Revisit of McCullagh–Barreto Two-Party ID-Based Authenticated Key Agreement Protocols*

Kim-Kwang Raymond Choo

Information Security Institute, Queensland University of Technology
GPO Box 2434, Brisbane, QLD 4001, Australia (Email: k.choo@qut.edu.au)

(Received June 29, 2005; revised and accepted July 31, 2005)

Abstract

We revisit the two-party identity-based authenticated key agreement protocol (2P-IDAKA) and its variant resistant to key-compromise impersonation due to McCullagh & Barreto (2005). Protocol 2P-IDAKA carries a proof of security in the Bellare & Rogaway (1993) model. In this paper, we demonstrated why both the protocol and its variant are not secure if the adversary is allowed to send a Reveal query to reveal non-partner players who had accepted the same session key (i.e., termed *key-replicating attack* in recent work of Krawczyk (2005)). We also demonstrate that both protocols do not achieve the *key integrity* property, first discussed by Janson & Tsudik (1995).

Keywords: Cryptographic protocols, identity-based cryptography, authenticated key agreement, provable security

1 Introduction

Despite cryptographic protocols being the *sine qua non* of many diverse secure electronic commerce applications, the design of secure cryptographic protocols is still notoriously hard. The difficulties associated in obtaining a high level of assurance in the security of almost any new or even existing protocols are well illustrated with examples of errors found in many such protocols years after they were published [2, 3, 4, 5, 18, 19, 21, 22, 23, 26, 31, 33, 34, 35, 36, 37, 40]. The many flaws discovered in published protocols for key establishment and authentication over many years, have promoted the use of formal models and rigorous security proofs.

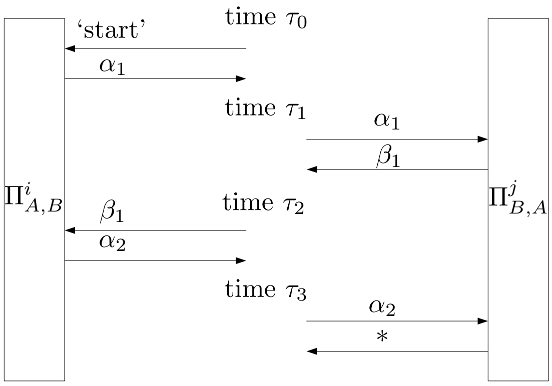
The treatment of computational complexity analysis adopts a deductive reasoning process whereby the emphasis is placed on a proven reduction from the problem of breaking the protocol to another problem believed to be hard. Such an approach for key establishment protocols was made popular by Bellare & Rogaway [9] who provided the first formal definition for a model of adversary capabilities with an associated definition of security (which we refer to as the BR93 model in this paper). Since then, the BR93 model is one of the widely used proof models in the computational complexity approach for protocol analysis [17]. An extension of the BR93 model was used to analyse a three-party server-based key distribution (3PKD) protocol by Bellare & Rogaway [10]. A more recent revision to the model was proposed in 2000 by Bellare, Pointcheval and Rogaway [8]. In independent yet related work, Bellare, Canetti, & Krawczyk [7] build on the BR93 model and introduce a modular proof model. However, some drawbacks with this formulation were discovered and this modular proof model was subsequently modified by Canetti & Krawczyk [14].

Case Study

McCullagh & Barreto propose a new two-party identity-based authenticated key agreement (2P-IDAKA) protocol in CT-RSA 2005 [30], which carries a proof of security in the BR93 model. In the BR93 model, there exists a powerful probabilistic polynomial-time (PPT) adversary, $\mathcal{A}$, which controls all the communications that take place between parties via a pre-defined set of oracle queries, namely:

- $\mathsf{Send}(U, s, m)$ query which $\mathcal{A}$ allows to send message m to oracle Π_U^s,
- $\mathsf{Reveal}(U, s)$ query which $\mathcal{A}$ allows to reveal session key (if any) accepted by Π_U^s,
- $\mathsf{Corrupt}(U, K)$ query which $\mathcal{A}$ allows to reveal state of U and/or set the long-term key of U to K, and
- $\mathsf{Test}(U, s)$ query returns to $\mathcal{A}$ a test key, in which $\mathcal{A}$ will determine whether the test session is random or the actual session key (i.e., indistinguishability).

