ICIT 2015 The 7th International Conference on Information Technology
doi:10.15849/icit.2015.0054

A New Authenticated Key Agreement Protocol

Kamal A. ElDahshan[1], Emad Masameer[2], AbdAllah A. Elhabshy[3]
Mathematics Department,
Faculty of Science, Al-Azhar University
Nasr City, Cairo, Egypt
[1]dahshan@gmail.com
[2]emadmasameer@yahoo.com
[3]abdallah@azhar.edu.eg

***Abstract*—Authenticated key agreement protocols play a significant role in securing communications over public network channels (Internet). This paper proposes a new key agreement protocol based on factorization problem over nonabelian groups. Then it presents two different ways to provide mutual authentication for the proposed protocol; this paper presents a new authenticated key agreement protocol using fixed shared password and a new authenticated key agreement protocol using a digital signature. It also provides security analysis for the proposed two authenticated key agreement protocols.**

Keywords— Cryptographic protocols; Key agreement protocol; Authentication; Digital signature; Security analysis

I. INTRODUCTION

To establish a secured communication, legitimate entities need to share a secret key. To limit the information available to the attacker, this key should be fresh each time they start a new communication (session). This can be done by using a key agreement protocol. A key agreement protocol is very important aspect in modern cryptography. Key agreement protocols [1] allow two or more entities in order to establish together a shared secret key. The value of this secret key is a function of the information contributed by the legitimate entities. In 1976, Diffie and Hellman proposed the first key agreement protocol [2] based on the public key cryptography. The security of the Diffie-Hellman protocol is based on the discrete logarithm problem (DLP) [3]. Nowadays, most secured communications use the Diffie-Hellman protocol in order to establish a secret key. If a polynomial algorithm is found to solve DLP, all these communications will be breakable at once. So, since Diffie-Hellman protocol, there are many attempts to construct a key agreement protocol based on other problems [4-12]. One of these problems is the factorization problem over non-abelian (non-commutative) groups [6]. Let $x \in G$, where G is non-abelian group, and $y = axb$, then the factorization problem is to find a, b satisfying $a^{-1}y = xb$. In this paper we propose a new protocol based on factorization problem over non-abelian groups. Then we present two directions in order to provide mutual authentication for our key agreement protocol. One of these directions use a fixed shared password between the legitimate entities, and the other use the digital signatures for authentication.

The rest of this paper is organized as follows. Section II proposes a new key agreement protocol. Section III presents two authenticated key agreement protocols. One of them uses fixed shared password and the other uses a digital signature for authentication. Section IV provides the security analysis of our two authenticated key agreement protocols. Finally, Section V gives the conclusion and further work.

II. A NEW KEY AGREEMENT PROTOCOL

This section proposes a new key agreement protocol. This protocol is similar to Katvickis-Vitkus protocol [13] and Cho et al. protocol [6]. Let $\mathbb{M}$ be the set of all $n \times n$ matrices over $\mathbb{Z}_p$, where p is a large prime. Let $\mathbb{M}_L, \mathbb{M}_R \subset \mathbb{M}$ such that $A_L B_L = B_L A_L \; \forall \, A_L, B_L \in \mathbb{M}_L$ and $A_R B_R = B_R A_R \; \forall \, A_R, B_R \in \mathbb{M}_R$. A singular matrix $P \in \mathbb{M}$ is publicly known. Also, $PA_L \neq A_L P \; \forall \, A_L \in \mathbb{M}_L$ and $PA_R \neq A_R P \; \forall \, A_R \in \mathbb{M}_R$. In this context our protocol can be described as follows:

1. Alice randomly selects two matrices $A_L \in \mathbb{M}_L$ and $A_R \in \mathbb{M}_R$. Then she computes and sends $Y_A = A_L P A_R \bmod p$ to Bob.
2. Bob randomly selects two matrices $B_L \in \mathbb{M}_L, B_R \in \mathbb{M}_R$. Then he computes and sends $Y_B = B_L P B_R \bmod p$ to Alice.
3. Alice computes the key $K_A = A_L Y_B A_R \bmod p = A_L B_L P B_R A_R \bmod p$.
4. Bob computes the key $K_B = B_L Y_A B_R \bmod p = B_L A_L P A_R B_R \bmod p$.

