PENGEMBANGAN APLIKASI DIGITAL SIGNATURE BERBASIS QRNG-ECC UNTUK AUTENTIKASI PESAN TERHADAP ANCAMAN KOMPUTASI KUANTUM

Agil Almunawar, Aulia Khamas Heikhmakhtiar
Rekayasa Pertahanan Siber, Universitas Pertahanan RI
Kawasan IPSC Sentul, Sukahati, Kec. Citeureup, Kabupaten Bogor, Indonesia
Agilmunawar011000@gmail.com

ABSTRAK

Perkembangan teknologi komputasi kuantum menghadirkan ancaman signifikan terhadap sistem kriptografi konvensional, khususnya pada algoritma seperti RSA dan Elliptic Curve Cryptography (ECC). Untuk menjawab tantangan ini, penelitian ini mengembangkan sebuah aplikasi tanda tangan digital (digital signature) berbasis ECC yang diperkuat dengan Quantum Random Number Generator (QRNG) guna meningkatkan autentikasi pesan terhadap potensi serangan kuantum. Berbeda dengan Pseudorandom Number Generator (PRNG), QRNG menghasilkan bilangan acak sejati berdasarkan fenomena mekanika kuantum, sehingga memberikan kualitas keacakan yang lebih tinggi pada proses pembuatan kunci kriptografi. Penelitian ini mencakup pembuatan kunci ECC menggunakan QRNG dan PRNG, perhitungan entropi untuk mengukur kualitas keacakan, implementasi proses penandatanganan pesan menggunakan kunci privat ECC, serta proses verifikasi tanda tangan menggunakan kunci publik QRNG. Evaluasi dilakukan melalui simulasi dan pengujian aplikasi berbasis antarmuka grafis untuk membandingkan performa QRNG dan PRNG dalam skenario autentikasi digital. Hasil penelitian menunjukkan bahwa integrasi QRNG dalam proses digital signature dapat meningkatkan keamanan dan integritas pesan secara signifikan, serta menjadi landasan penting menuju sistem kriptografi yang tahan terhadap serangan kuantum.

Kata kunci : *Quantum Random Number Generator (QRNG), Elliptic Curve Cryptography (ECC), Digital Signature, Autentikasi Pesan, Komputasi Kuantum, Keamanan Kriptografi*

1. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong pertumbuhan eksponensial dalam komunikasi digital, sehingga menjadikan aspek keamanan siber sebagai elemen krusial dalam berbagai sistem informasi modern. Salah satu mekanisme utama dalam menjaga kerahasiaan dan integritas data adalah melalui penggunaan Transport Layer Security (TLS) yang secara luas mengandalkan algoritma kriptografi seperti RSA dan ECC. Namun, kemunculan komputasi kuantum membawa ancaman nyata terhadap skema kriptografi klasik ini, terutama melalui Algoritma Shor yang mampu memecahkan faktor prima dan logaritma diskret secara eksponensial lebih cepat dibandingkan komputer klasik [1].

Dalam konteks ini, perhatian mulai bergeser pada solusi kriptografi yang tahan terhadap komputasi kuantum, termasuk pendekatan seperti Quantum Key Distribution (QKD) dan Post-Quantum Cryptography (PQC) [1][2].

Meskipun QKD menawarkan tingkat keamanan teoretis tinggi, implementasinya masih menghadapi tantangan besar dalam hal infrastruktur dan biaya. Sebagai alternatif yang lebih aplikatif, pemanfaatan QRNG menjadi solusi strategis karena dapat meningkatkan kualitas keacakan dalam proses pembangkitan kunci, yang selama ini masih mengandalkan PRNG [1][4].

QRNG menggunakan fenomena mekanika kuantum seperti quantum noise atau photon emission untuk menghasilkan bilangan acak sejati (true randomness), yang secara statistik memiliki entropi lebih tinggi daripada PRNG.

Selain aspek pertukaran kunci dalam TLS, tantangan autentikasi dan integritas pesan juga menjadi sorotan penting. Penerapan digital signature menjadi krusial dalam menjamin keaslian komunikasi dan mendeteksi manipulasi data. Namun, sebagian besar algoritma tanda tangan digital saat ini, seperti DSA dan RSA, menghadapi ancaman besar dari algoritma kuantum. Untuk menjawab tantangan ini, berbagai penelitian mengusulkan arsitektur digital signature yang lebih adaptif, seperti pendekatan berbasis ECC yang dikombinasikan dengan teknik optimasi aritmatika dan penghapusan operasi modulo inverse [5][6][7].