*A preliminary version of this work appears in [16].



Note that the construction of conversation shown in Definition 1 depends on the number of parties and the number of message flows. Informally, both $\Pi^i_{A,B}$ and $\Pi^j_{B,A}$ are said to be BR93 partners if each one responded to a message that was sent unchanged by its partner with the exception of perhaps the first and last message.

Figure 1: Matching conversation [9]

Xie pointed out a flaw in the 2P-IDAKA protocol, where a malicious adversary is able to successfully launch a key compromise attack on the protocol [38]. To address this attack pointed out by Xie, McCullagh & Barreto propose a fix resistant to key-compromise impersonation in their paper [30].

In this paper, we demonstrate why the 2P-IDAKA protocol and the fix (variant) are not secure if the adversary is allowed to reveal non-partner players who had accepted the same session key. However, such a Reveal query is important as it captures the notion of known key security, whereby a protocol should still achieve its goal in the face of a malicious adversary who has learned some other session keys [12, 24].

Organization of Paper

The remainder of this paper is structured as follows: Section 2 briefly explains the BR93 model. Section 3 describes both the 2P-IDAKA protocol and the fix (variant), and the attack sequences on both protocols. Section 4 presents the conclusions.

2 Overview of the BR93 Model

In this section, an informal overview of the BR93 model is provided primarily for the benefit of the reader who is unfamiliar with the model. For a more comprehensive description, the reader is referred to the original paper [9].

The BR93 model defines provable security for entity the authentication and key distribution goals. The adversary $\mathcal{A}$ in the model, is a probabilistic machine that controls all the communications that take place between parties by interacting with a set of $\Pi^i_{U_1,U_2}$ oracles ($\Pi^i_{U_1,U_2}$ is defined to be the i^{th} instantiation of a principal U_1 in a specific protocol run and U_2 is the principal with whom U_1 wishes to establish a secret key). The predefined oracle queries are described informally as follows.

– The $\mathsf{Send}(U_1, U_2, i, m)$ query allows $\mathcal{A}$ to send some message m of her choice to either the client $\Pi^i_{U_1,U_2}$ at will. $\Pi^i_{U_1,U_2}$, upon receiving the query, will compute what the protocol specification demands and return to $\mathcal{A}$ the response message and/or decision. If $\Pi^i_{U_1,U_2}$ has either accepted with some session key or terminated, this will be made known to $\mathcal{A}$.

– The $\mathsf{Reveal}(U_1, U_2, i)$ query allows $\mathcal{A}$ to expose an old session key that has been previously accepted. $\Pi^i_{U_1,U_2}$, upon receiving this query and if it has accepted and holds some session key, will send this session key back to $\mathcal{A}$.

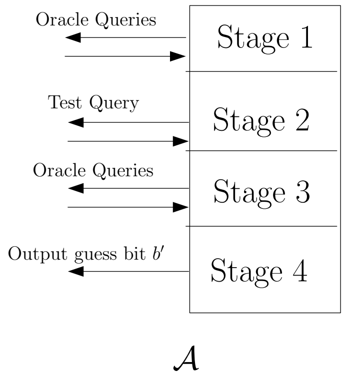
– The $\mathsf{Corrupt}(U_1, K_E)$ query allows $\mathcal{A}$ to corrupt the principal U_1 at will, and thereby learn the complete internal state of the corrupted principal. The corrupt query also gives $\mathcal{A}$ the ability to overwrite the long-lived key of the corrupted principal with any value of her choice (i.e. K_E). This query can be used to model the real world scenarios of an insider cooperating with the adversary or an insider who has been completely compromised by the adversary.

– The $\mathsf{Test}(U_1, U_2, i)$ query is the only oracle query that does not correspond to any of $\mathcal{A}$'s abilities. If $\Pi^i_{U_1,U_2}$ has accepted with some session key and is being asked a $\mathsf{Test}(U_1, U_2, i)$ query, then depending on a randomly chosen bit b, $\mathcal{A}$ is given either the actual session key or a session key drawn randomly from the session key distribution.

Note that in the original BR93 model, the Corrupt query is not allowed. However, such a query is important as it captures the notion of unknown key share attack [25] and insider attack. Hence, later proofs of security in the BR93 model [1, 11, 12, 15, 20, 29, 30, 37] allow such a query.

