Malaysian Journal of Mathematical Sciences

Journal homepage: https://einspem.upm.edu.my/journal

A Chronological Review of Key Establishment Models and Protocols

Yap, E. Y. Y.*[1], Chin, J. J.[2,3], and Goh, A.[3]

[1]*Faculty of Engineering, Multimedia University, Malaysia*
[2]*Faculty of Computing and Informatics, Multimedia University, Malaysia*
[3]*Information Security Lab, MIMOS Berhad, Malaysia*

E-mail: ernestyyy0306@gmail.com
**Corresponding author*

Received: 15 June 2021
Accepted: 8 October 2021

Abstract

This work is a review on existing authenticated key exchange (AKE) security models and protocols mainly based on Diffie-Hellman Key Exchange (DHKE). We provide a discussion on the various security models of AKEs, such as the Bellare Rogaway (BR) model, Canetti Krawczyk (CK) model and their variants. Then we provide a review covering over ninety protocols in chronological order. The security models' security features and protocol examples that fit in those security models are exhibited.

Keywords: security models; Bellare-Rogaway; Canetti-Krawczyk; authenticated key exchange; protocols; review.

1 Introduction

The Diffie-Hellman Key Exchange (DHKE) [30] was published in 1976 and it revolutionized asymmetric encryption. However, the DHKE protocol has a vulnerability that enables an adversary to perform a Man-In-The-Middle (MITM) attack on it, hence improvements were made to the DHKE over the years. Even though the improved DHKE could prevent MITM attacks, but more attacks are discovered throughout the years. Security models are getting stronger giving adversaries more capabilities, causing those protocols to be not as secure as the initial intentions of their proposals.

In this modern age, known key attacks such as Key Compromise Impersonation (KCI) and Unknown Key Share (UKS) attacks are common because pieces of information leaks that are uncontrollable every day. One key feature of an authenticated key exchange (AKE) protocol is that the adversary cannot differentiate between the session key and a random key as shown in Bellare-Rogaway(BR) and Canetti-Krawcyzk(CK) security models. This feature prevents the adversary from utilizing a compromised key to break the protocol.

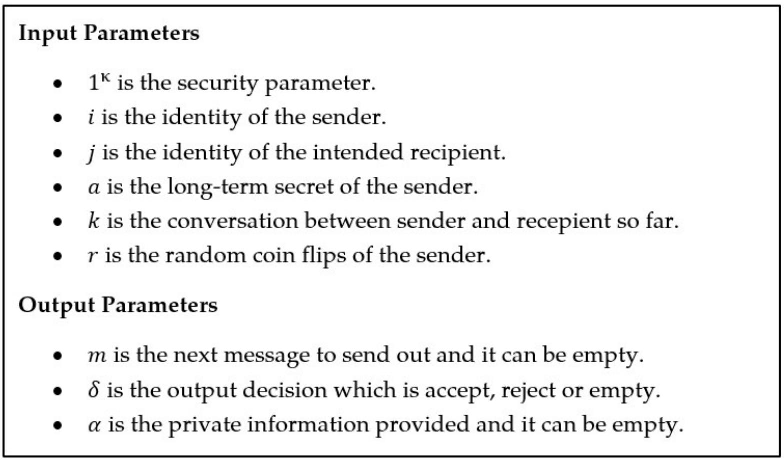
A common practice to fix a cryptographic scheme is to fix it when a problem is detected. This is known as the heuristic technique. However, this technique is undesirable because it is always too late when a vulnerability is detected. After the protocol is fixed and reapplied, another vulnerability may be discovered again, and the cycle continues. Starting from the 1980s, security models were defined to show what conditions must be fulfilled and what an adversary can do.

2 Security Models

2.1 Bellare-Rogaway Model (BR93)

Bellare and Rogaway [8] is the pioneer in AKE security modeling with computational cryptographic models. In contrast against the Dolev-Yao approach which takes a symbolic approach in modeling cryptographic attacks, the Bellare-Rogaway Model focuses on the computational cryptographic attack model. They provided provable security for entity authentication and associated problems of key distribution.

A communication model must be defined first in a security model. This model is appropriate in defining authentication and key distribution goals in a distributed environment. Function Π is a protocol that states the output of a specific principal when specific input is passed into it. In the BR93 model, six parameters are input into function Π and it outputs three parameters such that $(\Pi(1^k, i, j, a, \kappa, r) = (m, \delta, \alpha))$. Figure 1 shows the meaning of each parameter of those inputs and outputs.



Input Parameters

- 1^{κ} is the security parameter.
- i is the identity of the sender.
- j is the identity of the intended recipient.
- a is the long-term secret of the sender.
- k is the conversation between sender and recepient so far.
- r is the random coin flips of the sender.

Output Parameters

- m is the next message to send out and it can be empty.
- δ is the output decision which is accept, reject or empty.
- α is the private information provided and it can be empty.

Figure 1: Inputs and outputs in the BR93 protocol.

Besides that, the communication model also defines that the adversary entirely controls the principal's communication. The adversary can intercept messages and send them in any order, also to unintended recipients. The adversary can also modify and create massages freely. He can conduct as many sessions as intended with all the principals involved, and also controls the authentication process.

In every computational model, it is vital to identify who the messages are from, and this is commonly known as entity authentication. Bellare and Rogaway defined entity authentication using matching conversations and mutual authentication. Matching conversations are used to define partners. This is done by checking the message that is sent and giving confirmation to their respective partners. The problem with this is that the partner that sent the last message cannot know whether his message was ever received. Hence, a much more flexible rule is given to the party sending the last message.

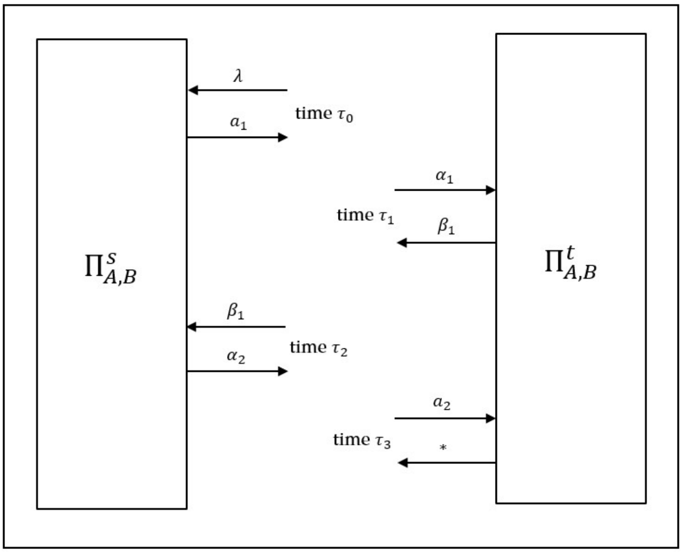


Figure 2: Matching conversation in BR93.

A conversation, (K) can be defined as $K = (\tau_1, x_1, y_1), (\tau_2, x_2, y_2), \ldots, (\tau_m, x_m, y_m))$ where (τ) is time, (x) is the received message and (y) is the respond message. Suppose Oracle $(\Pi^s_{i,j})$ models that principal (i) is attempting to authenticate (j) in a session (s) using conversation (K). If $(\alpha = \lambda)$ which means its empty in the first conversation then the Oracle is the initiator; if $(\alpha \neq \lambda)$ in the first conversation then the Oracle is the responder. Figure 2 helps to understand the definition of matching conversation easier; K is a matching conversation to (K') in a conversation as shown below and (a_p) is the last response in conversation (K).

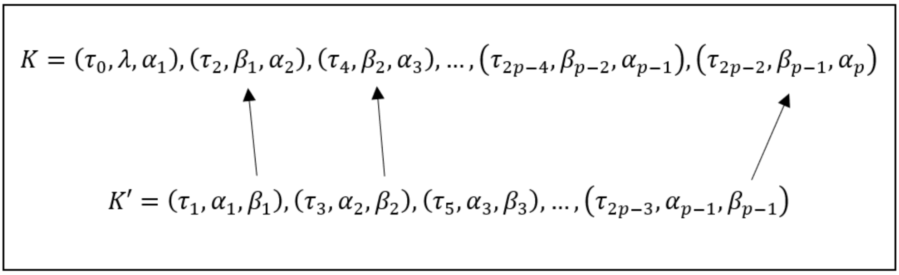

$K = (\tau_0, \lambda, \alpha_1), (\tau_2, \beta_1, \alpha_2), (\tau_4, \beta_2, \alpha_3), \ldots, (\tau_{2p-4}, \beta_{p-2}, \alpha_{p-1}), (\tau_{2p-2}, \beta_{p-1}, \alpha_p)$
$K' = (\tau_1, \alpha_1, \beta_1), (\tau_3, \alpha_2, \beta_2), (\tau_5, \alpha_3, \beta_3), \ldots, (\tau_{2p-3}, \alpha_{p-1}, \beta_{p-1})$

Figure 3: (K) matching conversation to (K').

