A New Secure Authenticated Key Agreement Protocol in Gaussian Field

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

***Abstract*—Key agreement protocols are a fundamental building block for ensuring authenticated and private communications between two parties over an insecure network. In this paper we propose an efficient and secure authenticated key agreement protocol based on DLP (Discrete Logarithm Problem) and Gaussian number field. The main purpose of this paper is to use the Gaussian integers; the set of all complex numbers $a+ib$ with $a,b \in Z$ in the Gaussian integers, to design new key agreement protocol that can help the system to be more secure. We show that our protocol meets the security attributes and strong against most of potential attacks. Also it provides most of desirable performance attributes.**

***Index Terms*—DLP, Gaussian integers, key agreement.**

I. 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 achieve some cryptographic goal such as confidentiality or data integrity. Secure authenticated key establishment protocols are important as effective replacements for traditional key establishment achieved using expensive and inefficient couriers. Key establishment protocols come in various flavors. In key transport protocols, a key is created by one entity and securely transmitted to the second entity, while in key agreement protocols both entities contribute information which is used to derive the shared secret key. In symmetric protocols two entities a priori possess common secret information, while in asymmetric protocols the two entities share only public information that has been authenticated. This paper is concerned with two party authenticates key agreement protocols in the asymmetric setting [1]. The design of asymmetric authenticated key agreement protocols has a checkered history. Over the years, numerous protocols have been proposed to meet a variety of desirable security and performance requirements. Many of these protocols were subsequently found to be flawed.

In order to make the key agreement protocol strong against attacks, we extend the field of protocol not only real number but also Gaussian numbers.

Manuscript received November 16, 2012; revised March 09, 2013.

Hassan M. Elkamchouchi and Mohamed Rizk are with 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).

II. Proposed Key Agreement Protocol in Gaussian Field

In this paper, we design a new secure authenticated key agreement protocol that is secure and efficient in the domain of a Gaussian integer to be more difficult to break [2] that is the main objective of this work. Our 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 Gaussian prime: ($p' = iy$) normally at least 1024 bits.
- y: Long-term secret, $y \equiv 3 \bmod 4$ (at least 1024 bits).
- p: Long-term public is large safe Gaussian prime: ($n'p'+1$).
- n': Small prime number (normally taken by 2).
- $p1$: Long-term secret, Euler's totient function $p1 = (p^2 - 1)$.
- q: The largest prime factor of Euler's totient function $p1$.
- G: Subgroup of Z_p^* of order q.
- g: Generator of G.
- r_A, r_B: Short-term private keys are random integers: $2 \le r_A, r_B < p1$ and $GCD(r, p1) = 1$.
- t_A, t_B: Short-term public keys: $t_A \equiv g^{r_A} \bmod p$ and $t_B \equiv g^{r_B} \bmod p$.
- x_A, x_B Long-term private keys are random integers: $2 \le x_A, x_B < p1$ and $GCD(x, p1) = 1$.
- y_A, y_B Long-term public keys: $y_A \equiv g^{x_A} \bmod p$ and $y_B \equiv g^{x_B} \bmod p$.

B. The New Protocol Description

In this section we describe a proposed authenticated key agreement protocol in the domain of a Gaussian integer 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 prime Gaussian p, then calculates generator g. Each user selects two static secret keys x_A and x_B, such that $2 \le x_A, x_B < p1$. Next calculate $y_A \equiv g^{x_A} \bmod p$, $y_B \equiv g^{x_B} \bmod p$ and registers y_A, y_B to the public file.

DOI: 10.7763/IJET.2013.V5.565

2) The transfer and substantiation phase

1) A generates the ephemeral key r_A such that $2 \le r_A < p1$, then calculates $t_A \equiv g^{r_A} \bmod p$ and $\bar{r}_A$ from r_A $\bar{r}_A \equiv 1 \bmod p1$.
2) B generates the ephemeral key r_B such that $2 \le r_B < p1$, then calculates $t_B \equiv g^{r_B} \bmod p$ and $\bar{r}_B$ from r_B $\bar{r}_B \equiv 1 \bmod p1$.
3) A calculates:

$$a_1 \equiv (y_B)^{-r_A} \equiv g^{-x_B r_A} \bmod p$$

$$b_1 \equiv (t_B)^{x_A + r_A} \equiv g^{r_B (x_A + r_A)} \bmod p$$

$$d_1 \equiv a_1 \bullet b_1 \equiv g^{-x_B r_A + r_B (x_a + r_A)} \bmod p$$

and sends d_1 to B .

