ANALISIS DAN SIMULASI PENGIRIMAN DATA DENGAN METODE ENKRIPSI ELLIPTIC CURVE CRIPTOGRAPHY (ECC) PADA SISTEM TRANSIMISI ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING (OFDM)

ANALYSIS AND SIMULATION OF DATA TRANSMISSION WITH ELLIPTIC CURVE CRIPTOGRAPHY (ECC) ENCRYPTION METHOD IN ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING (OFDM) TRANSMISSION SYSTEM

Rheza Rivaldi H.[1], Dr. Ir. Rina Pudji Astuti, M.T. [2],Nur Andini S.T., M.T.[3]
Jurusan S1 Teknik Telekomunikasi Universitas Telkom 40287
rhezarivaldii@gmail.com [1], rina.pudjiastuti@gmail.com[2] , andini_dhine@yahoo.com[3]

ABSTRAK

Saat ini, kebutuhan akan keamanan informasi pada data menjadi semakin besar. Pada jaringan Wi-Fi, telah terdapat suatu metode enkripsi Wifi Protected Access 2 (WPA2), yang mengimplementasikan AES pada enkripsinya. Selain dari masalah keamanan, kendala yang banyak dihadapi pada sistem komunikasi mobile saat ini adalah bagaimana mengatasi propagasi yang bersifat multipath.

Pada tugas akhir ini ditawarkan penggunaan algoritma ECC untuk pengamanan data. Pada simulasi ini juga digunakan skema transmisi OFDM untuk mengatasi kanal yang bersifat frequency-selective fading. Parameter yang diuji adalah Bit Error Rate (BER), dan hasil ciphertext dan plaintext pada sisi pengirim dan penerima untuk nilai Eb/No berkisar antara 0-20 dB.

Simulasi performansi memberikan hasil correlation sebesar 0.018, nilai entropy sebesar 7.9877, sensitif terhadap perubahan kunci, dan membutuhkan waktu yang sangat lama untuk mencari nilai kunci menggunakan teknik Brute Force Attack. Data yang diterima setelah proses dekripsi memiliki 6 buah karakter yang berubah dari data asli pada nilai Eb/No 8 dB, dan memiliki 1 buah karakter yang berubah pada nilai Eb/No 20 dB. Nilai BER sistem yang memakai metode enkripsi ECC sedikit lebih besar dari sistem yang tidak memakai metode enkripsi ECC. Nilai BER sistem yang memakai modulator QPSK lebih kecil dari sistem yang memakai modulator 16-QAM.

Kata Kunci : ***kriptografi, ECC, OFDM***

ABSTRACT

Nowadays, the need of data security becomes even greater. In Wi-Fi network, there is an existing encryption method called Wifi Protected Access (WPA2), which implements AES in the encryption Another problem that occurs apart from security problems in mobile telecommunication system is resolving the *multipath fading* in propagation.

ECC encryption method is implemented in this research as an algorithm to increase data security. This research also implements *Orthogonal Frequency Division Multiplexing* (OFDM) in its simulation. The parameters used and compared in this research are *Bit Error Rate* (BER) and the result of decrypted data when being compared with the original data for the value of Eb/No from 0 dB to 20 dB.

Performance simulation shows that the ECC encryption gives correlation for a value of 0.018, entropy with value of 7.9877, sensitive with key changes, and need a lot of time to calculate the key using Brute Force Attack. Data received after decryption proses have 6 characters errors in total compared to original data in Eb/No with value of 8 dB, and have 1 character errors in total compared to original data in Eb/No with value of 20 dB. The system using ECC encryption method has higher BER results than system without ECC encryption method. The system using QPSK modulation scheme has lower BER than system using 16-QAM modulation scheme..

Keywords : cryptography, ECC, OFDM

I. PENDAHULUAN

Sistem komunikasi *mobile* telah mengalami perkembangan yang cukup pesat beberapa tahun terakhir ini, dengan mengintegrasikan beberapa teknologi jaringan *wireless* untuk mendukung bertambahnya fungsi dan layanan yang dapat digunakan oleh *user* dengan menggunakan *User Equipment* (UE)[1].

