Formal Proof of Relative Strengths of Security between ECK2007 Model and other Proof Models for Key Agreement Protocols

Xia Jinyue*, Wang Jiandong, Fang Liming, Ren Yongjun, Bian Shizhu

(College of Information Science and Technology,
Nanjing University of Aeronautics and Astronautics, Nanjing 210016,P.R.China)
*corresponding author E-mail: xiajinyue@yahoo.com.cn

Abstract: In 2005, Choo, Boyd & Hitchcock compared four well-known indistinguishability-based proof models for key agreement protocols, which contains the Bellare & Rogaway (1993, 1995) model, the Bellare , Pointcheval & Rogaway 2000 model and the Canetti & Krawczyk (2001) model. After that, researchers from Microsoft presented a stronger security model, called Extended Canetti-Krawczyk model (2007). In this paper, we will point out the differences between the new proof model and the four previous models, and analyze the relative strengths of security of these models. To support the implication or non-implication relation between these models, we will provide proof or counter-example.

Key Words: cryptography, key agreement protocol, proof model

CLC number: TP309

1 Introduction

Choo, Boyd & Hitchcock[1] examined the Bellare-Rogaway models(i.e. Bellare & Rogaway (1993) model[2], Bellare & Rogaway (1995) model[3], Bellare , Pointcheval & Rogaway (2000) model[4]) and the Canetti & Krawczyk (2001) model[5]. They concluded that the Canetti & Krawczyk (2001) model, which will be referred to as the CK2001 model in this paper, has the strongest definition of security among those four models if the partnership is defined via matching conversation. Besides, the Bellare, Pointcheval & Rogaway (2000) model (which we refer to as the BPR2000 model in this paper) is the weakest model. Series of attacks, however, were not covered by these models. Krawczyk[6] presented the variant of CK2001 model that captures several security properties which includes resistance of key-compromise impersonation (KCI) attacks and weak perfect forward secrecy (wPFS). In addition, he adopted matching session to define the partnership. Recently, LaMacchia et al.

presented us a new model—Extended Canetti & Krawczyk (2007) model[7], hereafter we refer to as the ECK2007. The new model includes a large number of desirable security properties, and indicates that the only corruption ability they do not give an adversary in the experiment is that would trivially break a key agreement protocol. Conveniently, the Bellare & Rogaway (1993) model, Bellare & Rogaway (1995) model will be referred to as the BR93 model, the BR95 model respectively.

Obviously, the relation between the latest model and the old ones is not observed. As a result, it triggers us to do a comparison between these models. Based on the work of Choo et al., we still need to examine the definition of security of these models that focus on definition of partnership, the ability of adversary, and the definition of cleanness (or freshness). Furthermore, the function requirement mentioned in [1], will also be checked in the ECK2007 model as this requirement is significant in the process of the comparison.

Contributions

Our main contributions are illustrated on the right in the Fig.1, the dashed arrows represents the section in which the proof is provided. On the left, the real line represents the results which have already been proved. In addition, we show that differences of those proof models for key agreement protocols.

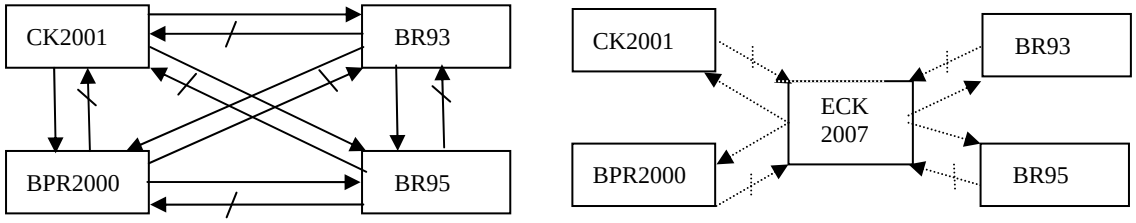

Fig 1 Notions of security among models

2 Overview of Models

Choo et al. have a concise summary of differences among the models which appeared before the ECK2007 model. We suggest the reader to obtain the detail from [1]. Here we stress the differences between the ECK2007 model and the previous ones by figures. It is important for us to know how the partnership and clean session are defined, and what powers the adversary does have.