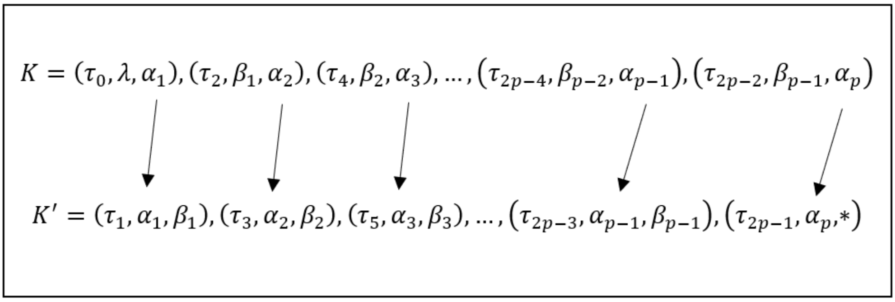

$K = (\tau_0, \lambda, \alpha_1), (\tau_2, \beta_1, \alpha_2), (\tau_4, \beta_2, \alpha_3), \ldots, (\tau_{2p-4}, \beta_{p-2}, \alpha_{p-1}), (\tau_{2p-2}, \beta_{p-1}, \alpha_p)$
$K' = (\tau_1, \alpha_1, \beta_1), (\tau_3, \alpha_2, \beta_2), (\tau_5, \alpha_3, \beta_3), \ldots, (\tau_{2p-3}, \alpha_{p-1}, \beta_{p-1}), (\tau_{2p-1}, \alpha_p, *)$

Figure 4: (K') matching conversation to (K).

To match a conversation, the received message must be the same as the corresponding principal's response message. The Oracle that has conversation (K) is the initiator oracle while (K') is the responder oracle. Hence, since the initiator oracle does not know whether the corresponding principle receives the last response, it will still accept it. Oppositely, the responder oracle can receive every response from the initiator oracle; hence it requires all responses from the initiator oracle to be accepted.

Another critical feature needed to fulfill entity authentication is mutual authentication meaning that each party should make sure that they know whom they are talking to. It is required that any mutual authentication protocol that satisfies this security model have at least three rounds of conversation between two parties.

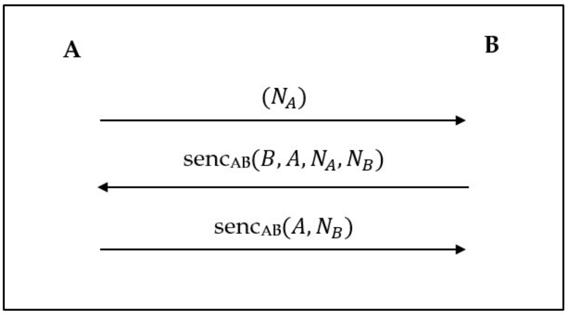
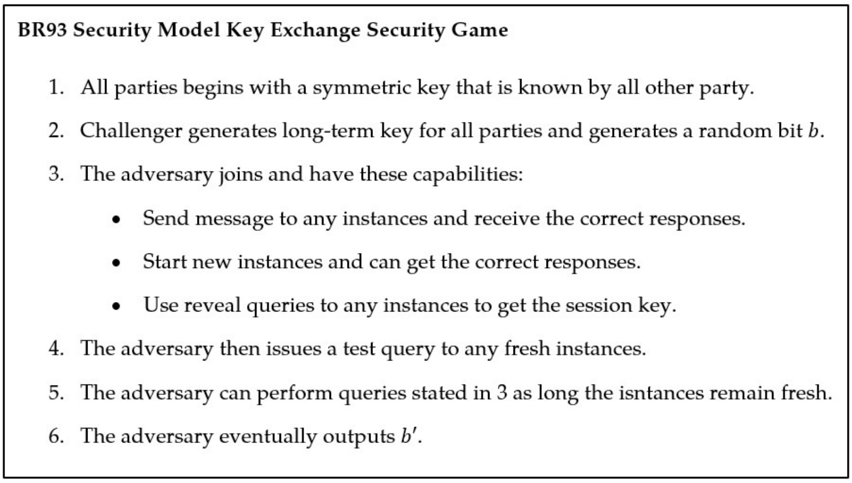

A
B
(N_A)
$\text{senc}_{\text{AB}}(B, A, N_A, N_B)$
$\text{senc}_{\text{AB}}(A, N_B)$

Figure 5: BR93 MAP1 protocol.

To satisfy the requirement mentioned above, each party needs to add their own identity inside the message to show whom the message is for. Bellare and Rogaway created the protocol shown in Figure 5, showing that it fulfills the requirement of the BR93 security model. Alice first sends a random nonce to choose by herself to Bob; Bob replies with asymmetric encryption using a key that was shared before containing both parties' identities, the nonce sent by Alice, and a random nonce selected by Bob. Finally, Alice replies with her own identity and Bob's nonce with encryption and finally accepts. Each party will check whether the message they receive fulfills the right form. A protocol is considered as a secure mutual authentication protocol in the security model if conversations of $(\Pi^s_{i,j})$ and $(\Pi^t_{i,j})$ match and they accept each other. On a side note, the probability of having one of the conversations in an accepted state without the other oracle existing is considered negligible.

Bellare and Rogaway had specified a formal definition for AKE and provided examples that met their security model's requirements. After successfully executing a key establishment protocol, the principals will obtain a session key in part of their output in (α) as shown before. One reason to use a session key is that every session that is built is independent of one another. The adversary is able to get a session key from a specific session, but it cannot compromise other sessions. Hence, the BR93 security model allows an adversary to get the session key from any instances it chooses. The adversary is able to perform a *reveal query* to output the session key by giving input of $((i, j, s))$. However, the adversary is only allowed to use a *reveal query* on instances that had outputted an accept.

To win the BR93 model's security game, the adversary does not need to show the values of the session key correctly. It only needs to differentiate between the session key from a random value of string with an equal length. This process is done when the adversary has decided executing a *test query* by giving the inputs $((i, j, s))$ specifying instances and the session it wishes to target. The *test query* can only be executed once throughout the whole security game, but it can be executed anytime. When the *test query* is issued, a challenger chooses a random bit like tossing a fair coin, to define bit b. That is, if $(b = 0)$ then the *test query* output the session key of the instances the adversary requested; else $(b = 1)$ then a random string with its length equals to that of the session key is outputted. The adversary's aim is to provide a bit, b' to be compared to the value of the correct bit, b. If $(b' = b)$, the adversary wins the game.



BR93 Security Model Key Exchange Security Game

1. All parties begins with a symmetric key that is known by all other party.
2. Challenger generates long-term key for all parties and generates a random bit b.
3. The adversary joins and have these capabilities:
    - Send message to any instances and receive the correct responses.
    - Start new instances and can get the correct responses.
    - Use reveal queries to any instances to get the session key.
4. The adversary then issues a test query to any fresh instances.
5. The adversary can perform queries stated in 3 as long the isntances remain fresh.
6. The adversary eventually outputs b'.

Figure 6: BR93 security game ([14], p.63).

The adversary can request the session key of the targeted session using *reveal query* and win the game easily. Hence, freshness is introduced so that the adversary plays the security game fairly. The adversary is only allowed to use a *test query* on a fresh session, which means that the fresh session has never revealed its session keys to the adversary. According to the definition of freshness given in BR93, an instance is fresh if it has accepted; has not been inquired a *reveal query*; and a *reveal query* was not issued to other instances that have a matching conversation with the targeted instances.

A security game is an asymptotic experiment and it cannot be simulated. The challenger is responsible for selecting the long-term keys for both parties and the random bit b. Since the security game has only two possible answers, it is said that the adversary will win half of the time by merely guessing. If the adversary can obtain a probability of guessing the bit more than half of the time, the adversary can have an advantage. A protocol, Π is said to be a secure AKE protocol in the BR93 model if it fulfills the condition of a secure mutual authentication protocol. Besides that, the adversary's probability in beating the security game must be negligible.

Although the BR93 model idea is widely used today, it still has its limitations simply because it is not a very strong model in the present time. The cryptographic setting in BR93 is too simple because the challenger sets the long-term key for all parties. This setting is not valid for most distributed cryptography settings. Moreover, a public key is an essential key aspect that can help break a protocol, but it is not considered in this security model. Besides, the BR93 model focuses heavily on authentication and key exchange, but most of the protocols proposed during that time do not meet the requirements set by BR93.

