Teknologi Komputasi Kuantum: Revolusi Teknologi Komputasi yang Menjadi Ancaman pada Sistem Kriptografi Saat Ini

Fadel Nararia Rahman
18217005
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
fadelnararia rahman31@gmail.com

***Abstrak*-Teknologi *quantum computing* merupakan pengembangan lebih lanjut dari teknologi komputer generasi saat ini (konvensional). Teknologi ini menawarkan berbagai kemampuan komputasional yang jauh lebih *powerful* pada berbagai bidang. Salah satu aspek yang paling terkena dampak dari adanya teknologi quantum ini adalah pada domain *security* khususnya pada sistem kriptografi yang digunakan saat ini (era *pre-quantum*). Kemungkinan *threats* yang dibawa oleh *quantum computing* pada era post-quantum nantinya menyebabkan diperlukannya tindakan mitigasi agar dampak negatif yang dibawa tidak menyebar luas. Rencana migrasi sistem kriptografi dan pengembangan perangkat IoT lebih lanjut dapat menjadi salah satu solusi dalam tindakan mitigasi tersebut.**

Kata Kunci-Quantum Computing, Sistem Kriptografi, Pre-Quantum, Post-quantum

I. Pendahuluan

I.1. Latar Belakang

Saat ini perkembangan teknologi komputasi yang dikembangkan oleh manusia dapat dikatakan berada pada laju yang amat pesat dan sangat dinamis. Perubahan teknologi komputasi yang dinamis ini terlihat dari beberapa perbandingan yang dapat kita lakukan antara teknologi komputasi yang ada pada saat ini dengan teknologi yang ada pada 5 hingga 10 tahun yang lalu. Walaupun hanya terlewat beberapa tahun, namun teknologi yang menjadi kegunaan oleh manusia secara massal sangat terasa perbedaannya.

Salah satu terobosan teknologi komputasi yang saat ini menjadi perhatian adalah teknologi *quantum computing*. Pada sekitar akhir tahun 2019, salah satu perusahaan teknologi raksasa dunia yakni Google mengumumkan *quantum supremacy* mereka. Hal ini diikuti dengan fakta bahwa mereka berhasil mengembangkan komputer kuantum pertama di dunia. Walaupun teknologi ini sebenarnya bukan merupakan hal yang baru dalam dunia *computer science*, namun realisasi nya menjadi suatu teknologi fisik yang bukan hanya konsep atau teori menyebabkan teknologi komputasi ini kembali menjadi perhatian bagi dunia teknologi.

Banyak sekali kemungkinan yang dapat dimunculkan dengan adanya teknologi komputer quantum yang saat ini tidak mungkin dilakukan dengan menggunakan komputer konvensional, yang berlandaskan pada pengolahan nilai bit 1 atau 0. Banyak riset sains yang menganalisis kemunculan teknologi komputer kuantum ini akan berdampak secara luas dan masif bila pemanfaatannya sudah diimplementasikan dalam skala yang besar. [1] Oleh karena itu dapat dikatakan era penggunaan komputer konvensional ini sebagai *pre-quantum* sedangkan era dimana komputer quantum menjadi lazim disebut dengan *post-quantum*.

Namun dengan kemunculan komputer quantum pertama ini pula, maka muncul juga berbagai riset dan analisis yang muncul mengenai dampak yang mungkin ada dan berpengaruh pada bagaimana teknologi komputasi kita saat ini bekerja. [2] *Domain* keamanan yang menjadi perhatian utamanya adalah *cryptosystem* atau sistem kriptografi yang melandasi protokol keamanan data dan informasi yang digunakan pada sistem saat ini. Menurut [3] dan [4], mulai dari sistem layanan internet, perangkat *Internet of Things*, dan masih banyak lagi perangkat komputasi yang dapat terkena dampaknya khususnya pada bidang *security*. Seperti yang dibahas oleh [5] terkait dengan sistem kriptografi keamanan saat ini yang menjadi ancaman dari munculnya teknologi komputasi kuantum. Metode kriptografi yang umum digunakan saat ini seperti RSA, ECC, TLS, dsb. menjadi rentan untuk dipecahkan atau di-*breakdown* oleh kemampuan komputasi oleh komputer kuantum. Adanya kemungkinan sistem kriptografi *pre-quantum* yang rentan dibobol oleh teknologi komputer kuantum inilah yang menjadi perhatian bahwa pengembangan dan riset sistem kriptografi untuk *post-quantum* menjadi penting untuk dikembangkan. Seperti yang dijelaskan oleh [6] dan [7], bahwa beberapa teknologi atau skema sitem kriptografi yang modern sekiranya masih mampu dalam menangani atau menahan kemungkinan ancaman dari teknologi komputer kuantum ini.

I.2. Rumusan Masalah

Berikut merupakan rumusan masalah yang akan dibahas pada makalah ini.

1. Apa itu teknologi *quantum computing*?
2. Bagaimana dampak yang dapat dibawa oleh teknologi ini khususnya pada *security cryptosystem* untuk sistem informasi dan perangkat IoT saat ini?
3. Bagaimana riset dan pengembangan yang telah dilakukan untuk melakukan mitigasi dampak negatif yang dibawa oleh teknologi *quantum computing*?

