Security Management in E-Government using Zero-Knowledge Authentication

Assistant Lecturer \ Noor Dhia Kadhm Al-Shakarchy
Computer Science Department, Science College, Karbala University, Karbala, IRAQ

Email: noor.dhiya@gmail.com

Abstract:

E-Government refers to the use of new information and communication technologies (ICTs) by governments as applied to the full range of government functions. In particular, the networking potential offered by the Internet and related technologies has the potential to transform the structures and operation of government. The real benefit of e-government lies not in the use of technology, but in its application to processes of transformation. The sensitivity level of all E-Government systems will be determined based on the sensitivity of the data processed or the importance of the system to mission accomplishment. Security is one of the most important issues in E-government. All systems must include security controls that reflect the true importance of the information processed on the system and/or the government investment embodied in the components of the E-Government system.

Zero-knowledge are proofs that show a statement to be true without revealing anything other than the veracity of the statement to be proven. In the other word, The Zero-Knowledge is a concept used in many cryptography systems to allow a party to prove that he/she knows something, without having to send over the value of this knowledge. In this implementation, it will be used to prove the identification of the user without sending over the some pseudo- random numbers. These numbers changing with any sending.

In this research we illustrates the zero-knowledge proofs (ZKPs) in e-government security with the fact that there is no additional hardware required. This research managed the security of transmission during e-government process depending on zero-knowledge proofs to Indentify and verify the transmission. The data transmitted over this system are not usable by the hacker to help fake an identity .

الملخص:

الحكومة الإلكترونية تعنى قدرة القطاعات الحكومية على تبادل المعلومات وتقديم الخدمات فيما بينها وبين المواطن وبين قطاع الأعمال عبر شبكة الإنترنت بسرعة وبدقة عالية وبأقل التكاليف مع ضمان سرية أمن المعلومات . أي هي استخدام تكنولوجيات المعلومات والاتصالات من جانب الحكومات وتطبيقها على مجموعة كاملة من وظائف الحكومة عن طريق شبكة الإنترنت. الفائدة الحقيقية من الحكومة الإلكترونية لا تكمن في استخدام التكنولوجيا، ولكن في تطبيقها لمعالجات التحول. الأمن هو واحد من أهم القضايا في الحكومة الإلكترونية. بحيث جميع النظم يجب أن تحتوي على نظم سيطرة امنية, التي تعكس الأهمية الحقيقية للمعلومات التي تم معالجتها قي النظام أو الاستثمارات الحكومية المتمثلة في مكونات نظام الحكومة الإلكترونية.

معلومة اللا شيء او المعلومة الصفرية هي البراهين التي تظهر صحة البيانات دون الكشف عن أي شيء آخر غير صحة البيانات المراد اثباتها. في عبارة أخرى، المعلومة الصفرية هي مفهوم يستخدم في العديد من أنظمة التشفير لتسمح لطرف ان يثبت أنه / أنها تعرف شيئا ما، دون الحاجة إلى إرسال غير قيمة المعلومة. في هذا البحث، تم استخدام مبدأ معلومة اللا شيء لإثبات هوية المستخدم دون إرسال أكثر من عدة ارقام شبه عشوائية تتغير مع كل اتصال خلال معالجات منظومة الحكومة الالكترونية. وهذا بدوره يوفر ادارة امينة لاتصالات الحكومة الالكترونية. البيانات المرسلة عبر هذا النظام ليست قابلة للاستخدام من قبل القراصنة كوسيلة مساعدة لتزوير الهوية.

1- Introduction:

The concept of an e-government system is to provide access to government services anywhere at any time over open networks. Electronic delivery of Government services (e-government) refers to the use of new Information and Communication Technologies (ICTs) by governments as applied to the full range of government functions. In particular, the networking potential offered by the Internet and related technologies has the potential to transform the structures and operation of government.

