SKEMA PEMILU ELEKTRONIK (*E-VOTING*) BERBASIS ENKRIPSI HOMOMORFIS PADA SISTEM KRIPTOGRAFI *THRESHOLD ELGAMAL*

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh

IRVAN HILMY FAUZI

12610037

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2019

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal :
Lamp :

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Irvan Hilmy Fauzi
NIM : 12610037
Judul Skripsi : Skema Pemilu Elektronik Berbasis Enkripsi Homomorfis Pada Sistem Kriptografi *Threshold* ElGamal.

sudah dapat diajukan kembali kepada Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Matematika

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 1 Februari 2019
Pembimbing

M. Zaki Riyanto, M.Sc.
NIP. 198401132015031001

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-621/Un.02/DST/PP.00.9/02/2019

Tugas Akhir dengan judul : SKEMA PEMILU ELEKTRONIK (E-VOTING) BERBASIS ENKRIPSI HOMOMORFIS PADA SISTEM KRIPTOGRAFI THRESHOLD ELGAMAL

yang dipersiapkan dan disusun oleh:

Nama : IRVAN HILMY FAUZI
Nomor Induk Mahasiswa : 12610037
Telah diujikan pada : Jumat, 15 Februari 2019
Nilai ujian Tugas Akhir : A

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Muhamad Zaki Riyanto, S.Si., M.Sc.
NIP. 19840113 201503 1 001

Penguji I

Dr. Muhammad Wakhid Musthofa, S.Si., M.Si.
NIP. 19800402 200501 1 003

Penguji II

Pipit Pratiwi Rahayu, S.Si., M.Sc.
NIP. 19861208 201503 2 006

Yogyakarta, 15 Februari 2019
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
D E K A N

Dr. Murtono, M.Si.
NIP. 19691212 200003 1 001

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : Irvan Hilmy Fauzi

NIM : 12610037

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Dengan ini menyatakan bahwa isi skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi dan sesungguhnya skripsi ini merupakan hasil pekerjaan penulis sendiri sepanjang pengetahuan penulis, bukan duplikasi atau saduran dari karya orang lain kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 11 Februari 2019

Yang Menyatakan

Irvan Hilmy Fauzi

HALAMAN PERSEMBAHAN

Karya sederhana ini penulis persembahkan

untuk Ayah dan Ibu tercinta

MOTTO

When you walk through a storm

Hold your head up high

And don't be afraid of the dark

At the end of a storm

There's a golden sky

And the sweet silver song of a lark

Walk on through the wind

Walk on through the rain

Though your dreams be tossed and blown

Walk on, walk on

With hope in your heart

And you'll never walk alone

You'll never walk alone !

PRAKATA

Assalamu'alaikum Wr. Wb. Puji syukur kepada Allah SWT yang telah memberikan rahmat, hidayah, dan karunia-Nya sehingga penulis dapat menyelesaikan tugas akhir skripsi yang berjudul "*Skema Pemilu Elektronik (E-Voting) Berbasis Enkripsi Homomorfis Pada Sistem Kriptografi Threshold ElGamal* ". Penyusunan skripsi ini ditujukan untuk memenuhi sebagai syarat kelulusan guna memperoleh gelar Sarjana Matematika Progam Studi Matematika di Fakultas Sains dan Teknologi Universitas Negeri Islam Sunan Kalijaga Yogyakarta.

Shalawat serta salam semoga tetap tercurah kepada Rasulullah Muhammad *Sholallahu 'alaihi wassalam*, yang memberikan teladan bagi kita, sehingga kita dapat mengenal apa itu iman, islam dan ihsan. Semoga kita mendapatkan syafaatnya pada hari kiamat nanti. Aamiin Ya Rabb Al'Alamiin.