I.3. Tujuan

Berikut merupakan tujuan dari pembahasan dan penulisan makalah ini.

1. Memberikan pemahaman mengenai teknologi *quantum computing,*
2. Memberikan gambaran mengenai kemungkinan dampak yang dibawa oleh teknologi *quantum computing* khususnya pada *domain security* yang ada saat ini,
3. Mengetahui riset serta pengembangan teknologi *security cryptosystem* seperti apa yang dapat mencegah berbagai kemungkinan dampak negatif dari *quantum computing* ini.

I.4. Metodologi

Metodologi yang akan digunakan dalam penulisan makalah ini adalah analisis deskriptif terhadap berbagai kajian dan studi literatur pada publikasi relevan yang terdahulu. Penulisan sendiri menjadi empat bagian utama, yakni pendahuluan, kajian dasar teori, pembahasan alternatif solusi, serta kesimpulan dan saran.

II. Dasar Teori

II.1. Teknologi Sistem Kriptografi *Pre-Quantum*

Sistem kriptografi merupakan salah satu teknologi yang dikembangkan untuk menyediakan level keamanan tertentu pada sistem komputasi yang berkaitan dengan pengamanan serta pencegahan dari data atau informasi yang dikelola dari kemungkinan adanya penyalahgunaan pada data yang sifatnya *private* [1]. Menurut [2] teknologi kriptografi saat ini dapat dikatakan sebagai primitif, dikarenakan masih berdasarkan pada tingkat kompleksitas dari besarnya angka faktorisasi yang digunakan untuk melakukan algoritma kriptografi. Tingkat kompleksitas ini yang menentukan bagaimana tingkat kerentanan dari suatu algoritma dalam menahan kemungkinan *brute-force* dari pihak tidak bertanggung jawab untuk membobol keamanan tersebut. Teknik kriptografi saat ini dapat

diklasifikasikan menjadi tiga kelas utama, yakni *asymmetric cryptography, symmetric cryptography,* dan *hash function*.

II.1.1. Kriptografi Asimetrik

Teknologi kriptografi yang menggunakan skema *asymmetric* merupakan salah satu teknik pengamanan data yang menggunakan prinsip pemanfaatan *key* untuk melakukan enkripsi dan dekripsi suatu data. Menurut [3] dan [5] skema kriptografi *asymmetric* ini memiliki dua jenis *key,* yakni *public* dan *private* key yang berbeda. Sehingga dapat dikatakan skema ini memanfaatkan dua jenis kunci yang berbeda (asimetris).

Konsep utama dari skema ini adalah dengan melakukan manipulasi matematis berdasar beberapa parameter tertentu untuk menghasilkan dua kunci yang saling berhubungan tersebut. Satu buah *public key* hanya dapat membuka satu *private key*. Adapun parameter yang dimaksud salah satu nya adalah tingkat kompleksitas dari manipulasi matematis yang digunakan. [3] Semakin kompleks tingkat kesulitan dari faktorisasi matematis yang digunakan serta logaritma matematis yang diterapkan maka algoritma kriptografi tersebut akan menjadi semakin tidak rentan untuk dibobol.

II.1.2. Kriptografi Simetrik

Teknologi kriptografi yang menggunakan skema *symmetric* merupakan salah satu teknik pengamanan data yang menggunakan prinsip pemanfaatan suatu *key* untuk melakukan proses enkripsi dan dekripsi. Menurut [3] skema *symmetric* kriptografi ini menggunakan satu buah *key* yang disebut dengan *secret key* yang sama untuk melakukan kedua proses tersebut. Sehingga dapat dikatakan skema ini menggunakan hanya satu tipe kunci (simetris).

Konsep utama dari skema ini adalah dengan menggunakan manipulasi matematis berdasar parameter lain tertentu untuk menghasilkan kunci *secret* tersebut. Menurut penelitian yang dilakukan oleh [5], diketahui bahwa skema kriptografi ini dapat dikatakan masih cukup valid untuk diterapkan dan diimplementasikan dalam era *post-quantum*. Adapun pengertian valid yang dimaksud adalah skema ini masih cukup kuat untuk menahan berbagai kemungkinan serangan dari teknologi *quantum computer*.

II.1.3. Kriptografi *Hash Function*

Teknologi kriptografi yang menggunakan skema *hash function* merupakan salah satu teknik pengamanan data yang menggunakan suatu fungsi matematis untuk mengubah data input yang diperlukan untuk menjadi suatu kode *hash* agar dapat merahasiakan informasi yang disimpan. Sedikit berbeda dengan skema kriptografi sebelumnya yang memanfaatkan *key* untuk melakukan enkripsi dan dekripsi, mekanisme pengecekan yang dimiliki oleh skema ini adalah dengan bergantung pada *output* dari fungsi *hash* tersebut.

Data yang disimpan dapat dinilai sebagai data yang benar dan valid selama kode *hash* yang dihasilkan tidak berubah sama sekali selama proses transmisi data berlangsung. Menurut [3], sama seperti skema *symmetric cryptography*, skema ini juga dinilai cukup valid untuk digunakan dan diimplementasikan dalam era *post-quantum*. Dapat dikatakan valid karena skema kriptografi ini cukup rentan untuk dibobol oleh teknologi komputer kuantum sekalipun, berhubung fungsi *hash* yang dilakukan bersifat *irreversible*.

