Towards Security Two-part Authenticated Key Agreement Protocols

Songping Li [1], Quan Yuan[1] and Jin Li [2]

[1]School of Mathematical Sciences, Peking University, Beijing 100871, P. R.China

[1]{lsp,yq2uan}@pku.edu.cn

[2]Huawei Technologies Co., Shenzhen 518129, P. R.China

[2]jingle@huawei.com

September 7, 2005

Abstract. We first present a new security 2-AK protocol, which is more secure and more efficient than previously proposed ones. Meanwhile, we point that Xie's ID-2-AK protocol modified from McCullagh-Barreto in CT-RSA 2005 doesn't provide protection against KCI attack likewise, and finally utilize the modular arithmetic, first proposed in MQV and also used in Kim, to get a modified new ID-2-AK protocol. On second thoughts, we give another ID-2-AK protocol utilizing the operation of addition in finite field like our forenamed 2-AK protocol . The two ID-2-AK protocols are in possession of all the desired security attributes. We also compare our new protocols with others in terms of computational cost and security properties.

Keywords. key management, authenticated protocol, ID-based, Key Compromise Impersonation

1 Introduction

Authenticated key establishment protocols are designed to provide two or more specified entities communicating over an open network with a shared secret key that may subsequently be used to achive some cryptographic goal such as confidentiality or data integrity. There are two fundamental types of key establishment protocols [7]: key transport and key agreement. Key agreement protocols are more reliable because both entities contribute information that is used to derive the shared secret key.

A key agreement protocol is desired to have these fundamental security goals: implicit key authentication and explicit key authentication [8,9]. A key agreement protocol which provides implicit key authentication to both participating entities is called an authenticated key agreement(AK) protocol, while one providing explicit key authentication to both participating entities is called an authenticated key agreement with key conformation(AKC) protocol.

As it has been proved to be difficult to deploy a public key infrastructure (PKI) system. Thus it is preferred to design easy to deploy authenticated key agreement systems. Identity-based key agreement system is such an example. The basic idea of an identity-based cryptosystem is that end users can choose an arbitrary string relating to their identities, for example email addresses or network IP addresses, as their public keys. This eliminates much of the overhead associated with key management. In traditional PKI settings, key agreement protocols relies on the parties obtaining each other's certificates, extracting each other's public keys, checking certificate chains (which may involve many

signature verifications) and finally generating a shared secret. The technique of identity-based cryptography greatly simplifies this process.

In addition to implicit key authentication and key confirmation, a number of desirable security attributes of AK and AKC protocols have been identified. Typically the importance of supplying these attributes will depend on the application.

1. **Known-key security.** Each run of a key agreement between A and B should produce a unique secret key : such keys are called session keys. A protocol should still achieve its goal in the face of an adversary who has learned some other session keys.
2. **Forward secrecy.** If long-term private keys of one or more entities are compromised, the secrecy of previous session keys established by honest entities is not affected.
3. **Key-compromise impersonation resistent attribute.** Suppose A's long-term private key is disclosed. Clearly an adversary that knows this value can now impersonate A, since it is precisely this value that identifies A. However, it may be desirable in some circumstances that this loss does not enable the adversary to impersonate other entities to A.
4. **Unknown key-share attribute**. Entity B cannot be coerced into sharing a key with entity A without B's knowledge, i.e., when B believes the key is shared with some entity C≠ A, and A (correctly) believes the key is shared with B.
5. **Key Control.** Neither entity should be able to force the session key to be a pre-selected value. That is, the session key is determined by all the entities and no one can influence the generation of the session key.

Since the basic Diffie-Hellman key agreement scheme that provides the first practical solution to the key distribution problem, numerous protocols have been proposed. But many of these protocols were subsequently found to be flawed. For example, it is known that Unified Model, MTI/C0 and MQV protocol are vulnerable to key-compromise impersonation attack, small subgroup attack, and unknown key-share attack, respectively [10]. At Asiacrypt'96, Just and Vaudenay [11] proposed a 2-AK protocol whose elliptic curve version was subsequently proposed by Song and Kim [12] At Indocrypt'00. But in 2002, Kim [8] pointed that Just-Vaudenay protocol didn't provide protection against KCI attack, and finally present a modified version that can provide.

Based on Weil and Tate pairing techniques, several practical ID-AK protocols, e.g., Smart [13], Chen-Kudla [14], Scott [15], Shim [16], and McCullagh-Barreto [6] etc., have been proposed. However, none of these protocols is secure (see,[17]). Resently, Xie [5] proposed an ID-AK protocol which is modified from McCullagh-Barreto[6] and asserted it can resistant KCI attack. Wang[18] also presented a new security ID-AK protocol not long ago.

The remainder of the paper is organized as follows. Section 2 introduces Technical Backgrounds. In section 3, we briefly describe Kim's protocol. In section 4, we present a new security 2-AK protocol, which is more secure and more efficient than previously proposed ones. In section 5, we give a KCI attack to Xie's modified protocol after review McCullagh-Barreto's protocol and Xie's modification. In section 6, we present two new ID-2-AK protocols that are in possession of all the desired security attributes. In section 7, we compare our new protocols with others in terms of computational cost and security properties. The concluding remark will be followed in section 8.

