Towards a Framework for Supporting Unconditionally Secure Authentication Services within E-Government Infrastructures*

Sufyan T. Faraj Al-Janabi

[2]College of Science and Technology, UHD
Sulaimani, KRG-Iraq
[1]College of Computer Science and IT
University of Anbar, Ramadi, Iraq
saljanabi@fulbrightmail.org

***Abstract*—It has been noticed by many researchers that the speed of ICT advancement in developing, deploying, and using e-government infrastructures is much faster than the development and deployment of security services. Therefore, government organizations are still suffering from the existence and emerging of security risks. One important category of cryptographic primitives that needs to be considered in this respect is the unconditionally secure message authentication codes (or A-codes). These A-codes are cryptographically approached based on information theory. They offer unconditional security, i.e., security independent of the computing power of an adversary. For many years, it was widely thought that A-codes were impractical for real applications. However, in recent years, many A-codes have been developed which are extremely efficient in terms of computations and key requirements.**

The aim of this work is to show the importance and validation of including unconditionally secure authentication services within e-government infrastructures. We believe that all main e-government services can get benefit from that in a way or another. This includes Government to Citizen (G2C), Government to Business (G2B), Government to Government (G2G), and Government to Constituents (E-Democracy) services. The work highlights the basic requirements for a general framework that facilitates the inclusion of such authentication services within the security infrastructure of e-government.

***Keywords*—A-codes; authentication; e-government; unconditional security**

I. INTRODUCTION

The theory of authentication is concerned with providing evidence to the receiver of a message that it was sent by an authorized sender. This should truly hold even in the existence of an active adversary who can intercept sent messages and/or fabricate fraudulent messages. Despite the fact that both confidentiality and authenticity can be achieved by the techniques of cryptography, authentication theory is more subtle than the theory of secrecy. For example, the strongest possible definition of secrecy is Shannon's definition of perfect secrecy, which means that plaintext and ciphertext are statistically independent. However, it is not clear yet how perfect authenticity should be defined [1].

Entities in e-government setting can use a variety of methods and technologies to authenticate each other. These methods might include the use of personal identification numbers (PINs), passwords, PKI-based digital certificates, smart cards, various types of "tokens", biometrics, etc. Each of these techniques provides a certain level of security. Thus, selecting the use of any authentication technique or method must depend on the value of the information being authenticated, expected security threat, and the appropriate security service required. In general, properly combining more than one authentication method is considered to be more secure than using a single authentication technique. However, the success of any authentication method is not only a technology dependent. In fact, this also depends on the choice of appropriate policies, controls, and procedures [2], [3].

Generally speaking, authentication consists of the following properties [4]:

- Data integrity; which means protecting the data from modification by malicious parties.
- Data origin authentication; which is the validation of the identity of the origin of the data.
- Non-repudiation; which is to guarantee that the data origin entity cannot deny the creation and send of data.

In order to satisfy different authentication requirements, messages are usually appended either a digital signature, a message authentication code (MAC), or an unconditionally secure message authentication code (A-code). MACs and A-codes can provide data integrity and data origin authentication while digital signatures can also ensure non-repudiation. It is important to emphasize that MACs are only proven to be computationally secure while the security of A-codes is unconditional. Thus, MACs are suitable for short-term security but they are not useful for long-term (say 20 years) requirements, especially when considering new technologies like quantum computers. Digital signature schemes can be

*This paper was presented at the Third International Scientific Conference of University of Human Development (April, 2016)

constructed for both computational security and unconditional security [4].

Digital signatures are very widely used technology for ensuring unforgeability and non-repudiation of information. While some information only requires the assurance of authenticity (or integrity) for a relatively short period of time (e.g., one or two years), there are situations where it is crucial for some signed documents to be protected (and remain as legally valid) for longer periods of time. Examples of documents that need long-term integrity include court records, long-term leases and contracts. The current traditional computationally secure authentication techniques (mainly based on the public key infrastructure of PKI) is increasingly threatened by the rapid advancement in the speed of computers and the possibility of the emergence of innovative mathematical algorithms for solving the assumed number theoretic problems [5].