Lastly, the adversary in this model is not strong as it has limited capabilities. For example, the adversary does not have any way to get the long-term key, meaning that it does not include dishonest insiders threat, which is practised commonly. These limitations are improved along the way as many AKE security models that use the BR93 model as a foundation to be built on.

2.2 Bellare-Pointcheval-Rogaway Model (BPR2000)

A new AKE security model was introduced in 2000 by Bellare et al., known as BPR2000 [7]. They did some modifications and improved the BR93 model introducing new security properties known as forward secrecy. The primary enhancement is the security game of BR93 introducing new queries and increasing the adversary capabilities, including analysis of password-based protocols.

The BR93 security model was initially created for non-password-based AKE. This is because the security game provided by BR93 demands the adversary to differentiate between a real session key and a random string with the same length, giving a non-negligible adversary's advantage. A password-based protocol cannot possibly achieve this as most users have a low-entropy password giving the adversary advantage of always winning. Therefore, the security definition for password-based protocol must be relaxed by forcing the adversary to have a significantly higher probability of winning rather than merely correctly guessing the password.

An adversary can check whether a password is correct using a *send queries* any time. Hence, the number of *send query* must be limited, lowering the security guarantees of this model. To overcome this problem, the adversary is allowed to perform a considerable amount of passive eavesdropping action. This can be done using a new query called *execute query*. If an excellent password-based protocol is modeled after this, it can limit the amount of advantage an adversary can have by limiting the number of *send query*. A practical example of this is like locking a user out after a certain number of password keys in failed attempts.

As the BR93 model uses matching conversations, it is no longer used in the BPR2000 model as a new way of entity authentication is used. BPR2000 uses session identifiers, also known as SIDs, although its exact form is not specified in the paper, but it defines a session between two parties by concatenation of a protocol message. Besides that, this model had introduced partner identifiers, also known as PIDs, to specify the identity of the intended party to communicate with. Each partner must decide on a SID and PID when a session key is accepted. Users in a same session should have the similar SID and session key but different PID.

A new feature called forward secrecy was introduced in BPR2000, it redefined the definition of freshness from BR93. For a protocol to have forward secrecy, compromised long-term key does not give the adversary advantage in cracking the session key. For a protocol that needs to be modeled with forward secrecy, an instance is not fresh if a *corrupt query* is issued before the *test query*. This is because the session key can be easily cracked if the long-term key is leaked before the challenger chooses a random bit b. For a protocol that lack forward secrecy to be fit in BPR2000, every parties will be unfresh if a *corrupt query* is used on any party. If every party is unfresh, the *test query* can no longer be used, causing the security game to be no longer valid. Therefore, the *corrupt query* is modified. It can be used to check the state of the party, or getting the long-term key.

Table 1: BPR2000 security game query.

Queries	Uses
Send	Active attacks such as message modifying
Execute	Passive attacks such as eavesdropping
Reveal	Adversary can get session key and cause the instance not to be fresh
Corrupt	Adversary can get the state of the principal or get the long-term key
Test	Adversary begin the challenge by guessing the bit

2.3 Canetti-Krawczyk Model (CK2001)

In 2001, Canetti and Krawczyk [16] created a new security model for AKE using the foundations given in BR93, called CK2001. It specifically manipulates the interactions on all sides. In CK2001, sessions are now identified using a tuple (i, j, s), where (i) is the sender principal starting a session with responding principal, (j) with a session identifier, (s). The session identifier, (s) is different from the one used in BR93. The main difference between this security model compared to the BR variation is the security game queries.

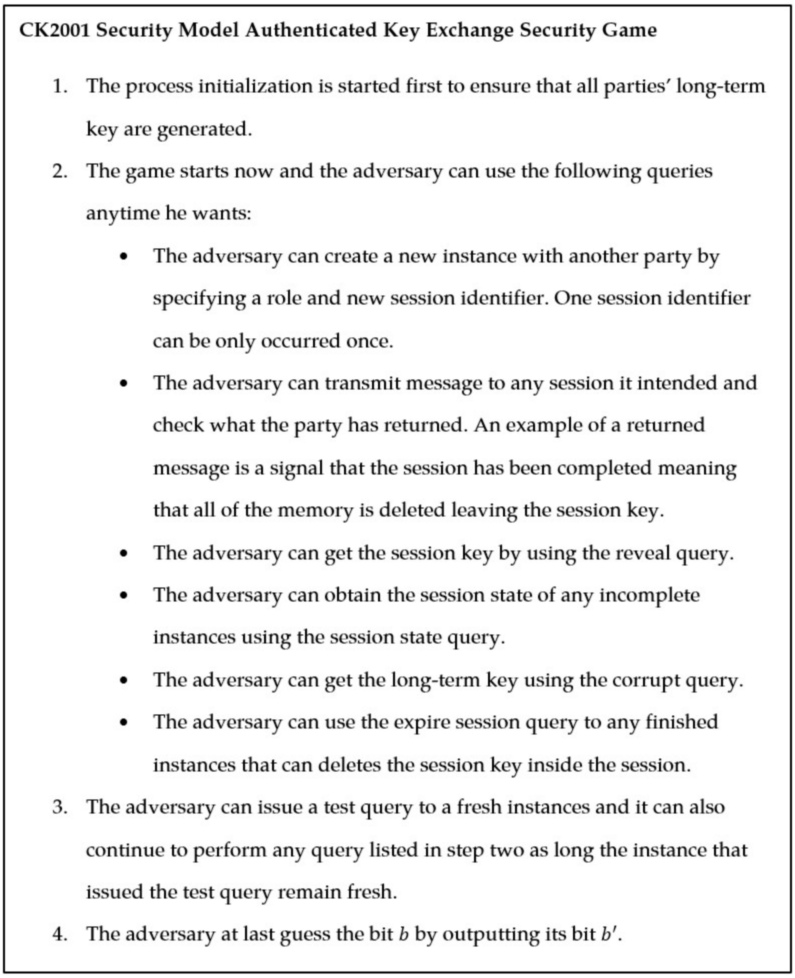
The CK2001 is a revamp of BR93 with the model's adversarial setting redesigned. Then the unauthenticated-links adversarial model, commonly known as UM, was introduced. In this setting, the adversary has control over the communications network entirely, meaning it can intercept and modify any message in the network. The adversary can also obtain any key, which imitates the leaking of information in the practical world.

Table 2: CK2001 security game query.

Queries	Uses
Party Corruption	Adversary obtain long-term key
Session Key Reveal	Adversary obtain session key
Session State Reveal	Adversary obtain internal state of an incomplete session
Session Expire	Delete session key

The goal of the security game is similar to the BR93 model, which is testing the probability of adversary being able to differentiate between the session key and a random string. In CK2001, an adversary can use a *party corruption query* to get the long-term key, that is similar to the BPR2000 model. A party that receives the corrupt query is like giving administrator's rights to the adversary. A corrupted party could potentially give away everything because the long-term key and memory left inside could have traces of a used key.

The second query is the *session key reveal query*. It is the same as the *reveal query* in BR93 model, that is providing session keys to the adversary. The BR93 model showed its limitation by not allowing the adversary to get information concerning the session state. Therefore, the CK2001 model created the session state reveal that allows the adversary to get the internal state of a session. The last query is the *session expire query* which is mainly used to model forward secrecy. This query prompts the party to erase the session key from the session that is chosen by the adversary. This ensures that the adversary does not get the session key from an expired session using a *corrupt query*. All of the queries and the security game is shown Figure 7.



CK2001 Security Model Authenticated Key Exchange Security Game

1. The process initialization is started first to ensure that all parties' long-term key are generated.
2. The game starts now and the adversary can use the following queries anytime he wants:
   - The adversary can create a new instance with another party by specifying a role and new session identifier. One session identifier can be only occurred once.
   - The adversary can transmit message to any session it intended and check what the party has returned. An example of a returned message is a signal that the session has been completed meaning that all of the memory is deleted leaving the session key.
   - The adversary can get the session key by using the reveal query.
   - The adversary can obtain the session state of any incomplete instances using the session state query.
   - The adversary can get the long-term key using the corrupt query.
   - The adversary can use the expire session query to any finished instances that can deletes the session key inside the session.
3. The adversary can issue a test query to a fresh instances and it can also continue to perform any query listed in step two as long the instance that issued the test query remain fresh.
4. The adversary at last guess the bit b by outputting its bit b'.

Figure 7: CK2001 security game ([14], p.72).

The definition of entity authentication in CK2001 was changed. It uses the session identifiers as partnering between two parties. To be specific, the input sent by one party to another is denoted as (i, j, s, r). As stated before, (i) is the party sending the message and (j) is the intended party that receives the message; (s) is the session identifier, and it cannot be repeated in a different session, and finally, (r) is the role which is either the initiator or the responder.