II.2. Teknologi *Quantum Computing*

Teknologi *quantum computing* adalah salah satu pengembangan teknologi pada bidang komputer yang berdasarkan pada prinsip fisika kuantum. Menurut [3] yang dimaksud dari teknologi *quantum* pada komputer adalah suatu perangkat yang memiliki kemampuan untuk melakukan kekuatan pemrosesan yang jauh lebih besar dibanding dengan kemampuan komputasional yang dimiliki oleh komputer konvensional. Hal ini dapat dicapai dikarenakan set struktur perangkat dari komputer *quantum* ini sangat berbeda dengan yang dimiliki oleh komputer konvensional.

Adapun kemampuan yang dimiliki oleh komputer *quantum* paling kentara menurut [1] adalah kemampuan komputasinya untuk menyelesaikan perhitungan permasalahan matematis yang sangat kompleks dalam waktu polinomial yang sangat singkat. Berdasarkan [3], kemampuan komputer *quantum* ini disebabkan pada penggunaan prinsip kombinasi *logic states* yang berbeda dengan komputer konvensional. Pada komputer *quantum*, *logic states* tersebut terbagi menjadi tiga, yakni: *state* 1, *state* 0, dan *state* 1 dan 0 dalam waktu yang bersamaan. Formasi seperti ini disebut sebagai superposisi dalam teori fisika kuantum. Kombinasi tiga *states* tersebut yang disebut dengan *quantum bits* atau *qubits*.

II.3. Teknologi *Internet Of Things*

Teknologi *Internet of Things* atau disingkat IoT merupakan salah satu pengembangan perangkat teknologi yang saat ini berkembang dengan cukup dinamis seiring dengan revolusi industri ke-4. Menurut [4], teknologi ini menawarkan set *network* baru yang sangat adaptif dan dinamis dengan menambahkan kemampuan konektivitas pada perangkat melalui penanaman komponen komputasi tambahan seperti sensor dan aktuator. Implementasi teknologi ini tersebar pada berbagai domain yang ada saat ini, seperti transportasi pintar, otomasi perangkat rumah, otomasi manufaktur, dsb.

Salah satu perhatian yang saat ini sedang dianalisis oleh peneliti menurut [4] dan [5] adalah terkait dengan keamanan data yang dikelola oleh perangkat tersebut. Keterbatasan perangkat yang dimiliki oleh perangkat IoT ini utamanya disebabkan karena umumnya perangkat IoT dibatasi oleh kemasan perangkat yang terbatas. Hal ini menimbulkan adanya *resource constraint* untuk menambahkan tambahan komponen lainnya khususnya untuk keamanan data. Selain itu kemampuan komputasional yang dimiliki oleh perangkat IoT juga terbatas karena tidak dapat dikatakan selevel dengan komputer konvensional.

III. Pembahasan

III.1. Kelemahan Sistem Kriptografi Saat ini dan Ancaman Kuantum

Berdasarkan kajian literatur pada bagian sebelumnya, dapat diketahui bahwa teknologi kriptografi yang ada dan digunakan saat ini relatif rentan untuk dibobol dengan menggunakan teknologi komputer *quantum*. Menurut [1] sistem keamanan yang ada saat ini dapat dikatakan sebagai primitif dan telah pada kondisi yang memerlukan penggantian segera. Berikut merupakan pembahasan dari tiap sistem kriptografi yang ada saat ini.

III.1.1. Pembahasan Sistem Kriptografi *Pre-Quantum*

Skema kriptografi pertama yang merupakan *asymmetric* ini memiliki *drawbacks* khususnya pada kemungkinan suatu perangkat komputasi untuk dapat memecahkan manipulasi matematis tersebut dan menemukan kunci yang dapat membobol algoritma keamananya. Menurut [3] kekuatan skema kriptografi ini masih tidak akan mampu menyediakan level keamanan yang cukup bila dibandingkan dengan *attack* yang mungkin dilakukan oleh teknologi *quantum computing*.

Kemudian untuk skema kriptografi berupa *symmetric*, berdasarkan penelitian yang dilakukan oleh [5] dapat diketahui bahwa skema ini bisa dikatakan cukup valid

untuk menahan serangan komputer *quantum*. Hal ini didasari oleh analisis mengenai metode untuk meningkatkan level keamanan yang dimiliki oleh skema ini. Parameter yang dapat dipertimbangkan salah satunya adalah dengan meningkatkan *key size/output* yang dihasilkan. Melalui metode ini maka tingkat kompleksitas dari kunci yang akan dihasilkan untuk melakukan proses yang dijelaskan pada bagian sebelumnya akan menjadi semakin rumit dan susah untuk dipecahkan.

Adapun untuk skema kriptografi terakhir yang berupa *hash function*, kurang lebih sama dengan skema *symmetric* yakni dapat dikatakan cukup valid untuk dikembangkan untuk era *post-quantum* [3]. Namun tetap saja diperlukan beberapa pengembangan tertentu untuk meningkatkan level keamanan yang dapat diberikan oleh skema kriptografi ini. Meningkatkan *size output* dari *hash function* minimal dua kali lipat, menurut [5] sudah mampu menahan usaha *attacks* yang mungkin dilakukan dengan menggunakan komputer quantum sekalipun. Hal ini dikarenakan semakin besar nilai kode *hash* yang dihasilkan, maka semakin rumit dan kompleks pula informasi tersebut tersimpan didalamnya.

