UNIVERSIDAD DE LA FRONTERA
FACULTAD DE INGENIERÍA, CIENCIAS Y ADMINISTRACIÓN
DEPARTAMENTO DE INGENIERÍA DE SISTEMAS

"Titulo de la tesis"

JAVIER IGNACIO FUENTES MUÑOZ
2016

UNIVERSIDAD DE LA FRONTERA
FACULTAD DE INGENIERÍA, CIENCIAS Y ADMINISTRACIÓN
DEPARTAMENTO DE INGENIERÍA DE SISTEMAS

"Titulo de la tesis"

TRABAJO PARA OPTAR AL TÍTULO DE INGENIERO INFORMÁTICO

PROFESOR GUÍA: SAMUEL EDUARDO SEPÚLVEDA CUEVAS

JAVIER IGNACIO FUENTES MUÑOZ
2016

Titulo de la tesis

JAVIER IGNACIO FUENTES MUÑOZ

COMISIÓN EXAMINADORA

MG. SAMUEL EDUARDO SEPÚLVEDA CUEVAS
Profesor Guía

Dr. CARLOS FERNANDO CARES GALLARDO
Profesor Examinador 1

Mg. JORGE ALBERTO HOCHSTETTER DIEZ
Profesor Examinador 2

Nota trabajo escrito	:
Nota examen	:
Nota final	:

A mi abuela Joaquina

RESUMEN

Resumen here

Índice general

Índice de figuras

Índice de tablas

CAPÍTULO 1
INTRODUCCIÓN

CAPÍTULO 2
ANTECEDENTES GENERALES

CAPÍTULO 3
DESCRIPCIÓN DE ACTIVIDADES REALIZADAS

CAPÍTULO 4
RESULTADOS Y DISCUSIÓN

CAPÍTULO 5
CONCLUSIONES

Conclusiones

Referencias

ANEXO A
TABLA DE PUNTAJES

Tabla A.1: Simbología

Sigla	**Significado**	**Sigla**	**Significado**
NR	Non-Repudation	FT	Fault Tolerance
RU	Resource Utilisation	EU	Ease of Use
CON	Confidentiality	INT	Integrity
AUT	Authentification	COM	Security Compliance
IMPL	Implementación	MOD	Modelo
PROP	Propuesta	SOL	Solución

Tabla A.2: Tabla de puntajes de mapeo sistemático

ID	**NR**	**FT**	**RU**	**EU**	**CON**	**INT**	**AUT**	**COM**	**IMPL**	**MOD**	**PROP**	**SOL**
1		X										X
2					X					X		
3			X							X		
4			X									X
5					X					X		
6			X								X	
7					X					X		
8							X			X		
9				X							X	
10			X		X					X		
11		X								X		
12			X			X				X		
13					X					X		
14	X									X		
15					X						X	
16			X		X					X		
17			X						X			
18			X							X		
19			X							X		
20					X	X				X		
21			X	X					X			
22					X					X		
23			X							X		
24					X						X	
25					X						X	
26					X						X	
27					X				X			

Tabla A.2: Tabla de puntajes de mapeo sistemático

ID	NR	FT	RU	EU	CON	INT	AUT	COM	IMPL	MOD	PROP	SOL
28			X							X		
29					X							X
30			X				X			X		
31	X									X		
32					X						X	
33						X				X		
34			X									X
35				X					X			
36		X								X		
37	X										X	
38					X					X		
39					X					X		
40					X					X		
41					X						X	
42			X			X				X		
43			X							X		
44							X			X		
45					X					X		
46			X							X		
47			X							X		
48					X						X	
49								X			X	
50			X							X		
51						X				X		
52		X								X		
53			X							X		
54				X		X				X		
55								X		X		
56						X		X				X
57	X		X								X	
58						X					X	
59		X							X			
60						X			X			

