Terbit pada laman web jurnal : **http://ojsamik.amikmitragama.ac.id**

JURNAL JARINGAN SISTEM INFORMASI ROBOTIK (JSR)
Vol. 7 No. 1 TAHUN 2023 E - ISSN : 2579-373X

STUDI PERBANDINGAN SKEMA ENKRIPSI HOMOMORFIK DALAM VOTING SYSTEM E-SUARA

Supriyadi[*1], Ronal[2], Yuliana[3]
[1,2]Magister Sistem Informasi, STMIK LIKMI, Bandung, Indonesia
[3]Magister Sistem Informasi, STMIK "AMIKBANDUNG", Bandung, Indonesia
Email: [1*] spridy@gmail.com,, [2]ronal.nambela@gmail.com [3]yuliana@stmik-amikbandung.ac.id
(* : coressponding author)

Abstrak
Sistem pemungutan suara elektronik yang disediakan melalui internet dapat meningkatkan peserta pemilu karena menghilangkan ketidaknyamanan untuk pergi ke tempat pemungutan suara yang ditentukan. *Homomorphic encryption* adalah salah satu algoritma yang dapat di terapkan pada system voting e-suara, karna memungkinkan untuk melakukan perhitungan pada data terenkripsinya tanpa terlebih dahulu mendekripsinya. Pada penelitian ini dilakukan *analysis* algoritma *homomorphic encryption* pada sistem voting e-suara dari penelitian sebelumnya. Dengan menggunakan algoritma *homomorphic encryption* tidak dilakukannya dekripsi data rekapitulasi hasil pemilihan. Sifat homomorfik dari algoritma *homomorphic encryption* dapat memberikan hasil yang akurat antara hasil perhitungan menggunakan ciphertext yang serupa dengan hasil yang diinginkan yang dihitung secara manual setelah didekripsi. Sehingga properti dapat digunakan untuk mengantisipasi kecurangan oleh pihak luar untuk memanipulasi data yang disimpan atau pihak luar yang mencoba mengganggu proses penghitungan. Hasil *analysis* algoritma *homomorphic encryption* dalam voting system e-suara, menggunakan skema Pailier cryptosystem, Okamoto-Uchiyama cryptosystem dan Schmidt-Takagi versi 2 dapat di manfaatkan untuk membangun sistme e-voting dan dapat meningkatkan keamanan data suara pada system e-voting.

Kata Kunci: Enkripsi Homomorfik, Pailier cryptoystem, Schmidt-Takagi, *Okamoto-Uchiyama cryptosystem* System Voting

Abstract
Electronic voting systems provided via the internet can increase electoral participation because it eliminates the inconvenience of going to a designated polling place. Homomorphic encryption is one of the algorithms that can be applied to e-voice voting systems, because it makes it possible to perform calculations on encrypted data without first decrypting it. In this study, an analysis of the homomorphic encryption algorithm was carried out on the e-voice voting system from previous studies. By using the homomorphic encryption algorithm, data decryption of the election result recapitulation is not performed. The homomorphic nature of the homomorphic encryption algorithm can provide accurate results between the results of calculations using ciphertext that are similar to the desired results which are calculated manually after being decrypted. So that property can be used to anticipate fraud by outsiders to manipulate stored data or outsiders who try to interfere with the calculation process. The results of the analysis of the homomorphic encryption algorithm in the e-voting voting system, using the Pailier cryptosystem scheme, Okamoto-Uchiyama cryptosystem and Schmidt-Takagi version 2 can be used to build an e-voting system and can improve the security of voting data in the e-voting system.