Penelitian ini bertujuan untuk mengembangkan sebuah sistem aplikasi digital signature berbasis kombinasi QRNG dan ECC yang mampu memberikan autentikasi kuat terhadap pesan digital serta meningkatkan ketahanan terhadap ancaman serangan kuantum. Sistem yang diusulkan akan mengintegrasikan pembangkitan kunci ECC dengan sumber keacakan dari QRNG untuk meningkatkan kualitas kunci kriptografi, sekaligus menerapkan proses tanda tangan digital yang efisien dan dapat diverifikasi oleh pihak penerima. Rancang bangun ini juga diuji melalui simulasi dan pengukuran entropi untuk membandingkan kualitas keacakan antara QRNG dan PRNG, serta dievaluasi efektivitasnya dalam skenario komunikasi pesan.

Dengan pendekatan ini, diharapkan sistem yang dikembangkan tidak hanya relevan untuk era pasca-kuantum, tetapi juga dapat diimplementasikan pada berbagai infrastruktur kritis yang membutuhkan keamanan komunikasi tingkat tinggi.

2. TINJAUAN PUSTAKA

Dalam bagian ini, menjelaskan konsep-konsep dasar yang menjadi acuan dalam merumuskan permasalahan, menyusun kerangka berpikir, serta mendukung analisis terhadap data penelitian.

2.1. Quantum Computing dan Ancaman terhadap Kriptografi Klasik

Perkembangan pesat komputasi kuantum menghadirkan tantangan baru terhadap kriptografi konvensional. Algoritma kuantum seperti Shor memungkinkan pemfaktoran bilangan besar secara efisien, yang mengancam keamanan sistem berbasis RSA dan ECC. Dalam konteks ini, protokol keamanan yang saat ini digunakan dalam sistem komunikasi digital menjadi rentan terhadap serangan berbasis komputasi kuantum [8].

2.2. QRNG) vs PRNG

Sumber bilangan acak yang digunakan dalam kriptografi memiliki peran sentral dalam menentukan kekuatan keamanan sistem. PRNG bersifat deterministik dan rentan terhadap prediksi, sedangkan QRNG memanfaatkan fenomena kuantum seperti fluktuasi vakum atau foton untuk menghasilkan bilangan acak sejati (*true randomness*) [9].

Studi oleh Ge et al. menunjukkan efektivitas QRNG berbasis coherent optical receiver dalam menghasilkan entropi tinggi yang ideal untuk aplikasi kriptografi.

2.3. Elliptic Curve Cryptography (ECC) sebagai Kriptografi Ringan

ECC menjadi solusi populer untuk implementasi kriptografi pada perangkat dengan keterbatasan sumber daya, seperti IoT dan mobile. Efisiensi ECC yang tinggi dalam menghasilkan keamanan yang kuat dengan ukuran kunci kecil menjadikannya pilihan utama dalam desain sistem keamanan modern [10].

2.4. Digital Signature dalam Sistem Keamanan Modern

Digital signature digunakan untuk memastikan integritas dan autentikasi pesan dalam berbagai sistem digital. Berbagai arsitektur dan algoritma telah dikembangkan untuk meningkatkan efisiensi dan keamanan digital signature, termasuk pendekatan baru yang menggabungkan teknik tanpa operasi invers modular dan kombinasi dengan watermarking [11].

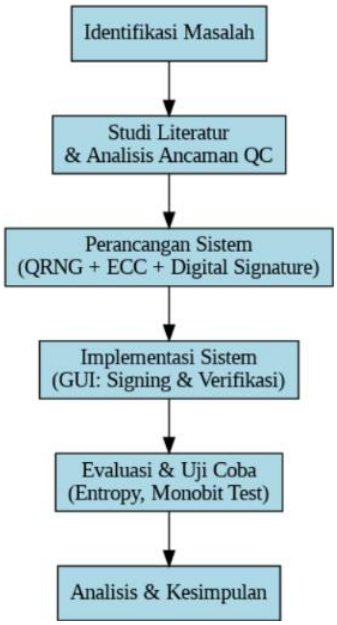
2.5. Integrasi QRNG-ECC untuk Autentikasi Pesan

Penelitian ini memadukan keunggulan ECC dan QRNG untuk membangun sistem tanda tangan digital yang lebih aman dan tahan terhadap ancaman kuantum. QRNG digunakan sebagai sumber entropi dalam pembentukan kunci publik ECC, sedangkan PRNG digunakan untuk kunci privat. Pendekatan ini bertujuan untuk memperkuat proses autentikasi pesan, sekaligus menjadi solusi transisi menuju era kriptografi pasca-kuantum [12].