2.1 Definition of Partnership

Partnership is defined using the notion of matching conversations, where a conversation is defined to be the sequence of messages sent and received by an oracle. The sequence of messages exchanged (i.e., only the Send oracle queries) are recorded in the transcript, T. At the end of a protocol run, T will contain the record of the Send queries and the responses as shown in Figure 1. Definition 1 gives



Stage 1: $\mathcal{A}$ is able to send any Send, Reveal, and Corrupt oracle queries at will.
Stage 2: At some point during $\mathcal{G}$, $\mathcal{A}$ will choose a fresh session on which to be tested and send a Test query to the fresh oracle associated with the test session. Note that the test session chosen must be fresh. Depending on a randomly chosen bit b, $\mathcal{A}$ is given either the actual session key or a session key drawn randomly from the session key distribution.
Stage 3: $\mathcal{A}$ continues interacting with the protocol by making any Send, Reveal, and Corrupt oracle queries of its choice.
Stage 4: Eventually, $\mathcal{A}$ terminates the game simulation and outputs a bit b', which is its guess of the value of b.

Figure 2: Game simulation $\mathcal{G}$

a simplified definition of matching conversations for the case of the protocol shown in Figure 1.

Definition 1 (BR93 Definition of Matching Conversations [9]). *Let n be the maximum number of sessions between any two parties in the protocol run. Run the protocol shown in Figure 1 in the presence of a malicious adversary $\mathcal{A}$ and consider an initiator oracle $\Pi^i_{A,B}$ and a responder oracle $\Pi^j_{B,A}$ who engage in conversations C_A and C_B respectively. $\Pi^i_{A,B}$ and $\Pi^j_{B,A}$ are said to be partners if they both have matching conversations, where*

$$\begin{aligned} C_A &= (\tau_0, 'start', \alpha_1), (\tau_2, \beta_1, \alpha_2) \\ C_B &= (\tau_1, \alpha_1, \beta_1), (\tau_3, \alpha_2, *), \textit{ for } \tau_0 < \tau_1 < \ldots \end{aligned}$$

The matching conversations play a significant role as they bind together incoming and outgoing messages, and uniquely identify a particular session.

2.2 Definition of Freshness

The notion of freshness is used to identify the session keys about which $\mathcal{A}$ ought not to know anything because $\mathcal{A}$ has not revealed any oracles that have accepted the key and has not corrupted any principals knowing the key. Definition 2 describes freshness in the BR93 model, which depends on the notion of partnership in Definition 1.

Definition 2 (Definition of Freshness). *Oracle $\Pi^i_{A,B}$ is fresh (or it holds a fresh session key) at the end of execution, if, and only if, oracle $\Pi^i_{A,B}$ has accepted with or without a partner oracle $\Pi^j_{B,A}$, both oracle $\Pi^i_{A,B}$ and its partner oracle $\Pi^j_{B,A}$ (if such a partner oracle exists) have not been sent a* Reveal *query, and the principals A and B of oracles $\Pi^i_{A,B}$ and $\Pi^j_{B,A}$ (if such a partner exists) have not been sent a* Corrupt *query.*

2.3 Definition of Security

Security is defined using the game $\mathcal{G}$, played between a malicious adversary $\mathcal{A}$ and a collection of $\Pi^i_{U_x,U_y}$ oracles for players $U_x, U_y \in \{U_1, \ldots, U_{N_p}\}$ and instances $i \in \{1, \ldots, N_s\}$. The adversary $\mathcal{A}$ runs the game simulation $\mathcal{G}$, whose setting is described in Figure 2.

Success of $\mathcal{A}$ in $\mathcal{G}$ is quantified in terms of $\mathcal{A}$'s advantage in distinguishing whether $\mathcal{A}$ receives the real key or a random value. $\mathcal{A}$ wins if, after asking a $\mathsf{Test}(U_1, U_2, i)$ query, where $\Pi^i_{U_1,U_2}$ is fresh and has accepted, $\mathcal{A}$'s guess bit b' equals the bit b selected during the $\mathsf{Test}(U_1, U_2, i)$ query. Let the advantage function of $\mathcal{A}$ be denoted by $\mathsf{Adv}^{\mathcal{A}}(\mathsf{k})$, where

$$\mathsf{Adv}^{\mathcal{A}}(\mathsf{k}) = 2 \times \Pr[\mathsf{b} = \mathsf{b}'] - 1.$$

We require the definition of a negligible function, as described in Definition 3 .