III.1.2. Analisis Bahaya dari Teknologi Komputer *Quantum*

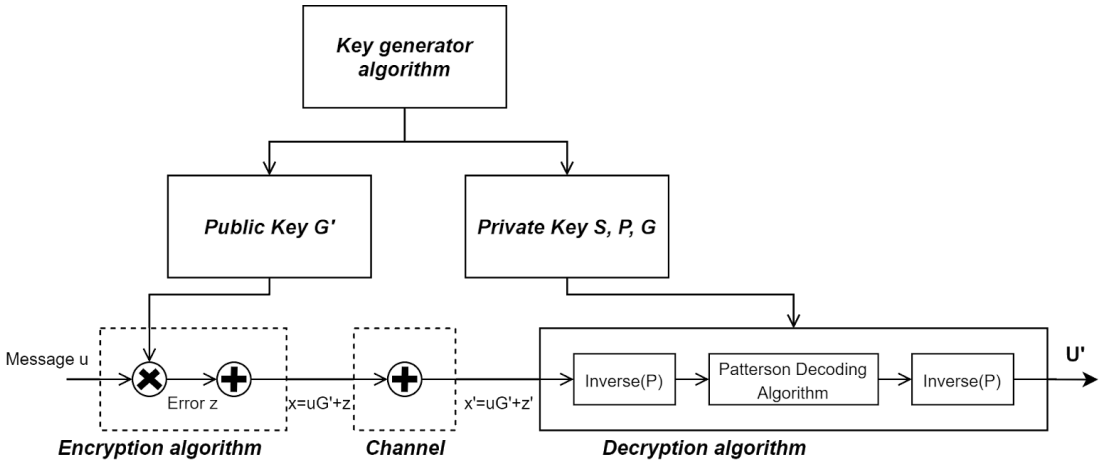
Berdasarkan penelitian yang dilakukan oleh [3] diketahui bahwa terdapat beberapa macam *threats* yang dapat ditimbulkan dari adanya teknologi komputer *quantum* ini. Ancaman yang mungkin ditimbulkan dari adanya teknologi ini adalah walaupun besaran dimensi dari kunci kriptografi yang digunakan sudah berlipat, namun skema ini tidak dapat bertahan lama karena kemampuan dari komputer *quantum* juga akan semakin meningkat seiring waktu. Seperti yang diteliti oleh Mosca [3] sebagai contoh sistem RSA-2048 akan dapat dibobol dengan *probability* sebesar 1/7 hingga tahun 2026 dan menjadi lebih besar hingga menjadi ½ pada tahun 2031.

III.2. *Post-Quantum:* Alternatif Sistem Kriptografi

Berdasarkan analisis yang telah diketahui pada bagian sebelumnya mengenai kelemahan sistem kriptografi *pre-quantum* yang ada saat ini maka diperlukan penelitian dan pengembangan sistem kriptografi yang mampu menahan kemungkinan *attack* lebih lanjut khususnya yang berasal dari komputer *quantum*. Berikut merupakan analisis pada beberapa alternatif skema kriptografi yang telah diteliti dan diajukan untuk dapat digunakan pada era *post-quantum*, berdasarkan penelitian oleh [5].

III.2.1. Alternatif Kriptosistem 1 : *Code Based*

Skema sistem kriptografi ini menggunakan prinsip teori *error-correction codes* untuk menjalankan fungsinya. Skema ini merupakan pengembangan dari sistem kriptografi yang memanfaatkan suatu *key* yang berasal dari *asymmetric* dan *symmetric cryptography*, yakni berdasarkan pada penggunaan kode tertentu untuk melakukan proses enkripsi dan dekripsi [5]. Berdasarkan pada analisis dan penelitian dalam [7] salah satu contoh kriptografi dari kategori *code based* yang dapat digunakan secara luas pada era *post-quantum* adalah McEliece *cryptosystem*. Hal ini didasarkan pada penggunaan prinsip Goppa *Code* untuk dapat memberikan level *security* yang setara dengan *threats* dari *quantum* komputer, serta menyelesaikan pengolahan proses enkripsi dan dekripsi dalam waktu yang relatif singkat. Berikut merupakan mekanisme McEliece [7].



