Twords Security ID-based Two-party Authenticated Key Agreement Protocol

Songping Li [1], Jin Li [2] and Maozhi Xu[1]
[1]School of Mathematical Sciences, Peking University,P. R.China
{lsp,mzxu}@pku.edu.cn
[2]Huawei Technologies Co., Shenzhen, P. R.China
jingle@huawei.com

Abstract: In this paper we point out that Xie's ID-2-AKP (ID-based two-party authenticated key agreement protocol) [5] modified from McCullagh and Barreto's [6] which is proposed in CT-RSA 2005 doesn't provide protection against KCI attack likewise, and finally utilize the modular arithmetic, first proposed in MQV[1,2,3] and also used in Kim[8], to get a new modified ID-2-AKP which is more security and more efficient than existing protocols. We also compare our new protocol with Wang's [18] in terms of computational cost to show our new protocol is more efficient.
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 which 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 which is used to derive the shared secret key.

A key agreement protocol is desired to have this 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 protocol(AKP), while one providing explicit key authentication to both participating entities is called an authenticated key agreement with key conformation protocol (AKCP).

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. An AKP is called identity-based if in the protocol, users use an identity based asymmetric key pair

instead of a traditional public/private key pair for authentication and determination of the established key.

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.

Since the basic Diffie-Hellman key agreement scheme which 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-AKP 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 which can provide.

Based on Weil and Tate pairing techniques, Several practical ID-AKPs, 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-AKP which is modified from McCullagh-Barreto[6] and asserted it can resistant KCI attack. Wang[18] also presented a new security ID-AKP not long ago.

The remainder of the paper is organized as follows. In section 2, we briefly explain Kim's protocol and show how they can resist KCI attack in deed. In section 3, we give a KCI attack to Xie's modified protocol after giving an explanation of McCullagh-Barreto's protocol and Xie's modification. In section 4, we present a new ID-2-AKP which can surely provide protection against KCI attack and which is more efficient than Wang's protocol. The concluding remark will be followed in section 5.

2. 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 then select random values, r_A and r_B 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 shown in Figure 1. The shared secret is $Z_{AB} = g^{r_B s_A + \overline{Z}_A \overline{Z}_B r_A r_B + r_A s_B}$.