Definition 3 ([6]). *A function $\epsilon(k) : \mathbb{N} \to \mathbb{R}$ in the security parameter k, is called negligible if it approaches zero faster than the reciprocal of any polynomial. That is, for every $c \in \mathbb{N}$ there is an integer k_c such that $\epsilon(k) \leq k^{-c}$ for all $k \geq k_c$.*

Definition 4 describes the BR93 security definition.

Definition 4 (BR93 Definition of Security [9]). *A protocol is secure in the BR93 model if for all PPT adversaries $\mathcal{A}$,*

1) *if uncorrupted oracles $\Pi^i_{A,B}$ and $\Pi^j_{B,A}$ complete with matching conversations, then the probability that there exist i, j such that $\Pi^i_{A,B}$ accepted and there is no $\Pi^j_{B,A}$ that had engaged in a matching session is negligible.*

2) $\mathsf{Adv}^{\mathcal{A}}(\mathsf{k})$ *is negligible.*

If both requirements of Definition 4 are satisfied, then $\Pi^i_{A,B}$ and $\Pi^j_{B,A}$ will also have the same session key.

2.4 Protocol Security

Security of a protocol is proved by finding a reduction to some well known computational problem whose intractability is assumed, and in this paper, the Bilinear Inverse Diffie-Hellman (BIDH) problem. Let $\mathbb{G}_1, \mathbb{G}_2$ be two groups of prime order q, $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, P be a generator of $\mathbb{G}_1$, and $a, b \in_R \mathbb{Z}_q^*$.

Bilinear Inverse Diffie-Hellman (BIDH) Problem.

$$\begin{aligned} \textit{Instance} &: (P, aP, bP) \\ \textit{Output} &: \hat{e}(P,P)^{a^{-1}b} \in \mathbb{G}_2. \end{aligned}$$

The BIDH problem has been shown to be polynomial time equivalent to the better known Bilinear Diffie-Hellman (BDH) problem [13] in recent work of Zhang, Safavi-Naini, & Susilo [39]. In order to help the descriptions later we here introduce another property which is often ignored.

Definition 5 (Key Integrity [27]). *Key integrity is the property that the key has not been modified by the adversary, or equivalently only has inputs from legitimate principals.*

- *For a key transport protocol, key integrity means that if the key is accepted by any principal it must be the same key as chosen by the key originator.*

- *For a key agreement protocol, key integrity means that if a key is accepted by any principal it must be a known function of only the inputs of the protocol principals.*

3 McCullagh–Barreto Protocols

In this section, we revisit the 2P-IDAKA protocol and its variant due to McCullagh & Barreto [30]. Example executions of the protocols in the presense of a malicious adversary are used to demonstrate why the protocols are not secure if the adversary is allowed access to Reveal query. We omit the standard (mathematical preliminaries) details, which are not necessary to understand the key replicating attack in this section. Interested reader can refer to the original paper of McCullagh & Barreto.

Notation used in the protocols is as follows: $(s + a)P$ denotes the public key of A, $A_{pri} = ((s + a))^{-1}P$ denotes the private key of A, $(s + b)P$ denotes the public key of B, and $B_{pri} = ((s + b))^{-1}P$ denotes the private key of B, x_a and x_b denote random nonces where $x_a, x_b \in_R Z_r^*$.

3.1 2P-IDAKA Protocol

The 2P-IDAKA protocol is shown in Figure 3. There are two entities in the protocol, namely an initiator player A and a responder player B. The 2P-IDAKA protocol shown in Figure 3 carries a proof of security in the BR93 model.