Keywords: *Homomorphic Encryption, Pailier Cryptosystem, Schmidt-Takagi, Okamoto-Uchiyama cryptosystem, E-Voting*

1. PENDAHULUAN

Sistem pemungutan suara elektronik yang disediakan melalui Internet dapat meningkatkan peserta pemilu karena menghilangkan ketidaknyamanan untuk pergi ke tempat pemungutan suara yang ditentukan. Voting system merupakan salah satu sistem yang dapat membantu untuk membuat proses pemilu (pemilihan umum) menjadi lebih efisien. Ada banyak masalah dalam sistem pemungutan suara elektronik, seperti

kesalahan sistem, keamanan jaringan, keamanan data, dll. Untuk mengatasi masalah tersebut, kriptografi perlu diterapkan[1]

Kriptografi merupakan salah satu teknik untuk menjamin kerahasiaan informasi yang dikomunikasikan. Teknik kriptografi dapat dimanfaatkan untuk mendukung keamann pada suatu informsi. Aspek keamanan informasi yang dapat didukung oleh kriptografi adalah kerahasiaan *(confidentiality)*, keutuhan data *(integrity)*, otentikasi penyedia/penerima informasi *(authentication)* serta penyangkalan (nonrepudiation).[2]

Enkripsi homomorfik adalah salah satu algoritma dalam teknik kriptografi yang dapat membantu menyembunyikan isi surat suara dengan menghitung penghitungan tanpa mendekripsi salah satu surat suara [3]. Penelitian terkait Enkripsi homomorfik dilakukan oleh Konstantin G dkk, penelitian tersebut berfokus pada pemanfaatan Enkripsi homomorfik dalam pengamanan suatu data dan dengan menggunakan enkripsi keamanan menyimpan data meningkat namun waktu yang dibutuhkan dalam menyimpan data bertambah.[4]

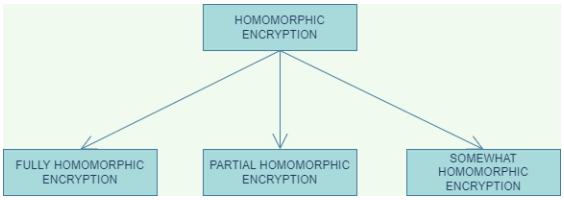
Algoritma homomorphic encryption dapat di implementasikan dalam berbagai bidang untuk tujuan mengamankan data. Salah satu implementasi algoritma HE adalah pada bidang voting system. Ada beberapa skema yang diusulkan yang mengadopsi enkripsi homomorfik dalam voting system. Salah satu penelitian tentang Homomorphic Encryption dalam bidang pemilihan suara adalah Shubhangi S pada tahun 2013 [5]

2. METODOLOGI PENELITIAN

Pada penelitian ini dilakukan perbandingan antara algoritma homomorphic encryption pada sistem voting. Dengan membandingkan algoritma Homomorphic Encryption pada penelitian sebelumnya tentang konsep dan kinerja pada sistem voting. Berikut ini akan menjelaskan konsep serta ukuran penyelesaian setiap algoritma pada sistem voting.

2.1. Enkripsi Homomorfik

Homomorphic Encryption adalah bentuk enkripsi yang memungkinkan untuk melakukan perhitungan pada data terenkripsinya tanpa terlebih dahulu mendekripsinya. Perhitungan yang dihasilkan dari perhitungan data terenkripsi dibiarkan dalam bentuk terenkripsi, dan ketika hasil terenkripsi tersebut didekripsi, akan menghasilkan keluaran yang identik dengan yang dihasilkan seandainya operasi dilakukan pada data plaintextnya.



Gambar 2.1 Jenis enkripsi homomorphic

Ada beberapa jenis enkripsi yang dapat melakukan operasi pada data terenkripsi dengan tingkatan kelas yang berbeda seperti pada gambar 2.1. Beberapa jenis enkripsi homomorphic yang umum adalah enkripsi *Somewhat homomorphic encryption* (SWHE) adalah kriptosistem homomorfik yang memiliki kemampuan untuk melakukan homomorfisme aditif dan perkalian, namun, dengan jumlah operasi yang terbatas. *Partially homomorphic encryption* (PHE) adalah homomorfisme yang bersifat additif, atau homomorfisme yang bersifat multiplicative yang memiliki kemampuan komputasi pada jumlah yang tidak terbatas. *Fully Homomorphic Encryption* (FHE) bersifat additif dan multiplicative yang memiliki kemampuan komputasi pada jumlah yang tidak terbatas. Secara matematis sebuah cryptosystem yang bersifat homomorfisme jika memungkinkan dilakukannya perhitungan pada data yang terenkripsi. Homomorphic bersifat aditif jika:

$$\varepsilon\,(x+y) = \varepsilon(x) \otimes \varepsilon(y)$$

di mana ε adalah notasi dari fungsi enkripsi, $\otimes$ adalah notasi dari operasi pada ciphertext dan x dan y adalah pesan plaintext. Homomorphic bersifat multiplicative jika

$$\varepsilon\,(x \cdot y) = \varepsilon(x) \otimes \varepsilon(y)$$

di mana ε adalah notasi dari fungsi enkripsi, $\otimes$ adalah notasi dari operasi pada ciphertext dan x dan y adalah pesan plaintext.[6]

2.2. *Pailier cryptosystem*

Kriptosistem Paillier adalah skema dari partial homomorphic encryption yang bersifat homomorfiknya dengan enkripsi non-deterministiknya. Karena fungsi enkripsi secara aditif homomorfik, homomorphic properties pailer dapat dijelaksan sebagai berikut:

Penjumlahan plainteks yang homomorfik, Operasi aritmethic dari dua ciphertext akan didekripsi menjadi jumlah dari plaintext yang sesuai.

$$D(E(m_1, r_1)(m_1, r_1) mod\ n^2) = m_1 m_2\ mod\ n$$

Operasi aritmethic dari ciphertext dengan peningkatan plaintext g akan didekripsi menjadi jumlah plaintext yang sesuai.

$$D\ (E(m_1, r_1) \cdot g^{m_2}\ mod\ n^2) = m_1 m_2\ mod\ n$$

Perkalian plainteks yang homomorfik, Sebuah ciphertext yang dipangkatkan dengan plaintext akan dideskripsi menjadi operasi dari dua plaintext,

$$D\ (E(m_1, r_1)^{m_2}\ mod\ n^2) = m_1 m_2\ mod\ n$$

$$D\ (E(m_2, r_2)^{m_1}\ mod\ n^2) = m_1 m_2\ mod\ n$$

Secara umum, ciphertext yang dinaikkan ke konstanta k akan didekripsi menjadi operasi dari plaintext dan konstanta,

$$D\ (E(m_1, r_1)^{k}\ mod\ n^2) = k m_1\ mod\ n$$

Namun, enkripsi Paillier dari dua pesan, tidak dapat menghitung enkripsi produk dari pesan-pesan tersebut tanpa mengetahui kunci pribadi.[7]

Algorithm Pailier Cryptosystem
Key generation

1. Choose two large prime numbers *p* and *q*
2. Compute $n = pq$ and $\lambda = lcm\ (p-1, q-1)$
3. select random integer g where $g \in \mathbb{Z}^*_{n^2}$
4. Ensure n divides the order of g
   The public (encryption) key is
   The private (decryption) key is

Encryption

1. Let m be a message to be encrypted where $0 \leq m < n$
2. Select random r where $0 < r < n$
3. Compute ciphertext as: $c = g^m \cdot r^n\ mod\ n^2$

Decryption

1. Let c be the ciphertext to decrypt, where $c \in \mathbb{Z}^*_{n^2}$
2. Compute the plaintext message as: $m = L\left(c^{\lambda}\ mod\ n^2\right) \cdot \mu\ mod\ n$

