ISSN No. 0976-5697

Volume 3, No. 3, May-June 2012

International Journal of Advanced Research in Computer Science

TECHNICAL NOTE

Available Online at www.ijarcs.info

Electronic Voting System: An Issue of Voter's Privacy against the security of the system

Vinod. M. Patil
Head, Associate Professor
Department of Computer Science,
Shri Shivaji College, Akola
Akola-444001, MS, India
vinmpatil2@yahoo.co.in

Sanjay Dhopte
Associate Professor
Department of Information Technology
Prof. Ram Meghe Institute of Technology and Research
Badnera 444601 Dist. Amravat,i , MS ,
sanjaydhopte@gmail.com

Dr. V. M. Thakare
Prof & Head
Post Graduate Department of Computer Science
S. G. B Amravati University, Amravati-444602, MS, India
vilmthakare@yahoo.co.in

Abstract: This electronic document is a "live" template. The various components of your paper [title, text, heads, etc.] are already defined on the style sheet, as illustrated by the portions given in this document. Do not use special characters, symbols, or math in your title or abstract. The authors must follow the instructions given in the document for the papers to be published. You can use this document as both an instruction set and as a template into which you can type your own text. In order to increase a faith over e-voting systems, several research efforts have focused on making such systems auditable (or verifiable) so that all actions taken during the elections process can inspected and verified by everyone and simultaneously preserve the voter privacy and this is the challenging task. Since two things occur in parallel and it is very difficult to manage it at a time during the voting process.

Keywords: Secrete key, Private Key, privacy etc.

I. INTRODUCTION

Electronic balloting and voting can make the election process more convenient and efficient if it can be achieved securely as well as preserve the voters privacy. The basic principles of democracy are base on collective decision making of societies. It may be consider as an important indicator of civilization. The principle of some form of population voting as a society decision-making process is the basis of the paradigm. Assuming that the ultimate democracy would provide for all citizens to vote on all decisions, the purpose here is to show how the use of Information Technology could be considered as an important factor for a new step towards democratic process. Not only because it changes the scale of decision making but also because it permits creation of new communication and decision links that do not exist in the present political structures. Here try to achieved the two things that are voter's privacy and security simultaneously practically.

In order to preserve the voter's privacy, generate pseudonyms of the voters that cannot directly link to the voters registration. This cannot identify the voters by the election authority or any political party or anything else without the permission of voter and other three groups. The group means consider the different groups related to the political party, related to the NGO or social group or any individual verification and related to the election authority itself.

II. GENERATION OF PSEUDONYM TO THE VOTER

Pseudonym PVi Є PV is a unique number generated for each voter. Voter can apply for his / her Pseudonym PVi as per the identity based on these registration list on the election day and that is applicable only for that particular election only (next election voter will generate an another pseudonym). PVi Є PV – is a list of pseudonym identity of the voter which are unlikable to the voter's registration identity. This would be helping the voter that voter's real registration identity is hide from the voting authorities and during the communication, in order to preserve the voter's privacy. Thus, the voter becomes anonymous while he / she are using the PVi during his communications with the voting authorities. The central election authority can easily check validity of any PVi by applying the common key Y which are require the three secrete Key of three different group. Thus the election authority also cannot open the identity of the voter without concerning of voter and other three groups.

The pseudonyms are generated by the equation as:

$$\mathbf{PVi = Yi\ CKi \bmod P}$$

$$\mathbf{(or\ Consider\ PVi = E\ CKi\ (Yi))}$$

Where

$$\mathbf{CKi = Q\ Xi\ Xa\ Xb\ Xc \bmod P; \ \ --}$$

$$\mathbf{= Y * Q\ Xi}$$

$$\mathbf{[\ Y = Q\ Xa\ Xb\ Xc \bmod P\ \ ]}$$

E CKi (Yi) -- is computed by encrypting Y (with suitable method) with secrete key CKi.

