On the Relations Between Diffie-Hellman and ID-Based Key Agreement from Pairings *

Shengbao Wang

New Star Institute of Applied Technology, China
shengbaowang@gmail.com

Abstract. This paper studies the relationships between the traditional Diffie-Hellman key agreement protocol and the identity-based (ID-based) key agreement protocol from pairings.
For the Sakai-Ohgishi-Kasahara (SOK) ID-based key construction, we show that identical to the Diffie-Hellman protocol, the SOK key agreement protocol also has three variants, namely *ephemeral*, *semi-static* and *static* versions. Upon this, we build solid relations between authenticated Diffie-Hellman (Auth-DH) protocols and ID-based authenticated key agreement (IB-AK) protocols, whereby we present two *substitution rules* for this two types of protocols. The rules enable a conversion between the two types of protocols. In particular, we obtain the *real* ID-based version of the well-known MQV (and HMQV) protocol.
Similarly, for the Sakai-Kasahara (SK) key construction, we show that the key transport protocol underlining the SK ID-based encryption scheme (which we call the "SK protocol") has its non-ID counterpart, namely the Hughes protocol. Based on this observation, we establish relations between corresponding ID-based and non-ID-based protocols. In particular, we propose a highly enhanced version of the McCullagh-Barreto protocol.

Key words. Authenticated Diffie-Hellman, SOK protocol, ID-based key agreement, ID-MQV, eMB

1 Introduction

In 2005, Boyd and Choo [7] and Wang *et al.* [35] noticed that there are some similarities between (pairing-based) ID-based and non-ID-based authenticated key agreement (AK) protocols. This study further investigate this observation. Interestingly, we discover much more than those researchers previously might imagined.

1.1 Proposed Novel Protocols

We discover some important *substitution rules* (see Table 3, 4) between the two different types of protocols. The rules enable a useful conversion between the authenticated version of the two types of protocols. By applying these rules, we present three novel protocols (namely, the protocols which are highlighted in bold in Table 1 and 2) which possesses remarkable performance and security.

1. The real ID-based version of the MQV (and, HMQV) protocol — ID-MQV. (See Fig. 12.)
2. The enhanced MB (McCullagh–Barreto) ID-based protocol — eMB. (See Fig. 16.)
3. The non-ID-based version of the SYL protocol — nID-SYL (See Appendix A, Fig. 18).

* First version, January 2008; This version (July 2009) is a minor revison.

Table 1. Corresponding Protocols (non-ID-Based *vs.* ID-Based)

Protocol Type	Prot. Message	Auth. DH Protocols	$\Leftrightarrow$	ID-Based Protocols
A0	$T_A = xP$	MTI/A0	$\Leftrightarrow$	Smart [31]
Enhanced A0		(H)MQV	$\Leftrightarrow$	**ID-MQV** (See Fig. 12)
A1	$T_A = xQ_A$	MTI/A1	$\Leftrightarrow$	Chen–Kudla [11]
Enhanced A1		(H)MQV-1	$\Leftrightarrow$	Wang [33], Chow–Choo [10]
C0	$T_A = xQ_B$	MTI/C0	$\Leftrightarrow$	MB-1 [20]
Enhanced C0		ECKE-1N [37]	$\Leftrightarrow$	**eMB** (See Fig. 16)
B0		MTI/B0	$\Leftrightarrow$	MB-2 [21]
C1	$T_A = xF_{AB}$	MTI/C1	$\Leftrightarrow$	Scott [26]
Enhanced C1		Enhanced MTI/C1 (See Fig. 19)	$\Leftrightarrow$	Open Problem!

Table 2. Corresponding Protocols (Broken and Repaired Ones)

Protocol Type	Protocol Message	Auth. DH Protocols	$\Leftrightarrow$	ID-Based Protocols
A0 Variant-1	$T_A = xP$	Reduced MQV	$\Leftrightarrow$	Shim [28]
Repaired Protocol		**nID-SYL** (See Fig. 18)	$\Leftrightarrow$	SYL [40]
C0 Variant-1	$T_A = xQ_B$	$K = (x + y + xy)P$	$\Leftrightarrow$	Xie [39]
Repaired Protocol		$K = (x + y)P \| xyP$	$\Leftrightarrow$	LYL [19]

2 Preliminaries

2.1 Bilinear Pairings

Let $\mathbb{G}_1$ denotes an additive group of prime order q and $\mathbb{G}_2$ a multiplicative group of the same order. We let P denote a generator of $\mathbb{G}_1$. For us, an admissible pairing is a map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ with the following properties:

1. The map e is bilinear: given $Q, R \in \mathbb{G}_1$ and $a, b \in Z_q^*$, we have $e(aQ, bR) = e(Q, R)^{ab}$.
2. The map e is non-degenerate: $e(P, P) \neq 1_{\mathbb{G}_2}$.
3. The map e is efficiently computable.

Typically, the map e will be derived from either the Weil or Tate pairing on an elliptic curve over a finite field.

