining popularity. Smart home is one of them; home security and safety, home automation, energy management and health surveillance are some applications of smart homes. Smart homes have enormous potential as well as enormous threat to security and privacy of the end users. Pay TV is considered asthe likely entry points for IoT services into smart homes. Pay TV has evolved security techniques very similar to of IoT based smart homes services. Pay TV is an application of broadcast encryption schemes in which premium content is broadcasted only to subscribed users. The broadcaster needs assurance that only subscribed user can access premium content, so the program is encrypted with a group key shared among all subscribers. Thus, to share the key, Pay-TV systems require efficient and secure group key agreement (GKA). This research proposes an efficient and secure, dynamic, ID-based authenticated, asymmetric group key agreement (AAGKA) protocol for Pay-TV networks. Security is proved under the assumptions of the discrete logarithm problem (DLP) and decisional Diffie-Hellman problem (DDHP). Finally, comparison of the protocol with state-of-art protocols shows that the proposed protocol is highly efficient.

Keywords: Internet-of-Things (IoT), Authentication, Asymmetric group key agreement, Bilinear pairing, Pay-TV network

1 Introduction

Smart homes, an IoT based application is next big thing in the rapidly growing technology-based lifestyle. Pay -TV has much to offer to the fast-developing smart home era. Over the years, Pay-TV had gained trust among the customers with secure data management and determination without compromising the privacy of the subscribers. In order to avail the benefits of smart homes and IoT, consumers have to allow the new technology to go deeper into their homes.

With established subscriber relationship, Pay-TV can enable IoT to manage smart homes with robustness and reliability and without any attack on their privacy.

Group key agreement (GKA) protocols provide a secure and robust approach to establishing group session keys for public networks and hence aim to provide secure communication over an insecure network. Wu et al. [20], introduced the concept of the asymmetric group key agreement (AGKA) protocol, in which all group members compute a common secret group key and only group members can broadcast secret messages to the group. In asymmetric protocols, unlike in symmetric protocols, all group members compute a common group encryption key (GEK) and hold different group decryption keys (GDKs).

The authenticated asymmetric protocol proposed here has the following advantages: (1) messages can also be broadcasted by any non-registered member in the group (using the GEK); (2) asymmetric protocols use short signatures to achieve mutual authentication; and (3) the protocol complements dynamic networks by maintaining backward and forward secrecy. Thus, an authenticated, asymmetric group key agreement (AAGKA) protocol preserves benefits of both the GKA protocol and broadcast encryption.

In a Pay-TV system, broadcasters generate revenue by charging subscribers for viewing programs. Thus, broadcasters need a mechanism so that only the paid subscribers can view the program. We present only a brief discussion here of the specific requirements of Pay-TV systems, but greater detail may be found in [7-8, 11, 13]. A Pay-TV system is asymmetric with respect to computational and communication capabilities between the broadcaster and the subscribers. Since the broadcaster has greater computational capabilities than the subscribers, a GKA protocol for Pay-TV should place greater computational and communication load on the broadcaster than on the subscribers.

Further, a key agreement protocol for Pay-TV must

[*] Corresponding Author: Shaheena Khatoon; E-mail: shaheenataj.28@gmail.com

DOI: 10.3966/160792642020092105014

be contributive; that is, each user in the group must equally contribute to the computation of the group decryption key, so that no user gets an undue computational advantage over another. Also, since Pay-TV is a dynamic system, with subscribers frequently joining or leaving the group, the rekeying mechanism should be efficient and secure. Additionally, the key agreement protocol must provide both forward and backward secrecy, so that joining or leaving subscribers can obtain no knowledge of any previously or newly established group decryption key.

A typical model for Pay-TV. Broadcasters have a database storing keys, link values, and other relevant information. Broadcasters have enough resources to undertake greater computational and communications load than subscribers. Broadcasters perform initial setup, generating the necessary public parameters, distributing them, and storing them securely. Meanwhile, each subscriber has a set-top box with a smart card that performs the necessary cryptographic operations. The set-top box makes registration and subscription requests to the broadcaster, receives encrypted content, and decrypts the content to make it available to the subscriber. Figure 1 illustrates a typical model for a Pay-TV communications and broadcasting network.