CONFERENCE PAPER
National Conference on Information and Communication Technology for Development
Organized by PRMITR, Amravati (MS) India
http://mitra.ac.in/forthcoming.html

Xi – is a secrete key of voter Vi and
Y – is a common key
(Y = Q Xa Xb Xc mod P)
i = 1, 2,……….. n.

This process is carry out for voter's authentication and authorization stage. In this scheme, election authority perform blind signature with PVi in order to authenticate the PVi and included in the PV-list of centre server CDB.

Thus voter can get its (Id, Xi, Yi, PVi, Bm) during election stage.

Where Xi Є X, Yi Є Y & PVi Є PV.

III. PRESERVE THE PRIVACY'S VOTER:

In the proposed protocol, in order to preserve the privacy of the voters the following steps are essentials:

a. Generates a unique pseudonym PVi for each voter Vi which is unlinkable to the Voter's registration and that preserves the privacy of voters.

This pseudonyms obtain by encryption of Yi by using the secrete key from equitation as follows:

CKi = Q Xi Xa Xb Xc mod P

By Compute Yi with PVi by suitable method as

PVi = Yi CKi log P;

b. This secrete keys are different for the different voters therefore it is impossible to obtain the secrete keys to each voter.

c. Here the secrete key VYi can be form by the agreements of four parties the voter secrete key Xi and three groups A, B and C secrete key Xa, Xb and Xc and also it impossible by method of discrete logarithm of modulo P to compute it.

d. The only election authority also cannot perform the operation of formation of pseudonyms to the voter because this can be form with the agreement of these four different parties.

e. The election pseudonyms are created to every voter before the election and those are unique and store in the central database CDB and publish in a bulletin board BB.

f. The pseudonyms PVi are valid for particular election only. when voter insert the election card and use the biometric Bm as the password then PVi temporally store in the voter's election card in that day only and readable only by voting terminals for the election day since for that terminals or voting centre use different code specification other than ASCII or universal code specification.

Compute the value of pseudonymous of the voter Vi as follows:

CKi = Q Xi Xa Xb Xc mod P

By compute PVi by suitable method as:

PVi = Yi CKi log P;

Consider the Xi and group A, group B and group C's secrete key

Xa = 1.1234;
Xb = 1.5234;
Xc = 1.4562;
Q = 4.0000
P = 1997;

Compute the value of common keys CKi of the voters Vi as follows:

Table I: Generation Of Common Key

V	Voter public key Y_i	Voter secrete key X_i	X = Xi*Xa*Xb*Xc	$Q1 = Q^X$	Common key CK_i
V1	11.63985497	2.23412	5.567708341	2249.54370731663	252.54370731663
V2	11.66982947	2.23646	5.5735424	2267.81116516937	270.81116516938
V3	11.69988117	2.23881	5.579376459	2286.22696422364	289.22696422364
V4	11.73001025	2.24115	5.585210518	2304.79230908665	307.79230908665
V5	11.76021692	2.24349	5.591044577	2323.50841414771	326.50841414771
V6	11.79050137	2.24583	5.596878636	2342.37650365755	345.37650365755
V7	11.82086382	2.24817	5.602712695	2361.39781180846	364.39781180846
V8	11.85130445	2.25051	5.608546754	2380.57358281503	383.57358281503
V9	11.88182347	2.25285	5.614380813	2399.90507099550	402.90507099550
V10	11.91242109	2.25519	5.620214872	2419.39354085381	422.39354085381
V11	11.94309749	2.25753	5.626048931	2439.04026716236	442.04026716236
V12	11.9738529	2.25987	5.631882989	2458.84653504532	461.84653504532
V13	12.0046875	2.26222	5.637717048	2478.81364006276	481.81364006276
V14	12.03560151	2.26456	5.643551107	2498.94288829535	501.94288829535
V15	12.06659513	2.26690	5.649385166	2519.23559642985	522.23559642985