E-government will fundamentally transform the relationship between governments and citizens. At this point, nearly all of the models become quite normative when describing a fully developed e-government, and they assert what e-government should become. The models implicitly presume that fully transactional systems are better and that more citizen interaction equals improved service [1].

The sensitivity level of all e-government systems will be determined based on the sensitivity of the data processed or the importance of the system to mission accomplishment. All systems must include security controls that reflect the true importance of the information processed on the system and/or the government investment embodied in the components of the e-government system. The sensitivity level of all e-government systems will be identified in one of the following categories:

(1) Secure Systems contain information, which requires protection against unauthorized disclosure

(2) Sensitive Systems include those that require some degree of protection for confidentiality, integrity or availability.

(3) Non-Sensitive Systems contain only public data, which has no protection required for confidentiality, and the services of the County can be accomplished without the system.

Five major categories of information are protected through some form of government secrecy[12]:

(1) National defense information, encompassing military operations and weapons technology.

(2) Foreign relations information, including that concerning diplomatic activities.

(3) Information developed in the context of various law enforcement investigations.

(4) Information relevant to the maintenance of a commercial advantage (typically proprietary in nature).

(5) Information pertaining to personal privacy. Of these, the first two categories together define the sphere of "national security information" covered by security classification executive orders and are the primary subjects of this Commission's inquiry.

America's National Information Systems Security Glossary defines information security as: Protecting information systems against unauthorized access or manipulation of information, whether in storage, processing or exchange and the exclusion of services for authorized users or providing services to unauthorized users that includes these necessary actions to discover, document and dealing with such threats [2]. Information security, including techniques such as technical measures and management measures that protect information assets are used against unauthorized acquisition, damage, disclosure, or manipulation, change and loss or abuse of information [3]. The scope of information security includes the protection of all verbal and print information, and information that are automatically recorded for the use of people in organization. This scope also includes the protection of all resources that are used for creating, processing, transmitting, storing, using, viewing or controlling the facilities of restricted environments, communication networks, information staff, peripheral devices, storage and recorded media [4]. Therefore, information security is an interdisciplinary concept that includes a group of related topics on information life-cycle. The importance of information security is seen when most organizations show off their misuse information assets or eliminated assets [4,5]. Information security management is a series of management activities with the aim of protecting and securing information assets within the framework of the organization in which information system is running [5]. Information security management process is an iterative process with feedback and continuous improvement, which

consists of several processes that started with Identify and specify security requirements and will be continued to meet these needs with the required strategies and measuring results to improve information security management [6]. Three general Information security management objectives can be mentioned; information confidentiality, integrity, and availability. Information confidentiality is related to prevent unauthorized disclosure of information. That considered the main task of information security management, it is to give us confidence that, the security requirements that have been imposed on the system are adequate to protect data and resources. Integrity refers to prevent tampering and unauthorized changes to information. Availability refers to limiting the use of information or resources[4, 7]. Another task is to ensure that information security management system is working somehow to meet the security needs [8].

Zero-Knowledge proof is a much popular concept utilized in many cryptography systems. In this concept, two parties are involved, the prover A and the verifier B. Using this technique, it allows prover A to show that he has a credential, without having to give B the exact credential. The purpose of Zero-Knowledge Proof (ZKP) protocols is to help a prover convince a verifier that she holds some knowledge (usually secret), without leaking any information about the knowledge during the verification process (zero-knowledge). The concept of ZKP was first introduced by Goldwasser et al. in [10], and has since been employed in many authentication and identification protocols. Loosely speaking, a ZKP is an interactive proof system which is comprised of a prover and a verifier. The principle rule is that the prover demonstrates knowledge of a secret to the verifier through several interactive rounds. During the process, the prover does not reveal any sensitive information to the verifier or any other parties. Each round involves a challenge (say, a question) from the verifier, and a response (say, an answer) from the prover. If the secrets are related to user identities, ZKP can be used for identification and, in this case, is called Zero-Knowledge Proof of Identity (ZKPI). The security of ZKPI protocols is often based on the intractability of factoring large integers [10] or computing a discrete logarithm problem. Some have been improved to employ mutual authentication and key exchanges [11]. However, since almost all ZKP-based identification schemes are dependent on a trusted third party as an authorized central server.