Another significant threat comes from the progress in developing quantum computers. In 1994, Shor already showed that quantum computers can break most of digital signatures traditionally used today. In 2001, some researchers had implemented Shor's algorithm on a 7-qubit quantum computer. It is now prudent to predict that within the next few years there will be reliable quantum computers for breaking traditional digital signature schemes. For this reason, many researchers started a new hot research field of post-quantum cryptography in recent years. Thus, it is clear that we need to devise authentication procedures and digital signature techniques that can provide long-term security. One possible important solution is to use mathematical techniques whose security does not rely on any unproven assumptions, i.e. A-codes [5], [6].

The remaining of this paper is organized as follows: Section 2 reviews the basic e-government services and related modeling approaches. Section 3 is a theoretical background on A-codes and their properties. Our proposed convergence approach to developing a security framework for supporting unconditionally secure authentication services in e-government settings is described in Section 4. Next, some provisioned advantages and interesting applications of including unconditionally secure authentication services in e-government infrastructure are outlined in Section 5. Finally, the paper is concluded in Section 6.

II. E-GOVERNMENT MATURITY MODELS AND SERVICES

E-government can be defined in different ways by various sources; however, there is a common theme in these definitions. E-government always involves using Information and Communication Technology-ICT (especially the Internet) to improve the delivery of government services to citizens, businesses, and other government agencies. E-government also enables citizens to interact and receive reliable and dependable services from governmental agencies [7].

There are three main distinguished target groups in e-government setting (In this paper, the terms e-government and e-governance are used as synonyms), which are government, citizens and businesses/interest groups. Thus, the main e-government services include [7]:

1. *Government to Citizen (G2C);* which are those activities in which the government provides citizens with reliable and dependable access to information and services.
2. *Government to Business (G2B);* in which the government deals with businesses using the Internet and/or other communication networks.
3. *Government to Government (G2G);* which deals with the activities that happen between various governmental organizations /agencies. This can be considered as internally-focused e-government service.
4. *Government to Constituents (E-Democracy);* which refers to online democratic-oriented activities of governments, elected representatives, political parties, and citizens. One especially important application within this category is electronic voting (e-voting).

Despite the fact that relying on ICT for supporting important operations to both government and business is increasing, however, advancement in ICT aspects of e-government infrastructures is much faster than the development and deployment of security services. This indeed applies for both technical and non-technical (social) sides of security practice. Hence, there are many security challenges still facing e-government applications. In this direction, we can notice that there are several e-Government Maturity Models (eGMMs) that have been developed by international organizations and researchers in order to guide and benchmark e-government systems implementation and delivery of service. A maturity stage in eGMM enables us to measure the progress of e-government implementation. However, these eGMMs models were designed with the main focus on functionality. In other words, they account for the quantity of e-government implementation and service rather delivery than quality (including security aspects) [8].

On the other hand, Information Security Maturity Models (ISMMs) main focus is on the quality of the offered security services to organizations. It is crucial that confidentiality, integrity, and other security aspects become an integral part of all phases of e-government services. Thus, it is necessary to fill the gap between these two types of models, especially in their critical stages. This can only be done by proposing detailed strategic frameworks that facilitate the integration of ICT security services into eGMM critical stages [8], [9].

One more thing that we want to give more emphasis here is that we should consider all e-government components and parameters whenever proposing any security framework for e-government environments. The basic building block components of e-government, in general, are shown in Figure 1. This figure represents a cubic visualization of e-government strategy from a practical perspective in the three major directions; organization, infrastructure, and guidelines [10].

III. UNCONDITIONALLY-SECURE AUTHENTICATION CODES (A-CODES)

There are three basic approaches in modern cryptography for message authentication. These are [11]:

1. *Information-theoretic approach:* This method offers unconditional security (i.e., security independent of the computing power of an opponent). These are A-codes which are the main interest of this paper. It is important to remember that both unconditionally secure encryption and authentication are only probabilistic. This means that there always a non-zero probability of the adversary to cheat. However, the value of such probability can be significantly reduced to exponentially small levels.
2. *Complexity-theoretic approach:* This approach starts from an abstract computational model. It assumes that the adversary has limited computing power.
3. *System-based approach:* In this approach, we try to produce practical solutions whose security is based on realistic estimates of known breaking algorithms and the required computing power to carry out them. Both the second and third approaches are considered to be only computationally secure.