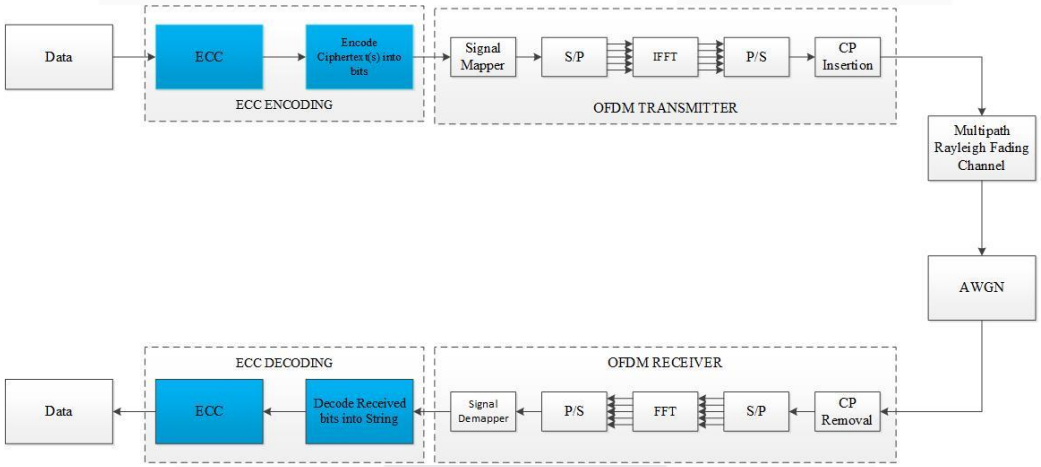
Seiring dengan berjalannya waktu, kebutuhan akan keamanan informasi pada data yang ditransmisikan menjadi semakin besar. Pada sistem komunikasi saat ini, contohnya Wi-Fi, terdapat suatu algoritma enkripsi yang bernama *Wifi Protected Access 2* (WPA), yang didalamnya menerapkan algoritma enkripsi AES untuk pengamanan data[10]. Kelemahan dari algoritma AES ini adalah dibutuhkannya kesamaan kunci yang digunakan antara pengirim dan penerima, sehingga proses pertukaran kunci harus melalui jaringan yang benar-benar aman.

Selain dari masalah keamanan, kendala yang banyak dihadapi pada sistem komunikasi *mobile* saat ini adalah bagaimana mengatasi propagasi yang bersifat *multipath*, sehingga menyebabkan terjadinya *multipath fading*. *Multipath fading* adalah suatu bentuk gangguan atau interferensi sinyal pada *Radio Frequency* (RF) yang timbul ketika sinyal memiliki lebih dari satu jalur dari *transmitter* ke *receiver*, yang disebabkan oleh pantulan sinyal terhadap objek-objek yang memisahkan keduanya[1]. Salah satu jenis *multipath fading* yang dibahas pada penelitian ini adalah *frequency-selective fading.*

Pada tugas akhir ini ditawarkan penggunaan algoritma *Elliptic Curve Cryptography* (ECC) sebagai algoritma untuk pengamanan informasi pada data. Metode ini diakui keunggulannya karena memiliki kualitas keamanan yang baik dan menghasilkan ukuran kunci yang relatif kecil. Algoritma ini dianggap lebih baik dari algoritma asimetrik lainnya, salah satunya RSA. Untuk tingkat keamanan yang sama, pada ECC dibutuhkan 160-bit kunci, sedangkan pada RSA dibutuhkan kunci sebesar 2048-bit[11]. Selain itu, pada simulasi tugas akhir ini akan digunakan skema transmisi *Orthogonal Frequency Division Multiplexing* (OFDM), untuk mengatasi efek *frequency-selective fading*, dengan dua tipe modulasi, yaitu *16-Quadrature Amplitude Modulation* (16-QAM) dan *Quadrature Phase Shift Keying* (QPSK), serta penambahan *Additive White Gaussian Noise* (AWGN) dan *Rayleigh Fading* pada kanal transmisi agar lingkungan transmisi pada simulasi menyerupai lingkungan transmisi sebenarnya.

