Otomatisasi Simulasi *Quantum Key Distribution* Berdasarkan Protokol BB84 pada EDU-QCRY1

Naufal Hafiz Syahidan[1)], Mohamad Syahral[2)]

1) Rekayasa Perangkat Keras Kriptografi, Poltek SSN, naufalhafiz.syahidan@student.poltekssn.ac.id

2) Rekayasa Perangkat Keras Kriptografi, Poltek SSN, mohamad.syahral@poltekssn.ac.id

Abstrak

Perangkat EDU-QCRY1 dirancang untuk menyimulasikan protokol BB84, yang termasuk dalam teknik Quantum Key Distribution (QKD). yang merupakan teknik pendistribusian kunci menggunakan metode kuantum dengan memanfaatkan sifat cahaya sebagai partikel dalam bentuk foton. Perangkat EDU-QCRY1 yang dijalankan secara manual memiliki berbagai keterbatasan dalam penggunaannya seperti waktu operasi dan akurasi simulasi yang tergantung pada keterampilan dan ketelitian pengguna. Penelitian ini merancang-bangun sebuah sistem otomatisasi perangkat EDU-QCRY1 yang bertujuan untuk menghasilkan kunci dengan lebih cepat dan akurat.

Perancangan sistem dibagi menjadi dua versi, sistem versi I menggunakan skenario motor servo sederhana, friksi langsung servo, sensor Light Dependent Resistor (LDR) dengan lakban, dan penyimpanan hasil simulasi pada serial monitor mikrokontroler Arduino. Sistem versi I terdapat kegagalan dalam integrasi fungsi rotor polarisator sehingga perlu dirancang system versi II. Sistem versi II menggunakan skenario motor servo, skema spur gear servo, sensor LDR dengan penutup, dan penyimpanan hasil simulasi pada database MySQL. Sistem versi II merupakan sistem utama pada sistem otomatisasi sekaligus sistem versi terakhir yang dirancang. Pengambilan data hasil otomatisasi dilakukan dengan mentransmisikan 100 bit dalam setiap percobaan yang dilakukan 10 kali. Waktu proses otomatisasi diambil dari langkah awal sesuai protocol BB84 pembangkitan angka acak hingga bit kunci hasil simulasi diproduksi yang didapatkan hasil waktu proses rata rata dari 100 bit yang ditransmisikan adalah selama 7 menit 34,9 detik atau 4 kali lebih cepat dibandingkan proses QKD secara manual. Pengambilan data akurasi didapatkan dari total jumlah bit yang diterima dibandingkan dengan total jumlah bit yang dikirimkan dan didapatkan hasil akurasi sebesar 94%.

Kata kunci: *Arduino (1), BB84 (2), EDU-QCRY1 (3), Otomatisasi (4), Quantum Key Distribution (5)*

Abstract

The EDU-QCRY1 device is designed to simulate the BB84 protocol, which falls under the Quantum Key Distribution (QKD) technique. This is a key distribution technique using quantum methods by leveraging the properties of light as particles in the form of photons. The manually operated EDU-QCRY1 device has several limitations in its use, such as operational time and simulation accuracy, which depend on the user's skill and precision. This research developed an automation system for the EDU-QCRY1 device aiming to produce keys more quickly and accurately. The system design is divided into two versions. Version I uses a simple servo motor scenario, direct servo friction, a Light Dependent Resistor (LDR) sensor with tape, and storage of simulation results on the Arduino microcontroller's serial monitor. Version I experienced a failure in the integration of the polarizer rotor function, necessitating the design of Version II. Version II uses a servo motor scenario, a servo spur gear scheme, an LDR sensor with a cover, and storage of simulation results in a MySQL database. Version II is the primary system in automation and is the final designed version. Data collection from the automation is done by transmitting 100 bits in each of the 10 trials conducted. The automation process time is taken from the initial steps according to the BB84 protocol of random number generation to the production of the simulated key bit. The average process time for transmitting 100 bits is 7 minutes 34.9 seconds, which is four times faster than the manual QKD process. Accuracy data is obtained from the total number of bits received compared to the total number of bits sent, yielding an accuracy result of 94%.

Keywords: A*rduino (1), Automation (2), BB84 (3), EDU-QCRY1 (4), Quantum Key Distribution (5)*

1. PENDAHULUAN

Perangkat EDU-QCRY1 merupakan perangkat untuk menyimulasikan protokol BB84 yaitu salah satu protokol *Quantum Key Distribution* (QKD) [1]. *Quantum Key Distribution* merupakan teknik pendistribusian kunci dengan menggunakan metode kuantum dengan memanfaatkan sifat cahaya sebagai partikel dalam bentuk foton [2]. Perangkat simulasi terdiri atas beberapa komponen utama untuk membentuk rekayasa komunikasi antara Alice sebagai pengirim, Bob sebagai penerima, dan Eve yang diasumsikan sebagai penyadap [1]. Komponen utama perangkat EDU-QCRY1 antara lain, laser diode sebagai sumber foton dalam simulasi, polarisator untuk menentukan basis yang digunakan, beamsplitter sebagai pemisah cahaya yang diteruskan atau dibelokkan, dan detektor bit sebagai penerima cahaya bit ‘0’ dan bit ‘1’ [1]. Dalam menyimulasikan protokol BB84 pada perangkat, penentuan basis pada pengirim dan penerima dilakukan oleh polarisator dengan menentukan sudut-sudut tertentu [2]. Cara kerja protokol BB84 diawali pengiriman nilai acak yang melewati dua polarisator sebagai basis,

selanjutnya basis yang digunakan antara pengirim dan penerima dilakukan pencocokkan melalui jaringan publik secara manual [3]. Bit dengan basis yang cocok/sama antara pengirim dan penerima akan menjadi kunci [4]. Kelebihan QKD yang berdasarkan pada prinsip ketidakpastian Heisenberg yang berarti bahwa seorang penyadap akan terdeteksi apabila melakukan penyadapan sehingga pendistribusian kunci tergolong lebih aman [3].

