SCIS 2012 The 29th Symposium on
Cryptography and Information Security
Kanazawa, Japan, Jan. 30 - Feb. 2, 2012
The Institute of Electronics,
Information and Communication Engineers

非対称ペアリングを用いたIDベース認証鍵交換方式における id-eCK安全性の考察

A study on id-eCK security of ID-based authenticated key exchange using asymmetric pairing

鈴木 幸太郎* 藤岡 淳 * 米山 一樹 * 小林 鉄太郎 *
Koutarou Suzuki Atsushi Fujioka Kazuki Yoneyama Tetsutaro Kobayashi
星野 文学 *
Fumitaka Hoshino

あらまし ID を用いて相互認証し鍵交換を行う ID ベース認証鍵交換（ID-based authenticated key exchange）に関して、非対称ペアリングを用いて ID ベース eCK（ID-based extended Canetti-Krawczyk）安全性を実現する方法について考察する。ID ベース eCK 安全性は、公開鍵ベースの eCK 安全性を ID ベース認証鍵交換に適用したものであり、master secret key、static secret key、ephemeral secret key の任意の非自明な組合せの漏洩に対して安全性を保証することができるため、ID ベース認証鍵交換方式は ID ベース eCK 安全性を満たすことが望まれる。また、非対称ペアリングは、対称ペアリングより計算効率のよいパラメータが取れるため、非対称ペアリングを用いて ID ベース認証鍵交換方式を構成することが望まれる。しかし、従来の ID ベース eCK 安全性を実現する ID ベース認証鍵交換方式は、対称ペアリングを必要としており、より効率のよい非対称ペアリングを用いて eCK 安全性を実現する方式は知られていなかった。本研究では、非対称ペアリングを用いて ID ベース eCK 安全性な ID ベース認証鍵交換方式を実現する際に問題となる点について考察し、ID ベース eCK 安全性な ID ベース認証鍵交換方式を提案する。

キーワード ID ベース認証鍵交換、ID ベース eCK 安全性、非対称ペアリング

1 はじめに

認証鍵交換プロトコルとは、2 人のユーザが安全でない通信路を介して秘密裏に同一の session key を共有するプロトコルである。従来の認証鍵交換は、PKI に登録された公開鍵に対応する秘密鍵を持っていることを認証の条件とするプロトコルが一般的であったが、近年では、ID ベース暗号技術の成熟に伴い、ユーザの ID に対応する秘密鍵を持っていることを認証の条件とする ID ベース認証鍵交換（ID-based authenticated key exchange）の研究が行われている。ID ベース認証鍵交換では、各ユーザは鍵生成センタ（KGC）と呼ばれる信頼できる機関に、自分の ID に対応する秘密鍵（static secret key）を発行してもらう必要がある。KGC は、KGC だけが持つ master secret key を元にユーザの秘密鍵発行を行う。ユーザは、鍵交換セッションごとに一時的な秘密情報（ephemeral secret key）を生成し、それを元にセッション内のメッセージをやり取りする。

ID ベース認証鍵交換の安全性モデルは、PKI ベース認証鍵交換の安全性モデル [2, 1, 4, 9, 5, 6] を ID ベース認証鍵交換用に変形することによって得られる。現在、ID ベース認証鍵交換の最も強い安全性モデルの 1 つとして、ID ベース eCK 安全性 [8] が知られている。ID ベース eCK 安全性は、秘密情報の漏洩を利用するような強力な攻撃（例：key-compromised impersonation 攻撃）に対する安全性を捉えており、master secret key、static secret key、ephemeral secret key の任意の非自明な組合せの漏洩に対して安全性を保証することができる。よって、ID ベース認証鍵交換は ID ベース eCK 安全性を満たすことが望ましい。

多くの ID ベース認証鍵交換方式が提案されているが [3]、ID ベース eCK 安全性を満たす ID ベース認証

* NTT 情報流通プラットフォーム研究所, 180-8585 東京都武蔵野市緑町 3-9-11, NTT Information Sharing Platform Laboratories, 3-9-11 Midori-cho, Musashino-shi, Tokyo, 180-8585 Japan, { suzuki.koutarou, fujioka.atsushi, yoneyama.kazuki, kobayashi.tetsutaro, hoshino.fumitaka } @lab.ntt.co.jp

鍵交換としては、Huang らの方式 [8] と Fujioka らの方式 [7] がある。これらの方式は、対称ペアリングを用いて構成されており、対称ペアリング上の求解問題の困難性を根拠として安全性証明が行われている。しかし、対称ペアリングは取りうるパラメータが制限されており、非対称ペアリングに比べて計算効率のよいパラメータが取れないという問題がある。