A		B
$x_a \in_R Z_r^*$	$\xrightarrow{A_{KA} = x_a(s+b)P}$	$x_b \in_R Z_r^*$
$\hat{e}(B_{KA}, A_{pri})^{x_a}$	$\xleftarrow{B_{KA} = x_b(s+a)P}$	$\hat{e}(A_{KA}, B_{pri})^{x_b}$

Figure 3: McCullagh–Barreto 2P-IDAKA protocol

At the end of the 2P-IDAKA protocol execution, both A and B accept session keys

$$\begin{aligned} SK_{AB} &= \hat{e}(B_{KA}, A_{pri})^{x_a} = \hat{e}(P,P)^{x_a x_b} \\ SK_{BA} &= \hat{e}(A_{KA}, B_{pri})^{x_b} = \hat{e}(P,P)^{x_a x_b} \\ &= SK_{AB}. \end{aligned}$$

3.2 A Variant of 2P-IDAKA Protocol

Figure 4 describe a variant of the 2P-IDAKA protocol proposed to address Xie's attack [38].
At the end of the fixed protocol execution, both A and B accept session keys

$$\begin{aligned} SK_{AB} &= e(P,P)^{x_a} e(B_{KA}, A_{pri}) = e(P,P)^{x_a + x_b} \\ SK_{BA} &= e(P,P)^{x_b} e(A_{KA}, B_{pri}) = e(P,P)^{x_a + x_b} \\ &= SK_{AB}. \end{aligned}$$

3.3 Key Replicating Attacks on the Protocols

We now describe the key replicating attack first discussed by Krawczyk [28] as presented in Definition 6.

Definition 6 (Key Replicating Attack [28]). *A key replicating attack is defined to be an attack whereby the adversary, $\mathcal{A}$, succeeds in forcing the establishment of a session, S, (other than the* Test *session or its matching session) that has the same key as the* Test *session. In this case, $\mathcal{A}$ can distinguish whether the* Test*-session key is real or random by asking a* Reveal *query to the oracle associated with S.*

Figures 5 and 6 illustrate example execution of the protocols in the presence of a malicious adversary, $\mathcal{A}$.

In the attack sequences shown in Figures 5 and 6, both A and B have accepted the same session key. However, both A and B are non-partners since they do not have matching conversations as described in Definition 1. Hence, $\mathcal{A}$ succeeds in forcing the establishment of a session, Π_B, (other than the Test session or its matching session) that has the same key as the Test session (i.e.,

A		B
$x_a \in_R Z_r^*$	$\xrightarrow{A_{KA} = x_a(s+b)P}$	$x_b \in_R Z_r^*$
$e(P,P)^{x_a} e(B_{KA}, A_{pri})$	$\xleftarrow{B_{KA} = x_b(s+a)P}$	$e(P,P)^{x_b} e(A_{KA}, B_{pri})$

Figure 4: Proposed fix to Xie (2004)'s attack – variant protocol

key-replicating attack as described in Definition 6). Consequently, $\mathcal{A}$ is able to trivially expose a fresh session key by asking a Reveal query to either A or B, and has a non-negligible advantage in distinguishing the Test key (i.e. $\mathsf{Adv}^{\mathcal{A}}(k)$is non-negligible). Furthermore, session keys comprise keying material contributed by $\mathcal{A}$, x_E, in violation of the key integrity property described in Definition 5.

3.4 Remarks

In recent work [20], we demonstrate that the McCullagh–Barreto 2P-IDAKA protocol can be proven secure in the BR93 model without restricting the adversary, $\mathcal{A}$, from asking the Reveal queries in most situations (i.e., $\mathcal{A}$ is restricted from asking Reveal queries to any sessions associated with the owner of the target Test session), by simply making a small change to the way that session keys are constructed in the protocol. However, if the Gap Bilinear Diffie-Hellman (GBDH) assumption due to Okamoto & Pointcheval [32] is used, then the improved McCullagh–Barreto 2P-IDAKA protocol can be proven secure in the BR93 model without any restriction.

4 Conclusion

Through a detailed study of the McCullagh–Barreto 2P-IDAKA protocol and its variant, we had demonstrated why the protocol and its variant are insecure if the adversary is allowed to reveal non-partner players who share the same session key and obtain a fresh session key, in violation of the definition of security in the BR93 model (in which the protocol is proven secure). We also demonstrated that the protocols do not achieve the key integrity property.

Acknowledgments

This work was partially funded by the Australian Research Council Discovery Project Grant DP0345775.