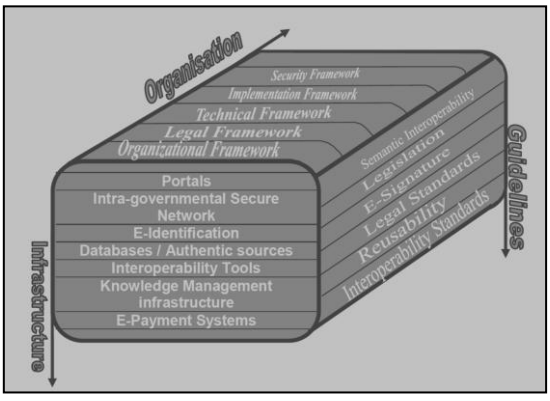

Fig. 1. Different building blocks of e-government [10].

A-codes enable two trusting entities to communicate securely even in the presence of an adversary who is capable of fabricating fraudulent messages and/or substituting a transmitted message with a fabricated one. Development and construction of A-codes can be considered as a multidisciplinary task, where it is required to investigate several areas such as coding theory, information theory, design theory, and finite geometry [12]. In spite of that the original idea of A-codes dates back to more than four decades ago, recently, it was widely thought that A-codes were as impractical as the Vernam scheme (This is the only known unconditionally secure encryption scheme. It is sometimes also called as One-Time Pad encryption or OTP). However, this has started to change recently when new extremely efficient A-codes have been developed. This correctly applies in both terms of computation and key usage. To achieve unconditional security, A-codes need shared secret (keys) between legitimate entities [11], [13]. For more details on the mathematical aspects of A-codes, see for example [14] and [15].

A major research achievement in the field of A-codes was pioneered by Wegman and Carter in 1981 when they invented the so-called universal hash approach for constructing A-codes [16], [17]. Since that time, many successor A-codes have been developed with increased efficiency and performance based on similar approaches. Besides the unconditional security property, A-codes developed based on universal hash approach can offer more advantages compared to other MAC approaches [18]:

- *Speed:* They are very simple to implement. Experimental evaluations have shown that some new such A-code constructions are faster than computationally secure ones based on MD5, for example.
- *Parallelizable:* This property holds whenever a part of the universal hash function is linear, which is usually the case.
- *Incremental:* When a part of the message is modified or new part is added, it is not required to redo the whole (A-code) calculations again. We only need to recalculate for the modified or added part.

One important step in studying very fast software implementations of A-codes based on universal hashing was achieved by Rogaway who introduced a very efficient hashing technique called “bucket hashing”. Ideally, this technique requires no more than 10 simple instructions per word (to be authenticated) [19]. A variant of bucket hashing had been also developed with similar efficiency and much lower key size requirements [18].

Some important extensions to A-codes have been studied by various researchers. The most important of these are [5]:

- *A-codes with arbitration (A^2-codes):* These codes involve an arbiter (a trusted third party) who can help resolve disputes that may appear between sender and receiver.
- *A^3-codes:* These represent improved A^2-codes with a less trustworthy arbiter as a requirement. Both A^2-codes and A^3-codes require the receiver of the message to be designated (This also applies to digital signature schemes based on such codes).
- *Multi-receiver authentication codes (MRA):* In these codes, a broadcast message can be verified by any one of the receivers. They require the sender to be designated.
- *MRA with dynamic sender (DMRA):* These schemes have been developed to simplify the requirement of the designated sender. Both MRA and DMRA are only used in the case of broadcasting. They cannot be used for point-to-point authentication. Furthermore, neither MRA nor DMRA satisfies the non-repudiation requirement of a digital signature.

It is also possible to transform an A-code into an unconditionally secure digital signature. However, in doing so, we usually face two problems. The first is related to A-codes (especially the conventional Cartesian ones) that do not provide the non-repudiation function. The second is that A-codes require that the receiver be always designated. This means that a signature cannot be verified by a party who does not have the shared secret key [5].

