A New Secure Protocol for Authenticated Key Agreement

H. Elkamchouchi, M. R. M. Rizk, and Fatma Ahmed

***Abstract*—Authenticated key agreement protocols have an important role in building secure communications between two or more parties over the open network. In this paper we propose an efficient and secure authenticated key agreement protocol based on RSA factoring and Discrete Logarithm Problem (DLP). We try to design strong protocol depends on the relation between two assumption (RSA factoring and DLP). We show that our protocol meets the security attributes and strong against most of potential attacks.**

***Index Terms*—DLP, key agreement, RSA factoring.**

I. Introduction

In order for two parties to communicate securely over an unreliable public network, they must be able to authenticate one another and agree on a secret encryption key. To achieve this, key establishment protocols are used at the start of a communication session in order to verify the parties' identities and establish a common session key. There are two basic categories of protocols. The first includes so-called key transport protocols, in which the session key is created by one entity and is securely transmitted to the other. A second category includes key agreement protocols, where information from both entities is used to derive the shared secret key. A protocol is said to be symmetric if both entities a-priori possess some common secret data, and asymmetric if the two entities share only authenticated public information [1].

The most well-known assumptions of public-key cryptographic algorithms are the computational problems of a discrete logarithm (DL) with complexity $O(e^{((\ln p)^{(1/3)}(\ln(\ln p))^{(2/3)})})$ [2], an elliptic curve (EC) with complexity $O(e^{(1.098+o(1))n^{1/3}(\ln(\ln p))^{(2/3)})})$, in GF (2^n) finite fields [3], and factoring (RSA) with the same complexity as a DL [4]. The most famous protocol for key agreement was proposed by Diffie and Hellman which is based on concept of public-key cryptography (DL) [5]. There are two versions of the Diffie-Hellman protocol namely static and ephemeral. In the first one, the entities exchange static public keys, and in the second, the entities exchange ephemeral public keys.

Therefore, the static protocol has a major drawback, is that the entities A and B compute the same session key for each run of the protocol. Also the ephemeral Diffie-Hellman protocol is vulnerable to a man-in-the-middle attack.

Manuscript received November 16, 2012; revised January 21, 2013.

Hassan M. Elkamchouchi and Mohamed Rizk are with the Electrical Engineering Department, Faculty of Engineering, Alexandria University, Alexandria, Egypt (e-mail: Helkamchouchi@ieee.org, mrmrizk@ieee.org).

Fatma Ahmed is with the Electrical Engineering Department, Alexandria Higher Institute of Engineering and Technology, Alexandria, Egypt (e-mail:moonyally@yahoo.com).

In order to counter these weaknesses, a new authenticated key agreement protocol is introduced in this paper. The important feature of the proposed protocol is the established session key is formed as combination of static and ephemeral private keys of two entities A and B. Also in our protocol we provide desirable performance attributes. The discussion shows the present protocol meets the most security and efficiency attributes.

II. Proposed Key Agreement Protocol

We design a new protocol for authenticated key agreement that is secure, efficient and provides authentication between two entities before exchanging the session keys. The new protocol consists of three phases; The Registration Phase, The Transfer and Substantiation Phase, and The Key Generation Phase.

A. Notations Used

The notation used in this paper is included as following:

- p' : Long-term secret is large prime chosen by entity A (at least 512 bits).
- q' : Long-term secret is large prime chosen by entity B (at least 512 bits).
- p : Long-term secret is large safe prime: $(n'p'+1)$ normally at least 512 bits.
- q : Long-term secret is large safe prime: $(n'q'+1)$ normally at least 512 bits.
- n' : Small prime number (normally equal 2).
- n : Long-term public key, $n = pq$ (at least 1024 bits).
- $n1$: Long-term secret, Euler's totient function $n1 = (p-1)(q-1)$.
- G : Subgroup of Z_p^* of order $p'q'$.
- g : Generator of G .
- r_A, r_B : Short-term private keys are random integers: $2 \le r_A, r_B < n1$ and $GCD(r, n1) = 1$.
- t_A, t_B : Short-term public keys: $t_A \equiv g^{r_A} \bmod n$ and $t_B \equiv g^{r_B} \bmod n$.
- x_A, x_B Long-term private keys are random integers: $2 \le x_A, x_B < n1$ and $GCD(x, n1) = 1$.
- y_A, y_B : Long-term public keys: $y_A \equiv g^{x_A} \bmod n$ and $y_B \equiv g^{x_B} \bmod n$.
- K_{AB} : The shared secret key calculated by the principals.