2 Technical Backgrounds

2.1 Bilinear Pairing

In this section, we shall briefly describe the properties of the bilinear pairings. The bilinear parings include Weil pairing and Tate pairing in elliptic curve cryptography. The MOV attack using Weil pairing and the FR attack using Tate pairing reduce the discrete logarithm problem on some elliptic curves to the discrete logarithm problem in a finite field [25,26]. Later, the bilinear pairings have been used in construction of the identity-based cryptography.

We let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q. We assume that the discrete logarithm problem (DLP) in both G_1 and G_2 are hard. We let $\hat{e} : G_1 \times G_1 \rightarrow G_2$ be a pairing which satisfies the following properties:

1. Bilinear
   $\hat{e}(P_1 + P_2, Q) = \hat{e}(P_1, Q)\, \hat{e}(P_2, Q)$
   $\hat{e}(P, Q_1 + Q_2) = \hat{e}(P, Q_1)\, \hat{e}(P, Q_2)$
2. Non-degenerate
   if P is a generator of G1, then $\hat{e}(P, P) \neq 1$.
3. Computability
   There is an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P, Q \in G1$ in polynomial-time.

The non-degeneracy does not hold for the standard Weil pairing e(P, Q), but it does hold for the modified Weil pairing $\hat{e}(P, Q)$. We note that the Weil and Tate pairings associated with supersingular elliptic curves or abelian varieties can be modified to create such bilinear maps. We may refer to [19,27] for more details.

2.2 Diffie-Hellman Assumptions

With the group G1 described in Section 2.1, there are the following problems in elliptic curve cryptography:

- Discrete Logarithm (DL) Problem: Given $P, Q \in G1$, find an integer n such that $P = nQ$ whenever such integer exists.
- Computational Diffie-Hellman (CDH) Problem: Given a triple $(P, aP, bP) \in G1$ for $a, b \in Zq$, find the element abP .
- Decision Diffie-Hellman (DDH) Problem: Given a quadruple $(P, aP, bP, cP) \in G1$ for $a, b, c \in Zq$, decide whether $c = ab \bmod q$ or not.
- Gap Difffie-Hellman (GDH) Problem: A class of problems where the CDH problem is hard but DDH problem is easy.

3 Kim's Protocol

In 2002, Kim[8] proposed a modified version of the Just-Vaudenay protocol[11] to resist the KCI attack. We will briefly explain Kim's protocol as follows. Let p is an 1024 bits prime; q is an 160 bits prime divisor of p-1 and G is a q order subgroup of Z_p^*. Kim utilizes the following notation

proposed in the MQV protocol: If $X \in [1, p-1]$ then $\overline{X} = (X \bmod 2^{80}) + 2^{80}$. Note that $\overline{X} \bmod q \neq 0$. In the protocol, two principals A and B agree publicly on an element g in a multiplicative group G and their private keys are s_A and s_B respectively and public keys are $p_A = g^{s_A}$ and $p_B = g^{s_B}$ correspondingly. They select random values r_A and r_B ,

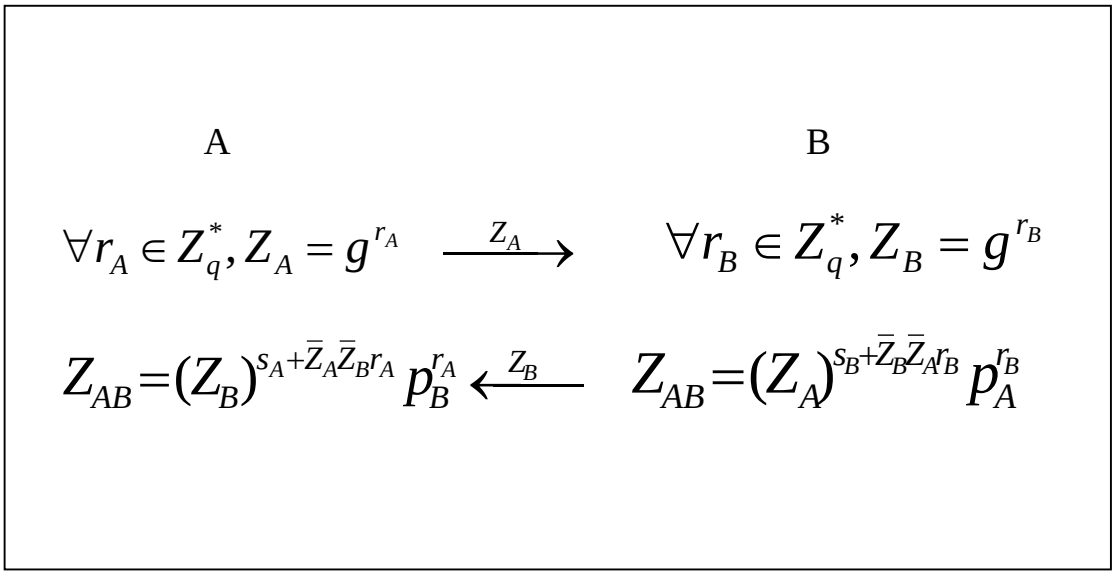

Figure 1: Kim's Protocol

respectively , in the range between 1 and q. A calculates $Z_A = g^{r_A}$ and B calculates $Z_B = g^{r_B}$ and they exchange these values as is shown in Figure 1. The shared secret is $Z_{AB} = g^{r_B s_A + \overline{Z}_A \overline{Z}_B r_A r_B + r_A s_B}$.