Gambar 1 McEliece *Cryptosystem* [7]

III.2.2. Alternatif Kriptosistem 2 : *Supersingular Elliptic Curve Isogeny Based*

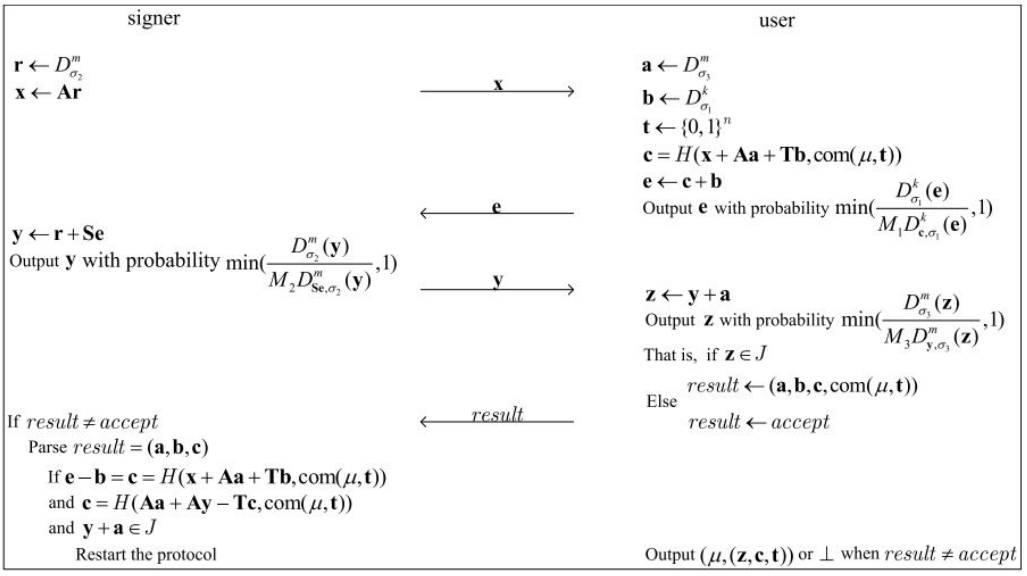
Sistem kriptografi ini berdasarkan pada prinsip protokol *isogeny* untuk *ordinary elliptic curve* yang diajukan dalam penelitian oleh [5]. Mekanisme yang digunakan adalah prinsip kurva matematis yang digunakan berbentuk *non-commutative*, sedangkan *attacks* yang ada *relies* pada *commutative form*. Namun terdapat *drawbacks* dari skema ini yaitu memiliki *key size* yang terdiri dari ribuan *bits*, sehingga mungkin kurang sesuai untuk perangkat IoT yang memiliki keterbatasan kemampuan komputasional.

III.2.3. Cryptosystem #3 : *Hybrid*

Sistem kriptografi ini merupakan gabungan dari sistem kriptografi yang ada pada *pre-quantum* dan *post-quantum*. Tujuannya adalah untuk dapat memberikan level keamanan secara *end-to-end* dan ganda pada berbagai lapis sistem yang menggunakan protokol keamanan salah satu dari era tersebut [5]. Namun skema ini baru dapat diimplementasikan pada era *full post-quantum.*

III.2.4. Cryptosystem #4 : *Lattice-Based*

Sistem kriptografi ini menggunakan prinsip yang berdasarkan pada *lattices* atau yang merupakan set poin pada suatu struktur n-dimensional *spaces* [5]. Salah satu contoh skema yang mendukung sistem ini mampu memberikan level keamanan untuk kemungkinan *attacks* dari *quantum* komputer adalah adanya skema *blind signature* yang diajukan oleh [6]. Hal ini dilandasi oleh fakta bahwa kebutuhan untuk *digital signature* menjadi penting dalam protokol komunikasi melalui internet saat ini. Dikutip dari [6] berikut merupakan gambaran mekanisme skema *blind signature*.



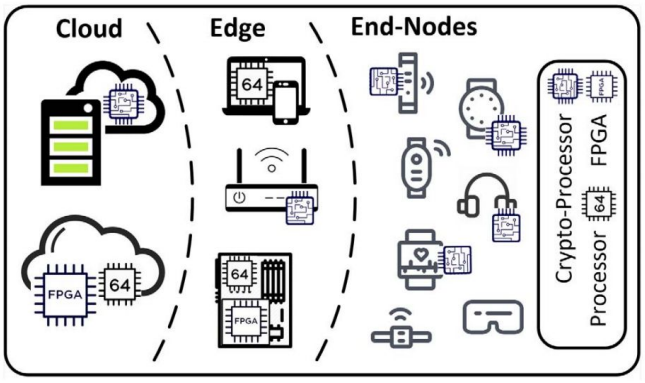
Gambar 2 Protokol *Blid Signature Lattice-Based* [6]

III.2.5. Cryptosystem #5 : *Multivariate*

Sistem kriptografi ini didasarkan pada prinsip sistem penyelesaian dari persamaan *multivariate* [5]. Kelebihan yang dimiliki skema ini yakni telah terbukti sebagai *NP-hard* atau *NP-complete*. Namun skema ini memiliki *drawbacks* khususnya implementasi pada perangkat yang memiliki keterbatasan kemampuan komputasional berhubung skema ini memerlukan pengolahan matematis yang cukup kompleks.

III.3. *Post-Quantum:* Proyek Inisiatif untuk Sistem Kriptografi pada IoT

Selain membahas mengenai beberapa alternatif sistem kriptografi yang dapat diterapkan pada *post-quantum*, maka untuk perangkat IoT sendiri juga perlu dilakukan penyesuaian dan pengembangan agar dapat memenuhi kriteria *security* dari *post-quantum*. Berikut merupakan penelitian oleh [4] mengenai *projects* yang dapat diterapkan untuk mengembangkan perangkat IoT dari domain *security* melalui pengembangan *cryptoprocessor*.