V16	12.09766856	2.26924	5.655219225	2539.69309184513	542.69309184513
V17	12.12882201	2.27158	5.661053284	2560.31671269913	563.31671269913
V18	12.16005568	2.27392	5.666887343	2581.10780801628	584.10780801628
V19	12.19136979	2.27626	5.672721402	2602.06773777580	605.06773777580
V20	12.22276453	2.27860	5.678555461	2623.19787300065	626.19787300065
V21	12.25424012	2.28094	5.68438952	2644.49959584719	647.49959584720
V22	12.28579677	2.283284	5.690223579	2665.97429969563	668.97429969563
V23	12.31743468	2.285625	5.696057638	2687.62338924112	690.62338924112
V24	12.34915406	2.287966	5.701891697	2709.44828058568	712.44828058568
V25	12.38095513	2.290307	5.707725755	2731.45040133080	734.45040133080
V26	12.41283808	2.292648	5.713559814	2753.63119067082	756.63119067082
V27	12.44480315	2.294989	5.719393873	2775.99209948712	778.99209948712
V28	12.47685052	2.29733	5.725227932	2798.53459044295	801.53459044295
V29	12.50898043	2.299671	5.731061991	2821.26013807917	824.26013807917
V30	12.54119307	2.302012	5.73689605	2844.17022891064	847.17022891064
V31	12.57348867	2.304353	5.742730109	2867.26636152352	870.26636152352
V32	12.60586743	2.306694	5.748564168	2890.55004667326	893.55004667326
V33	12.63832957	2.309035	5.754398227	2914.02280738340	917.02280738340
V34	12.67087531	2.311376	5.760232286	2937.68617904525	940.68617904525
V35	12.70350486	2.313717	5.766066345	2961.54170951828	964.54170951828
V36	12.73621844	2.316058	5.771900404	2985.59095923138	988.59095923138
V37	12.76901625	2.318399	5.777734463	3009.83550128491	1012.83550128491
V38	12.80189853	2.32074	5.783568521	3034.27692155364	1037.27692155364
V39	12.83486549	2.323081	5.78940258	3058.91681879047	1061.91681879047
V40	12.86791734	2.325422	5.795236639	3083.75680473099	1086.75680473099
V41	12.9010543	2.327763	5.801070698	3108.79850419889	1111.79850419889
V42	12.9342766	2.330104	5.806904757	3134.04355521232	1137.04355521232
V43	12.96758445	2.332445	5.812738816	3159.49360909093	1162.49360909093
V44	13.00097807	2.334786	5.818572875	3185.15033056399	1188.15033056399
V45	13.03445769	2.337127	5.824406934	3211.01539787919	1214.01539787919
V46	13.06802352	2.339468	5.830240993	3237.09050291249	1240.09050291249
V47	13.10167579	2.341809	5.836075052	3263.37735127873	1266.37735127873
V48	13.13541472	2.34415	5.841909111	3289.87766244326	1292.87766244326
V49	13.16924054	2.346491	5.84774317	3316.59316983434	1319.59316983434
V50	13.20315346	2.348832	5.853577229	3343.52562095658	1346.52562095658
V51	13.23715371	2.351173	5.859411288	3370.67677750524	1373.67677750524

From the common key, the pseudonymous of the voters are created as follows:

PVi = Yi CKi mod P;