The definition of freshness in an instance must also be redefined because some new queries were added to the model. It is said that an instance remains fresh if a *session state query* or a *reveal query* had not been used on it before. A instance that experienced an *expired session query* will remain fresh even a *corrupt query* is performed on it. The matching partners in any instance will remain fresh if all those terms is met. If a protocol lacks forward secrecy, the *corrupt query* will cause any instances not to be fresh. The *corrupt query* cannot be used on the test session or its matching partner.

Since this is a slightly new and different form of the AKE security model, the CK model also redefined security by stating that a protocol has secure authentication if two uncompromised parties had finished matching partners, and both of them accepted with a similar session key. The other condition is the adversary must has a negligible probability of correctly differentiate between the session key and a random string provided by the challenger.

Besides that, CK2001 also has a model that can help analyze protocols that allowed the adversary to act as a wire and only relay messages in the communication network. This kind of attack is commonly known as a passive attack. The adversarial model is called the authenticated-links model, also known as AM. In CK2001, it is said that a protocol that is proven secure in the AM model can be also be proven to be secure in the UM model after incorporating a unique algorithm called authenticators.

Although CK2001 fixed most of the limitations posed by BR93, it still has its flaws. First, the methods to obtain the session identifiers are still unclear. Second, it is unclear that what is outputted when the adversary gets the session state of an instance. Third, most AKE protocols nowadays uses an ephemeral key to help create a session key. However, the test session is not considered fresh after its ephemeral keys are obtained by the adversary. This issue cannot be modeled in CK2001.

2.4 Extended Canetti-Krawczyk Model (eCK)

In 2005, the CK and BR security models were among the famous models used for proving AKE security. Since then, researchers have found ways to improve it furthermore by providing a more robust security model. This security model, proposed in 2007, is known as the extended Canetti-Krawczyk Model or eCK model [66].

The eCK is relatively straightforward as it solves the main limitation shown in CK2001, by letting the adversary to get hold of the ephemeral key. Besides that, the adversary can also get the long-term key of the test session even before using the *test query*, meaning that using the *corrupt query* to get the long-term key no longer affects the freshness of an instance.

The eCK model allows an adversary to get the ephemeral key, because of the hypothesis that the possession of ephemeral key and the partner's long-term key does not affect the probability of winning. Nevertheless, the adversary cannot have both the long-term key and ephemeral key of a test session. It can only allow getting either the ephemeral key or the long-term key.

Table 3: eCK security game query.

Queries	**Uses**
Send	Adversary can perform active attacks
Reveal	Adversary can obtain session key
Ephemeral	Adversary can obtain ephemeral key
Longterm	Adversary can obtain long-term key
Test	Adversary begin the challenge by guessing the bit b

Since this is a variation from CK2001, partner matching is similar using session identifiers but with a small difference. Alice and Bob message is considered a match if Alice outputs the message tuple (r, A, B, out, in) and Bob replies with (r', B, A, in, out) where (r) is not equal to (r').

A new *ephemeral query* is added causing the freshness of an instance to be redefined. A session is still fresh if it had not been issued a *reveal query*. If a session has matching partners, then the session is still considered fresh if the adversary had not obtained both the ephemeral key and long-term key of one of the partners. If a party has no partner, it is still considered fresh if the adversary had not taken its long-term key.

There is a technique for a protocol to fit in the eCK model: the NAXOS trick [66], as suggested by the creators of eCK. The protocol is shown in Figure 8 below.

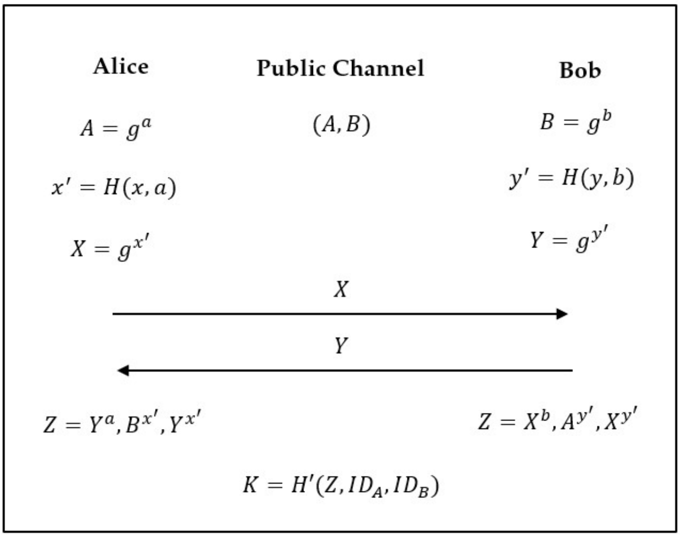


Figure 8: NAXOS protocol.

(A) and (B) are the public long-term key of Alice and Bob, while (a) and (b) are the private long-term key of Alice Bob. Alice and Bob each create their ephemeral key that is (x) and (y) and then hash it together with their private long-term key; this is known as the NAXOS trick. Since the adversary cannot get the ephemeral key and private long-term key of Alice and Bob if they are in the test session, the adversary cannot compute $H(x, a)$ or $H(y, b)$. The protocol continues by letting each party sending their ephemeral public key to each other and then compute (Z), that is the shared secret. The shared secret is proof to be equal as it is equal to $Z = g^{(H(y,b))a}, g^{b(H(x,a))}, g^{((H(y,b))(H(x,a)))}$ for both parties. Both parties conclude by hashing the shared secret together with their identity to obtain the session key.

2.5 Canetti-Krawcyzk Plus Model (CK+)

Although the eCK model introduced a new query to allow an adversary to capture the party's ephemeral key, it took away the query that allows the adversary to get the session state of a session. Hence, the CK+ model [40] was proposed for the purpose of allowing the adversary to get the session state. The CK+ model shares many commonalities with the eCK model, with only a few changes to adversarial queries in the security game.

Table 4: CK+ security game query.

Queries	Uses
Send	Used by adversary to get response from party
SessionStateReveal	Used by adversary to get the session state
SessionKeyReveal	Used by adversary to get the session key from a party
Corrupt	Used by adversary to obtain all information
Test	Used by adversary to guess the bit b

In CK+ model, the message relays between parties have one of these forms: (Π, I, j, i), $(\Pi, R, j, i, input)$ and $(\Pi, I, i, j, Output, Input)$. (Π) is the protocol that is used; (I) and (R) stands for the initiator and the responder; (i) and (j) is the identity of the party. One of these messages can be used by the adversary to use the *send query* to any party. The adversary can only get a session key from a complete session and get a session state from an incomplete session. The adversary's captured session state contains information such as the ephemeral keys but not the long-term key. Finally, the *corrupt query* can let the adversary get all information from a party but then will cause the party to be not fresh also dishonest.

For eCK model, the definition for freshness in this model is almost identical to the CK+ model. If a party had sent a *SessionKeyReveal query* or a *SessionStateReveal query*, then the party is considered not fresh. This is also true if the party's matching session had also been sent a *SessionKeyReveal query* or a *SessionStateReveal query*.

2.6 Comparison Between Security Models

Choo completed a study [26] in analyzing the models described above and comparing them. The main feature to be compared is the security model's strength in terms of adversarial capabilities and security. It can be seen that the Bellare and Rogaway model mainly focuses on mutual authentication, but the Canetti and Krawczyk model mainly focuses on a key exchange using implicit authentication.

The main difference between all the security models mentioned above is partner matching, adversarial capabilities, and definition of freshness. BR93 uses matching conversations; BPR2000 uses session identifiers; CK2001 also uses session identifiers with role added; eCK uses roles, identity, and input-output messages; and CK+ uses a protocol, roles, identity, and input-output messages. It is said in [26] that protocols that are proven secure in BR93 can be modified to be insecure in the CK2001 model with the addition of random parameters that each party can neglect. He showed that a protocol that is secure in one model does not mean it is secure in the others, although all of the models are designed from the same fundamental practice.

Overall, [26] stated that the CK2001 model is more robust than BR93 and BPR2000; while BR93 is still stronger than BPR2000 although BPR2000 had overcome the weaknesses in BR93. The critical aspect that helps CK2001 be more advantageous against both BR models is introducing the *session state query*; BPR2000 is seen as weaker than BR93 because of an ill representation of its *corrupt query* despite having forward secrecy.

Cremers [29] conducted a similar research comparing among the CK models. He stated that a protocol that fits in one of the CK models may not fit in the other models, similar to what Choo had proposed. Since the adversary cannot perform the *session state query* on the test session, it is said that CK2001 is less reliable as compared to the eCK or CK+ model in this respect. However, the eCK model cannot model complete forward secrecy but only weak forward secrecy because it does not control the adversary *corrupt query* usage in relation of the *test query* timing, causing eCK to seem weaker than CK2001.