Since $A_L B_L = B_L A_L \; \forall A_L, B_L \in \mathbb{M}_L$ and $A_R B_R = B_R A_R \; \forall \, A_R, B_R \in \mathbb{M}_R$. Thus, Alice and Bob generate the same key $K = K_A = K_B = A_L B_L P B_R A_R \bmod p$. Now, Alice and Bob can use the shared key in any cryptographic systems discussed in [14],[15] according to their needs.

doi:10.15849/icit.2015.0054

According to [16], the complexity of matrix multiplication is $O(n^{2.37286})$, where n is the dimension of the square matrices. This mean the complexity of our protocol is $O(n^{2.37286})$.

Let $\mathbb{M}_C \subset \mathbb{M}$ be the set of all commutative matrices over $\mathbb{Z}_p$, i.e. $AB = BA \; \forall \, A, B \in \mathbb{M}_C$, and $\alpha, \beta \in \mathbb{N}$, where $\mathbb{N}$ is the set of natural numbers. In our protocol, let $A_L = AP^{\alpha-1}$, $A_R = A^{-1}$, $A \in \mathbb{M}_C$, $B_L = BP^{\beta-1}$, and $B_R = B^{-1}, B \in \mathbb{M}_C$. Then we get an instance of Sakalauskas et al. schema [17]. Which also is similar to Eftekhari protocol [18] and Cho et al. protocol [6]. In this context, and instance protocol of Sakalauskas et al. schema can be described as follows:

1. Alice randomly selects an invertible matrix $A \in \mathbb{M}_C$ and $\alpha \in \mathbb{N}$. Then she computes and sends $Y_A = AP^{\alpha}A^{-1} \bmod p$ to Bob.
2. Bob randomly selects an invertible matrix $B \in \mathbb{M}_C$ and $\beta \in \mathbb{N}$. Then he computes and sends $Y_B = BP^{\beta}B^{-1} \bmod p$ to Alice.
3. Alice computes the key $K_A = A(Y_B)^{\alpha}A^{-1} \bmod p = A(BP^{\beta}B^{-1})^{\alpha}A^{-1} \bmod p = ABP^{\alpha\beta}B^{-1}A^{-1} \bmod p$.
4. Bob computes the key $K_B = B(Y_A)^{\beta}B^{-1} \bmod p = B(AP^{\alpha}A^{-1})^{\beta}B^{-1} \bmod p = BAP^{\alpha\beta}A^{-1}B^{-1} \bmod p$.

Since $AB = BA \; \forall \, A, B \in \mathbb{M}_C$, then Alice and Bob share the same key $K = K_A = K_B = ABP^{\alpha\beta}B^{-1}A^{-1} \bmod p$.

As mentioned, our protocol is similar to both Cho et al. and Eftekhari protocol. All of these protocols based on the factorization problem over the group of square matrices. They use the same security parameters (n, p). Thus, our protocol is secure as Cho et al. and Eftekhari protocols, with the same values of security parameters. For more details see [6] and [18].

In our protocol if P is not a singular matrix and $AP = PA$ for some $A \in \mathbb{M}_L$ and $A \in \mathbb{M}_R$, then the attacker (Eve) can compute $A_L A_R$ and deduce the shared key.

For more clarification, let $A_R P = PA_R \bmod p$, $A_R B_L = B_L A_R \bmod p$ and P is invertible matrix. Since P, Y_a and Y_b are publicly known. Then

1. $Y_a = A_L P A_R \bmod p = A_L A_R P \bmod p$ (since $A_R P = PA_R \bmod p$)
2. $A_L A_R = Y_a P^{-1} \bmod p$.
3. $K_E = A_L A_R Y_a \bmod p = A_L A_R B_L P B_R \bmod p = A_L B_L A_R P B_R \bmod p$ (since $B_L A_R = A_R B_L \bmod p$)
4. $K_E = A_L B_L P A_R B_R \bmod p$ (since $A_R P = PA_R \bmod p$)
5. $K_E = A_L B_L P B_R A_R \bmod p$ (since $A_R B_R = B_R A_R \bmod p$)
6. $K_E = K \#$

III. Authenticated Key Agreement Protocols

Due the lack of authentication [19], the proposed protocol in Section II is vulnerable to the man-in-the-middle attack [3]. To provide an authentication, one can use a fixed shared password or a digital signature [20]. In this section we will use each of these ways in order to providing the authentication.