The reason for the use of a Zero-Knowledge Proof in this situation for an authentication system is because it has the following properties [9]:

- Completeness: if the statement is true, the honest verifier (that is, one following the protocol properly) will be able to prove that the statement is true to an honest verifier every time.
- Soundness: if the statement is false, it is not possible (with a very small chance) to fake the result to the verifier that the statement is true.
- Zero-knowledge: if the statement is true, the verifier will not know anything other than that the statement is true. Information about the details of the statement will not be revealed.

Zero-knowledge protocol provides provably secure entity authentication based on a hard computational problem. The general problem we address is the classical problem of interactive entity authentication.

In this research, the proposed system presents authority and identity to transmission in e-government. The proposed system depends on zero-knowledge as a manner to provide secure management. This system used the concept of zero-knowledge to identify the sender person without sending any information about him/her. The proposed system algorithm and who it is used in by experimental world presented with figures explain steps. Then the attempts to cryptanalysis this system discuss; which gives the system the more strong against the attackers.

2- Related works:

Security in government is not a new concept. Since antiquity politicians, military leaders and other government "agents" have been trying to protect "sensitive" information from unauthorized or accidental loss, destruction, disclosure, modification, misuse or access. Information systems, which are the foundation of e-government, are recognized as socio-technical infrastructures that rely heavily on people. This is particularly true in the case of security, where human factors have played a major part in many security failures. A widely researches done in the field of transmission secrecy with using different ways, algorithms and concepts. The goal of these researches is providing the authentication to them systems. Zero- knowledge proofs is used in that purpose. Many researchers presented dependent on using hard problems that can be employed in these realizations include (Sub)graph Isomorphism, Graph Color ability, Diophantine Problem as a zero-knowledge proof authentication to authenticate new entities requiring entry into network applications while preserving entity privacy and identity works well in these instances[13, 14].

In this research we apply Zero- knowledge proofs dependent on using information security problems of public and privet keys with some number theory (moduli theory) that can be employed in these realizations to authenticate the identification and personality in each side of sender and receiver.

3- Security Management in Communications:

With the development of using networks in different field; security management procedures increasing also to provide the security (uncovered data from deliberate and undeliberate) , integrity (the data is same to source without any modification) and privacy (save unauthorized data and prevent uncovering) to transmission data. These procedures used to manag the protection of computer communications are:

1- Cryptography: the encryption and decryption process to transmission data depending on secret keys. Cryptography considered the active means to prevent passive attack.

2- Access control: access control process confirms all access process are authorized. That's done independent on two points. First is user identification, that's mean nobody can be able to asked for access claim to other users. This point done using authentication process. Second point is protect the information that describe access claim to each user to any modification (delete, modify, insert) from un-authorized

3- Authentication: the requirement to authentication methodes is very important when deal with computer networks. Generally we can distinguish two kinds of authentication algorithms depending on the information available and needed:

   a- User Authentication: it can be release directly using some specific properties founded in the user such as Fingerprint, frequency sound waves , forms the retina and digital signatures. Or indirect when the user have pass word, which it's a secret word or phrase that must be used to gain admission to something. This pass word defined only to actual user.

   b- Message Authentication: it's similar to indirect user authentication, in which this method imposing specific structure of the message. This kind of authentication depending on interaction between sender and receiver. That kind gives the actualization different activities; such as:

   - The message transmit from actual sender.
   - The message contain not modified during transmission process.
   - The message reached to intended receiver. That's done by sending any notification sign to the sender.

