Comparison of Existing Key Establishment Protocols

Boyeon Song and Kwangjo Kim

Information and Communications University (ICU)
58-4 Hwaam-dong, Yusong-gu, Taejon, 305-732, S. Korea
{bysong, kkj}@icu.ac.kr

Abstract

This paper classifies existing key establishment protocols according to cryptographic techniques, models of environment used, and the number of pass. The protocols' messages are described briefly and its properties are compared in four groups; key transport protocols using symmetric techniques, key transport protocols using asymmetric techniques, key agreement protocols using symmetric techniques, and key agreement protocols using asymmetric techniques.

1 Introduction

Cryptographic keys need to be established to the communicating parties prior to secure communications for security services which is based on cryptographic mechanisms like data encipherment, message authentication, and digital signatures. *Key establishment* protocol is a process whereby a shared secret key becomes available to participating entities, for subsequent cryptographic use. It is broadly subdivided into key transport and key agreement protocol[11]. In *key transport* protocols, a key is created by one entity and securely transmitted to the other entity. In *key agreement* protocols, both entities contribute information to generate the shared secret key[4].

Key establishment protocol employs symmetric or asymmetric key cryptography. A *symmetric* cryptographic technique is a system involving two transformations - one for the initiator and one for the responder - both of which make use of the same secret key[11]. In this system the two entities previously possess common secret information, so the key management problem is a crucial issue. An *asymmetric* cryptographic technique is a system involving two related transformations - one defined by a public key (the public transformation), and another defined by a private key (the private transformation) - with the property that it is computationally infeasible to determine the private transformation from the public transformation[11]. In this system the two entities share only public information that has been authenticated[5].

Key establishment protocol can be grouped into three models by the nature of the communication links, the trust relationships involved, and the cryptographic techniques used: point-to -point key establishment, key establishment within one domain, and key establishment between domains.

This paper classifies key establishment protocols, describes existing protocols, and compare them according to some requirements needed for secure key establishment. The remaining of this paper is organized as follows. Section 2 explains general models for key establishment environment, basic requirements of key establishment, and notations common to all the protocols. Section 3 classifies existing key transport protocols as cryptographic techniques, models of environment used, and the number of pass, and describes the briefs of the protocols' messages. Section 4 classifies and describes key agreement protocols in the same way. Section 5 compares key establishment protocols according to the requirements described in section 2. Finally, Section 6 makes concluding remarks.

2 Preliminary

2.1 Models for Key Establishment Environment

Key establishment protocols are influenced by the nature of the communication links, the trust relationships involved and the cryptographic techniques used; the entities may either communicate directly or indirectly, may belong the same or different security domains, and may or may not use the services of a trusted authority. The environments for the establishment of keys are illustrated[14].

2.1.1 Point-to-Point Key Establishment

Point-to -point key establishment is the basic mechanism of every key establishment scheme. It is required that the entities have to share a key so that further keys may be established directly between the entities[7, 14].

- When the entities use symmetric techniques,

  the two parties involved already share a key that can be used to protect the keying material to be established.

- When the entities use asymmetric techniques,

  each of the parties has a public key with its associated private key, and that the authenticated public key is known to the other party; for data integrity of data origin authentication, the recipient requires the sender's corresponding public key certificate, and for confidentiality, the sender does a public key certificate of the intended recipient.

2.1.2 Key Establishment Within One Domain

Key establishment within one domain employs a single *Trusted Third Party* (TTP) for the entire system. This authority may offer key management services such as the generation, certification, distribution or translation or keying material[7, 14].

- When the entities use symmetric techniques,

  a sender and a receiver are required to share keys with the authority. Key establishment then is initiated in one of two ways.

  ◦ *Key Distribution Center* (KDC) : By one entity asking a KDC to generate a key for subsequent distribution. The KDC then either distributes the key directly to both entities, or it sends it back to the initiator, who forwards it to the other entity.

  ◦ *Key Translation Center* (KTC) : By one entity generating the key and sending it to a KTC. The KTC may either forward directly it to the other entity, or send it back to the first entity, who forwards it to the second entity.

- When the entities use asymmetric techniques,

  each entity may need to contact its authority to get an appropriate public key certificate. Then the TTP typically is called *Certification Authority* (CA).

Key establishment for large systems usually is organized in a hierarchical way. *Security Domain* is a group of entities served by one authority[7, 14].

2.1.3 Key Establishment Between Domains

This model involves entities belonging to different security domains which share at least one cryptographic technique. Each security domain has its own security authority[7].

- When the entities use symmetric techniques and do not have access to a common directory service that offers public key certificates,

  each entity shall contact its respective authority to get its partner's public key certificate. The authorities of A and B may exchange the public key certificates of entities A and B and forward them to A and B, respectively.