3 Three Versions of the SOK Protocol and the Substitution Rules

We first focus on the SOK ID-based key setting [32]. We show that the *static* SOK protocol from [32] has two more variants, *i.e.*, the *semi-static* and *ephemeral* SOK protocols.

Note that the figures given in the rest of the paper are all self-explaining.

3.1 Static DH and the SOK-NIKD Protocols

As observed by Boyd, Mao and Paterson [4] and Ryu *et al.* [25], the two *non-interactively* shared static secret from the Diffie-Hellman protocol [12] and the SOK non-interactive ID-based key distribution (SOK-NIKD) protocol [32] are $F_{DH} = abP$ and $F_{SOK} = e(Q_A, Q_B)^s$, respectively.

Alice		**Bob**
long-term private/public key pair: $\langle a, Q_A = aP\rangle$		long-term private/public key pair: $\langle b, Q_B = bP\rangle$
	$cert_A \dashrightarrow$	
	$\dashleftarrow cert_B$	
$F_{DH} = \mathbf{aQ_B} = abP$		$F_{DH} = bQ_A = abP$

Fig. 1. The Static DH Protocol [12]

Alice		**Bob**
long-term private/public key pair: $\langle S_A = sQ_A, Q_A = H(ID_A)\rangle$		long-term private/public key pair: $\langle S_B = sQ_B, Q_B = H(ID_B)\rangle$
	$ID_A \dashrightarrow$	
	$\dashleftarrow ID_B$	
$F_{SOK} = \mathbf{e(S_A, Q_B)} = e(Q_A, Q_B)^s$		$F_{SOK} = \mathbf{e(S_B, Q_A)} = e(Q_A, Q_B)^s$

Fig. 2. The SOK-NIKD Protocol [32] — Static SOK

Important observation #1: $aQ_B \longrightarrow e(S_A, Q_B)$.

3.2 Semi-Static and Ephemeral SOK Protocols

The Semi-Static SOK Protocol It is well-known that the ElGamal encryption scheme [13] is derived from the semi-static (or half-static, half-ephemeral) Diffie-Hellman protocol [22]. Based on this seemingly obvious relation, we find that the Boneh-Franklin ID-based encryption (IBE) [3, 27] is derived from the semi-static SOK protocol (presented in Fig. 3). Note that Paterson and Srinivasan [24] also, independently, noticed the relation. However, they do not give the term "semi-static SOK protocol" explicitly (let alone the ephemeral SOK) and only uses the static SOK protocol, *i.e.* the SOK-NIKD protocol. We stress that the explicit classification of the SOK protocol, corresponding to the three version of the Diffie-Hellman protocol, is essential for the main result of this paper.

In the rest of the paper, P_0 stands for the public key of the private key generator (PKG), with $P_0 = sP$ and s being the master private key of the PKG.

Alice		**Bob**
(Alice has no static keys.)		long-term private/public key pair: $\langle S_B = sQ_B, Q_B = H(ID_B) \rangle$
$x \in_R Z_q^*$ $T_A = xP$		
	$\xrightarrow{T_A}$	
	$\dashleftarrow ID_B$	
$F_{sSOK} = e(P_0, xQ_B)$		$F_{sSOK} = e(S_B, T_A)$

Fig. 3. The Semi-Static SOK Protocol

The Ephemeral SOK Protocol The protocol is presented in Fig. 4.

Alice		**Bob**
(Alice has no static keys.)		(Bob has no static keys either.)
$x \in_R Z_q^*$ $T_A = xP$		$y \in_R Z_q^*$ $T_B = yP$
	$\xrightarrow{T_A}$	
	$\xleftarrow{T_B}$	
$F_{eSOK} = e(P_0, xT_B) = e(P_0, P)^{xy}$		$F_{eSOK} = e(P_0, xT_A) = e(P_0, P)^{xy}$

Fig. 4. Ephemeral SOK Protocol

3.3 The UM and the RYY Protocols

The RYY protocol [25] is build upon the UM protocol [1, 15][1]. The two session secrets of the two protocols are $K = F_{DH}||xyP$ and $K = F_{SOK}||xyP$, respectively. A common weakness of them is that they do not possess K-CI resilience [7, 35].

[1] Later, however, we will see that in the exact ID-based version of the UM protocol, xyP should be replaced by $e(xsP, yp)$. This creates an escrowable RYY protocol.

Alice		**Bob**
long-term private/public key pair: $\langle a, Q_A = aP \rangle$		long-term private/public key pair: $\langle b, Q_B = bP \rangle$
$x \in_R Z_q^*$ $T_A = xP$		$y \in_R Z_q^*$ $T_B = yP$
	$\xrightarrow{T_A}$	
	$\xleftarrow{T_B}$	
$F_{DH} = \mathbf{aQ_B} = abP$ $k = xT_B = xyP$ $sk = H_2(A\|\|B\|\|F_{DH}\|\|k)$		$F_{DH} = bQ_A = abP$ $k = yT_A = xyP$ $sk = H_2(A\|\|B\|\|F_{DH}\|\|k)$

Fig. 5. The UM Protocol [1]