Penulisan skripsi ini tidak lepas dari dukungan, motivasi, kerjasama maupun bimbingan dari berbagai pihak baik secara langsung maupun tidak langsung. Oleh karena itu, penulis mengucapkan terimakasih kepada:

1. Prof. Drs. Yudian Wahyudi, MA, Ph.D. selaku Rektor UIN Sunan Kalijaga Yogyakarta.

2. Dr. Murtono, M.Si., selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.

3. Dr. Muhammad Wakhid Musthofa, M.Si., selaku Ketua Progam Studi Matematika UIN Sunan Kalijaga Yogyakarta.

4. Bpk. Muhamad Zaki Riyanto M.Sc., selaku pembimbing yang telah mencurahkan kesabaran dan ketekunannya dalam meluangkan waktu, tenaga, serta pikiran guna memberikan bimbingan dan arahan yang sangat berarti dalam penyusunan dan penyelesaian skripsi.

5. Bpk. Muchammad Abrori, M. Kom., selaku Dosen Penasihat Akademik mahasiswa Program Studi Matematika angkatan 2012 atas segala pengarahan dan semangat yang selalu bapak berikan selama penulis belajar di Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.

6. Bapak/Ibu dosen yang dengan ikhlas telah memberikan ilmu pengetahuan dan pengalaman yang berharga kepada penulis, sehingga ilmu yang telah didapat memudahkan dalam penyusunan skripsi ini.

7. Kedua orang tua penulis Bapak Ali dan Ibu Jarwasih, Mbak Helmy Fauzi Awaliyah, Mbak Irviani Helma Tama, Ghulam Faqih Maulana, Halim Pandu Latifah, Ghilman Mudhofar Ali dan Halmy Izzatus Sholikhah yang tidak pernah lelah memanjatkan doa, memberikan motivasi, dukungan moril maupun materiil selama ini.

8. Seseorang yang selalu ada untuk memberikan motivasi, kritik, saran serta doa dari awal penulisan skripsi ini.

Penulis hanya bisa mendoakan semoga bantuan, arahan, bimbingan, dan doa yang baik tersebut mendapatkan pahala yang setimpal dari Allah *Azza Wa Jalla*, Aamiin. *Wassalamu'alaikum Wr. Wb.*

Yogyakarta, 20 Februari 2019

Penulis

DAFTAR ISI

INTISARI

SKEMA PEMILU ELEKTRONIK (*E-VOTING*) BERBASIS ENKRIPSI HOMOMORFIS PADA SISTEM KRIPTOGRAFI *THRESHOLD ELGAMAL*

Oleh

IRVAN HILMY FAUZI

12610037

Pemilu elektronik (*e-voting*) merupakan salah satu aplikasi dari kriptografi. Pemilu elektronik dipercaya lebih memudahkan bagi pemilih, efisien, transparan, murah, dan memberikan hasil rekapitulasi suara yang lebih cepat dibandingkan dengan pemilu konvensional. Kelebihan-kelebihan tersebut dapat meningkatkan partisipasi pemilih yang cenderung terus menurun dalam pemilu-pemilu sebelumnya. Dengan kata lain, pemilu elektronik dapat meningkatkan kepercayaan masyarakat terhadap penyelenggara pemilu. Di lain pihak, penggunaan teknologi elektronik memungkinkan penyerang untuk mengganggu pelaksanaan pemilu dengan cara yang lebih mudah, meskipun hanya terdapat sedikit celah keamanan pada sistem. Oleh karena itu suatu skema pemilu elektronik harus didesain untuk memenuhi standar keamanan seperti pada pemilu konvensional dan juga keamanan dari kemungkinan serangan siber. Pada skripsi ini dipresentasikan suatu skema pemilu elektronik berbasis enkripsi homomorfis pada sistem kriptografi *threshold* ElGamal. Skema ini menjamin terpenuhinya persyaratan dasar dari suatu sistem pemilu yaitu *eligibility, unreusability, privacy, verifiability, receipt-freeness* dan *uncoercibility*.

Kata Kunci : Pemilu elektronik, Kriptografi, Enkripsi homomorfis.

ABSTRACT

ELECTRONIC VOTING SCHEME BASED ON HOMOMORPHIC ENCRYPTION OF THRESHOLD ELGAMAL CRYPTOSYSTEM.