A. A New Authenticated Key Agreement Protocol Using Fixed Password (AKAP-Pwd)

Let Alice and Bob be two entities who share a secret password (Pwd) in advance. To use this password for authentication, they construct a secret matrix S from Pwd using a predetermined algorithm. Let H_K be a keyed hash function [21] and let $\bigoplus_M$ be the bitwise XOR operation defined over matrices. The XOR operation of two matrices is done by XOR the corresponding coordinates of the entries of the two matrices. The matrices must be of the same order. In this context a new authenticated key agreement protocol can be described as follows:

1. Alice selects randomly two matrices $A_L \in \mathbb{M}_L$ and $A_R \in \mathbb{M}_R$ where $\mathbb{M}_L, \mathbb{M}_R \subset \mathbb{M}$. Then she computes and sends $Y_A = (A_L P A_R \bmod p \bigoplus_M S)$ to Bob.
2. Bob
   a. selects randomly two matrices $B_L \in \mathbb{M}_L, B_R \in \mathbb{M}_R$.
   b. computes the key $K_B = B_L(Y_A \bigoplus_M S)B_R \bmod p = B_L A_L P A_R B_R \bmod p$.
   c. computes $Y_B = (B_L P B_R \bmod p \bigoplus_M S)$.
   d. computes $V_B = H_{K_B}(Y_A \| Y_B \| \text{AliceID})$.
   e. sends Y_B and V_B to Alice.
3. After receiving Y_B and V_B, Alice
   a. computes the key $K_A = A_L(Y_B \bigoplus_M S)A_R \bmod p = A_L B_L P B_R A_R \bmod p$.
   b. checks whether $V_B ? = H_{K_A}(Y_A \| Y_B \| \text{AliceID})$ or not. If it holds, Alice accepts the communication, otherwise Alice refuses the communication.
   c. Alice computes and sends $V_A = H_{K_A}(Y_B \| Y_A \| \text{BobID})$ to Bob.
4. After receiving V_A, Bob checks whether $V_A ? = H_{K_B}(Y_B \| Y_A \| \text{BobID})$ or not. If it holds, Bob accepts the communication, otherwise he refuses it.

Since $A_L B_L = B_L A_L \; \forall A_L, B_L \in \mathbb{M}_L$ and $A_R B_R = B_R A_R \; \forall \, A_R, B_R \in \mathbb{M}_R$. Thus, Alice and Bob generate the same key $K = K_A = K_B = A_L B_L P B_R A_R \bmod p$.

B. A New Authenticated key Agreement Protocol Using Digital Signatures (AKAP-DS)

Let the entity's E public key be PuK_E and the entity's E private key be PdK_E. Let $\text{Sign}_E(M)$ be the E's digital signature of the message M. And let $\text{Ver}_E(\text{Sign}_E(M)) = M$ be the verification algorithm of the digital signature $\text{Sign}_E(M)$. In this context, a new authenticated key agreement protocol can be described as follows:

1. Alice
   a. selects randomly two matrices $A_L \in \mathbb{M}_L$ and $A_R \in \mathbb{M}_R$ where $\mathbb{M}_L, \mathbb{M}_R \subset \mathbb{M}$.
   b. computes $Y_A = A_L P A_R \bmod p$.
   c. computes the digital signature $S_A = \text{Sign}_{\text{Alice}}(H_t(Y_A))$, where t is a timestamp which has a unique value in each session.
   d. Sends Y_A, t and S_A to Bob

doi:10.15849/icit.2015.0054

2. Bob
   a. ensures that t has never been used before, i.e. the value of t is new.
   b. verifies S_A, i.e. checkes whether $H_t(Y_A)? = Ver_{Alice}(S_A) = Ver_{Alice}\left(Sign_{Alice}(H_t(Y_A))\right)$ or not. If it holds, Bob proceeds with the protocol, otherwise he refuses the communication.
   c. selects randomly two matrices $B_L \in \mathbb{M}_L, B_R \in \mathbb{M}_R$.
   d. computes $Y_B = B_L P\, B_R \bmod p$.
   e. computes the key $K_B = B_L Y_A B_R \bmod p = B_L A_L P\, A_R B_R \bmod p$.
   f. computes $S_B = Sign_{Bob}(H_{K_B}(Y_A \| Y_B \| AliceID))$
   g. sends Y_B and S_B to Alice.
3. Alice
   a. computes the key $K_A = A_L Y_B A_R \bmod p = A_L B_L P\, B_R A_R \bmod p$.
   b. verifies S_B, i.e. checks whether $H_{K_A}(Y_A \| Y_B \| AliceID)? = Ver_{Bob}(S_B)$ or not. If it holds, Alice accepts the communication, otherwise she refuses the communication.
   c. computes and sends $H_{K_A}(Y_B \| Y_A \| BobID)$ to Bob.
4. Bob checks whether $H_{K_A}(Y_B \| Y_A \| BobID)? = H_{K_B}(Y_B \| Y_A \| BobID)$ or not. If it holds, Bob accepts the communication, otherwise he refuses the communication.