Shim believes that an adversary C cannot implement the KCI attack since she cannot determine the value $\overline{Z}_B$ in advance. We can prove that as follows:

In fact, C wants to counteract $p_B^{r_A}$ which is indispensable in the calculation of $Z_{AB} = g^{r_B s_A + \overline{Z}_A \overline{Z}_B r_A r_B + r_A s_B}$. So he should get Z_B to s.t. $Z_B = g^{r_C} P_B^{\overline{Z}_A^{-1} \overline{Z}_B^{-1}} = g^{r_C} (M)^{\overline{Z}_B^{-1}}$ (r_C is a random value selected by C, $M = P_B^{\overline{Z}_A^{-1}}$). We know that M is a positive constant, so C should get Z_B by the solution of discrete equation $Z_B (M)^{\overline{Z}_B^{-1}} = g^{r_C}$. $\forall r_C \in Z_q^*$, let $\overline{Z}_B = Z_B + k \cdot 2^{80}$ (k is a positive integer) , and then we want to solve the equation $Z_B (M)^{\overline{Z}_B^{-1}} = g^{r_C}$ in turn with variable k . In other words, we want to get a solution of the discrete transcendental equation $xa^{\frac{1}{x+c}} = b$ (a>0,a, b, and c are constants) which we denote as α..

Actually we have known that it is a difficult problem to get the analytic solution of the transcendental equation yet. We know neither whether it has a solution nor the number of solutions up to the present. There are only several approximate solutions to the transcendental equation, such as iterative method and dichotomy etc.. So it is naturally hard to get the solution α of the discrete transcendental equation in big prime field. It seems at least as hard as discrete logarithm problem in big prime field. So Kim's protocol provides protection against KCI attack for sure. The protocol also has other attributes, such as Known Key-Security, Perfect-Forward-Secrecy etc..

4 A new 2-AK Protocol

With the help of the addition operation in the finite field, we will give another modified version. The parameters are similar to section 3: p is an 1024 bits prime, q is an 160 bits prime divisor of p-1, and G is a q order subgroup of the multiplicative group F_p^* of finite field F_p. But we append the + operation that is the addition in finite field F_p. The two entities exchange the messages as is shown in Figure 2. The shared secret is $Z_{AB} = g^{r_A r_B} + g^{r_B s_A} g^{r_A s_B}$.

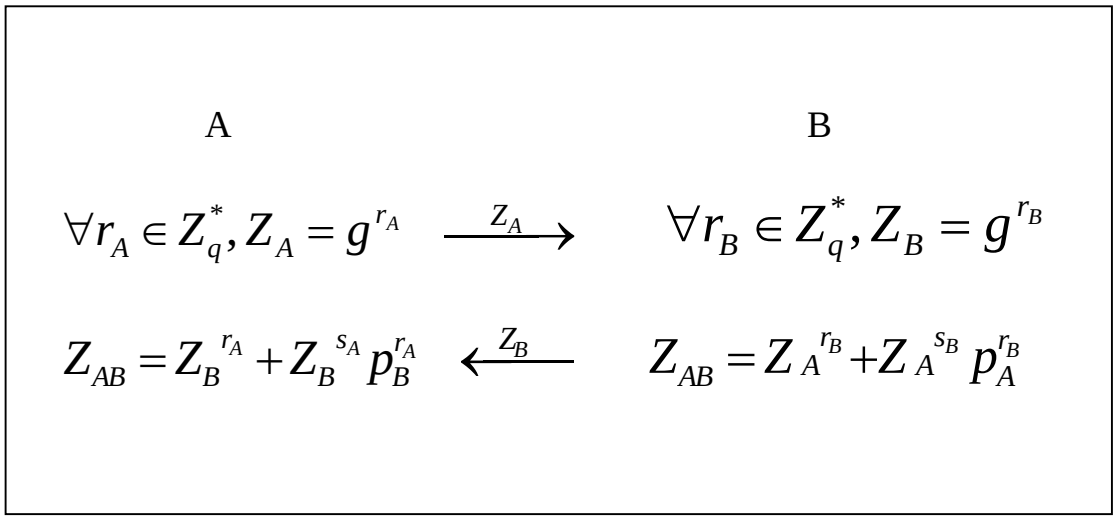

Figure 2: A new 2-AK Protocol

As the calculations is in finite field, so we know entity A and entity B share the same value above. We also know the value of the shared secret is in finite field F_p but not only in G. The protocol provides security property of KCI resistance for the adversary couldn't kill or get $p_B^{r_A}$ which is indispensable in the calculation of Z_{AB} . Actually the protocol is the combination of MTI/A(0) and MTI/C(0) [29], so our new 2-AKP provide other security properties such as Known Key Security, Perfect Forward-Secrecy etc. . But our new 2-AK protocol is superior to Kim's in computational cost in evidence.

Now we make a farther consideration whether the distribution of the shared keys is uniformity. As r_A and r_B are random values, so $Z_B^{r_A}$ and $Z_B^{s_A} p_B^{r_A}$ are random and $Z_{AB} = Z_B^{r_A} + Z_B^{s_A} p_B^{r_A}$ can be expressed as $g^i + g^k = g^i(1 + g^{k-i})$ (i≤k,i,k∈ℝ), so it is uniformity as gcd(g^i ,$1 + g^{k-i}$)=1.

5 McCullagh-Barreto's ID-2-AK Protocol and Modifications

Resently, McCullagh and Barreto[6] proposed a ID-2-AK protocol in CT-RSA 2005. But later Xie[4] pointed out McCullagh-Barreto's protocol proposed in [6] didn't provide protection against KCI attack and proposed a new ID-2-AK protocol[5] modified from that and asserted it can resistant KCI attack. But we find the modification is unsuccessful.