2.3. *Okamoto-Uchiyama cryptosystem*

Algoritma Okamoto-Uchiyama cryptosystem Dikembangkan oleh T.Okamoto dan S.Uchiyama pada tahun 1998, algoritma berumur 15 tahun ini mengambil beberapa prinsip yang sangat mirip dengan algoritma kriptografi kunci publik lainnya, yakni algoritma ElGamal. Algoritma Okamoto-Uchiyama menyandarkan kekuatannya pada sulitnya melakukan faktorisasi dan operasi logaritma diskrit pada bilangan prima dengan digit yang sangat besar.[8]

Algorithm Okamoto-Uchiyama cryptosystem
Key generation

1. Choose two large prime numbers *p* and *q*
2. Compute $n = p^2 q$
3. Select random integer g where $g \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$, $g^p \neq 1\ mod\ n$
4. Compute $h = g^p mod\ n$
   The public (encryption) key is (n, g, h)
   The private (decryption) key is (p, q)

Encryption

1. Compute $C = g^m h^r\ mod\ n$

Decryption

1. Compute $m = \frac{L(C^{p-1}\ mod\ p^2)}{L(g^{p-1}\ mod\ p^2)}\ mod\ n$

2.4. *Algoritme Schmidt-Takagi versi 2*

Pada tahun 2008, Takato Hirano, Koichiro Wada, dan Keisuke Tanaka mengajukan variasi baru dari algoritme enkripsi Schmidt-Takagi. Terdapat tiga proses utama dalam algoritma Schmidt-Takagi versi 2 ini yaitu, key generation, encryption, dan decryption.[9]

Algoritme Schmidt-Takagi versi 2 cryptosystem
Key generation

1. Choose two large prime numbers *p* and *q*
2. Compute $n = p^2 q$
3. Compute $d = n^{-s}\ (mod\ (p-1)(q-1))$
4. Select random integer l where $l \in \mathbb{Z}$
   The public (encryption) key is (n, l, s)
   The private (decryption) key is (p, q, d)

Encryption

1. Compute $E(m, r) = r^{(n^s)(1+mn)}\ mod\ n^{(s+1)}$

Decryption

1. Compute:
   $D\ (c) = L_{n^t}(c(r^{(n^s)})^{-1}\ mod\ n^{(s+1)}$

3. HASIL DAN PEMBAHASAN

Beberapa penelitian sebelumnya tentang pemanfaatan algoritma Homomorphic Encryption dalam sistem voting, dimana hasil penelitian menyatakan bahwa Dengan algoritma HE, dapat memastikan kerahasiaan data dan memanfaatkan sifat homomorfik dari algoritma untuk menghitung suara yang diproses oleh system. Muhtar hartopo dkk [10] menjamin keamanan sistem yang diusulkan dan menunjukkan bahwa aplikasi e-voting yang dibangun memiliki kualitas keamanan berupa aspek kriptografi dan kesesuaian dengan asas-asas pemilihan dengan nilai masing-masing 5 dan 6.

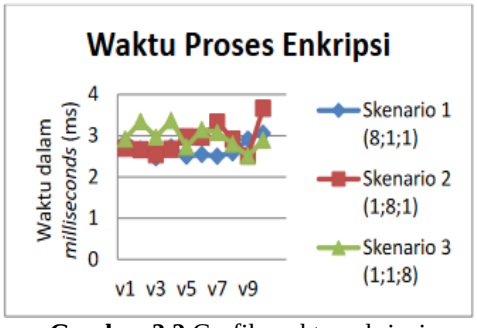
Core Area	Maturity Level										
	0	1	2	3	4	5	6	7	8	9	10
Software - Compliance with Election Principles		A				B					
Software - Data integrity			A			B					
Software - Cryptography			A				B			C	
Software - Transparency				A				B			
Software - Protection of Software				A					B		C