Alice		**Bob**
long-term private/public key pair: $\langle S_A = sQ_A, Q_A = H(ID_A) \rangle$		long-term private/public key pair: $\langle S_B = sQ_B, Q_B = H(ID_B) \rangle$
$x \in_R Z_q^*$ $T_A = xP$		$y \in_R Z_q^*$ $T_B = yP$
	$\xrightarrow{T_A}$	
	$\xleftarrow{T_B}$	
$F_{SOK} = \mathbf{e}(\mathbf{S_A}, \mathbf{Q_B}) = e(Q_A, Q_B)^s$ $k = xT_B = xyP$ $sk = H_2(A\|\|B\|\|F_{SOK}\|\|k)$		$F_{SOK} = \mathbf{e}(\mathbf{S_B}, \mathbf{Q_A}) = e(Q_A, Q_B)^s$ $k = yT_A = xyP$ $sk = H_2(A\|\|B\|\|F_{SOK}\|\|k)$

Fig. 6. The RYY Protocol [25]

3.4 The MTI/A0 and the Smart Protocols

For those who are unfamiliar with the MTI protocol family, we refer to [22, 9, 8]. The same design idea that produces the MTI/A0 and the Smart protocols was previously noticed, e.g. in [36], the authors used the term "Encrypt–Decrypt method". Concretely, the MTI/A0 protocol is based on the standard ElGamal encryption, while Smart's protocol [31] is based on the Boneh–Franklin IBE [3]. However, the relations between the computation of the two session secrets (c.f. the following observation No. 2) has not yet been identified before. The two session secrets of the two protocols are $K = aT_B + xQ_B$ and $K = e(S_A, T_B)e(sP, xQ_B)$, respectively. A common weakness of the two protocol is that they do not have perfect forward secrecy (PFS).

Alice		**Bob**
long-term private/public key pair: $\langle a, Q_A = aP \rangle$		long-term private/public key pair: $\langle b, Q_B = bP \rangle$
$x \in_R Z_q^*$ $T_A = xP$		$y \in_R Z_q^*$ $T_B = yP$
	$\xrightarrow{T_A}$	
	$\xleftarrow{T_B}$	
$K = aT_B + \mathbf{xQ_B} = (ay + bx)P$ $sk = H_2(A\|\|B\|\|K)$		$K = bT_A + yQ_A = (ay + bx)P$ $sk = H_2(A\|\|B\|\|K)$

Fig. 7. The MTI/A0 Protocol [23]

Alice		**Bob**
long-term private/public key pair: $\langle S_A = sQ_A, Q_A = H(ID_A) \rangle$		long-term private/public key pair: $\langle S_B = sQ_B, Q_B = H(ID_B) \rangle$
$x \in_R Z_q^*$ $T_A = xP$		$y \in_R Z_q^*$ $T_B = yP$
	$\xrightarrow{T_A}$	
	$\xleftarrow{T_B}$	
$K = e(S_A, T_B)\mathbf{e}(\mathbf{sP}, \mathbf{xQ_B})$ $sk = H_2(A\|\|B\|\|K)$		$K = e(S_B, T_A)e(sP, yQ_A)$ $sk = H_2(A\|\|B\|\|K)$

Fig. 8. The Smart Protocol [31]

From our first observation, aT_B should be changed to $e(S_A, T_B)$. Here we further notice that xQ_B is changed to $e(sP, xQ_B)$, with the help of the master public-key P_0 ($P_0 = sP$) [2]. Therefore, we get our second observation. Here Q_i ($i = \{1, 2\}$) are any publicly computable elements in group $\mathbb{G}_1$, such as $Q_A + Q_B$, $Q_A + T_B$, with Q_A, Q_B being public keys and T_B being the protocol message sent out by Bob.

Important observation #2: $aQ_1 + xQ_2 \longrightarrow e(S_A, Q_1)e(P_0, xQ_2)$.

[2] In [34], it was shown that under the SOK key setting, IBE also exists if the master public-key of the PKG is set to be $P_0 = \mathbf{s^{-1}}P$. We stress that this is also true with ID-based key agreement protocols, namely setting $P_0 = s^{-1}P$ will *not* affect the correctness and security of the A0 type ID-based protocols (e.g., Smart's, the SYL and our proposed ID-MQV), all that needed is to replace the protocol message $T_A = xP$ with $T_A = xP_0$, and then adjust the computation of the session secrets accordingly.

We summarize the above two observations with the following two substitution rules in Table 3.

Table 3. Substitution Rules for the SOK Key Construction

	Auth. DH		ID-Based Protocols
Notations	Static Private-key: a Static Public-key: $Q_A = aP$ Ephemeral Private-key: x Publicly-computable group element: Q, Q_1, Q_2		Static Private-key: $S_A = sQ_A$ Static Public-key: $Q_A = H(ID_A)$ Ephemeral Private-key: x Publicly-computable group element: Q, Q_1, Q_2
Two Rules	Rule 1. $K = aQ$ Rule 2. $K = aQ_1 + xQ_2$	$\Leftrightarrow$ $\Leftrightarrow$	$K = e(S_A, Q)$ $K = e(S_A, Q_1)e(P_0, xQ_2)$

4 Relations between Pairs of Existing Protocols

Applying the above two important substitution rules, we discover some unpublished relations between some pairs of existing protocols.

