"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XIX – 2016 – Issue 1
Published by "Mircea cel Batran" Naval Academy Press, Constanta, Romania // The journal is indexed in: PROQUEST / DOAJ / DRJI / JOURNAL INDEX / I2OR / SCIENCE LIBRARY INDEX / Google Scholar / Crossref / Academic Keys / ROAD Open Access / OAJI / Academic Resources / Scientific Indexing Services / SCIPIO

DEVELOPING AND MODELING A NEW E-LOTTERY SYSTEM USING ANONYMOUS SIGNATURES

Florin MEDELEANU[1]
Ciprian RACUCIU[2]
Dan Laurentiu GRECU[3]
[1]Phd.cand. Eng. Ministry of National Defense
[2]Ph.D Prof. Eng. Titu Maiorescu University
[3]Ph.D Prof. Eng. Titu Maiorescu University

Abstract: *In traditional lottery systems, the players choose some numbers on a ticket, enroll it to the lottery organizer and pay an amount of money for it. But this perspective offers no guarantee to the players that the lottery organizer doesn't manipulate the number selection in order to pay the least. This suspicion could be avoided if the lottery organizer didn't know the numbers selected by the players before the draw. Such a system is possible to be realized by using anonymous signatures, but the design should also guarantee that forging lottery tickets after the moment of the draw or claim of a different ticket is not possible. This paper will propose and analyze a model in order to fulfill all requirement described before, using several cryptographic primitives.*

Keywords: *e-lottery, anonymity, anonymous signing, encryption.*

INTRODUCTION

Lottery is probably the most ancient and known chance game, being practiced long time ago starting from antiquity. The idea of the game in its basic structure is simple and very intuitive: objects (usually balls) containing symbols (numbers, figures etc.) are drawn at random from a container, every player who guessed the draw being awarded a prize, according to some specific rules that depends of the lottery system.

During the present time, the most spread lottery system is that with numbers extracted at random and different prizes for different winning classes according to the correct guessed numbers, the more numbered are hit the better the prize is.

One of the drawbacks of the current lottery system is the lack of trust coming from the suspicion that the organizer of the draw knows in advance all played combinations and can manipulate the extracted of numbers. This reasonable suspicion is justified by the fact that it is in the advantage of the lottery not to award the biggest prize in order to accumulate even bigger sum of money for the highest class of prizes. This situation leads on attracting even more players and increasing the profit lottery has, but also raises questions about the fairness of the game. Theoretically, the existence of a fair lottery game should be in the advantage of the both parts, the organizer and the players equally. The fair game should be in the benefit of the lottery because suspicious people who otherwise wouldn't play could be convinced that the chance to win is equal for all participants in the game, this fact leading on increasing the number of players and augment the profit. Such system would also be in the advantage of the players by guaranteeing them that the lottery can't chose to award or not to award the prizes as it pleases.

STANDARD SIGNATURES AND ANONYMOUS SIGNATURES

Standard digital signature schemes are mathematical schemes for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to trust that the message was created by a known sender, that the sender cannot deny having sent the message (authentication and non-repudiation), and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

RSA cryptosystem (Rivest-Shamir-Adleman) is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

Below the RSA cryptosystem is described how it works. The users of RSA algorithm create and then publish a public key based on the two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the

