ID2S Password-Authenticated Key Exchange Protocols

A.Sreedhar Reddy[1], Prof.M.Padmavathamma[2].
[1]*Student, Dept. of MCA, Sri venkateswara university, Tirupati.*
[2] *Professor, Dept. of MCA, Sri venkateswara university, Tirupati*

Abstract- **The paper Password authenticated key exchange (PAKE) is the process of where more than one parties, depends on their knowledge of the password only, establish a cryptographic key using an exchange of messages, for that an unauthorized party (who control a communication system but does not possess the password) cannot participate in the method and is constrained as much as possible from brute force guessing the password. Two forms of PAKE(Password authenticated key exchange) are Balanced and Augmented methods .In this the two-server password-authenticated key exchange (PAKE) protocol, the clients splits there password and stores two shares of there password in the two servers, respectively, and the two servers then cooperate to authenticate the client without knowing the password of the client. In case of one server is compromised to unauthorized party, the password of the client is required to secure in remaining server. In this paper, we present two compilers that transform any two-party PAKE protocol to a two-server PAKE protocol on the basis of the identity-based cryptography, called ID2S PAKE protocol. By the compilers, we can construct ID2S PAKE protocols which we achieve the implicit authentication. As long as the underlying two-party PAKE protocol and identity-based encryption or signature scheme have provable security without random oracles, the ID2S PAKE protocols constructed by the compilers can be proved to be secure without random oracles. Compare with a two-server PAKE protocol with provable security without random oracles, our ID2S PAKE protocol can save from 22% to 66% of computation in each server. Identity-based systems it allows any party to generate a public key from a known identity value such as an ASCII string values. And a trusted third party, called the Private Key Generator (PKG), generates a corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key. It Give the master public key, any party can compute a public key corresponding to the identity ID by combining the master public key with the identity value. To obtain a corresponding private key, the party authorized to use the identity ID contacts the PKG, which uses the master private key to generate the private key for identity ID.**

I. INTRODUCTION

TO secure communications between two parties, an authenticated encryption key is required to agree on in advance. So far, two models have existed for authenticated key exchange. One model assumes that two parties already share some cryptographically-strong information: either a secret key which can be used for encryption/authentication of messages, or a public key which can be used for encryption/ signing of messages. These keys are random and hard to remember. In practice, a user often keeps his keys in a personal device protected by a password/PIN. Another model assumes that users, without help of personal devices, are only capable of storing "human-memorable" passwords. Bellovin and Merritt [4] were the first to introduce password-based authenticated key exchange (PAKE), where two parties, based only on their knowledge of a password, establish a cryptographic key by exchange of messages. A PAKE protocol has to be immune to on-line and off-line dictionary attacks. In an off-line dictionary attack, an adversary exhaustively tries all possible passwords in a dictionary in order to determine the password of the client on the basis of the exchanged messages. In on-line dictionary attack, an adversary simply attempts to login repeatedly, trying each possible password. By cryptographic means only, none of PAKE protocols can prevent on-line dictionary attacks. But on-line attacks can be stopped simply by setting a threshold to the number of login failures. PAKE, numerous PAKE protocols have been proposed. In general, there exist two kinds of PAKE settings, one assumes that the password of the client is stored in a single server and another assumes that the password of the client is distributed in multiple servers. PAKE protocols in the single-server setting can be classified into three categories as follows.

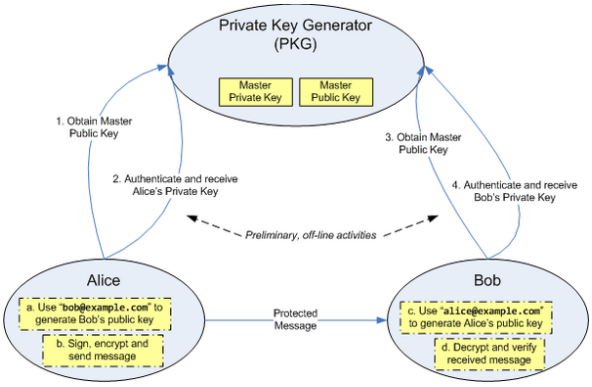
Password-only PAKE: Typical examples are the "encrypted key exchange" (EKE) protocols given by Bellovin and Merritt [4], where two parties, who share a password, exchange messages encrypted by the password, and establish a common secret key. The formal model of security for PAKE was firstly given in [3], [8]. Based on the security model, PAKE protocols [10], [11], [16] have been proposed and proved to be secure.