The Secrecy and protection can be classified to:

a- Identification: it's a specific definition to each person connected to the network. That definition can be any symbol or number and must be abbreviated and not repeated. In developing case using fingerprint or audio tones to determine user personality. This way

used to protect data and prevent unauthorized used to network by determine the authorized users. The determination done by giving specific identification to each user.

b- Authorization: this protection Identifies users who have licensed civil or fitness for use of network resources and data stored. Usually these resources and data classified into levels of security depending on the degree of secrecy. Such as very secret, secret and authoritative. The authorization determined the processes and fields allowed to each user.

In this research we present this two categories of security and protection the identification represented by privet numbers and authorization presented during zero-knowledge steps.

4. The proposed system :

In cryptography, Zero Knowledge Proofs ZKPs are primarily used as a means of entity authentication. Sender (prover such as Alice) proves to receiver (such as Bob) that he/she is indeed sender (Alice) (and not an impostor) by proving that she possesses S. Of course, she wants to do so without revealing S to Victor (or any potential eavesdroppers).

The proposed system imposed each organization in e-government has identification number. That number must be unique and public. Each user (employer) has two identification numbers first number must be public and unique also. The second identification number must be secret (private) and compute dependence on public identifier. The public numbers used together from sender (prover) and receiver (verifier) to authentication without sending any one of these numbers.

The proposed system makes in three sides the sender (prover) side and receiver (verifier) side and trusted center side which managed the secrecy and protection. A trusted center chose and public number N which comes from two prime numbers N = p.q .The two prime numbers remain secret only N is public. A trusted center also save the public identification numbers to each employer (user).

The process of proposed system divided to two phrase the initialization phrase which done in e-government by a trusted center and identification phrase which done in sender/ receiver sides.

Initialization:

1. A trusted center T selects and publishes an RSA-like modulus n = pq ; but keeps the primes p and q secret.
2. The prover selects a secret s_1,s_2 coprime to n, $1 \leq s_i \leq n - 1$, computes v_i such it satisfy the equation ($s_i^2 * v_i$) mod n = 1, and registers v_i with T as her public key.

Identification Protocol

The following steps are executed t times, each time using independent random coin tosses.

(P1) The prover chooses i random numbers r_i, $1 \leq r_i \leq n - 1$ and sends $x_i = r_i^2 \bmod n$ to the verifier.

(V1) The verifier randomly selects a bit matrix E that size i* 2. E € {0, 1} and sends E to the prover.

(P2) The prover computes and sends to the verifier y_i, where $y_i = r_i \, s_1^{\,e[i,1]} \, s_2^{\,e[i,2]} \bmod n$.

(V2) The verifier rejects if y = 0 or if $y2 \neq x \cdot ve \pmod n$. (Depending on e, $y^2 = x$ or $y^2 = x.v \bmod n$, since $v = s^2 \bmod n$. Note that checking for y = 0 precludes the case r = 0.)

If the verifier has completed all t iterations of the above steps, then he accepts.

5. Experimental Work of Proposed Algorithm:

Initialization

The initialization of proposed system as shown in figure (1) :

1. Let p = 7 and q = 11. Then, n = pq = 77. n is published to a trusted center.
2. prover secretly chooses $s_1 = 9$ and $s_2 = 10$, which are coprime (relatively prime) to n. prover publishes v_1 , v_2 to the trusted center:
   ($s_i^2 * v_i$) mod n = 1
   ($9^2 * v_1$) mod 77 = 1 using inverse algorithm to find the value of v_1, inverse(81,77) = 58.
   ($10^2 * v_2$) mod 77 = 1 using inverse algorithm to find the value of v_2, inverse(100,77) = 67.