To compare the eCK and CK+ models, the main difference is the adversary can get the session state of a party for the CK+ model. The eCK model allows an adversary to get the ephemeral keys and long-term keys whenever it needs, but the CK+ model controls how the adversary gets the ephemeral keys. To summarize all of this, Figure 9 is created to help determine the models' strengths, ranging from the weakest security model in the bottom to the strongest security model on top.

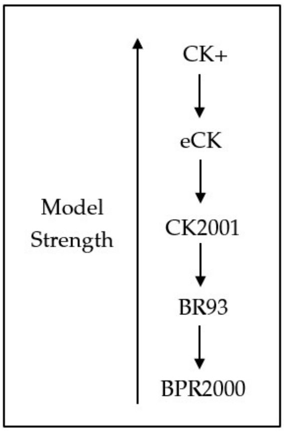


Figure 9: Model strength.

3 Protocols

Table 5 below will show all the reviewed protocols sorted by year of publication beginning from 1978 till 2020, which is the year this work was completed; Several types of protocols will be included, such as Key Transport Protocol (KTP), AKE, and Identity-Based Authenticated Key Agreement (IBAKA); The attacks will be categorized as man-in-the-middel (MITM), reflection attack, key compromise impersonation (KCI), and unknown key share (UKS) attacks. All reviewed protocols are two-parties asymmetric protocols that exist since DHKE. Note that password-based protocols are not included.

Table 6 and Table 7 show that most reviewed protocols are AKE and IBAKA, while the most frequently found attacks are the UKS and KCI attacks. This shows that most protocols are vulnerable to these attacks, and cryptographers should take notice to prevent them. An in-depth analysis can be performed by classifying AKE and IBAKA protocols in UKS and KCI attacks. Since the IBAKA protocol is more secure than the AKE protocol, it shows less successful attacks, as depicted in Figure 10.

Table 5: List of reviewed protocols sorted by year.

No.	Protocols	Year
1	Needham-Schroeder [82]	1978
2	Okamoto [85]	1987
3	Günther [44]	1989
4	Girault [43]	1991
5	STS [31]	1992
6	MSR [9]	1993
7	Beller-Yacobi [10]	1993
8	Arazi [2]	1993
9	Carlsen MSR-DH [17]	1994
10	Lim-Lee [71]	1995
11	SKEME [63]	1996
12	Lowe Needham [72]	1996
13	Just-Vaudenay-Song-Kim [60]	1996
14	MQV [78]	1997
15	Blake-Wilson & Menezes [110]	1997
16	KEA [83]	1998
17	Hirose-Yoshida [51]	1998
18	Oakley [86]	1998
19	IKE [46]	1998
20	Ateniese-Steiner-Tsudik [3]	2000
21	Saeednia Günther [92]	2000
22	Harn-Lin [48]	2001
23	Wong-Chan [111]	2001
24	Yuhmin-Tseng [105]	2002
25	Smart [98]	2002
26	SIG-DHM [104]	2003
27	Shim's [96]	2003
28	SIGMA [64]	2003
29	Chen-Kudla [18]	2003
30	JFK [1]	2004
31	Popescu [88]	2004
32	Jan-Chen [57]	2004
33	Jeong-Katz-Lee [58]	2004
34	Ryu-Yoon-Yoo [91]	2004
35	Boyd-Mao-Paterson [13]	2004
36	Yoon [120]	2005
37	Harn-Hsin-Mehta [47]	2005
38	Choie-Jeong-Lee [24]	2005
39	Lee-Choi-Min [70]	2005
40	Tseng [106]	2005
41	HMQV [65]	2005
42	McCullagh-Barreto [77]	2005
43	Choi et al. [23]	2005
44	Lu-Cao-Zhu [73]	2007
45	Cheng-Chen [22]	2007
46	Naxos [66]	2007
47	Chow-Choo [28]	2007
48	CMQV [107]	2008
49	NETS [68]	2008
50	Tian et al. [103]	2008
51	Pan-Li-Zheng [87]	2008
52	Luo-Wen-Zhao [76]	2008
53	Elkamchouchi-Eldefrawy [34]	2008
54	Schridde et al. [94]	2008
55	Hölbl-Welzer [52]	2009
56	Juang-Wu [59]	2009
57	SMEN [112]	2009
58	Hu-Liu-Zhang [54]	2009
59	Chen-Zhang-Qin-Wu-Zhang [19]	2009
60	CK-T-AKA [42]	2009
61	Moriyama-Okamoto [80]	2009
62	Zhong-Ma [116]	2010
63	Li-Zhang [113]	2010
64	Sun-Wang [55]	2010
65	Yak [45]	2010
66	FG IB-KA [38]	2010
67	IKEv2 [62]	2010
68	Elkamchouchi-Saleh-Sary [35]	2011
69	OAKE [117]	2011
70	Yu-Zhang-He [121]	2011
71	Lee-Park [69]	2011
72	Hölbl-Welzer-Brumen [53]	2012
73	Zhang et al. [124]	2012
74	He et al. CLAKA [50]	2012
75	Vallent-Kim-Yoon-Kim [108]	2013
76	Nabil et al. [81]	2013
77	Wang [109]	2013
78	DIKE [118]	2013
79	FS-AKA [32]	2014
80	Basin-Needham-Schroeder-Lowe [6]	2014
81	Reddy-Satyanarayana [90]	2014
82	Bergsma-Jager-Schwenk [11]	2015
83	Elashry-Mu-Susilo [33]	2015
84	Fujioka [39]	2016
85	Taparia-Panigrahy-Jena [102]	2017
86	Unified Model [5]	2017
87	DH-MM-KE [79]	2017
88	SIDH-UM [41]	2018
89	Zhang-Huang-Wang-Yue [123]	2018
90	Qi-Chen [89]	2020
91	LR-AKE [122]	2020
92	LB-2PAKA [56]	2020

Table 6: Protocols, sorted by types.

Type	Protocols	Total
KTP	1, 6, 7, 9, 12, 15, 80	7
AKE	5, 8, 10, 11, 13, 14, 16, 17, 18, 19, 20, 22, 23, 24, 26, 28, 30, 31, 32, 33, 37, 39, 40, 41, 44, 46, 48, 49, 51, 52, 53, 56, 57, 59, 60, 61, 65, 67, 68, 69, 70, 71, 73, 76, 78, 79, 81, 82, 85, 86, 87, 88, 89, 90, 91, 92	56
IBAKA	2, 3, 4, 21, 25, 27, 29, 34, 35, 36, 38, 42, 43, 45, 47, 50, 54, 55, 58, 62, 63, 64, 66, 72, 74, 75, 77, 83, 84	29

Table 7: Protocols, sorted by attacks.

Attacks	Protocols	Total
MITM	1 [72], 7 [14], 8[15], 27 [101], 32 [95] , 55 [125], 60 [115], 83 [49]	8
Reflection	3 [37], 19 [36], 31 [119], 39 [25]	4
UKS	6 [17], 14 [61], 16 [67], 17 [4], 22 [97], 72 [84]	6
KCI	12 [6], 13 [99], 20 [14], 23 [25], 31 [100][119], 32 [27], 33 [14], 34 [12], 35 [14], 41 [93], 42 [114], 52 [75], 53 [20], 57 [74], 78 [14], 86 [14], 89 [21]	17

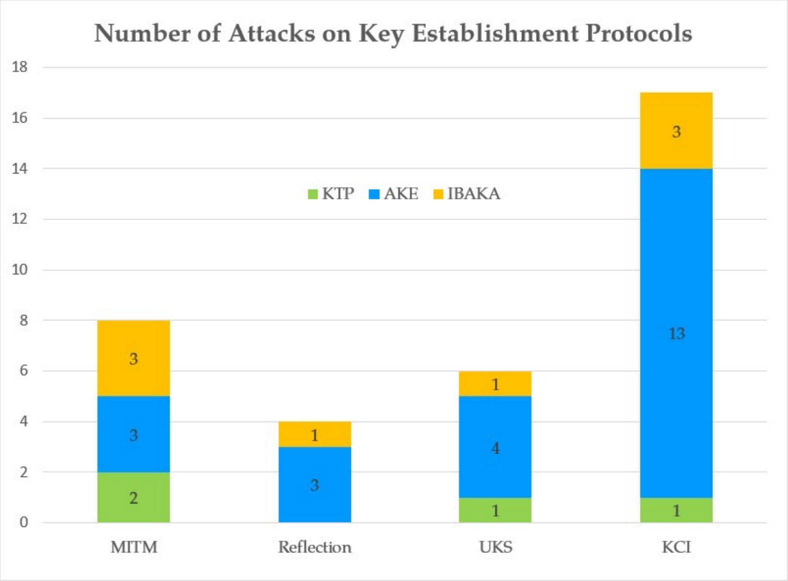


Figure 10: Number of attacks on key establishment protocols.