B. The New Protocol Description

In this section we describe a proposed authenticated key

DOI: 10.7763/IJET.2013.V5.551

agreement protocol between two parties A and B . The protocol works in the following steps:

1) The registration phase

Each user like A and B selects a safe primes p and q , then calculates $n = pq$ and generator g . Each user selects two static secret keys x_A and x_B , such that $2 \le x_A, x_B < n1$.

Next calculates $y_A \equiv g^{x_A} \bmod n$, $y_B \equiv g^{x_B} \bmod n$ and registers y_A , y_B to the public file.

2) The transfer and substantiation phase

1) A generates the ephemeral key r_A such that $2 \le r_A < n1$, then calculates $t_A \equiv g^{r_A} \bmod n$ and $\bar{r}_A$ from r_A $\bar{r}_A \equiv 1 \bmod n1$.
2) B generates the ephemeral key r_B such that $2 \le r_B < n1$, then calculates $t_B \equiv g^{r_B} \bmod n$ and $\bar{r}_B$ from r_B $\bar{r}_B \equiv 1 \bmod n1$.
3) A calculates $s_1 \equiv (y_B)^{-r_A} \bullet (t_B)^{x_A} \equiv g^{x_A r_B - x_B r_A} \bmod n$ and sends outs it to B .
4) B calculate $s_2 \equiv (y_A)^{-r_B} \bullet (t_A)^{x_B} \equiv g^{x_B r_A - x_A r_B} \bmod n$ and sends outs it to A .
5) A receives B 's value and checks:

$$v_2' = \left((t_B)^{x_A} \bullet s_2\right) \equiv g^{r_B x_A} \bullet g^{x_B r_A - x_A r_B} \equiv y_B{}^{r_A} \bmod n$$

$$v_2 \equiv \left(v_2'\right)^{\bar{r}_A} \bmod n$$

$$\equiv g^{x_B} \bmod n \equiv y_B$$

If the comparison is true, then it accepts the received vector.

6) B receives A 's value and checks:

$$v_1' \equiv \left((t_A)^{x_B} \bullet s_1\right) \equiv g^{r_A x_B} \bullet g^{x_A r_B - x_B r_A} \equiv y_A{}^{r_B} \bmod n$$

$$v_1 \equiv \left(v_1'\right)^{\bar{r}_B} \bmod n$$

$$\equiv g^{x_A} \bmod n \equiv y_A$$

If the comparison is true, it accepts the received vector.

3) The key generation phase

7) A calculates the session key

$$K_{AB} \equiv y_B{}^{r_A} \bullet t_B{}^{x_A} \bullet t_B{}^{r_A} \equiv g^{x_B r_A + x_A r_B + r_A r_B} \bmod n$$

If the comparison is not true, A will reject the received vector.

8) B calculates the session key

$$K_{AB} \equiv y_A{}^{r_B} \bullet t_A{}^{x_B} \bullet t_A{}^{r_B} \equiv g^{x_A r_B + x_B r_A + r_A r_B} \bmod n$$

Unless the comparison is true, B will reject the received vector.

In our protocol, we have only one message sends from one entity to another. The message sends from A to B and the message sends from B to A both have the same structure and independent on each other. The total number of transmitted bits (communication overhead) is $|n|$. Our protocol has low complexity (complexity is 4) since we need only four exponential operations. So our protocol provides desirable performance attributes. The following figure shows the overall operation in our new protocol.