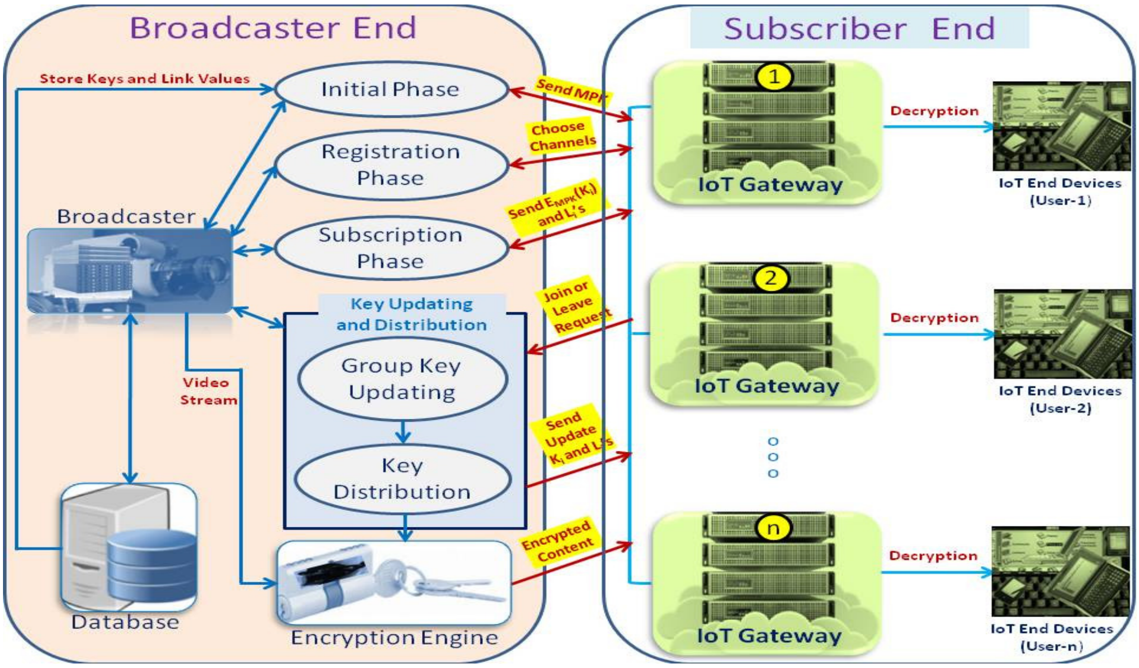


Figure 1. A typical communication model for Pay-TV system network

Organization of the Paper. The next section summarizes existing research in the same domain. In Section 3 describes the preliminaries of the cryptographic primitives to enable better understanding of the proposed protocol. The proposed protocol is detailed in Section 4. Section 5 describes the contributions of the subscribers in a model Pay-TV network and demonstrates the correctness of the proposed protocol. A detailed security analysis of the suggested protocol is presented in Section 6 while Section 7 analyzes the performance with respect to the computational and communications costs of the protocol. Finally, Section 8 concludes.

2 Related Works

There is an increasing interest to incorporate the IoT-based smart home service using Pay TVs. The genesis of IoT can be dated back in the year 1982, [22] when a coke vending machine was connected through internet. However, M. Weiser [24] gave a contemporary vision of IoT in the year 1991. Later in year 1999, B. Joy [19] demonstrated device to device communication. In the year 2009, K. Ashton [1] first coined the term “Internet of Things’’. But still there is no universally accepted definition of IoT, different group define it in different way. Concisely, IoT can be define as a system of interconnected physical objects, to exchange and collect data over the internet. Since its inception, IoT aims to improve one’s comfort and efficiency, by enabling cooperation among smart objects [12]. Further, Gubbi et al. [12] estimates that about 50 billion objects will be connected through IoT by 2020. So, the security challenges involved with IoT should be addressed at the design level.

Effective security practices, especially mutual authentication and key agreement schemes are needed to protect anonymity and privacy of the users. Fiat et al. [10] formalized the definition and paradigm of broadcasting encryption schemes. Since then, many schemes have been proposed for secure cryptographic broadcasting, with the most prominent among them being [5, 14-15, 18, 21]. However, these broadcasting encryption schemes do allow a sender to broadcast any content to a group of receivers but do not provide a key management mechanism, as security of these schemes basically trusts upon a key server for generation as well as distribution of encrypted keys. Since the trusted server can read all the communicated keys, it representsa threat to the security of the scheme.

Furthermore, schemes such as [14, 18] do not provide forward secrecy, hence making them poorly suited for Pay-TV. Some authentication schemes were suggested for Pay-TV in [7, 11], but these only authenticate the user to the group without providing a key exchange mechanism. Group key agreement protocols seem to offer solutions to the problems discussed above. Existing, group key agreement protocols assume pre-determined group members and once all these members participate in the protocol then only a secure channel for broadcasting is established. Since Pay-TV model is highly dynamic, traditional GKA protocol seem not applicable to it. Hence, Kim et al. [14] and Kumar et al. [16] offered group key agreement protocols for Pay-TV, but both are symmetric, meaning they provide only a key agreement mechanism without having a broadcast-encryption ability. Hence, an asymmetric, group key agreement protocol seems to offer a better solution for key management and broadcasting of premium content in Pay -TV applications.

Some asymmetric group key agreement exist in literature like, [26-29]. But as pointed by [27], Zhang et al.'s [26] scheme requires an identity-based signature to assure the security of the protocol, and it only provides partial forward secrecy (PFS). Ermi et al. [9] demonstrated that [27] is mainly suitable for small group communication like instant messaging applications [17], conference communication applications similarly Li and Zhang's [29] protocol is suitable for instant messaging applications, such as Messenger, We-chat and Whats App, whereas Zhang's protocol works well in a vehicular ad hoc networks (VANETS). But, none of the above research considers the issues with Pay-TV in IoT infrastructure. So, the present paper proposes an efficient, two-round, authenticated, asymmetric group key agreement (AAGKA) protocol specifically for Pay-TV that fulfills the above-discussed requirements in IoT infrastructure. The suggested protocol is simple and efficient, minimizing subscribers' computational cost by shifting the burden to the broadcaster.

3 Preliminaries

The following section gives a widely accepted definition of bilinear pairing and also defines discrete logarithm problem (DLP) and decision Diffie-Hellman Problem (DDHP).

Definition 3.1 (Bilinear Pairing). Suppose, $\langle G_1,+\rangle$ be acyclic additive group and $\langle G_2,.\rangle$ be a cyclic multiplicative group and the order of both the group is a large prime p. A bilinear pairing e is a map defined by $e: G_1 \times G_1 \rightarrow G_2$ and it has the following properties:

(1) Bilinear: According to this property, for given $(R,S) \in G_1, e(aR,bS) = e(R,S)^{ab}$, where $a,b \in Z_p^*$.