DOI: 10.21279/1454-864X-16-I1-042

message. The RSA algorithm involves three steps: key generation, encryption and decryption.
The algorithm for key generation in RSA involves generation of two keys: a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.
Anonymous signatures schemes use standard signature algorithms, but instead of proving the signer identity of the message m at any moment, the signature σ conceals the identity of the signer up to a specific moment in time. Anonymous signatures are used in many applications where the identity of the signer needs to be protected (e.g. key exchange protocols, electronic auction systems or electronic paper review systems). The authors of the present paper also used an anonymous signature scheme in designing an e-voting system presented in [1].
There are several anonymous signature schemes, but most important and prevalent schemes are Yang [2] and Saraswat [3]. Yang’s scheme for anonymous signature guarantees the anonymity of the signer when the adversary obtains only the signature but not the message, or when the message contains a random string, called security parameter, which is kept hidden until the verification phase. To keep secret a part of the message may be not appropriate in some applications, but there are also enough applications which require not revealing the complete message.
Saraswat’s scheme for anonymous signature splits the digital signature σ^* in two segments of data, $\sigma^* = (\sigma, \tau)$. The first part of digital signature (σ) is called anonymous signature or simply signature, and the second part of the digital signature (τ) is called verification token or simply token. The generation of signature (σ) and token (τ) makes use of signature generation algorithm which uses as inputs the signer’s secret key and the message m. Verification phase occurs when anonymous signer decides to prove publicly the anonymous signed message m belongs to him. At this moment, the signer has to make public m, σ and τ, and then the validity of the signature can be verified by everybody making use of the public key of the signer. During the time τ is hidden, nobody can determine who the signer is, so the anonymity of the signer cannot be break only from the message m and the signature σ. At the end everybody who is revealed the token τ and the identity of the signer (his public key certificate) can verify the signature.
An anonymous signature scheme Σ is a triple of algorithms Σ = (Gen, Sig, Vf), where the key generation algorithm Gen() produces a key pair (pk, sk) □ Gen(), the signature generation algorithm Sig() produces a pair of a signature and a verification token $\sigma^* = (\sigma, \tau)$ □ Sig(sk, m) using the secret key sk and a message m□{0,1}*, and the deterministic signature verification algorithm Vf(pk, m, σ, τ) produces an output „*true*” or „*false*”. In the case that the signature, token or the message was not tampered, the following relation holds:

$$Vf(pk, m, Sig(sk,m)) = true \quad (1)$$

for (pk, sk) □ Gen(), and for any m□{0,1}*.

THE EXISTING LOTTERY SYSTEM

The Romanian lottery system 6/49 started on August 8th 1993 (*www.loto49.ro*), but the official lottery site (*www.loto.ro*) displays the results of the draws starting only from January 4th 1998. The rules of the Romanian lottery are the same as other similar lotteries. Players participate to the lottery by buying tickets. On a ticket it is possible to choose one or two from the following variants: trying to guess 6 numbers from 1 to 49 and/or trying to guess a luck number consisting of 7 figures. It is possible to buy tickets for the next draw, but not latter than the day before the draw. The tickets are filled by the players at theirs choice and then the ticket is validated by an electronic machine which scans it and prints on the ticket a code which confirm the numbered chosen by the player. The winning numbers are extracted by a machine, under the supervision of a commission formed with people from the Ministry of Finance, the Ministry of the Interior. The draw is public and anybody can assist on it at request. The draw machine consists of a bowl with balls labeled from 1 to 49. The machine chooses six balls at random, without replacement. These balls are the “regular balls”. After the regular 6 balls are extracted, another draw is made, this time only with 10 balls, numbered from 0 to 9. The second extraction is repeated 7 times, with balls replacement. In this way it is formed a number composed of 7 figures, the so called Luck number.

TESTING THE RANDOMNESS OF THE LOTTERY

In order to evaluate the opportunity to develop and implement the proposed anonymous lottery system, the authors considered it is necessary to investigate the randomness of the draws in some countries. For this purpose the randomness of three lotteries (Romanian, British and Canadian) was investigated. The testing methods and comparative results are presented in this section.
For lottery systems of the type $k=N$ (for example the system 6/49), a natural issue is whether all the numbers forming the winning combination appear with equal probability. Of similar concern is the

DOI: 10.21279/1454-864X-16-I1-042

randomness of the selections generated by the randomization algorithms, for example “QuickPick” algorithm. A drawing mechanism, be it electronic or mechanical, failing this criterion would clearly induce inequity and should be revised. For a thorough testing, a way to follow is to test that all subsets of two numbers have the same probability of occurrence, and likewise for subsets of size three, four, and so on.

In most of the countries, lottery regulators continually monitor the operating procedures to check that winning selections are drawn randomly. An important part of this process involves physical checks of the mechanical draw equipment; another involves supervising and verifying the conduct of the draws; a third involves statistical analyses to assess the numbers drawn. This part of the paper focuses on the last of these issues. There are three main purposes for the monitoring and testing: to identify possible sources of bias, to warn of possible corruption and to reassure the public that the draws are random. Although statistical analyses might be able to detect very specific sources of bias or corruption, their purpose is mainly to reassure the public that the numbers drawn accord with the assumption of randomness.