4) B calculates:

$$a_2 \equiv (y_A)^{-r_B} \equiv g^{-x_A r_B} \bmod p$$

$$b_2 \equiv (t_A)^{x_B + r_B} \equiv g^{r_A (x_B + r_B)} \bmod p$$

$$d_2 \equiv a_2 \bullet b_2 \equiv g^{-x_A r_B + r_A (x_B + r_B)} \bmod p$$

and sends d_2 to A .

5) A receives B 's value and checks:

$$a_{22} \equiv (t_B)^{x_A} \equiv g^{r_B x_A} \bmod p$$

$$b_{22} \equiv a_{22} \bullet d_2 \equiv g^{r_A (x_B + r_B)} \bmod p$$

$$v_2 \equiv (b_{22})^{\bar{r}_A} \equiv g^{r_B + x_B} \bmod p \equiv y_B \bullet t_B$$

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

6) B receives A 's value and checks:

$$a_{11} \equiv (t_A)^{x_B} \equiv g^{r_A x_B} \bmod p$$

$$b_{11} \equiv a_{11} \bullet d_1 \equiv g^{r_B (x_A + r_A)} \bmod p$$

$$v_1 \equiv (b_{11})^{\bar{r}_B} \equiv g^{r_A + x_A} \bmod p \equiv y_A \bullet t_A$$

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

3) The key generation phase

1) A calculates the session key

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

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

2) B calculates the session key

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

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

The following table shows the overall operation in our new protocol

TABLE I: OVERALL OPERATION IN THE PROPOSED PROTOCOL

A		B
$a_1 \equiv y_B{}^{-r_A} \equiv g^{-x_B r_A}$ $b_1 \equiv t_B{}^{x_A + r_A} \equiv g^{r_B (x_A + r_A)}$ $d_1 \equiv a_1 \bullet b_1 \equiv g^{-x_B r_A + r_B (x_a + r_A)}$	$d_1 \rightarrow$ $\leftarrow d_2$	$a_2 \equiv y_A{}^{-r_B} \equiv g^{-x_A r_B}$ $b_2 \equiv t_A{}^{x_B + r_B} \equiv g^{r_A (x_B + r_B)}$ $d_2 \equiv a_2 \bullet b_2 \equiv g^{-x_A r_B + r_A (x_B + r_B)}$
$a_{22} \equiv t_B{}^{x_A} \equiv g^{r_B x_A}$ $b_{22} \equiv a_{22} \bullet d_2 \equiv g^{r_A (x_B + r_B)}$ $v_2 \equiv b_{22}{}^{\bar{r}_A} \equiv g^{r_B + x_B} \equiv y_B \bullet t_B$		$a_{11} \equiv t_A{}^{x_B} \equiv g^{r_A x_B}$ $b_{11} \equiv a_{11} \bullet d_1 \equiv g^{r_B (x_A + r_A)}$ $v_1 \equiv b_{11}{}^{\bar{r}_B} \equiv g^{r_A + x_A} \equiv y_A \bullet t_A$
$K_{AB} \equiv y_B{}^{x_A} \bullet t_B{}^{r_A}$		$K_{AB} \equiv y_A{}^{x_B} \bullet t_A{}^{r_B}$
$K_{AB} \equiv g^{x_B x_A + r_A r_B}$		$K_{AB} \equiv g^{x_A x_B + r_A r_B}$

In our protocol, we have only one message sends from one entity to another (minimal number of passes). The message sends from A to B and the message sends from B to A both have the same structure (role symmetry) and independent on each other (non-interactiveness). The total number of transmitted bits (communication overhead) is $|p|$. Our protocol has complexity 5 since we need five exponential operations. So our protocol provides desirable performance attributes.