Simulasi QKD dengan protokol BB84 pada perangkat EDU-QCRY1 dasarnya dilakukan secara manual [1]. Terdapat sembilan tahapan langkah dalam protokol BB84, langkah pertama pengirim memilih bit dan basis secara acak, selanjutnya penerima memilih basis secara acak, setelah itu pengirim mengirimkan bit foton, kemudian penerima menerima bit hasil transmisi. Setelah semua bit diterima, pengirim memberikan basis yang digunakan (dilakukan pada jaringan publik), lalu penerima menerima basis pengirim, kemudian pengirim dan penerima mencocokkan basis yang digunakan, pada akhirnya bit dengan basis yang berbeda diabaikan dan bit yang tersisa (dengan basis sama) menjadi bit hasil simulasi yang selanjutnya dapat digunakan untuk proses enkripsi [5]. Kompleksitas langkah pengoperasian sebanyak sembilan langkah serta cara operasi yang masih manual menjadi latar belakang dalam merancang sistem otomatisasi.

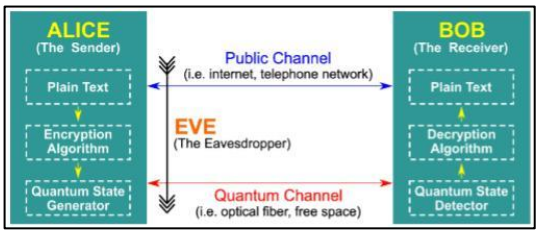
Perangkat EDU-QCRY1 yang dijalankan secara manual memiliki berbagai keterbatasan dalam penggunaannya seperti kecepatan dan keakuratan yang tergantung pada keterampilan dan ketelitian pengguna [6] serta hasil bit kunci harus diperiksa dan didokumentasikan secara manual [2]. Keterbatasan ini dapat diatasi dengan otomatisasi yang diharapkan dapat mempersingkat waktu pemrosesan sehingga lebih banyak data yang diproses dan dapat meminimalisir tingkat kesalahan [7] serta penyimpanan bit kunci dalam database. Otomatisasi skema penerimaan bit pada perangkat penerima dengan menggunakan sensor *Light Dependent Resistor* (LDR) pada penelitian [8] masih menginputkan basis pengirim dan penerima secara manual untuk menghasilkan bit kunci dari QKD dengan protokol BB84. Penelitian [6] membuat skema rotasi otomatis polarisator dengan input acak dari sensor akselerometer dengan aktuator piezomotor untuk merotasi polarisator. Sementara penelitian [4] mengusulkan sebuah skema mengenai otomatisasi pencocokkan basis pengirim dan penerima secara paralel dengan menggunakan Arduino sebagai modul mikrokontroler untuk mengatur pengiriman foton.

Pada penelitian ini akan dilakukan pembuatan otomatisasi simulasi QKD pada EDU-QCRY1. Otomatisasi dilakukan dengan rotasi otomatis pada polarisator, pembacaan bit pada perangkat penerima dengan sensor LDR, pencocokkan basis pengirim dan penerima secara otomatis, dan pencatatan/dokumentasi hasil simulasi secara otomatis. Pengiriman foton dilakukan setelah polarisator sudah berada pada sudut tertentu berdasarkan input acak dari salah satu pin analog sebagai *seed* dari fungsi random pada arduino, pembacaan bit pada perangkat penerima dilakukan dengan sensor LDR [8], pembangkitan bit kunci secara otomatis dengan mencocokkan basis pengirim dan penerima [4], dan hasil simulasi yang meliputi bit dan basis acak, dan bit kunci disimpan pada *database* MySQL.

2. LANDASAN TEORI

2.1 Quantum Key Distribution

Quantum Key Distribution (QKD) merupakan metode aman untuk mendistribusikan kunci kriptografi dengan memanfaatkan mekanika kuantum. Dalam praktiknya QKD digabungkan dengan saluran klasik yang terotentikasi, dan algoritma enkripsi klasik [9]. Pengirim dan penerima dapat mendeteksi kemungkinan terjadinya penyadapan oleh pihak ketiga dengan membandingkan urutan bit yang dikirim dengan yang diterima [10]. QKD didasarkan pada dua prinsip utama yakni prinsip ketidakpastian Heisenberg dan teorema *anti-cloning* [2] sehingga memungkinkan pertukaran informasi rahasia yang aman antara dua atau lebih partisipan [11]. Pada protokol QKD, partisipan yang terlibat adalah Alice (pengirim), Bob (penerima), dan Eve (penyadap). Pada gambar 1 merupakan gambaran skema quantum key distribution [2].



Gambar 1. Skema *Quantum Key Distribution* [2]

QKD dapat menyediakan kemampuan yang tidak dimiliki oleh teknik kriptografi klasik yakni kemampuan untuk mendeteksi keberadaan penyadap. Dengan protokol QKD, jika seorang penyadap (Eve) mencoba mencuri kunci, maka pihak yang berkomunikasi akan dapat mendeteksinya dengan memanfaatkan hukum kuantum yaitu *anti-cloning* [11]. Jika Eve mencoba menyadap komunikasi kuantum antara Alice dan Bob, maka Eve akan meninggalkan beberapa jejak yang dapat dideteksi.