Now, both Alice and Bob have the same secret key $K = K_A = K_B = A_L B_L P\, B_R A_R \bmod p$.

In our AKAP-DS one can use any secure digital signature schema such as Yang-Liao schema [22] or Wu et al. schema [23] [24].

IV. Security Analysis

This section provides a security analysis of our two authenticated key agreement protocols mentioned in Section III. It is desirable for authenticated key agreement protocols to possess a numerous of security attributes [25, 26]. This section shows that our AKAP-Pwd and AKAP-DS possess these attributes. This section also shows that our AKAP-Pwd and AKAP-DS are immune to both passive and active attacks [27].

A. Security attributes

This section shows that our protocols possess the security attributes of Known-key security, Forward secrecy, Key compromise impersonation, Unknown key-share, Loss of information, Key control, and message independence [25, 26]. In what follows, Alice and Bob are two legitimate entities and Eve is an attacker.

Known-Key Security: In our two protocols both Alice and Bob choose new private matrices in each session. This means, Alice and Bob construct a new key in each session. So, knowning an old session key does not affect the security of the current key.

Forward secrecy: In our two protocols if the long-term keys (password in our AKAP-Pwd and private keys in our AKAP-DS) are revealed by an attacker, there is no effect of the previous session keys. This is because in our protocols the long-terms are used only for authentication purposes, and do not affect the value of the key.

Key-compromise impersonation: As any protocol uses a secret shared password for authentication, in our AKAP-Pwd if Eve knows the secret password she can impersonate Alice to Bob and impersonate Bob to Alice. In other words, our AKAP-Pwd does not provide the attribute of "key-compromise impersonation". While in our AKAP-DS, if Eve covers the private key of a legitimate entity (say Alice), then Eve can impersonate Alice but Eve cannot impersonate others to Alice. In other words, our AKAP-DS guarantees the attribute of "key-compromise impersonation".

Unknown key-share: Both AKAP-Pwd and AKAP-DS are designed in such ways that make it impossible for Eve to fool a legitimate entity (say Bob) to share a session key with Alice without his knowledge. In our AKAP-Pwd, the password is shared only between Alice and Bob, which means Eve neither can establish a session key with Bob as Alice nor with Alice as Bob. In our AKAP-DS, each entity has her/his own private key to prove her/his identity, i.e. Eve cannot impersonate a legitimate entity.

Loss of information: Loss of information that is not usually available to Eve does not affect the security of our protocols in other sessions. For example if Eve knows A_L or/and A_R in some session(s), she cannot know the secret key that has been (will be) established in any other session(s). This is because in each session both Alice and Bob choose new random matrices in order to construct a new key.

Key control: In both AKAP-Pwd and AKAP-DS, neither Alice nor Bob can control the value of the key. This is because the value of the key is a function of the information supplied by each of Alice and Bob. So, both AKAP-Pwd and AKAP-DS guarantee the attribute of key control.

Message independence: The flows in AKAP-Pwd and AKAP-DS are deliberately independent. The attribute of message-independence is important, it prevents many possible attacks such as "on-line/off-line password guessing attack", and replay attacks.

B. Passive and Active attacks

There are two main types of attacks, passive attacks and active attacks. In passive attacks, an attacker (Eve) can only eavesdrop the communication between Alice and Bob. Meanwhile, Eve analyzes the transformed message in order to compute the secret key or any other useful information (guessing the password or cryptanalysising the key agreement protocol). Our protocol is based on the factorization problem which is a generalization of the conjugacy search problem [28]. To break the protocol using the brute force attack, Eve needs to check out all possible keys. As discussed in [29] for a similar protocol, the protocol is secured if $p = 251$ and $n = 32$ which make the key

doi:10.15849/icit.2015.0054

length equals to 8192 bits, i.e. the key space equal to 2^{8192}. If Eve has a computer with CPU speed $1\text{THz} = 10^{12}\text{Hz}$ which does not exist until now, she needs time $\cong 2^{8127}$ year $\cong 2^{8097}$ billion year (since since $10^{12} * 60 * 60 * 24 * 365.25 \cong 2^{65}$) to check every possible key. This is much larger than the age of the universe (the age of the universe is ≅13.8 billion year [30]). In other words, our protocols are immune to brute force attack.