IV. THE PROPOSED CONVERGENCE APPROACH

The best methodology for solving a complex problem is to divide it into smaller distinguishable parts. Then, one can try to solve each of these parts individually based on step-by-step approach. The solution of the whole problem will be the integral sum of individual solutions. This is very typical in professional networking and security practice, where the layered (or structured) approach is usually used. Thus, to design a security framework that enables the inclusion of unconditionally secure authentication services within e-government environment and simultaneously fulfills all requirements of security, availability, and scalability, an N-Tier architecture is proposed.

The N-Tier architecture is a suitable development choice for such tasks since it meets the requirements of project development in terms of open architecture, rapid deployment, separated content/presentation, and workflow capabilities. Indeed, this architecture is characterized by the functional decomposition of applications, service components, and distributed deployment. However, this is a distributed architecture. Thus, in order to maintain the quality of service, an efficient asynchronous communication strategy should be used among different layers [20].

The proposed architecture is composed of the following (See Figure 2):

- *Data Tier:* This tier represents the Database Management System (DBMS).
- *Data Access Tier:* This tier includes the generic interfaces with the databases required by upper tiers.
- *Security Tier:* This tier is responsible for all security services such as authorization, authentication, confidentiality, etc. A major task in this tier is the issue of key management to be explained shortly.
- *Business logic Tier:* This tier includes all common business logic for the parties involved in the e-government architecture (other than security issues).
- *Presentation Tier:* This tier provides an interface to e-government entities and/or the end user into the offered services. Indeed, this tier could include a Proxy Tier that facilitates providing services in multi-platform environments.

The basic idea behind this layered architecture is to encapsulate the security-relevant functions and separate them from other operational functionalities and applications. Thus, an e-government application delegates the security functions to the security layer, i.e. the application needs not be aware of the implementation details. Typically, the application only needs a few basic security-related functions such as [21]:

Fig. 2. The proposed N-Tier framework architecture.

- *Signature-creation:* The application can request creating a signature whenever it is required. It is also possible that the application selects a signature format (Based on A-codes or based on computationally secure techniques). The signature creation process will be done by the security tier.
- *Signature-verification:* The application passes the signed data to the security tier which carries out the process and returns the result.

- *Info-box access:* The application can read and write "info-boxes" which contain information on functional security associations and involved security devices. Note that the access control policy is delegated to the security layer.
- *Session certificates:* The security layer is also responsible for the functions to create session keys and to create session certificates. These are required for PKI-based cryptography.

Some additionally suggested security-related functions could be:

- *Session encryption:* The application can request to encrypt some sensitive sessions and possibly it can also select the encryption technique and its parameters from a list supported by the security layer.
- *Session decryption:* the application passes encrypted data to the security layer for decryption.
- *Key-synchronization:* This function is used by applications to prepare the security tier for correctly manage secret keys required for A-codes based security services.

When proposing a certain framework that enables A-codes based security services within e-government settings, it is important to consider mutual authentication between involved parties. Thus, if we assumed a client-server communications environment, it is no longer adequate to only concentrate on client (user) identification and authentication issues. Instead, server authentication assurance should also be considered. Of course, as typically adopted by the standards for network security such as X.800 (Security Architecture for Open Systems Interconnection), the following two types of authentication should be considered [22]:

1. *Data Origin Authentication;* which ensures that the source of data received is as claimed.
2. *Peer-Entity Authentication;* which ensures that a peer entity in an association is the one claimed.

