

DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN ORISINALITAS	iii
ABSTRAK	vi
ABSTRACT	viii
KATA PENGANTAR	x
UCAPAN TERIMA KASIH	xi
DAFTAR ISI	xii
DAFTAR GAMBAR	xvii
DAFTAR TABEL	xxi
I USULAN GAGASAN	1
1.1 Deskripsi Umum Masalah	1
1.1.1 Latar Belakang	1
1.1.1.1 <i>Machine Learning for Channel Estimation</i>	1
1.1.1.2 Eksperimen Lapangan untuk mendapatkan <i>Path</i> <i>Loss Exponent</i> pada Komunikasi 6G	2
1.1.1.3 <i>Quantum Cryptography</i>	3
1.2 Analisis Masalah	4
1.2.1 Aspek Teknis	5
1.2.2 Aspek Regulasi	7
1.2.3 Aspek Ekonomi	9
1.2.4 Aspek Lingkungan	10
1.3 Analisis Solusi Saat Ini	11
1.3.1 <i>Machine Learning for Channel Estimation</i>	11

1.3.2	Eksperimen Lapangan untuk mendapatkan <i>Path Loss Exponent</i> pada Komunikasi 6G	13
1.3.3	<i>Quantum Cryptography</i>	13
1.4	Tujuan Penelitian Tugas Akhir	14
1.5	Batasan Tugas Akhir	14
1.6	Manajemen proyek dan identifikasi <i>working package</i>	15
1.6.1	Identifikasi WP 1 (Status Proyek: Selesai)	15
1.6.2	Identifikasi WP 2 (Status Proyek: Selesai)	16
1.6.3	Identifikasi WP 3 (Status Proyek: Selesai)	16
II	Tinjauan Pustaka	17
2.1	<i>Machine Learning for Channel Estimation</i>	17
2.1.1	<i>5G Standardization</i>	17
2.1.2	<i>5G Spectrum</i>	18
2.1.3	<i>5G Use Cases</i>	18
2.2	Eksperimen Lapangan untuk mendapatkan <i>Path Loss Exponent</i> pada Komunikasi 6G	18
2.2.1	<i>Recommendation ITU-R P.1411-9</i>	19
2.2.2	<i>Path Loss</i>	19
2.2.3	<i>Coverage Area</i>	20
2.2.4	<i>Reference Signal Received Power (RSRP)</i>	21
2.2.5	Metode <i>Curve Fitting</i> untuk <i>Path Loss Exponent</i>	21
2.3	<i>Quantum Cryptography</i>	22
2.3.1	<i>Quantum Key Distribution</i>	23
2.3.2	<i>Quantum Gates</i>	24
2.3.3	<i>Bell States</i> atau <i>EPR Pair</i>	25
2.3.4	<i>CHSH Inequality</i>	25
2.3.5	<i>One Time Pad</i>	27
2.3.6	<i>Depolarizing Channel</i>	27
2.3.7	<i>Eavesdropper Interception</i>	28
2.3.8	<i>Secret Key Rate (SKR)</i>	29
III	SPESIFIKASI DAN DESAIN SISTEM	30
3.1	Spesifikasi Sistem	30
3.1.1	<i>Machine Learning for Channel Estimation</i>	30
3.1.2	Eksperimen Lapangan untuk mendapatkan <i>Path Loss Exponent</i> pada Komunikasi 6G	31
3.1.3	<i>Quantum Cryptography</i>	31

3.2	Desain Sistem	32
3.2.1	<i>Machine Learning for Channel Estimation</i>	33
3.2.1.1	Model Sistem	33
3.2.1.2	Tahapan Implementasi Solusi	33
3.2.2	Eksperimen Lapangan untuk mendapatkan <i>Path Loss Expo-</i> <i>nent</i> pada Komunikasi 6G	34
3.2.2.1	Model Sistem <i>Path Loss</i> ITU - R P.1411 dan 3GPP	34
3.2.3	<i>Quantum Cryptography</i>	35
3.2.3.1	Model Sistem Protokol E91 untuk <i>Quantum</i> <i>Cryptography</i>	35
3.3	Metode Pengukuran yang Sesuai dengan Solusi Terpilih	36
3.3.1	<i>Machine Learning for Channel Estimation</i>	36
3.3.2	Eksperimen Lapangan untuk mendapatkan <i>Path Loss Expo-</i> <i>nent</i> pada Komunikasi 6G	38
3.3.3	<i>Quantum Cryptography</i>	38
IV	IMPLEMENTASI	41
4.1	Deskripsi Umum Implementasi	41
4.1.1	<i>Machine Learning for Channel Estimation</i>	41
4.1.2	Eksperimen Lapangan untuk mendapatkan <i>Path Loss Expo-</i> <i>nent</i> pada Komunikasi 6G	42
4.1.3	<i>Quantum Cryptography</i>	42
4.2	Detail Implementasi	43
4.2.1	<i>Machine Learning for Channel Estimation</i>	43
4.2.1.1	<i>Transmitter</i>	43
4.2.1.2	<i>Receiver</i>	44
4.2.2	Eksperimen Lapangan untuk mendapatkan <i>Path Loss Expo-</i> <i>nent</i> pada Komunikasi 6G	46
4.2.2.1	<i>Set Up</i> Perangkat	46
4.2.2.2	Parameter Eksperimen	49
4.2.3	<i>Quantum Cryptography</i>	50
4.2.3.1	<i>Eavesdropper Interception</i>	50
4.2.3.2	<i>Depolarizing Channels</i>	51
4.3	Prosedur Pengoperasian Solusi	51
4.3.1	<i>Machine Learning for Channel Estimation</i>	51
4.3.2	Eksperimen Lapangan untuk mendapatkan <i>Path Loss Expo-</i> <i>nent</i> pada Komunikasi 6G	52
4.3.3	<i>Quantum Cryptography</i>	54