II. PERANCANGAN SISTEM DAN PARAMETER SIMULASI

II.I. Diagram Alir Simulasi



Gambar 1 Blok Diagram Transmitter dan Receiver Sistem

Data pada awalnya akan dienkripsi terlebih dahulu menggunakan metode enkripsi ECC. Data kemudian masuk ke *signal mapper*. Di penelitian ini digunakan dua *signal mapper* yang nantinya akan diketahui pengaruhnya terhadap BER sistem, yaitu QPSK dan 16-QAM. Data kemudian diubah menjadi data paralel, dengan jumlah masing-masing blok data sebesar 64 bit, yang kemudian akan dilakukan proses *Inverse Fast Fourier Transform* (IFFT) untuk mengubah data dari domain frekuensi ke domain waktu. Disini frekuensi data dibuat orthogonal satu sama lain. Setelah proses IFFT berakhir, data diubah menjadi kumpul bit serial, dan ditambahkan Cyclic Prefix ditiap awalan data untuk mengatasi *Intersymbol Interference* (ISI) pada kanal fading nantinya. Data kemudian dikirim melewati kanal *frequency-selective fading* dan AWGN. Proses ini akan diulang pada *receiver* dengan fungsi masing-masing blok yang hampir sama.

II.II. Parameter Simulasi

Parameter yang akan digunakan pada simulasi ini mengikuti standart IEEE 802.11a untuk sistem OFDM[8].

Tabel 1 Parameter simulasi menggunakan skema OFDM Transceiver

PARAMETER	VALUE
FFT Size	64
Jumlah *Sub-Carrier*	52
FFT Sampling Frequency	20 MHz
Sub-Carrier Spacing	312.5 KHz
Durasi Simbol Data	3.2 µs
Durasi *Cyclic Prefix*	0.8 µs
Total Durasi Simbol	4 µs
Modulasi	QPSK dan 16-QAM
Kecepatan User (v)	30 km/jam
Delay Spread	500 ns

III. ANALISIS HASIL SIMULASI

III.I. Performansi Algoritma Enkripsi Terhadap Data Masukan

Tabel 2 Data Masukan Untuk Simulasi Performansi Algoritma

Data Masukan
Kriptografi (cryptography) berasal dari bahasa Yunani, yaitu kryptos dan graphein. Kryptos berarti rahasia atau menyembunyikan, dan graphein berarti sebuah ilmu. Kriptografi sendiri merupakan keahlian dan ilmu untuk menyembunyikan informasi dari kehadiran pihak ketiga. Kriptografi dapat juga diarti

Data masukan yang digunakan berjumlah 4394 karakter. Tabel 4.6 menunjukkan 300 karakter pertama pada masukan. Data kemudian akan dienkripsi dengan metode enkripsi ECC. Hasil enkripsi data ditunjukkan pada tabel 3.

Tabel 3 Data Hasil Enkripsi Index 1-300

Data Terenkripsi Index 1-300
FŸw>N4• ¡, Å<€ • ñò_uÎ2å½JBà—• 4xÍªÒªcÃÙnÂå‹ ˜ é{.ÆÍYëƒ C ƒ VIC¬¢}BMZ!u´mìôáÓXÏ?R• \t"Üñ¾€ ÆCóãZ\²§tÞønpQÝ¢• ³gD?B □ÇI½2G□©Ālðý^□,4o¦ º¹×åÖùýØÉË□‡gl‡]N□,ÚjùÒ“□¬˜J‘GµNHiÍ 0Úµ¢Ò'Ãúúåïå•‹Ã.-ëª*,ºI¾I³PMCL«£7Ýâó~N˜eC!ûÃRØæwmáŸ<\÷^ü Z3c¡øÊÆÒÍ]t,¸ÂƒÊQBã?'ß£¢2ÝI§³□,©liÙÿýðp,—^

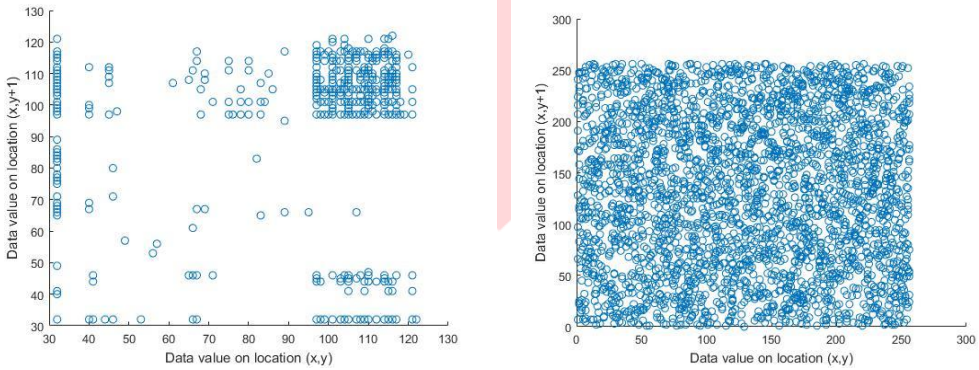
a. Perbandingan *Adjacent Correlation* Antara Data Awal dan Data Terenkripsi

