International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.3, No.6, December 2014, pp. 346~353
ISSN: 2089-3337

Analysis and Verification of a Key Agreement Protocol over Cloud Computing Using Scyther Tool

Hazem A. Elbaz[1], Mohammed H. Abd-Elaziz[1], Taymoor M. Nazmy[1]
1 Ain-Shams University – Cairo, Egypt, Faculty of Computer Science and information system
{hazem.baz@gmail, mhashem100@yahoo, ntaymoor19600@gmail}.com

Article Info

Article history:

Received Jun 12th, 2014
Revised Aug 20th, 2014
Accepted Aug 26th, 2014

Keyword:

Cloud Security
Security Analysis
Key Management
Hierarchical Identity-Based Authentication
Securtiy and Verifying Tools

ABSTRACT

The mostly cloud computing authentication mechanisms use public key infrastructure (PKI). Hierarchical Identity Based Cryptography (HIBC) has several advantages that sound well align with the demands of cloud computing. The main objectives of cloud computing authentication protocols are security and efficiency. In this paper, we clarify Hierarchical Identity Based Authentication Key Agreement (HIB-AKA) protocol, providing lightweight key management approach for cloud computing users. Then, we analyze the security properties of HIB-AKA protocol. We also show, a HIB-AKA security protocol proof using formal automated security analysis Scyther tool.

Corresponding Author:

Taymoor Mohamed Nazmy
AinShams University, Cairo - Egypt
Faculty of Computers and Informatiom Sciences
Department Computer Science
Offical Mail Timor.Mohammad@cis.asu.edu.eg

1. INTRODUCTION

Security protocols play more and more important roles with wide use in many applications nowadays. The cryptographic key management systems Managing and protecting throughout their life cycles by cryptographic techniques use cryptographic keys. Exchange or distribute secret keys between two or more participants who want to establish a secure communication over an insecure channel is one of the most important part of cryptographic keys. For this objective, key agreement protocols are widely used. Key agreement protocols allow two or more entities to establish a shared secret key to use in securing subsequent communication over an insecure channel [1, 13]. Security and efficiency are aspects taken into consideration to design the key agreement protocols. A secret key agreed between parties should be not disclosed to any entity is the aspect of security. An efficiency aspect is should be take care about optimum of computational and communication costs of the key agreement protocol [2].

Communicating over insecure channel, between two users' needs authentication key agreement protocol to create a shared secret key to be guaranteed that they are indeed sharing this secret key with each other. Later, increasingly researched have been on identity based authenticated key agreement protocol, because of simplicity of public key management. Bilinear pairings on elliptic curves is most using on identity based two parties key agreement schemes as proposed in [21, 22]. According to Sanjit Chatterjee, Palash Sarkar [2], each of two parties in the system using identity based cryptography, has its own private key and public key of each other, to calculate the secret shared key between them

In this paper, we aim to analysis and verify the hierarchal identity-based authenticated key agreement (HIB-AKA) protocol. We will use the formal automated security analysis Scyther tool. There are many researches

on verification of security protocols, therefor we will summarize some related works on security verifier tools as well as formalized and verification of privacy properties.
There are many tools for verifying and specifying security protocols as AVISPA, ProVerif, SeVe , CASRUL or Scyther. Most of these tools focus on authentication and secrecy properties [3,7,10].
The AVISPA project aims at developing a push-button, industrial-strength technology for the analysis of large-scale Internet security-sensitive protocols and applications. AVISPA can use four methods in order to check a given security protocol: 1. OFMC (On the Fly Mode Checker) which uses symbolic techniques. 2. CL-AtSe that uses simplification heuristics and redundancy elimination techniques. 3. SATMC (SAT based Model Checker) that uses SAT-solvers in order to find a proposition leading to a fail in the model. 4. TA4SP that build regular grammar in order to interpret and evaluate the intruder knowledge there exists two different modes that can be used in AVISPA: Basic and Expert modes [1, 4].
CASRUL manages the knowledge of principals and checks if protocol is runnable. CASRUL is a system for automatically verifying cryptographic protocols. Its outputs a set of rewrite rules describing to protocol itself, the goal to achieve the strategy of an intruder. CASRUL aims to model behavior of intrude and permits to handle parallel sessions and composition of keys [5, 6].
ProVerif is fully automatic, efficient, and can handle an unbounded number of sessions, an unbounded message space, and any cryptographic primitives that can represent by an equation theory and/or rewrite rules. Even if it does not always terminate, it was shown very efficient for many case studies [7, 8].
Scyther is a tool for automatic verification of security protocols. The Dolev-Yao intrude model is used in Scyther analyses protocols. Its algorithm is guarantee to terminate, at which point Scyther establishes unbounded verification or bounded verification of a wide range of basic authentication and secrecy properties. Scyther has deployed to analyze the standards of industrial security protocols IKE (v1 & v2) and ISO/IEC 9798. It used to verify more advanced security properties of authenticated key exchange security models [9, 11].
The rest of the paper is organized as follows: The next section briefly explains the hierarchical identity-based key management and the corresponding concepts (bilinear pairing and the associated computational problems). Section3 gives details on HIB-AKA protocol and the security analysis of properties desired for our proposed authenticated key agreement protocol. Section 4 shows our proposed protocol is provably secure using a formal security protocol verification Scyther Tool. Finally, a conclusion is made in section 5.