In active attacks, an attacker (Eve) can capture, modify, and resend messages or even initiate and construct new messages. There are many types of active attacks such as modification attacks, replay attacks and off-line password guessing attacks. In what follows, we will discuss the security of our protocols under each type of these active attacks.

Modification attacks: In modification attacks, Eve captures and modifies the messages (flows) in order to modify the shared key. Consider the scenario in which Eve tries to modify Y_A to Y'_A. Then, in our AKAP-Pwd (Section III.A), Alice will not accept the communication as soon as she checks V_B in step 3. Also, in our AKAP-DS (Section III.B) Bob will not accept the communication as soon as she checks the Alice's digital-signature in step 2. Now, consider the scenario in which Eve tries to modify Y_B to Y'_B. Then, Alice will refuse the communication as soon as she checks V_B (step 3) in our AKAP-Pwd, or as soon as she checks Bob's digital-signature (step 3) in our AKAP-DS.

Replay attacks: Each of our protocols is deliberately designed in a way to ensure that it is impossible for an attacker (Eve) to replay any message without the knowledge of the legitimate entities.

Off-line password guessing attack: Off-line password attack could be done by a passive or an active attacker. In off-line password attack, the attacker (Eve) tries to find the shared password between the legitimate entities and prove the correctness of this password. Since the flows (messages) are independent in our AKAP-Pwd, there is no way to find the secret shared password using the transmitting messages.

V. Conclusion and Further Work

This paper proposed a new authenticated key agreement protocol. Then it presented two authentication methods. The first uses a fixed shared password (AKAP-Pwd) and the second uses a digital signature (AKAP-DS). Then this paper provided security analysis for both AKAP-Pwd and AKAP-DS. It proved that our authenticated protocols guarantee the desirable security attributes for authenticated key agreement protocols. Moreover, the paper showed that both AKAP-Pwd and AKAP-DS are immune to passive and active attacks.

This work will be enhanced by presenting a new reference schema for authenticated key agreement protocols [31].

Reference

[1] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, Handbook of Applied Cryptography: CRC Press, 1997.

[2] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, pp. 644-654, 1976.

[3] W. Stallings, Cryptography and Network Security: Principles and Practice, 6th ed.: Prentice Hall Press, 2014.

[4] V. M. Sidelnikov, M. A. Cherepnev, and V. Y. Yashcenko, "Systems of open distribution of keys on the basis of noncommutative semigroups," Acad. Sci. Dokl. Math, vol. 48, pp. 384-386, 1993.

[5] K. Ko, S. Lee, J. Cheon, J. Han, J.-s. Kang, and C. Park, "New Public-Key Cryptosystem Using Braid Groups," in Advances in Cryptology — CRYPTO 2000. vol. 1880, M. Bellare, Ed., ed: Springer Berlin Heidelberg, 2000, pp. 166-183.

[6] S. Cho, K.-C. Ha, Y.-O. Kim, and D. Moon, "Key Exchange Protocol Using Matrix Algebras and Its Analysis," Journal of Korean Mathematical Society, vol. 42, pp. 1287–1309, 2005.

[7] V. Shpilrain and A. Ushakov, "The Conjugacy Search Problem in Public Key Cryptography: Unnecessary and Insufficient," Applicable Algebra in Engineering, Communication and Computing, vol. 17, pp. 285-289, 2006/08/01 2006.

[8] E. Sakalauskas, A. Katvickis, and G. Dosinas, "Key Agreement Protocol over the Ring of Multivariate Polynomials," Information Technology and Control, vol. 39, pp. 51-54, 2010.

[9] H. K. Pathak and M. Sanghi, "Public key cryptosystem and a key exchange protocol using tools of non-abelian group," International Journal on Computer Science and Engineering, vol. 2, pp. 1029-1033, 2010.

[10] V. Ottaviani, A. Zanoni, and M. Regoli, "Conjugation as public key agreement protocol in mobile cryptography," in Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on, 2010, pp. 1-6.

[11] J.-J. Climent, P. Navarro, and L. Tortosa, "Key exchange protocols over noncommutative rings. The case of," Int. J. Comput. Math., vol. 89, pp. 1753-1763, 2012.