Table II: Pseudonymous of voters Vi are generated

Voter Vi	**Voter public key Yi**	**Common key CKi**	**Y = POW(Yi, CKi)**	**Pseudonymous of voters PVi = MOD(Y, CKi)**
V1	11.63985497	11.63985496526	2.555495398205E+12	11.63985496526
V2	11.66982947	11.66982947063	2.834398201210E+12	11.66982947063
V3	11.69988117	11.69988116520	3.144821759275E+12	11.69988116520
V4	11.73001025	11.73001024773	3.490447342337E+12	11.73001024773
V5	11.76021692	11.76021691751	3.875399694635E+12	11.76021691751
V6	11.79050137	11.79050137435	4.304302054426E+12	11.79050137435
V7	11.82086382	11.82086381854	4.782338193677E+12	11.82086381854
V8	11.85130445	11.85130445094	5.315322397711E+12	11.85130445094
V9	11.88182347	11.88182347287	5.909778428473E+12	11.88182347287
V10	11.91242109	11.91242108621	6.573028655800E+12	11.91242108621
V11	11.94309749	11.94309749335	7.313294701311E+12	11.94309749335
V12	11.9738529	11.97385289718	8.139811121878E+12	11.97385289718
V13	12.0046875	12.00468750115	9.062953867415E+12	12.00468750115
V14	12.03560151	12.03560150919	1.009438548440E+13	12.03560150919
V15	12.06659513	12.06659512580	1.124721930636E+13	12.06659512580
V16	12.09766856	12.09766855597	1.253620518023E+13	12.09766855597
V17	12.12882201	12.12882200524	1.397793962822E+13	12.12882200524
V18	12.16005568	12.16005567968	1.559110374546E+13	12.16005567968
V19	12.19136979	12.19136978586	1.739673259051E+13	12.19136978586
V20	12.22276453	12.22276453092	1.941852034773E+13	12.22276453092
V21	12.25424012	12.25424012252	2.168316613666E+13	12.25424012252
V22	12.28579677	12.28579676885	2.422076602461E+13	12.28579676885
V23	12.31743468	12.31743467864	2.706525757741E+13	12.31743467864
V24	12.34915406	12.34915406115	3.025492417359E+13	12.34915406115
V25	12.38095513	12.38095512619	3.383296732584E+13	12.38095512619
V26	12.41283808	12.41283808410	3.784815641910E+13	12.41283808410
V27	12.44480315	12.44480314578	4.235556660932E+13	12.44480314578
V28	12.47685052	12.47685052266	4.741741715458E+13	12.47685052266
V29	12.50898043	12.50898042670	5.310402420151E+13	12.50898042670
V30	12.54119307	12.54119307043	5.949488405576E+13	12.54119307043
V31	12.57348867	12.57348866691	6.667990526626E+13	12.57348866691
V32	12.60586743	12.60586742977	7.476081049077E+13	12.60586742977
V33	12.63832957	12.63832957318	8.385273213763E+13	12.63832957318
V34	12.67087531	12.67087531184	9.408602925294E+13	12.67087531184
V35	12.70350486	12.70350486103	1.056083571120E+14	12.70350486103
V36	12.73621844	12.73621843658	1.185870255560E+14	12.73621843658
V37	12.76901625	12.76901625486	1.332116873814E+14	12.76901625486
V38	12.80189853	12.80189853282	1.496974041414E+14	12.80189853282
V39	12.83486549	12.83486548796	1.682881436815E+14	12.83486548796
V40	12.86791734	12.86791733832	1.892607717376E+14	12.86791733832
V41	12.9010543	12.90105430254	2.129296091421E+14	12.90105430254
V42	12.9342766	12.93427659979	2.396516367946E+14	12.93427659979
V43	12.96758445	12.96758444981	2.698324427722E+14	12.96758444981
V44	13.00097807	13.00097807292	3.039330200383E+14	13.00097807292

V45	13.03445769	13.03445769001	3.424775394374E+14	13.03445769001
V46	13.06802352	13.06802352251	3.860622413772E+14	13.06802352251
V47	13.10167579	13.10167579245	4.353656111910E+14	13.10167579245
V48	13.13541472	13.13541472242	4.911600280850E+14	13.13541472242
V49	13.16924054	13.16924053558	5.543251063376E+14	13.16924053558
V50	13.20315346	13.20315345566	6.258629806358E+14	13.20315345566
V51	13.23715371	13.23715370699	7.069158258133E+14	13.23715370699

IV. SECURITY AND PRIVACY ANALYSIS OF THE ALGORITHMS

Electronic voting system is nothing but to maintain the huge digital database any one change, modify, copy, the data very easily from the public communication channel. Therefore, it will need to satisfy the basic requirement of voting system in order to maintain the security and privacy. Here discuss the main achievements of the propose algorithms and most of the requirements like legal, political, social and economical feasibility are satisfied.

a. Voter's privacy can easily be satisfied due to the issue of PVi to registered vote by providing the blind signature of election authority & there is not any link between PVi & registered ID.