本研究では、非対称ペアリングを用いて ID ベース eCK 安全な ID ベース認証鍵交換方式を構成するための方法について考察する。まず、従来の対称ペアリングを用いた方式を、非対称ペアリングを用いた方式に変換する際に問題となる点について考察する。次に、上記の考察結果を踏まえて、非対称ペアリングを用いた ID ベース eCK 安全性を満たす ID ベース認証鍵交換方式を提案する。

2 ID ベース eCK 安全性

本章では、Huang ら [8] により提案された、ID ベース認証鍵交換に対する ID ベース eCK 安全性の定義を示す。ID ベース eCK 安全性は、LaMacchia ら [9] による eCK 安全性を、ID ベースに拡張したものである。

Session. ここでは、2-pass の ID ベース認証鍵交換の場合について記述する。ユーザを U_i、ユーザ U_i の ID を ID_i、ユーザ U_i の ephemeral public key を X_i と書く。プロトコル識別子を Π、ロール識別子を $\mathcal{I}, \mathcal{R}$ と書く。

（片方のユーザの）プロトコルの実行を *session* という。*session* は、$(\Pi, \mathcal{I}, ID_A, ID_B)$ または $(\Pi, \mathcal{R}, ID_A, ID_B, X_B)$ を受信することで開始される。U_A が $(\Pi, \mathcal{I}, ID_A, ID_B)$ を受信した場合、U_A を *initiator* という。U_A が $(\Pi, \mathcal{R}, ID_A, ID_B, X_B)$ を受信した場合、U_A を *responder* という。

U_A が *initiator* の場合、U_A は、ephemeral public key X_A を計算して $(\Pi, \mathcal{I}, ID_A, ID_B, X_A)$ を送信し、$(\Pi, \mathcal{R}, ID_A, ID_B, X_A, X_B)$ を受信し、session key を計算する。

U_A が *responder* の場合、U_A は、ephemeral public key X_A を計算して $(\Pi, \mathcal{R}, ID_A, ID_B, X_B, X_A)$ を送信し、session key を計算する。

実行順序が渡ると U_A は受信したメッセージに ephemeral public key X_A を付け加え、送信メッセージとして送る。もし U_A が *responder* なら、session key を計算する。もし U_A が *initiator* であり、$(\Pi, \mathcal{I}, ID_A, ID_B)$ によって最初の実行順序を渡されたならば、$(\Pi, \mathcal{R}, ID_A, ID_B, X_A, X_B)$ によって次の実行順序を渡された後、session key を計算する。

メッセージの 3 つ目の要素が ID_A なら、U_A をそのセッションの *owner* と呼び、4 つ目の要素が ID_A なら、*peer* と呼ぶ。*owner* が session key を計算し終わったら、そのセッションは *completed* であるとする。

もし U_A が *initiator* なら、そのセッションは $\mathtt{sid} = (\Pi, \mathcal{I}, ID_A, ID_B, X_A, \times)$、または $\mathtt{sid} = (\Pi, \mathcal{I}, ID_A, ID_B, X_A, X_B)$ によって識別される。もし U_A が *responder* なら、そのセッションは $\mathtt{sid} = (\Pi, \mathcal{R}, ID_A, ID_B, X_B, X_A)$ によって識別される。セッション $(\Pi, \mathcal{I}, ID_A, ID_B, X_A, X_B)$ に対して、セッション $(\Pi, \mathcal{R}, ID_B, ID_A, X_A, X_B)$ を *matching session* と呼ぶ。ロール識別子は X_A と X_B の順序によって定まるので、以後 $\mathcal{I}$ と $\mathcal{R}$ を省略する。

Adversary. 攻撃者 $\mathcal{A}$ は確率的多項式時間チューリング機械としてモデル化され、実行順序の受け渡しを含むユーザ間の全ての通信を Send(message) クエリを用いて制御する。ユーザに与えるメッセージは、(Π, ID_A, ID_B) か (Π, ID_A, ID_B, X_A) か $(\Pi, ID_A, ID_B, X_A, X_B)$ のいずれかの形を取る。それぞれのユーザは与えられたメッセージに応じたレスポンスを攻撃者に返す。攻撃者は KGC とユーザ間の通信は制御できないことに注意。