The published literature on, and practical applications of, statistical analyses for assessing lottery randomness have almost exclusively adopted frequentist methods of inference, in the form of goodness-of-fit tests; see Joe (1993), Haigh (1997) and the University of Salford (2004-2005).

To determine whether Romania's Lotto 6/49 is fair, the results of n=1140 draws (from 2000 to 2016) were extracted from the site of Romanian Lottery. Figure 1 displays the observed variability in the occurrence of the various numbers in the six-ball winning combination.

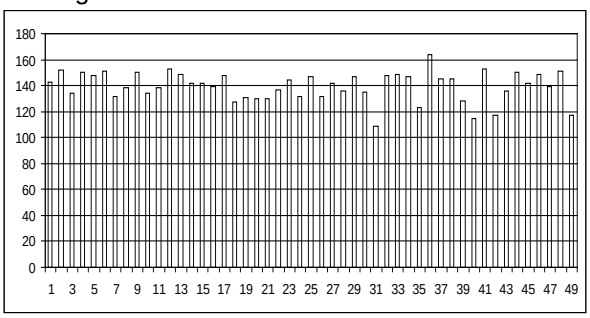

Fig.1. Observed frequency of occurrence of balls 1 to 49 in the six-number winning combination of the first n = 1140 draws of Romania's Lotto 6/49.

The minimum and maximum observed frequencies were 109 and 164, corresponding to balls 31 and 36, respectively.

For testing equiprobability of the N individual numbers, a natural way to proceed is to determine the frequency O_i with which the numbers i = 1,…,N occurred in n lottery draws, and then attempt to compare these observed counts with expected counts $E_i = nk/N$ using the traditional Pearson statistic:

$$\chi^2_{N-1} = \sum_{i=1}^{N} \frac{(O_i - E)^2}{E} \quad (1).$$

However, the asymptotic distribution of this statistic is not the usual chi-square with $N - 1$ degrees of freedom, denoted by χ^2_{N-1}, under the null hypothesis of equiprobability. This is because the observations are not drawn with replacement. Indeed, once a number has been selected among the k winning numbers drawn on a particular occasion, it cannot be chosen again in that same draw; the variability of the standard statistic (23) is thereby reduced.

According to [Joe], it is mentioned that it is necessary to modify χ^2 to $J = (N-1)\chi^2/(N-k)$ in order to obtain for the latter the limiting distribution χ^2_{N-1}.

Let O_α be the observed frequency of the event α in n independent (unordered) k-tuples, where α is a subset of {1, …, N} with cardinality between 1 and k inclusive.

For the univariate margin, $O_{\{i\}} = O_i$ is the observed frequency of the number i. An asymptotic chi-square with (N – 1) degrees of freedom test statistic is:

$$\chi^2_{N-1} = \frac{N-1}{N-k}\frac{1}{E}\sum_{i=1}^{N}(O_i - E)^2 \quad (2).$$

Using the frequency of occurrence of balls 1 to 49 observed in the period 2000 – 2016, displayed in fig.1, the calculated test statistic is:

$$\chi^2_{48} = \frac{49-1}{49-6}\frac{49}{1040\cdot 6}\sum_{i=1}^{49}(O_i - \frac{1040\cdot 6}{49})^2 = \frac{48}{43}\frac{49}{1040\cdot 6}\sum_{i=1}^{49}(O_i - \frac{1040\cdot 6}{49})^2 \quad (3).$$

The result for test statistic is:

$$\chi^2_{48} = \frac{48}{43}\frac{49}{1040\cdot 6}\cdot 6131.837 = 49.0346821 \quad (4).$$

For this value of test statistic χ^2_{48}, the corresponding p-value is:

$$p\text{-}value = 0{,}431389 > 0.05 \quad (5),$$

The hypothesis of equidistribution cannot be rejected at the 5% level for sets of individual numbers, suggesting that the drawing mechanism used is fair and implying the extracted numbers,

DOI: 10.21279/1454-864X-16-I1-042

seen as individual numbers, are random.

THE PROPOSED E-LOTTERY SYSTEM

By fair lottery, in the context of this paper, the authors refer only to the lottery system in which the organizer of the lottery doesn't know the numbers that players choose before the moment of the draw. By knowing the played numbers before the moment of the draw, the lottery could have the theoretical possibility to manipulate the draw in such a way that nobody wins some intended prizes.