First we briefly review McCullagh-Barreto's protocol. McCullagh-Barreto's protocol like all other ID-AKPs has three algorithms: **Setup**, **Extract** and **Key agreement**.

Setup: The KGC (Key Generation Centre) is responsible for the creation and secures distribution of users private keys. G_1 and G_2 are two groups, both of prime order q, suitable bilinear map $\hat{e}: G_1 \times G_1 \to G_2$ (which can be modified from Tate pairing or Weil Pairing in elliptic curve, see, [19,20]). P is a generator element of G_1. H is an one-way hash fountion as H : {0, 1}* → Z_q^*. The KGC randomly generates a master secret s $\in_R$Zq*, and calculates a master public key sP. The parameters and master public key are distributed to the users of the system through a secure authenticated channel. The system public parameters is <E,q, G_1 , G_2 ,P,sP, ê,H>.

Extract: The identities of the two principles, A and B, are ID_A and ID_B respectively. Let $a = H(ID_A)$ and $b = H(ID_B)$. A's public key is $P_A = (a+s)P$, which can be computed as aP + sP. The KGC computes Alice's private key as $S_A = (a+s)^{-1}P$ and then sends it to A through a secret channel. The same is to B and so the public key and the private key of B are $P_B = (b+s)P$ and $S_B = (b+s)^{-1}P$ respectively.

Key Agreement: Assume that A and B have private keys issued by the same KGC. The key agreement is shown in Figure 3, and the shared secret is $Z_{AB} = \hat{e}(P,P)^{r_A r_B}$.

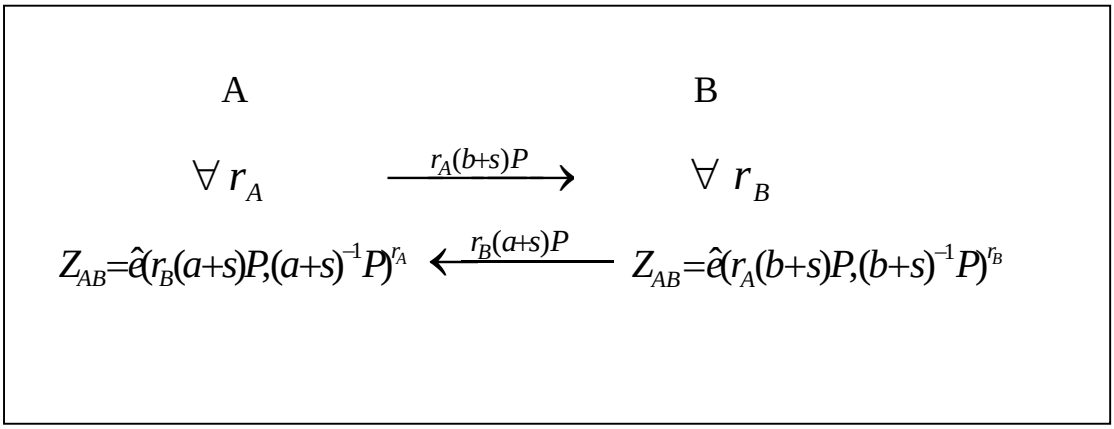

Figure 3: McCullagh-Barreto's Protocol

But later Xie[4] pointed out that McCullagh-Barreto's protocol was vulnerable to KCI attack: the adversary C can send $r_B(b+s)P$ to A and then get the shared secret by calculating $Z_{AB} = \hat{e}(r_A(b+s)P,(a+s)^{-1}P)^{r_B}$. McCullagh and Barreto's modified version to resist Xie's KCI attack is to change the expression of the shared secret calculation to $Z_{AB} = \hat{e}(P,P)^{r_A + r_B}$.

But we know, it does not provide Perfect Forward Secrecy property. Because the adversary C can get the previous session keys by calculating $Z_{AB} = \hat{e}(r_A(b+s)P,(b+s)^{-1}P)\hat{e}(r_B(a+s)P,(a+s)^{-1}P)$.

Xie then gave a modified version to McCullagh-Barreto's protocol. His protocol only changes the expression of the shared secret calculation likewise. The algorithms of Setup and Extract are the same as McCullagh-Barreto's. In the Key Agreement, the shared secret is $Z_{AB} = \hat{e}(P,P)^{r_A r_B + r_A + r_B}$,as is shown in Figure 4.