In our approach, one of the basic components required for successful and reliable delivery of unconditionally secure authentication services within e-government setting is the "key bank" agent. These key bank agents are responsible for all functionalities necessary for the management of shared (random) secret keys required by A-codes. Three main key management and distribution approaches can be initially suggested for the key bank agents, which are:

- *Courier-based approach:* This is the most traditional approach. However, it has well-known limitations. Thus, it can only be proposed for a limited number of capable entities or organizations.
- *Quantum cryptographic-based approach:* Recently, there have been significant advancements in quantum cryptography field, especially in Quantum Key Distribution (QKD). From a cryptographic viewpoint, the most important feature of QKD is its ability to offer established keys with the unconditional secure property. For details on the integration of QKD in security infrastructures, the reader is kindly advised to refer to [23] and [24], for example.
- *Hybrid PKI-based approach:* There are some researchers (See for example [25]) who think that properly combining QKD with public-key based authentication can also provide working environment with enhanced properties. Such hybrid schemes are easier for implementation than pure QKD systems. However, we think these schemes still need more research investigation.

Due to limitations imposed by current commercially-available technology required for random secret key distribution, we only propose unconditionally-secure services for G2G and G2B settings only. This can be considered as a first adaptation stage. In the second stage, e-democracy (especially e-voting) can be included. The G2C setting has to be delayed to a final future stage in accordance with the rate of technology advance in QKD mainly. Figure 3 represents a typical topology for deployment of key bank agents in the first stage. The figure depicts governmental agencies connected with the business organizations via the Internet to offer G2G and G2B services. Each of these entities includes a key bank agent. All key bank agents are connected with a central key management authority via secure channels (represented by dotted lines). These can be either in-band or out-band channels depending on the chosen key management and distribution approach.

V. PROVISIONED ADVANTAGES OF INTEGRATING A-CODES WITHIN E-GOVERNMENT SETTING

We have mentioned previously that universal hash-based A-codes offer some important advantages compared to traditional "computationally-secure" MAC techniques. These advantages include unconditional-security, speed, parallelization, and incremental properties. Furthermore, there are some other provisioned advantages and interesting applications of A-codes, which can be beneficial to various e-government services including G2G, G2B, G2C, and e-democracy (Despite the fact that we are only advising unconditionally secure authentication techniques for G2G and G2B settings for the time being). Some of these provisioned advantages and/or interesting applications are:

- *Multicast (multi-receiver) authentication:* This is an extension to the basic point-to-point authentication scenario. In simple words, the sender in multicast authentications scheme broadcast a single authenticated message such that its authenticity can be independently verified by

all receivers. In fact, such schemes can be divided into unconditionally secure authentication and computationally secure authentication. Unconditionally-secure authentication provides very strong security guarantees, however, they traditionally considered being less practical than computationally-secure techniques. Recently, unconditionally-secure schemes with increased efficiency have been invented [26], [27].

- *Multiple-authentication:* Universal-hashing based A-codes have been generalized to enable the authentication of a sequence of messages with the same key. This simplifies the requirements of key management and distribution [28], [15].
- *Potentially efficient constructions:* Because of the simplicity of the requirements from universal hashing, it is possible to construct very efficient A-codes. This efficiency can be further enhanced with supporting certain arithmetic types such as single-precision arithmetic [29].
- *Unconditionally-secure digital signatures:* These digital signature schemes have recently received considerable attention because they provide a foundation for long-term integrity and non-repudiation of data. Despite their high memory requirement for storing key information compared to traditional schemes, their memory requirements have been continuously decreased [5], [30].
- *Group authentication codes (GA-codes):* These are A-codes that also offer anonymity (like group signatures). Using GA-code, any authenticated user can send an authenticated message. The receiver can verify that the message has been sent from a legitimate user but at the same time retains his anonymity [31], [32].
- *Network coding:* A-codes that are linear in the keys can be used for application to distributed authentication schemes. On the other hand, A-codes that are linear in the messages are useful in the context of network coding. Network coding was proposed to maximize the throughput of multicast networks. Thus, intermediate nodes not only can store and forward the messages but also can encode the received messages before forwarding them. However, systems exploiting network coding are vulnerable to pollution attacks that are amplified by the network coding process. Pollution attacks consist of injecting malicious packets in the network. The mentioned category of A-codes can be efficiently used to prevent such pollution attacks [33], [4], [34].
- *A-codes with partially-known authentication key:* A-codes are needed in QKD to avoid man-in-the-middle attacks. It can be shown that such systems can still support the unconditional security property even in the case that an attacker has a partial knowledge of authentication (secret) keys [13].
- *Dedicated authenticated encryption:* The generic approach to constructing authenticated encryption is to compose the system by combining an encryption primitive and an authentication primitive. On the other hand, dedicated authenticated encryption schemes are designed to achieve the two goals in one primitive. It is possible to use A-codes to construct dedicated authenticated encryption schemes with reduced amount of key material required for unconditionally secure authentication [35].
- *Authenticating short encrypted messages:* A-codes can also be used to build constructions for efficiently authenticating short encrypted messages that are directed to meet the requirements of mobile and pervasive applications [36].