Pada bagian pendeteksian penyadap, protokol QKD dapat dibedakan menjadi 2 jenis secara eksperimental [2].

a. *Prepare and measure*

Protokol QKD disebut sebagai "prepare and measure" karena Alice harus "mempersiapkan" terlebih dahulu qubit berupa foton terpolarisasi yang akan dikirim dan kemudian Bob akan "mengukur" hasil qubit yang diterimanya. Prinsip

ini didasarkan pada prinsip ketidakpastian Heissenberg [5]. Jenis ini memungkinkan pihak yang sah untuk mendeteksi penyadap dengan membandingkan jumlah kesalahan yang mungkin terjadi dalam komunikasi mereka dengan kesalahan sebenarnya pada pengukuran mereka [12]. Contoh dari protokol QKD jenis ini ialah BB84, SARG-04, B-92, S-13.

b. *Entanglement*

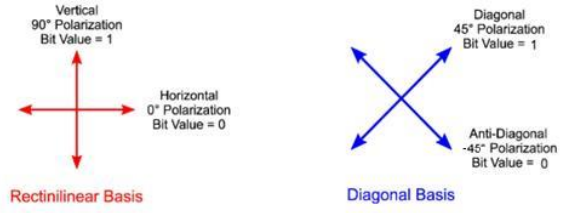
Protokol QKD *entanglement* dilakukan dengan mengirimkan dua buah foton berikatan secara bersamaan kepada pengirim dan penerima. Masing-masing pengirim dan penerima akan menerima satu partikel foton dari sepasang foton berikatan [5]. Dua partikel dari pasangan ini saling berhubungan dan jika salah satu berubah maka akan mempengaruhi partikel lainnnya [13]. Properti *entanglement* dari suatu sistem ialah berdasarkan pada:

1) Partikel dapat dihubungkan dan diubah satu sama lain dengan suatu interaksi.
2) Partikel yang saling berhubungan dapat disebut sebagai variabel tersembunyi.

Contoh dari protokol QKD jenis ini ialah E-91, BBM-92, DPS, COW.

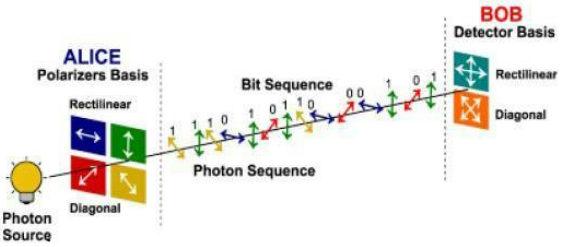
2.2 Protokol BB84

Protokol BB84 merupakan protokol QKD pertama yang diperkenalkan oleh Bennet dan Brassard pada tahun 1984 [5]. Protokol BB84 memanfaatkan prinsip mekanika quantum yang dikenal dengan prinsip ketidakpastian Heisenberg. Protokol ini termasuk dalam jenis protokol QKD "*prepare and measure*". Protokol ini menggunakan 2 basis polarisasi yaitu *rectilinear* dan diagonal. Pada basis rectilinear (+) nilai 0 direpresentasikan dengan sudut 0° dan nilai 1 direpresentasikan dengan sudut 90°. Selain itu, pada basis diagonal (X) nilai 0 direpresentasikan oleh sudut -45° dan nilai 1 direpresentasikan oleh sudut 45° [5]. Basis serta bit protokol ditunjukkan pada gambar 2.



Gambar 2. Basis dan State pada Protokol BB84

Protokol BB84 merupakan protokol pertama yang menjelaskan bagaimana menggunakan polarisasi foton untuk mengirimkan kunci rahasia melalui saluran komunikasi quantum. Pada protokol ini digunakan polarisasi foton tunggal (*single photon*) untuk mengirim dan mendistribusikan bit kunci rahasia [14]. Skema pengiriman foton pada protokol BB84 ditunjukkan pada gambar 3.



Gambar 3. *Basis dan State* pada Protokol BB84

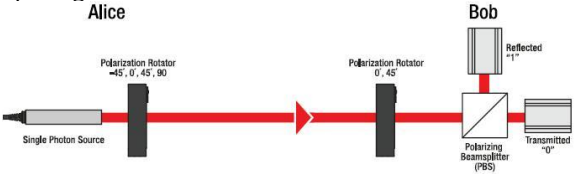
Langkah protokol BB84 antara lain:

1. Alice memilih rangkaian bit sebanyak k bit.
2. Alice menentukan rangkaian basis sebanyak k string dan mengkodekan setiap bit data sebagai {|0, |1} berdasarkan basis yang digunakan.
3. Bob menentukan rangkaian basis sebanyak k string.
4. Alice mengirim bit/state kepada Bob.
5. Bob menerima bit dengan basis + atau X yang telah ia tentukan sebelumnya.
6. Bob memberitahukan basis yang digunakan kepada Alice melalui jaringan publik.
7. Alice dan Bob membuang semua bit yang digunakan oleh Bob dengan basis yang berbeda dengan Alice. Bit yang tersisa kemudian dijadikan bit kunci.
8. Untuk memastikan interferensi dari Eve, Alice memilih subset dari n bit untuk memeriksa bit dan menginformasikannya kepada Bob. Apabila terdapat ketidaksamaan/ ketidaksesuaian maka proses dibatalkan.

Proses pembuangan bit yaitu mengabaikan bit dengan basis yang berbeda pada Bob dan Alice pada langkah ke-7 dikarenakan adanya eror yang menyebabkan Bob tidak dapat menerima dengan pasti bit yang dikirimkan Alice.

2.3 EDU-QCRY1

EDU-QCRY1 merupakan perangkat yang digunakan untuk pembelajaran manual *quantum cryptography* [1]. Perangkat ini terdiri atas beberapa komponen untuk membentuk rekayasa komunikasi antara Alice sebagai pengirim dan Bob sebagai penerima serta Eve yang diasumsikan sebagai penyadap. Perangkat ini dapat digunakan untuk menyimulasikan protokol *quantum key distribution* BB84. Dalam perangkat ini, protokol BB84 digunakan untuk menentukan dua basis yang masing-masing mencakup dua polarisasi cahaya. Ilustrasi pengiriman foton ditunjukkan pada gambar 4 dan perangkat Alice dan Bob EDU-QCRY1 ditunjukkan pada gambar 5.