- When the entities use asymmetric techniques,

  At least one of them has to contact its authority to receive a secret key for communication. The authorities then establish a common secret key to be used by the entities. This key may be distributed by one authority to both entities using the other authority as a KTC, or via one of the entities which is responsible for forwarding the key to the other entity.

In situations where the authorities of A and B neither have a mutual trust relationship nor a direct communications path, they have to involve one of more additional TTPs until a chain of trust is established.

2.2 Requirements

Required properties for a key establishment protocol may include the followings[7, 16].

- **Entity Authentication of A to B** : the assurance of the identity of A for B
- **Implicit Key Authentication from A to B** : the assurance for B that A is the only other entity that can possibly be in possession of the correct key.
- **Key Confirmation from A to B** : the assurance for B that A is in possession of the correct key.
- **Explicit Key Authentication from A to B** : the assurance for B that A is the only other entity that is in possession of the correct key. (Implicit key authentication from A to B and key confirmation from A to B together imply explicit key authentication from A to B)
- **Efficiency** : Considerations include the number of message exchanges (passes) required, the number of bits transmitted, the complexity of computations required by each party, and possibility of precomputations.
- **Key Freshness** : a guarantee that the established keying material is new, as opposed to the reuse of old keying material.
- **Key Control** : the ability to choose the key or the parameters used in the key computation.

Security requirements are concerned with the confidentiality of a key, modification and replay detection and the detection of substitution. In practical implementations of key establishment protocols the key data may be need to further processing prior to being used for cryptographic communication. Key establishment protocols may contain optional data, depending upon the specific application. One such possible application is message authentication[15].

2.3 Notation

The following notations are used throughout this paper.

notation	meaning
I_X	distinguishing identifier of entity X
KDC	Key Distribution Center
KTC	Key Translation Center
CA	Certification Authority
T	distinguishing identifier of KDC or KTC
K	secret key for a symmetric cryptosystem
K_X	secret symmetric session key chosen by entity X
K_{XY}	secret key associated with the entities X and Y
$r,\ m$	random number
r_X	random number issued by entity X
t/n	time stamp or a sequence number
t_X/n_X	time stamp or a sequence number issued by entity X
L	validity period (life time)
TVP	time variant parameter
TVP_X	time variant parameter issued by entity X
$E_K(Z)$	encipherment of data Z with a symmetric algorithm using the key K
$D_K(Z)$	decipherment of data Z with a symmetric algorithm using the key K
$P_X(Z)$	entity X's public encipherment transformation of data Z
$S_X(Z)$	entity X's private signature transformation on data Z
$MAC_K(Z)$	message authentication code (MAC) on data Z using the key K
f	key generating function
X, Y	concatenation of data items X and Y in that order
$Cert_X$	entity X's public key certificate
$a,\ b$	entity A and B's static private keys; $a, b \in_R [1, q-1]$
$z_A,\ z_B$	entity A and B's static public keys; $z_A = g^a\ mod\ p, z_A = g^b\ mod\ p$
$x,\ y$	entity A and B's ephemeral private keys; $x, y \in_R [1, q-1]$
p	a large prime
q	a prime divisor of $p-1$
g	an element of order q in Z_p^* which is shared public by all the entities
H	cryptographic hash function
$A \longrightarrow B : Z$	A sends Z to B
$A \Longrightarrow B : Z$	A sends Z to B over a secure channel
$A : Z$	A executes Z

For the implementation of the protocols specified in this paper[15, 16], it is assumed that

- When the entities use symmetric techniques
  - ○ Point-to-Point
    A key K_{AB} is shared by A and B.
  - ○ TTP (KDC, KTC)
    There is a TTP T, with which A and B share secret keys, K_{AT} and K_{BT} respectively. T shall be able to generate or otherwise acquire a key K.
- When the entities use asymmetric techniques
  1. The entities are aware of each other's claimed identities. This may be achieved by the inclusion of identifiers information exchanged between the two entities, or it may be apparent from the context of the use of the mechanism.(Verifying the identity means to check that a received identifier field agrees with some known value or prior expectation.)

2. If a public key is registered with an entity then that entity shall make sure that the entity who registers the key is possession of the corresponding private key.
3. The authenticated public keys of entities A and B, z_A and z_B, are known between A and B.

3 Key Transport

Key transport protocols make use of symmetric or asymmetric encipherment techniques.

3.1 Symmetric techniques

This section presents the brief protocols of key transport protocols based on symmetric techniques. They are subdivided into protocols using three environments models: Point to Point, Key Distribution Centre (KDC) and Key Translation Centre (KTC). A point-to-point environment exists when two entities already share a key that can establish further keys. If two entities wish to communicate with each other using only symmetric techniques but do not currently share such a key, they shall make use of a KDC or KTC.