(2) Non-degenerate: According to this property, there exists $(R,S) \in G_1$, such that $e(R,S) \neq 1$ where 1 is the identity of G_2.

(3) Computable: This property assures, that there exist an algorithm which can efficiently compute $e(R,S)$ for all $(R,S) \in G_1$.

Two pairings used extensively for cryptography are the Weil pairing and its modifications and the Tate pairing. A full description of these pairings may be found in [2-4, 6].

Discrete logarithm problem (DLP). According to this problem, for given $(R,S) \in G$, it is computationally in feasible to find an integer $n \in Z_p^*$, such that $S = nR$.

Note, that discrete logarithm problem (DLP) is hard in both G_1 and G_2.

Decision Diffie-Hellman Problem (DDHP). According to this problem, for given (P, aP, bP, cP). Where $a,b,c \in Z_p^*$. It is computationally infeasible to decide whether $c = ab \bmod p$.

4 Proposed Group Key Agreement Protocol

This section presents an ID-based authenticated, asymmetric group key agreement (AAGKA) protocol suitable for Pay-TV. The following notations are used throughout for better understanding of the proposed protocol.

e: Denotes the bilinear map, $e: G_1 \times G_1 \rightarrow G_2$.

s: Denotes the master private key, $s \in Z_p^*$.

P: Denotes a generator of G_1.

P_{pub}: Denotes the system public key, $P_{pub} = sP$.

H_0: Denotes a hash function, $H_0: \{0,1\}^* \rightarrow \{0,1\}.^*$

H_1: Denotes a hash function, $H_1: \{0,1\}^* \rightarrow Z_p^*$.

U_i: Denotes the subscriber to Pay-TV, $1 \leq i \leq n-1$.

U_n: Denotes the broadcaster of Pay-TV.

ID_i: Denotes the identity of U_i.

PK_i: Denotes the long-term public key of a participant $U_i, PK_i = H_0(ID_i) = Q_i$.

SK_i: Denotes the long-term private key of a participant $U_i, SK_i = sH_0(ID_i) = sQ_i$.

GEK: Denotes the group encryption key.

GDK: Denotes the group decryption key.

Let $U = \{U_1, U_2, \ldots. U_n\}$ be the set of users in the AAGKA protocol, where $U_i \in U, (1 \le i \le n-1)$ are the subscribers and U_n is the broadcaster. Each has the unique identity $ID_i, (1 \le i \le n)$. The protocol is executed in three phases: (1) the AAGKA phase, (2) the subscriber leaving phase (SLP) and (3) subscriber joining phase (SJP).

(1) AAGKA phase.

(a) Setup: With the security parameter $k \in Z$, the trusted key generator center (KGC) generates a set of system parameters as follow

- KGC executes k to generate a large prime p, cyclic groups G_1 and G_2, where G_1 is additive and G_2 is multiplicative group, both the groups have same order p and pairing e which maps element of $G_1 \times G_1$ to G_2
- KGC randomly selects $s \in Z_q^*$, and computes system public key $P_{pub} = sP$, where s is the master private key (MPK).

(b) Authenticated Key Exchange

Round 1: Each subscriber $U_i \in U$, $(1 \le i \le n-1)$ randomly selects two numbers $m_i, r_i \in Z_p^*$ and computes $R_i = r_i P, M_i = m_i PK_n P_{pub}$ and $T_i = \left(\dfrac{m_i + SK_i}{r_i}\right)P$ and sends the tuple (U_i, R_i, M_i, T_i) to the broadcasting node U_n.

Note: Each subscriber can pre-compute these (R_i, M_i, T_i) off-line, reducing the computational burden.

Round 2: The broadcaster verifies the equation $e(R_i, T_i) = e(P, SK_n^{-1} M_i + PK_i P_{pub})$ for all $1 \le i \le n-1$. If the equation holds, U_n is assured that (U_i, R_i, M_i, T_i) has been sent by each U_i Then, the broadcaster randomly selects two numbers $m_n, r_n \in Z_p^*$, computing $R_n = r_n P, T_n = \left(\dfrac{m_n + SK_n}{r_n}\right)P, PK = \sum_{i=1}^{n-1} PK_i$ $RT = \prod_{i=1}^{n-1} e(R_i T_i)$, $Q_1 = RT^{m_n^2}$, $Q_2 = m_n PKP_{pub}$ and $X_i = SK_n^{-1} m_n M_i$. Next the broadcaster computes the group encryption key and decryption key $GEK = (Q_1, Q_2), GDK = e(f_n, \sum_{i=1}^{n-1} X_i)$ and $f_n = m_n P$. Finally, the broadcaster broadcasts (U_n, X_1, X_2, ,… X_{n-1}, R_n, T_n, Q_1, Q_2) to each U_i.

(c) Common Group Key Computation: Each U_i verifies the equation $e(R_n, T_n) = e(P, M_i^{-1} X_i + PK_n P_{pub})$. If the equation holds, each U_i is assured that the message has been broadcasted by U_n. Each U_i then computes, $GDK = e(f_j, \sum_{j=1}^{n-1} X_j) = e(m_n P, \sum_{j=1}^{n-1} X_j)$ $GEK = (Q_1, Q_2), f_j = X_i m_i^{-1}$.

If equation $e(Q_2, f_1) GDK = Q_1$ the GEK and GDK keys are correct.