2.1 Partnership

The BR93 model used matching conversation to define the partnership. In other words, the conversation is concatenation of exchanged communications by parties. In the BR95 model, the partnership is defined using the notion of a partner function. However, this method is not seemed as a good way to define the partnership since no explicit definition of partnership was described in the original paper. The CK2001 model and the BPR2000 model defined partnership via session identifiers (SIDs). However, Choo et al. claimed that there is no formal definition of SIDs in the CK2001 model. To avoid complexity, although differs from the original paper, in this paper we use **session identifiers defined via matching conversation in the CK2001 model** which is commonly used in the variant of the CK2001 model when Krawczyk analyzed HMQV protocol[6].

Matching Conversation	BR93
Partner Function	BR95
SIDs	BPR2000, CK2001, ECK2001

Table.2 definition of partnership in each model

2.2 Ability of Adversary

In all models, the adversary, *M*, is a probabilistic Turing machine and controls all communications of the parties. Besides, he can query the oracles that the model allows to be queried. Furthermore, these queries of the adversary are adaptive and non-order. To save space, we only illustrate what query an adversary can make in each model in Table. 3, and its last column describes the results of the queries to which the adversary can access. The detail of those queries can be found in the original paper which presents the model.

It is notable to see there is no Corrupt query in the ECK2007 model, where allows the attacker to do **Long-term Key Reveal** and **Ephemeral-term Key Reveal**, as the adversary can achieve the result of the **Corrupt** query by revealing the secrecy of the party via **Long-term Key Reveal**, **Ephemeral-term Key Reveal** and **Session-Key Reveal** queries.

Oracle Queries	BR93	BR95	BPR2000	CK2001	ECK2007	Result to attacker
Send	Yes	Yes	Yes	Yes	Yes	
Session-Key Reveal(U_1,U_2,i)	Yes	Yes	Yes	Yes	Yes	Session key from $\prod_{U_1,U_2}^{i}$
Session-State Reveal(U_1,U_2,i)	No	No	No	Yes	No	Ephemeral state from $\prod_{U_1,U_2}^{i}$
Long-term Key Reveal(U_1)	No	No	No	No	Yes	Static key of U_1
Ephemeral-term Key Reveal(U_1,U_2,i)	No	No	No	No	Yes	Ephemeral key from $\prod_{U_1,U_2}^{i}$
Corrupt (U_1)	No	Yes	No	Yes	**No**	All internal state of U_1
Test(U_1,U_2,i)	Yes	Yes	Yes	Yes	Yes	A challenge from $\prod_{U_1,U_2}^{i}$

Table 3 Comparison of adversarial powers

Definition 1 (Definition of Cleanness)

Let oracle $\prod_{B,A}^{j}$ be the partner of oracle $\prod_{A,B}^{i}$ if it exists, then oracle $\prod_{A,B}^{i}$ is clean (or holds a clean session key) at the end of execution, if none of the conditions hold:

1. either $\prod_{A,B}^{i}$ or $\prod_{B,A}^{j}$ oracle has been issued a **Session-Key Reveal** query (or **Session-State Reveal** query in CK2001 model);

2. either *A* or *B* has been sent a **Corrupt** query;

3. especial for the ECK2007 model

(i) $\prod_{B,A}^{j}$ exists and an adversary makes either of the following queries:

---both **Long-Term Key Reveal (*A*) and Ephemeral Key Reveal (*A,B,i*)** or

---both **Long-Term Key Reveal (*B*) and Ephemeral Key Reveal (*B,A,j*)**

(ii) $\prod_{B,A}^{j}$ does not exist and an adversary makes either of the following queries:

---both **Long-Term Key Reveal (*A*) and Ephemeral Key Reveal (*A,B,i*)** or

---both **Long-Term Key Reveal (*B*)**

2.4 Adversarial Goal

The adversary's aim is to guess whether the challenge is a real session key or a randomly chosen key. At the end of the game, it outputs a bit *b'*. In the game, the adversary, *M*, will choose a clean session on which to be tested and send a **Test**(U_1,U_2,i)

query to the clean oracle associated with the test session. *M* wins if, after asking a **Test** query, where $\prod_{U_1,U_2}^{i}$ is clean and has accepted, *M's* guess bit *b'* equals the bit *b* selected during the **Test** query. Let $adv^{M}(k)$ denote advantage of the adversary in breaking the protocol and the security, where $adv^{M}(k) = 2 \times \Pr[b = b'] - 1$.

2.5 Definition of Security

Now that we have the definition of fresh session and adversarial goal, it is easy to define the security.

Definition 2 (BR93, CK2001, ECK2007 Security) A protocol is secure in these models if both of the following requirement are satisfied

1. if two uncorrupted oracles $\prod_{A,B}^{i}$ and $\prod_{B,A}^{j}$ complete matching sessions, then both $\prod_{A,B}^{i}$ and $\prod_{B,A}^{j}$ must hold the same session key, and,
2. for all PPT adversaries *M*, $adv^{M}(k)$ is negligible.

Definition 3 (BR95 Security) A protocol is secure in these models if

1. When a protocol is run between two oracles $\prod_{A,B}^{i}$ and $\prod_{B,A}^{j}$ in the absence of malicious adversary, both $\prod_{A,B}^{i}$ and $\prod_{B,A}^{j}$ accept and hold the same session key，
2. for all PPT adversaries *M*, $adv^{M}(k)$ is negligible

Definition 4 (BPR2000 Security) A protocol is security in the BPR2000 model under the notion of key establishment if for all PPT adversaries *M*, $adv^{M}(k)$ is negligible.

Considering the security definition of those models, we observe that the ECK 2007 model also has the function requirement (requirement 1 in the definition 2) which is needed in both of the BR93 model and the CK2001 model. If the requirement that two parties in the same session must accept the same session key is not satisfied, in our view, this does not violate BR95 and BPR2000 security described above, however, violates BR93, CK2001, and ECK2007 security. It is helpful for us to find counter-examples to complete the proof of non-implication relation between two models.

3 Relative strengths of security

In this section, our major work is to compare the relations between the ECK2007 model and other models. We still use the comparing approach shown in [1] to finish our work. Note that two requirements are needed in checking whether the primary adversary could answer the queries from the secondary adversary. The first one: Non-partners in the simulation of *SA* are also non-partners in the simulation of *PA*. Alternatively, we require that partners in the simulation of *PA* are also partners in the simulation of *SA*. The second one: A clean oracle in the simulation of *SA* is also a clean oracle the simulation of *PA*

3.1 Proof of Implication Relation: ECK2007→ CK2001

Let M_{07}, M_{01} denote adversary in the ECK2007 model and adversary in the CK2001 model respectively. Clearly, the former can do **Long-Term Key Reveal** query, however, the latter can not do it. Intuitively, the power M_{07} has is greater.

Lemma 1 For any key establishment protocol and for any M_{01}, there exists an M_{07}, such that $adv^{M_{01}} = adv^{M_{07}}$.

Proof: We construct an adversary M_{07} against the key agreement protocol in the ECK2007 model by secondary adversary, M_{01}, against the same protocol in CK2001 model. M_{07} must perfectly simulate the view of M_{01} so that M_{01} can not discover M_{07} is cheating. That means M_{07} should answer the queries from M_{01} by asking oracles to which he has access. The simulation proceeds as follows. M_{01} makes any sequence of the following queries:

Send: M_{07} upon receiving a **Send** query from M_{01}, he is able to answer this query by asking its **Send** oracle.

Session-Key Reveal: M_{07} is restricted from asking a **Session-Key Reveal** query to the target test oracle or its partner oracle in its own game. Similarly, M_{01} faces the same restriction which is subject to the two requirements described above. Hence,

M_{07} is able to answer this query by asking its **Session-Key Reveal** oracle and simulate the **Session-Key Reveal** query perfectly.