3.1.1 Point-to-Point

1. One-Pass

   - **KTS 1: Mechanism 1 of [15]**
     $A \longrightarrow B \;:\; TVP$
     $K = f(K_{AB}, TVP)$
   - **KTS 2: Mechanism 2 of [15]**
     $A \longrightarrow B \;:\; E_{K_{AB}}(K)$
   - **KTS 3: Mechanism 3 of [15]**
     $A \longrightarrow B \;:\; E_{K_{AB}}(t/n, I_B, K)$

2. Two-Pass

   - **KTS 4: Mechanism 4 of [15]**
     $A \longleftarrow B \;:\; r_B$
     $A \longrightarrow B \;:\; E_{K_{AB}}(r_B, I_B, K)$

3. Three-Pass

   - **KTS 5: Authenticated Key Exchange Protocol 2 (AKEP2) [11]**
     $A \longrightarrow B \;:\; r_A$
     $A \longleftarrow B \;:\; I_B, I_A, r_B, r_A, MAC_{K_{AB}}(I_B, I_A, r_B, r_A)$
     $A \longrightarrow B \;:\; I_A, r_B, MAC_{K_{AB}}(I_A, r_B)$
     $K = f(r_B, K'_{AB})$
   - **KTS 6: Authenticated Key Exchange Protocol 1 (AKEP1) [11]**
     $A \longrightarrow B \;:\; r_A$
     $A \longleftarrow B \;:\; I_B, I_A, r_B, r_A, r'_B, K \oplus f(r'_B, K'_{AB}), MAC_{K_{AB}}(I_B, I_A, r_B, r_A, r'_B, K \oplus f(r'_B, K'_{AB}))$
     $A \longrightarrow B \;:\; I_A, r_B, MAC_{K_{AB}}(I_A, r_B)$
     $K = f(r_B, K'_{AB})$
   - **KTS 7: Shamir's no-key protocol**
     $A \longrightarrow B \;:\; K^{r_A}\; mod\; p$
     $A \longleftarrow B \;:\; (K^{r_A})^{r_B}\; mod\; p$
     $A \longrightarrow B \;:\; (K^{r_A r_B})^{{r_A}^{-1}}\; mod\; p$
     $B:\; K = (K^{r_B})^{r_B^{-1}}\; mod\; p$

3.1.2 KDC

1. Three-Pass

   - **KTS 8: Mechanism 7 of [15]**
     $A \longrightarrow T \; : \; I_B$
     $A \longleftarrow T \; : \; E_{K_{AT}}(K, I_B), E_{K_{BT}}(K, I_A)$
     $A \longrightarrow B \; : \; E_{K_{BT}}(K, I_A)$
   - **KTS 9: Mechanism 10 of [15]**
     $A \longrightarrow T \; : \; E_{K_{AT}}(t_A/n_A, I_B)$
     $A \longleftarrow T \; : \; E_{K_{AT}}(t_T/n_T, K, I_B)$
     $T \longrightarrow B \; : \; E_{K_{BT}}(t'_T/t'_T, K, I_A)$

2. Four-Pass

   - **KTS 10: Mechanism 8 of [15]**
     $A \longrightarrow T \; : \; TVP_A, I_B$
     $A \longleftarrow T \; : \; E_{K_{AT}}(TVP_A, K, I_B), E_{K_{BT}}(t_T/n_T, K, I_A)$
     $A \longrightarrow B \; : \; E_{K_{BT}}(t_T/n_T, K, I_A), E_K(t_A/n_A, I_B)$
     $A \longleftarrow T \; : \; E_K(t_B/n_B, I_A)$
   - **KTS 11: Basic Kerberos authentication protocol [11]**
     $A \longrightarrow T \; : \; r_A, I_A, I_B$
     $A \longleftarrow T \; : \; E_{K_{AT}}(r_A, K, I_B, L), E_{K_{BT}}(K, I_A, L)$
     $A \longrightarrow B \; : \; E_{K_{BT}}(K, I_A, L), E_K(t_A, I_A)$
     $A \longleftarrow T \; : \; E_K(t_A)$
   - **KTS 12: Otway-Rees protocol [11]**
     $A \longrightarrow B \; : \; m, I_A, I_B, E_{K_{AT}}(r_A, m, I_A, I_B)$
     $B \longrightarrow T \; : \; m, I_A, I_B, E_{K_{AT}}(r_A, m, I_A, I_B), E_{K_{BT}}(r_B, m, I_A, I_B)$
     $B \longleftarrow T \; : \; E_{K_{AT}}(r_A, K), E_{K_{BT}}(r_B, K)$
     $A \longleftarrow B \; : \; E_{K_{AT}}(r_A, K)$