4 Conclusion

In this review, the Bellare-Rogaway Model, the Canetti-Krawczyk Model and various extensions were described in detail. A few protocol examples were given to show what conditions must be fulfilled for a protocol to fit in the security model. The CK+ model has the strongest security properties while the BPR2000 has the least because the proposal does not provide a clear description of the model.

As for the key establishment protocols, most reviewed protocols were AKE and it is found that most of the AKE protocols are vulnerable to KCI attacks. Although IBAKA protocols are an improvement of AKE protocols, some of them are still unprotected from KCI and MITM attacks. For a protocol to be secure, it is recommended to define its security model initially before designing it to prevent known key attacks such as KCI and UKS.

Acknowledgement The authors wish to thank the Ministry of Education of Malaysia and TM R&D for supporting this work with the Fundamental Research Grant Scheme (FRGS/1/2019/ICT04/MMU/02/5) and the TM R&D Fund. The second author wishes to thank Information Security Labs at MIMOS Berhad for hosting his research visit, during which this work was completed.

Conflicts of Interest The authors declare no conflict of interest.

References

[1] W. Aiello, S. M. Bellovin, M. Blaze, R. Canetti, J. Ioannidis, A. D. Keromytis & O. Reingold (2004). Just fast keying: Key agreement in a hostile internet. *ACM Transactions on Information and System Security (TISSEC)*, *7*(2), 242–273.

[2] B. Arazi (1993). Integrating a key distribution procedure into the digital signature standard. *Electronics Letters*, *29*(11), 966–967.

[3] G. Ateniese, M. Steiner & G. Tsudik (2000). New multiparty authentication services and key agreement protocols. *IEEE journal on selected areas in communications*, *18*(4), 628–639.

[4] J. Baek & K. Kim (2000). Remarks on the unknown key share attacks. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, *83*(12), 2766–2769.

[5] E. Barker, L. Chen, S. Keller, A. Roginsky, A. Vassilev & R. Davis. Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography. Technical report National Institute of Standards and Technology 2017.

[6] D. Basin, C. Cremers & M. Horvat (2014). Actor key compromise: Consequences and countermeasures. In *2014 IEEE 27th Computer Security Foundations Symposium*, pp. 244–258. IEEE, Vienna, Austria.

[7] M. Bellare, D. Pointcheval & P. Rogaway (2000). Authenticated key exchange secure against dictionary attacks. In *International conference on the theory and applications of cryptographic techniques*, pp. 139–155. Springer, Berlin, Heidelberg.

[8] M. Bellare & P. Rogaway (1993). Entity authentication and key distribution. In *Annual international cryptology conference*, pp. 232–249. Springer, Berlin, Heidelberg.

[9] M. J. Beller, L. F. Chang & Y. Yacobi (1993). Privacy and authentication on a portable communications system. *IEEE Journal on Selected Areas in Communications*, *11*(6), 821–829.

[10] M. J. Beller & Y. Yacobi (1993). Fully-fledged two-way public key authentication and key agreement for low-cost terminals. *Electronics Letters*, *29*(11), 999–1001.

[11] F. Bergsma, T. Jager & J. Schwenk (2015). One-round key exchange with strong security: An efficient and generic construction in the standard model. In *IACR International Workshop on Public Key Cryptography*, pp. 477–494. Springer, Berlin, Heidelberg.

[12] C. Boyd & K. K. R. Choo (2005). Security of two-party identity-based key agreement. In *International conference on cryptology in Malaysia*, pp. 229–243. Springer, Berlin, Heidelberg.

[13] C. Boyd, W. Mao & K. G. Paterson (2004). Key agreement using statically keyed authenticators. In *International Conference on Applied Cryptography and Network Security*, pp. 248–262. Springer, Berlin, Heidelberg.

[14] C. Boyd, A. Mathuria & D. Stebila (2020). *Protocols for authentication and key establishment Second Edition*. Springer, Berlin, Heidelberg.

[15] D. Brown & A. Menezes (2001). A small subgroup attack on Arazi's key agreement protocol. *Bulletin of the ICA*, *37*, 45–50.

[16] R. Canetti & H. Krawczyk (2001). Analysis of key-exchange protocols and their use for building secure channels. In *International conference on the theory and applications of cryptographic techniques*, pp. 453–474. Springer, Berlin, Heidelberg.

[17] U. Carlsen (1994). Optimal privacy and authentication on a portable communications system. *ACM SIGOPS Operating Systems Review*, *28*(3), 16–23.

[18] L. Chen & C. Kudla (2003). Identity based authenticated key agreement protocols from pairings. In *16th IEEE Computer Security Foundations Workshop*, pp. 219–233. IEEE, Pacific Grove, CA.

[19] W. Chen, L. Zhang, B. Qin, Q. Wu & H. Zhang (2009). Certificateless one-way authenticated two-party key agreement protocol. In *2009 Fifth International Conference on Information Assurance and Security*, volume 1 pp. 483–486. IEEE, Xi'an, China.

[20] Q. Cheng, G. Han & C. Ma (2009). Analysis of two authenticated key exchange protocols. In *2009 International Conference on Multimedia Information Networking and Security*, volume 2 pp. 398–400. IEEE, Wuhan, China.

[21] Q. Cheng, Y. Li, Q. Jiang & X. Li (2020). Security analysis of two unbalancing pairing-free identity-based authenticated key exchange protocols. *International Journal of Network Security*, *22*(4), 597–601.

[22] Z. Cheng & L. Chen (2007). On security proof of McCullaghBarreto's key agreement protocol and its variants. *International Journal of Security and Networks*, *2*(3-4), 251–259.

[23] K. Y. Choi, J. Y. Hwang, D. H. Lee & I. S. Seo (2005). ID-based authenticated key agreement for low-power mobile devices. In *Australasian Conference on Information Security and Privacy*, pp. 494–505. Springer, Berlin, Heidelberg.

[24] Y. J. Choie, E. Jeong & E. Lee (2005). Efficient identity-based authenticated key agreement protocol from pairings. *Applied Mathematics and Computation*, *162*(1), 179–188.

[25] K. K. R. Choo (2006). *Key Establishment: Proofs and Refutations*. PhD thesis, Queensland University of Technology, Brisbane, Australia.

[26] K. K. R. Choo, C. Boyd & Y. Hitchcock (2005). Examining indistinguishability-based proof models for key establishment protocols. In *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 585–604. Springer, Berlin, Heidelberg.

[27] K. K. R. Choo, C. Boyd & Y. Hitchcock (2006). The importance of proofs of security for key establishment protocols: Formal analysis of Jan–Chen, Yang–Shen–Shieh, Kim–Huh–Hwang–Lee, Lin–Sun–Hwang, and Yeh–Sun protocols. *Computer Communications*, *29*(15), 2788–2797.

[28] S. S. Chow & K. K. R. Choo (2007). Strongly-secure identity-based key agreement and anonymous extension. In *International Conference on Information Security*, pp. 203–220. Springer, Berlin, Heidelberg.

[29] C. Cremers (2011). Examining indistinguishability-based security models for key exchange protocols: The case of CK, CK-HMQV, and eCK. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, pp. 80–91. ACM, Hong Kong.

[30] W. Diffie (1976). New direction in cryptography. *IEEE Transactions on Information Theory*, *22*, 472–492.

[31] W. Diffie, P. C. Van Oorschot & M. J. Wiener (1992). Authentication and authenticated key exchanges. *Designs, Codes and cryptography*, *2*(2), 107–125.

[32] E. El-Hamawi, B. Bakhache & R. Rostom (2014). An improved authenticated key agreement protocol for low power networks. In *MELECON 2014-2014 17th IEEE Mediterranean Electrotechnical Conference*, pp. 426–431. IEEE, Beirut, Lebanon.

[33] I. Elashry, Y. Mu & W. Susilo (2015). A resilient identity-based authenticated key exchange protocol. *Security and Communication Networks*, *8*(13), 2279–2290.

[34] H. Elkamchouchi & M. Eldefrawy (2008). An efficient and confirmed protocol for authenticated key agreement. In *2008 National Radio Science Conference*, pp. 1–8. IEEE, Tanta, Egypt.

[35] H. M. Elkamchouchi, Y. A. Saleh & A. M. Sary (2011). New authenticated key agreement protocols. In *The 2011 International Conference on Computer Engineering & Systems*, pp. 58–63. IEEE, Cairo, Egypt.

[36] N. Ferguson & B. Schneier (2000). A cryptographic evaluation of IPsec. Counterpane Internet Security, San Jose.

[37] D. Fiore & R. Gennaro (2010). Identity-based key exchange protocols without pairings. In *Transactions on computational science X*, pp. 42–77. Springer, Berlin, Heidelberg.