VI. CONCLUSIONS AND FUTURE WORK

It is important to emphasize that the inclusion of unconditionally secure authentication techniques in e-government security infrastructure is not intended to be a replacement for other authentication methods. In this paper, we tried to show that using A-codes can offer some additional security benefits especially in situations when long-term and/or significantly high level of security is required. Considering the current status of commercially-available technology, we advise A-codes based services for G2G and G2B settings only. It is possible in next stages to include e-democracy (especially e-voting) and then G2C settings according to the rate of required technological advancements (especially in QKD). Our future research in this direction might include proposing a detailed security framework that enables integrating unconditionally-secure services within e-government setting. Carrying a detailed security risk analysis for such environments is another important future research step to better understand the requirements and necessities of offering such security services.

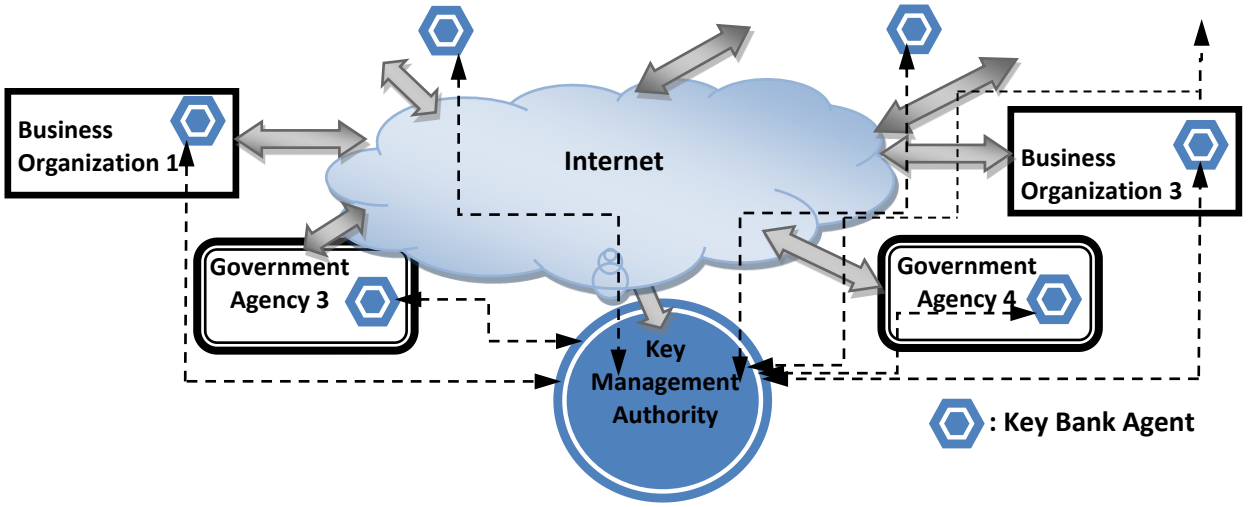

Fig. 3. A typical topological view for the deployment of key bank agents.

REFERENCES

[1] Ueli M. Maurer, "A Unified and Generalized Treatment of Authentication Theory," Proceedings of the 13th Symposium on Theoretical Aspects of Computer Science (STACS'96), Lecture Notes in Computer Science, Berlin: Springer-Verlag, vol. 1046, pp. 387-398, 1996.

[2] _____, "Authentication in an Internet Banking Environment," Federal Financial Institutions Examination Council (FFIEC), Arlington, VA, USA, 2009, http://www.ffiec.gov.