By

IRVAN HILMY FAUZI

12610037

Electronic voting (e-voting) is an application of cryptography. It is believed to be more convenient for voters, efficient, transparent, cheaper, and gives faster result than paper-based election. These advantages could increase the voter turnout which has been declined in the previous elections. In other word e-voting could increase public trust to the election conductor. However, the use of electronic technology allows adversaries to intrude the voting process in an easier way. Thus, an e-voting system should be designed to be as secure as the conventional paper-based and robust against the possibility of cyber attacks. In this final task we present an e-voting scheme based on homomorphic encryption of *threshold* ElGamal cryptosystem. This scheme guarantees eligibility, unreusability, privacy, verifiability, receipt-freeness and uncoercibility as a basic requirements of e-voting system.

Key words : E-voting, cryptography, homomorphic encryption.

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Indonesia sebagai negara demokrasi menyelenggarakan pemilihan umum (pemilu) setiap lima tahun sekali. Pemilu diadakan untuk memilih Presiden dan Wakil Presiden, anggota Legislatif, dan Kepala Daerah. Luasnya wilayah Indonesia yang terdiri dari banyak provinsi dan kabupaten/kota serta banyaknya warga negara yang tercatat sebagai pemilih seringkali memunculkan masalah dalam penyelenggaraan pemilu. Permasalahan tersebut diantaranya adalah anggaran biaya penyelenggaraan pemilu yang tinggi dan lamanya waktu yang dibutuhkan untuk menyelesaikan rekapitulasi suara (Simbolon,2018). Selain itu terjadi kencenderungan peningkatan angka golput dari tahun ke tahun (Nurhasim, 2014). Jika ditambah dengan banyaknya dugaan kecurangan yang terjadi pada pemilu, maka hal ini akan menurunkan tingkat kepercayaan masyarakat terhadap penyelenggara pemilu.

Pemilu elektronik (*e-voting*) dianggap oleh banyak pihak sebagai solusi untuk mengatasi permasalahan tersebut. Menurut $Smartmatic$ [1], penerapan pemilu elektronik dapat membuat penyelenggaraan pemilu menjadi lebih transparan, aman, akurat dan dapat diaudit (*auditable*). Pemilu elektronik juga dapat mempercepat proses pemilu dan dapat meningkatkan partisipasi masyarakat, yang kemudian dapat meningkatkan tingkat kepercayaan masyarakat. Akan tetapi penggunaan teknologi juga membuat pemilu menjadi rentan terhadap serangan siber (*cyber attack*). Oleh karena itu suatu skema pemilu harus didesain tidak hanya untuk memenuhi

[1] Perusahaan developer sistem *e-voting*

persyaratan seperti pada pemilu konvensional, tetapi juga aman terhadap kemungkinan adanya serangan siber.

Berdasarkan permasalahan yang telah disebutkan, pada skripsi ini akan dibahas mengenai "*Skema Pemilu Elektronik Berbasis Enkripsi Homomorfis Pada Sistem Kriptografi Threshold ElGamal*". Skema pemilu elektronik ini akan dianalisa apakah memenuhi persyaratan dan memenuhi asas pemilu di Indonesia.

1.2. Rumusan Masalah

Dari latar belakang diatas, kemudian dirumuskan latar belakang masalah sebagai berikut:

1. Bagaimana konsep enkripsi homomorfis pada sistem kriptografi *threshold* ElGamal.
2. Bagaimana penerapan enkripsi homomorfis pada sistem kriptografi *threshold* ElGamal dalam pemilu elektronik.
3. Apakah skema pemilu elektronik berbasis enkripsi homomorfis pada sistem kriptografi *threshold* ElGamal dapat diterapkan pada pemilu di Indonesia.

1.3. Batasan Masalah

Agar pembahasan menjadi terfokus pada konsep matematika, maka penelitian ini tidak membahas masalah sistem informasi dan politik seperti bagaimana teknik pemilih melakukan pemungutan suara, bagaimana kandidat (peserta pemilu) lolos verifikasi, dan lain-lain.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Untuk mengetahui bagaimana konsep enkripsi homomorfis pada sistem kriptografi *threshold* ElGamal.
2. Untuk mengetahui bagaimana penerapan enkripsi homomorfis pada sistem kriptografi *threshold* ElGamal dalam pemilu elektronik.
3. Untuk mengetahui apakah skema pemilu elektronik berbasis enkripsi homomorfis pada sistem kriptografi *threshold* ElGamal dapat diterapkan pada pemilu di Indonesia

1.5. Manfaat Penelitian

1. Memberikan wawasan mengenai skema pemilu elektronik yang dapat diterapkan pada pemilu di Indonesia.
2. Memberikan pengetahuan bagi mahasiswa tentang konsep-konsep dalam kriptografi.
3. Memberikan pengetahuan bagi mahasiswa tentang penerapan konsep-konsep kriptografi pada kehidupan nyata.