Session-State Reveal: M_{01} is not allowed to make **Session-State Reveal** queries against the target test session or its matching session (if it exists). However, M_{07} is allowed to make **Ephemeral Key Reveal** queries to the test oracle or its partner except the partner having no ephemeral secret. M_{07}, of course, is able to do **Ephemeral Key Reveal** to any session at any time if the session holds ephemeral key. Hence, M_{07} is able to answer this query by asking its **Ephemeral Key Reveal** oracle and to simulate the **Session-State Reveal** query perfectly.

Corrupt: M_{01} is disallowed from asking a **Corrupt** query to the participants of the target test session or whom the target test session thinks it is communicating with in its own game. Similarly, M_{07} faces the same restriction. Therefore, M_{07} is able to answer this query by asking its **Ephemeral Key Reveal** oracle, **Session-Key Reveal** oracle and **Long-term Key Reveal** oracle, and simulate the **Corrupt** query perfectly.

Test: Assuming both M_{07} and M_{01} choose the same **Test** session, M_{07} queries its **Test** oracle and is given a challenge that is either a real value or a random value depending on a random bit , b_{test} , chosen by the oracle to which M_{07} has access. M_{07} then forwards this challenge to M_{01}. At last, M_{01} outputs a bit b_{01}, and M_{07} will also output b_{01} as its answer. Thus, M_{07} succeeds and wins the game if M_{01} does.

Note that M_{07} queries its **Test** oracle if following conditions are satisfied: the **Test session** in both $M_{07}'s$ and $M_{01}'s$ simulation have accepted and must be clean.

To show the primary adversary, M_{07} , can answer the queries from the secondary adversary, M_{01}, we need to validate two requirements as mentioned above to be satisfied in both $M_{07}'s$ and $M_{01}'s$ simulation. In section 2.1, we have

introduced the matching session in the ECK2007 model, where a session executed by one party has the matching session executed by the other party with the same communications being transmitted. For instance, in the executed protocol shown in Fig. 4, the session with session identifier $sid = (O, A, B, comm_A, comm_B)$ executed by A is said to have matching session $sid^* = (P, B, A, comm_A, comm_B)$ executed by B. We stress that session identifiers (SIDs) are defined via matching session in the CK2001 model (it is same as in variant of the CK2001 model, albeit differs from the original definition). Namely, the session $(B, A, comm_B, comm_A)$ (if it exists) is said to be matching to the session $(A, B, comm_A, comm_B)$. As we see, SIDs is defined in the same manner for the CK2001 and ECK2007 model. If a session has matching session, then the two parties in the session are partner. Thus, if A and B are partners in ECK2007 model, then A and B are also partners in CK2001 model. Since partners in the simulation of M_{07} are also partners in the simulation of M_{01}, requirement 1 is satisfied.

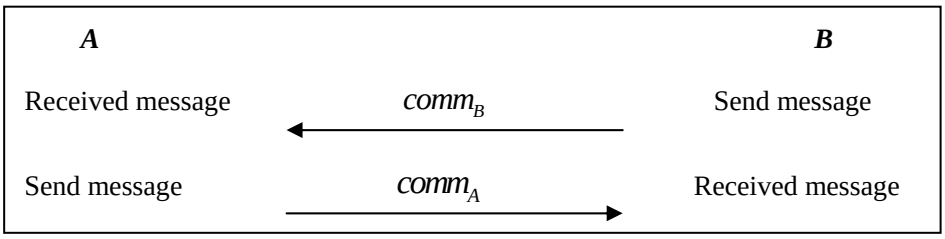

Fig.4 Communication transmitted in protocol

An oracle is called clean in the CK2001 model if the adversary does not perform any following actions on said oracle (or its associated partner, if such a partner exists): **Session-Key Reveal, Session-State Reveal,** or **Corrupt query**. An oracle is considered clean in the ECK2007 model if the adversary does not do: i.) **Session-Key Reveal** query, ii.) both **Long-Term Key Reveal** and **Ephemeral Key Reveal** query (or its associated partner, if such a partner exists), iii.) **Long-Term Key Reveal** and **Ephemeral Key Reveal** query or **Long-Term Key Reveal** query of the other party (if its associated partner does not exist). LaMacchia et al. claimed that, the adversary's power that **Ephemeral Key Reveal** in the ECK2007 model is better than the