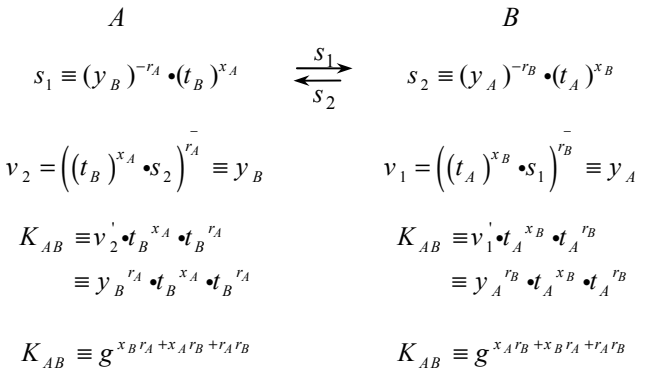

Fig. 1. Overall operation in the proposed protocol

III. Security Consideration

Our protocol involves both RSA factoring and DL cryptographic assumptions. Although, this protocol involves two cryptographic assumptions, their security relation is a logic AND relationship. To our knowledge, one possible way for an attacker to break this protocol is to first factor n into two large primes (p and q) and then solves the DL in order to find either the long-term or the short-term private key from its long-term or short-term public key, respectively. This is similar to a safe deposit box in a bank. To break a safe deposit box, one would have to break into the strong room, and then break the box. Because these two assumptions are logic AND related (in particular, RSA factoring comes before the DL) [6]. RSA factoring has the same complexity as a DL. The security of this protocol depends on the more secure of the two assumptions, which is RSA factoring. Here we prove our protocol meets the following desirable security attributes [7] [8].

Known-Key Security (K-KS): A protocol should still achieve its goal in the face of an adversary who has learned some other session keys. The session key is a unique secret key which in each run of a key agreement protocol between A and B is produced.

The proposed protocol provides known-key security. Each run of the protocol between two parties A and B should produce a unique session key which depends on r_A and r_B . Although an opponent has learned some other session keys, he can't compute ephemeral private keys r_A and r_B . Therefore the protocol still achieves its goal in the face of the opponent.

(Perfect) 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.

The protocol also possesses forward secrecy. Suppose that static private keys x_A and x_B of two parties are compromised. Even so, the secrecy of previous session keys established by honest parties is not affected, because an opponent who captured their private keys x_A or x_B should extract the

ephemeral keys r_A or r_B from the exchanged values to know the previous or next session keys between them. However, this is RSA factorization problem and DLP (Discrete Logarithm Problem).

Key-Compromise Impersonation (K-CI): When A 's static private key is compromised, it may be desirable that this event does not enable an adversary to impersonate other entities to A .

Suppose A 's long-term private key x_A , is disclosed. Now an opponent who knows this value can clearly impersonate A . But he can't impersonates B to A without knowing the B 's long-term private key x_B . For the success of the impersonation, the opponent must know A 's ephemeral key r_A . So, also in this case, the opponent should extract the value r_A from $t_A \equiv g^{r_A} \bmod n$, this is DLP, and then compute $\bar{r}_A$ from $r_A \bar{r}_A \equiv 1 \bmod n1$ which is RSA factorization problem.

Unknown Key-Share (UK-S): 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 $C \neq A$, and A correctly believes the key is shared with B .

Our protocol also prevents unknown key-share. Consequent to the assumption of this protocol that s_1 has verified that A possesses the private key x_A corresponding to his static public key y_A , an opponent can't register A 's public key y_A as its own and subsequently deceive B into believing that A 's messages are originated from the opponent. Therefore B cannot be coerced into sharing a key with entity A without B 's knowledge.

Subgroup Confinement Attack: Also small subgroup attack [9], the generator g in is a primitive root of the prime p . If the selected prime p is such that $p-1$ has several small prime factors, then some values between 1 and $p-1$ do not generate groups of order $p-1$, but of subgroups of smaller orders. If the public parameter of either A or B lies within one of these small subgroups, so the shared secret key would be confined to that subgroup. The intruder may launch a brute force attack to determine the exact value of the shared secret key.

The Solution to counter this kind of an attack is to choose a Safe Prime and use g that generates a large prime order subgroup or at the very least make sure that composite order subgroup are not vulnerable for instance the order's prime number factorization contains only large primes, which we provided in our protocol, we choose two safe prime numbers and use generator of order $p'q'$.

IV. Conclusion

In this paper we proposed a secure and efficient protocol for authenticated key agreement based on RSA factoring. We proved that our protocol meets the security attributes under the assumption that the RSA factorization problem and DLP. Our protocol is more efficient and provides desirable performance attributes which is, minimal number of passes because every party sends only one message to another party. Each message transmitted has the same structure (role symmetry) and are independent of each other (non-interactiveness). So our protocol can be used to improve the security in an open Internet network.

References

[1] K. Chalkias, F. Mpaldimtsi, D. H. Varsakelis, and G. Stephanides, "On the Key-compromise impersonation vulnerability of one-pass key establishment protocols," in *Proc. International Conference on Security and Cryptography (SECRYPT 2007)*, Barcelona, Spain, July 28-31, 2007.