Adjacent correlation merupakan parameter yang dihitung untuk melihat tingkat kemiripan data tersebut. *Adjacent correlation* mempunyai nilai antara 0 sampai dengan 1, dengan nilai 0 berarti tidak ada kemiripan sama sekali dan nilai 1 yang berarti tingkat kemiripan tinggi. Untuk sistem enkripsi yang baik, nilai *Adjacent correlation* harus mendekati 0. Perhitungan nilai *adjacent correlation* dilakukan menggunakan persamaan 1.

$$r_{x,y} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (1)$$

Tabel 4 Perbandingan Nilai Adjacent Correlation plaintext dan ciphertext

Adjacent Correlation	
Plaintext	Ciphertext
0.0115	0.0064



Gambar 2 Scatter Plot Adjacent Correlation Plaintext dan Ciphertext

Dari tabel 4, dapat dilihat bahwa nilai *adjacent correlation* untuk plaintext lebih besar nilainya dari ciphertext dengan nilai 0.0115, sedangkan untuk ciphertext hampir mencapai 0 dengan nilai 0.0064. Nilai *adjacent correlation* ini penting dalam melihat performansi algoritma ECC, karena ketika nilai data yang berdekatan hasil enkripsi mempunyai perbedaan yang jauh, itu berarti nilai data ini memiliki distribusi simbol yang merata, sehingga akan sulit bagi pihak ketiga untuk menganalisis nilai kunci yang digunakan ketika melihat dari pola ciphertext

b. Analisis Nilai Entropy pada Data

Nilai entropy merupakan nilai skalar yang menunjukkan tingkat keacakan nilai pada suatu data. Nilai entropy dihitung menggunakan persamaan 2.

$$r_{x,y} = -\sum_{i=0}^{n} P_i log_2 P_i \quad (2)$$

Metode enkripsi ECC dikatakan baik performanya ketika nilai entropy memiliki nilai yang semakin mendekati 8. Perbandingan nilai entropy antara plain *image* dan cipher *image* ditunjukkan pada tabel 5.

Tabel 5 Perbandingan Nilai Entropy Plain Image dan Cipher Image

Data	Nilai Entropy
Plaintext	4.3233
Chipertext	7.4186

Dari tabel 5, dapat dilihat bahwa nilai entropy chipertext atau pesan terenkripsi lebih mendekati nilai 8 dibanding plaintext. Hal ini menunjukkan bahwa proses enkripsi membuat nilai suatu data menjadi acak.

c. Analisis *Key Sensitivity* Pada Algoritma ECC

Algoritma yang aman harus benar-benar sensitif pada perubahan *secret key* yang dimiliki oleh penerima. Tabel 6 menunjukkan data dekripsi ketika nilai kuncinya benar, dan data dekripsi ketika kunci berubah nilainya sebesar 1 bit.

Tabel 6 Data Dekripsi dengan Kunci Yang Benar dan Data Dekripsi dengan Kunci yang Nilainya Berubah 1 Bit

Data Dekripsi dengan Kunci Benar	Data Dekripsi Dengan Perubahan Kunci
Kriptografi (cryptography) berasal dari bahasa Yunani, yaitu kryptos dan graphein. Kryptos berarti rahasia atau menyembunyikan, dan graphein berarti sebuah ilmu. Kriptografi sendiri merupakan keahlian dan ilmu untuk menyembunyikan informasi dari kehadiran pihak ketiga. Kriptografi dapat juga diarti	FŸw>N4• ¡, Å<€ • ñò_uÎ2å½JBà—• 4xÍªÒªcÃÙnÂå ‹ ˜ é{.ÆÍYëƒ Cƒ VIC¬¢}BMZ!u´mìôáÓXÏ?R• \t"Üñ ¾€ ÆCóãZ\²§tÞønpQÝ¢□³gD?B□ÇI½2G□©Ālðý^□ ,4o¦ º¹×åÖùýØÉË□‡gl‡]N□,ÚjùÒ“□¬˜J‘GµNHiÍ 0Úµ¿Ò'Ãúúåĭå•‹Ã.-ë*,ºI¾I³PMCL«£7Ýâó~N˜eC!ûÃ RØæwmáŸ<\÷^üZ3c¡øÊÆÒÍ]t,,ÂƒÊQBã?'ß£¿2ÝI§³ □,©liÙÿýðp,—^