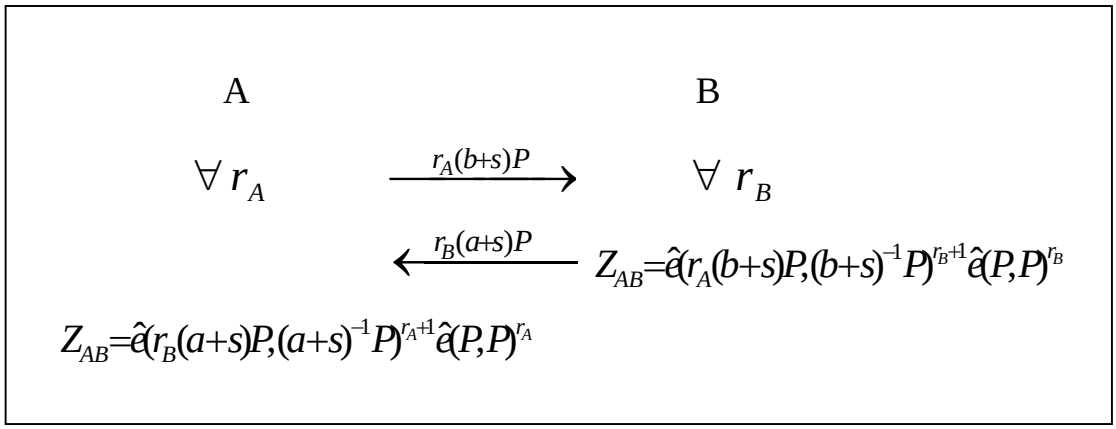

Figure 4: Xie's Protocol

But we find the modification is unsuccessful because it is vulnerable to the KCI attack yet. Actually the protocol has a leak of -1. When the adversary C let $r_C = -1$, he can succeed in man-in-middle attack that is shown in Figure 5 and gets the shared secret $Z_{AB} = \hat{e}(P,P)^{-1}$.

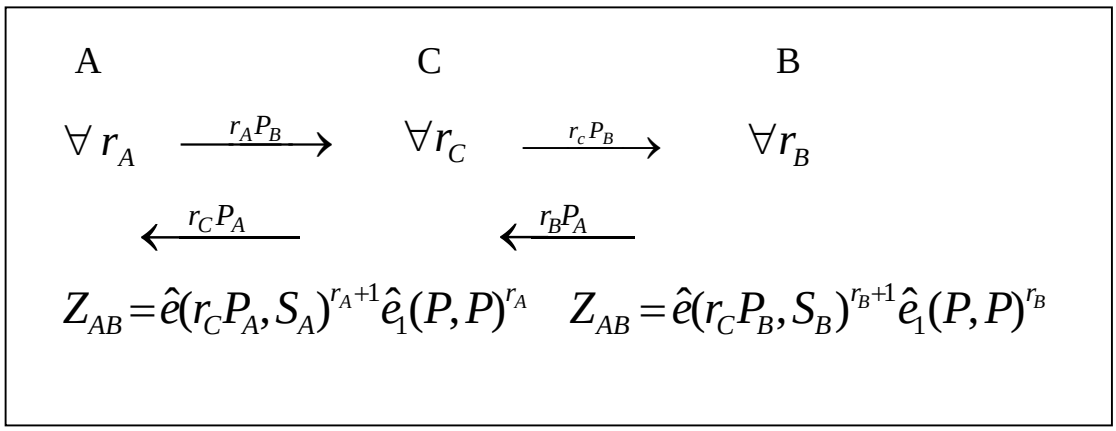

Figure 5: man-in-middle attack to Xie's Protocol

Although A and B can reject the random value -1from the other side to prevent it, but the leak is intrinsic as long as the shared secret is calculate by $Z_{AB} = \hat{e}(r_C P_A, S_A)^{r_A+1}\hat{e}_1(P,P)^{r_A}$. We can utilize the leak of -1 to carry out KCI attack, as is shown in Figure 6. After the attack, the adversary C can impersonate B to share secret $Z_{AC} = \hat{e}(P_B, S_A)^{r_A r_C + r_C - 1}$ with A while A belives he has shared the secret with B.