ユーザの秘密情報に攻撃者は原則としてアクセスできないが、秘密情報の漏洩を考慮するために以下のような攻撃者用クエリを定義する。

- SessionKeyReveal(sid) セッション sid の session key がすでに生成されているならば、攻撃者は session key を得る。
- EphemeralKeyReveal(sid) 攻撃者はセッション sid に付随する ephemeral secret key を得る。
- StaticKeyReveal(ID_i) 攻撃者はユーザ U_i の static secret key を得る。
- MasterKeyReveal() 攻撃者は KGC の master secret key を得る。
- EstablishParty(ID_i) 攻撃者はユーザ U_i の static secret key を KGC に発行させ、このユーザを完全に制御下に置く。もしあるユーザが EstablishParty(ID_i) によって鍵発行を受けたならば、そのユーザを *dishonest* と呼び、そうでなければ *honest* と呼ぶ。すなわち、このクエリは悪意ある内部者を考慮している。

Freshness. 以下のように freshness を定義する。

Definition 1 (freshness) $\mathtt{sid}^*$ を honest なユーザ U_A が owner（honest なユーザ U_B が peer）であるような completed なセッションのセッション識別子とする。matching session が存在するならば、$\overline{\mathtt{sid}^*}$ を $\mathtt{sid}^*$ の matching session のセッション識別子とする。もし次の条件のいずれにも該当しないならば、$\mathtt{sid}^*$ を *fresh* であると定義する。

1. $\mathcal{A}$ が SessionKeyReveal($\mathtt{sid}^*$) クエリ、または SessionKeyReveal($\overline{\mathtt{sid}^*}$) クエリを発している。（$\overline{\mathtt{sid}^*}$ が存在する場合）

2. $\overline{\mathtt{sid}^*}$ が存在し $\mathcal{A}$ が次のクエリのいずれかを発している。
   - StaticKeyReveal(ID_A) クエリと EphemeralKeyReveal($\mathtt{sid}^*$) クエリの両方、または
   - StaticKeyReveal(ID_B) クエリと EphemeralKeyReveal($\overline{\mathtt{sid}^*}$) クエリの両方。

3. $\overline{\mathtt{sid}^*}$ が存在せず $\mathcal{A}$ が次のクエリのいずれかを発している。
   - StaticKeyReveal(ID_A) クエリと EphemeralKeyReveal($\mathtt{sid}^*$) クエリの両方、または
   - StaticKeyReveal(ID_B) クエリ。

$\mathcal{A}$ が MasterKeyReveal() クエリを発したときは、StaticKeyReveal(ID_A) クエリと StaticKeyReveal(ID_B) クエリの両方を発したとみなす。

Security Experiment. 攻撃者 $\mathcal{A}$ は適応的に選んだ ID に対応する *honest* なユーザ集合によるプロトコル実行を対象とし、上記のクエリを任意に組み合わせた攻撃を行うものとする。ゲームの中で、攻撃者 $\mathcal{A}$ は特別なクエリとして Test($\mathtt{sid}^*$) クエリを発することができる。Test($\mathtt{sid}^*$) クエリによって、攻撃者は $\mathtt{sid}^*$ の session key かランダムな鍵のいずれかをそれぞれ 1/2 の確率で得る。Test($\mathtt{sid}^*$) クエリを発した後も、攻撃者 $\mathcal{A}$ が受け取った鍵がランダムか否かを予想した結果を出力するまでゲームは続行する。もし $\mathtt{sid}^*$ が最後まで fresh、かつ $\mathcal{A}$ の予想が正しい場合、攻撃者はゲームに *win* したと定義する。

Definition 2 (security) *ID* ベース認証鍵交換プロトコル Π に対する攻撃ゲームにおける攻撃者 $\mathcal{A}$ のアドバンテージを次のように定義する。

$$\mathrm{Adv}_{\Pi}^{\text{ID-AKE}}(\mathcal{A}) = \Pr[\mathcal{A}\ wins] - \frac{1}{2}.$$

次の条件が満たされたとき、Π は *ID* ベース *eCK* モデルにおいて安全な *ID* ベース認証鍵交換という。

1. もし *2* 人の honest なユーザが completed な matching session を実行したならば、セキュリティパラメータ κ に対して無視出来る確率を除いて両者は同じ *session key* を計算する。

2. 任意の確率的多項式時間攻撃者 $\mathcal{A}$ について、セキュリティパラメータ κ に対して $\mathrm{Adv}_{\Pi}^{\text{ID-AKE}}(\mathcal{A})$ が無視出来る。