2.6. Keterkaitan dengan Penelitian Terdahulu

Penelitian sebelumnya telah membahas implementasi QRNG untuk TLS, pengembangan QKD untuk komunikasi aman, serta evaluasi PRNG dalam konteks post-quantum security. Namun, masih terbatas penelitian yang mengkaji aplikasi digital signature menggunakan QRNG-ECC dalam konteks autentikasi pesan secara praktikal dan terukur seperti yang dilakukan dalam penelitian ini.

3. METODE PENELITIAN



Gambar 1. Metode Penelitian

Penelitian ini menggunakan pendekatan eksperimental dengan beberapa tahapan, yakni identifikasi permasalahan, perancangan sistem, implementasi, dan evaluasi. Tujuan utama dari penelitian ini adalah membangun sistem digital signature berbasis QRNG-ECC yang mampu memberikan autentikasi pesan dengan kekuatan kriptografi yang tahan terhadap ancaman komputasi kuantum.

3.1. Identifikasi Masalah dan Studi Literatur

Tahapan awal dilakukan dengan mengkaji kelemahan sistem kriptografi klasik (RSA dan ECC) terhadap ancaman komputasi kuantum, serta mengevaluasi kebutuhan akan sumber bilangan acak yang aman (true randomness). Studi literatur dilakukan terhadap berbagai pendekatan QRNG, digital signature, dan sistem kriptografi modern untuk mendapatkan dasar teoritis dan teknis dalam pengembangan sistem.

3.2. Perancangan Sistem

Sistem yang dikembangkan memanfaatkan QRNG untuk menghasilkan kunci publik dalam algoritma ECC. Sedangkan PRNG digunakan untuk pembuatan kunci privat. QRNG dipilih untuk meningkatkan entropi dan ketidakpastian kunci publik yang digunakan dalam proses verifikasi tanda tangan digital. Digital signature dibentuk menggunakan algoritma ECDSA (Elliptic Curve Digital Signature Algorithm).

3.3. Implementasi Sistem

Implementasi sistem dilakukan dengan membangun aplikasi GUI berbasis Python menggunakan Tkinter, serta library kriptografi modern. Sistem terdiri dari dua tahap utama:

a. Tahap 1 (Signing): Pengguna memasukkan pesan, sistem akan melakukan proses generate kunci (PRNG dan QRNG), lalu menandatangani pesan menggunakan ECDSA.
b. Tahap 2 (*Verification*) : Sistem memverifikasi keabsahan tanda tangan digital menggunakan kunci publik hasil QRNG.

Sistem juga menyimpan kunci, pesan, dan signature ke file eksternal agar dapat diuji ulang dan divalidasi

3.4. Evaluasi Sistem

Evaluasi dilakukan terhadap dua aspek:

a. Kualitas Randomness: Menggunakan uji Shannon Entropy dan Monobit Test (NIST SP 800-22) terhadap output PRNG dan QRNG.
b. Keakuratan Digital Signature: Melalui proses verifikasi terhadap pesan dan signature yang dihasilkan, untuk mengukur tingkat keberhasilan autentikasi.

3.5. Analisis Hasil

Setelah implementasi dan evaluasi, dilakukan analisis terhadap efisiensi, ketahanan terhadap prediksi, dan perbandingan entropi antara PRNG dan QRNG. Hasil dari validasi digital signature menjadi penentu utama keberhasilan sistem.

4. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil dari implementasi dan evaluasi sistem tanda tangan digital berbasis ECC dengan integrasi QRNG. Evaluasi dilakukan melalui pengujian keacakan, proses penandatanganan, dan verifikasi pesan secara digital. Pembahasan mencakup efektivitas penggunaan QRNG dibandingkan PRNG, serta kontribusinya dalam meningkatkan keamanan sistem terhadap ancaman komputasi kuantum.