3. Five-Pass

   - **KTS 13: Mechanism 9 of [15]**
     $A \longleftarrow B \; : \; r_B$
     $A \longrightarrow T \; : \; r_A, r_B, I_B$
     $A \longleftarrow T \; : \; E_{K_{AT}}(r_A, K, I_B), E_{K_{BT}}(r_B, K, I_A)$
     $A \longrightarrow B \; : \; E_{K_{BT}}(r_B, K, I_A), E_K(r'_A, r_B)$
     $A \longleftarrow B \; : \; E_K(r_B, r'_A)$
   - **KTS 14: Needham-Schroeder shared-key protocol [11]**
     $A \longrightarrow T \; : \; I_A, I_B, r_A$
     $A \longleftarrow T \; : \; E_{K_{AT}}(r_A, I_B, K, E_{K_{BT}}(K, I_A))$
     $A \longrightarrow B \; : \; E_{K_{BT}}(K, I_A)$
     $A \longleftarrow B \; : \; E_K(r_B)$
     $A \longrightarrow B \; : \; E_K(r_B - 1)$

3.1.3 KTC

1. **Three-Pass**

   - **KTS 15: Mechanism 11 of [15]**
     $A \longrightarrow T \; : \; E_{K_{AT}}(I_B, K)$
     $A \longleftarrow T \; : \; E_{K_{BT}}(K, I_A)$
     $A \longrightarrow B \; : \; E_{K_{BT}}(K, I_A)$

2. **Four-Pass**

   - **KTS 16: Mechanism 12 of [15]**
     $A \longrightarrow T$: $E_{K_{AT}}(TVP_A, I_B, K)$
     $A \longleftarrow T$: $E_{K_{AT}}(TVP_A, I_B), E_{K_{BT}}(t_T/n_T, K, I_A)$
     $A \longrightarrow B$: $E_{K_{BT}}(t_T/n_T, K, I_A), E_K(t_A/n_A, I_B)$
     $A \longleftarrow B$: $E_K(t_B/n_B, I_A)$

3. **Five-Pass**

   - **KTS 17: Mechanism 13 of [15]**
     $A \longleftarrow B$: r_B
     $A \longrightarrow T$: $E_{K_{AT}}(r_A, r_B, I_B, K)$
     $A \longleftarrow T$: $E_{K_{AT}}(r_A, I_B), E_{K_{BT}}(r_B, K, I_A)$
     $A \longrightarrow B$: $E_{K_{BT}}(r_B, K, I_A), E_K(r'_A, r_B)$
     $A \longleftarrow B$: $E_K(r_B, r'_A)$

3.2 Asymmetric techniques

This section discusses key transport protocols based on asymmetric techniques. They are subdivided into protocols with and without signature.

3.3 Key Transport without signature

1. One-Pass

   - **KTA 1: Key transport mechanism 1 of [16]**
     $A \longrightarrow B$: $P_B(I_A, K, TVP)$
     ex) ElGamal, RSA

2. Three-Pass

   - **KTA 2: Needham-Schroeder public-key protocol [11]**
     $A \longrightarrow B$: $P_B(K_A, I_A)$
     $A \longleftarrow B$: $P_A(K_A, K_B)$
     $A \longrightarrow B$: $P_B(K_B)$
     $K = f(K_A, K_B)$
   - **KTA 3: Key transport mechanism 6 of [16]**
     $A \longrightarrow B$: $P_B(I_A, K_A, r_A)$
     $A \longleftarrow B$: $P_A(I_B, K_B, r_A, r_B)$
     $A \longrightarrow B$: r_B
     $K = f(K_A, K_B)$

3.4 Key Transport with signature

1. One-Pass

   - **KTA 4: Encrypting signed keys [11]**
     $A \longrightarrow B$: $P_B(K, t_A, S_A(I_B, K, t_A)$

   - **KTA 5: Encrypting and signing separately [11]**
     $A \longrightarrow B$: $P_B(K, t_A), S_A(I_B, K, t_A)$

   - **KTA 6: Signing encrypted keys [11]**
     $A \longrightarrow B$: $t_A, P_B(I_A, K), S_A(I_B, t_A, P_B(I_A, K))$

2. Two-Pass

   - **KTA 7: Key transport mechanism 4 of [16]**
     $A \longrightarrow B \ : \ r_A$
     $A \longleftarrow B \ : \ I_A, r_A, r_B, P_A(I_B, K), S_B(I_A, r_A, r_B, P_A(I_B, K))$

   - **KTA 8: X.509 strong two-way authentication [11]**
     $A \longrightarrow B \ : \ t_A, r_A, I_B, P_B(K_A), S_A(t_A, r_A, I_B, P_B(K_A))$
     $A \longleftarrow B \ : \ t_B, r_B, I_A, r_A, P_A(K_B), S_B(t_B, r_B, I_A, r_A, P_A(K_B))$

3. Three-Pass

   - **KTA 9: Key transport mechanism 5 of [16]**
     $A \longrightarrow B \ : \ r_A$
     $A \longleftarrow B \ : \ S_B(r_A, r_B, I_A, P_A(I_B, K_B))$
     $A \longrightarrow B \ : \ S_A(r_A, r_B, I_B, P_B(I_A, K_A))$
   - **KTA 10: X.509 strong three-way authentication [11]**
     $A \longrightarrow B \ : \ r_A, I_B, P_B(K_A), S_A(r_A, I_B, P_B(K_A))$
     $A \longleftarrow B \ : \ r_B, I_A, r_A, P_A(K_B), S_B(r_B, I_A, r_A, P_A(K_B))$
     $A \longrightarrow B \ : \ r_B, I_B, S_A(r_B, I_B)$

3.5 Hybrid Key Transport

Hybrid key transport protocol uses symmetric encryption in addition to both asymmetric encryption and signatures.