(d) Encryption: Any user $U_i, (1 \le i \le n)$ encrypts plain text m as follows: randomly selects $t \in Z_p^*$, and computes $\delta = tP$, $\eta = m \oplus H_1(Q_1 . e(P, f_j)^{-1})^t)$. The cipher-text is $c = (\delta, \eta)$.

(e) Decryption: Any valid user can decrypt message $m = \eta \oplus H_1(e(\delta, GDK))$.

(2) Subscriber Leave Phase (SLP)

Let the set of subscribers $\{U_{j+1,} U_{J+2}, \ldots. U_{n-1}\}$ decide to leave the group U. Then, U_n updates the group to $U' = \{U_{i,}, \ldots. U_{i-1}, U_n\}$ and executes the SLP phase in the following way:

Round 1: U_n randomly selects two numbers $m_n', r_n' \in Z_p^*$ and computes $R_n' = r_n' P$ $T_n' = \left(\dfrac{m_n' + SK_n}{r_n'}\right)P$, $PK' = \sum_{1 \le j \le n-1, j \ne i} PK_j$, $RT' = \sum_{1 \le j \le n-1, j \ne i} e(R_j, T_j)$, $Q_1' = (RT')^{m_n' 2}$, $Q_2' = m_n' PK' P_{pub}$ and $X_j' = SK_n^{-1} m_n M_j$. Next the broadcaster computes the group encryption key $GEK' = (Q_1', Q_2')$, $f_n' = m_n' P$, and decryption key $GDK' = e(f_n', \sum_{1 \le j \le n-1, j \ne i} X_j')$. Finally, the broadcaster broadcasts $(U_n, X_1', X_2', \ldots., X_{i-1}', X_{i+1}', R_n', T_n', Q_1', Q_2')$ to each U_i'

Round 2: Common Group Key Computation: Each $U_j, (1 \le j \le n-1, j \ne i)$, verifies the equation $e(R_n', T_n') = e(P, M_j^{-1} X_j' + PK_n P_{pub})$. If the equation holds, each U_j is assured that the message has been broadcasted by U_n. Each U_j then computes $GEK' = (Q_1', Q_2'), f_j = X_j' M_j^{-1}$ and $GDK' = e(f_j', \sum_{1 \le j \le n-1, j \ne i} X_j') = e(m_n P, \sum_{1 \le j \le n-1, j \ne i} X_j')$. If $e(P', f_j') GDK' = Q'$, GEK and GDK keys are correct.

(2) Subscriber join phase (SJP).

Let the set of subscribers $\{U_{n+1,} U_{n+2}, \ldots. U_l\}$ decide to join the group U. Then, U_n updates the group to $U'' = \{U_{i,}, \ldots., U_n, U_{n+1}, \ldots\ldots U_l\}$ and executes the SJP phase in the following way:

Round 1: Each $U_k = (n+1 \le k \le l)$ register its identity with U_n randomly selects two numbers $m_k, r_k \in Z_p^*$ and computes $R_k = r_k P, M_k = m_k PK_n P_{pub}$ and $T_k =$

$\left(\dfrac{m_k + SK_k}{r_k}\right)P$ sending the tuple (U_k, R_k, M_k, T_k) to the broadcasting node U_n.

Note: In this case, nodes can also pre-compute (R_k, M_k, T_k) and store the tuple on their memory cards.

Round 2: The broadcaster verifies the equation $e(R_k, T_k) = e(P, SK_n^{-1}M_k + PK_k P_{pub})$ for all $n+1 \le n \le l$. If the equation holds, U_n is assured that (U_k, R_k, M_k, T_k) has been sent by each U_k Then, the broadcaster randomly selects two numbers $m_n^{''}, r_n^{''} \in Z_p^*$, computing $R_n^{''} = r_n^{''}P$, $T_n^{''} = \left(\dfrac{m_n^{''} + SK_n}{r_n^{''}}\right)P$, $PK_n^{''} = \sum_{k=n+1}^{l} PK_k$ $RT^{''} = \prod_{k=n+1}^{l} e(R_k T_k)$, $Q_1^{''} = (RT + RT^{''})^{m_n^{''2}}$ and $Q_2 = m_n^{''}(PK + PK^{''})P_{pub}$, and $X_i^{''} = SK_n^{-1} m_n^{''} M_k, (1 \le k \le l, l \ne n)$. Next the broadcaster computes the group encryption key and decryption key $GEK^{''} = (Q_1^{''}, Q_2^{''}), GDK^{''} = e(f_n^{''}, \sum_{i=1, i\ne n}^{l} X_i)$ and $f_n^{''} = m_n^{''}P$. Finally, the broadcaster broadcasts $(U_n, X_1^{''}, \ldots X_{n-1}^{''}, X_{n+1}^{''}, \ldots X_n^{''}, R_n^{''}, T_n^{''}, Q^{''})$ to each joining node $U_k = (n+1 \le k \le l)$

Common group key computation. Each $U_k = (n+1 \le k \le l)$ verifies the Equation $e(R_n^{''}, T_n^{''}) = e(P, M_k^{-1}X_k + PK_n P_{pub})$.

If the equation holds, each U_k is assured that the message has been broadcasted by U_n.

Then each U_k computes $GDK^{''} = e(f_j^{''}, \sum_{i=1, i\ne n}^{l} X_i)$ $= e(m_n^{''}P, \sum_{i=1, i\ne n}^{l} X_i)$ $GEK = (Q_1^{''}, Q_2^{''}), f_j^{''} = X_i M_i^{-1}$.