ANEXO B
LISTA DE PUBLICACIONES

ID	Título	Año	Publicacion	Autores
1	An anonymous and efficient e-voting scheme	2013	e-Commerce in Developing Countries: With Focus on e-Security (ECDC), 2013 7th Intenational Conference on	Ghavamipoor, H.; Shahpasand, M.
2	A generic approach to prevent board flooding attacks in coercion-resistant electronic voting schemes	2013	Computers & Security	Rolf Haenni and Reto E. Koenig
3	A multiple ballots election scheme using anonymous distribution	2010	TENCON 2010 - 2010 IEEE Region 10 Conference	Okamoto, M.
4	A New and Secure Electronic Voting Protocol Based on Bilinear Pairings	2009	CONIELECOMP '09: Proceedings of the 2009 International Conference on Electrical, Communications, and Computers	Gina Gallegos G., Roberto Gomez C., Moises Salinas R., Gonzalo I. Duchen S.
5	A new approach towards coercion-resistant remote e-voting in linear time	2011	FC'11: Proceedings of the 15th international conference on Financial Cryptography and Data Security	Oliver Spycher, Reto Koenig, Rolf Haenni, Michael Schläpfer

ID	Título	Año	Publicacion	Autores
6	A New Coercion-Resistant and Receipt-Free Electronic Voting System with Verifiability and Secrecy	2012	ICEE '12: Proceedings of the 2012 3rd International Conference on E-Business and E-Government - Volume 02 , Volume 02	Ying-Ching Chiu, Wen-Bing Horng
7	A New E-Voting Scheme Based on Improved DLP	2010	e-Business and Information System Security (EBISS), 2010 2nd International Conference on	Yang Huaiqing; Wang Shaobin
8	A New Electronic Voting Protocol Using a New Blind Signature Scheme	2010	ICFN '10: Proceedings of the 2010 Second International Conference on Future Networks	Behnam Kharchineh, Mehdi Ettelaee
9	A novel protocol to allow revocation of votes a hybrid voting system	2010	Information Security for South Africa (ISSA), 2010	Spycher, O.; Haenni, R.
10	A Practical Approach to a Reliable Electronic Election	2009	ICCSA '09: Proceedings of the International Conference on Computational Science and Its Applications: Part II	Kwangwoo Lee, Yunho Lee, Seungjoo Kim, Dongho Won
11	A secure and anonymous voter-controlled election scheme	2009	Journal of Network and Computer Applications , Volume 32 Issue 3	Thomas E. Carroll, Daniel Grosu

ID	Título	Año	Publicacion	Autores
12	A secure and available electronic voting service for a large-scale distributed system	2003	Future Generation Computer Systems	Gianluca Dini
13	A Secure and Efficient Voter-Controlled Anonymous Election Scheme	2005	ITCC '05: Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume I - Volume 01 , Volume 01	Thomas E. Carroll, Daniel Grosu
14	A secure and private clarke tax voting protocol without trusted authorities	2004	ICEC '04: Proceedings of the 6th international conference on Electronic commerce	Changjie Wang, Ho-fung Leung
15	A Secure E-Voting System Based on List Signature for Large Scale	2006	Communications and Networking in China, 2006. ChinaCom '06. First International Conference on	Guo-Hua Cui; Li Su; Mu-xiang Yang; Yang Wang
16	A Secure Multi Authority Electronic Voting Protocol Based on Blind Signature	2010	ACE '10: Proceedings of the 2010 International Conference on Advances in Computer Engineering	Sujata Mohanty, Banshidhar Majhi
17	A write-in electronic voting scheme based on ring signature	2007	Communications, Circuits and Systems, 2007. ICCCAS 2007. International Conference on	Yong Yang; Zhiguang Qin; Hu Xiong; Yang Zhao; Tian Lan

ID	Título	Año	Publicacion	Autores
18	A zero knowledge proof for subset selection from a family of sets with applications to multiparty/multicandidate electronic elections	2005	TCGOV'05: Proceedings of the 2005 international conference on E-Government: towards Electronic Democracy	Tassos Dimitriou, Dimitris Foteinakis
19	An anonymous voting mechanism based on the key exchange protocol	2006	Computers & Security	Chin-Chen Chang and Jung-San Lee
20	An Application Architecture for E-Voting	2009	Computational Intelligence and Software Engineering, 2009. CiSE 2009. International Conference on	Pfundstein, N.; Chao, J.; Kresman, R.
21	An efficient implementation of electronic election system	2007	Computer and information technology, 2007. iccit 2007. 10th international conference on	Fauzia, N.; Dey, T.; Bhuiyan, I.; Rahman, M.S.
22	An efficient multi-receipt mechanism for uncoercible anonymous electronic voting	2008	Mathematical and Computer Modelling: An International Journal , Volume 48 Issue 9-10	Chun-I Fan, Wei-Zhe Sun
23	An efficient shuffling based eVoting scheme	2011	Journal of Systems and Software , Volume 84 Issue 6	Kun Peng