b. Voter had already been registered & provided a private key Xi & public Yi uniquely with bio-matrix information to avoid multiple or duplicate registration of voter by linking with central database CDB. Hence, this can prove the voter's eligibility & identity and the uniqueness of the voter.

c. Voter and any political party can check the every vote with individually & in a universally. Therefore, it can satisfy the accuracy of EVS and faith to the system.

d. There is no any chance of vote buying / selling. Since privacy of votes, are maintain and only last casting of vote will be counted in a final tally and voting is possible in a voting centre and election period only.

e. Any fraud or modification of single vote or tapping of information can be deleting. Hence system is Robust & verifiable at any intermediate time.

While carefully observing the security needs of the system, at all levels in the voting process, the design of the system also caters for a number of important functional and nonfunctional requirements, which are sufficiently addressed in every facet of system design that entail hardware, software, and the underlying encryption and network infrastructure.

V. CONCLUSION

Due to the importance of the election process, it is now necessary to develop a system for voters electronically in a secure manner by using electronic voting system (e-election), this leaded to finding a way to do the guarantee to fulfill the requirements. Electronic voting system can developed in such a way to achieve requirements of election process with a relative high degree of security and accuracy against the preserving the privacy of the voters.

VI. RERENCES

[1]. Antonyan, T.; Davtyan, S.; Kentros, S.; Kiayias, A.; Michel, L.; Nicolaou, N.;Russell, A.; Shvartsman, A.A.; "State-Wide Elections, Optical Scan Voting Systems, and the Pursuit of Integrity " , Information Forensics and Security, IEEE Journals , Transactions on Volume: 4 , Issue: 4 , Part: 1, Page(s): 597 – 610.

[2]. Fauzia, N.; Dey, T.; Bhuiyan, I.; Rahman,M.S.;"An efficient implementation of electronic election system ", IEEE, 10th international conference on Computer and information technology, 2007. ICCIT- 2007, Page(s): 1 – 6.

[3]. Weldemariam, K.; Villafiorita, A.; Mattioli, A.; "Experiments and data analysis of electronic voting system", Fourth IEEE International Conference on Risks and Security of Internet and Systems (CRiSIS), 2009, Page(s): 105 – 112.

[4]. Seo-Il Kang and Im-Yeong Lee, "A Study on the Electronic Voting System using blind Signature for Anonymity", Hybrid Information Technology, 2006. ICHIT'06. Vol 2. International Conference on Volume 2, Nov. 2006 Page(s): 660 – 663.

[5]. Athanassios Kosmopoulos,"Aspects of regulatory and legal implementations on e-Voting",s. wang et al.(Eds):ER workshop 2004. LNCS 3289, pp. 589-600, 2004.

[6]. J W Bryans, B Littlewood, P Y A Ryan, L Strigini," E-voting: Dependability Requirements and Design for Dependability", Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on 20-22 April 2006 Page(s):8 pp.

[7]. Kiayias, A.; Korman, M.; Walluck, D.; "An Internet Voting System Supporting User Privacy", Computer Security Applications Conference, 2006. ACSAC '06. 22nd Annual Dec. 2006 Page(s):165 – 174.

[8]. Anthony Watson, Vincent Cordonnier , "Information Technology Improves Most of the Democratic Voting Processes " Professor, Edith Cowan University - Perth, Australia , Professor, UniversitC des Sciences et Technologies de Lille – France , 1529-4188/01, 2001 IEEE ,page 388-393.

[9]. Jared Karro and Jie Wang "Towards a Practical, Secure, and Very Large Scale Online Election", Computer Security Applications Conference, 1999. (ACSAC '99) Proceedings. 15th Annual 6-10 Dec. 1999 Page(s):161 – 169.

[10]. Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach, "Analysis of an Electronic Voting System",

Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on 9-12 May 2004 Page(s):27 – 40.

[11]. Lorrie Faith Cranor, Ron K. Cytron, "Sensus: A Security-Conscious Electronic Polling System for the Internet", Public Policy Research AT&T Labs Research, 1060-3425197, 1997 IEEE, pp 561-570.