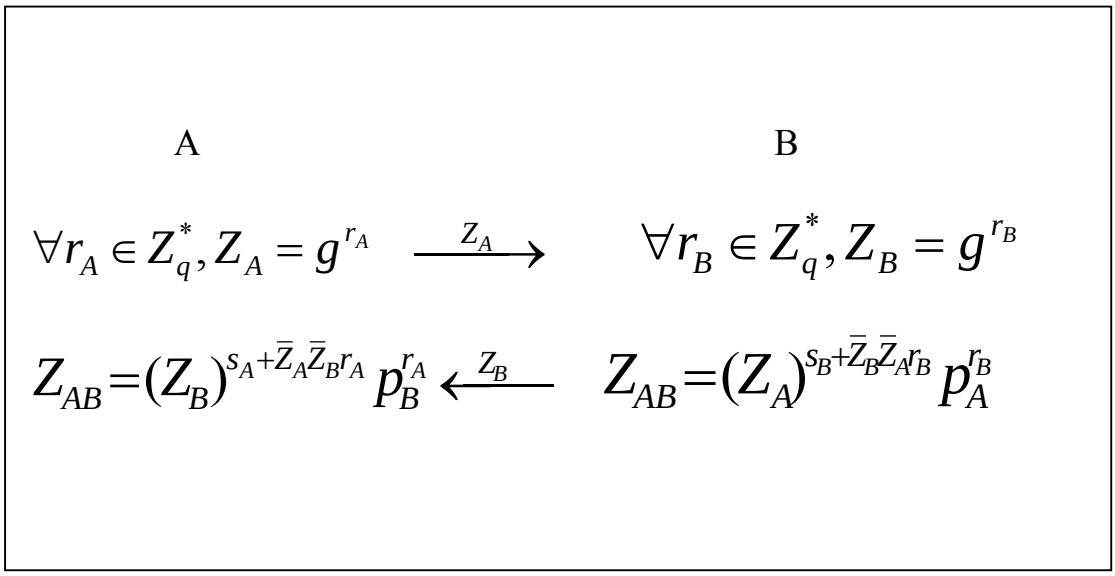

Figure 1: Kim's Protocol

Shim believes that an adversary C can not 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. $Z_B = g^{r_C} P_B^{\frac{-1}{\overline{Z}_A \overline{Z}_B}} = g^{r_C} (M)^{-1/\overline{Z}_B}$ (r_C is a random value selected by C, $M = P_B^{1/\overline{Z}_A}$). We know that M is a positive constant, so C should get Z_B by the solution of discrete equation $Z_B (M)^{1/\overline{Z}_B} = g^{r_C}$. $\forall r_C \in Z_q^*$, let $\overline{Z}_B = Z_B + k \cdot 2^{80}$ (k is a positive integer), and then we want to solve the equation $Z_B (M)^{1/\overline{Z}_B} = g^{r_C}$ 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. .

3. McCullagh-Barreto's Protocol and Xie's Modified Version

Resently, McCullagh and Barreto[6] proposed a ID-2-AKP 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-AKP[5] modified from that and asserted it can resistant KCI attack. But we find the modification is unsuccessful.

First we briefly explain 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 secure 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 2, and the shared secret is $Z_{AB} = \hat{e}(P,P)^{r_A r_B}$.

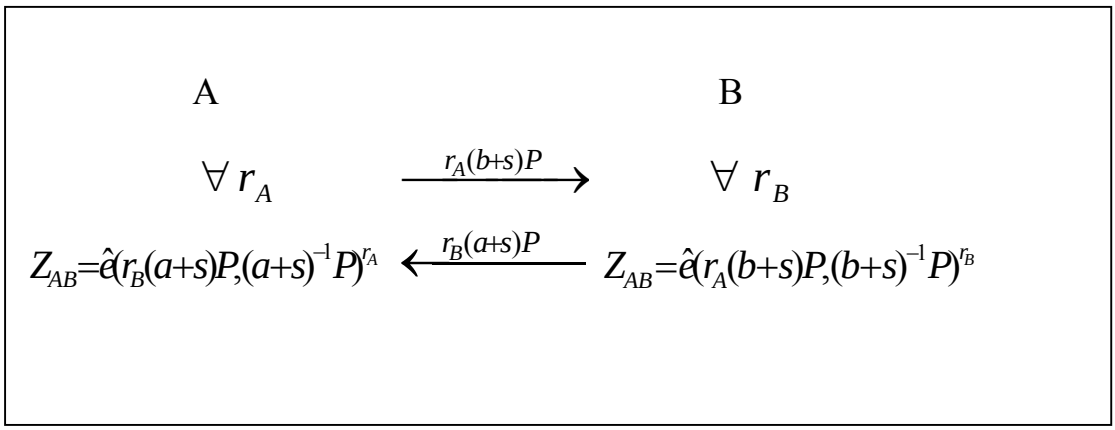

Figure 2: McCullagh-Barreto's Protocol

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 for the adversary C can calculate $Z_{AB} = \hat{e}(r_A(b+s)P,(b+s)^{-1}P)\hat{e}(r_B(a+s)P,(a+s)^{-1}P)$ to get the previous session keys .

Xie then gave a modified version to McCullagh-Barreto's protocol. His protocol only change 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 3.