1. Two-Pass

   - **KTA 11: 2-pass Beller-Yacobi key transport [11]**
     $A \longleftarrow B \ : \ r_B, Cert_B$
     $A \longrightarrow B \ : \ P_B(v), E_v(Cert_A, w)$ (where $(v, w) = S_A(r_B, I_B)$)

2. Four-Pass

   - **KTA 12: 4-pass Beller-Yacobi key transport [11]**
     $A \longleftarrow B \ : \ Cert_B$
     $A \longrightarrow B \ : \ P_B(K)$
     $A \longleftarrow B \ : \ E_K(m)$
     $A \longrightarrow B \ : \ E_K(S_A(m), Cert_A)$

4 Key Agreement

Key agreement protocols can be classified into protocols using symmetric and asymmetric encipherment techniques.

4.1 Symmetric techniques

This section concisely presents key agreement protocols based on symmetric techniques. The protocols are grouped in accordance with the use of a TTP.

4.1.1 Point-to-Point

1. Two-Pass

   - **KAS 1: Mechanism 5 of [15]**
     $A \longrightarrow B \ \ : E_{K_{AB}}(t_A/n_A, I_B, K_A)$
     $A \longleftarrow B \ \ : E_{K_{AB}}(t_B/n_B, I_A, K_B)$
     $K = f(K_A, K_B)$

2. Three-Pass

   - **KAS 2: Mechanism 6 of [15]**
     $A \longleftarrow B \ \ : r_B$
     $A \longrightarrow B \ \ : E_{K_{AB}}(r_A, r_B, I_B, K_A)$
     $A \longleftarrow B \ \ : E_{K_{AB}}(r_B, r_A, K_B)$
     $K = f(K_A, K_B)$

4.1.2 TTP (CA)

- **KAS 3: Blom's scheme [11]**
  (public information) $p_A, p_B \in_R Z_p$
  $T: \ a, b, c \in_R Z_p$
  $\quad f(x,y) = a + b(x+y) + cxy \ mod \ p$
  $\quad g_A(x) = f(x, p_A)$
  $\quad g_B(x) = f(x, p_B)$
  $T \Longrightarrow A \ \ : g_A(x)$
  $T \Longrightarrow B \ \ : g_B(x)$
  $A: \ K = g_A(p_B), \quad B: \ K = g_B(p_A)$
  $K = f(p_A, p_B)$

4.2 Asymmetric techniques

This section describes the briefs of key agreement protocols using asymmetric techniques. They are based on Diffie-Hellman protocol[6].

4.2.1 Diffie-Hellman and related key agreement protocols

1. Non-interactive key agreement protocol

   - **KAA 1: Static Diffie-Hellman key agreement [11]**
     $A \ \cdots \ B$
     $A: \ K = z_B^{\,a} \ mod \ p, \quad B: \ K = z_A^{\,b} \ mod \ p$
     $K = g^{ab} \ mod \ p$

2. One-Pass

   - **KAA 2: ElGamal key agreement [11]**
     $A \longrightarrow B \ \ : g^x \ mod \ p$
     $A: \ K = z_B^{\,x} \ mod \ p, \quad B: \ K = (g^x)^b \ mod \ p$
     $K = g^{xb} \ mod \ p$
   - **KAA 3: Nyberg-Rueppel key agreement [15]**
     $A: \ e = g^r \ mod \ p$
     $\quad K = z_B \ r \ mod \ p$
     $\quad e' = e \cdot H(K, I_A, TVP) \ mod \ p$
     $\quad y = r - ae'$
     $A \longrightarrow B \ \ : I_A, TVP, e, y$

$B: \ K = e^b \ mod \ p$
$e' = e \cdot H(K, I_A, TVP) \ mod \ p$
$e = g^y \cdot z_A^{e'} \ mod \ p$