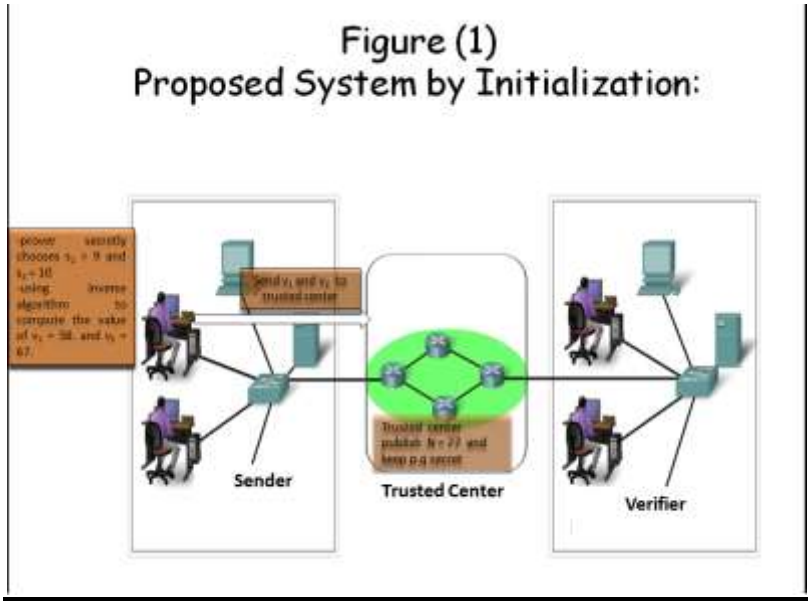


Figure (1)
Proposed System by Initialization:

Protocol

The Prover can be able to identify himself/herself to receiver (verifier) without sending secret (private) numbers {9, 10} or public numbers {58,67}. Each time you wish to identify himself/herself is thus :

Step1: Chose t , t = 2 . so that it requires only 2 successful iterations of the protocol in order to accept.

Step2: Repeat the following steps of protocols until t = 2 ; as shown in figure (2) and figure (3):

(P11) Prover randomly selects many numbers such as 3, $r_1 = 19$, $r_2 = 24$, $r_3 = 51$.

Prover sends $x_i = r_i^2 \bmod n$

$x_1 = r_1^2 \bmod 77 = 19^2 \bmod 77 = 53$

$x_2 = r_2^2 \bmod 77 = 24^2 \bmod 77 = 37$

$x_3 = r_3^2 \bmod 77 = 51^2 \bmod 77 = 60$

X = { 53, 37, 60} sends to verifier.

($V1_1$) verifier randomly selects E and sends it to Prover.

E =

0	1
1	0
1	1

($P2_1$) Prover computes y_i and sends them to Verifier.

$(19 * 9^0 * 10^1) \bmod 77 = 36$

$(24 * 9^1 * 10^0) \bmod 77 = 62$

$(51 * 9^1 * 10^1) \bmod 77 = 47$

Y = { 36, 62, 47}

($V2_1$) Verifier verifies by computes :

$(36^2 * 58^0 * 67^1) \bmod 77 = 53$

$(62^2 * 58^1 * 67^0) \bmod 77 = 37$

$(47^2 * 58^1 * 67^1) \bmod 77 = 60$

X appears again but in verifier side.

Step3: Prover has successfully completed t = 2 rounds. Then the verifier sure that the transmission from actually sender, so Verifier accepts.

Algorithm inverse:

Inv(a,n); return x such that (ax mod n = 1)

Begin

$g_0 := n;\quad g_1 := a;$

$u_0 := 1;\quad v_0 := 0;$

$u_1 := 0;\quad v_1 := 1;$

$i := 1;$

while $g1 \neq 0$ do

begin

$y := g_{i-1} \text{ div } g_i;$

$g_{i+1} := g_{i-1} - y * g_i;$

$u_{i+1} := u_{i-1} - y * u_i;$

$v_{i+1} := v_{i-1} - y * v_i;$

$i := i+ 1;$

end ;

$x := v_{i-1};$

if $x \geq 0$ then inv := x

else inv := x + n ;

end ;