[38] D. Fiore & R. Gennaro (2010). Making the Diffie-Hellman protocol identity-based. In *Cryptographers' Track at the RSA Conference*, pp. 165–178. Springer, Berlin, Heidelberg.

[39] A. Fujioka (2016). One-round exposure-resilient identity-based authenticated key agreement with multiple private key generators. In *International Conference on Cryptology in Malaysia*, pp. 436–460. Springer, Cham.

[40] A. Fujioka, K. Suzuki, K. Xagawa & K. Yoneyama (2015). Strongly secure authenticated key exchange from factoring, codes, and lattices. *Designs, Codes and Cryptography*, *76*(3), 469–504.

[41] A. Fujioka, K. Takashima, S. Terada & K. Yoneyama (2018). Supersingular isogeny Diffie-Hellman authenticated key exchange. In *International Conference on Information Security and Cryptology*, pp. 177–195. Springer, Cham.

[42] M. Geng & F. Zhang (2009). Provably secure certificateless two-party authenticated key agreement protocol without pairing. In *2009 International Conference on Computational Intelligence and Security*, volume 2 pp. 208–212. IEEE, Beijing, China.

[43] M. Girault (1991). Self-certified public keys. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 490–497. Springer, Berlin, Heidelberg.

[44] C. G. Günther (1989). An identity-based key-exchange protocol. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 29–37. Springer, Berlin, Heidelberg.

[45] F. Hao (2010). On robust key agreement based on public key authentication. In *International Conference on Financial Cryptography and Data Security*, pp. 383–390. Springer, Berlin, Heidelberg.

[46] D. Harkins, D. Carrel et al. (1998). The internet key exchange (IKE). *RFC*, *2409*, 1–41.

[47] L. Harn, W. J. Hsin & M. Mehta (2005). Authenticated Diffie–Hellman key agreement protocol using a single cryptographic assumption. *IEE Proceedings-Communications*, *152*(4), 404–410.

[48] L. Harn & H.-Y. Lin (2001). Authenticated key agreement without using one-way hash functions. *Electronics Letters*, *37*(10), 629–630.

[49] Y. Hatri, A. Otmani & K. Guenda (2018). Cryptanalysis of an identity-based authenticated key exchange protocol. *International Journal of Communication Systems*, *31*(3), e3477. https://doi.org/10.1002/dac.3477.

[50] D. He, S. Padhye & J. Chen (2012). An efficient certificateless two-party authenticated key agreement protocol. *Computers & Mathematics with Applications*, *64*(6), 1914–1926.

[51] S. Hirose & S. Yoshida (1998). An authenticated Diffie-Hellman key agreement protocol secure against active attacks. In *International Workshop on Public Key Cryptography*, pp. 135–148. Springer, Berlin, Heidelberg.

[52] M. Hölbl & T. Welzer (2009). Two improved two-party identity-based authenticated key agreement protocols. *Computer Standards & Interfaces*, *31*(6), 1056–1060.

[53] M. Hölbl, T. Welzer & B. Brumen (2012). An improved two-party identity-based authenticated key agreement protocol using pairings. *Journal of Computer and System Sciences*, *78*(1), 142–150.

[54] X. Hu, W. Liu & J. Zhang (2009). An efficient ID-based authenticated key exchange protocol. In *2009 WASE International Conference on Information Engineering*, volume 2 pp. 229–233. IEEE, Taiyuan, China.

[55] S. Hua & W. Aimin (2010). An identity-based authenticated key agreement protocol for P2P. In *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, pp. V2–633. IEEE, Chengdu, China.

[56] S. H. Islam (2020). Provably secure two-party authenticated key agreement protocol for post-quantum environments. *Journal of Information Security and Applications*, *52*, 102468.

[57] J. K. Jan & Y. H. Chen (2004). A new efficient MAKEP for wireless communications. In *18th International Conference on Advanced Information Networking and Applications, AINA 2004*, pp. 347–350. IEEE, Fukuoka, Japan.

[58] I. R. Jeong, J. Katz & D. H. Lee (2004). One-round protocols for two-party authenticated key exchange. In *International conference on applied cryptography and network security*, pp. 220–232. Springer, Berlin, Heidelberg.

[59] W. S. Juang & J. L. Wu (2009). Two efficient two-factor authenticated key exchange protocols in public wireless lans. *Computers & Electrical Engineering*, *35*(1), 33–40.

[60] M. Just & S. Vaudenay (1996). Authenticated multi-party key agreement. In *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 36–49. Springer, Berlin, Heidelberg.

[61] B. S. Kaliski Jr (2001). An unknown key-share attack on the MQV key agreement protocol. *ACM Transactions on Information and System Security (TISSEC)*, *4*(3), 275–288.

[62] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen & T. Kivinen (2014). Internet key exchange protocol version 2 (IKEv2). *RFC*, *7296*, 1–142.

[63] H. Krawczyk (1996). SKEME: A versatile secure key exchange mechanism for internet. In *Proceedings of Internet Society Symposium on Network and Distributed Systems Security*, pp. 114–127. IEEE, San Diego, CA, USA.

[64] H. Krawczyk (2003). SIGMA: The 'SIGn-and-MAc' approach to authenticated Diffie-Hellman and its use in the IKE protocols. In *Annual International Cryptology Conference*, pp. 400–425. Springer, Berlin, Heidelberg.

[65] H. Krawczyk (2005). HMQV: A high-performance secure Diffie-Hellman protocol. In *Annual International Cryptology Conference*, pp. 546–566. Springer, Berlin, Heidelberg.

[66] B. LaMacchia, K. Lauter & A. Mityagin (2007). Stronger security of authenticated key exchange. In *International conference on provable security*, pp. 1–16. Springer, Berlin, Heidelberg.

[67] K. Lauter & A. Mityagin (2006). Security analysis of KEA authenticated key exchange protocol. In *International Workshop on Public Key Cryptography*, pp. 378–394. Springer, Berlin, Heidelberg.

[68] J. Lee & C. S. Park (2008). An efficient authenticated key exchange protocol with a tight security reduction. *IACR Cryptology ePrint Archieve*, *2008*, 345.

[69] J. Lee & J. H. Park (2011). Efficient and secure authenticated key exchange protocols in the eCK model. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, *94*(1), 129–138.

[70] Y. Lee, E. Choi & D. Min (2005). An authenticated key exchange mechanism using one-time shared key. In *International Conference on Computational Science and Its Applications*, pp. 187–194. Springer, Berlin, Heidelberg.

[71] C. H. Lim & P. J. Lee (1995). Several practical protocols for authentication and key exchange. *Information Processing Letters*, *53*(2), 91–96.

[72] G. Lowe (1996). Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In *International Workshop on Tools and Algorithms for the Construction and Analysis of Systems*, pp. 147–166. Springer, Berlin,Heidelberg.

[73] R. Lu, Z. Cao & H. Zhu (2007). An enhanced authenticated key agreement protocol for wireless mobile communication. *Computer Standards & Interfaces*, *29*(6), 647–652.

[74] S. Lu, J. Zhao & Q. Cheng (2016). Cryptanalysis and improvement of an efficient authenticated key exchange protocol with tight security reduction. *International Journal of Communication Systems*, *29*(3), 567–578.

[75] Y. Lu, Q. Zhang & J. Li (2019). A certificate-based AKA protocol secure against public key replacement attacks. *International Arab Journal of Information Technology*, *16*(4), 754–765.

[76] M. Luo, Y. Y. Wen & H. Zhao (2008). A certificate-based authenticated key agreement protocol for SIP-based VoIP networks. In *2008 IFIP International Conference on Network and Parallel Computing*, pp. 3–10. IEEE, Shanghai, China.

[77] N. McCullagh & P. S. Barreto (2005). A new two-party identity-based authenticated key agreement. In *Cryptographers' Track at the RSA Conference*, pp. 262–274. Springer, Berlin, Heidelberg.

[78] A. Menezes (1997). Some new key agreement protocols providing implicit authentication. In *Workshop on Selected Areas in Cryptography, SAC'97,*. CRC Press, Canada.

[79] N. H. Minh, N. N. Hai, J. Hur, D. H. Minh, H. S. Tan et al. (2017). Authenticated key exchange, signcryption and deniable signcryption protocols based on two hard problems. In *2017 International Conference on Advanced Computing and Applications (ACOMP)*, pp. 16–22. IEEE, Ho Chi Minh City, Vietnam.

[80] D. Moriyama & T. Okamoto (2009). An eCK-secure authenticated key exchange protocol without random oracles. *KSII Transactions on Internet and Information Systems*, *5*(3), 607–625.