Of course, by having the possibility to control the winning numbers, the lottery still have the chance to collude with a specific player and to choose as winning numbers the combination played on a specific ticket by this colluding player. This aspect is beyond the scope of the present paper.

In this chapter the authors are focusing on designing a fair e-lottery system based on anonymous signature, having main features as follows:

- The player can participate to the draw and keep secret the numbers he chose;
- Any modification of the e-ticket by the player after the bet placing should be noticeable. Also nobody can forge a winning ticket or impersonate a winner to claim a prize that not belongs to him;
- It is unfeasible for the lottery or other party to determine played numbers before the claiming phase;
- The lottery can validate or reject the claimed e-tickets through a secure and reliable mechanism.

The proposed system is composed of several systems including Registration Authority, Certification Authority, E-Coupon Issuer, Public Board, Lottery Draw Machine and E-Token. Usually E-Lottery systems use secure cryptographic primitives for random number generation. For example, in [4], the random bit stream used to produce the winning numbers, is generated using a combination of physical random number generators, a post-processing pseudo-random function (Naor-Reingold), an algebraic number generators (RSA and BBS) and a secure software random number generators based on block ciphers (DES and AES).

In this paper the authors tried to improve the security of traditional lotteries, but in the same time tried to preserve as much as possible from the existing system. In this way, the authors supposed that the generation of the random numbers is made by a traditional draw machine (using physical balls marked with numbers). This fact permits to use a combination of the traditional lottery system with the authors' proposal. It is up to the players to choose between one and another system, ultimately being a matter of costs, trust and security. The proposed system allows the players to take part to the lottery in the traditional manner (on paper coupons) and also to play with e-tickets in anonymous way, revealing their chosen numbers only after the draw. In this way, the lottery cannot manipulate the selected numbers in such a way to avoid awarding prizes, to accumulate more money and to increase the interest for big prizes.

The components in the scheme are presented below, including theirs role and responsibilities.

(1) Player. A player is a person who wants to submit e-coupons on which he chooses some numbers in order to participate to the draw for which the lottery opened subscription, before the pre-established dead line. The player for the e-lottery has a secure smartcard for holding the credentials of the player for identification purposes and critical security parameter (private key). The public-private key pair is generated by the player and is submitted to the Registrar along with personal identification data (name, surname etc.).

(2) Registration Authority. The Registration Authority (RA) is an entity which establishes an accord with the Certification Authority for implementing registration, identification and authentication processes of users for data centralizing and identity check and information validity concerning public key certificates. RA operates according to a written set of rules described in Certification Practice. RA records the identification data of the player and keeps his public key certificate.

(3) Certification Authority. The Certification Authority (CA) is an entity authorized for creating, signing, issuing and managing public key certificates. CA is comprised of hardware, software, personnel and procedures required for implementing the certificate lifecycle management undertaken by Certificate Policy. CA is responsible for whole aspects of management and issuance of public key certificates. This responsibility includes control upon the registration process, certificate manufacturing process, publication of certificates, revocation of certificates, and rekey of certificates. The public key certificate of the player, which includes his public key, is digitally signed with the private key of CA.

(4) E-coupon Issuer. The E-coupon Issuer is an application server responsible for managing the electronic transactions related to E-coupons purchasing and processing. This server is connected to Internet and receives requests from the clients (players of lottery) from Internet. The E-coupon Issuer calculates the amount of money that the player has to pay for the requested E-coupon. The player enters into a normal secure

DOI: 10.21279/1454-864X-16-I1-042

paying transaction, and if this transaction finishes successfully the server time-stamps and signs the E-coupon. The player can check on the Public Board that his E-coupon was processed and it enters into the contest for the next or following draw.

(5) E-coupon. The E-coupon Form is an electronic collection of data coming from the player to the E-coupon Issuer. This collection has a predefined format and could contain different data fields, for example the date of the draw, the quantity of number played, and other information considered relevant by the lottery. This collection of data includes the anonymous signature of chosen numbers, but not the chosen numbers in any format.