Figure(2)
Proposed System Protocol

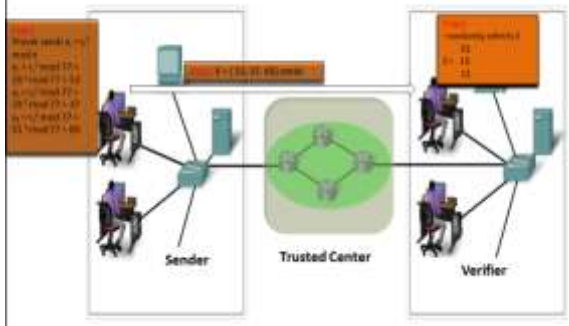
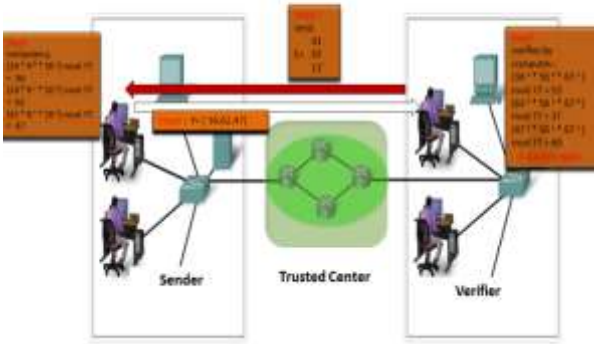


Figure (3)
Proposed System Protocol



6. Proposed System Analysis :

In order to test and analysis the proposed system against varies attempts of attacking and impersonation is discuss in the situations bellow:

Situation 1:

The proposed system upholds the properties of completeness, soundness, and zero-knowledge:

- Completeness: Suppose the prover possesses the secret s. Then she can always correctly provide the verifier with $y_i = r_i\, s_1^{e[i,1]}\, s_2^{e[i,2]} \bmod n$ upon request. Therefore, an honest verifier will complete all t iterations and accept with probability 1.
- Soundness: Suppose the prover does not possess the secret s. Then, during any given round, she can provide only one of $y_i = r_i\, s_1^{e[i,1]}\, s_2^{e[i,2]} \bmod n$. Therefore, an honest verifier will reject with probability 1/2 in each round (which implies an overall probability of 2^{-t} that a cheating prover will not be caught).
- Zero-knowledge: The only information revealed in each round is $x = r^2 \bmod n$ (in step P1) and either $y_i = r_i\, s_1^{e[i,1]}\, s_2^{e[i,2]} \bmod n$ (in step P2). Such pairs (x, y) could be simulated by

choosing y randomly, then defining $x = y^2$ or $x = y^2 /v$. Such pairs, while not generated in the same way as in the protocol, are computationally indistinguishable from them.

Situation 2:

The proposed system success because the private identifier {9,10} and the public identifier { 58,67} satisfy the equation : $(9^2 * 58) \bmod 77$ and $(10^2 * 67) \bmod 77$

That's mean the numbers 9^2 and 58 are invertible multiplication operators of criterion residue (77), also the numbers 10^2 and 67. Therefore :

$$36^2 * 58^0 * 67^1 \equiv 19^2 * 9^{2*0} * 58^0 * 10^{2*1} * 67^1$$
$$\equiv 19^2 * (9^2 * 58)^0 * (10^2 * 67)^1$$
$$\equiv 19^2 \equiv 53 \pmod{77}$$
$$62^2 * 58^1 * 67^0 \equiv 24^2 * 9^{2*1} * 58^1 * 10^{2*0} * 67^0$$
$$\equiv 24^2 * (9^2 * 58)\ 1 * (10^2 * 67)^0$$
$$\equiv 24^2 \equiv 37 \pmod{77}$$
$$47^2 * 58\ 1 * 67^1 \equiv 51^2 * 9^{2*1} * 58^1 * 10^{2*1} * 67^1$$
$$\equiv 51^2 * (9^2 * 58)^1 * (10^2 * 67)^1$$
$$\equiv 51^2 \equiv 60 \pmod{77}$$

If we suppose the sender (prover) is A and the receiver (verifier) is B and the eavesdropper is C. The proposed system is successful to identify A to B also C can't conclude any things about A identify to impersonate his/her later.