2. BACKGROUND OF HIERARCHICAL IDENTITY-BASE MANAGEMENT

2.1. Bilinear Pairing

In this section, we describe bilinear pairings and their properties. More details can be found in Sanjit-Sarkar [2] and Boneh-Franklin [3].
Let G1 and G2 denote two groups of prime order q. G1 is an additive group and G2 a multiplicative group. Let P be a generator of G1. A pairing is a computable bilinear map between these two groups. Two pairings have studied for cryptographic use, namely the Weil pairing and the Tate pairing.
For our purpose, let ê denote a general bilinear map ê: G1 ×G1 → G2, which satisfies the following three properties:

- Bilinear: If P,Q ∈ G1 and a,b ∈ Z^*_q, then ê(aP,bQ) = ê(P,Q)^{ab}.
- Non-degenerative: There exist non-trivial points P,Q ∈ G1 both of order q such that ê(P,Q)≠1.
- Computable: If P,Q ∈ G1, ê (P,Q) ∈ G2 is efficiently computable (in polynomial time).

We say that G1 is a bilinear group if the group action in G1 can be computed efficiently and there exists a group G2 and an efficiently computable bilinear map ê : G1×G1 →G2 as above. Weil and Tate pairings associated with super singular elliptic curves or Abelian varieties can be modified in order to create such bilinear maps.

2.2. Computational Problems

Many pairing-based cryptographic protocols based on the hardness of the BDHP (Bilinear Diffie-Hellman Problem) for their security [6, 3]. Some computational problems related to the elliptic curve cryptography:

- *Bilinear Diffie-Hellman Problem (BDHP):* Let G1 and G2 be two groups of prime order q. Let ê : G1 × G1 → G2, be a bilinear map and let P be a generator of G1. The BDH problem in (G1,G2,ê) is defined as: Given (P,xP,yP,zP) ∈ G1 for some x,y,z chosen at random from Z^*_q, compute ê(P,P)^{xyz} ∈G2.
- *Discrete Logarithm Problem (DLP):* Given P,Q ∈ G1, find an integer n such that P = nQ.
- *Computational Diffie-Hellman Problem (CDHP):* Given a tuple (P,aP,bP) ∈ G1 for a,b ∈ Z^*_q, find the element abP.

2.3. Hierarchal identity based key management

The hierarchical identity-based key management scheme is composed of three levels using authenticated key agreement protocol. The top level is root PKG. The level-1 is domain PKGs, which are the cloud services in the cloud computing. The level-2 is users in the cloud computing. The user's public key consists of their identity and their domain's identity. For example, the cloud service identity is ID1, the user M's identity is IDm, and the identity of user M in hierarchical key management system is ID1 || IDm [13, 21].
For example, root PKG creates identity ID_Uni to a private cloud of a University. Identities of all users and servers in a private cloud or public cloud manage and allocate by using sub-domain PKG. A hierarchal identity created for user and server, which is combine both identity of the user or server and the identity of the sub- domain. For example, the identity of email server in the private cloud of a University can be ID_Uni.email_server.
The Figure 1 shows the hierarchical PKGs architecture in cloud computing as follows:

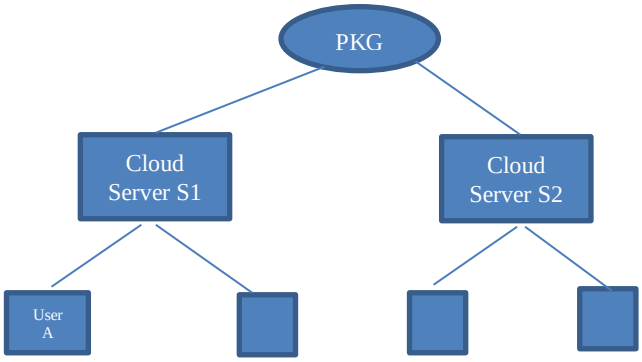


Figure 1: Hierarchical PKGs architecture in cloud computing

2.3.1. Key generation
Root Setup: The root PKG operate as follow:
Step 1: Generate two cyclic groups G1, G2 of large prime order q and bilinear map e:G1xG1→G2, chooses an arbitrary generator P0∈G1 ;
Step 2: Root PKG picks a random s0 ∈ Z^*_q and sets Q0=s0P0 .Choose two hash functions: H1:{0,1}* → G1, H2:G2 → $\{0,1\}^n$. The root PGK's secret is s0 .The system public parameters are (G1, G2, e, P0, Q0, H1, H2).
Lower-level setup: level-1 set up. The level-1 is cloud services. The cloud server S1 is the domain PKG. The cloud server S1 identity is ID1 , then it picks a random s1 ∈ Z^*_q and keeps it secret .To obtain the cloud service, let S0 be the identity element of G1. The root PKG that is the cloud server S1 parent operates as follow:
Step 1: computes P1=H1(ID1) ∈ G1 ;
Step 2: set the cloud server S1 private key S1=s0P1 ;
Level-2 set up. Level-2 is the users. The user's private key is extracted in this phrase. Let 2-tuple (ID1,IDA) be an identity of Level-2 user A. The cloud server S1 that is the user's parent generates the private key as follows:
Step 1: computes PA = H1(ID1 || IDA) ∈ G1;
Step 2: sets the user's private key SA = S1 + s1PA ;
Step 3: also gives the user the values of Q1 = s1P0 as "verification points "to the user and needs to return (SA, Q1).

2.3.2. Hierarchical Identity-Based Authenticated Key Agreement (HIB-AKA)
The main problem here is that this digital identity can only use in one cloud, private one or public one. Users in a hybrid cloud may be want to access services that provided by different clouds, so it need multiple identities for each one of services on these clouds. Here is show clearly not user friendly [14, 15]. In this paper, we propose a system for cloud computing environment where each user and server will have its own unique identity, with this unique, the key distribution and mutual authentication can be greatly simplified.
This paper was proposed to solve this problem by using identity management in clouds computing with hierarchal identity based cryptography, where this proposed scheme allow users from one cloud to access to service in other one with single digital identity, and also allow them in hybrid cloud to simplified a mutual authentication and key distribution. Our protocol design should achieve the following security and performance guarantee, to enable privacy-preserving public accessing for cloud environment.

Alice and Bob wish to establish shared key. Each of them choose a random element as private key a, b ∈ Z*q, and compute the values of corresponding element as public keys WA = aPA , WB = bPB and S1 = s0P1. They can exchange the public keys as following:
Alice send a message M1 to Bob contains WA. Bob send a message M2 to Alice WB. Then they may produce the algorithm. Where Alice computes:

$KAB = e(SA, WB + aPB) / e(S1, WB + aPB)$
$= e(s0P1+s1PA, WB + aPB) / e(s0P1, WB + aPB)$
$= e(s1PA, WB + aPB)$
$= e(s1PA, bPB + aPB)$
$= e(PA, PB)^{s1(a+b)}$

In addition, Bob computes:

$KBA = e(WA + bPA, SB) / e(WA + bPA, S1)$
$= e(WA + bPA, s0P1 + s1PB) / e(WA + bPA, s0P1)$
$= e((a+b)PA, s1PB)$
$= e(PA,PB)^{s1(a+b)}$

If Alice and Bob follow the algorithm, then they get the same share key.