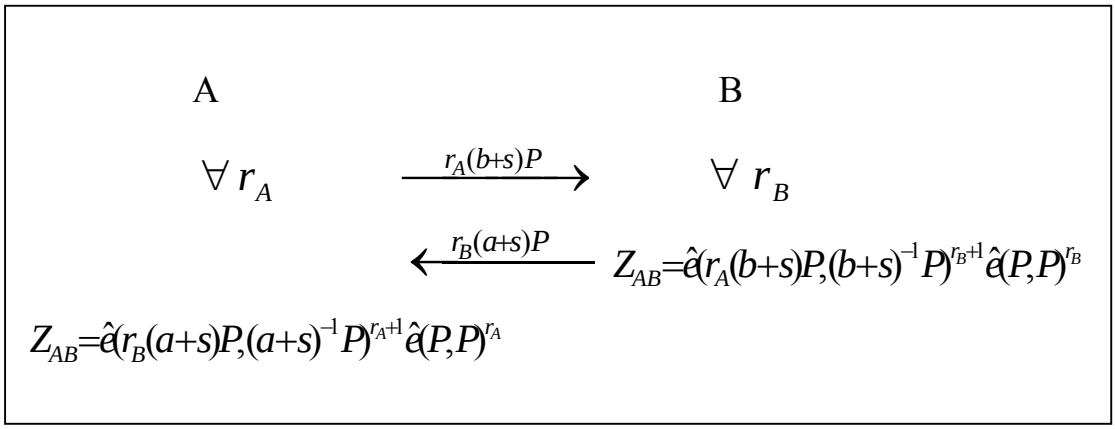

Figure 3: Xie's Protocol

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 which is shown in Figure 4 and gets the shared secret $Z_{AB}=\hat{e}(P,P)^{-1}$.

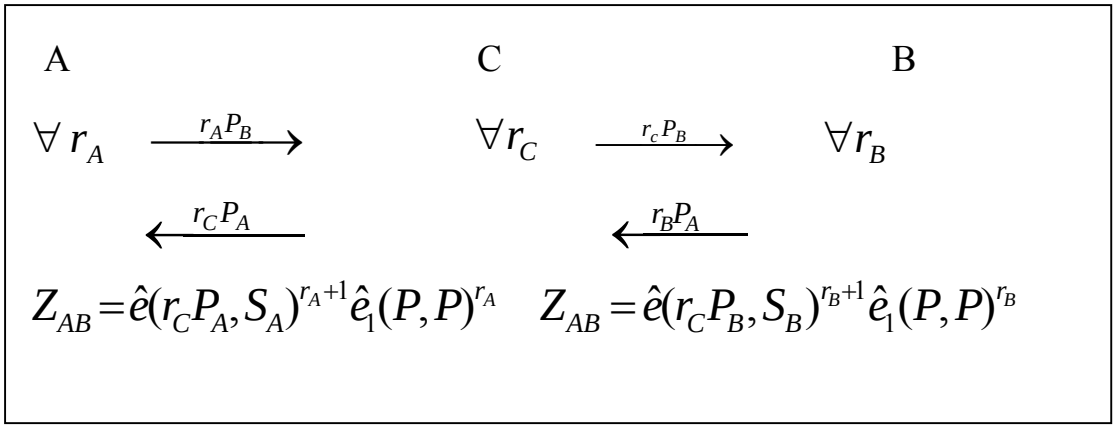

Figure 4: man-in-middle attack to Xie's Protocol

Although A and B can reject the random value -1from the other side to prevent it, 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 5. 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.