Dari tabel 6 dapat dilihat bahwa perubahan satu bit pada nilai *secret key* membuat pesan hasil enkripsi tidak dapat didekripsi lagi. Dapat disimpulkan bahwa ketika ada pihak ketiga yang berusaha melakukan dekripsi terhadapt ciphertext, pihak ketiga tersebut harus memiliki *secret key* yang benar.

d. Perhitungan Lama Waktu Yang Dibutuhkan Untuk Mendapatkan Kunci dengan Metode *Brute Force Attack*

Waktu yang dibutuhkan untuk melakukan *Brute Force Attack* pada panjang kunci yang lain ditunjukkan pada tabel 7.

Tabel 7 Panjang Kunci dan Waktu yang Dibutuhkan Untuk Melakukan Brute Force Attack

Panjang Kunci	Waktu
32-bit	0.008 detik
64-bit	526 detik
128-bit	734,000 tahun
256-bit	2,880,000,000 tahun

Dari tabel 7 dapat dilihat bahwa dengan menaikkan nilai kunci yang digunakan, maka keamanan data semakin terjaga.

III.II. Performansi Metode Enkripsi ECC pada Sistem Transmisi OFDM

a. Hasil Metode Enkripsi ECC Terhadap Data Masukan

Data yang digunakan pada simulasi ini ditunjukkan pada tabel 8.

Tabel 8 Data Masukan Simulasi

Data Input
It is really not unusual for teens to experience the blue or depression. This can be caused by so many things, one of them is how they are being treated in home or school. Even when nothing seems wrong with how they act or behave everyday, maybe deep down, they feel abandoned. When you are in this situation…

Perbandingan data asli dan data enkripsi ditunjukkan pada tabel 9.

Tabel 9 Perbandingan Data Asli dengan Data Hasil Enkripsi

Data Input	Data hasil enkripsi
It is really not unusual for teens to experience the blue or depression. This can be caused by so many things, one of them is how they are being treated in home or school. Even when nothing seems wrong with how they act or behave everyday, maybe deep down, they feel abandoned. When you are in this situation…	’½i²¼i»®ªµµÂi·¸½i¾·¾¼¾ªµi¯¸»i½®®·¼i½¸i®Á¹®»²®·¬ ®i½±®i«µ¾®i¸»i-®¹»®¼¼²¸·w• ±²¼i¬ª·i«®i¬ª¾¼®-i«Âi ¼¸i¶ª·Âi½±²·°¼ui¸·®i¸¯i½±®¶i²¼i±¸Ài½±®Âiª»®i«®²·°i½ »®ª½®-i²·i±¸¶®i¸»i¼¬±¸¸µwiŽ¿®·iÀ±®·i·¸½±²·°i¼®®¶¼i À»¸·°iÀ²½±i±¸Ài½±®Âiª¬½i¸»i«®±ª¿®i®¿®»Â-ªÂui¶ªÂ«®i -®®¹i-¸À·ui½±®Âi¯®®µiª«ª·-¸·®-

Dari tabel 7 dapat diperhatikan bahwa data asli dan data yang telah dienkripsi tidak memiliki kemiripan sama sekali. Hal ini membuat kerahasiaan isi informasi atau data tetap terjaga.

b. Perbandingan Data Asli dengan Data Yang Diterima Setelah Penggunaan ECC

Data hasil enkripsi yang telah diperlihatkan pada tabel 9 kemudian akan dikirimkan menggunakan sistem transimisi OFDM dan modulator QPSK pada kanal fading dan AWGN.