3. SECURITY ANALYSIS OF HIB-AKA PROTOCOL

Our proposed algorithm is secure, because it have hierarchical design. Regular identity-based cryptography has one PKG that distributes private keys to users. If the root PKG exposes the private key, all users' private key are also revealed. Our proposed algorithm level-2 users cannot influence if the root PKG is reveals all private keys. Since they have different parents, the user's private keys are secure. In addition, any other domain that not connected with the root PGK cannot expose their domain private keys. So it can greatly reduce the workload, also can allows key escrow at several levels.
If Alice assures that no other entity besides Bob can possibly ascertain the value of the secret key, then we can say that a key agreement protocol is implicit key authentication [16]. When this condition is achieved you called the mutual implicit key authentication is an authentication key agreement protocol [18, 22].
Here, we will analyze the security attributes of our proposed authenticated key agreement protocol HIB-AKA [19].
Known-key Security: A unique secret session key should create in each run of protocol. The compromise of one session key should not compromise other session keys.
Forward Secrecy: If long-term private keys of one or more of the entities are compromised, the secrecy of previously established session keys should not be affected. We say that a system has partial forward secrecy if some but not all of the entities long-term keys can be corrupted without compromising previously established session keys, and we say that a system has perfect forward secrecy if the long-term keys of all the entities involved may be corrupted without compromising any session key previously established by these entities. There is a further perhaps stronger notion of forward secrecy in identity-based systems, which is called PKG forward secrecy, which implies perfect forward secrecy. This is the idea that the PKG's long-term private key may be corrupted and hence all users long-term private keys without compromising the security of session keys previously established by any users.
Key-compromise Impersonation Resilience: Compromising an entity Alice's long-term private key will allow an adversary to impersonate Alice, but it should not enable the adversary to impersonate other entities to Alice.
Unknown Key-share Resilience: An entity Alice should not be able to be coerced into sharing a key with any entity adversary when in fact Alice thinks that she is sharing the key with another entity Bob.
Key Control: Neither entity should be able to force the session key to be a preselected value.

4. VERIFICATION OF HIB-AKA PROTOCOL USING SCYTHER TOOL

Our proposed secure and efficient HIB-AKA algorithm for cloud computing has the following properties: a) less computational cost so to be more efficient.
b) Hierarchy, due to cloud computing environment scalability and dynamic features.
c) one-round, less network overload so more efficient.
d) The users (i.e., Alice, Bob) can help to meet frequent mutual authentication requests between users and resources.
e) Unique node's registered distinguished name (DN) from root to node, to provide cross-trust domain in which each domain comprises one PKG.
Before authentication, trust relationship has built between PKGs to shared system parameters with each other.

If Alice and Bob follow the algorithm, then they get the same share key. Our proposed HIB-AKA algorithm is depicted in Figure 2.