If equation $e(Q_2^{''}, f_j^{''})GDK^{''} = Q_1^{''}$ the GEK and GDK keys are correct.

5 Contributiveness and Correctness of the Proposed Protocol

The present section will demonstrate that the suggested protocol is correct and satisfies the property of contributiveness.

Theorem 5.1 (Contributiveness) In the proposed protocol, an identical contributory group encryption (GEK) and group decryption (GDK) keys are established by all the nodes, and each node's contribution is included in the construction of the group key.

Proof 5.1: We note that, $GEK = (Q_1, Q_2)$ $= (m_n PKP_{pub}, RT^{m_n^2}) = (m_n \sum_{i=1}^{n-1} PK_i P_{pub}, RT^{m_n^2})$. In the above equation, each PK_i (each user's public key) is used in the construction of the GEK. This proves that each node's contribution is included in the construction of the GEK. Further, $\sum_{j=1}^{n-1} X_j = SK_n^{-1} m_n M_i \; = m_n m_j P$ and $f_j = X_j m_j^{-1}$, from which $GDK =$ $e(f_j, \sum_{j=1}^{n-1} X_j)$ $= e(m_n P, \sum_{j=1}^{n-1} m_n m_j P)$. From this equation, we can observe that GDK contains $m_i, (1 \le i \le n)$, the secret number of all nodes. This proves that each node's contribution is included in the construction of the GDK.

Theorem 5.2 (Correctness): Each user $U_i, (1 \le i \le n)$ computes the identical group decryption key GDK.

Proof 5.2: The group decryption key can be computed

$$GDK = e(f_j, \sum_{j=1}^{n-1} X_j)$$

as follows:

$$\begin{aligned} &= e(m_n P, \sum_{j=1}^{n-1} m_n m_i P) \\ &= e(m_n P, m_n(m_1 + m_2 + \ldots m_{(n-1)})p) \\ &= e(P,P)^{(m_1 + m_2 + \ldots m_{(n-1)})m_n^2} \end{aligned}$$

observing the above derivation it can be concluded that each user $U_i, (1 \le i \le n)$ can compute the identical group decryption key GDK.

Theorem 5.3 (Correctness): The verification equations that are used in the proposed protocol are correct i.e.,

$$\begin{gathered} e(R_i, T_i) = e(P, SK_n^{-1} M_i + PK_i P_{pub}), (1 \le i \le n-1), \\ e(R_n, T_n) = e(P, M_i^{-1} X_i + PK_n P_{pub}), (1 \le i \le n-1), \\ e(Q_2, f_j)GDK = Q_1, (1 \le j \le n-1). \end{gathered}$$

Proof 5.3: By the definition of bi-linear pairing,

$$e(R_i, T_i) = e(r_i P, \left(\frac{m_i + SK_i}{r_i}\right)P), = e(P,P)^{(m_i + SK_i)}$$

and

$$\begin{aligned} e(R_i, T_i) &= e(P, SK_n^{-1} M_i + PK_i P_{pub}), (1 \le i \le n-1), \\ &= e(P, s^{-1} Q_i^{-1} m_i PK_n P_{pub} + PK_i P_{pub} \\ &= e(P, s^{-1} Q_i^{-1} m_i PK_n sP \;\; + PK_i sP\,) \\ &= e(P,P)^{(m_i + SK_i)} \end{aligned}$$

This derivation establishes the equation, $e(R_i, T_i) =$

$e(P, SK_n^{-1} M_i + PK_i P_{pub})$.

In the similar way we can show, $e(R_n, T_n) = e(P, M_i^{-1} X_i + PK_n P_{pub})$.

Lastly, we will show, $e(Q_2, f_j) GDK = Q_1, (1 \le j \le n-1)$.

$$\begin{aligned} Q_2 &= m_n PKP_{pub} \\ &= m_n \sum_{i=1}^{n-1} PK_i sP \\ &= m_n P \sum_{i=1}^{n-1} SP\, K_i \\ &= m_n P \sum_{i=1}^{n-1} SK_i \end{aligned}$$

So, by the property of bi-linearity we have,

$$\begin{aligned} & e(Q_2, f_j) GDK \\ &= e\left(m_n P \sum_{i=1}^{n-1} SK_i, m_n p \right) e(P,P)^{(m_1+m_2+\ldots m_{(n-1)}) m_n^2}, \\ &= e(P,P)^{(\sum_{i=1}^{n-1} SK_i) m_n^2} e(P,P)^{(\sum_{i=1}^{n-1} m_i) m_n^2}, \\ &= e(P,P)^{(\sum_{i=1}^{n-1} (SK_i + m_i)) m_n^2} \end{aligned}$$

and

$$\begin{aligned} Q_1 &= RT^{m_n^2} \\ &= \left[\prod_{i=1}^{n-1} (R_i, T_i) \right]^{m_n^2}, \\ &= \left[\prod_{i=1}^{n-1} e(r_i P, (\frac{m_i + SK_i}{r_i}) P) \right]^{m_n^2}, \\ &= \left[\prod_{i=1}^{n-1} (P,P)^{\sum_{i=1}^{n-1} SK_i + m_i} \right]^{m_n^2}, \\ &= e(P,P)^{(\sum_{i=1}^{n-1} (SK_i + m_i)) m_n^2} \end{aligned}$$

Thus, all the verification equations are correct.

6 Security Analysis

The present section, shows that the suggested protocol is secure under the assumptions of DLP and DDHP.