adversary's power that **Session-State Reveal** in the CK2001 model, since the definition of the session-state reveal query must be specified in the CK2001 model. Besides, M_{01} is not allowed to ask any **Long-Term Key Reveal** in the CK2001 model, therefore, M_{01} will not be asking any such queries in the simulation. Hence, it follows easily that a clean oracle in the CK2001 model is also clean in the ECK2007 model. So, both of requirements 1 and 2 are satisfied.

Consider the case in which the challenge given to M_{07} is a random key, i.e. a random value from the distribution of key generated by the protocol. The probability of M_{01} guessing the correct b_{07} bit is $1/2$ because it cannot gain any information about the hidden b_{07}. We then consider the case where the Test oracle associated with M_{07} returns the actual session key. In this case, the proof simulation (of M_{01}) is perfect and M_{07} runs M_{01} exactly in the game defining the security of M_{01}. Therefore, if M_{01} has a non-negligible advantage, so does M_{07} (i.e. $Adv^{M_{07}} = Adv^{M_{01}}$). This is in violation of our assumption and Lemma 1 follows. □

3.2 Proving Non-Implication Relation: ECK2007 $\not\leftarrow$ CK2001

Some attacks are not allowed in the CK2001 model, however, permitted in the ECK2007. Although Krawczyk[6] reinforces the CK2001 model by adding resistance to KCI attacks and weak Perfect Forward Secrecy (wPFS) in the variant of CK2001 model, the extension does not include other attacks. For instance, two honest parties execute matching sessions, and the adversary reveals the ephemeral secret keys of both of the parties and tries to learn the session key. Unfortunately, SIG-DH protocol, as shown in Fig.5, proved to be secure in the CK2001 model by Canetti and Krawczyk can not resist this attack, since the attacker is able to compute the session key g^{xy} if he reveals the ephemeral keys both of the parties by asking **Ephemeral Key Reveal** query. Thus, it is not secure in the ECK2007 model even the attacker does not know the long-term secret key of party. Hence, the SIG-DH protocol is

secure in the CK2001 model, is insecure in the ECK2007 model.

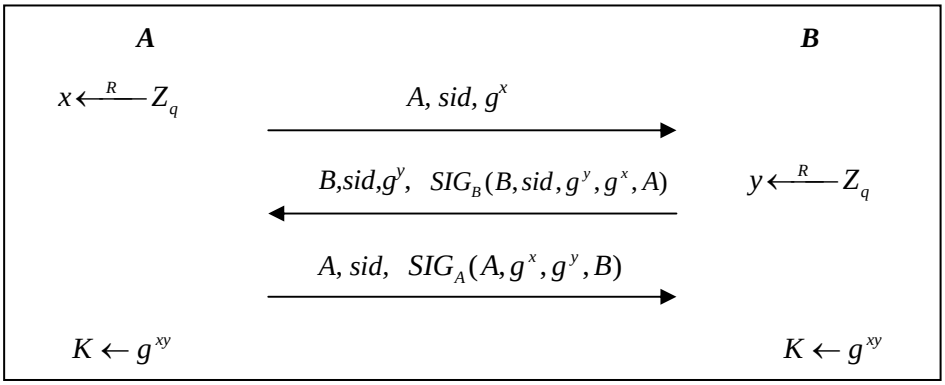

Fig.5 SIG-DH key-exchange protocol

3.3 Proof of Implication Relation: ECK2007→BR93, BR95, BPR2000

Choo et al. demonstrated that the security of the CK2001 model is the strongest if its SIDs defined via matching conversation. In section 3.1, we prove **ECK2007→ CK2001** under this assumption. Hence, the security of the ECK2007 model is the strongest.