4.1 The MTI/A1 and the Chen–Kudla Protocols

The Chen–Kudla protocol [11] can be obtained by directly applying the above two substitution rules. In MTI/A1, the session secret is $K = aT_B + axQ_B$. Therefore in its ID-based counterpart, the session secret is $K = e(S_A, T_B)e(S_A, xQ_B) = e(S_A, T_B + xQ_B)$. This is exactly the Chen–Kudla [11] protocol!

Alice		**Bob**
long-term private/public key pair: $\langle a, Q_A = aP \rangle$		long-term private/public key pair: $\langle b, Q_B = bP \rangle$
$x \in_R Z_q^*$ $T_A = xQ_A$		$y \in_R Z_q^*$ $T_B = yQ_B$
	$\xrightarrow{T_A}$	
	$\xleftarrow{T_B}$	
$K = aT_B + axQ_B = \mathbf{a(T_B + xQ_B)}$ $sk = H_2(A\|\|B\|\|K)$		$K = bT_A + byQ_A = b(T_A + yQ_A)$ $sk = H_2(A\|\|B\|\|K)$

Fig. 9. The MTI/A1 Protocol [23]

Alice		**Bob**
long-term private/public key pair: $\langle S_A = sQ_A, Q_A = H(ID_A)\rangle$		long-term private/public key pair: $\langle S_B = sQ_B, Q_B = H(ID_B)\rangle$
$x \in_R Z_q^*$ $T_A = xQ_A$		$y \in_R Z_q^*$ $T_B = yQ_B$
	$\xrightarrow{T_A}$	
	$\xleftarrow{T_B}$	
$K = \mathbf{e}(\mathbf{S_A}, \mathbf{T_B} + \mathbf{xQ_B})$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K)$		$K = e(S_B, T_A + yQ_A)$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K)$

Fig. 10. The Chen–Kudla Protocol [11]

4.2 The MQV-1 and Wang's Protocols

Wang's protocol [33] can be obtained from the so-called MQV-1 protocol by directly applying the above two rules.

We first review the famous MQV [18] protocol. Note that the HMQV protocol [17] is a hashed variant of the MQV protocol.

Alice		**Bob**
long-term private/public key pair: $\langle a, Q_A = aP\rangle$		long-term private/public key pair: $\langle b, Q_B = bP\rangle$
$x \in_R Z_q^*$ $T_A = xP$		$y \in_R Z_q^*$ $T_B = yP$
	$\xrightarrow{T_A}$	
	$\xleftarrow{T_B}$	
$h_A = H_1(Q_B, T_A)$ $h_B = H_1(Q_A, T_B)$ $K = (x + ah_A)(T_B + h_BQ_B)$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K)$		$h_B = H_1(Q_A, T_B)$ $h_A = H_1(Q_B, T_A)$ $K = (y + bh_B)(T_A + h_AQ_A)$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K)$

Fig. 11. The (H)MQV Protocol [18, 17]

The MQV-1 protocol can be obtained by simply changing the protocol message $T_A = xP$ to be $T_A = xQ_A$, and then adjust the protocol accordingly. The session secret of the MQV-1 protocol is $K = (x + h_A)a(T_B + h_BQ_B)$. Therefore in its ID-based counterpart, the session secret is $K = e((x + h_A)S_A, T_B + h_BQ_B)$, this is exactly the Chow–Choo protocol [10] — a hashed variant of Wang's protocol [33].

5 Obtaining the Real ID-Based MQV Protocol

5.1 Our ID-MQV Protocol

The session secret in (H)MQV is as follows:

$$K = (x + h_A a)(T_B + h_B Q_B) = x(T_B + h_B Q_B) + h_A a(T_B + h_B Q_B).$$

We let $Q_1 = T_B + h_B Q_B$ and $Q_2 = h_A(T_B + h_B Q_B) = h_A Q_1$, then

$$K = xQ_1 + aQ_2,$$

Applying Rule #2, we obtain the ID-based version of this protocol — ID-MQV, its session secret K is as follows:

$$K = e(P_0, xQ_1)e(S_A, Q_2) = e(xP_0, Q_1)e(h_A S_A, Q_1) = e(xP_0 + h_A S_A, Q_1),$$

recall that $Q_1 = T_B + h_B Q_B$, thus we have

$$K = e(xP_0 + h_A S_A, T_B + h_B Q_B).$$

Alice		**Bob**
long-term private/public key pair: $\langle S_A = sQ_A, Q_A = H(ID_A)\rangle$		long-term private/public key pair: $\langle S_B = sQ_B, Q_B = H(ID_B)\rangle$
$x \in_R Z_q^*$ $T_A = xP$		$y \in_R Z_q^*$ $T_B = yP$
	$\xrightarrow{T_A = xP}$	
	$\xleftarrow{T_B = yP}$	
$h_A = H_1(Q_B, T_A)$ $h_B = H_1(Q_A, T_B)$ $K = e(xP_0 + h_A S_A, h_B Q_B + T_B)$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K)$		$h_B = H_1(Q_A, T_B)$ $h_A = H_1(Q_B, T_A)$ $K = e(yP_0 + h_B S_B, h_A Q_A + T_A)$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K)$