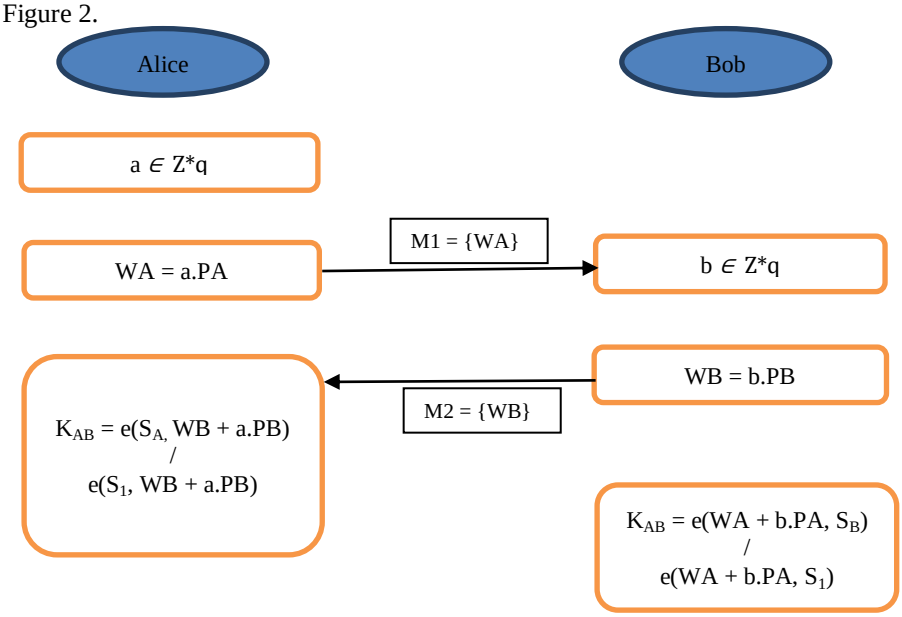


Figure 2: Proposed Key Agreement HIB-AKA

We use automated security protocol verification tool Scyther version compromise-0.9.2 to provide us a formal security analysis, on laptop 2.4 GHz Intel core i3 processor, with 3 GB RAM. Scyther tool present a framework for modeling adversaries in security protocol analysis, ranging from a Dolev-Yao style adversary to more powerful adversaries, supports notions such as weak perfect forward secrecy, key compromise impersonation, and adversaries capable of state-reveal queries [20].

Figure 3 shows the settings of the adversary model used in verifying our proposed HIB-AKA protocol.

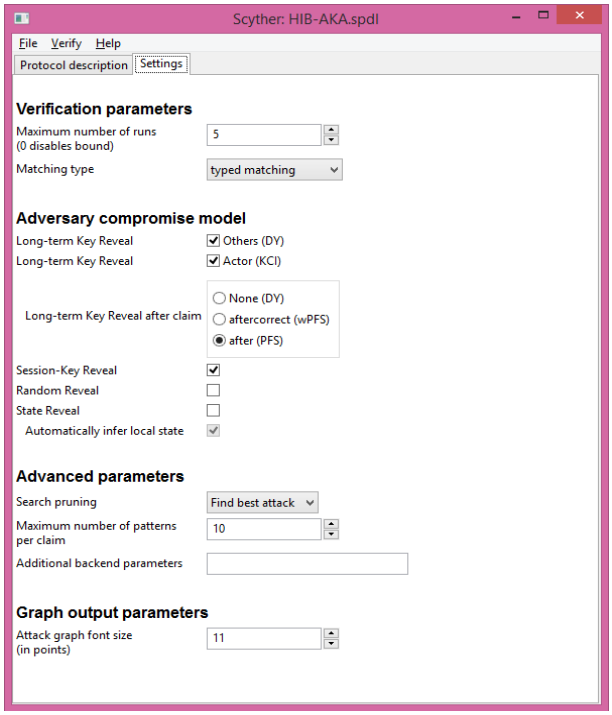


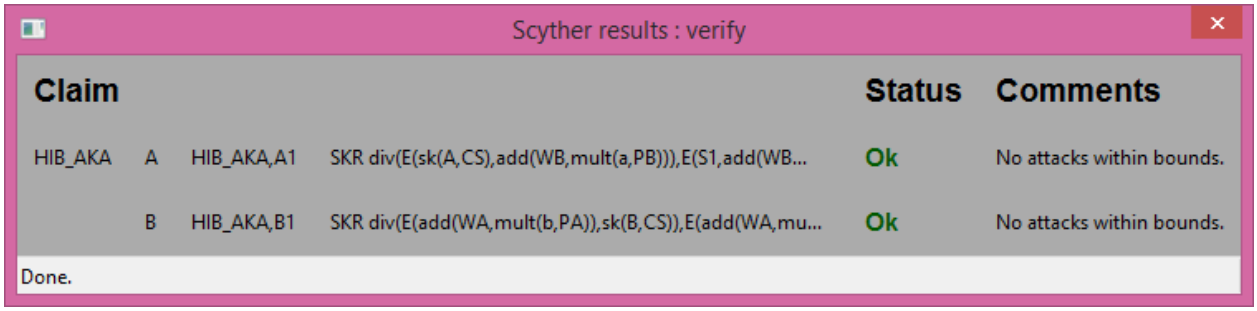
Figure 3: Scyther adversary model used for HIB-AKA verifying.