PKI-based PAKE: PKI-based PAKE protocol was first given by Gong et al. [17], where the client stores the server's public key in addition to share a password with the server. Halevi and Krawczyk [18] were the first to provide formal definitions and rigorous proofs of security for PKI-based PAKE.

ID-based PAKE: ID-based PAKE protocols were proposed by Yi et al. [32], [33], where the client needs to remember a password in addition to the identity of the server, whereas the server keeps the password in addition to a private key related to its identity. ID-based PAKE can be thought as a trade-off between password-only and PKI-based PAKE. In the single-server setting, all the passwords necessary to authenticate clients are stored in a single server. If the server is compromised, due to, for example, hacking or even insider attacks, passwords stored in the server are all disclosed. This is also true to Kerberos [12], where a user authenticates against the authentication server with his username and password and obtains a token to authenticate against the service server. To address this problem, the multi-server setting for PAKE was first suggested in [15], [19], where the password of the client is distributed in n servers. PAKE protocols in the multi-server setting can be classified into two categories as follows.

Threshold PAKE: The first PKI-based threshold PAKE protocol was given by Ford and Kaliski [15], where n severs, sharing the password of the client, cooperate to authenticate the client and establish independent session keys with the client. As long as n 1 or fewer servers are compromised, their protocol remains secure. Jablon [19] gave a protocol with similar functionality in the password-only setting. MacKenzie et al. proposed a PKI-based threshold PAKE protocol which requires only t out of n servers to cooperate in order to authenticate the client. Their protocol remains secure as long as t 1 or fewer servers are compromised. Di Raimondo and Gennaro [26] suggested a password-only threshold PAKE protocol which requires fewer than 1/3 of the servers to be compromised.

Two-server PAKE: Two-server PKI-based PAKE was first given by Brainard [9], where two servers cooperate to authenticate the client and the password remains secure if one server is compromised. A variant of the protocol was later proved to be secure in [27]. A two-server password-only PAKE protocol was given by Katz et al. [23], in which two servers symmetrically contribute to the authentication of the client. The protocol in the server side can run in parallel. Efficient protocols [21], [29], [30], [31] were later proposed, where the front-end server authenticates the client with the help of the back-end server and only the front-end server establishes a session key with the client. These protocols are asymmetric in the server side and have to run in sequence. Yi et al. gave a symmetric solution [34] which is even more efficient than asymmetric protocols [21], [29], [30], [31]. Recently, Yi et al. constructed an ID2S PAKE protocol with the identity-based encryption scheme (IBE) [35]. To address this problem, the multi-server setting for PAKE was first suggested in [15], [19], where the password of the client is distributed in n servers.



II.EXISTING SYSTEM

Earlier password-based authentication systems transmitted a cryptographic hash of the password over a public channel which makes the hash value accessible to an attacker. When this is done, and it is very common, the attacker can work offline, rapidly

testing possible passwords against the true password's hash value. Studies have consistently shown that a large fraction of user-chosen passwords are readily guessed automatically. The following are the some drawbacks of an existing system : The hash value accessible to an attacker, the attacker can work offline, rapidly testing possible passwords against the true password's hash value, An adversary can always succeed by trying all passwords one-by-one in an on-line impersonation attack. A protocol is secure if this is the best an adversary can do. The on-line attacks correspond to Send queries.