Tabel 10 Perbandingan Data Hasil Dekripsi untuk Eb/No 8 dB dan 20 dB

Eb/No (dB)	Data Hasil Dekripsi
8	It is really not un#sual fo# teens to experien#e #he blue or#depression. This c#n be#cau#ed by so many things, one of them is how they ar# #eing trea#ed in hom# or school. Even when nothing seems wrong with how t#ey act or beh#ve#everyday, maybe de## down, they feel #bando#I#. When you#### in#this situation....
20	It is really not unusual for teens to experience the blue or depression. This can be caused by so many things, one of them is how they are being treated in home or school. Even when nothing seems wron# with how they act or behave everyday, maybe deep down, they feel abandoned. When you are in this situation....

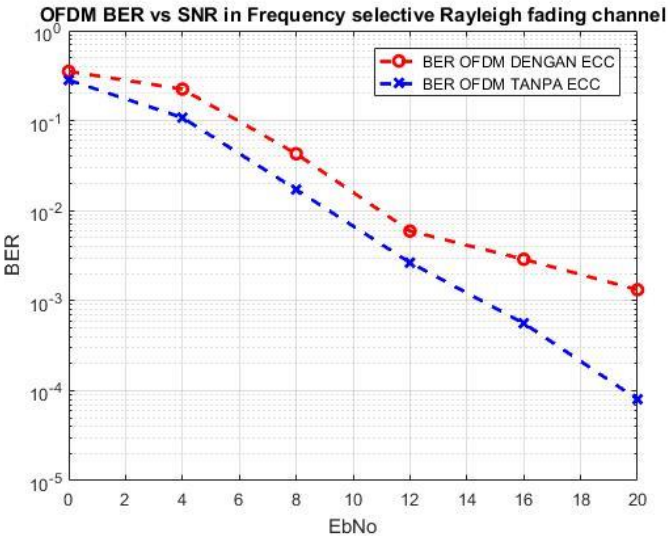
Dari tabel 10 dapat dilihat bahwa data pada nilai Eb/No 20 dB terdapat satu karakter yang mengalami *error*, sedangkan data pada nilai Eb/No 8 dB memiliki cukup banyak *error* pada data yang diterima.

c. Perbandingan Hasil BER Sistem OFDM Menggunakan ECC dan Sistem OFDM Tanpa ECC

Simulasi selanjutnya adalah perbandingan hasil BER antara sistem yang memakai metode enkripsi ECC dengan sistem yang tidak memakai metode enkripsi ECC.

Tabel 11 Perbandingan BER Sistem Tanpa ECC dan Sistem Dengan ECC Menggunakan QPSK

Eb/No(dB)	BER tanpa ECC	BER dengan ECC
0	0.28213	0.35300
4	0.10801	0.22399
8	0.01714	0.04286
12	0.00264	0.00592
16	0.00056	0.00288
20	0.00008	0.00132



Gambar 2 Grafik Perbandingan Sistem Tanpa ECC dan Sistem Dengan ECC Menggunakan QPSK

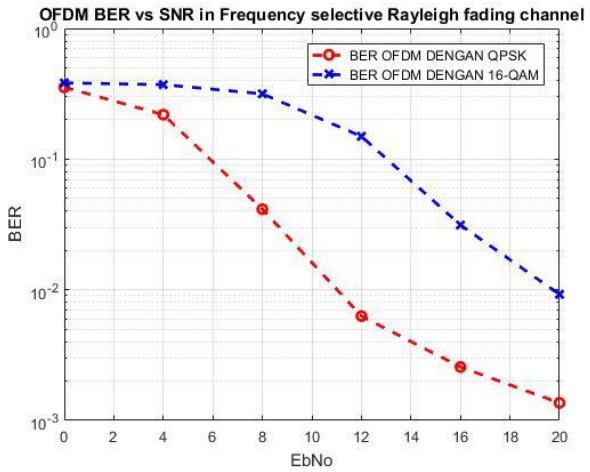
Dari tabel 4 serta gambar 2 dapat dilihat bahwa sistem yang menggunakan metode enkripsi ECC memiliki nilai BER yang lebih tinggi dari sistem yang tidak memakai metode enkripsi ECC. Akan tetapi dengan penggunaan metode enkripsi ECC, informasi data akan terjaga keamanannya, seperti yang telah dijelaskan pada subbab sebelumnya.

d. Perbandingan Hasil BER Antara Modulator QPSK dan 16-QAM

Simulasi selanjutnya adalah perbandingan hasil BER untuk sistem yang menggunakan ECC, namun menggunakan modulator yang berbeda.