4.3.3.1	Skenario untuk <i>Quantum Cryptography</i>	54
4.3.3.2	Proses Pembuatan Key	56
4.3.3.3	Parameter-parameter Pengujian pada Simulasi yang Dilakukan	58
V	PENGUJIAN	60
5.1	Skema Pengujian Sistem	60
5.1.1	<i>Machine Learning for Channel Estimation</i>	60
5.1.2	Eksperimen Lapangan untuk mendapatkan <i>Path Loss Expo-</i> <i>nent</i> pada Komunikasi 6G	61
5.1.3	<i>Quantum Cryptography</i>	61
5.2	Proses Pengujian dan Analisis Hasil	63
5.2.1	Flowchart Proses Pengujian	63
5.2.1.1	<i>Machine Learning for Channel Estimation</i>	63
5.2.1.2	Eksperimen Lapangan untuk mendapatkan <i>Path</i> <i>Loss Exponent</i> pada Komunikasi 6G	64
5.2.1.3	<i>Quantum Cryptography</i>	65
5.2.2	Pengujian <i>Machine Learning for Channel Estimation in</i> <i>Multipath AWGN Channel</i>	67
5.2.2.1	Pembuktian Jumlah Minimum <i>Cyclic Prefix (CP)</i>	67
5.2.2.2	Derivasi Formula <i>Eigenvalues</i> Kanal	68
5.2.2.3	FER terhadap Variasi <i>Pilot Value</i>	70
5.2.2.4	FER terhadap <i>DL-Based Channel Estimation in</i> <i>Multipath AWGN Channel</i>	70
5.2.2.5	BER terhadap Variasi <i>Pilot Value</i>	78
5.2.2.6	BER terhadap <i>DL-Based Channel Estimation in</i> <i>multipath AWGN channel.</i>	79
5.2.3	Analisis Hasil <i>Machine Learning for Channel Estimation in</i> <i>Multipath AWGN Channel</i>	80
5.2.3.1	FER terhadap Variasi <i>Pilot Value</i>	80
5.2.3.2	FER terhadap <i>DL-Based Channel Estimation in</i> <i>multipath AWGN channel.</i>	81
5.2.3.3	BER terhadap Variasi <i>Pilot Value</i>	83
5.2.3.4	BER terhadap <i>DL-Based Channel Estimation in</i> <i>multipath AWGN channel.</i>	84
5.2.4	Analisis Hasil <i>Machine Learning for Channel Estimation in</i> <i>Multipath Rayleigh Fading Channels</i>	85

5.2.5	Pengujian Eksperimen Lapangan untuk mendapatkan <i>Path Loss Exponent</i> pada Komunikasi 6G	91
5.2.6	Analisis Hasil Eksperimen Lapangan untuk mendapatkan <i>Path Loss Exponent</i> pada Komunikasi 6G	91
5.2.7	Estimasi Luas Cakupan Berdasarkan <i>Path Loss Exponent</i>	93
5.2.8	Pengujian <i>Quantum Cryptography</i>	95
5.2.8.1	<i>Probability of resulted keys</i> dari protokol E91 dan BB84	96
5.2.8.2	Skenario dengan <i>Eavesdropper Interception under a Perfect Channels</i>	98
5.2.8.3	Skenario dengan <i>Eavesdropper Interception Combined under The Erroneus Channels</i>	101
5.2.9	Analisis Hasil <i>Quantum Cryptography</i>	103
5.2.9.1	<i>Probability of resulted keys</i>	103
5.2.9.2	Perbandingan protokol E91 dan BB84	105
5.2.9.3	Kinerja <i>Secret Key Rate to Total Probability of Intercept under Perfect Channel</i>	110
5.2.9.4	Kinerja <i>Secret Key Rate to Total Probability of Eavesdropper Interception dan Erroneus Channels</i>	111
5.3	Rangkuman Hasil Pengujian	112
5.3.1	<i>Machine Learning for Channel Estimation</i>	112
5.3.2	Eksperimen Lapangan untuk mendapatkan <i>Path Loss Exponent</i> pada Komunikasi 6G	117
5.3.3	<i>Quantum Cryptography</i>	119
VI	Kesimpulan dan Saran	123
6.1	Kesimpulan	123
6.2	Saran	124
	DAFTAR PUSTAKA	126