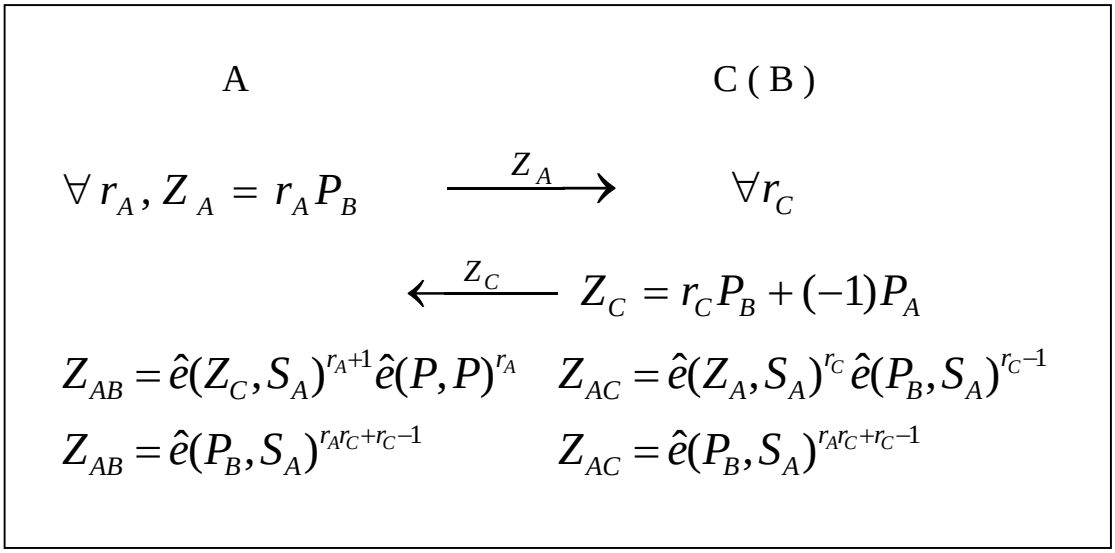

Figure 6: KCI attack to Xie's Protocol

6 Two New ID-2-AK Protocols

6.1 ID-2-AK Protocol I

Inspired on Kim's protocol in section 3, here we give a modified version of McCullagh , Barreto and Xie's ID-2-AK protocols [5, 6] with the help of the notation first proposed in the MQV protocol: If $X \in [1, p-1]$ then $\overline{X} = (X \bmod 2^{80}) + 2^{80}$. Our modified protocol can prevent from the KCI attack. The algorithms of Setup and Extract are the same as McCullagh , Barreto and Xie's , except the additions of the notation $\overline{X}$ and a system public parameter $\hat{e}(P,P)$. The main modification is in the Key Agreement as is shown in Figure 7. The final shared secret is $Z_{AB} = \hat{e}(P,P)^{r_A r_B \overline{\lambda}_A \overline{\lambda}_B}$ (where $\lambda_A = \hat{e}(P,P)^{r_A}, \lambda_B = \hat{e}(P,P)^{r_B}$) . The adversary C couldn't construct message to make KCI attack like Kim's protocol. Because C have no knowledge of either r_A or S_B and he couldn't get $\lambda_A = \hat{e}(P,P)^{r_A} = \hat{e}(r_A P_B, S_B)$ which is indispensable in the calculation of Z_{AB}.

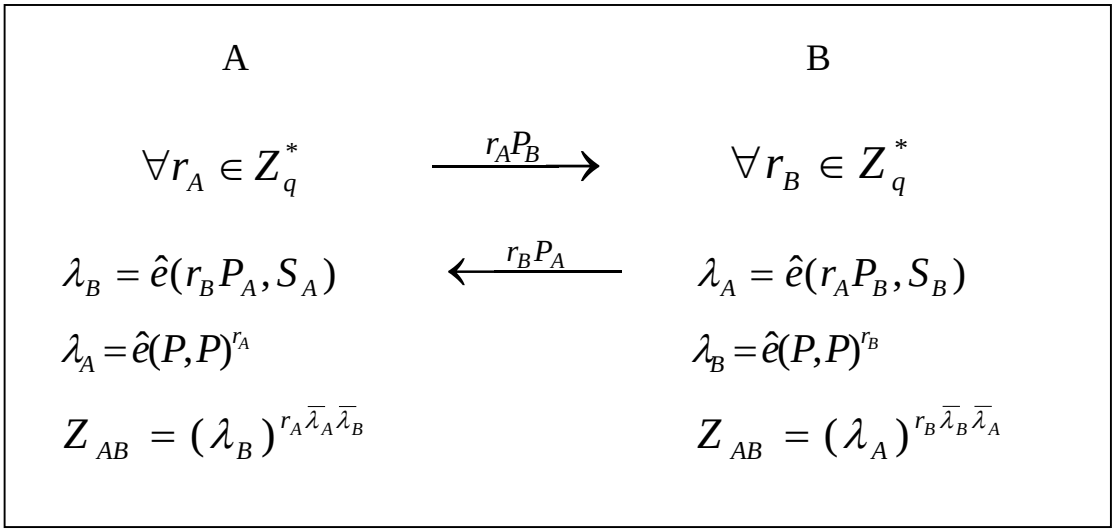

Figure 7: A New ID-2-AK Protocol (*ID-2-AKP I*)

Our modified protocol also provides other security properties as is provided in McCullagh, Barreto and Xie's, such as Known Key Security, Perfect Forward-Secrecy etc. . That is similar to the explanations to be described in section 6.2.

6.2 ID-2-AK Protocol II

Likewise section 4, with the help of the addition operation in the finite field, we will give another modified version. The algorithms of Setup and Extract are similar to McCullagh , Barreto and Xie's , except the + operation and a system public parameter $\hat{e}(P,P)$. Let p is an 1024 bits prime, q is an 160 bits prime divisor of p-1, G_1 is a q order subgroup of Z_p^* and G_2 is a q order subgroup of the multiplicative group F_p^* of finite field F_p. The + operation is the addition operation in finite field F_p.

The remainder modification is in the Key Agreement as is shown in Figure 8. The final shared secret is $Z_{AB} = \hat{e}(P,P)^{r_A r_B} + \hat{e}(P,P)^{r_A}\hat{e}(P,P)^{r_B}$. As the calculations is in finite field, so we know entity A and entity B share the same value above. We also know the value of the shared secret is in finite field F_p but not only in G_2. In order to avoid the particular value 0 which is the zero in finite field F_p, we select G_2 such that $\forall g \in G_2, -g \notin G_2$ ($-g$ is negative element of g in F_p). But it seems that it is very hard to find the desired G_2 and validate it for sure. But we can settle the matter by checking the shared key Z_{AB} and redoing a new key agreement after drawing it away while $Z_{AB} = o$.