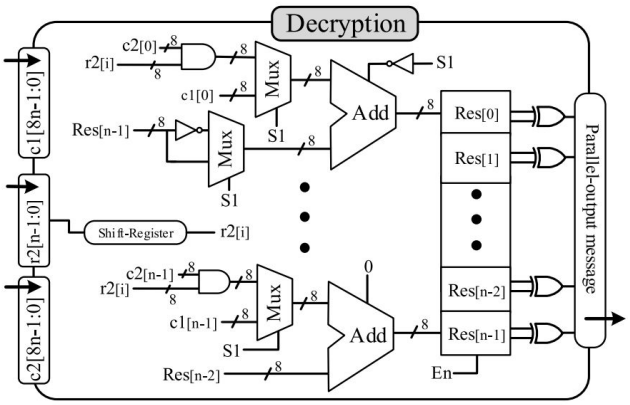


Gambar 3 Arsitektur Jaringan IoT dan *Resource Hardware* Tiap *Layer* [4]

Pengembangan kriptoprosesor yang dibahas dibagi menjadi dua arsitektur utama, masing-masing dibedakan berdasarkan pada fokus arsitektur perangkat IoT yang memiliki perbedaan. Arsitektur pertama merupakan *high-speed architecture*, merupakan perangkat yang berfokus pada *high performance* dan *low complexity*. Arsitektur kedua merupakan *ultra low-power* yang ditargetkan untuk perangkat yang memiliki *limited energy resources* [4].

III.3.1. Proyek 1 : *Ring-BinLWE High Speed Architecture*

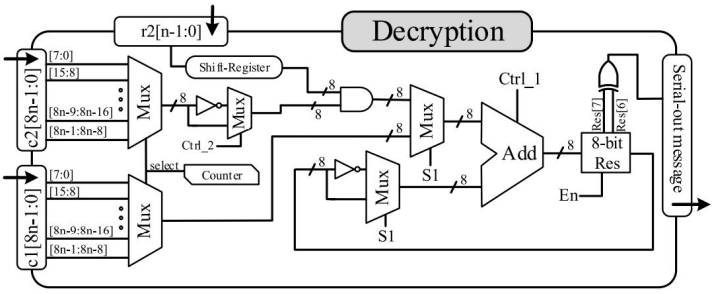
Berdasarkan penelitian diketahui bahwa tipe arsitektur perangkat IoT ini merupakan *high performance device*. Oleh karena itu komponen yang diajukan merupakan gabungan dari tiga fungsi utama yakni *key generation*, *encryption,* dan *decryption*. Berikut merupakan gambaran arsitektur untuk melakukan dekripsi oleh perangkat, dikutip dari [4].



Gambar 4 Arsitektur Fase Dekripsi untuk *High-Speed Device* [4]

III.3.2. Proyek 2 : *Ring-BinLWE Ultralightweight Architecture*

Berbeda dengan arsitektur sebelumnya, pada arsitektur ini berfokus pada perangkat yang memiliki limitasi dari segi *power energy* dan *computational power*. Oleh karena itu untuk membuat penyederhanaannya, maka ketiga fungsi yang dilakukan dijadikan menjadi 1 komponen utama yang merangkap keseluruhannya. Berikut merupakan gambaran arsitektur untuk melakukan dekripsi oleh perangkat, dikutip dari [4].



Gambar 5 Arsitektur Fase Dekripsi untuk *Ultralightweight Device* [4]

IV. Penerapan Solusi

IV.1. Rancangan Persiapan Menuju *Post-Quantum*

Berdasarkan analisis yang telah dilakukan pada bagian sebelumnya, telah diketahui beberapa alternatif solusi yang dapat digunakan untuk mempersiapkan sistem kriptografi untuk era *post-quantum* beserta inisiatif proyek pengembangan perangkat IoT yang dapat dilakukan. Maka selanjutnya yang perlu dilakukan adalah mengurutkan prioritas alternatif solusi mana yang dapat dilakukan dalam kaitannya untuk melaksanakan migrasi sistem kriptografi dari *pre-quantum* menjadi *post-quantum*.

IV.1.1. Plan Migrasi Sistem Kriptografi

Cakupan migrasi yang dimaksud untuk melakukan persiapan sistem kriptografi dari *pre-quantum* menuju *post-quantum* yang dibahas pada makalah kali ini mencakup sistem protokol keamanan pada sistem layanan internet dan perangkat IoT yang menjadi salah satu komponen dari layanan itu sendiri. Langkah pertama yang dilakukan adalah menentukan prioritas penerapan alternatif solusi sistem kriptografi tersebut dari yang paling *feasible* untuk diterapkan dan paling luas dampak yang diberikan.