Theorem 6.1: Under the DDHP assumption, the proposed protocol is secure. This means, no adversary can get the group decryption key (GDK) by eavesdropping the public parameters and messages broadcasted over the public channel.

Proof 6.1: Let adversary Adv try to construct the group decryption key (GDK) by eavesdropping on public parameters and messages broadcasted over the public channel. Adv cannot do so, as $(M_j, X_j, GDK = e(f_j, \sum X_j))$ and $(M_j, X_j, GDK = e(\beta, \sum X_j))$ for $(1 \le j \le n-1)$ are computationally indistinguishable where $\beta \in G_1$ is a random value.

Adversary Adv uses the algorithm A to construct A' (another algorithm) to differentiate between (aP, abP, bP) and $(aP, abP, \beta P)$ where $\beta \in G_1$ is a random value and $a, b \in Z_p^*$.

Let $M_1 \in aP$, and $X_1 \in abP$. Then A' randomly selects $\lambda_1, \ldots.. \lambda_{n-1}$ and calculates $M_1, \ldots.. M_{n-1}$ as below:

$$\begin{aligned} & M_2 = \lambda_1 P, X_2 = \lambda_1 M_1; \\ & M_3 = \lambda_2 P, X_3 = \lambda_2 M_2; \\ & \vdots \\ & M_{n-1} = \lambda_{n-2} P, X_{n-1} = \lambda_{n-2} M_1; \end{aligned}$$

in this way, A' constructs all $\left(M_j, X_j\right), \left(1 \le j \le n-1\right),;$ calculating the group decryption key, $GDK = e(\beta, \sum X_j)$. It then calls A with this value. If $GDK = e(\beta, \sum X_j)$ means that $\beta = bP$, adversary Adv can differentiate between (aP, abP, bP) and $(aP, abP, \beta P)$ which contradicts tothe DDHP assumption. Therefore, the suggested protocol is secure under the DDHP assumption.

Theorem 6.2: The suggested protocol provides forward secrecy under the DLP assumption. That is, newly joined members cannot obtain previously established group decryption keys.

Proof 6.2: To prove the theorem, we show that newly joined members $U_k, (m-1 \le k \le l)$ cannot obtain a previously established group decryption key, $GDK = e(X_i m_i^{-1}, \sum X_i), (1 \le i \le n-l)$.

Because of the DLP assumption, the newly joined member U_k cannot obtain the ephemeral secret m_i from the broadcasted message $M_i = m_i PK_n P_{pub}$ for $(1 \le i \le n-l)$, nor, similarly, can they get the ephemeral secret m_n from X_i . Hence, U_k cannot construct the previously established group decryption key.

Theorem 6.3: The proposed protocol provides backward secrecy under the DLP assumption. That is, members who leave the group can get no knowledge of any newly established group decryption keys.

Proof 6.3: Let the members $\left\{U_{j+1}, \ldots.., U_{n-1}\right\}$ decide to leave the group. The remaining members then compute the new group decryption key GDK$^{'}$ (as described in the member leaving phase). However, the new ephemeral secret $m_n^{'}$ is not known to leaving members, nor can it be derived from public parameters or the broadcasted message $T_n' = \left(\frac{m_n' + SK_n}{r_n'}\right)P$ or $X_j' = SK_n^{-1} m_n' M_j$, due to the DLP assumption. Hence, leaving members cannot construct the newly established group decryption key, which proves the theorem.

7 Performance Evaluation and Comparison

In this section, we evaluate the performance of the proposed protocol and compare it with the protocols of Wu et al. [20] and Zhao et al. [25]. For a more realistic comparison and evaluation, we used the data given in [23]. According to [23], a133-MHz Strong ARM microprocessor was used. Table 1 summarizes the energy costs used to evaluate the performance of the protocols, on the other hand Table 2 compares the efficiency of the protocols. Figure 2 and Figure 3 compare the computational and communication costs, respectively. From Table 2 and Figure 2 and Figure 3, we conclude that the proposed protocol is more efficient in terms of computational and communication resources than the other protocols.

Table 1. Comparison table considering energy consumption

Operation	Energy costs/mJ
Cost of computation for a modular exponentiation (E)	9.1
Cost of computation for a scalar multiplication (M)	8.8
Cost of computation for a Tate pairing (T)	47.0
Sign. Gen. by elliptic curve digital signature algorithm (Sign)	8.8
Sign. Gen. by elliptic curve digital signature verify algorithm (Ver)	10.9
Cost of computation for transmitting a bit	0.00066
Cost of computation for receiving a bit	0.00031

Table 2. Comparison table considering efficiency

	Wu et al. [20]	Zhao et al. [25]	Proposed
Round	1	3	2
Forward secrecy	No	Yes	Yes
Contributory GKA	Yes	Yes	Yes
Dynamic	No	Yes	Yes
Computational cost of each subscriber	(n-1) Sign+ (n-1)Ver+ 2nM	3Sign+2nVer+(n-1) M+4E	5T+nM
Computational cost of the broadcaster	-	-	E+(3n+2) T+(2n+2)M
Transmission cost of each subscriber	n|G|	(2n + 7)|G|	(n + 8)|G|
Transmission cost of the broadcaster	-	-	(n + 3)|G| + |U|