Gambar 4. Ilustrasi Pengiriman Foton EDU-QCRY1 [1]

Gambar 5. Perangkat Alice dan Bob EDU-QCRY1 [1]

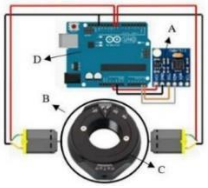
Komponen utama dari perangkat Alice adalah laser sebagai sumber cahaya dan pelat $\frac{\pi}{2}$ sebagai polarisator yang ditunjukkan pada gambar 5. Terdapat saklar foton elektronik berwarna merah sebagai pengatur pengiriman foton yang dilakukan dengan cara menekan tombol berkali kali sesuai dengan jumlah foton yang dikirimkan sebagai simulasi *single photon*. Pelat $\frac{\pi}{2}$ sebagai polarisator terdapat sudut-sudut tertentu, yaitu: -45°, -0°, 45°, dan 90° yang harus diputar secara manual. Sementara komponen pada perangkat Bob antara lain: pelat $\frac{\pi}{2}$ sebagai polarisator, beamsplitter sebagai pemisah cahaya untuk diteruskan atau dibelokkan, dan detektor sebagai penerima bit '0' dan bit '1'.

2.4 *Database* Mysql

Basis data atau *database* dapat diartikan sebagai kumpulan data tentang suatu benda atau kejadian yang saling berhubungan satu sama lain. Sedangkan data merupakan fakta yg mewakili suatu objek seperti manusia atau hewan yang dapat dicatat dan mempunyai arti yg implisit. Data dicatat/rekam dalam bentuk angka, huruf, simbol, gambar bunyi/kombinasinya [15]. Database digital dikelola menggunakan *Database Management System* (DBMS) yang menyimpan isi *database*, mengizinkan pembuatan dan *maintenance* data dan pencarian dan akses yang lain [16].

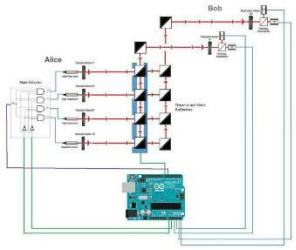
2.5 Penilitian Terdahulu

Beberapa penelitian terkait menghasilkan skema/perangkat otomatisasi yang bertujuan untuk menjalankan perangkat EDU-QCRY lebih efektif dan efisien. Penelitian [6] mengusulkan sebuah skema polarisator otomatis dengan *menggunakan ultrasonic piezomotor* sebagai rotor. *Ultrasonic piezomotor* bekerja dengan menggetarkan polarisator sehingga polarisator dapat berotasi. Kelemahan pada penggunaan sistem ini adalah perangkat piezomotor yang harus dipasangkan/dibubuhkan pada polarisator sehingga sangat beresiko merusak polarisator.



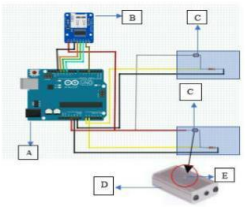
Gambar 6. Skema Otomatisasi Rotasi dengan *Piezomotor* [6]

Sementara skema otomatisasi pada penelitian [4] menggunakan otomatisasi polarisator dengan sudut yang pasti secara paralel, sehingga memerlukan 6 polarisator, 10 reflektor, 2 beamsplitter, dan 4 detektor bit. Penentuan bit dan basis pengirim ditentukan oleh *demultiplexer Integrated Circuit* (IC) secara acak. Penambahan komponen polarisator yang berjumlah hampir 2 kali lipat dari komponen EDU-QCRY1 asli membuat otomatisasi ini tidak efisien dari segi penggunaan perangkat.



Gambar 7. Skema Otomatisasi Polarisator Paralel [4]

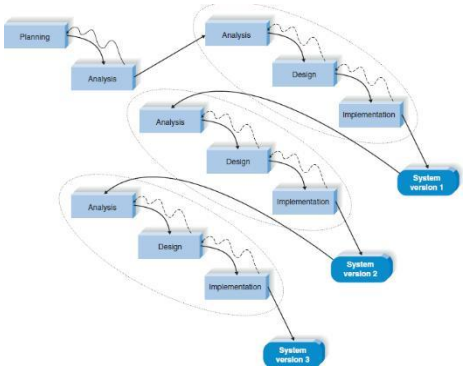
Satu-satunya hasil penelitian terkait yang diterapkan pada sistem otomatisasi yang dibuat adalah pada penelitian [8]. Otomatisasi ini berkaitan pada penerimaan bit dengan sensor LDR yang diletakkan pada setiap detektor bit. Sensor LDR diletakkan pada kotak tempat yang dipasang pada detektor bit yang berfungsi untuk mengurangi interferensi pembacaan LDR pada detektor bit. Hasil dari otomatisasi ini terbukti efektif dan efisien dengan rata rata waktu pembangkitan kunci hasil otomatisasi sebanyak 0.0604 detik, dibandingkan rata rata waktu pembangkitan kunci secara manual sebanyak 24.008 detik. Skema penelitian [8] ditunjukkan pada gambar 2.10 dengan A melambangkan Arduino, B melambangkan modul SD Card, C melambangkan sensor LDR, D melambangkan detektor bit, dan E melambangkan LED detektor bit.



Gambar 8. Skema Otomatisasi Pembacaan Bit dengan Sensor LDR [8]

3. METODE PENELITIAN

Penelitian ini didesain menggunakan metodologi *System Development Life Cycle* (SDLC) dengan pendekatan *iterative development.* SDLC merupakan proses untuk memahami cara merancang dan membangun suatu sistem dapat mendukung kebutuhan bisnis dengan merancang, membangun, dan mengirimkan sistem kepada pengguna [16]. Pendekatan *iterative development* termasuk dalam kategori *Rapid Application Development* (RAD), kategori tersebut melakukan pengembangan terhadap beberapa bagian dari sistem melalui pengulangan.