ID	Título	Año	Publicacion	Autores
24	An electronic voting scheme based on undeniable blind signature scheme	2003	Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on	Sung-Hyun Yun; Sung-Jin Lee
25	An Identity-Based Restricted Deniable Authentication Protocol	2009	Parallel and Distributed Processing with Applications, 2009 IEEE International Symposium on	Chengyu Fan; Shijie Zhou; Fagen Li
26	An improved electronic voting scheme without a trusted random number generator	2011	Inscrypt'11: Proceedings of the 7th international conference on Information Security and Cryptology	Yining Liu, Peiyong Sun, Jihong Yan, Yajun Li, Jianyu Cao
27	An Internet Voting System Supporting User Privacy	2006	ACSAC '06: Proceedings of the 22nd Annual Computer Security Applications Conference on Annual Computer Security Applications Conference	Aggelos Kiayias, Michael Korman, David Walluck
28	Anonymity and independence in multiparty protocols	2006	Anonymity and independence in multiparty protocols	Alejandro Hevia / Daniele Micciancio
29	Bare-handed electronic voting with pre-processing	2007	EVT'07: Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology	Ben Riva, Amnon Ta-Shma

ID	Título	Año	Publicacion	Autores
30	Casting Ballots over Internet Connection Against Bribery and Coercion	2012	The Computer Journal , Volume 55 Issue 10	Yu-Fang Chung, Zhen-Yu Wu
31	Caveat Coercitor: Coercion-Evidence in Electronic Voting	2013	SP '13: Proceedings of the 2013 IEEE Symposium on Security and Privacy	Gurchetan S. Grewal, Mark D. Ryan, Sergiu Bursuc, Peter Y. A. Ryan
32	Coercion-Resistant Cryptographic Voting: Implementing Free and Secret Electronic Elections	2008	Coercion-Resistant Cryptographic Voting: Implementing Free and Secret Electronic Elections	Stefan G. Weber
33	Cryptographic protocols: revocable anonymity and e-voting	2009	Cryptographic protocols: revocable anonymity and e-voting	Bekir Arslan / Richard E. Newman
34	Defeating malicious servers in a blind signatures based voting system	2006	FC'06: Proceedings of the 10th international conference on Financial Cryptography and Data Security	Sébastien Canard, Matthieu Gaud, Jacques Traoré
35	Dispute resolution in accessible voting systems: the design and use of audiotegrity	2013	Vote-ID'13: Proceedings of the 4th international conference on E-Voting and Identity	Tyler Kaczmarek, John Wittrock, Richard Carback, Alex Florescu, Jan Rubio, Noel Runyan, Poorvi L. Vora, Filip Zagórski

ID	Título	Año	Publicacion	Autores
36	E-voting: Dependability Requirements and Design for Dependability	2006	ARES '06: Proceedings of the First International Conference on Availability, Reliability and Security	J W. Bryans, B Littlewood, P Y. A. Ryan, L Strigini
37	Electronic Elections: Trust Through Engineering	2009	RE-VOTE '09: Proceedings of the 2009 First International Workshop on Requirements Engineering for e-Voting Systems	Carsten Schürmann
38	Electronic jury voting protocols	2004	Theoretical Computer Science , Volume 321 Issue 1	Alejandro Hevia, Marcos Kiwi
39	Formalization of Receipt-Freeness in the Context of Electronic Voting	2011	Availability, Reliability and Security (ARES), 2011 Sixth International Conference on	Braunlich, K.; Grimm, R.
40	Full privacy preserving electronic voting scheme	2012	The Journal of China Universities of Posts and Telecommunications	Lei PANG and Mao-hua SUN and Shou-shan LUO and Bai WANG and Yang XIN