Gambar 3.1 hasil EVSSO

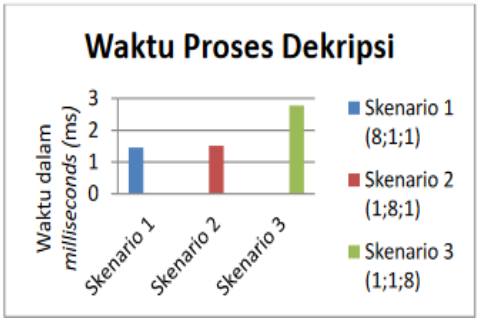
Penelitian Muhtar hartopo dkk [10] menggunakan matriks Electronic Voting System Security Optimization. Matriks ini berisi core area yaitu aspek keamanan yang diuji dan maturity level yang berarti posisi pada tiap level keamanan. Evaluasi dilakukan berdasarkan kriteria-kriteria yang telah ditentukan. Terdapat tiga level yaitu level A, B dan C. Secara umum core area pada matriks EVSSO terbagi atas tiga yaitu hardware, software dan human factor. Pada pengujian Muhtar hartopo dkk hanya mengambil core area software telihat pada gambar 3.1.

Bersasarkan penelitian Muhtar hartopo dkk hasil Enkripsi homomorfik parsial yang bersifat additive dapat diterapkan pada sistem pemilihan elektronik (e-voting). Selain itu menurut Muhtar hartopo dkk enkripsi homomorfik memungkinkan tidak dilakukannya dekripsi data terlebih dahulu ketika melakukan rekapitulasi hasil pemilihan. Aplikasi yang dibangun telah menyediakan fitur keamanan yang baik dari sisi kesesuaian dengan asas-asas pemilihan dan dari sisi kriptografi.

Ivan faturahman [9] dengan menggunakan algoritme homomorphic property yang terdapat pada algoritme Schmidt-Takagi versi 2, kemungkinan adanya kecurangan yang dilakukan oleh pihak administrator melalui known-plaintext attack sangatlah minim. Administrator tidak mampu memperoleh data tentang ciphertext dan plaintext dikarenakan adanya data tally. [9]



Gambar 3.2 Grafik waktu enkripsi



Gambar 3.3 Grafik waktu deskripsi

Pada penelitian Ivan faturahman [9] Kinerja algoritme Schmidt-Takagi versi 2 pada sistem e-voting dalam sisi tallying data dapat dilakukan dengan baik (sesuai kebutuhan sistem), dapat dilihat pada gambar 3.2 waktu yang di butukan untuk mengenkripsi hasil pemilihan dari scenario yang di usulkan dan pada gambar 3.3 adalah waktu yang di butukan untuk mendekripsi hasil pemilihan dari scenario yang di usulkan pada penelitian Ivan faturahman [9]

Algoritme mampu melakukan dekripsi pada data tally yang terbentuk dari hasil perkalian sepuluh ciphertext yang dienkripsi menggunakan variabel r acak. Berkat homomorphic property yang terdapat pada algoritme Schmidt-Takagi versi 2, kemungkinan adanya kecurangan yang dilakukan oleh pihak administrator melalui known-plaintext attack sangatlah minim.

Rifki suwandi dkk,ini mengimplementasikan algoritma Okamoto Uchiyama sebagai solusi yang ditawarkan yang memanfaatkan kriptografi tentang keamanan sistem e-voting untuk memastikan keamanan dan kerahasiaan data pemungutan suara, serta pemanfaatan sifat homomorfik dari algoritma ini untuk melakukan penghitungan.Algoritma ini akan menyembunyikan data dengan mengenkripsi suara yang dipilih oleh pemilih dan sistem dapat melakukan perhitungan menggunakan data yang terencrypted tanpa perlu mendecrypt terlebih dahulu. Sifat homomorfik yang digunakan dalam penelitian Rifki suwandi dkk [1] terbukti memberikan hasil yang akurat antara hasil perhitungan menggunakan ciphertext yang serupa dengan hasil yang diinginkan yang dihitung secara manual setelah didekripsi. Jadi kita bisa menggunakan properti itu untuk mengantisipasi kecurangan oleh pihak luar untuk memanipulasi data yang disimpan atau mencoba mengganggu proses penghitungan.