[3] A. Adegun, A. Adigun, and E. Asani, "A REVIEW OF TRENDS OF AUTHENTICATION MECHANISMS FOR ACCESS CONTROL," Computing, Information Systems, Development Informatics & Allied Research Journal, Vol. 5, No. 2, June 2014.

[4] Frederique Oggier and Hanane Fathi, "An Authentication Code against Pollution Attacks in Network Coding," IEEE/ACM Transactions on Networking, Vol. 19, Issue 6, pp. 1587 – 1596, Dec. 2011.

[5] Goichiro Hanaoka, Junji Shikata, Yuliang Zheng, and Hideki Imai, "Efficient and Unconditionally Secure Digital Signatures and a Security Analysis of a Multireceiver Authentication Code," D. Naccache and P. Paillier (Eds.): PKC 2002, LNCS, Vol. 2274, Springer-Verlag, pp. 64–79, 2002.

[6] Johannes Buchmann et al, "Post-Quantum Signatures," eprint.iacr.org, September 30, 2004

[7] Shailendra C. Jain Palvia and Sushil S. Sharma, "E-Government and E-Governance: Definitions/Domain Framework and Status around the World," Foundations of E-government, Computer Society of India.

[8] Geoffrey Karokola, Stewart Kowalski and Louise Yngström, "Secure e-Government Services: Towards A Framework for Integrating IT Security Services into e-Government Maturity Models," Department of Computer and Systems Sciences, Stockholm University/Royal Institute of Technology, Forum 100, SE-164 40 Kista, Sweden

[9] Geoffrey Rwezaura Karokola, "A Framework for Securing e-Government Services- The Case of Tanzania," Doctoral Thesis in Computer and Systems Sciences, Stockholm University, Sweden, 2012.

[10] A. Rabaiah and E. Vandijck, "A Strategic Framework of e-Government: Generic and Best Practice," Electronic Journal of e-Government, Vol. 7, Issue 3, 2009, pp. 241-258.

[11] Bart Preneel, "Cryptographic Primitives for Information Authentication: State of the Art," Appeared in State of the Art and Evolution of Computer Security and Industrial Cryptography, Lecture Notes in Computer Science, vol. 1528, Springer-Verlag, 1998, pp. 50-105.

[12] Huaxiong Wang, Chaoping Xing, and Rei Safavi-Naini, "Linear Authentication Codes: Bounds and Constructions," IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 49, NO. 4, APRIL 2003, pp. 866-872.

[13] Aysajan Abidin and Jan-°Ake Larsson, "Direct Proof of Security of Wegman-Carter Authentication with Partially Known Key," Quantum Information Processing, Vol. 13, No. 10, pp. 2155-2170, 2013.

[14] D.R. Stinson, "Universal hashing and authentication codes," *Advances in Cryptology-CRYPTO'91*, Lect. Notes in Comput. Sci., Vol. 576, pp. 74-85, 1992.

[15] Sufyan T. Faraj Al-Janabi, "Unconditionally Secure Authentication in Quantum Key Distribution," i-manager's Journal on Software Engineering, India, Vol. 1, No. 3, 2007, pp.31-42

[16] J.L Carter and M.N. Wegman, "Universal classes of hash functions," *J. Comput. and System. Sci.*, Vol. 18, pp. 143-154, 1979.

[17] M.N. Wegman and J.L Carter, "New hash functions and their use in authentication and set equality," *J. Comput. and System. Sci.*, Vol. 22, pp. 256-279, 1981.

[18] Thomas Johansson, "Bucket hashing with a small key size," W. Fumy (Ed.): Advances in Cryptology - EUROCRYPT '97, LNCS 1233, Springer-Verlag, pp. 149-162, 1997.

[19] Phillip Rogaway, "Bucket Hashing and its Application to Fast Message Authentication," Department of Computer Science, University of California, Davis, October 13, 1997 (an Earlier version appeared in Advances in Cryptology – CRYPTO '95).

[20] Lj. Antovski, M. Gušev, "E-BANKING – DEVELOPING FUTURE WITH ADVANCED TECHNOLOGIES," Proceedings of the Second International Conference on Informatics and Information Technology (2nd Int. Conf. CiiT), Molika, 20-23 Dec. 2001, 154-164.