Fig. 12. ID-MQV: ID-Based (H)MQV Protocol

If we wipe off h_A and h_B, then the above ID-MQV protocol degenerate into the Shim protocol [28] which is given in Fig 13. However, the Shim protocols is totally broken by Sun and Hsie [29]. In 2005, Yuan and Li [40] repaired the Shim protocol using a very simple idea, namely just adding an ephemeral Diffie-Hellman value. The improved protocol is called the Shim-Yuan-Li (SYL) protocol (see Fig. 17) and was proven to be secure by Chen *et al.* [5]. In Fig. 18, we present the non-ID-based version of the SYL protocol — nID-SYL.

Alice		**Bob**
long-term private/public key pair: $\langle S_A = sQ_A, Q_A = H(ID_A)\rangle$		long-term private/public key pair: $\langle S_B = sQ_B, Q_B = H(ID_B)\rangle$
$x \in_R Z_q^*$ $T_A = xP$		$y \in_R Z_q^*$ $T_B = yP$
	$\xrightarrow{T_A}$	
	$\xleftarrow{T_B}$	
$K = e(xP_0 + S_A, Q_B + T_B)$ $sk = H_2(A\|\|B\|\|K)$		$K = e(yP_0 + S_B, Q_A + T_A)$ $sk = H_2(A\|\|B\|\|K)$

Fig. 13. The Shim Protocol [28]

5.2 Remarks on the ID-MQV Protocol

Alice		**Bob**
long-term private/public key pair: $\langle S_A = sQ_A, Q_A = H(ID_A)\rangle$		long-term private/public key pair: $\langle S_B = sQ_B, Q_B = H(ID_B)\rangle$
$x \in_R Z_q^*$ $T_A = xP$		$y \in_R Z_q^*$ $T_B = yP$
	$\xrightarrow{T_A}$	
	$\xleftarrow{T_B}$	
$h_A = H_1(Q_B, T_A)$ $h_B = H_1(Q_A, T_B)$ $K_1 = e(xP_0 + h_A S_A, h_B Q_B + T_B)$ $\mathbf{K_2 = xT_B = xyP}$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K_1\|\|\mathbf{K_2})$		$h_B = H_1(Q_A, T_B)$ $h_A = H_1(Q_B, T_A)$ $K_1 = e(yP_0 + h_B S_B, h_A Q_A + T_A)$ $\mathbf{K_2 = yT_A = xyP}$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K_1\|\|\mathbf{K_2})$

Fig. 14. Escrowless ID-MQV: ID-Based (H)MQV Protocol with PKG-FS

Our ID-MQV protocol has remarkable superiorities over all the existing ID-based key agreement protocols (from pairings).

1. From the format of the protocol messages, we argue that our ID-MQV is the real ID-based version of the famous (H)MQV protocol. As mentioned above, the Chow–Choo and Wang protocols are ID-based version of the so-called (H)MQV-1 protocols, which have different protocol messages.
2. Separating *perfect forward secrecy* (PFS) from *PKG forward secrecy* (PKG-FS). Note that PKG-FS also means escrowless. We argue that in some applications (as also pointed out by McCullagh

and Barreto [20]) key escrow is a requirement or even, a must. However, if we remove $K_1 = abP$ from the SYL protocol [40] to open escrow, then it become totally insecure (which is exactly Shim's protocol [28]), let alone PFS. Our new protocol can be securely used in escrowed model (*i.e.*, w/o xyP), providing PFS. When xyP is added, the protocol becomes escrowless (and achieves PKG-FS, see Fig. 14). In a word, xyP separates clearly PFS from PKG-FS, and our new protocol (ID-MQV) can be used with or without escrow.

3. Compared with Wang's protocol [33] (and the Chow-Choo protocol [10]), our protocol does not need extra message exchange to close escrow, while the latter requires a party to send out an extra point. At the same time, brings extra computation for the party.
4. The new protocol can be further strengthened to achieve stronger security, *i.e.*, to be secure in the extended Canetti–Krawczyk (eCK) model which allows *ephemeral* secret key reveal. (Using the same idea from [6].)

6 Beyond the SOK ID-Based Key Construction

Now we look at the SK key setting. For details on the key setting, please refer to [30] and [20, 38]. Here we note that the master private and public key pair of the PKG is $\langle s, P_0 = sP \rangle$. u is part of a user's static public key and for Alice $u_A = H'(ID_A) \in \mathbb{Z}_q^*$.

We discover that the key transport protocol behind the SK-IBE [30] is simply the ID-based version of the Hughes protocol [16]. This is mainly because the static private key of the receivers in the two protocols are both inversion-based. The substitution rules are listed in Table 4.