1.6. Tinjauan Pustaka

Dalam penelitian ini, penulis mengacu pada literatur - literatur yang tercantum di dalam daftar pustaka, yang dilakukan dengan mempelajari beberapa buku, jurnal, karya ilmiah dan penelitian sebelumnya yang berkaitan dengan penelitian ini. Penulisan ini merujuk pada jurnal *"A homomorphic encryption-based secure electronic voting scheme"* yang ditulis oleh Andrea Huszti (2011) sebagai rujukan utama. Dalam penulisan ini akan dibahas tema yang sama akan tetapi dengan lebih memperdalam pembahasan dalam konsep matematika. Selain itu juga dilakukan beberapa penyesuaian agar sesuai dengan pelaksanaan pemilu di Indonesia.

1.7. Sistematika Penulisan

Sistematika penulisan dari penelitian ini adalah

BAB I PENDAHULUAN

Berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, tinjauan pustaka, dan sistematika penulisan.

BAB II DASAR TEORI

Berisi tentang beberapa pembahasan definisi dan teorema yang digunakan sebagai landasan pada bab-bab selanjutnya, seperti : pemilu, pemilu elektronik (*e-voting*), bilangan bulat, dasar struktur aljabar, persamaan kongruen dan *residue class modulo*, bilangan bulat modulo dan kriptografi.

BAB III PROTOKOL KRIPTOGRAFI

Berisi pembahasan tentang *cryptographic primitives* yang digunakan dalam skema pemilu elektronik, seperti : skema enkripsi (sistem kriptografi), enkripsi homomorfis, tanda tangan digital, *blind signatures* dan *zero knowledge proof*.

BAB IV SKEMA PEMILU ELEKTRONIK

Berisi pembahasan tentang skema pemilu elektronik yang digunakan meliputi deskripsi umum, tahapan pelaksanaan pemilu, alur pemungutan suara, analisis kemananan (pemenuhan syarat) dan analisis kelayakan (pemenuhan asas pemilu Indonesia), serta simulasi pemilu elektronik dalam skala kecil.

BAB V PENUTUP

Berisi kesimpulan dari penelitian yang dilakukan serta saran untuk peneliti selanjutnya.

BAB V

PENUTUP

5.1. Kesimpulan

Skema pemilu elektronik berbasis enkripsi homomorfis pada sistem kriptografi *threshold* ElGamal dalam skripsi ini memenuhi persyaratan yang diberikan yaitu: *eligibility, privacy, unreusability, fairness, robustness, individual* dan *universal verifiability, receipt-freeness* dan *uncoercibility*. Selain itu skema ini juga aman dari *randomization attack* dan *forced abstention attack.* Sehingga dapat dikatakan bahwa skema pemilu ini aman untuk digunakan dalam suatu pelaksanaan pemilu. Dilihat dari analisis kelayakan, skema pemilu ini juga memenuhi asas pemilu Indonesia, yaitu : langsung, umum, bebas, rahasia, jujur dan adil. Oleh karena itu secara teori, skema pemilu ini dapat digunakan dalam pelaksanaan pemilu di Indonesia, khususnya pada pemilu yang bersifat *1 out of n voting*.

5.2. Saran

Penulis berharap bahwa penelitian tentang skema pemilu berbasis enkripsi homomorfis ini dapat dilanjutkan terutama dalam pembuatan sistem informasi pemilu yang lebih efektif dan efisien bagi pengguna (pemilih) dalam melakukan pemungutan suara.

DAFTAR PUSTAKA

Anton, H., 2000, *Elementary Linear Algebra*, Eight Edition, John Wiley and Sons, Inc., New York.