[21] Herbert Leitold, Arno Hollosi, and Reinhard Posch, "Security Architecture of the Austrian Citizen Card Concept," Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC '02), p. 391, 2002.

[22] Audun Josang, Kent A. Vardemal, Christophe Rosenberger, and Rajendra Kumar, "Service Provider Authentication Assurance," International Conference on Privacy, Security and Trust (PST), 2012, Paris, France, 2012.

[23] R. Alléaumea et al, "Using quantum key distribution for cryptographic purposes: a survey," arXiv:quant-ph/0701168v3, 4 Dec. 2014.

[24] Sufyan T. Faraj Al-Janabi, "A Novel Extension of SSL/TLS Based on Quantum Key Distribution," Proceedings of the International Conference on Computer and Communication Engineering 2008 (ICCCE08), VOLUME I, pp. 919-922, Malaysia, May 13-15, 2008.

[25] M. Peev, M. Nolle, O. Maurhardt, T. Lorunser, M. Suda, A. Poppe, R. Ursin, A. Fedrizzi, and A. Zeilinger, "A novel protocol-authentication algorithm ruling out a man-in-the-middle attack in quantum cryptography," quant-ph/0407131, June 2005.

[26] JUNG MIN PARK, EDWIN K. P. CHONG, and HOWARD JAY SIEGEL, "Efficient Multicast Stream Authentication Using Erasure Codes", 2001 ACM 1073-0516/01/0300-0034.

[27] Rei Safavi-Niani and Huaxiong Wang," New results on multi-receiver authentication codes," In Advances in Cryptology - Eurocrypt'98, volume 1403 of Lecture Notes in Computer Science, pp. 527 – 541, Espoo, Finland, June 1998. Springer - Verlag.

[28] M. Atici and D.R. Stinson, "Universal hashing and multiple authentication," *Advances in Cryptology-CRYPTO'96*, Lect. Notes in Comput. Sci., Vol. 1109, pp. 16-30, 1996.

[29] Shai Halevi and Hugo Krawczyk," MMH: Software message authentication in the Gbit/second rates," Proceedings of the 4th Workshop on Fast Software Encryption, LNCS, Vol. 1267, Springer, 1997, pp. 172-189.

[30] Goichiro Hanaoka, Junji Shikata, Yuliang Zheng, and Hideki Imai, "Unconditionally Secure Digital Signature Schemes Admitting Transferability," T. Okamoto (Ed.): ASIACRYPT2000, LNCS, Vol. 1976, Springer-Verlag, pp. 130–142, 2000.

[31] G. Hanaoka, J. Shikata, Y. Hanaoka, and H. Imai, "Unconditionally secure anonymous encryption and group authentication," The Computer Journal, Vol. 49, pp.310-321, May 2006.

[32] T. Seito, Y. Watanabe, K. Kinose, and J. Shikata, "Information-Theoretically Secure Anonymous Group Authentication with Arbitration: Formal Definition and Construction," Proc. of Annual Workshop on Mathematical and Computer Science, Josai Mathematical Monograph 7, pp.85-110, Tokyo, Japan, March 2014.

[33] Zhaohui Tang, "Homomorphic Authentication Codes for Network Coding," CONCURRENCY AND COMPUTATION: PRACTICE AND EXPERIENCE, Wiley InterScience, Volume 27, Issue 15, October 2015, pp. 3892–3911

[34] Hong Yang and Mingxi Yang, "An Unconditionally Secure Authentication Code for Multi-Source Network Coding," I. J. Wireless and Microwave Technologies, MECS, 2012, 1, pp. 45-52.

[35] Basel Alomair and Radha Poovendran, "Information Theoretically Secure Encryption with Almost Free Authentication", Journal of Universal Computer Science, vol. 15, no. 15 (2009), pp. 2937-2956.

[36] Basel Alomair and Radha Poovendran, "Efficient Authentication for Mobile and Pervasive Computing," IEEE Transactions on Mobile Computing, Vol. 13, Issue No. 03, March 2014, pp: 469-481.