Dalam penelitian Rifki suwandi dkk, dapat memastikan kerahasiaan data dan memanfaatkan sifat homomorfik dari algoritma untuk menghitung suara yang diproses oleh sistem. Hasil pengujian dan analisis menunjukkan bahwa data pemungutan

suara terenkripsi dengan baik dan memiliki keunikan nilai untuk setiap ciphertext. Hasil akhir yang dihitung menggunakan properti homomorfik mirip dengan hasil yang diinginkan setelah sedang didekripsi. Pada tahun 2018, rifki suwandi membandingkan penggunaan algoritma Paillier dan Okamoto-Uchiyama dalam E-Voting sebagai dua algoritma enkripsi homomorfik. Tujuan utamanya adalah untuk menghindari manipulasi dan pemalsuan data saat pemungutan suara. Hasilnya Algoritma Okamoto-Uchiyama memiliki ukuran ciphertext yang lebih kecil daripada algoritma Paillier tetapi memiliki pemrosesan penghitungan waktu yang lebih lama [5].

4. KESIMPULAN

Pada penelitian ini, kami melakukan *analysis algoritma homomorphic encryption* untuk *System e-voting* pada penelitian sebelumnya. Dari beberapa penelitian sebelumnya algoritma homomorphic enkripsi, Pailier cryptosystem, Okamoto-Uchiyama cryptosystem dan Schmidt-Takagi versi 2 dapat di manfaatkan untuk membangun voting system e-suara. Dan dapat ditunjukan dengan menggunakan algoritma homomorphic enkripsi dapat meningkatkan keamanan. Disarankan untuk melakukan Algoritma homomorphic dapat di kombinasikan metode lain untuk meningkatkan waktu proses enkripsi pada data yang besar dalam system e-voting.

5. DAFTAR PUSTAKA

[1] Asosiasi Pendidikan Tinggi Ilmu Komputer Indonesia, Institute of Electrical and Electronics Engineers. Indonesia Section, and Institute of Electrical and Electronics Engineers, *2016 International Conference on Informatics and Computing (ICIC).*

[2] E. Rahmawati Agustina, A. Kurniati, L. Sandi Negara, J. R. Harsono No, P. Minggu, and J. Selatan, "PEMANFAATAN KRIPTOGRAFI DALAM MEWUJUDKAN KEAMANAN INFORMASI PADA e-VOTING DI INDONESIA," *Seminar Nasional Informatika*, pp. 23–2009, 2009.

[3] G. Pötzelsberger and B. Eng, "KV Web Security: Applications of Homomorphic Encryption," 2013.

[4] A. El-Yahyaoui and M. Dafir, "Fully Homomorphic Encryption: State of Art and Comparison New cryptographic methods for big data and cloud computing View project," 2016, doi: 10.6084/M9.FIGSHARE.3362338.

[5] R. Suwandi, S. M. Nasution, and F. Azmi, "Secure E-voting system by utilizing homomorphic properties of the encryption algorithm," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 16, no. 2, pp. 862–867, Apr. 2018, doi: 10.12928/TELKOMNIKA.v16i2.8420.

[6] L. Morris, "Analysis of Partially and Fully Homomorphic Encryption," 2013.

[7] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 1999, vol. 1592, pp. 223–238. doi: 10.1007/3-540-48910-X_16.

[8] "Implementasi Algoritma Kriptografi Kunci Publik Okamoto- Uchiyama".

[9] I. Faturahman, A. Kusyanti, and R. A. Siregar, "Implementasi Algoritme Enkripsi Homomorphic Schmidt-Takagi Versi 2 pada Sistem E-Voting," 2020. [Online]. Available: http://j-ptiik.ub.ac.id

[10] M. Hartopo and I. Rinaldi Munir, "Pengembangan Aplikasi E-Voting Menggunakan Enkripsi Homomorfik."