3. Two-Pass

- **KAA 4: Ephemeral Diffie-Hellman key agreement [6]**
  $A \longrightarrow B \ : \ g^x \ mod \ p$
  $A \longleftarrow B \ : \ g^y \ mod \ p$
  $A: \ K = (g^y)^x \ mod \ p, \quad B: \ K = (g^x)^y \ mod \ p$
  $K = g^{xy} \ mod \ p$
- **Matsumoto-Takashima-Imai (MTI) key agreement [10]**
  - **KAA 5-1: MTI A(0) key agreement**
    $A \longrightarrow B \ : \ g^x \ mod \ p$
    $A \longleftarrow B \ : \ g^y \ mod \ p$
    $A: \ K = (g^y)^a \cdot z_B^x \ mod \ p, \quad B: \ K = (g^x)^b \cdot z_A^y \ mod \ p$
    $K = g^{ay+bx} \ mod \ p$
  - **KAA 5-2: MTI B(0) key agreement**
    $A \longrightarrow B \ : \ z_B^x \ mod \ p$
    $A \longleftarrow B \ : \ z_A^y \ mod \ p$
    $A: \ K = (z_A^y)^{a^{-1}} g^{\ x} \ mod \ p, \quad B: \ K = (z_A^y)^{b^{-1}} g^{\ y} \ mod \ p$
    $K = g^{x+y} \ mod \ p$
  - **KAA 5-3: MTI C(0) key agreement**
    $A \longrightarrow B \ : \ z_B^x \ mod \ p$
    $A \longleftarrow B \ : \ z_A^y \ mod \ p$
    $A: \ K = (z_A^y)^{a^{-1}x} \ mod \ p, \quad B: \ K = (z_A^y)^{b^{-1}y} \ mod \ p$
    $K = g^{xy} \ mod \ p$
  - **KAA 5-4: MTI C(1) key agreement**
    $A \longrightarrow B \ : \ z_B^{ax} \ mod \ p$
    $A \longleftarrow B \ : \ z_A^{by} \ mod \ p$
    $A: \ K = (z_A^{by})^x \ mod \ p, \quad B: \ K = (z_B^{ax})^y \ mod \ p$
    $K = g^{aybx} \ mod \ p$
- **KAA 6: LLK key agreement [9]**
  $A \longrightarrow B \ : \ z_B^x \ mod \ p$
  $A \longleftarrow B \ : \ z_A^y \cdot (z_B^x)^{y/b} \ mod \ p$
  $A: \ K = z_B^x \cdot (z_A^y)^{a/(a+x)} \ mod \ p, \quad B: \ K = z_B^x \cdot z_A^y \ mod \ p$
  $K = g^{ay+bx} \ mod \ p$
- **KAA 7: KEA key agreement [13]**
  $A \longrightarrow B \ : \ g^x \ mod \ p$
  $A \longleftarrow B \ : \ g^y \ mod \ p$
  $A: \ K = (g^y)^a + z_B^x \ mod \ p, \quad B: \ K = (g^x)^b + z_A^y \ mod \ p$
  $K = g^{ay} + g^{bx} \ mod \ p$
- **KAA 8 : Unified Model key agreement [1]**
  $A \longrightarrow B \ : \ g^x \ mod \ p$
  $A \longleftarrow B \ : \ g^y \ mod \ p$
  $A: \ K = H(z_B^a, (g^y)^x), \ B: \ K = H(z_A^b, (g^x)^y)$
  $K = K = H(g^{ab}, g^{xy})$
- **KAA 9 : MQV key agreement [8]**
  $A \longrightarrow B \ : \ g^x \ mod \ p$
  $A \longleftarrow B \ : \ g^y \ mod \ p$
  $A: s_A = (x + a\overline{g^x}) mod \ q, K = (g^y (z_B)^{\overline{g^y}})^{s_A} mod \ p, \quad B: s_B = (y + b\overline{g^y}) mod \ q, K = (g^x (z_A)^{\overline{g^x}})^{s_B} mod \ p$
  $K = g^{s_A s_B} mod \ p$

- **KAA 10: Song-Kim key agreement [12]**
  $A \longrightarrow B \ \ : \ g^x \ mod \ p$
  $A \longleftarrow B \ \ : \ g^y \ mod \ p$
  $A: \ K = (g^y)^{(a+x)} \cdot z_B^x \ mod \ p, \quad B: \ K = (g^x)^{(b+y)} \cdot z_A^y \ mod \ p$
  $K = g^{xy+ay+bx} \ mod \ p$

4. Three-Pass

- **KAA 11: Station-to-Station protocol (STS) [5]**
  $A \longrightarrow B \ \ : \ g^x \ mod \ p$
  $A \longleftarrow B \ \ : \ g^y \ mod \ p, E_K(S_B(g^y, g^x, I_A))$
  $A \longrightarrow B \ \ : \ E_K(S_A(g^x, g^y, I_B))$
  $A: \ K = (g^y)^x \ mod \ p, \quad B: \ K = (g^x)^y \ mod \ p$
  $K = g^{xy} \ mod \ p$

- **KAA 12: AKC protocols [1]**
  $A \longrightarrow B \ \ : \ g^x \ mod \ p$
  $A \longleftarrow B \ \ : \ g^y \ mod \ p, MAC_K(2, g^y, g^x, I_B, I_A)$
  $A \longrightarrow B \ \ : \ MAC_K(3, g^x, g^y, I_A, I_B)$

  ex) MTI AKC, KEA AKC, Unified Model AKC, MQV AKC, Song-Kim AKC

5 Comparison

This section compares key establishment protocols classified in Sections 3 and 4. Table 1 and Table 2 summarize the properties of the key transport protocols using symmetric techniques and asymmetric techniques, respectively. In Table 3 and Table 4, the major properties of the key agreement protocols using symmetric techniques and asymmetric techniques are showed, respectively.