Table 4. Substitution Rules for the SK Key Construction

	Auth. DH		ID-Based Protocols
Notations	Static key pair: $\langle a, Q_A = aP \rangle$ Ephemeral Private-key: x Publicly-computable element: Q		Static key pair: $\langle S_A = s + u_A)^{-1} Q_P$, $Q_A = P_0 + u_A P = (s + u_A)P \rangle$ Ephemeral Private-key: x Publicly-computable element: Q
Two Rules	Rule 1. $K = a^{-1} Q$ Rule 2. $K = xP$,	$\Leftrightarrow$ $\Leftrightarrow$	$K = e(S_A, Q)$ $K = e(P, P)^x$

Using the above rules, we can establish the relations between the MB protocols [20, 21] and the MTI/C0 and MTI/B0 [23] protocols (c.f. Table 1), the details are omitted here. Next, based on the enhanced MTI/C0 protocol (*i.e.* the ECKE-1N protocol), we propose a highly efficient ID-based protocol — eMB.

6.1 Review of the ECKE-1N Protocol

This protocol was initially designed using the ideas from MQV. It was later included in a Letter appeared in IEEE Communications Letters entitled "Cryptanalysis and Improvement of an Elliptic Curve Diffie-Hellman Protocol" [37]. (Also available at IACR ePrint, report 2007/026.) The protocol is give in Fig. 15.

Alice		**Bob**
long-term private/public key pair: $\langle a, Q_A = aP \rangle$		long-term private/public key pair: $\langle b, Q_B = bP \rangle$
$x \in_R Z_q^*$ $T_A = xQ_B$		$y \in_R Z_q^*$ $T_B = yQ_A$
	$\xrightarrow{T_A}$	
	$\xleftarrow{T_B}$	
$h_A = H_1(Q_B, T_A)$ $h_B = H_1(Q_A, T_B)$ $K = a^{-1}(x + h_A)(T_B + h_B Q_A)$ $= (x + h_A)(y + h_B)P$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K)$		$h_B = H_1(Q_A, T_B)$ $h_A = H_1(Q_B, T_A)$ $K = b^{-1}(y + h_B)(T_A + h_A Q_B)$ $= (x + h_A)(y + h_B)P$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K)$

Fig. 15. The Enhanced MTI/C0 Protocol — ECKE-1N

6.2 The eMB Protocol

Applying the substitution rules from Table 4, we converse our ECKE-1N into an ID-based authenticated key agreement protocol which is the enhanced version of the McCullagh-Barreto protocol [20, 21] — eMB.

Alice		**Bob**
long-term private/public key pair: $\langle S_A = (s + u_A)^{-1}P$, $Q_A = P_0 + u_A P = (s + u_A)P \rangle$		long-term private/public key pair: $\langle S_B = (s + u_B)^{-1}P$, $Q_B = P_0 + u_B P = (s + u_B)P \rangle$
$x \in_R Z_q^*$ $Q_B = P_0 + u_B P = (s + u_B)P$ $T_A = xQ_B$		$y \in_R Z_q^*$ $Q_A = P_0 + u_A P = (s + u_A)P$ $T_B = yQ_A$
	$\xrightarrow{T_A}$	
	$\xleftarrow{T_B}$	
$h_A = H(Q_B, T_A)$ $h_B = H(Q_A, T_B)$ $K = e((x + h_A)S_A, T_B + h_B Q_A)$ $= e(P, P)^{(x+h_A)(y+h_B)}$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K)$		$h_B = H(Q_A, T_B)$ $h_A = H(Q_B, T_A)$ $K = e((y + h_B)S_B, T_A + h_A Q_B)$ $= e(P, P)^{(x+h_A)(y+h_B)}$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K)$

Fig. 16. The eMB Protocol

We remark that the substitution rules in the SK ID-based key setting can also be applied to the SK variants, e.g. Gentry's key setting [14] and the second Boneh-Boyen (BB_2) scheme [2].

Acknowledgements

The author wishes to thank Liqun Chen, Zhaohui Cheng, Kenny Paterson and Yongge Wang for comments on the first version of this paper.