Gambar 9. Model Sistem *Iterative Development* [17]

Adapun langkah-langkah yang dilakukan dalam penelitian ini adalah sebagai berikut:

1) *Planning* (Perencanaan)

Pada penelitian ini, proses penentuan penelitian yang akan dilakukan adalah dengan melakukan studi literatur mengenai topik penelitian terkait yang telah dilakukan sebelumnya. Hasil dari studi literatur yang didapatkan adalah efektivitas perangkat EDU-QCRY1 pada kriptografi dalam menyimulasikan *Quantum Key Distribution*.

2) *Analysis* (Analisis Kebutuhan)

Pada penelitian ini akan dibuat skema otomatisasi simulasi *Quantum Key Distribution* dari perangkat EDU-QCRY1 berdasarkan protokol BB84. Dilakukan analisis terhadap sistem yang ada, mengidentifikasi perbaikan yang diperlukan dan mengembangkan konsep sistem yang baru. Pada tahap analisis juga mulai dilakukan perbandingan perangkat maupun komponen yang dilanjutkan dengan identifikasi kebutuhan fungsional dan nonfungsional dalam sistem. Perbandingan perangkat dilakukan dengan studi literatur terhadap penelitian terkait pada otomatisasi perangkat EDU-QCRY1.

3) *Design* (Desain)

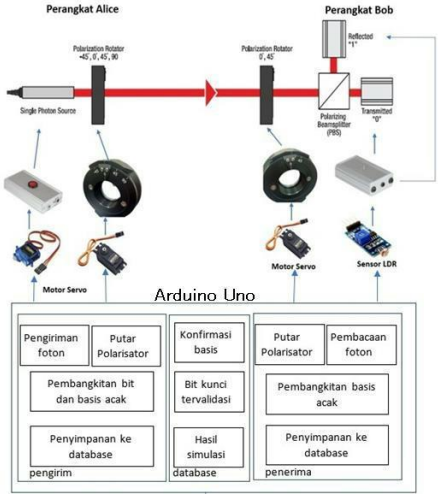
Pada penelitian ini, skema otomatisasi yang akan dibuat didesain menggunakan skematik diagram yang akan menggabungkan skema [4], [6], [8] dengan sedikit modifikasi pada rotor polarisator, dan penyimpanan hasil simulasi pada database MySQL. Perangkat EDU-QCRY1 disusun pada jarak yang paling efisien dan efektif berdasarkan penelitian [18] dan [19].

4) *Implementation* (Implementasi)

Tahap implementasi merupakan tahap yang dilakukan setelah tahap desain yang bertujuan untuk mengimplementasikan desain yang telah dibuat dan menguji hasil skema yang dibuat. Pada penelitian ini akan diimplementasikan penggunaan skema otomatisasi *quantum key distribution*. Tahap ini menggunakan Arduino IDE untuk membuat dan mengunggah program otomatisasi simulasi *quantum key distribution* dengan pengiriman dan penerimaan bit secara otomatis, serta pencocokkan basis yang digunakan oleh pengirim dan penerima melalui fungsi random polarisator pada Arduino.

4. HASIL PENELITIAN

Pada penelitian ini, dibuat sistem otomatisasi perangkat EDU-QCRY1 sehingga tidak diperlukannya lagi pengoperasian secara manual. Perangkat otomatisasi menggunakan beberapa komponen yaitu mikrokontroller Arduino Uno, Motor Servo, serta Sensor LDR.Gambaran umum perangkat otomatisasi yang dibangun dapat dilihat pada gambar 10.



Gambar 10. Gambaran Umum Sistem

Pada gambar 10 dijabarkan mengenai perangkat yang digunakan dalam membangun sistem otomatisasi yang meliputi pergerakkan motor/sensor dan penyimpanan hasil simulasi pada database. Proses dari sistem yang akan dibangun adalah sebagai berikut:

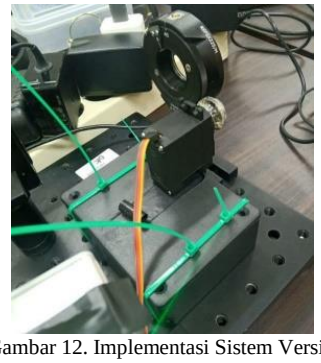
1. Arduino Uno terintegrasi dengan 2 motor servo pada perangkat Alice serta 1 motor servo dan 2 Sensor LDR pada perangkat Bob. Arduino Uno juga digunakan sebagai pembangkit bilangan acak yang akan digunakan untuk menentukan rangkaian bit dan basis yang akan digunakan. Pada perangkat Alice diimplementasikan 2 motor servo yang memiliki spesifikasi torsi yang berbeda dengan berdasarkan fungsi yang dilakukan.
2. Setelah bilangan acak dibangkitkan maka rangkaian bit dan basis pengirim serta basis penerima dapat ditentukan. Pembangkitan angka acak digunakan untuk membangkitkan angka acak yang digunakan untuk bit pengirim, basis pengirim, dan basis penerima.
3. Bit dan basis pengirim serta basis penerima kemudian diterjemahkan oleh Arduino untuk menggerakkan servo untuk merotasi arah polarisator sesuai indeks sudut polarisator. Servo diimplementasikan berdasarkan feedback sudut pada pemrograman [16].
4. Kemudian foton ditembakkan apabila polarisator yang sudah diarahkan pada sudut tertentu. Pengaktifan saklar laser foton elektronik dilakukan oleh motor servo yang berbeda.