3 非対称ペアリングを用いた ID ベース認証鍵交換方式

本章では、まず、従来の対称ペアリングを用いた方式を、非対称ペアリングを用いた方式に変換する際に問題となる点について考察する。次に、上記の考察結果を踏まえて、非対称ペアリングを用いた ID ベース eCK 安全性を満たす ID ベース認証鍵交換方式を提案する。

3.1 非対称ペアリングを用いる際の問題点

以下では、ID ベース eCK 安全性を満たす対称ペアリングを用いた Fujioka らの方式 [7] を、非対称ペアリングを用いた方式に変換する際の問題点について述べる。

G、G_T を素数位数 q の巡回群とし、g、$g_T = e(g,g)$ をこれらの巡回群の生成元とし、$e : G \times G \to G_T$ を対称ペアリングとする。$H : \{0,1\}^* \to \{0,1\}^\kappa$、$H_1 : \{0,1\}^* \longrightarrow G$、をハッシュ関数とする。

Fujioka らの方式 [7] では、ユーザ U_A は以下のようにユーザ U_B と同じ shared value σ_i を計算することができ、これによりユーザ U_A とユーザ U_B は共通の session key $K = H(\sigma_1, \sigma_2, \sigma_3, ...)$ を共有することができる。

$$\sigma_1 = e(D_A, Q_B) = g_T^{z q_A q_B} \in G_T,$$

$$\sigma_2 = e(D_A Z^{x_A}, Q_B X_B) = g_T^{z(q_A + x_A)(q_B + x_B)} \in G_T,$$

$$\sigma_3 = (X_B)^{x_A} = g^{x_A x_B} \in G.$$

ただし、$Z = g^z \in G$ を master public key、$Q_i = H_1(ID_i) = g^{q_i} \in G$ を ID のハッシュ値、$D_i = Q_i^z = g^{z q_i} \in G$ を static secret key、$X_i = g^{x_i} \in G$ を ephemeral public key、とする。

上記の Fujioka らの方式 [7] を、非対称ペアリング $e : G_1 \times G_2 \to G_T$ を用いて実現することを考える。まず、σ_1 を計算するためには、$D_A, Q_A \in G_1$, $D_B, Q_B \in G_2$ となる必要がある。さらに、σ_2 を計算するためには、$X_A \in G_1$, $X_B \in G_2$ となる必要がある。この場合に、ユーザ U_A は $\sigma_3^2 = X_B^{x_A} \in G_2$ を計算し、ユーザ U_B は $\sigma_3^1 = X_A^{x_B} \in G_1$ を計算する。しかし、これらの値は違う群の元であるため一致しないので、ユーザ U_A とユーザ U_B は共通の session key K を共有することができない。

このように、既存の対称ペアリングを用いた Fujioka らの方式 [7] を、単純に非対称ペアリングを用いた方式に書き直しただけでは上手くいかないことが分かる。提案方式では、ephemeral public key を $X_i^1 \in G_1$ と $X_i^2 \in G_2$ との 2 つにし、対応する 2 つの shared value $\sigma_3^1 \in G_1$ と $\sigma_3^2 \in G_2$ とを計算することがで、この問題を解決している。

3.2 提案 ID ベース認証鍵交換方式

以下では、非対称ペアリングを用いた ID ベース認証鍵交換方式を提案する。提案方式は、gap BDH 仮定とランダムオラクルモデルのもとで、ID ベース eCK 安全性を満たす。

κ をセキュリティパラメータとする。q を κ-bit の素数とする。G_1、G_2、G_T を位数 q の巡回群とし、g_1、g_2、$g_T = e(g_1, g_2)$ をこれらの巡回群の生成元とし、$e : G_1 \times G_2 \to G_T$ を非対称ペアリングとする。$H : \{0,1\}^* \to \{0,1\}^\kappa$、$H_1 : \{0,1\}^* \longrightarrow G_1$、$H_2 : \{0,1\}^* \longrightarrow G_2$、をハッシュ関数とする。$\Pi$ をプロトコル識別子とする。

以下に、提案 ID ベース認証鍵交換方式を示す。鍵生成センタ KGC は、以下のように master key 生成を行う。

1. KGC randomly selects master secret key $z \in \mathbb{Z}_q$, and publishes master public keys $Z^1 = g_1^z \in G_1$ and $Z^2 = g_2^z \in G_2$.