References

1. R. Ankney, D. Johnson, M. Matyas. The Unified Model. contribution to X9F1, October 1995. [4, 5]
2. D. Boneh and X. Boyen. Efficient selective-ID secure identity based encryption without random oracles. Advances in Cryptology C EUROCRYPT'04, LNCS vol. 3027, pp.223C238, Springer-Verlag. [13]
3. D. Boneh, M. Franklin. Identity-based encryption from the Weil pairing. In *Proc. of CRYPTO 2001*, LNCS vol. 2139, pp. 213-229, Springer-Verlag, 2001. [3, 5]
4. C. Boyd, W. Mao, and K. Paterson. Key agreement using statically keyed authenticators. In *Proc. of ACNS 2004*, LNCS vol. 3089, pp. 248-262. Springer-Verlag,, 2004 [3]
5. L. Chen, Z. Cheng, and N. P. Smart. Identity-based key agreement protocols from pairings. Cryptology ePrint Archive, Report 2006/199. [9]
6. B. LaMacchia, K. Lauter and A. Mityagin. Stronger Security of Authenticated Key Exchange. Cryptology ePrint Archive: Report 2006/073 [11]
7. C. Boyd and K.-K. R. Choo. Security of two-party identity-based key agreement. In *Proc. of MYCRYPT 2005*, LNCS vol. 3715, pp. 229-243, Springer-Verlag, New York, 2005. [1, 4]
8. S. Blake-Wilson, C. Johnson and A. Menezes. Key Agreement Protocols and their Security Analysis. In *Proc. of the sixth IMA International Conference on Cryptography and Coding*, LNCS vol. 1355, New York, Springer-Verlag, 1997, pp. 30-45. [5]
9. S. Blake-Wilson, A. Menezes. Authenticated Diffie-Hellman key agreement protocols. In *Proc. of SAC 1998*, LNCS vol. 1556, New York, Springer-Verlag, 1999, pp. 339-361. [5]
10. S. S.-M. Chow, K.-K.R. Choo, Strongly-secure identity-based key agreement and anonymous extension, in: Proc. ISC'07, LNCS vol. 4779, 2005, pp. 203-220. [2, 8, 11]
11. L. Chen, C. Kudla. Identity based key agreement protocols from pairings. In *Proc. of the 16th IEEE Computer Security Foundations Workshop*, IEEE Computer Society, 2002, pp. 219-213. See also Cryptology ePrint Archive, Report 2002/184. [2, 7, 8]
12. W. Diffie, M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory* 22(6): 644 - 654, 1976. [3]
13. T. ElGamal. A public key cryptosystem and signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* 31(4): 469-472, 1985. [3]
14. C. Gentry. Practical identity-based encryption without random oracles. Advances in Cryptology C EUROCRYPT'06, LNCS, Springer-Verlag, 2006. [13]
15. K. C. Goss. Cryptographic method and apparatus for public key exchange with authentication. US Patent 4,956,863, September 1990. [4]
16. E. Hughes. An encrypted key transmission protocol. Presented at the rump session of CRYPTO'94, Aug 1994. [11]
17. H. Krawczyk. HMQV: A high performance secure Diffie-Hellman protocol. In *Proc. of Crypto'05*, LNCS 3621, pp. 546-566, Springer-Verlag, New York, 2005. [8]
18. L. Law, A. Menezes, M. Qu, J. Solinas and S. A. Vanstone, "An efficient protocol for authenticated key agreement," *Des. Codes Cryptography*, vol.28, no.2, pp. 119-134, 2003. [8]
19. S. Li, Q. Yuan and J. Li. Towards security two-part authenticated key agreement protocols. Cryptology ePrint Archive, Report 2005/300, 2005. Available at http://eprint.iacr.org/2005/300. [2]
20. N. McCullagh, P.S.L.M. Barreto. A new two-party identity-based authenticated key agreement. In *Proc. of CT-RSA 2005*, LNCS vol. 3376, pp. 262-274, Springer-Verlag, New York, 2005. [2, 11, 12, 13]
21. N. McCullagh, P.S.L.M. Barreto. A new two-party identity-based authenticated key agreement. Cryptology ePrint Archive, Report 2004/122, 2004. Available at http://eprint.iacr.org/2004/122. (Updated paper of [20].) [2, 11, 12]