References

[1] Sattam S. Al-Riyami and Kenneth G. Paterson, "Tripartite authenticated key agreement protocols from pairings," in *9th IMA Conference on Cryptography and Coding* (Kenneth G. Paterson, ed.), LNCS 2898, pp. 332–359, Springer-Verlag, 2003.

[2] F. Bao, "Security analysis of a password authenticated key exchange protocol," in *6th Information Security Conference - ISC 2003* (Colin Boyd and Wenbo Mao, eds.), LNCS 2851, pp. 208–217, Springer-Verlag, 2003.

[3] F. Bao, "Colluding attacks to a payment protocol and two signature exchange schemes," in *Advances in Cryptology - Asiacrypt 2004* (Pil Joong Lee, ed.), LNCS 3329, pp. 417–429, Springer-Verlag, 2004.

[4] David A. Basin, S. Mödersheim, and L. Viganó, *An On-the-Fly Model-Checker for Security Protocol Analysis*, Technical report 404, Information Security Group, ETH Zentrum, 2003.

[5] David A. Basin, S. Mödersheim, and L. Viganó, "An on-the-fly model-checker for security protocol analysis," in *8th European Symposium on Research in Computer Security - ESORICS 2003* (Einar Snekkenes and Dieter Gollmann, eds.), LNCS 2808, pp. 253–270, Springer-Verlag, 2003.

[6] M. Bellare, "A note on negligible functions," *Journal of Cryptology*, vol. 15, no. 4, pp. 271–284, 2002.

[7] M. Bellare, R. Canetti, and H. Krawczyk, "A modular approach to the design and analysis of authentication and key exchange protocols," in *30th ACM Symposium on the Theory of Computing - STOC 1998* (Jeffrey Vitter, ed.), pp. 419–428, ACM Press, 1998.

[8] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Advances in Cryptology – Eurocrypt 2000* (Bart Preneel, ed.), LNCS 1807, pp. 139–155, Springer-Verlag, 2000.

[9] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in *Advances in Cryptology - Crypto 1993* (Douglas R. Stinson, ed.), LNCS 773, pp. 110–125, Springer-Verlag, 1993.

[10] M. Bellare and P. Rogaway, "Provably secure session key distribution: the three party case," in *27th ACM Symposium on the Theory of Computing - STOC 1995* (F. Tom Leighton and Allan Borodin, eds.), pp. 57–66. ACM Press, 1995.

[11] S. Blake-Wilson, D. Johnson, and A. Menezes, "Key agreement protocols and their security analysis," in *6th IMA International Conference on Cryptography and Coding* (Michael Darnell, ed.), LNCS 1355, pp. 30–45, Springer-Verlag, 1997.

[12] S. Blake-Wilson and A. Menezes, "Security proofs for entity authentication and authenticated key transport protocols employing asymmetric techniques," in *Security Protocols Workshop* (Bruce Christianson,

A		$\mathcal{A}$		B
$x_a \in_R \mathbb{Z}_r^*$	$\xrightarrow{A_{KA} = x_a(s+b)P}$	Intercept		
		$x_E \in_E Z_r^*$		
		Impersonate A	$\xrightarrow{A_{KA} \cdot x_E}$	$x_b \in_R \mathbb{Z}_r^*$
		Intercept	$\xleftarrow{B_{KA} = x_b(s+a)P}$	
	$\xleftarrow{B_{KA} \cdot x_E}$	Impersonate B		

$$SK_A = \hat{e}(x_b(s+a)P \cdot x_E, A_{pri})^{x_a} = \hat{e}(P,P)^{x_a x_b x_E} = SK_B$$

Figure 5: Execution of the 2P-IDAKA protocol in the presence of a malicious adversary, $\mathcal{A}$

Bruno Crispo, T. Mark A. Lomas, and Michael Roe, eds.), LNCS 1361, pp. 137–158, Springer-Verlag, 1997.

[13] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 585–615, 2003.

[14] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels (Extended version available from `http://eprint.iacr.org/2001/040/`)," in *Advances in Cryptology - Eurocrypt 2001* (Birgit Pfitzmann, ed.), LNCS 2045, pp. 453–474, Springer-Verlag, 2001.

[15] L. Chen and C. Kudla, "Identity based authenticated key agreement protocols from pairings (Corrected version at `http://eprint.iacr.org/2002/184/`)," in *16th IEEE Computer Security Foundations Workshop - CSFW 2003*, pp. 219–233. IEEE Computer Society Press, 2003.