Berikut merupakan pembahasan mengenai prioritas penerapan sistem kriptografi berdasarkan pada beberapa alternatif yang telah dibahas pada bagian sebelumnya.

a. Prioritas 1: Pengembangan *Code-Based Cryptography*

   Skema kriptografi yang berupa *code-based* merupakan prioritas pertama, dikarenakan sistem kriptografi yang ada pada *pre-quantum* saat ini mayoritas menggunakan kode tertentu untuk melakukan proses enkripsi dan dekripsi. Hal ini kemudian menimbulkan suatu *needs* bahwa skema sistem kriptografi pertama yang perlu menjadi *post-quantum*, adalah pengembangan lebih lanjut dari sistem yang sudah ada saat ini (*existing*). Kebutuhan ini didasarkan pada perubahan tersebut harus bersifat perlahan-lahan, sehingga komponen-komponen awal yang menerapkan sistem kriptografi ini nantinya tidak akan membutuhkan penyesuaian yang signifikan dan memakan biaya tinggi.

b. Prioritas 2: Pengembangan *Lattice-Based Cryptography*

   Kemudian prioritas selanjutnya adalah pengembangan dan penerapan sistem kriptografi yang berlandaskan skema *lattice*. Hal ini didasarkan pada kebutuhan sistem saat ini khususnya yang berkaitan dengan *digital signature* yang semakin berkembang pada berbagai domain, maka skema ini perlu untuk menjadi fokus selanjutnya dalam era *post-quantum*.

c. Prioritas 3: Pengembangan *Multivariate* dan *Supersingular Elliptic Curve Isogeny Based Cryptography*

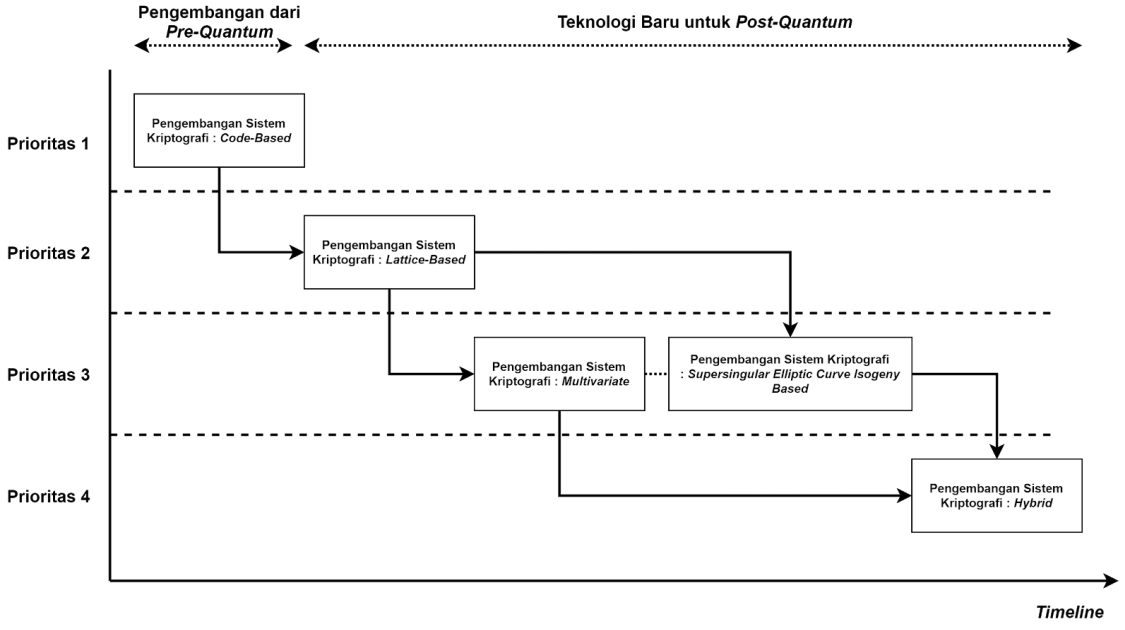
   Kedua skema kriptografi ini yang berdasarkan skema *multivariate* dan *supersingular elliptic curve isogeny based*, dapat dikatakan membutuhkan

usaha yang lebih banyak untuk diterapkan dan diimplementasikan pada sistem layanan internet saat ini. Khususnya hal ini disebabkan karena kedua skema ini membutuhkan perangkat komputasi yang cukup *powerful* dibanding dengan yang ada pada kondisi rata-rata saat ini. Masih perlu dilakukan riset dan pengembangan agar dapat dilakukan simplifikasi pada skema kriptografi ini sehingga dapat diterapkan secara luas.

d. Prioritas 4: Pengembangan *Hybrid Cryptography*

Skema kriptografi *hybrid* merupakan gabungan dari sistem kriptografi yang berasal dari era *pre-quantum* dengan *post-quantum*. Skema ini menjadi prioritas terakhir dikarenakan pengembangannya membutuhkan keseluruhan skema kriptografi diatas untuk sudah *established* terlebih dahulu. Sehingga komponen-komponen sistem layanan yang nantinya akan menggunakan skema ini telah memiliki beberapa parameter standar yang mampu untuk menjalankan skema ini. Faktor lain yang menjadi pertimbangan juga adalah bahwa skema ini merupakan langkah akhir yang nantinya akan menjadi landasan pengembangan lebih lanjut lagi untuk era setelah *post-quantum*.

Adapun berikut merupakan gambaran mengenai rencana migrasi sistem kriptografi *pre-quantum* menuju *post-quantum* yang menjadi solusi pada makalah ini.