鍵生成センタ KGC は、以下のようにユーザ U_i の ststic secret key 生成を行う。

1. User U_i with identity ID_i is assigned static secret keys $D_i^1 = (Q_i^1)^z = g_1^{zq_i} \in G_1$ and $D_i^2 = (Q_i^2)^z = g_2^{zq_i} \in G_2$, where $Q_i^1 = H_1(ID_i) = g_1^{q_i} \in G_1$ and $Q_i^2 = H_2(ID_i) = g_2^{q_i} \in G_2$.

ユーザ U_A とユーザ U_B は、以下のようにして鍵交換を行う。以下では、U_A は session initiator であり、ユーザ U_B は session responder である。

1. U_A selects a random ephemeral secret key $x_A \in_U \mathbb{Z}_q$, computes the ephemeral public key $X_A^1 = g_1^{x_A}$ and $X_A^2 = g_2^{x_A}$, and sends $(\Pi, ID_B, ID_A, (X_A^1, X_A^2))$ to U_B.

2. Upon receiving $(\Pi, ID_B, ID_A, (X_A^1, X_A^2))$, U_B selects a random ephemeral secret key $x_B \in_U \mathbb{Z}_q$, computes the ephemeral public key $X_B^1 = g_1^{x_B}$ and $X_B^2 = g_2^{x_B}$, and sends $(\Pi, ID_A, ID_B, (X_A^1, X_A^2), (X_B^1, X_B^2))$ to U_A.

   U_B computes the following shared values

$$\sigma_1 = e(Q_A^1, D_B^2) \in G_T,$$

$$\sigma_2 = e(Q_A^1 X_A^1, D_B^2 (Z^2)^{x_B}) \in G_T,$$

$$\sigma_3^1 = (X_A^1)^{x_B} \in G_1,$$

$$\sigma_3^2 = (X_A^2)^{x_B} \in G_2,$$

   computes the session key $K = H(\sigma_1, \sigma_2, \sigma_3^1, \sigma_3^2, \Pi, ID_A, ID_B, (X_A^1, X_A^2), (X_B^1, X_B^2))$, and completes the session.

3. Upon receiving $(\Pi, ID_A, ID_B, (X_A^1, X_A^2), (X_B^1, X_B^2))$, U_A checks if U_A has sent (Π, ID_B, ID_A, X_A) to U_B or not, and aborts the session if not.

   U_A computes the following shared values

$$\sigma_1 = e(D_A^1, Q_B^2) \in G_T,$$

$$\sigma_2 = e(D_A^1 (Z^1)^{x_A}, Q_B^2 X_B^2) \in G_T,$$

$$\sigma_3^1 = (X_B^1)^{x_A} \in G_1,$$

$$\sigma_3^2 = (X_B^2)^{x_A} \in G_2,$$

   computes the session key $K = H(\sigma_1, \sigma_2, \sigma_3^1, \sigma_3^2, \Pi, ID_A, ID_B, (X_A^1, X_A^2), (X_B^1, X_B^2))$, and completes the session.

ユーザ U_A とユーザ U_B は、以下のように同じ shared value σ_i を計算することができるので、共通の session key K を共有することができる。

$$\sigma_1 = e(D_A^1, Q_B^2) = g_T^{zq_Aq_B} \in G_T,$$

$$\sigma_2 = e(D_A^1 (Z^1)^{x_A}, Q_B^2 X_B^2) = g_T^{z(q_A+x_A)(q_B+x_B)} \in G_T,$$

$$\sigma_3^1 = (X_B^1)^{x_A} = g_1^{x_Ax_B} \in G_1,$$

$$\sigma_3^2 = (X_B^2)^{x_A} = g_2^{x_Ax_B} \in G_2.$$

提案方式は、2 回のペアリング計算と、3 回の指数関数計算（ephemeral public key の計算を含めて）を必要とする。

以下では、提案方式の安全性証明に必要となる gap BDH 仮定について説明する。BDH 関数 CBDH : $G_1^3 \times G_2^3 \to G_T$ を、$\mathrm{CBDH}(g_1^u, g_1^v, g_1^w, g_2^u, g_2^v, g_2^w) = e(g_1, g_2)^{uvw}$ と定義する。BDH 判定述語 $\mathrm{DBDH}^{a,b,c} : G_a \times G_b \times G_c \times G_T \to \{0,1\}$ $(a, b, c \in \{1,2\})$ を、$(g_a^u, g_b^v, g_c^w, e(g,g)^x)$ を入力とし、$uvw = x \bmod q$ のとき 1 を出力し、そうでないときに 0 を出力すると定義する。