Situation 3:

When any one attempt to find the invertible multiplication operators of criterion residue (77) according to the public numbers {58, 67}. To explain that, suppose C attempt to personate A (C fool B her A) if C can be able to generate same number that generated from A {53, 37, 60} and sends to B. Then suppose B generate same matrix E and sends to C. In this step C in problem because she don't know the secret numbers {9, 10}. She can expect them value. The protocol required to send three numbers {x, y, z} to B. B attempt to verify :

$x^2 * 58^0 * 67^1 \equiv 53 \pmod{77}$

$y^2 * 58^1 * 67^0 \equiv 37 \pmod{77}$

$z^2 * 58^1 * 67^1 \equiv 60 \pmod{77}$

C can be success to impersonate A if she chose the numbers {x, y, z} that make investigations above be true, but :

$67^{-1} \equiv 10^2 \equiv 23 \pmod{77}$

$58^{-1} \equiv 9^2 \equiv 4 \pmod{77}$

Therefore the values :

$x^2 \equiv 53 * 23 \equiv 64 \pmod{77}$

$y^2 \equiv 37 * 4 \equiv 71 \pmod{77}$

$z^2 \equiv 60 * 23 * 4 \equiv 53 \pmod{77}$

C can be able to solve Quadratic Equation and find the values x= 36, y = 62, z = 47 with small value to N . but if N = p. q is large value (selected p and q are large prime numbers; such as each number consist of 80 digit) and kept these numbers (p, q) secret, the solution of theses equations became very difficult. And calculate square roots to the number consist of product of two prime numbers is a infeasible process, especially if N is large value.

Situation 4:

Another possibility, the transmission between A and B can be gives some information to B which leads to impersonate A. That's done in one case, when the transmission between them repeated. Suppose B attempt to convinces C he is A. B attempts to imitate A by sending the numbers {53, 37,60} to C . thus begin the verification of identifier process. C not necessary selects same B matrix E. suppose she chooses F:

F =

1	1
0	0
0	1

Then sends F to B. In this moment B in impasses, B attempt imitates A by sending the numbers {36, 62,47} to C. C verify from :

$36^{2} * 58^{1} * 67^{1} \equiv 71 \pmod{77}$

$71 \neq 53 \pmod{77}$; C discovers B is cheat (swindler) without continuing other verifications. B can be sends the numbers { r, s, t} instead of { 36, 62, 47} only if satisfy the following:

$r^{2} * 58^{1} * 67^{1} \equiv 53 \pmod{77}$

$s^{2} * 58^{0} * 67^{0} \equiv 37 \pmod{77}$

$t^{2} * 58^{0} * 67^{1} \equiv 60 \pmod{77}$

as above :

$r^{2} \equiv 58^{-1} * 67^{-1} * 53 \equiv 25 \pmod{77}$

$s^{2} \equiv 37 \pmod{77}$

$t^{2} \equiv 71 \pmod{77}$

if N= 77 (small value) B can solves Quadratic Equations to find the values of { r, s, t}, but he can't with large N. There is a possibility one of the 64 to choose C F = E, and this makes the B case is unexposed, but with large numbers this case has very small possibility.

Situation 5:

Another possibility, when A is trying to define itself to B may give some information without notice. This information enable B to know secret numbers { 9, 10}, thus allow impersonates A. That's should not happened with zero-knowledge.