We model the HIB-AKA protocol in security protocol description language (SPDL) using Scyther tool as follows:

/* Proposed Hierarchal identity based authentication key agreement for Cloud (HIB-AKA) */

```
// Hash functions
hashfunction E; // E is e pairing function
// Addition, multiplication, division simply hashes
hashfunction mult,add,div;
// The protocol description
protocol HIB-AKA(CS,A,B)
// CS = Cloud Server A = Alice as user, B = Bob as user
{
	const S1,PA,PB;
	role CS // Cloud Server
	{
		send_1(CS,A,S1); // Publish public params
		send_2(CS,B,S1);
	}

	role A // Alice as User
	{
		fresh a: Nonce; // Ephemeral Secret
		var WB: Ticket;

		recv_1(CS,A,S1);
		send_3(A,B,mult(a,PA)); // Send WA
		recv_4(B,A,WB);

		// Secret Session Key
		claim(A,SKR,div(E(sk(A,CS),add(WB,mult(a,PB))), E(S1,add(WB,mult(a,PB)))));
	}

	role B // Bob as User
	{
		fresh b: Nonce; // Ephemeral Secret
		var WA: Ticket;

		recv_2(CS,B,S1);
		recv_3(A,B,WA);
		send_4(B,A,mult(b,PB)); // Send WB

		// Secret Session Key
		claim(B,SKR,div(E(add(WA,mult(b,PA)),sk(B,CS)),E(add(WA,mult(b,PA),S1))));
	}
}
```

Figure 4 shows the proposed HIB-AKA verification using Scyther tool.



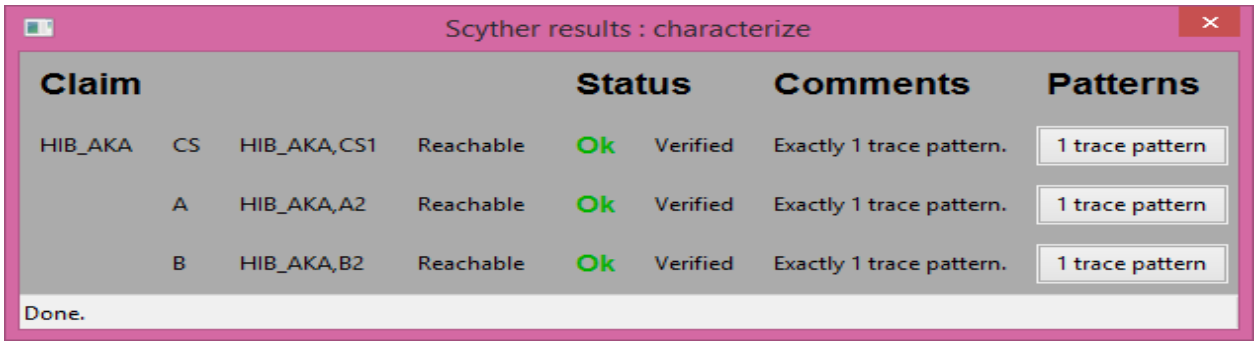


Figure 4: HIB-AKA Scyther security protocol verification.

5. CONCLUSIONS

In this paper, we proposed an efficient identity-based authenticated key agreement protocol for configurable hierarchical cloud computing environment. There are tools for specifying and verifying security protocols like AVISPA, CASRUL, ProVerif and Scyther tools were descried. We had demonstrated a background of Hierarchical Identity-Based Key management as well as explained our proposed HIB-AKA security protocol through the observing features and advantages of our proposed protocol, then we analyzing security attributes of our proposed protocol, finally our proposed protocol is provably secure using a formal security protocol verification Scyther Tool.