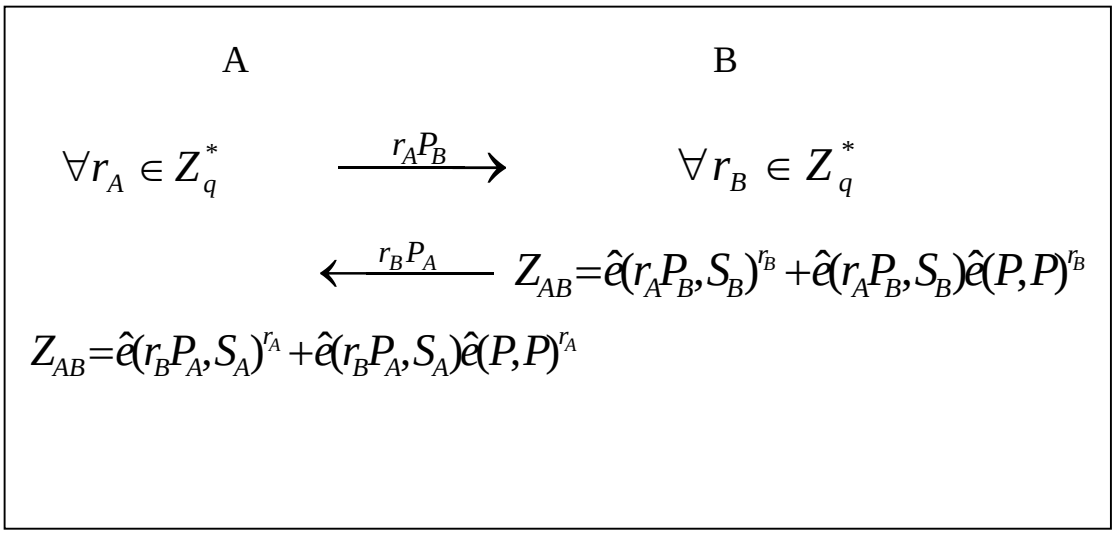

Figure 8: Another ID-2-AK Protocol (*ID-2-AKP II*)

Now we explain our protocol providing the desirable security attributes:

1. **Known-key security.** Each run of the key agreement between A and B produces a unique session key due to the random numbers r_A and r_B , and there are no ways to get some session key from other session keys.

2. **Forward secrecy.** Even if all the long-term private keys of A and B are compromised, it is hard to get $\hat{e}(P,P)^{r_A r_B}$ for the adversary that is indispensable in the calculation of Z_{AB}. This can be concluded by the assumptions in section 2.2. So the previous session keys are not affected.

3. **Key-compromise impersonation resistant attribute**. Suppose A's long-term private key is disclosed, the adversary C couldn't construct message to make KCI attack like Figure 6. Because C have no knowledge of either r_A or S_B and he couldn't kill $\hat{e}(P,P)^{r_A}$ which is indispensable in the calculation of Z_{AB}.

4. **Unknown key-share attribute.** As we know, the unknown key-share attack usually utilizes the method of tampering the public-key certificates. In ID-based key agreement since the public-keys are the identities and the public-key certificates are discarded, so unknown key-share attack is hard to be carried into execution and the security attribute of Unknown Key-Share resistant is naturally owned by all ID-based protocols.

5. **Key Control**. Neither entity should be able to force the session key to be a pre-selected value for they offer the random numbers r_A and r_B each other.

Our new ID-2-AKPs inherits other merits from McCullagh-Barreto. For example, it can be used Between Members of Distinct Domains as the shared secret has not the master key s and we can also modify the bilinear map to get an Authenticated Key Agreement Without Escrow likewise.

7. Comparison of computation and security

We have compared the security attributes between some famous protocols in Figure 9. There are only four protocols that provide all the desirable security attributes. But Shim's protocol was vulnerable to man-in-middle attack[28], so Wang's and ours are more secure than others.

Security attributes / Protocols	Know-key security	PFS	KCI	Unknown key share	Key Control
Smart[13]	√	×	√	√	√
Chen-Kudla[14]	√	×	√	√	√
Shim[16]	√	√	√	√	√
McCullagh-Barreto[6]	√	√	×	√	√
Xie[5]	√	√	×	√	√
Wang[18]	√	√	√	√	√
ID-2-AKP I	√	√	√	√	√
ID-2-AKP II	√	√	√	√	√

Figure 9: Comparison of the Security Attributes

At last we compare our new protocols with Wang's in computational cost. In the two ID-2-AK protocols, Pairing calculation is only once for A , i.e. $\hat{e}(r_B P_A, S_A)$, and used by twice. There is no other Pairing calculation, as the system public parameter $\hat{e}(P,P)$ is public. The same is to B and the result of comparison is shown in Figure 10.

Calculations \ Protocols	Wang' s	ID-2-AKP I	ID-2-AKP II
Pairing	1	1	1
EC Scalar Multiplication	3	2(1)	2(1)
EC Addition	1	1(1)	1(1)
Finite field Multiplication	1	2	1
Finite field Power-Multiplication		2	2
Finite field Addition	1		1
$\overline{X}$		2	
Hash	2		

Figure 10: Comparison of New ID-2-AKPs with Wang's in Computational Cost

As is known to all, the arithmetics in EC spend much more time than in finite field(see,[21,22]) .Modular arithmetic spends less time than Hash's arithmetic in evidence. With the help of pre-calculations (figures in brackets) our modified protocols needs less time in the calculations. So if we select a good arithmetic for finite field power-multiplication, the two new ID-2-AKPs are more efficient. Between the two new ID-2-AKPs, the ID-2-AKP II is superior to the ID-2-AKP I because it is only once finite-field-addition more than the latter but decreases the modular arithmetic $\overline{X}$ and once finite-field-multiplication. In protocol I it is important to choose some modular arithmetic. In protocol II we only need get good arithmetic for finite field and prevent the particular value in the key agreement by checking them. The selection of G_2 is also very important in protocol II from our analysis above.