攻撃者 $\mathcal{A}$ は、ランダムに選ばれた $U_1, V_1, W_1 \in_R G_1$, $U_2, V_2, W_2 \in_R G_2$ を入力とし、$\mathrm{DBDH}^{*,*,*}(\cdot,\cdot,\cdot,\cdot)$ にオラクルアクセスし、$\mathrm{CBDH}(U_1, V_1, W_1, U_2, V_2, W_2) \in G_T$ を計算する。攻撃者 $\mathcal{A}$ のアドバンテージを、以下のように定義する。

$$Adv^{\mathrm{gapBDH}}(\mathcal{A}) = \Pr[U_1, V_1, W_1 \in_R G_1, U_2, V_2, W_2 \in_R G_2,$$

$$\mathcal{A}^{\mathrm{DBDH}^{*,*,*}(\cdot,\cdot,\cdot,\cdot)}(U_1, V_1, W_1, U_2, V_2, W_2)$$

$$= \mathrm{CBDH}(U_1, V_1, W_1, U_2, V_2, W_2)],$$

ここで、確率は $U_1, V_1, W_1 \in_R G_1$, $U_2, V_2, W_2 \in_R G_2$ と攻撃者 $\mathcal{A}$ のランダムテープに関してとるものとする。

gap BDH 仮定を以下のように定義する。

Definition 3 (gap BDH assumption) 任意の確率的多項式時間攻撃者 $\mathcal{A}$ に対して、攻撃者 $\mathcal{A}$ のアドバンテージが無視できるとき、G_1, G_2, G_T が *gap BDH* 仮定を満たすという。

提案 ID ベース認証鍵交換方式は、gap BDH 仮定とランダムオラクルモデルのもとで、ID ベース eCK 安全性を満たす。

Theorem 4 G_1, G_2, G_T が *gap BDH* 仮定を満たし H, H_1, H_2 がランダムオラクルであるとき、提案 *ID* ベース認証鍵交換方式は *ID* ベース *eCK* 安全性を満たす。

4 おわりに

本研究では、非対称ペアリングを用いて ID ベース eCK 安全な ID ベース認証鍵交換方式を構成するための方法について考察した。まず、従来の対称ペアリングを用いた方式を非対称ペアリングを用いた方式に変換する際に問題となる点について考察し、次に、非対称ペアリングを用いた ID ベース eCK 安全性を満たす ID ベース認証鍵交換方式を提案した。

参考文献

[1] S. Blake-Wilson, D. Johnson, and A. Menezes, "Key Agreement Protocols and Their Security Analysis," Darnell, M. (ed.) IMA CC '97, LNCS, vol. 1355, pp. 30–45. Springer, Heidelberg (1997)

[2] M. Bellare and P. Rogaway, "Entity authentication and key distribution," Crypto 1993, LNCS 773, pp. 110–125, 1993.

[3] L. Chen, Z. Cheng, and N. P. Smart, "Identity-based key agreement protocols from pairings," *International Journal of Information Security*, 6(4):213–241, 2007.

[4] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," Eurocrypt 2001, LNCS 2045, pp. 453–474, 2001.

[5] C. J. F. Cremers, "Session-state Reveal is Stronger than Ephemeral Key Reveal: Attacking the NAXOS Authenticated Key Exchange Protocol," In: Abdalla, M., Pointcheval, D., Fouque, P.-A., Vergnaud, D. (eds.) ACNS 2009. LNCS, vol. 5536, pp. 20–33. Springer, Heidelberg (2009)

[6] C. J. F. Cremers, "Examining Indistinguishability-Based Security Models for Key Exchange Protocols: The Case of CK, CK-HMQV, and eCK," In: 6th ACM Symposium on Information, Computer and Communications Security, pp. 80–91. ACM, New York (2011)

[7] A. Fujioka, K. Suzuki, and B. Ustaoğlu, "Ephemeral key leakage resilient and efficient ID-AKEs that can share identities, private and master keys," Pairing 2010, LNCS 6487, pp. 187–205, 2010.

[8] H. Huang and Z. Cao, "An id-based authenticated key exchange protocol based on bilinear diffie-hellman problem," In R. Safavi-Naini and V. Varadharajan, editors, *ASIACCS '09: Proceedings of the 2009 ACM symposium on Information, computer and communications security*, pages 333–342, New York, NY, USA, 2009.

[9] B. LaMacchia, K. Lauter, and A. Mityagin, "Stronger security of authenticated key exchange," ProvSec 2007, LNCS 4784, pp. 1–16, 2007.