III.PROPOSED SYSTEM

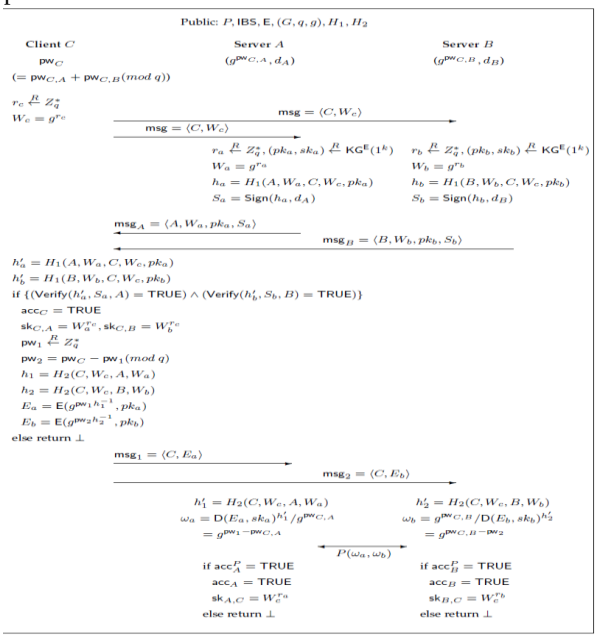
The examples are the "encrypted key exchange" (EKE) protocols given by Bellovin and Merritt, where two parties, who share the password, and exchange messages encrypted by the password, and establish the common secret key. The formal model of a security for PAKE was firstly Based on a security model, PAKE protocols have been proposed for secure and proved to be secure. A security model for ID2S PAKE protocol was given and a compiler that transforms any two-party PAKE protocol to an ID2S PAKE protocol was proposed on the basis of the Cramer-Shoup public key encryption scheme and any identity-based encryption scheme, such as the Waters' scheme. The second model is called password-only model. The persons Merritt and Bellovin was the first who to consider authentication based on the password only, and they introduced a set of so-called "encrypted key exchange" protocols, where the password is used as a secret key to encrypt random numbers for key exchange purpose. Formal models of the security for the password-only authentication were first given independently by Bellare et al. and Boyko et al.. Katz et al. were the first to give a password-only authentication protocol which is both practical and provably secure under standard cryptographic assumption.

Modules Description

We present two compilers transforming any two-party PAKE protocol P to an ID2S PAKE protocol P0 with identity-based cryptography. The first compiler is built on identity-based signature (IBS) and the second compiler is based on identity-based encryption (IBE).

1.ID2S PAKE Based on IBS.

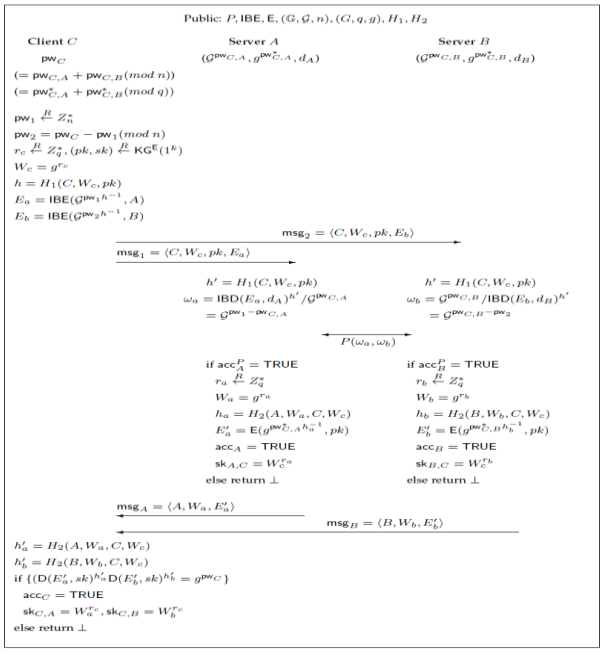
We need an identity-based signature scheme (IBS) as our cryptographic building block. A high-level description of our compiler in which the client C and two servers A and B establish two authenticated keys, respectively. If we remove authentication elements from our compiler, our key exchange protocol is essentially the Diffie-Hellman key exchange protocol. We present the protocol by describing initialization and execution. The Diffie-Hellman key exchange protocol was invented by Diffie and Hellman in 1976. It was the first practical method for two users to establish the shared secret key over an unprotected communications channel. Although it is a non authenticated key exchange protocol, it provides the basis for a variety of authenticated protocols. Diffie-Hellman key exchange protocol is followed shortly afterward by RSA, the first practical public key cryptosystem. Key Generation: On input the identity S of a server S 2 Server, params IBS, and the secret sharing master-key IBS, PKGs cooperate to run Extract IBS of the IBS scheme and generate a private (signing) key for S, denoted as in a manner that any coalition of PKGs cannot determine dS as long as one of the PKGs is honest to follow the protocol.