If B attempt to conclusion secret numbers {9,10} from the two groups { 53, 37, 60}, {36, 62, 47} and the matrix E , he suppose the following :

B know A begin with three numbers {a, b, c} but he doesn't know the values of these numbers. also B know A has two secret numbers {u, v} , but he doesn't know them values. He know a relationship between public and secret numbers :

$u^{2} \equiv 58^{-1} \equiv 4 \pmod{77}$ ……(1)

$v^{2} \equiv 67^{-1} \equiv 23 \pmod{77}$ ……(2)

{a, b, c} can be calculates:

$a^{2} \equiv 53 \pmod{77}$ ……(3)

$b^{2} \equiv 37 \pmod{77}$ ……(4)

$c^{2} \equiv 60 \pmod{77}$ ……(5)

$a * u^{0} * v^{1} \equiv 36 \pmod{77}$ ……(6)

$b * u^{1} * v^{0} \equiv 62 \pmod{77}$ ……(7)

$c * u^{1} * v^{1} \equiv 47 \pmod{77}$ ……(8)

B has 8 equations to conclusion values of {u, v}. the first 5 equation can't solve with large N, and the last 3 equation repeated.

7. Conclusion:

The proposed system gives sufficient amount of secrecy to be applied and indicate the following points:

a. The proposed system gives fewer possibility to impersonate equal to 1 from 64 .
b. The sender (prover such as A) recognized by proofing he/she has secret identification numbers (such as {9, 10}).
c. The sender (A) is recognized in Single. Any person does not know the numbers of confidentiality (secret numbers) can't impersonate A.
d. The sender (A) secret numbers can't discovered during verification process because he/she doesn't send any information about himself/herself.

e. We can increasing the secrecy of this system and decreasing possibility of impersonation simplicity by using large number to N , and sender's (A) identity consist of 4 or 5 numbers also the random numbers generated then sending to verifier (receiver such as B) increases such as (4 or 5).

8. Reference:

[1] David Coursey, Donald F. Norris , "Models of E-Government: Are They Correct? An Empirical Assessment" , Public Administration Review , June 2008

[2] Hone KJ, Eloff HP, " Information security policy what do international information security standards say?", Rand Afrikaans University, 2002.

[3] Eloff J, Eloff M ," Information security management - a new paradigm", ACM. pp. 130-136, 2003.

[4] Finne TA, " Conceptual framework for information security management", J. Computer Security, 17(4): 303-3071998.

[5] Solms RV, "Information security management: the code of practice for information security management (BS 7799)", Information Management Computer Security, 6(5): 224-225, 1998.

[6] Bjorck F, " Security scandinavian style, interpreting the practice of managing information security in organizations", Stockholm University & Royal Institute of Technology, 2001.

[7] Mitchell R, Marcella R, Baxter C, " Corporate information security management", New Lib. World, pp. 213-227, 1999.

[8] Mehdi Kazemi, Hamid Khajouei and Hashem Nasrabadi, "Evaluation of information security management system success factors: Case study of Municipal organization", Faculty of Management and Accounting, University of Sistan and Bluchestan, Iran, 28 November, 2011.

[9] Lum Jia Jun, Brandon, "Implementing Zero-Knowledge Authentication with Zero Knowledge (ZKA_wzk)", PyCon Asia-Pacific 2010.

[10] S. Goldwasser, S. Micali, and C. Rackoff, "The Knowledge Complexity of Interactive Proof Systems," SIAM J. Computing, vol. 18, pp. 186 - 208, 1989.

[11] J. Brandt, I. B. Damgard, P. Landrock, and T. Pedersen, "Zeroknowledge Authentication Scheme with Secret Key Exchange," Proc. Advances in Cryptology, 1990.

[12] Salahuddin Alfawaz, Lauren May, Kavoos Mohanak, "E-government security in developing countries: A managerial conceptual framework" ,Queensland University of Technology, Brisbane, Australia.

[13] Joseph M. Kizza, Lindsay Bramlett and Elizabeth Morgan, "Using Subgraph Isomorphism as a Zero Knowledge Proof Authentication in Timed Wireless Mobile Networks", Chattanooga, Tennessee International Journal of Computing and ICT Research 2010.

[14] Dima Grigoriev and Vladimir Shpilrain, "Zero -Knowledge Authentication Schemes From Actions On Graphs, Groups, Or Rings", Department of Mathematics, The City College of New York, New York, NY 10031.