5. Pengiriman foton dinyatakan berhasil apabila terdapat salah satu LED dari detektor bit yang menyala pada perangkat Bob. Detektor bit dengan LED yang menyala mengindikasikan nilai bit yang diterima.
6. Sensor LDR digunakan sebagai penangkap sinar LED mana yang menyala sehingga dapat menentukan nilai bit yang diterima secara otomatis.
7. Setelah semua rangkaian bit dikirimkan. Arduino akan membandingkan rangkaian basis dan bit pengirim dan penerima. Apabila basis yang digunakan dalam satu kali pengiriman adalah basis yang berbeda, maka bit dengan basis tersebut diabaikan. Sehingga pada akhirnya hanya tersisa bit dengan basis yang sama. Bit yang tersisa disebut dengan bit kunci.
8. Hasil simulasi berupa rangkaian bit dan basis pengirim, bit dan basis penerima, serta bit kunci dikirimkan ke Arduino yang selanjutnya disimpan pada *database* MySQL.

Arduino mengontrol/mengatur alur data dari pembangkitan angka acak, penerjemahan angka acak ke bit dan basis, penerjemahan ke power motor servo, pencocokkan basis, pembacaan nilai sensor LDR, dan penyimpanan bit hasil simulasi. Penyimpanan bit hasil simulasi dilakukan dengan penyimpanan pada file dengan format txt yang dilakukan secara serial pada Arduino setelah semua bit ditransmisikan. Kemudian file tersebut dibaca oleh fungsi dari bahasa PHP untuk dimasukkan ke dalam *database* MySQL.

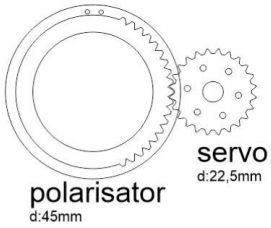
Penelitian ini merancang menjadi 2 sistem versi, dimana sistem versi I dirancang berdasarkan eksperimen yang telah dilakukan, terdapat 3 fungsi utama yang dilakukan eksperimen untuk menemukan skenario yang paling efektif yaitu pengiriman foton otomatis menggunakan skenario motor servo, rotasi polarisator otomatis menggunakan friksi langsung dari motor servo, dan pembacaan bit otomatis dengan sensor LDR yang direkatkan dengan lakban.

Gambar 11. Perancangan Sistem Versi I

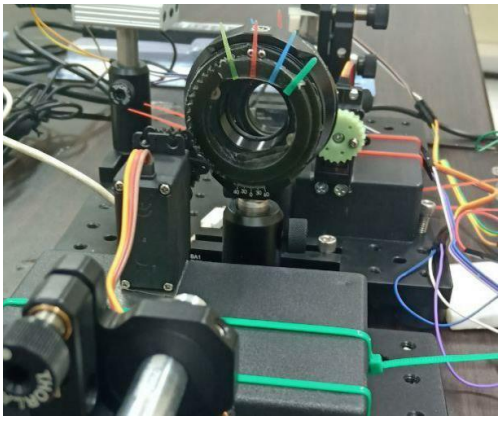


Gambar 12. Implementasi Sistem Versi I

Sementara eksperimen perangkat sistem versi II dilakukan setelah melakukan perancangan terhadap sistem versi I. Sistem versi II diharapkan dapat mendapatkan hasil yang lebih baik dibandingkan sistem versi I. Eksperimen sistem versi II yang tidak sebanyak eksperimen yang dilakukan pada sistem versi I karena bersifat memperbaiki atau meningkatkan tingkat performa dari sistem versi I. Skenario rotasi polarisator otomatis pada sistem versi II ini menggunakan *gear* yang dipasangkan pada polarisator dan servo. Gear ini menggunakan 3D printer dalam pembuatannya dengan hasil pengukuran yang telah dilakukan sebelumnya.



Gambar 13. Perancangan Sistem Versi II

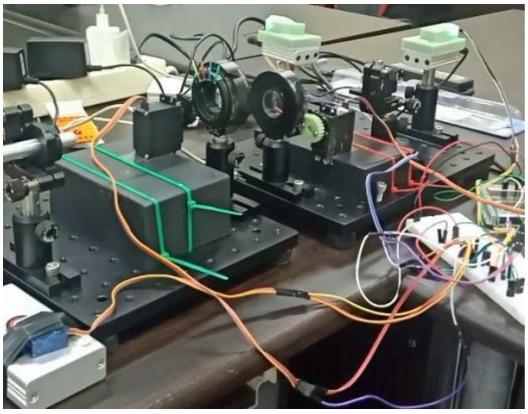


Gambar 14. Implementasi Sistem Versi II

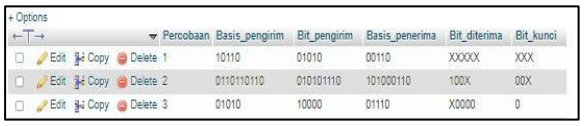
Sistem versi I terdapat kegagalan dalam integrasi fungsi rotor polarisator sehingga pengujian integration testing tidak dapat dilakukan. Sistem versi II dibangun dengan menggunakan skenario fungsi yang berbeda. Tidak semua fungsi dari sistem versi II diubah dari sistem versi I, hanya fungsi yang dapat dilakukan lebih baik ataupun memiliki kesesuaian yang lebih tepat.