8. Conclusion

We have proposed a new 2-AKP and two new ID-2-AKPs that are more security and more efficient than existing protocols. Furthermore, ID-2-AKP II is more efficient than ID-2-AKP I. Indeed, we have not proved our protocols to be secure. But several of these protocols were proved to be secure in the Bellare-Rogaway model for key agreement protocols and the proofs were found flawed later. For example, Chen and Kudla [14] proved that their protocol is secure in the Bellare-Rogaway model. However, Cheng et al. [22] pointed out that the proof in [14] is flawed. Similarly McCullagh , Barreto

and Xie's proofs in their protocols [5,6] are subsequently found invalid by Cheng et al. in [24]. The practical model of provable security is still expectant.

Acknowledgements

We would like to thank Mihir Bellare, Christian Cachin and Raymond Choo for their helpful advice on this paper and thank Guohong Xie for his kindly comments.

References

[1] A.J.Menezes, M.Qu & S.A.Vanstone. Some new key agreement protocols providing implicit authentication. In Workshop on Selected Areas in Cryptography(SAC'95),P22-32,1995.

[2] L.Law, A.Menezes, M.Qu, J.Solinas, S.Vanstone. An efficient protocol for authenticated key agreement. Designs,Codes and Cryptography. Marc 2003.

[3] IEEE. P1363 Standard Specifications for Public-Key Cryptography, January 2000. IEEE Std 1363-2000.

[4] Guohong 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. http://eprint.iacr.org/2004/308.

[5] Guohong Xie, An ID-Based Key Agreement Scheme from pairing, Cryptology ePrint Archive, Report2005/093, 2005. http://eprint.iacr.org/2005/093.

[6] N. McCullagh & P. S. L. M. Barreto, A New Two-Party Identity-Based Authenticated Key Agreement, Cryptology ePrint Archive, Report 2004/122, 2004. In Proceeding of CT-RSA 2005. http://eprint.iacr.org/2004/122.

[7] A. Menezes, P. vanOorschot, & S. Vanstone. Handbook of Applied Cryptograph. CRC Press. 1997.

[8] K. Shim. The Risks of Compromising Secret Information. ICICS 2002, LNCS 2513, pp. 122–133, 2002.

[9] S. B. Wilson, and A. Menezes, Authenticated Diffie-Hellman key agreement protocols, Proceedings of the 5th Annual Workshop on Selected Areas in Cryptography (SAC '98), Lecture Notes in Computer Science, pp. 339-361, 1999.

[10] C. Boyd & A.Mathuria. Protocols for Authentication and Key Establishment. Springer-Verlag Press. 2003.

[11] M. Just and S. Vaudenay, Authenticated multi-party key agreement, Advances in Cryptology, Asiacrypt'96, LNCS 537, pp. , 19.

[12] B. Song and K. Kim, Two-pass authenticated key agreemnet protocol with key confirmation, Progress in Cryptology, Indocrypto'00, LNCS 1977, pp. 237-249, 2000.

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

[14] L. Chen and C. Kudla. Identity based authenticated key agreement protocols from pairing. In: Proc. 16th IEEE Security Foundations Workshop, pages 219–233. IEEE Computer Society Press, 2003.

[15] M. Scott. Authenticated ID-based key exchange and remote log-in with insecure token and PIN number. http://eprint.iacr.org/2002/164.pdf

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

[17] M.C.Gorantla, R.Gangishetti and A.Saxena. A Survey on ID-Based Cryptographic Primitives. Cryptology ePrint Archive, Report2005/094, 2005. http://eprint.iacr.org/2005/094.

[18] Yongge Wang. Efficient Identity-Based and Authenticated Key Agreement Protocol. Cryptology ePrint Archive, Report2005/108, 2005. http://eprint.iacr.org/2005/108.

[19] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In Advances in Cryptology – Crypto'2001, volume 2139 of Lecture Notes in Computer Science, pages 213–229. Springer-Verlag, 2001.

[20] D. Boneh, B. Lynn, and H. Shacham, "Short signature from the Weil pairing," Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp.514-532, Springer-Verlag, 2001.

[21] E.D.Win & B.Preneel, Elliptic Curve Public-Key Cryptosystems: An Introduction, COSIC'97 Course, LNCS 1528, pp.131-141, 1998.

[22] M.Scott, Scaling Security in Pairing-Based Protocols, Cryptology ePrint Archive, Report2005/139, 2005. http://eprint.iacr.org/2005/139.

[23] Z. Cheng, M. Nistazakis, R. Comley, and L. Vasiu. On indistinguishability-based security model of key agreement protocols-simple cases. In Proc. of ACNS 04, June 2004.

[24] Z.Cheng & L.Chen, On Security Proof of McCullagh-Barreto's Key Agreement Protocol and its Variants, Cryptology ePrint Archive, Report2005/201, 2005. http://eprint.iacr.org/2005/201.

[25]. A. Menezes, T. Okamoto, and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Transaction on Information Theory*, Vol.39, pp.1639-1646,1993

[26]. G. Frey and H. Ruck, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves," *Mathematics of Computation*, Vol.62, pp.865-874,1994

[27] D. Boneh, B. Lynn, and H. Shacham, "Short signature from the Weil pairing," *Advances in Cryptology-Asiacrypt 2001*, LNCS 2248, pp.514-532, Springer-Verlag, 2001

[28] H.-M. Sun and B.-T. Hsieh, "Security Analysis of Shim's Authenticated Key Agreement Protocols from Pairings", Cryptology ePrint Archive, Report 2003/113.

[29] T.Matsumoto, Y.Takashima & H.Imai. On Seeking Smart Public-key-distribution systems. Transactions of the IECE of Japan,E69(2):99-106. February,1986.