2. ID2S PAKE Based on IBE.

A high-level description of our compiler based on identitybased encryption. We present the protocol by describing initialization and execution. Key

Generation: On input the identity S of a server S 2 Server, paramsIBE, and the secret sharing master-keyIBE, PKGs cooperate to run ExtractIBE of the IBE scheme and generate a private (decryption) key for S, denoted as dS, in a manner that any coalition of PKGs cannot determine dS as long as one of the PKGs is honest to follow the protocol. Each user has a private key x Each user has three public keys: prime modulus p, generator g and public Y = gxmod p Security is based on the difficulty of DLP Secure key size > 1024 bits (today even 2048 bits) Elgamal is quite slow, it is used mainly for key authentication protocols. Protocol Execution. Given a triple (C; A;B) 2 Client ServerTriple, the client C (knowing its password pwC) runs the protocol P0 with the two servers A (knowing GpwC;A , gpwC;A and its private key dA) and B (knowing GpwC;B , gpw C;B and its private key dB) to establish two session keys, respectively. At first, the client randomly chooses pw1 from Zn and computes pw2 = pwC □ pw1(mod n). Next the client C randomly generates a one-time public and private key pair (pk; sk) for the public key encryption scheme E, and randomly chooses an integer rc from Zq and computes Wc = grc ; h = H1(C;Wc; pk): Next, according to the identities of the two servers A and B, the client C performs the identity-based encryptions Ea = IBE(Gpw1h□1 ;A);Eb = IBE(Gpw2h□1 ;B): Then, the client sends msg1 = hC;Wc; pk;Eai and msg2 = hC;Wc; pk;Ebi to the two servers A and B, respectively.



3. Initialization

The two peer servers S1 and S2 jointly choose a cyclic group G of large prime order q with a generator g1 and a secure hash function H : {0; 1}*->Zq, which maps a message of arbitrary length into an l-bit integer, where l= log2 q. Next, S1 randomly chooses an integer s1 from Zq and S2 randomly chooses an integer s2 from Zq , and S1 and S2 exchange g1s1 and g1s2 . After that, S1 and S2 jointly publish public system parameters G; q; g1; g2;H where g2 = gs1s2 .

4.Registration

The two secure channels are necessary for all two server PAKE protocols, where a password is split into two parts, which are securely distributed to the two servers, respectively, during registration. Although we refer to the concept of public key cryptosystem, the encryption key of one server should be unknown to another server and the client needs to reme0mber a password only after registration.

IV. CONCLUSION

Here we give two efficient compilers to transform any two-party paper Password authenticated key exchange(PAKE) protocol to a ID2S PAKE protocol with the identity-based cryptography. In addition, we have to provide a rigorous proof of security for our compilers without random oracle. Our compilers are in particular suitable for the applications of password-based authentication where an identity-based system has already established. Our future work is to construct an identity-based multiple server PAKE protocol with any two-party PAKE protocol.

REFERENCES

[1] M. Abdalla, P. A. Fouque, and D. Pointcheval. Password-based authenticated key exchange in the three-party setting. In Proc. PKC'05, pages 65-84, 2005.1. https://crypto.stanford.edu/pbc/download.html 2. https://gmplib.org/ 3. https://tls.mbed.org/

[2] M. Abdalla and D. Pointcheval. Simple password-based encrypted key exchange protocols. In Proc. CT-RSA 2005, pages 191-208,2005.

[3] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In Proc. Eurocrypt'00,pages 139-155, 2000.

[4] S. M. Bellovin and M. Merritt. Encrypted key exchange: Passwordbased protocol secure against dictionary attack. In Proc. 1992 IEEE Symposium on Research in Security and Privacy, pages 72-84, 1992.

[5] J. Bender, M. Fischlin, and D. Kugler. Security analysis of the PACE key-agreement protocol. In Proc. ISC'09, pages 33-48, 2009.