Tabel 1. Perbedaan Skenario Sistem Versi I dan II

Versi sistem	Fungsi	Skenario
Sistem Versi I	Pengiriman foton	Motor servo
	Rotasi Polarisator	Friksi motor
	Pembacaan Bit	Sensor LDR
	Penyimpanan hasil	*Serial Monitor*
Sistem Versi II	Pengiriman foton	Motor *servo*
	Rotasi Polarisator	*Gear servo*
	Pembacaan Bit	Sensor LDR
	Penyimpanan hasil	Database MySQL



Gambar 15. Implementasi Sistem Keseluruhan

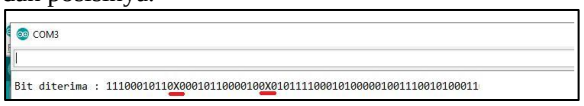


+ Options

	Percobaan	Basis_pengirim	Bit_pengirim	Basis_penerima	Bit_diterima	Bit_kunci
Edit Copy Delete	1	10110	01010	00110	XXXXX	XXX
Edit Copy Delete	2	0110110110	0101011110	1010001110	100X	00X
Edit Copy Delete	3	01010	10000	01110	X0000	0

Gambar 16. *Database* Hasil Simulasi

Pada proses implementasi sistem otomatisasi pada perangkat EDU-QCRY1 dapat terjadi beberapa ketidaksesuaian, salah satunya ialah kegagalan penerimaan bit. Hal ini disebabkan oleh beberapa faktor antara lain adalah: kegagalan pada pengiriman bit, detektor bit tidak menangkap foton (yang ditandai dengan tidak menyalanya detektor bit pada Bob EDU-QCRY1), ataupun kegagalan dari pembacaan sensor LDR. Pada sistem otomatisasi ini pembacaan bit yang dilakukan secara otomatis dengan sensor LDR, kegagalan bit didefinisikan sebagai pembacaan sensor LDR yang berada di luar *range* nilai yaitu 80-150 nilai analog sensor LDR. Bit yang gagal diterima ini ditandai dengan simbol 'X' pada tampilan serial monitor sehingga bit gagal dapat diidentifikasi jumlah dan posisinya.



Gambar 17. Tampilan *Serial Monitor* Bit Gagal Diterima

Hasil data kegagalan bit yang diterima diambil dari 10 kali percobaan transmisi yang dilakukan dengan setiap percobaan mentransmisikan 100 bit dari sistem versi II yang diimplementasikan. Tabel 2 menunjukkan hasil kegagalan penerimaan bit.

Tabel 2. Kegagalan Penerimaan Bit Sistem Otomatisasi

Percobaan	Jumlah Bit *error*
1	7
2	4
3	5
4	7
5	12
6	3
7	3
8	3
9	1
10	6
Rata-rata	**5.2**

Berdasarkan Tabel 2 rata-rata jumlah bit yang gagal diterima adalah 5.2 bit dari 100 bit yang ditransmisikan. Berdasarkan rata rata bit yang gagal diterima, maka didapatkan rata-rata jumlah bit yang berhasil diterima adalah 94,8 bit dari setiap 100 bit yang ditransmisikan. Data statistik rata-rata bit yang berhasil diterima tersebut menjadi dasar daripada hasil akurasi penerimaan bit sebesar 94,8%. Akurasi pada operasi secara manual didapatkan akurasi 100% atau tanpa kegagalan, sedangkan. Penelitian [18] mendapatkan kegagalan 2 bit dari 100 bit yang ditransmisikan pada jarak 100 cm transmisi yang dilakukan, sehingga akurasi pada operasi secara manual didapatkan 98%.

Sistem otomatisasi yang dilakukan berdampak terhadap waktu proses simulasi *Quantum Key Distribution* pada perangkat EDU-QCRY1. Dari 10 percobaan yang mentransmisikan 100 bit setiap percobaan, waktu proses simulasi dari sistem otomatisasi dibandingkan dengan proses simulasi QKD secara manual. Simulasi QKD secara manual dilakukan oleh dua pihak sebagai pengirim dan penerima. Proses waktu yang diambil merupakan dari langkah pertama pembangkitan angka acak hingga pembentukan bit kunci. Tabel 3 menunjukkan hasil perbandingan waktu sistem otomatisasi.

Tabel 3. Hasil Perbandingan Waktu Proses QKD

Percobaan	Waktu proses sistem otomatisasi	Waktu proses secara manual
1	7 menit 36 detik	33 menit 41 detik
2	7 menit 33 detik	31 menit 39 detik
3	7 menit 35 detik	29 menit 55 detik
4	7 menit 37 detik	30 menit 52 detik
5	7 menit 40 detik	30 menit 38 detik
6	7 menit 34 detik	31 menit 42 detik
7	7 menit 34 detik	30 menit 32 detik
8	7 menit 32 detik	29 menit 58 detik
9	7 menit 33 detik	32 menit 21 detik
10	7 menit 35 detik	31 menit 33 detik
Rata-rata	**7 menit 34,9 detik**	**31 menit 17,1 detik**

Rata rata waktu proses QKD dengan sistem otomatisasi adalah sebesar 7 menit 34,9 detik dan rata rata waktu operasi secara manual adalah sebesar 31 menit 17,1 detik. Berdasarkan data ini didapatkan perbandingan waktu simulasi QKD dengan sistem otomatisasi dengan waktu simulasi secara manual adalah 1 : 4,12. Hal ini menunjukkan sistem otomatisasi yang dibangun berdampak 4 kali lebih cepat dibandingkan dengan operasi perangkat EDU-QCRY1 secara manual.