[81] M. Nabil, Y. Abouelseoud, G. Elkobrosy & A. Abdelrazek (2013). Certificate-based authenticated key agreement protocols. In *2013 International Conference on Computer Applications Technology (ICCAT)*, pp. 1–7. IEEE, Sousse, Tunisia.

[82] R. M. Needham & M. D. Schroeder (1978). Using encryption for authentication in large networks of computers. *Communications of the ACM*, *21*(12), 993–999.

[83] NIST (1998). *SKIPJACK and KEA Algorithm Specification*. https://csrc.nist.gov/CSRC/media//Projects/Cryptographic-Algorithm-Validation-Program/documents/skipjack/skipjack.pdf.

[84] P. Nose (2014). Security weaknesses of a signature scheme and authenticated key agreement protocols. *Information Processing Letters*, *114*(3), 107–115.

[85] E. Okamoto & K. Tanaka (1989). Key distribution systems based on identification information. *IEEE Journal on Selected Areas in Communications*, *7*(4), 481 – 485.

[86] H. Orman et al. (1998). *The OAKLEY key determination protocol*. United State, US.

[87] H. Pan, J. F. Li & Q. S. Zheng (2008). A provable-security mutual authenticated key agreement protocol for mobile communication. In *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–4. IEEE, Dalian, China.

[88] C. Popescu (2004). A secure authenticated key agreement protocol. In *Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference (IEEE Cat. No. 04CH37521)*, volume 2 pp. 783–786. IEEE, Dubrovnik, Croatia.

[89] M. Qi & J. Chen (2020). An efficient one-way authenticated key exchange protocol for anonymity networks. *IEEE Systems Journal*, *15*(1), 377–382.

[90] Y. V. Reddy, G. Satyanarayana & M. V. Rao (2014). Authenticated Diffie-Hellman key exchange with forward secrecy.

[91] E. K. Ryu, E. J. Yoon & K. Y. Yoo (2004). An efficient ID-based authenticated key agreement protocol from pairings. In *International conference on research in networking*, pp. 1458–1463. Springer, Berlin, Heidelberg.

[92] S. Saeednia (2000). Improvement of Gunther's identity-based key exchange protocol. *Electronics Letters*, *36*(18), 1535–1536.

[93] A. P. Sarr & P. Elbaz Vincent (2016). On the security of the (F)HMQV protocol. In *International Conference on Cryptology in Africa*, pp. 207–224. Springer, Cham.

[94] C. Schridde, M. Smith & B. Freisleben (2008). An identity-based key agreement protocol for the network layer. In *International Conference on Security and Cryptography for Networks*, pp. 409–422. Springer, Berlin, Heidelberg.

[95] J. J. Shen, C. Y. Lin & H. W. Yang (2005). Cryptanalysis of a new efficient MAKEP for wirrenceeless communications. *IJ Network Security*, *1*(2), 118–121.

[96] K. Shim (2003). Efficient ID-based authenticated key agreement protocol based on Weil pairing. *Electronics Letters*, *39*(8), 653–654.

[97] K. Shim (2003). Unknown key-share attack on authenticated multiple-key agreement protocol. *Electronics Letters*, *39*(1), 38–39.

[98] N. P. Smart (2002). Identity-based authenticated key agreement protocol based on Weil pairing. *Electronics Letters*, *38*(13), 630–632.

[99] B. Song & K. Kim (2000). Two-pass authenticated key agreement protocol with key confirmation. In *International Conference on Cryptology in India*, pp. 237–249. Springer, Berlin, Heidelberg.

[100] M. A. Strangio (2006). On the resilience of key agreement protocols to key compromise impersonation. In *European Public Key Infrastructure Workshop*, pp. 233–247. Springer, Berlin, Heidelberg.

[101] H. M. Sun & B. T. Hsieh (2003). Security analysis of Shim's authenticated key agreement protocols from pairings. *IACR Cryptology ePrint Archive*, *2003*, 113.

[102] A. Taparia, S. K. Panigrahy & S. K. Jena (2017). Secure key exchange using enhanced Diffie-Hellman protocol based on string comparison. In *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 722–726. IEEE, Chennai, India.

[103] H. B. Tian, W. Susilo, Y. Ming & Y. M. Wang (2008). A provable secure ID-based explicit authenticated key agreement protocol without random oracles. *Journal of Computer Science and Technology*, *23*(5), 832–842.

[104] Y. S. T. Tin, C. Boyd & J. M. G. Nieto (2003). Provably secure mobile key exchange: Applying the Canetti-Krawczyk approach. In *Australasian Conference on Information Security and Privacy*, pp. 166–179. Springer, Berlin, Heidelberg.

[105] Y. M. Tseng (2002). Robust generalized MQV key agreement protocol without using one-way hash functions. *Computer Standards & Interfaces*, *24*(3), 241–246.

[106] Y. M. Tseng (2005). Efficient authenticated key agreement protocols resistant to a denial-of-service attack. *International Journal of Network Management*, *15*(3), 193–202.

[107] B. Ustaoglu (2008). Obtaining a secure and efficient key agreement protocol from (H) MQV and NAXOS. *Designs, Codes and Cryptography*, *46*(3), 329–342.

[108] T. F. Vallent, H. J. Kim, E. J. Yoon & H. Kim (2013). Improved two-party ID-based authenticated key agreement protocol. *The Journal of Korean Institute of Communications and Information Sciences*, *38*(7), 595–604.

[109] Y. Wang (2013). Efficient identity-based and authenticated key agreement protocol. In *Transactions on Computational Science Xvii*, pp. 172–197. Springer, Berlin, Heidelberg.

[110] S. B. Wilson & A. Menezes (1997). Entity authentication and authenticated key transport protocols employing asymmetric techniques. In *International Workshop on Security Protocols*, pp. 137–158. Springer, Berlin, Heidelberg.

[111] D. S. Wong & A. H. Chan (2001). Efficient and mutually authenticated key exchange for low power computing devices. In *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 272–289. Springer, Berlin, Heidelberg.

[112] J. Wu & B. Ustaoğlu (2009). Efficient key exchange with tight security reduction. *Cryptology ePrint Archive,Report 2009/288,*. http://eprint.iacr.org/2009/288.

[113] L. Xiaoyong & Z. Hui (2010). Identity-based authenticated key exchange protocols. In *2010 International Conference on Educational and Information Technology*, pp. V3–85. IEEE, Chongqing, China.

[114] G. Xie (2004). Cryptanalysis of Noel McCullagh and Paulo SLM Barreto's two-party identity-based key agreement. *IACR Cryptology ePrint Archieve*, *2004*, 308.

[115] G. Yang & C. H. Tan (2011). Strongly secure certificateless key exchange without pairing. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, pp. 71–79.

[116] Z. Yantao & M. Jianfeng (2010). A highly secure identity-based authenticated key-exchange protocol for satellite communication. *Journal of communications and networks*, *12*(6), 592–599.

[117] A. C. Yao & Y. Zhao. A new family of implicitly authenticated Diffie-Hellman protocols 2011.

[118] A. C.-C. Yao & Y. Zhao (2013). Privacy-preserving authenticated key-exchange over internet. *IEEE Transactions on Information Forensics and Security*, *9*(1), 125–140.

[119] E. J. Yoon & K. Y. Yoo (2006). An improved Popescu's authenticated key agreement protocol. In *International Conference on Computational Science and Its Applications*, pp. 276–283. Springer, Berlin, Heidelberg.

[120] S. B. Yoon (2005). An identity based authenticated key agreement protocol on the Tate pairing. *Communications-Korean Mathematical Society*, *20*(3), 611.

[121] YuXiu-Ying, ZhangWen-Fang & HeDa-Ke (2011). A new certificateless authenticated two-party key agreement. In *2011 IEEE International Conference on Computer Science and Automation Engineering*, volume 3 pp. 686–690.

[122] W. Zeng & J. Zhang (2020). Leakage-resilient and lightweight authenticated key exchange for e-health. In *2020 6th International Conference on Information Management* (*ICIM*), pp. 162–166. IEEE, London, UK.

[123] J. Zhang, X. Huang, W. Wang & Y. Yue (2018). Unbalancing pairing-free identity-based authenticated key exchange protocols for disaster scenarios. *IEEE Internet of Things Journal*, *6*(1), 878–890.

[124] M. Zhang, J. Zhang, Q.-Y. Wen, Z.-P. Jin & H. Zhang (2012). Analysis and improvement of a strongly secure certificateless key exchange protocol without pairing. In *2012 International Conference on Systems and Informatics* (*ICSAI2012*), pp. 1512–1516. IEEE, Antai, China.

[125] S. Zhang, Q. Cheng & X. Wang (2010). Impersonation attack on two identity-based authenticated key exchange protocols. In *2010 WASE International Conference on Information Engineering*, volume 2 pp. 113–116. IEEE, Beidai, China.