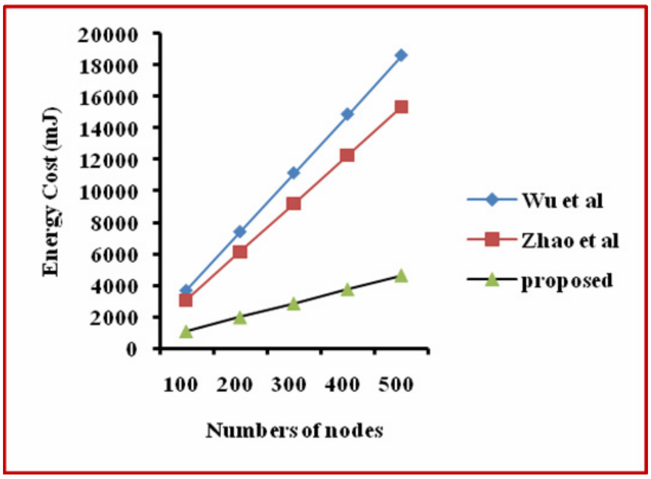


Figure 2. Comparison of computational cost

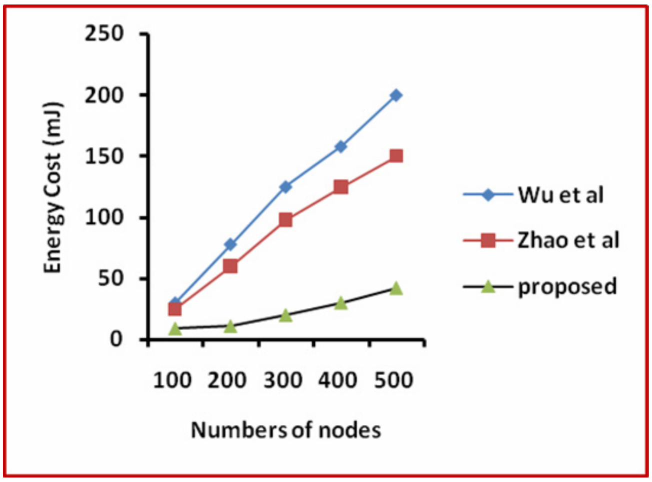


Figure 3. Comparison of communication cost

8 Conclusion

Pay TV has evolved security techniques very similar to those required by the IoT based smart homes services. So, the Pay TV are considered as the likely entry points for IoT services into smart homes. Over the years Pay TV has gained thrust among the subscribers, this trust is the biggest opportunity for Pay TV operators for extending their offering with IoT enabled smart home services. Hence the present paper, propose an ID-based authenticated, asymmetric group key agreement (AAGKA) protocol for Pay TV. The group members negotiate a common group encryption key (GEK) and compute a different group decryption key (GDK). So, any broadcaster of a secret message to the group need not join the group. Instead, such a broadcaster can share a secret key with the group members through a GKA protocol. Further, we have shown that the proposed protocol is secure under the DLP and DDHP assumptions in bilinear pairings. The proposed asymmetric protocol was also analyzed to be secure and efficient compared to existing protocols. Furthermore, it is contributory, which is a requirement for Pay-TV networks.

Acknowledgments

The authors are grateful to the Deanship of Scientific Research, King Saud University for funding through Vice Deanship of Scientific Research Chairs; Smart technologies; and by the Department of Science and Technology (DST), Government of India under Women Scientist Scheme A (WOS-A) No. under Grant no SR/WOS-A/PM-10/2018(G).

References

[1] K. Ashton, That Internet of Things, *RFID Journal*, Vol. 22, No. 7, pp. 97-114, June, 2009.

[2] D. Boneh, B. Lynn, H. Shacham, Short Signatures from the Weil Pairing, *International Conference on the Theory and Application of Cryptology and Information Security*, Gold Coast, Australia, 2001, pp. 514-532.

[3] P. Barreto, H. Kim, B. Lynn, M. Scott, Efficient Algorithms for Pairing-based Cryptosystems, *Annual International Cryptology Conference*, Santa Barbara, USA, 2002, pp. 354-368.

[4] D. Boneh, M. Franklin, Identity-based Encryption from the Weil Pairing, *SIAM Journal on Computing*, Vol. 32, No. 3, pp. 586-615, August, 2003.

[5] D. Boneh, C. Gentry, B. Waters, Collusion Resistant Broadcast Encryption with Short Cipher texts and Private Keys, *Annual International Cryptology Conference*, Santa Barbara, USA, 2005, pp. 258-275.

[6] L. Chen, Z. Cheng, N. P. Smart, Identity-based Key Agreement Protocols from Pairings, *International Journal of Information Security*, Vol. 6, No. 4, pp. 213-241, July, 2007.

[7] T. H. Chen, Y. C. Chen, W. K. Shih, H. W. Wei, An Efficient Anonymous Authentication Protocol for Mobile Pay-TV, *Journal of Network and Computer Applications*, Vol. 34, No. 4, pp. 1131-1137, July, 2011.

[8] K. Y. Chou, Y. R. Chen, W. Tzeng, An Efficient and Secure Group Key Management Scheme Supporting Frequent Key Updates on Pay-TV Systems, *Network Operations and Management Symposium*, Taipei, Taiwan, 2011, pp. 1-8.

[9] O. Ermis, S. Bahtiyar, E. Anarim, M. Ufuk Caglayan, A Comparative Study on the Scalability of Dynamic Group Key Agreement Protocols, *Conference on Availability, Reliability and Security*, Reggio Calabria, Italy, 2017, pp. 306-310.

[10] A. Fiat, M. Naor, Broadcast Encryption, *Annual International Cryptology Conference*, Santa Barbara, USA, 1993, pp. 480-491.