5. KESIMPULAN

Berdasarkan hasil pengujian dan analisis yang telah dilakukan dalam penelitian ini, maka didapatkan kesimpulan sebagai berikut:

a) EDU-QCRY1 merupakan perangkat simulasi dari protokol BB84 yang merupakan protokol

Quantum Key Distribution. Perangkat EDU-QCRY1 yang dijalankan secara manual memiliki berbagai keterbatasan dalam penggunaannya seperti kecepatan dan keakuratan yang tergantung pada keterampilan dan ketelitian pengguna. Penelitian ini merancang-bangun sebuah sistem otomatisasi perangkat EDU-QCRY1 dengan menggunakan beberapa perangkat tambahan seperti motor servo dan sensor LDR. Hasil dari sistem otomatisasi ini didapatkan bahwa dampak sistem otomatisasi yang empat kali lebih cepat dibandingkan pengoperasian perangkat EDU-QCRY1 secara manual dengan rata rata kecepatan dari sistem otomatisasi adalah 7 menit 34,9 detik dari 100 bit yang ditransmisikan, sedangkan untuk rata rata kecepatan pengoperasian perangkat EDU-QCRY1 secara manual adalah 31 menit 17,1 detik.

b) Terdapat 2 sistem versi yang dibangun, pada masing-masing versi hasil unit testing, integration testing, system testing, dan performance testing telah sesuai dengan yang diharapkan Berdasarkan pengujian yang dilakukan, sistem versi I belum dapat berfungsi dengan baik karena fungsi rotor otomatis belum berhasil dilakukan, sedangkan sistem versi II mampu untuk menjalankan semua tahapan otomatisasi dengan baik. Dari hasil pengambilan data sistem otomatisasi sesuai protokol BB84 terdapat beberapa kegagalan dari penerimaan bit. Dari 100 bit yang dikirimkan, rata rata bit yang diterima oleh sistem adalah 94,8 bit. Sementara akurasi dari pengoperasian secara manual didapatkan akurasi sebesar 100%.

REFERENSI

[1] D. T, "EDU-QCRY1 EDU-QCRY1/M Quantum Cryptography Demonstration Kit Manual," *Thorlabs Discov.*, 2017.

[2] I. Nurhadi, "Quantum Key Distribution (QKD) Protocols : A Survey," *2018 4th Int. Conf. Wirel. Telemat.*, pp. 1–5, 2018.

[3] K. Wai and C. Chan, *Multi-photon Quantum Secure Communication*. .

[4] R. Khairunnisa *et al.*, "Parallelizing Polarization Plate Design for Automating Quantum Key Distribution Device based on EDU-QCRY1," pp. 5–10, 2020.

[5] C. H. Bennett and G. Brassard, "Quantum cryptography : Public key distribution and coin tossing ☆," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, 2014, doi: 10.1016/j.tcs.2014.05.025.

[6] C. Donabela, "Design of Automated Polarization," pp. 439–443, 2020.

[7] G. Mishev, "Analysis of the Automation and the Human Worker , Connection between the Levels of Automation and Different Automation Concepts Grigor Mishev Department of Industrial Engineering and Management , Jönköping School of Engineering , Sweden," 2005.

[8] N. D, "Design Automation of Single Photon Counting Method for Quantum Random Number Generation," pp. 406–411, 2021.

[9] F. Cavaliere, J. Mattsson, and B. Smeets, "The security implications of quantum cryptography and quantum computing," *Netw. Secur.*, vol. 2020, no. 9, pp. 9–15, 2020, doi: 10.1016/S1353-4858(20)30105-7.

[10] M. Nakahara and T. Ohmi, "Quantum Computing From Linear Algebra to Physical Realizations," *Math. Comput.*, vol. 3, pp. 103–439, 2008.

[11] H. Zhang, Z. Ji, H. Wang, and W. Wu, "Survey on Quantum Information Security," pp. 1–36, 2019.

[12] V. J. Gawron, "Automation in Aviation — Definition of Automation," *MITRE Tech. Rep.*, no. 16, pp. 1–9, 2019, [Online]. Available: https://www.mitre.org/sites/default/files/pdf/pr-16-3426-lessons-lost-automation-in-aviation-definition-of-automation.pdf.

[13] M. Y. Abubakar, L. T. Jung, N. M. Zakaria, and O. M. Foong, "Proposed Method for Enhancing Quantum Bit Error Rate Using Quantum key Distribution Technique," pp. 6–11, 2014.

[14] H. F. Li, L. X. Zhu, K. Wang, and K. Bin Wang, "The improvement of QKD scheme based on BB84 protocol," *Proc. - 2016 Int. Conf. Inf. Syst. Artif. Intell. ISAI 2016*, pp. 314–317, 2017, doi: 10.1109/ISAI.2016.0073.

[15] O. Y. Saygili, "Relational Database Management System (RDBMS)," *Introd. to Priv. Cloud using Oracle Exadata Oracle Database*, pp. 5–8, 2020, doi: 10.1201/9780429020902-2.

[16] M. L. Calderon, "The design research methodology as a framework for the development of a tool for engineering design education," *DS 62 Proc. E PDE 2010, 12th Int. Conf. Eng. Prod. Des. Educ. - When Des. Educ. Des. Res. Meet*, no. September, pp. 298–303, 2010.

[17] A. Dennis, B. H. Wixom, and R. M. Roth, "System Analysis and Design 5th Edition," USA: John Wiley & Sons, lnc., 2015.

[18] M. Shafurah, R. Perangkat, and K. Kriptografi, "TUGAS AKHIR Kajian Awal Implementasi Protokol Quantum Key Distribution BB84 dan

SARG04 pada Perangkat EDUQCRY1," 2021.

[19] D. Suyitno, H. O. Asmar, R. W. Wardhani, M. Syahral, D. Ogi, and D. S. C. Putranto, "Analysis of Secure Bit Rate for Quantum Key Distribution based on EDU-QCRY1," Proc. - 2019 Int. Semin. Intell. Technol. Its Appl. ISITIA 2019, pp. 244–247, 2019, doi: 10.1109/ ISITIA.2019.8937140.

[20] A. A. Kadhum and M. M. Abdulhussein, "Implementation dc motor as servomotor by using arduino and optical rotary encoder," *Mater. Today Proc.*, no. xxxx, pp. 4–8, 2021, doi: 10.1016/ j.matpr.2021.03.576.

[21] A. S. Sadun, J. Jalani, and J. A. Sukor, "A comparative study on the position control method of dc servo motor with position feedback by using arduino," *ARPN J. Eng. Appl. Sci.*, vol. 11, no. 18, pp. 10954–10958, 2016