(6) Lottery - Draw Machine (LDM) is any existing electrical or mechanical machine used for extracting at random numbers from a pre-defined set. Existing lotto systems used in Romania are 5 out of 40 or 6 out of 49. LDM publishes extracted numbers on PB, where players can view the winning numbers and claim for the prizes. LDM can be improved or replaced with any secure cryptographic combination of primitives for random number generation.

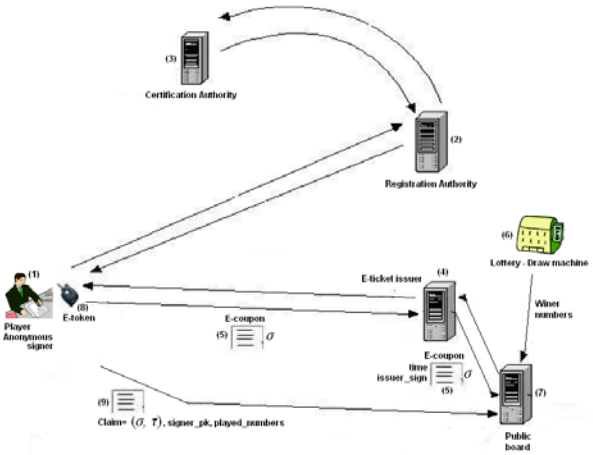

Fig.2. The proposed e-lottery system

(7) Public Board (PB) is a public data-base (public directory) where players can check the status of theirs E-coupons. Also, anybody can check the validity of the current draw E-coupons, the number of sold E-coupons, and the correctness of winning E-coupons. PB is responsible for updating information about winning numbers, miscellaneous information and for prize claiming. By using the PB, the total prize is publicly verifiable because every sold E-coupon is available at PB. Every user can view and check his E-coupons on PB, and signed E-coupons can be kept for dealing with possible disputes. The winning tickets are publicly verifiable, because after claiming phase the anonymous signature validity of the winning tickets can be proved at the public board. Inserting, deleting or modifying tickets after the end of sale is detectable based on the signature applied to the whole quantity of sold E-coupons.

(8) E-Token is a smart-card which stores the public key certificate and the corresponding private key. It supports and implements the public key infrastructure and executes security and cryptography computing required by the E-lottery system.

(9) Claim. The Claim is an electronic collection of data coming from the player to PB in order to prove the possession of a specific E-coupon listed at PB and to confirm that the anonymous signature provided to the E-coupon issuer in the purchasing phase matches the pretended numbers contained in the claim. The lottery system awards the prizes only after checking the validity of the received claims.

In Table 2 there are summarized the advantages, drawbacks and limitations of the existing system and proposed system.

SECURITY ANALYSIS

The anonymous signature scheme proposed by the authors uses a combination of Yang and Saraswat scheme in order to achieve the desired features and to obtain enough level of security. Having in mind that the numbers should not be known before the claim, the usage of Saraswat scheme alone is not appropriate because this scheme supposes that the message is entirely public, and the chosen numbers should be kept secret until the claiming phase. The usage of Yang anonymous signature scheme might be a choice, but still is not enough because using the chosen numbers as random string does not offer enough security.

Requirement	Existing system	Proposed system
Played numbers are known before the draw	Yes*	No
The organizer of the draw can chose to award or not to award the prizes	Yes*	No
The players are trust the system and believe it is fair	No*	Yes
The prize can be claimed by a different person	Yes*	No
Players can run the lottery 24/7 staying at home	No*	Yes
The lottery can collude with a specific player in order to win the jackpot	Yes*	Yes*
The cost of the system is high	No	Yes*
The system needs user	No	Yes*

DOI: 10.21279/1454-864X-16-I1-042

enrollment before the draw		
The system is simple and easy to understand	Yes	No*
The system difficult to be installed and maintained	No	Yes*

Table 2 – Comparative analysis between existing and proposed lottery system (* is a drawback)

For example, in the case of 6 out of 49 lottery system, a chosen number from 1 to 49 can be represented by 6 bits. It results that 6 numbers can be represented by 36 bits. The random string in Yang scheme represents the security parameter. An attacker should try exhaustively all possible combinations of random string to break the anonymity of the scheme. It is easy to notice that a 36 bit length string cannot offer an acceptable level of security. In order to achieve the desired level of security, the 36 bit length string should be concatenated with 92 bits generated at random. The authors considered inappropriate and useless to generate and to keep secret these 92 random bits and found more appropriate to combine Yang and Saraswat scheme. In this way the random string is represented by chosen numbers and the resulting signature σ^* is split in two parts (σ, τ), as described in the section 2. Only the message m, without the 36 bit length random string (chosen numbers), and the anonymous signature σ is published on PB.