III. SECURITY CONSIDERATION

Our protocol involves both DL cryptographic assumption and Gaussian field. The Gaussian method is recommended since the modified method provides an extension to the message space and the public exponent range [3]. The security of this protocol depends on the complexity of a DL [4]. Here we prove our protocol meets the following desirable security attributes [5].

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 singular 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 unparalleled session key which depends on r_A and r_B . Although an adversary 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 adversary.

(Perfect) Forward Secrecy: If long-term private keys of one or more entities are compromised, the secrecy of previous session keys established by honest parties is not affected.

The proposed protocol also possesses forward secrecy. Suppose that static private keys x_A and x_B of two parties are compromised. However, the secrecy of previous session keys established by honest parties is not affected, because an adversary 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 DLP (Discrete Logarithm Problem), and because we use the Gaussian numbers it provides an extension to the public exponent range.

Key-Compromise Impersonation (K-CI): Suppose A 's long-term private key is disclosed. It may be desirable that this loss does not enable an adversary to impersonate other parties to A .

Suppose A 's long-term private key x_A , is disclosed. Now an adversary 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 adversary must know A 's ephemeral key r_A . So, also in this case, the adversary should extract the value r_A from $t_A \equiv g^{r_A} \bmod p$, this is DLP.

Unknown Key-Share (UK-S): Entity A cannot be coerced into sharing a key with entity B without A 's knowledge, i.e., when A believes the key is shared with some entity $C \neq B$, and B (correctly) believes the key is shared with A .

Our protocol also prevents unknown key-share. Based on the assumption of this protocol that d_2 has verified that B possesses the private static and ephemeral keys x_B , r_B respectively corresponding to his public static and ephemeral keys y_B , t_B an adversary can't register B 's public keys y_B , t_B as its own and subsequently deceive A into believing that B 's messages are originated from the adversary. Therefore A cannot be coerced into sharing a key with party B without A 's knowledge.

Subgroup Confinement Attack: Also small subgroup attack [6], the small subgroup confinement attack is one common attack against discrete logarithm based key agreement protocols It exploits the structure of the group G where key agreement takes place. One choice of such a group is Z_p^* where p a large prime is. The order of this group is a composite, so there exist subgroups. Say G_w is one small subgroup of primer order w , then $w \mid p-1$. Suppose g is a non-identity element in G_w , then g^x for $x \in Z_p$ will also lie in the same subgroup. This can potentially cause problem if w is small: an adversary can then exhaustively search all elements in the subgroup. 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 e.g. The order's prime number factorization contains only large primes [7], which we provided in our protocol, we use safe Gaussian prime and we use generator with order q which is the largest prime factor of Euler's totient function $p1$.

IV. Conclusion

In this paper we extend the cryptosystem to the domain of Gaussian integer to make the cryptosystem more secure and very difficult to be broken. We proved that our protocol meets the security attributes under the assumption that the DL problem. Our protocol is more efficient and provides desirable performance attributes [5] which is, minimal number of passes because every party sends only one message to another party. Low communication overhead because each transmitted message has length $|p|$. 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] S. B. Wilson and A. Menezes, "Authenticated diffie-hellman key agreement protocols," in *Proc. the 5th Annual Workshop on Selected Areas in Cryptography (SAC '98)*, Kingston, Canada, pp. 339-361, 1999.

[2] K. Kobayashi, T. Suzuki and T. Hayata, "Public key cryptosystems over Gaussian integer ring," in *Proc. SCIS 2003*, pp.605–608, 2003.

[3] E. Kassar, A. N. R. Haraty, and Y. Awad. "Modified RSA in the domains of Gaussian integers and polynomials over finite fields," in *Proc. International Conference on Computer Science, Software Engineering, Information Technology, e-Business, and Applications (CSITeA'04)*. Cairo, Egypt, 2004.

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

[5] Certicom Corp., *Key Establishment Protocols*, Presentation to ANSI X9F1, July 1998.

[6] F. Hao, "On small subgroup non-confinement attacks," in *Proceedings of the 10th IEEE International Conference on Computer and Information Technology, CIT 2010*, pp. 1022-1025, 2010.

[7] A. P. Kate, P. S. Kalekar, 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 recevied 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.