[Symbol]

A	The property is provided to A in the protocol.
A, B	The property is provided to both entities, A and B in the protocol.
$A \rightarrow B$	The property is provided from A to B in the protocol.
$A \leftrightarrow B$	The property is provided from A to B and from B to A.
(A)	The property can be provided to A as an option in the protocol by using additional means.
$\cdot$	The property is not provided in the protocol.
$\circ$	The property is provided in the protocol.
$t/n, r$	The property is provided by using $t/n, r$.
i, j	The number of computations of asymmetric transformation. (*i.e.*, A needs i computations and B needs j computations.)

[Abbreviation]

Sig	Signature
TTP	Trust Third Party
NP	Number of Passes
KA	Key Authentication (key integrity and key origin authentication)
IKA	Implicit Key Authentication
EKA	Explicit Key Authentication
Con	Key Confirmation
EA	Entity Authentication
PKO	Public Key Operation
KF	Key Freshness
KC	Key Control
KTS	Key Transport using Symmetric techinques
KTA	Key Transport using Asymmetric techinques
KAS	Key Agreement using Symmetric techinques
KAA	Key Agreement using Asymmetric techinques

Table 1: Comparison of Key Transport Protocols using Symmetric Techniques

KTS	TTP	NP	KA	Con	EA	KC	KF
1	·	1	·	·	·	A	t/n
2	·	1	·	·	·	A	·
3	·	1	○	·	A	A	t/n
4	·	2	○	·	A	A	r
5	·	3	○	·	A, B	B	r
6	·	3	○	○	A, B	B	r
7	·	3	·	·	·	A	·
8	KDC	3	○	·	·	KDC	·
9	KDC	3	○	·	·	KDC	t/n
10	KDC	4	○	○	A, B	KDC	t/n
11	KDC	4	○	○	$A, (B)$	KDC	t/n
12	KDC	4	○	·	·	KDC	r, m
13	KDC	5	○	○	A, B	KDC	r
14	KDC	5	○	○	A	KDC	r
15	KTC	3	·	·	·	A	·
16	KTC	4	○	○	A, B	A	t/n
17	KTC	5	○	○	A, B	B	r

Table 2: Comparison of Key Transport Protocols using Asymmetric Techniques

KTA	Sig	NP	IKA	Con	EA	KC	KF	PKO
1	·	1	$A \leftarrow B$	·	A	A	TVP	1,1
2	·	3	$A \leftrightarrow B$	$A \leftrightarrow B$	A, B	A, B	·	3,3
3	·	3	$A \leftrightarrow B$	$A \leftrightarrow B$	A, B	A, B	r	2,2
4	○	1	$A \leftarrow B$	$A \rightarrow B$	A	A	t	2,2
5	○	1	$A \leftarrow B$	$A \rightarrow B$	A	A	t	2,2
6	○	1	$A \leftarrow B$	$A \rightarrow B$	A	A	t	2,2
7	○	2	$A \rightarrow B$	$A \leftarrow B$	B	B	r	2,2
8	○	2	$A \leftrightarrow B$	$A \leftrightarrow B$	A, B	A, B	t, r	4,4
9	○	3	$A \leftrightarrow B$	$A \leftrightarrow B$	A, B	A, B	r	4,4
10	○	3	$A \leftrightarrow B$	$A \leftrightarrow B$	A, B	A, B	r	5,5
11	○	2	$A \leftrightarrow B$	$A \leftrightarrow B$	A, B	A, B	·	2,2
12	○	4	$A \leftrightarrow B$	$A \leftrightarrow B$	A, B	A	·	2,2