[16] K.-K. R. Choo, *Revisit of McCullagh–Barreto Two-Party ID-Based Authenticated Key Agreement Protocols*, Cryptology ePrint Archive, Report 2004/343, 2004. `http://eprint.iacr.org/2004/343/`.

[17] K.-K. R. Choo, *The Provably-Secure Key Establishment and Mutual Authentication Protocols Lounge*, `http://sky.fit.qut.edu.au/~choo/lounge.html`, 2005.

[18] K.-K. R. Choo, C. Boyd, and Y. Hitchcock, "Errors in computational complexity proofs for protocols," in *(Accepted to appear in) Advances in Cryptology - Asiacrypt 2005* (Bimal Roy eds.), LNCS, Springer-Verlag, 2005.

[19] K.-K. R. Choo, C. Boyd, and Y. Hitchcock, "Examining indistinguishability-based proof models for key establishment protocols," in *(Accepted to appear in) Advances in Cryptology - Asiacrypt 2005* (Bimal Roy eds.), LNCS, Springer-Verlag, 2005.

[20] K.-K. R. Choo, C. Boyd, and Y. Hitchcock, "On session key construction in provably secure protocols (Extended version available from `http://eprint.iacr.org/2005/206`)," in *1st International Conference on Cryptology in Malaysia - Mycrypt 2005* (Ed Dawson and Serge Vaudenay, eds.), LNCS 3715, pp. 116–131, Springer-Verlag, 2005.

[21] K.-K. R. Choo, C. Boyd, and Y. Hitchcock, "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, & Yeh–Sun Protocols (Extended version available from `http://eprints.qut.edu.au/perl/user_eprints?userid=51`)," *(To appear in) Journal of Computer Communications - Special Issue of Internet Communications Security*, 2005.

[22] K.-K. R. Choo, C. Boyd, Y. Hitchcock, and G. Maitland, "On session identifiers in provably secure protocols: the Bellare-Rogaway three-party key distribution protocol revisited (Extended version available from `http://eprint.iacr.org/2004/345`)," in *4th Conference on Security in Communication Networks - SCN 2004* (Blundo Carlo and Stelvio Cimato, eds.), LNCS 3352, pp. 352–367, Springer-Verlag, 2004.

[23] K.-K. R. Choo and Y. Hitchcock, "Security requirements for key establishment proof models: revisiting Bellare–Rogaway and Jeong–Katz–Lee Protocols (Extended version available from `http://sky.fit.qut.edu.au/~choo/publication.html`)," in *10th Australasian Conference on Information Security and Privacy - ACISP 2005* (Colin Boyd and Juan Manuel Gonzalez-Nieto, eds.), LNCS 3574, pp. 429–442, Springer-Verlag, 2005.

[24] Dorothy E. Denning and G. M. Sacco, "Timestamps in key distribution protocols," *ACM Journal of Communications*, vol. 24, no. 8, pp. 533–536, 1981.

[25] W. Diffie, Paul C. van Oorschot, and Michael J. Wiener, "Authentication and authenticated key exchange," *Journal of Designs, Codes and Cryptography*, vol. 2, pp. 107–125, 1992.

[26] B. Donovan, P. Norris, and G. Lowe, "Analyzing a library of security protocols using Casper and FDR," in *Workshop on Formal Methods and Security Protocols*, 1999.

[27] P. Janson and G. Tsudik, "Secure and minimal protocols for authenticated key distribution," *Computer Communications*, vol. 18, no. 9, pp. 645–653, 1995.