In the claiming phase, the player reveals the 36 bit length random string which represents the chosen numbers and the verification token (τ). The lottery can validate the claims and proceed to award the prizes. Everybody can also check the validity of the winning E-coupons published to PB. An attacker cannot find out either the identity of the player or the specific chosen numbers, because he doesn't have the entire signature to match with every possible number combination and every possible signer public key.

CONCLUSIONS

Of course, as long as there is doubt about number selection, the lottery can collude with specific players and play some chosen numbers which follow to be drawn. This situation can be avoided only with impartial and truly random number selection. For the lottery system currently used in Romania, to play the lottery in anonymous way, without revealing the numbers before the draw, can only improve the trust into the lottery system to some extent, but cannot assure that the game is completely fair.

Even if there is no evidence about the unfairness of the Romanian lottery, other than the popular belief or some rumors, an anonymous lottery system could fill the lack of trust that exist among some players, and also could offer several new possibility to play the lottery remote (for example using the internet) or locally (on site, using the existing lottery system).

In order to improve the security of the proposed e-lottery system, the release of the anonymous signature σ might be done by using a commitment scheme. In this way the anonymity of the proposed scheme would be greatly improved.

BIBLIOGRAPHY

[1] Răcuciu Ciprian, Medeleanu Florin, Grecu Dan Laurenţiu Anonymous Signature Applications in E-votting Systems, Conferinţa Internaţională „Educaţie şi creativitate pentru o societate bazată pe cunoaştere", Ediţia a VIII-a, 20 – 22 noiembrie 2014

[2] Guomin Yang, Duncan S. Wong, Xiaotie Deng, and Huaxiong Wang, Anonymous Signature Schemes, http://eprint.iacr.org/2005/407.pdf

[3] G. Yang, D. Wong, and X. Deng. Efficient anonymous roaming and its security analysis, Proc. of the 3rd International Conference on Applied Cryptography and Network Security (ACNS 2005), pages 334–349. Springer-Verlag, 2005. LNCS 3531

[4] Vishal Saraswat and Aaram Yun, Anonymous Signatures Revisited, http://eprint.iacr.org/2009/307

[5] Elisavet Konstantinou, Vasiliki Liagkou et. al, Electronic National Lotteries, Springer Verlag Berlin Heidelberg 2004

[6] Cătălin Bărboianu, The Matematics of Lottery, Odds, Combinations, Systems, Infarom Publishing.

[7] L. Hussain El Fadil, An Electronic Voting Based on Multi-Party Computation, Cryptology ePrint Archive, Report 2014/663, 2014. http://eprint.iacr.org/

[8] Orzan Gh., Ioanăs M., Radu A., Stoica I., Popescu M. (2015), Conceptual model regarding security and protection consumers' rights in the online environement; Economic Computation and Economic Cybernetics Studies and Research; Vol.49, Number 1/ 2015; ASE Publishing, Bucharest

[9] Claude Shannon, A mathematical theory of communication; The Bell System Technical Journal, 27:379–423:623–656, 1948.

DOI: 10.21279/1454-864X-16-I1-042

[10] E. Van Herreweghen, Secure anonymous signature-based transactions; ESORICS '00: Proc. of the 6th European Symposium on Research in Computer Security, pp. 55–71. Springer-Verlag, 2000. LNCS 1895.
[11] Steinfield C. and Whitten P. (2006), Community Level Socio-economic Impacts of Electronics Commerce; Journal of Computer-Mediated Communication; Vol.5, pp.1-2;
[12] Joinson A.N., McKenna K., Postmes T. (2007), Self-disclosure,Privacy and the Internet; Oxford Handbook of Internet Psychology, Oxford University Press, Oxford;
[13] Joe H., Tests of uniformity for sets of lotto numbers; Statistics & Probability Letters 16 (1993), pp.181-188

DOI: 10.21279/1454-864X-16-I1-042