Table 3: Comparison of Key Agreement Protocols using Symmetric Techniques

KAS	TTP	NP	KA	Con	EA	KF
1	·	2	○	·	A, B	t/n
2	·	3	○	·	A, B	r
3	○	1	○	·	·	·

Table 4: Comparison of Key Agreement Protocols using Asymmetric Techniques

KAA	Sig	NP	IKA	Con	EA	KF	PKO
1	$\cdot$	0	$A \leftrightarrow B$	$\cdot$	$\cdot$	$\cdot$	1,1
2	$\cdot$	1	$A \leftarrow B$	$\cdot$	$\cdot$	$\circ$	2,1
3	$\circ$	1	$A \leftrightarrow B$	$A \leftarrow B$	A	$\circ$	2,3
4	$\cdot$	2	$\cdot$	$\cdot$	$\cdot$	$\circ$	2,2
5-1	$\cdot$	2	$A \leftrightarrow B$	$\cdot$	$\cdot$	$\circ$	3,3
5-2	$\cdot$	2	$A \leftrightarrow B$	$\cdot$	$\cdot$	$\circ$	3,3
5-3	$\cdot$	2	$A \leftrightarrow B$	$\cdot$	$\cdot$	$\circ$	2,2
5-4	$\cdot$	2	$A \leftrightarrow B$	$\cdot$	$\cdot$	$\circ$	2,2
6	$\cdot$	2	$A \leftrightarrow B$	$\cdot$	$\cdot$	$\circ$	2,2
7	$\cdot$	2	$A \leftrightarrow B$	$\cdot$	$\cdot$	$\circ$	3,3
8	$\cdot$	2	$A \leftrightarrow B$	$\cdot$	$\cdot$	$\circ$	3,3
9	$\cdot$	2	$A \leftrightarrow B$	$\cdot$	$\cdot$	$\circ$	2.5,2.5
10	$\cdot$	2	$A \leftrightarrow B$	$\cdot$	$\cdot$	$\circ$	3,3
11	$\circ$	3	$A \leftrightarrow B$	$A \leftrightarrow B$	A, B	$\circ$	3,3
12	$\cdot$	3	$A \leftrightarrow B$	$A \leftrightarrow B$	A, B	$\circ$	3,3

All the key establishment protocols using symmetric techniques offer at least implicit key authentication, because only parties knowing a specific secret key can recover the correct key. Key confirmation and entity authentication can be achieved for every protocol by using the some techniques[15]. Distinguishing identifiers included in messages are used to protect against certain type of substitution attacks.

6 Concluding Remarks

We have surveyed and classified many key establishment protocols proposed so far in accordance with cryptographic techniques, models of environment used, and the number of pass. And then the major properties of the protocols has been compared. Most important properties of key establishment protocols depend on the structure of the messages exchanged, not on the underlying cryptographic algorithms. Therefore, for reducing errors in key establishment protocol, the prudent design of protocol messages is rather of consequence. One of the important tasks of key establishment protocol is to devise protocols providing formally provable security[2, 3].

References

[1] R. Ankney, D. Hohnson and M. Matyas, “The Unified Model”, contribution to X9F1, October 1995.

[2] M. Bellare and P. Rogaway, “Entity Authentication and Key Distributions”, Advances in Cryptology-Crypto ’93, LNCS 773, pp.232-249, 1994.

[3] S. Blake-Wilson, C. Johnson and A. Menezes, “Key Agreement Protocols and their Security Analysis”, Proceedings of the sixth IMA International Conference on Cryptography and Coding, LNCS 1355, pp.30-45, 1997.

[4] S. Blake-Wilson and A. Menezes, “Authenticated Diffie-Hellman Key Agreement Protocols”, Proceedings of the 5th Annual Workshop on Selected Areas in Cryptography (SAC ’98), LNCS 1556, pp.339-361, 1999.

[5] S. Blake-Wilson and A. Menezes, "Unknown Key-Share Attacks on the Station-To-Station (STS) Protocol", Technical report CORR 98-42, University of Waterloo, 1998.

[6] W. Diffie and M. E. Hellman, "New Directions in Cryptography", IEEE Transaction on Information Theory, 22, pp.644-654, 1976.

[7] W. Fumy, "Key Management Techniques", COSIC'97 Course, LNCS 1528, pp.142-162, 1998.

[8] L. Law, A. Menezes, M. Qu, J. Solinas and S. Vanstone, "An Efficient Protocol for Authenticated Key Agreement Protocol ", Technical report CORR 98-5, University of Waterloo, Canada, March 1998.

[9] C. Lee, J. Lim, and J. Kim, "An Efficient and Secure Key Agreement", IEEE p1363a draft.

[10] T. Matsumoto, Y. Takashima and H. Imai, "On Seeking Smart Public-Key Distribution Systems", Transaction of the IECE of Japan, E69, pp.99-106, 1986.

[11] A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[12] B. Song and K. Kim, "Two-Pass Authenticated Key Agreement Protocol with Key Confirmation", Accepted to Indocrypt 2000, Calcutta, India, December, 2000.

[13] National Security Agency, "SKIPJACK and KEA Algorithm Specification", Version 2.0, May 29, 1998.

[14] ISO/IEC 11770-1, *Information Technology - Security Techniques - Key Management - Part 1: Key Management Framework*, draft, 1996.

[15] ISO/IEC 11770-2, *Information Technology - Security Techniques - Key Management - Part 2: Mechanisms Using Symmetric Techniques*, draft, 1996.

[16] ISO/IEC 11770-3, *Information Technology - Security Techniques - Key Management - Part 3: Mechanisms Using Asymmetric Techniques*, draft, 1996.