Tabel 12 Perbandingan Nilai BER Modulator QPSK dan 16-QAM

Eb/No(dB)	BER QPSK	BER 16-QAM
0	0.35432	0.38281
4	0.21883	0.37131
8	0.04138	0.31578
12	0.00629	0.14923
16	0.00256	0.03129
20	0.00136	0.00921



Gambar 3 Grafik Perbandingan BER Sistem Dengan Modulator QPSK dan 16-QAM

Dari tabel 12 dan gambar 3 dapat dilihat bahwa nilai BER untuk sistem dengan modulator QPSK memiliki nilai BER yang lebih kecil dibandingkan sistem dengan modulator 16-QAM. Hal ini disebabkan orde dari QAM yang bernilai lebih besar dari orde PSK.

IV. KESIMPULAN

Pesan asli dan pesan yang akan dikirimkan memiliki karakter yang sangat jauh berbeda. Selain itu, data yang nantinya akan dikirimkan bukan berupa bentuk *binary* dari string, namun merupakan *binary* dari pasangan nilai x dan y yang membentuk sebuah titik poin pada kurva. Performansi algoritma enkripsi ECC dapat dilihat melalui nilai *adjacent correlation* sebesar rata-rata 0.0064, nilai entropy sebesar 7.4186, sensitif terhadap perubahan kunci, dan membutuhkan waktu yang sangat lama untuk mencari nilai kunci menggunakan teknik *Brute Force Attack* pada nilai kunci yang tinggi. Dari data tersebut dapat disimpulkan data yang dienkripsi dengan metode enkripsi ECC menjadi aman dari pihak ketiga. Selain itu, penggunaan algoritma enkripsi ECC pada sistem transmisi OFDM dengan kanal *fading Rayleigh* tidak memberikan pengaruh besar pada nilai BER, sehingga dapat menjadi alternatif metode sistem keamanan data. Selanjutnya, semakin besar nilai Eb/No, semakin kecil nilai BER. Untuk mencegah kerusakan pada data yang dikirim melewati kanal *fading* dapat dilakukan dengan menaikkan nilai Eb/No. Selain itu, Nilai BER pada QPSK relatif lebih kecil dibandingkan nilai BER pada 16-QAM. Hal ini menunjukkan penggunaan modulator dengan orde lebih kecil lebih baik digunakan pada komunikasi *wireless*, jika mengabaikan efisiensi spektrum.

DAFTAR PUSTAKA

[1] O. Shoewu, Segun O.Olantinwo. *Securing Text Messages using Elliptic Curve Cryptography and Orthogonal Frequency Division Multiplexing.The Pacific Journal of Science and Technology,Volume 14,Number 2,November 2013.*

[2] Stallings, William. *Cryptography and Network Security*. *Sixth Edition*

[3] Priyanka Pimpale, Rohan Rayarikar dan Sanket Upadhyay, *SMS Encryption using AES Algorithm on Android*, IJCSNS International Journal of Computer Application, VOL. 50 No. 19, July 2012.

[4] Gerard Maral, Michel Bousquet. *Satellite Communication Systems:Systems, Techniques, and Technology, Fifth Edition*

[5] Simon Haykin. *Communication Systems, Fourth Edition*

[6] Ove Edfors, dkk. *An Introduction to Orthogonal Frequency Division Multiplexing*, September 1996.

[7] Mohd. Abuzer Khan, dkk. *BER performance of BPSK, QPSK, and 16-QAM with and without using OFDM over AWGN, Rayleigh and Rician Fading Channel*, International Journal of Advanced Research in Computer and Communication Engineering, VOL. 4, Issue 7, July 2015.

[8] Anurag Panday, Sandeep Sharma. *BER Performance of OFDM System in AWGN and Rayleigh Fading Channel*, International Journal of Engineering Trends and Technology, VOL 13, No. 3, July 2014.

[9] Ali Soleymani, Md Jan Nordin. *A Novel Public Key Image Encryption Based on Elliptic Curves over Prime Number Group Field*, Journal of Image and Graphics, Volume 1, No.1, March 2013.

[10] Samia Alblwi, Khalil Shujaee. *A Survey on Wireless Security Protocol WPA2*, International Conference Security and Management, 2017.

[11] Swadeep Singh, Anupriya Garg. *Comparison of CryptographicAlgorithm: ECC & RSA.* International Journal of Computer Science and Communication Engineering, NCRAET-2013.