Gambar 6 Rencana Migrasi Sistem Kriptografi Menuju *Post-Quantum*

IV.1.2. Perubahan yang Perlu Dilakukan pada *Pre-Quantum IoT Devices*

Kemudian untuk solusi pengembangan pada perangkat IoT *pre-quantum*, berdasarkan alternatif solusi yang telah dibahas pada bagian sebelumnya maka dapat diketahui bahwa pengembangan komponen pada perangkat IoT itu sendiri seperti *cryptoprocessor* dapat memberikan level keamanan yang cukup untuk menghadapi kondisi *post-quantum*. Hal ini tentu dilakukan bersamaan dengan penggunaan sistem kriptografi yang telah dikembangkan dan disesuaikan seperti yang telah dijabarkan sebelumnya. Proyek inisiatif yang telah dikembangkan oleh [4], dapat menjadi salah satu proyek pelopor untuk mengembangkan keamanan pada tiap perangkat IoT yang menjadi cukup banyak digunakan khususnya pada kondisi revolusi industri 4.0 ini.

IV.2. Analisis Dampak Persiapan Menuju *Post-Quantum*

Berikut merupakan beberapa analisis kemungkinan dampak yang akan terjadi dari beberapa perspektif terkait dengan migrasi sistem kriptografi dari *pre-quantum* menuju *post-quantum* yang diusulkan pada makalah ini.

IV.2.1. Perspektif perangkat

Berdasarkan sudut pandang perangkat yang merupakan komponen dari sistem layanan yang akan menerapkan dan mengimplementasikan sistem kriptografi yang disebutkan diatas maka kurang lebih akan terdapat beberapa penyesuaian yang perlu dilakukan. Penyesuaian yang diperlukan mencakup pembaharuan sistem perangkat lunak yang bekerja agar dapat mengenali perintah-perintah yang akan diterapkan oleh skema kriptografi dan juga peningkatan kemampuan komputasional perangkat seperti pembaharuan komponen perangkat agar dapat memberikan level kinerja yang sesuai dan setara dengan era nya.

IV.2.2. Perspektif sistem

Adapun dari perspektif sistem layanan yang akan menerapkan sistem kriptografi tersebut sebagai protokol komunikasi antara komponen-komponennya, maka penyesuaian yang mungkin diperlukan adalah lebih pada pembaharuan mekanisme integrasi sistem keamanan secara terpusat. Setiap komponen nantinya akan menerapkan sistem kriptografi yang telah diperbaharui, oleh karenanya perlu

dilakukan beberapa konfigurasi lanjutan mengenai integrasi komponen dari perspektif sistem.

V. Kesimpulan

Berdasarkan keseluruhan pembahasan dan analisis yang telah dilakukan pada bagian sebelumnya di makalah ini, maka dapat diketahui bahwa keberadaan teknologi *quantum computing* secara riil merupakan salah satu momentum yang menentukan bagi sistem komputasi layanan yang ada saat ini, karena berbagai kemungkinan dampak yang dapat ditimbulkannya khususnya pada domain *security*. Sistem kriptografi yang berperan dalam memberikan level keamanan tertentu pada berbagai komponen sistem layanan yang terkait satu sama lain, menjadi salah satu aspek yang terkena dampaknya dikarenakan adanya *threats* dari komputer *quantum* ini. Namun berdasarkan berbagai penelitian yang dikaji, dapat diketahui bahwa dengan pengembangan dan riset lebih lanjut, *threats* yang muncul tadi dapat dilakukan tindakan mitigasi dengan melakukan beberapa usaha migrasi sistem kriptografi itu sendiri. Sehingga ketika nantinya komputer *quantum* benar-benar sudah digunakan secara massal dan efisien, maka sistem layanan lainnya akan memiliki level *security* yang setara dan mumpuni untuk menahan berbagai macam *attacks* dari *quantum computer* tersebut.

Referensi

[1] M. Baldi, P. Santini and G. Cancellieri,"Post-quantum cryptography based on codes: State of the art and open challenges," *2017 AEIT International Annual Conference*, Cagliari, 2017, pp. 1-6.

[2] J. Bobrysheva and S. Zapechnikov,"Post-Quantum Security of Communication and Messaging Protocols: Achievements, Challenges and New Perspectives," *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, Saint Petersburg and Moscow, Russia, 2019, pp. 1803-1806.

[3] B. Arslan, M. Ulker, S. Akleylek and S. Sagiroglu,"A study on the use of quantum computers, risk assessment and security problems," *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, Antalya, 2018, pp. 1-6.

[4] S. Ebrahimi, S. Bayat-Sarmadi and H. Mosanaei-Boorani,"Post-Quantum Cryptoprocessors Optimized for Edge and Resource-Constrained Devices in IoT,"in *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5500-5507, June 2019.

[5] T. M. Fernández-Caramés,"From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things,"in *IEEE Internet of Things Journal*.

[6] P. Zhang, H. Jiang, Z. Zheng, P. Hu and Q. Xu, "A New Post-Quantum Blind Signature From Lattice Assumptions," in *IEEE Access*, vol. 6, pp. 27251-27258, 2018.

[7] S. H. Odin Hashemi and G. A. Hodtani, "A Modified McEliece Public-Key Cryptosystem Based On Irregular Codes Of QC-LDPC and QC-MDPC," *2019 27th Iranian Conference on Electrical Engineering (ICEE)*, Yazd, Iran, 2019, pp. 1373-1376.