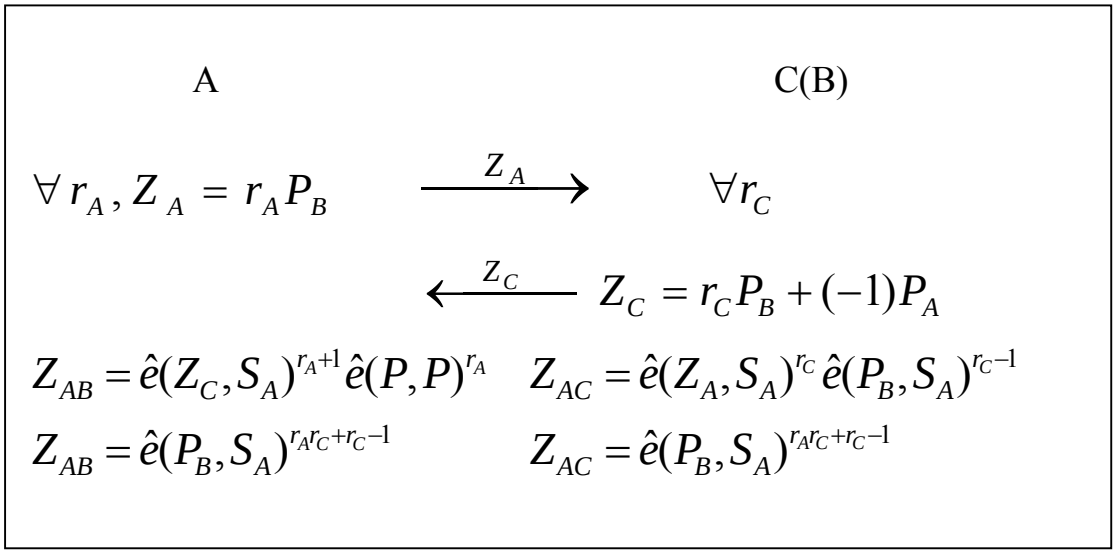

Figure 5: KCI attack to Xie's Protocol

4. A New ID-2-AKP

Inspired on Kim's protocol in section 2, here we give a modified version of McCullagh , Barreto and Xie's ID-2-AKPs [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 and has less computational cost than Wang's in [18].

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 6. 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 in section 2. 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} .

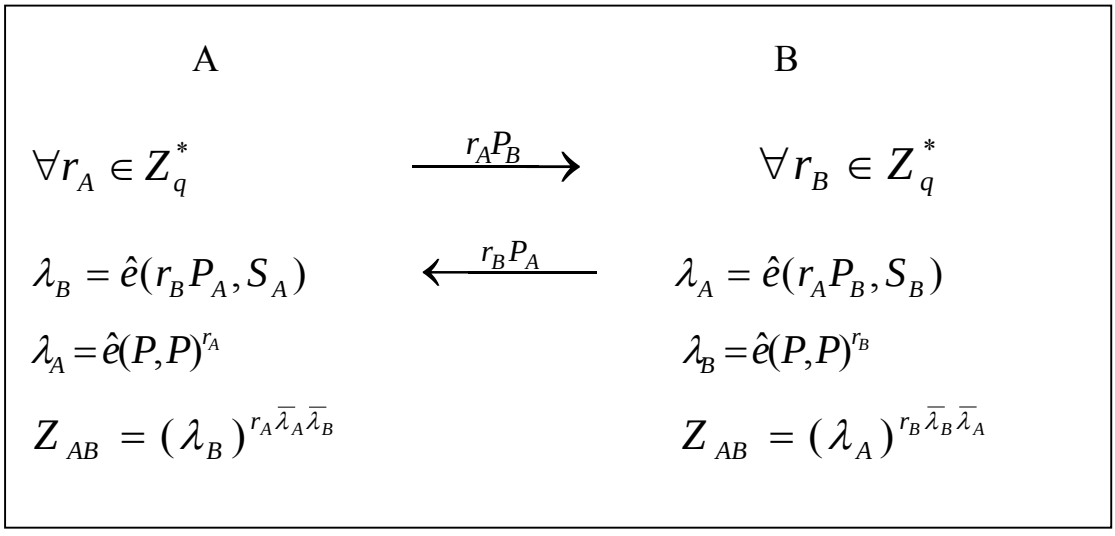

Figure 6: A New ID-2-AKP

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. We can also modify the bilinear map to get an

Authenticated Key Agreement Without Escrow likewise to get the security property which is entitled as TA-Forward-Secrecy in Wang[18]. Wang's protocol[18] can not be used Between Members of Distinct Domains as the shared secret has the master key s while the modified protocol can inheriting from McCullagh , Barreto and Xie's .

At last we compare our new protocol with Wang's in computational cost as is shown in Figure 7 :

Protocols→ ↓Calculations	Wang' s	New ID-2-AKP
Pairing	1	1
EC Scalar Multiplication	2	2(1)
EC Addition	1	1(1)
finite field Multiplication	1	2
finite field squaring		1
finite field Addition	1	
$\overline{X}$		2
Hash	4(2)	1(1)

Figure 7: Comparison of New ID-2-AKP with Wang's in Computational Cost

As is known to all, the arithmetics in EC spend more time than in finite field(see,[21,22]) , and modular arithmetic spends less time than Hash's arithmetic in evidence . So with the help of pre-calculations(figures in brackets) our modified protocol needs less time in the calculations .

5. Conclusion

We have proposed an new ID-2-AKP which are more security and more efficient

than existing protocols. 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 to be 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.

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.