Ardiyanti, H. 2016. *Uji Coba E-Verifikasi dan Masa Depan Pemilu Elektronik 2019*. Majalah Info Singkat, Vol VIII, No. 15/I/P3DI/Agustus/2016.

Buchmann, J.A. 2004. *Introduction to Cryptography, 2nd Edition*. New York: Springer.

Chaum, D., Jakobsson, M., Rivest, R.L., Ryan, P.Y.A., Benaloh, J., Kutylowski, M., Adida, B. 2010. Towards Trustworthy Elections: New Directions in Electronic Voting. Berlin: Springer.

Delfs, H., Knebl, H. 2007. *Introduction to Cryptography: Principles and Applications, 2nd Edition*. Berlin: Springer.

Diffie, W., Hellman, M.E. 1976. *New Directions In Cryptography*. Stanford: National Science Foundation.

Fine, B., Rosenberger, G. 2007. *Number Theory: An Introduction via The Distribution of Primes*. Boston: Birkhauser.

Fraleigh, John B., 2000, *A First Course in Abstract Algebra*, Sixth Edition, Addison-Wesley Publishing Company, Inc., USA

Gallian, J.A. 2017. *Contemporary Abstract Algebra, 9th Edition*. Boston: Cengage Learning.

Golle, P., Jakobsson, M. 2003. *Reusable Anonymous Return Channels*. Hal 94-100, ACM Press.

Goluch, S. 2010. *The Development of Homomorphic Cryptography from RSA to Gentry's Privacy Homomorphism*. Tesis. Wina: Vienna University of Technology.

Hoffstein, J., Pipher, J., Silverman, J.H. 2008. *An Introduction to Mathematical Cryptography*. New York: Springer.

Horster, P., Petersen, H., Michels, M. 1994. *Meta-ElGamal Signature Schemes*. Germany: University of Technology Chemnitz-Zwickau.

Huszti, A. 2011.*A Homomorphic Encryption-based Secure Electronic Voting Scheme*. Vol 79/3-4. Debrecen: University of Debrecen.

Lidl, R., Niederreiter, H. 1986. *Introduction to Finite Fields and Their Applications*. Cambridge: Cambridge University Press.

Malik, D.S., Mordeson, J.N., Sen, M.K. 2007. *Introduction to Abstract Algebra*. Amerika Serikat: Department of Mathematics.

Menezes, A.J., van Oorschot, P.C., Vanstone, S.A. 1996. *Handbook of Applied Cryptography*, CRC Press, Inc. USA.

Mollin, R.A. 2007. *Discrete Mathematics and Its Applications Series Editor Kenneth H. Rosen: An Introduction to Cryptography, 2nd Edition*. Boca Raton: Chapman and Hall/CRC.

Paar, C., Pelzl, J. 2010. *Understanding Cryptography: A Textbook for Students and Practitioners*. Berlin: Springer.

Rjaskova, Z. 2002. *Electronic Voting Scheme*. Disertasi. Bratislava: Comenius University.

Rosen, K.H. 2012. *Discrete Mathematics and Its Applications, 7th Edition*. New York: McGraw Hill.

Schneier, B. 1996. *Applied Cryptography: Protocols, Algorithms, and Source Code in C (Cloth), 2nd Edition*. New York: John Wiley & Sons.

Schoenmakers, B. 2018. *Lecture Notes Cryptographic Protocols*. Eindhoven: Technical University of Eindhoven.

Simbolon, M. 2018. *Measuring The Urgency and Preparedness of Indonesian Law In Conducting Electronic Based General Elections*. Majalah Actio, Issue No 7/ April 2018. Jakarta Selatan: Anggraeni and Partners.

Stallings, W. 2011. *Cryptography and Network Security: Principles and Practice, 5th Edition*. New York: Prentice Hall.

Stein, W. 2017. *Elementary Number Theory: Primes, Congruences, and Secrets*. Amerika Serikat: University of Washington.

Stinson, D.R. 2006. *Discrete Mathematics and Its Applications Series Editor Kenneth H. Rosen: Cryptography Theory and Practice, 3rd Edition*. Boca Raton: Chapman and Hall/CRC.

Yi X., Paulet R., Bertino E., 2014. *Homomorphic Encryption and Applications*. SpringerBriefs, USA.

...