REFERENCES

[1] Farash, Mohammad Sabzinejad, et al. "A new efficient authenticated multiple-key exchange protocol from bilinear pairings." *Computers & Electrical Engineering* 39.2 (2013): 530-541.
[2] Chatterjee, Sanjit, and Palash Sarkar. *Identity-based encryption*. Springer, 2011.
[3] Luu, Anh Tuan, et al. "SeVe: automatic tool for verification of security protocols." *Frontiers of Computer Science* 6.1 (2012): 57-75.
[4] Hurtado Alegría, Julio A., María Cecilia Bastarrica, and Alexandre Bergel. "Avispa: a tool for analyzing software process models." *Journal of Software: Evolution and Process* 26.4 (2014): 434-450.
[5] Cortier, Véronique, and Bogdan Warinschi. "Computationally sound, automated proofs for security protocols." *Programming Languages and Systems*. Springer Berlin Heidelberg, 2005. 157-171.
[6] Modersheim, Sebastian. "Algebraic properties in alice and bob notation." *Availability, Reliability and Security, 2009. ARES'09. International Conference on*. IEEE, 2009.
[7] Cheval, Vincent, and Bruno Blanchet. "Proving more observational equivalences with ProVerif." *Principles of Security and Trust*. Springer Berlin Heidelberg, 2013. 226-246.
[8] Blanchet, Bruno. "Using Horn clauses for analyzing security protocols." *Formal Models and Techniques for Analyzing Security Protocols* 5 (2011): 86-111.
[9] Cremers, Cas, and Sjouke Mauw. *Operational semantics and verification of security protocols*. Berlin: Springer, 2012.
[10] Basin, David, Cas Cremers, and Simon Meier. "Provably repairing the ISO/IEC 9798 standard for entity authentication." *Journal of Computer Security* 21.6 (2013): 817-846.
[11] Basin, David, et al. "Improving the Security of Cryptographic Protocol Standards." (2014): 1-1.
[12] Boneh, Dan, and Matthew Franklin. "Identity-based encryption from the Weil pairing." *SIAM Journal on Computing* 32.3 (2003): 586-615.
[13] Martin, Luther. *Introduction to identity-based encryption*. Artech house, 2008.
[14] Li, Ying, et al. "A lightweight identity-based authentication protocol." *Signal Processing, Communication and Computing (ICSPCC), 2013 IEEE International Conference on*. IEEE, 2013.
[15] Han, Jinguang, Willy Susilo, and Yi Mu. "Identity-based secure distributed data storage schemes." (2013): 1-1.
[16] Farash, Mohammad Sabzinejad, and Mahmoud Ahmadian Attari. "An enhanced and secure three-party password-based authenticated key exchange protocol without using server's public-keys and symmetric cryptosystems." *Information Technology And Control* 43.2 (2014): 143-150.
[17] Yao, A. C., & Zhao, Y. (2014). Privacy-Preserving Authenticated Key-Exchange Over Internet.
[18] Nabil, Mohamed, et al. "New Authenticated Key Agreement Protocols." *Proceedings of the International MultiConference of Engineers and Computer Scientists*. Vol. 1. 2013.
[19] Tsai, Chieh-Cheng, and Peng-Jen Lai. "Analysis of Authenticated Key Agreement Protocols From Weil Paring." SCA: International Journal of Soft Computing with Applications, Vol. 1, No. 1, pp. 10 ~ 19. 2013
[20] Basin, David, and Cas Cremers. "Modeling and analyzing security in the presence of compromising adversaries." *Computer Security–ESORICS 2010*. Springer Berlin Heidelberg, 2010. 340-356.
[21] Elbaz, Hazem A., Mohammed H. Abd-elaziz, and Taymoor Nazmy. "Trusting Identity Based Authentication on Hybrid Cloud Computing." *Cloud Computing*. Springer International Publishing, 2014. 179-188.
[22] Cao, Xuefei, Weidong Kou, and Xiaoni Du. "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges." *Information Sciences* 180.15 (2010): 2895-2903.

BIBLIOGRAPHY OF AUTHORS (10 PT)

	Name | hazem A. elbaz University | AinShams University Faculty | Faculty of Computers and Informatiom Sciences Degree | Phd Student at Faculty of Computers and Informatiom Sciences, Ain Shams University Department | Information Systems Offical Mail | hazem.baz@gmail.com
	Name | mohamed hsham abd el aziz ahmed University | AinShams University Faculty | Faculty of Computers and Informatiom Sciences Degree | Professor Emeritus Department | Information Systems Offical Mail | mhaziz@cis.asu.edu.eg
	Name | Taymoor Mohamed Nazmy University | AinShams University Faculty | Faculty of Computers and Informatiom Sciences Degree | Professor Department | Computer Science Offical Mail | Timor.Mohammad@cis.asu.edu.eg