[11] M. S. Farash, M. A. Attari, A Provably Secure and Efficient Authentication Scheme for Access Control in Mobile Pay-TV Systems, *Multimedia Tools and Applications*, Vol. 75, No. 1, pp. 405-424, January, 2016.

[12] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): A vision, Architectural Elements, and Future Directions, *Future Generation Computer Systems*, Vol. 29, No. 7, pp. 1645-1660, September, 2013.

[13] H. Kim, J. Nam, S. Kim, D. Won, Secure and Efficient ID-based Group Key Agreement Fitted for Pay-TV, *Pacific-Rim Conference on Multimedia*, Jeju Island, Korea, 2005, pp. 117-128.

[14] C. Kim, Y. Hwang, P. Lee, Practical Pay-TV Scheme Using Traitor Tracing Scheme for Multiple Channels, *International Workshop on Information Security Applications*, Jeju Island, Korea, 2004, pp. 264-277.

[15] F. Kanazawa, N. Ohkawa, H. Doi, T. Okamoto, E. Okamoto, Broadcast Encryption with Sender Authentication and Its Duality, *International Conference on Convergence Information Technology*, Gyeongju, South Korea, 2007, pp. 793-798.

[16] A. Kumar, S. Tripathi, P. Jaiswal, Design of Efficient ID-based Group Key Agreement Protocol Suited for Pay-TV Application, *International Conference on Advances in Computing, Communications and Informatics*, Kochi, India, 2015, pp. 1940-1944.

[17] J. Wang, Y. Miao, P. Zhou, M. S. Hossain, Sk M. M. Rahman, A Software Defined Network Routing in Wireless Multihop Network, *Journal of Network and Computer*, Vol. 85, pp. 76-83, May, 2017.

[18] Y. Mu, V. Varadharajan, Robust and Secure Broadcasting, *International Conference on Cryptology*, Chennai, India, 2001, pp. 223-231.

[19] J. Pontin, *ETC: Bill Joy's Six Webs*, https://www.technologyreview.com/2005/09/29/230292/etc-bill-joys-six-webs/, 2005.

[20] Q. Wu, Y. Mu, W. Susilo, B. Qin, J. Domingo-Ferrer, Asymmetric Group Key Agreement, *International Conference on the Theory and Applications of Cryptographic Techniques*, Cologne, Germany, 2009, pp. 153-170.

[21] D. H. Phan, D. Pointcheval, V. C. Trinh, Multi-channel broadcast encryption, *8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, Hangzhou, China, 2013, pp. 277-286.

[22] The Only Coke Machine on the Internet, Carnegie Mellon University, School of Computer Science.

[23] C. H. Tan, J. C. M. Teo, Energy-efficient ID-based Group Key Agreement Protocols for Wireless Networks, *20th International Parallel and Distributed Processing Symposium*, Rhodes Island, Greece, 2006, pp. 1-8.

[24] M. Weiser, The Computer for the 21st Century, *Scientific American*, Vol. 265, No. 3, pp. 94-105, September, 1991.

[25] X. Zhao, F. Zhang, H. Tian, Dynamic Asymmetric Group Key Agreement for Ad Hoc Networks, *Ad Hoc Networks*, Vol. 9, No. 5, pp. 928-939, July, 2011.

[26] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, Provably Secure One-round Identity-based Authenticated Asymmetric Group Key Agreement Protocol, *Information Sciences*, Vol. 181, No. 19, pp. 4318-4329, October, 2011.

[27] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, Z. Dong, Round-efficient and Sender-unrestricted Dynamic Group Key Agreement Protocol for Secure Group Communications, *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 11, pp. 2352-2364, November, 2015.

[28] L. Zhang, OTIBAAGKA: A New Security Tool for Cryptographic Mix-Zone Establishment in Vehicular Ad Hoc Networks, *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 12, pp. 2998-3010, December, 2017.

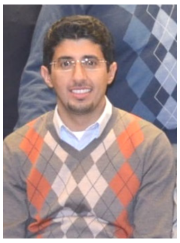
[29] J. Li, L. Zhang, Sender Dynamic, Non-Repudiable, Privacy-Preserving and Strong Secure Group Communication Protocol, *Information Sciences*, Vol. 414, pp. 187-202, November, 2017.

Biographies

Shaheena Khatoon is a full-time research scholar at Pt. Ravishankar Shukla University, India. She received the B.Sc., M.Sc. and MPhil degree in Mathematics form the same university in 2005, 2007 and 2009 respectively. She was awarded the gold medal for securing highest marks in the M.Sc. program. Her research interests are public key cryptography, information security and applied mathematics.

Sk Md Mizanur Rahman is a full-time professor in Centennial College. He has published around hundred peer reviewed journals and conference research articles and an industrial patent on cryptographic key generation and protection. Dr. Rahman’s main research focuses on cryptography, software and network security, machine learning in information security.

Raylin Tso is a Professor at the Department of Computer Science, National Chengchi University, Taiwan. He received his Ph.D. degree from Tsukuba University, Japan. His research interests include cryptography, privacy preserving technologies, and blockchain. He is also the Editor-in-Chief of the International Journal of Information and Computer Security.



Mohammed F. Alhamid received his Ph.D. degree in computer science from the University of Ottawa, Canada. He is currently an Assistant Professor with the Software Engineering Department, King Saud University, Riyadh, Saudi Arabia. His research interests include Artifical Inteliginet and Machine Learning.