[12] D. Kahrobaei, C. Koupparis, and V. Shpilrain, "Public Key Exchange Using Matrices Over Group Rings," Groups Complexity Cryptology, vol. 5, pp. 97–115, 2013.

[13] A. Katvickis and P. Vitkus, "Key Agreement Protocol Using Elliptic Curve Matrix Power Function," in Advanced Studies in Software and Knowledge Engineering, ed: Institute of Information Theories and Applications FOI ITHEA, 2008, pp. 103-106.

[14] D. S. A. Elminaam, H. M. A. Kader, and M. M. Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms," International Journal of Network Security, vol. 10, pp. 213-219, 2010.

[15] D. S. A. Minaam, H. M. Abdual-Kader, and M. M. Hadhoud, "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types," International Journal of Network Security, vol. 11, pp. 78-87, 2010.

[16] F. L. Gall, "Powers of tensors and fast matrix multiplication," presented at the Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation, Kobe, Japan, 2014.

[17] E. Sakalauskas, P. Tvarijonas, and A. Raulynaitis, "Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problems in Group Representation Level," Informatica (lithuanian Academy of Sciences), vol. 18, pp. 115-124, 2007.

[18] M. Eftekhari, "A Diffie-Hellman Key Exchange Using Matrices Over Non Commutative Rings," Groups, Complexity and Cryptology, vol. 4, pp. 167-176, 2012.

[19] J. E. Canavan, Fundamentals of Network Security: Artech House, 2001.

[20] B. A. Forouzan, Introduction to Cryptography and Network Security: McGraw-Hill Higher Education, 2008.

doi:10.15849/icit.2015.0054

[21] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," in Advances in Cryptology — CRYPTO '96. vol. 1109, N. Koblitz, Ed., ed: Springer Berlin Heidelberg, 1996, pp. 1-15.

[22] F.-Y. Yang and C.-M. Liao, "A Provably Secure and Efficient Strong Designated Verifier Signature Scheme," International Journal of Network Security, vol. 10, pp. 220-224, 2010.

[23] W. Wu, Y. Mu, W. Susilo, and X. Huang, "Server-Aided Verification Signatures: Definitions and New Constructions," in Provable Security. vol. 5324, J. Baek, F. Bao, K. Chen, and X. Lai, Eds., ed: Springer Berlin Heidelberg, 2008, pp. 141-155.

[24] Z. Wang, L. Wang, Y. Yang, and Z. Hu, "Comment on Wu et al.'s Server-aided Verification Signature Schemes," International Journal of Network Security, vol. 10, pp. 238-240, 2010.

[25] S. Blake-Wilson, D. Johnson, and A. Menezes, "Key Agreement Protocols and Their Security Analysis," presented at the Proceedings of the 6th IMA International Conference on Cryptography and Coding, 1997.

[26] S. Blake-Wilson and A. Menezes, "Authenticated Diffie-Hellman Key Agreement Protocols," presented at the Proceedings of the Selected Areas in Cryptography, 1999.

[27] R. A. MOLLIN, An Introduction to Cryptography, Second ed.: Taylor & Francis, 2007.

[28] D. Moldovyan and N. Moldovyan, "A New Hard Problem over Non-commutative Finite Groups for Cryptographic Protocols," in Computer Network Security. vol. 6258, I. Kotenko and V. Skormin, Eds., ed: Springer Berlin Heidelberg, 2010, pp. 183-194.

[29] E. Sakalauskas, N. Listopadskis, and P. Tvarijonas, "Key Agreement Protocol (KAP) Based on Matrix Power Function," in Sixth International Conference on Information Research and Applications Varna, Bulgaria, 2008, pp. 92 - 96.

[30] C. L. Bennett, D. Larson, J. L. Weiland, N. Jarosik, G. Hinshaw, N. Odegard, K. M. Smith, R. S. Hill, B. Gold, M. Halpern, E. Komatsu, M. R. Nolta, L. Page, D. N. Spergel, E. Wollack, J. Dunkley, A. Kogut, M. Limon, S. S. Meyer, G. S. Tucker, and E. L. Wright, "Nine-Year Wilkinson Microwave Anisotropy Probe (WMAP) Observations: Final Maps and Results," in Cosmology and Nongalactic Astrophysics, ed. NY , United States: Cornell University, 2013, pp. 1-177.

[31] A. A. Elhabshy., "A Generalized Form for Key Agreement Protocols.," PhD thesis, Faculty of Science - Department of Mathematics Al-Azhar University, Cairo - Egypt, expected summer 2015, unpublished.