ID	Título	Año	Publicacion	Autores
41	How to Publicly Verifiably Expand a Member without Changing Old Shares in a Secret Sharing Scheme	2008	PAISI, PACCF and SOCO '08: Proceedings of the IEEE ISI 2008 PAISI, PACCF, and SOCO international workshops on Intelligence and Security Informatics	Jia Yu, Fanyu Kong, Rong Hao, Xuliang Li
42	Mix-Network with stronger security	2005	PET'05: Proceedings of the 5th international conference on Privacy Enhancing Technologies	Jan Camenisch, Anton Mityagin
43	New receipt-free voting scheme using double-trapdoor commitment	2011	Information Sciences: an International Journal , Volume 181 Issue 8	Xiaofeng Chen, Qianhong Wu, Fangguo Zhang, Haibo Tian, Baodian Wei, Byoungcheon Lee, Hyunrok Lee, Kwangjo Kim
44	New voter verification scheme using pre-encrypted ballots	2009	Computer Communications , Volume 32 Issue 7-10	Victor Morales-Rocha, Miguel Soriano, Jordi Puiggalí
45	On the security of condorcet electronic voting scheme	2005	CIS'05: Proceedings of the 2005 international conference on Computational Intelligence and Security - Volume Part II , Volume Part II	Yoon Cheol Lee, Hiroshi Doi

ID	Título	Año	Publicacion	Autores
46	Performability of a Secure Electronic Voting Algorithm	2005	Electronic Notes in Theoretical Computer Science (ENTCS) , Volume 128 Issue 4	Nigel Thomas
47	Practical mobile electronic election	2011	System Integration (SII), 2011 IEEE/SICE International Symposium on	Xun Yi; Okamoto, E.
48	Provably secure randomized blind signature scheme based on bilinear pairing	2010	Computers & Mathematics with Applications , Volume 60 Issue 2	Chun-I Fan, Wei-Zhe Sun, Vincent Shi-Ming Huang
49	Remote Electronic Voting with Revocable Anonymity	2009	ICISS '09: Proceedings of the 5th International Conference on Information Systems Security	Matt Smart, Eike Ritter
50	Research and implementation of highly-efficient anonymous electronic voting scheme based on ring signature and blind signature	2012	World Automation Congress (WAC), 2012	Yan Yaojun; Hu Haiyan
51	Secure Internet Voting Based on Paper Ballots	2008	ICISS '08: Proceedings of the 4th International Conference on Information Systems Security	Łukasz Nitschke

ID	Título	Año	Publicacion	Autores
52	SELES: an e-voting system for medium scale online election	2005	Computer Science, 2005. ENC 2005. Sixth Mexican International Conference on	Garcia-Zamora, C.; Rodriguez-Henriquez, F.; Ortiz-Arroyo, D.
53	Towards trustworthy e-voting using paper receipts	2010	Computer Standards & Interfaces , Volume 32 Issue 5-6	Yunho Lee, Sangjoon Park, Masahiro Mambo, Seungjoo Kim, Dongho Won
54	Trivitas: voters directly verifying votes	2011	VoteID'11: Proceedings of the Third international conference on E-Voting and Identity	Sergiu Bursuc, Gurchetan S. Grewal, Mark D. Ryan
55	True trustworthy elections: remote electronic voting using trusted computing	2011	ATC'11: Proceedings of the 8th international conference on Autonomic and trusted computing	Matt Smart, Eike Ritter
56	Two Variations to the mCESG Pollsterless E-Voting Scheme	2005	COMPSAC '05: Proceedings of the 29th Annual International Computer Software and Applications Conference - Volume 01 , Volume 01	Tim Storer, Ishbel Duncan
57	Unconditionally secure electronic voting	2010	Towards Trustworthy Elections	Akira Otsuka, Hideki Imai

ID	Título	Año	Publicacion	Autores
58	Verifiable and Privacy Preserving Electronic Voting with Untrusted Machines	2013	TRUSTCOM '13: Proceedings of the 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications	Manzur Murshed, Tishna Sabrina, Anindya Iqbal, Mortuza Ali
59	Votebox: a tamper-evident, verifiable voting machine	2009	Votebox: a tamper-evident, verifiable voting machine	Daniel Robert Sandler / Dan S. Wallach
60	Who Counts Your Votes?	2005	EEE '05: Proceedings of the 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'05) on e-Technology, e-Commerce and e-Service	Halina Kaminski, Lila Kari, Mark Perry