[6] J. Bender, M. Fischlin, and D. Kugler. The PACEjCA protocol for machine readable travel documents. In INTRUST'13, pages 17-35, 2013.

[7] D. Boneh and M. Franklin. Identity based encryption from theWeil pairing. In Proc. Crypto'01, pages 213-229, 2001.

[8] V. Boyko, P. Mackenzie, and S. Patel. Provably secure passwordauthenticated key exchange using Diffie-Hellman. In Proc. Eurocrypt' 00, pages 156-171, 2000.

[9] J. Brainard, A. Juels, B. Kaliski, and M. Szydlo. Nightingale: A new two-server approach for authentication with short secrets. InProc. 12th USENIX Security Symp., pages 201-213, 2003.

[10] E. Bresson, O. Chevassut, and D. Pointcheval. Security proofs for an efficient password-based key exchange. In Proc. CCS'03, pages 241-250, 2003.

[11] E. Bresson, O. Chevassut, and D. Pointcheval. New security results on encrypted key exchange. In Proc. PKC'04, pages 145-158, 2004.

[12] B. Clifford Neuman and Theodore Ts'o. Kerberos: An authentication service for computer networks. IEEE Communications, 32 (9): 33-38, 1994.

[13] R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Proc. Crypto'98, pages 13-25, 1998.

[14] W. Diffie and M. Hellman. New directions in cryptography. IEE Transactions on Information Theory, 32(2): 644-654, 1976.

[15] W. Ford and B. S. Kaliski. Server-assisted generation of a strong secret from a password. In Proc. 5th IEEE Intl. Workshop on Enterprise Security, 2000.

[16] O. Goldreich and Y. Lindell. Session-key generation using human passwords only. In Proc. Crypto'01, pages 408-432, 2001.

[17] L. Gong, T. M. A. Lomas, R. M. Needham, and J. H. Saltzer. Protecting poorly-chosen secret from guessing attacks. IEEE J. on Selected Areas in Communications, 11(5):648-656, 1993.

[18] S. Halevi and H. Krawczyk. Public-key cryptography and password protocols. ACM Transactions on Information and System Security, 2(3):230-268, 1999.

[19] D. Jablon. Password authentication using multiple servers. In Proc. CT-RSA'01, pages 344-360, 2001.

[20] S. Jiang and G. Gong. Password based key exchange with mutual authentication. In Proc. SAC'04, pages 267-279, 2004.

[21] H. Jin, D. S. Wong, and Y. Xu. An efficient password-only twoserver authenticated key exchange system. In Proc. ICICS'07, pages 44-56,2007

[22] J. Katz, R. Ostrovsky, and M. Yung. Efficient passwordauthenticated key exchange using human-memorable passwords. In Proc. Eurocrypt'01, pages 457-494, 2001.

[23] J. Katz, P. MacKenzie, G. Taban, and V. Gligor. Two-server password-only authenticated key exchange. In Proc. ACNS'05, pages 1-16, 2005.

[24] P. MacKenzie, T. Shrimpton, and M. Jakobsson. Threshold password-authenticated key exchange. J. Cryptology, 19(1): 27-66, 2006.

[25] K. G. Paterson and J. C.N. Schuldt. Efficient identity-based signatures secure in the standard model. In ACISP'06, pages 207-222, 2006.

[26] M. Di Raimondo and R. Gennaro. Provably Secure Threshold Password-Authenticated Key Exchange. J. Computer and System Sciences, 72(6): 978-1001 (2006).

[27] M. Szydlo and B. Kaliski. Proofs for two-server password authentication. In Proc. CT-RSA'05, pages 227-244, 2005.

[28] B. Waters. Efficient identity-based encryption without random oracles. In Proc. Eurocrypt'05, pages 114-127, 2005.

[29] Y. Yang, F. Bao, R. H. Deng. A new architecture for authentication and key exchange using password for federated enterprise. In Proc. SEC'05, pages 95-111, 2005.

[30] Y. Yang, R. H. Deng, and F. Bao. A practical password-based two-server authentication and key exchange system. IEEE Trans. Dependable and Secure Computing, 3(2), 105-114, 2006.