[28] H. Krawczyk, "HMQV: A high-performance secure Diffie-Hellman protocol (Extended version available from `http://eprint.iacr.org/2005/176/`),"

A		$\mathcal{A}$		B
$x_a \in_R \mathbb{Z}_r^*$	$\xrightarrow{A_{KA} = x_a(s+b)P}$	Intercept		
		$x_E \in_E Z_r^*$		
		Impersonate A	$\xrightarrow{A_{KE} = x_a(s+b)P + x_E(s+b)P}$	$x_b \in_R \mathbb{Z}_r^*$
		Intercept	$\xleftarrow{B_{KA} = x_b(s+a)P}$	
	$\xleftarrow{B_{KE} = x_b(s+a)P + x_E(s+a)P}$	Impersonate B		

$$SK_A = e(P,P)^{x_a} e(B_{KE}, A_{pri}) = e(P,P)^{x_a + x_b + x_E} = e(P,P)^{x_b} e(A_{KE}, B_{pri}) = SK_B$$

Figure 6: Execution of the variant protocol in the presence of a malicious adversary, $\mathcal{A}$

in *Advances in Cryptology - Crypto 2005* (Victor Shoup, ed.), LNCS 3621, Springer-Verlag, 2005.

[29] Philip D. MacKenzie and R. Swaminathan, "Secure network authentication with password identification," Submitted to the IEEE P1363 Working Group, 1999. `http://cm.bell-labs.com/who/philmac/bib.html`

[30] N. McCullagh and Paulo S. L. M. Barreto, "A new two-party identity-based authenticated key agreement (Extended version available from `http://eprint.iacr.org/2004/122/`)," in *Cryptographers' Track at RSA Conference - CT-RSA 2005* (Alfred John Menezes, ed.), LNCS 3376, pp. 262–274, Springer-Verlag, 2005.

[31] J. Nam, S. Kim, and D. Won, *Attacks on Bresson-Chevassut-Essiari-Pointcheval's Group Key Agreement Scheme*, Cryptology ePrint Archive, Report 2004/251, 2004. `http://eprint.iacr.org/2004/251/`.

[32] T. Okamoto and D. Pointcheval, "The gap-problems: a new class of problems for the security of cryptographic schemes," in *2001 International Workshop on Practice and Theory in Public Key Cryptography - PKC 2001* (Kwangjo Kim, ed.), LNCS 1992, Springer-Verlag, 2001.

[33] K. Shim, "Cryptanalysis of mutual authentication and key exchange for low power wireless communications," *IEEE Communications Letters*, vol. 7, no. 5, pp. 248–250, 2003.

[34] V. Shoup, "OAEP reconsidered," in *Advances in Cryptology - Crypto 2001* (Joe Kilian, ed.), LNCS 2139, pp. 239–259, Springer-Verlag, 2001.

[35] Z. Wan and S. Wang, "Cryptanalysis of two password-authenticated key exchange protocols," in *9th Australasian Conference on Information Security and Privacy - ACISP 2004* (Huaxiong Wang, Josef Pieprzyk, and Vijay Varadharajan, eds.), LNCS 3108, Springer-Verlag, 2004.

[36] Jeannette M. Wing, "A symbiotic relationship between formal methods and security," in *Workshops on Computer Security, Fault Tolerance, and Software Assurance: From Needs to Solution*. IEEE Computer Press, 1998.

[37] Duncan S. Wong and Agnes H. Chan, "Efficient and mutually authenticated key exchange for low power computing devices," in *Advances in Cryptology - Asiacrypt 2001* (Colin Boyd, ed.), LNCS 2248, pp. 172–289, Springer-Verlag, 2001.

[38] G. Xie, *Cryptanalysis of Noel McCullagh and Paulo S. L. M. Barreto Two-Party Identity-Based Key Agreement*, Cryptology ePrint Archive, Report 2004/308, 2004. `http://eprint.iacr.org/2004/308/`.

[39] F. Zhang, R. Safavi-Naini, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," in *Public Key Cryptography - PKC 2004* (Feng Bao, Robert H. Deng, and Jianying Zhou, eds.), LNCS 2947, pp. 277–290, Springer-Verlag, 2004.

[40] M. Zhang, "Breaking an improved password authenticated key exchange protocol for imbalanced wireless networks," *IEEE Communications Letters*, vol. 9, no. 3, pp. 276–278, 2005.

Kim-Kwang Raymond Choo received his BSc Maths, BAppSci (Hons) Industrial & Applied Maths, and Master of Information Technology degrees in Dec 2000, Dec 2002, and May 2002 respectively. He is currently a full-time Ph.D. candidate with Information Security Institute, Queensland University of Technology, Australia; and a part-time MBA student with the University of Queensland. His research interests include formal specification and analysis of mutual authentication and/or key establishment protocols, and provably-secure protocols.