[2] T. Beth, M. Frisch, and G. Simmons, "Public-key cryptography: State of the art and future directions," Springer-Verlag, New York, USA, 1991.

[3] A. Menezes, "Elliptic curve public key cryptosystems," *Kluwer Int. Ser. Eng. Computer. Sci*., Kluwer, vol. 234, 1993.

[4] A. Lenstra and H. J. Lenstra, "The development of the number field sieve," *Lect. Notes Math.*, 1993.

[5] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-l 22, no. 6, PP. 644-654, November, 1976.

[6] L. Harn, W. J. Hsin, and M. Mehta, "Authenticated diffie-hellman key agreement protocol using a single cryptographic assumption," *IEEE Proceedings on Communications*, vol. 152, no. 4, pp. 404-410, 2005.

[7] S. B. Wilson and A. Menezes, "Authenticated diffie-hellman Key Agreement Protocols," in *Proceedings of the 5th Annual Workshop on Selected Areas in Cryptography (SAC '98)*, Kingston, Canada, 1999, pp. 339-361.

[8] K. A. Sultan, M. Saeb, M. Elmessiery, and U. A. Badawi, "A new two-pass key agreement protocol, Proceedings of the IEEE Midwest 2003 Symp," *Circuits, Systems and Computers*, pp. 509-511, vol. 1, 2003.

[9] A. P. Kate, P. S. Kalekar, and D. Agrawal, "Weak Keys in Diffie-Hellman Protocol," *Indian Institute of Technology*, Powai, Mumbai -400076, November 15, 2004.

H. Elkamchouchi obtained his B.Sc Electrical Communication Engineering - Excellent with First Class Honors - Faculty of Engineering - Alexandria University - June 1966, Master Communications Engineering (specialization accurate: antennas and propagation) - Faculty of Engineering - Alexandria University - September 1969, B.Sc of Science in Applied Mathematics - Excellent with honors - Britain's Royal College of Science - University of London - England - August 1970, Doctor Communications Engineering (specialization accurate: antennas and propagation) - Faculty of Engineering - Alexandria University - March 1972. He work Professor Emeritus, Faculty of Engineering, Alexandria University from September 2003 until now. He is Life Senior Member IEEE No 06656565 starting from first January 2009 till now, a member of the National Committee for Radio Science in the Arab Republic of Egypt - Academy of Scientific Research - Cairo since 1990 until now, member of the Association of Egyptian engineers., member of the Standing Scientific Committee for electronics and biomedical measurements and engineering functions professors - the Supreme Council of Universities in the period from 2002 to 2005 and then an arbitrator in the same Commission has so far completed the examination and testing of more than 66 cases., member of the Preparatory Committee for Radio Science Ministry of Scientific Research in the Arab Republic of Egypt from May 2000 until now, advisor of the municipal council of the city of Alexandria to electromagnetic pollution in 2001 and 2002, extent the members of the Committee or which pose environmental law of electromagnetic pollution in the Arab Republic of Egypt in June 2004, the expert electromagnetic detection of contamination of the city of Alexandria, delegate and coordinator of the relationship between the Faculty of Engineering - University of Alexandria and engineering education at the Faculty of Management Air Defense Alexandria Road - Rashid the Kilo 6 - since 2005 until now and within the framework of the degree of Bachelor of Telecommunications Engineering earned by supplementary year students in the Faculty of air defense grants from the Faculty of Engineering, Alexandria University.

M. R. M. Rizk obtained his B.Sc. from Alexandria University and his master's and Ph.D. from McMaster University, Canada. He worked as an assistant professor at McMaster University. He was a visiting professor at Sultan Qaboosuniversity, Oman, Beirut Arab University and the Arab Academy for Science and Technology. He is an Adjunct professor to Virginia Polytechnic and State University, Virginia, U.S.A. His research interests include Computer Aided Design, Encryption,Fuzzy Logic, Image processing and Computer networks.

Fatma Ahmed received a Bachelor degree in Electrical Engineering from Faculty of Engineering, Alexandria University, Masters' of science in Electrical Engineering from Faculty of Engineering, Alexandria University. She works on Alexandria Higher Institute of Engineering and Technology. She studies for Ph.D. in Electrical Engineering from Faculty of Engineering, Alexandria University.