3.4 Proving Non-Implication Relation: ECK2007 $\not\leftarrow$ BR93

Wong–Chan MAKEP[8] protocol proved secure in the BR93 model is insecure in the CK2001 model because the adversary can fabricate the communication between two parities using the ephemeral key which obtained by asking **Session-State Reveal** query. Choo et al. depicts how the adversary of the CK2001 model attacks in detail. As we know, an adversary of the ECK2007 model can obtain the ephemeral key by asking **Ephemeral Key Reveal** query. As a result, he is able to fabricate the communication between two parities like the one in the CK2001 model, so that Wong–Chan MAKEP protocol is also insecure in the ECK2007 model.

3.5 Discussion on Non-Implication Relation: ECK 2007 $\not\leftarrow$ BR95, BPR2000

The function requirement—two parties in the same session must accept the same session key in a key exchange protocol proven secure—is not required in the BR95 and BPR2000 model, however is required in the ECK2007 model as well as both of the BR93 model and BPR2000 model. It suggests that the counter-example used to prove non-implication between BR93 and BR95 (or CK2001 and BR95) will be a suitable counter-example to prove non-implication between ECK2007 and BR95,

since in the example execution of the protocol in the presence of malicious adversary, both uncorrupted principals *A* and *B* have accepted different session keys at the end of the protocol execution. According to Definition 2, this violates the ECK2007 security, however does not violate the BR95 security. Similarly, the counter-example used to prove non-implication between BR93 and BPR2000 (or CK2001 and BPR200) will be a suitable counter-example to prove non-implication between ECK2007 and BPR2000. We omit these counter-examples, the reader who is interested could see section 3.4 and section 3.5 in [1].

4 Conclusion and Future Work

We compared the proof models for key agreement protocols, mainly the ECK2007 model and the other models, and analyzed the differences of security definition of all models. Our conclusion is that ECK2007 model provides the strongest definition of security compared to others.

In future, we are interested in proof models for tripartite key agreement protocols, and hope to design more efficient protocol which can be proven secure in the ECK2007 model. Analyzing and comparing the recently protocols proven secure, such as CMQV [9], is also our interest.

References

[1] Choo K-K., Boyd C., and Hitchcock Y., Examining indistinguishability-based proof models for key establishment protocols [C]// Advances in Cryptology ASIACRYPT 2005, Springer-Verlag, 2005: 585–604

[2] Bellare M. and Rogaway P., Entity authentication and key distribution [C]// Advances in Cryptology CRYPTO ’93, Springer-Verlag, 1993: 110–125.

[3] Bellare M., and Rogaway P., Provably Secure Session Key Distribution: The Three Party Case [C]// ‘27th ACM Symposium on the Theory of Computing - STOC1995’, ACM Press 1995: 57–66.

[4] Bellare M., Pointcheval D., and Rogaway P., Authenticated Key Exchange Secure Against Dictionary Attacks [C]// ‘Advances in Cryptology – Eurocrypt 2000’, LNCS 1807 (2000), Springer-Verlag 2000: 139–155.

[5] Canetti, R. and Krawczyk, H., Analysis of Key-Exchange Protocols and Their Use

for Building Secure Channels [C] (Extended version available from http://eprint.iacr.org/2001/040/)// Advances in Cryptology Eurocrypt 2001, Springer-Verlag, 2001: 453–474.

[6] Krawczyk H., HMQV: A High-Performance Secure Diffie-Hellman Protocol [C]//Advances in Cryptology —CRYPTO ’05, Springer-Verlag, 2005: 546–566,

[7] LaMacchia B., Lauter K., and Mityagin A., Stronger security of authenticated key exchange [C]//Proceedings of International Conference on Provable Security 2007(ProvSec 2007), Springer-Verlag, 2007: 1-16.

[8] Wong, D. S. and Chan, A. H.,Efficient and Mutually Authenticated Key Exchange for Low Power Computing Devices [C]// Advances in Cryptology Asiacrypt 2001, Springer-Verlag, 2001: 172–289.

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