22. A. Menezes, P. van Oorschot and S. Vanstone. Handbook of Applied Cryptography, CRC Press, 1997. [3, 5]
23. T. Matsumoto, Y. Takashima and H. Imai. On seeking smart public-key distribution systems. *Trans. IECE of Japan*, E69, pp.99-106, 1986. [6, 7, 11, 15]
24. K. G. Paterson and S. Srinivasan. On the relations between non-interactive key distribution, identity-based encryption and trapdoor discrete log groups. Cryptology ePrint Archive, Report 2007/453, 2007. Available at http://eprint.iacr.org/2007/453. [3]
25. E.K. Ryu, E.J. Yoon, and K.Y. Yoo. An efficient ID-based authenticated key agreement protocol from pairings. In *Proc. of NETWORKING 2004*, LNCS vol. 3042, pp. 1458-1463. Springer-Verlag, 2004. [3, 4, 5]
26. M. Scott. Authenticated ID-based key exchange and remote log-in with insecure token and PIN number. http://eprint.iacr.org/2002/164.pdf [2]
27. A. Shamir. Identity-based cryptosystems and signature schemes. In *Proc. of CRYPTO 1984*, LNCS vol.196, Springer-Verlag, New York, 1984, pp. 47-53. [3]
28. K. Shim. Efficient ID-based authenticated key agreement protocol based on Weil pairing. *Electron. Lett.*, 39(8), pp. 653-654, 2003. [2, 9, 10, 11]
29. H. Sun, B. Hsieh. Security analysis of Shim's authenticated key agreement protocols from pairings. Cryptology ePrint Archive, Report 2003/113, 2003. Available at http://eprint.iacr.org/2003/113. [9]
30. R. Sakai and M. Kasahara. ID based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive, Report 2003/054. [11]
31. N.P. Smart. An identity based authenticated key agreement protocol based on the Weil pairing. *Electron. Lett.,* 38(13), 2002, pp. 630-632. [2, 5, 6]
32. R. Sakai, K. Ohgishi and M. Kasahara. Cryptosystems based on pairing. In *Proc. of the 2000 Symposium on Cryptography and Information Security*, Okinawa, Japan, 2000. [2, 3]
33. Y. Wang. Efficient identity-based and authenticated key agreement protocol. ePrint Achive. Available at http://eprint.iacr.org/2005/108. [2, 8, 11]
34. S. Wang. Practical Identity-Based Encryption (IBE) in Multiple PKG Environments. Available at http://arxiv.org/abs/cs/0703106 (Updated version available at Cryptology ePrint Archive, Report 2007/100.) [6]
35. S. Wang, Z. Cao and H. Bao. Security of an efficient ID-based authenticated key agreement protocol from pairings. In *Proc. of ISPA'05 Workshops*, LNCS vol. 3759, pp. 342-349. Springer-Verlag, New York, 2005. [1, 4]
36. S. Wang, Z. Cao and K-K. R. Choo. Provably secure identity-based authenticated key agreement protocols without random oracles, 2006 (Preprint, available at Cryptology ePrint Archive, Report 2006/446) [5]
37. S. Wang, Z. Cao, M. Strangio and L. Wang. Cryptanalysis and improvement of an elliptic Ccurve Diffie-Hellman key agreement protocol. to appear in *IEEE Communications Letters.* (Also available at Cryptology ePrint Archive, Report 2007/026) [2, 11]
38. G. Xie. Cryptanalysis of Noel McCullagh and Paulo S. L. M.Barreto's two-party identity-based key agreement. Cryptology ePrint Archive, Report 2004/308, 2004. Available at http://eprint.iacr.org/2004/308. [11]
39. G. Xie. An ID-based key agreement scheme from pairing. Cryptology ePrint Archive, Report 2005/093, 2005. Available at http://eprint.iacr.org/2005/093. [2]
40. Q. Yuan and S. Li. A new efficient ID-based authenticated key agreement protocol. Cryptology ePrint Archive, Report 2005/309, 2005. Available at http://eprint.iacr.org/2005/309. [2, 9, 11, 15]

A Obtaining an Authenticated DH Protocol from the SYL Protocol

The two protocols are presented in Fig. 17 and 18, respectively.

Alice		**Bob**
long-term private/public key pair: $\langle S_A = sQ_A, Q_A = H(ID_A)\rangle$		long-term private/public key pair: $\langle S_B = sQ_B, Q_B = H(ID_B)\rangle$
$x \in_R Z_q^*$ $T_A = xP$		$y \in_R Z_q^*$ $T_B = yP$
	$\xrightarrow{T_A = xP}$	
	$\xleftarrow{T_B = yP}$	
$K_1 = xT_B = xyP$ $K_2 = e(xP_0 + S_A, Q_B + T_B)$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K_1\|\|K_2)$		$K_1 = yT_A = xyP$ $K_2 = e(yP_0 + S_B, Q_A + T_A)$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K_1\|\|K_2)$

Fig. 17. The SYL Protocol [40]

Alice		**Bob**
long-term private/public key pair: $\langle a, Q_A = aP\rangle$		long-term private/public key pair: $\langle b, Q_B = bP\rangle$
$x \in_R Z_q^*$ $T_A = xP$		$y \in_R Z_q^*$ $T_B = yP$
	$\xrightarrow{T_A = xP}$	
	$\xleftarrow{T_B = yp}$	
$K_1 = xT_B = xyP$ $K_2 = (x + a)(Q_B + T_B)$ $= (x + a)(y + b)P$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K_1\|\|K_2)$		$K_1 = yT_A = xyP$ $K_2 = (y + b)(Q_A + T_A)$ $= (x + a)(y + b)P$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K_1\|\|K_2)$

Fig. 18. nID-SYL: A New Authenticated Diffie-Hellman Protocol

B Enhanced MTI/C1 Protocol

This protocol can be easily derived from our enhanced MTI/C0 protocol (*i.e.* the ECKE-1N protocol) using the idea from [23].

Alice		**Bob**
long-term private/public key pair: $\langle a, Q_A = aP\rangle$		long-term private/public key pair: $\langle b, Q_B = bP\rangle$
$x \in_R Z_q^*$ $T_A = xaQ_B = xF_{DH}$		$y \in_R Z_q^*$ $T_B = ybQ_A = yF_{DH}$
	$\xrightarrow{T_A = xabP}$	
	$\xleftarrow{T_B = yabP}$	
$h_A = H_1(Q_B, T_A)$ $h_B = H_1(Q_A, T_B)$ $K = (x + a^{-1}h_A)(T_B + h_BQ_A)$ $= (ax + h_A)(yb + h_B)P$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K)$		$h_B = H_1(Q_A, T_B)$ $h_A = H_1(Q_B, T_A)$ $K = (y + b^{-1}h_B)(T_A + h_AQ_B)$ $= (by + h_B)(xa + h_A)P$ $sk = H_2(A\|\|B\|\|T_A\|\|T_B\|\|K)$

Fig. 19. The Enhanced MTI/C1 Protocol