4.1. Implementasi Sistem

Sistem yang dikembangkan merupakan aplikasi berbasis (Graphical User Interface) GUI yang mengintegrasikan QRNG dengan ECC untuk menghasilkan tanda tangan digital (digital signature). Aplikasi ini dibangun menggunakan bahasa Python dengan pustaka cryptography, tkinter, dan API eksternal dari ANU QRNG.

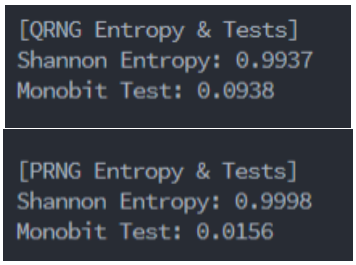
Fitur utama sistem terdiri dari:

a. Pembuatan pasangan kunci ECC dengan QRNG untuk kunci publik dan PRNG untuk kunci privat.
b. Proses penandatanganan pesan menggunakan algoritma ECDSA.
c. Penyimpanan pesan, tanda tangan digital, dan kunci ke file eksternal.
d. Verifikasi tanda tangan melalui input pesan, signature, dan kunci publik.

4.2. Pengujian Keacakan (QRNG vs PRNG)

Untuk mengukur tingkat keacakan data dari QRNG dan PRNG, dilakukan dua jenis pengujian:

a. Shannon Entropy: Mengukur seberapa acak distribusi byte.
b. Monobit Test: Mengukur keseimbangan jumlah bit 1 dan 0 dalam bitstream.

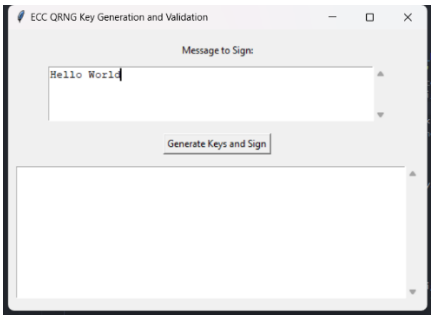


Gambar 2. Keacakan QRNG vs PRNG

4.3. Proses Tanda Tangan Digital

Langkah-langkah proses signing adalah sebagai berikut:

4.3.1. Pengguna Memasukkan Pesan Melalui Antarmuka

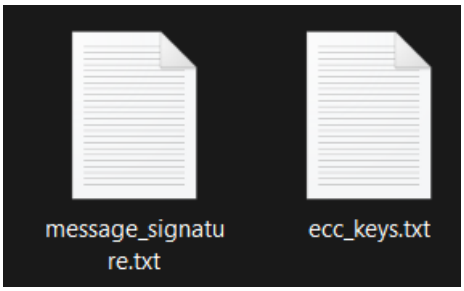


Gambar 3. Memasukkan Pesan

Setelah pengguna memasukkan pesan, lalu pengguna dapat melanjutkan dengan mengklik “Generate Key and Sign”

4.3.2. Sistem menghasilkan kunci ECC

a. Kunci publik berasal dari 32 byte QRNG.
b. Kunci privat berasal dari 32 byte PRNG.
c. Pesan ditandatangani menggunakan algoritma ECDSA.
d. Signature dan kunci disimpan sebagai file.



Gambar 4. ECC Disimpan sebagai File

4.4. Verifikasi Tanda Tangan

Proses verifikasi dilakukan melalui antarmuka validasi, di mana pengguna memasukkan:

a. Pesan asli, Signature, Public Key

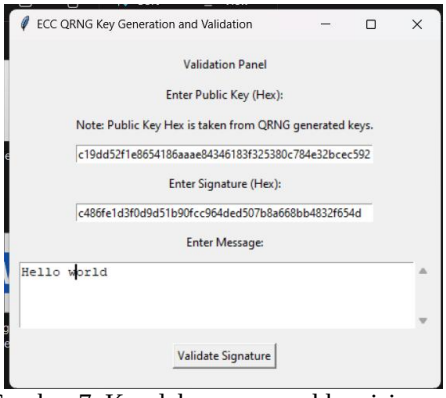
Gambar 5. Verifikasi Tanda Tangan

Sistem akan melakukan verifikasi ECDSA, dan memberikan hasil:

b. Jika valid → Signature is valid ☑

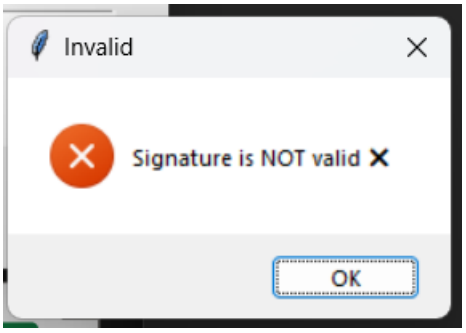
Gambar 6. Verifikasi Tanda Tangan Berhasil

c. Apabila terjadi kesalahan dalam memasukkan pesan, public key, atau signature, proses validasi akan gagal dan tanda tangan digital dinyatakan tidak sah. → Signature is NOT valid ❌



Gambar 7. Kesalahan memasukkan isi pesan

Sistem secara otomatis akan memberikan notifikasi bahwa tanda tangan digital tidak valid



Gambar 8. Verifikasi Tanda Tangan Gagal

4.5. Analisis Keamanan

Penggunaan QRNG sebagai sumber keacakan dalam pembuatan kunci publik ECC memberikan keuntungan signifikan dalam konteks keamanan post-quantum:

a. QRNG menjamin keacakan non-deterministik, sehingga lebih tahan terhadap prediksi maupun serangan berbasis analisis statistik.
b. Kombinasi QRNG dan ECDSA memperkuat proses autentikasi digital, karena tidak hanya mengandalkan kriptografi klasik, namun juga sumber entropi berbasis fenomena kuantum.

4.6. Kontribusi terhadap Penguatan Keamanan Post-Quantum

Penelitian ini memberikan kontribusi dalam:

a. Menunjukkan bahwa QRNG dapat diintegrasikan ke dalam sistem tanda tangan digital berbasis ECC.
b. Meningkatkan keamanan infrastruktur pesan digital dengan autentikasi berbasis signature yang tidak rentan terhadap prediksi deterministik.
c. Memberikan alternatif penerapan kriptografi pasca-kuantum tanpa mengganti sepenuhnya algoritma klasik (ECC tetap digunakan, namun diperkuat dengan QRNG).

5. KESIMPULAN DAN SARAN

Penelitian ini telah berhasil mengembangkan sistem digital signature berbasis Quantum Random Number Generator (QRNG) dan Elliptic Curve Cryptography (ECC) yang diimplementasikan dalam bentuk aplikasi GUI untuk autentikasi pesan. Integrasi QRNG sebagai sumber keacakan dalam proses pembangkitan kunci privat ECC terbukti mampu meningkatkan kualitas keacakan dibandingkan PRNG, yang ditunjukkan melalui pengujian entropi Shannon dan Monobit test. Sistem juga secara efektif mampu mendeteksi keaslian pesan, dengan validasi tanda tangan digital yang hanya sah ketika public key, pesan, dan signature sesuai. Keberhasilan sistem dalam menolak pesan yang telah dimodifikasi atau menggunakan kunci yang tidak sah menjadi indikator kuat bahwa pendekatan ini layak dijadikan alternatif solusi keamanan kriptografi di era ancaman komputasi kuantum. Dengan pencapaian ini, penelitian sangat potensial untuk dikembangkan lebih lanjut ke tingkat tesis, dengan perluasan fokus pada integrasi protokol TLS secara langsung menggunakan QRNG-ECC, implementasi real-time messaging dan pengujian serangan (*attack simulation*), studi performa dan skalabilitas sistem di lingkungan jaringan sesungguhnya, serta penerapan digital signature berbasis QRNG dalam infrastruktur keamanan nasional atau militer.

DAFTAR PUSTAKA

[1] Y. Park, J. Nam, dan Y. Chung, "Research on Quantum Key Distribution Key and Post-Quantum Cryptography Key Applied Protocols for Data Science and Web Security," in Proc. 2023 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea (South), 2023.

[2] K. Lal, H. P. Dwivedi, dan S. Choudhury, "Secure and Scalable Quantum Key Distribution Protocol for Next-Generation Networks," in Proc. 2022 IEEE 19th India Council International Conference (INDICON), 2022, pp. 1–6, doi: 10.1109/INDICON56171.2022.10039739.

[3] Y. Ge, J. Fan, X. Zhang, F. Wang, J. Shen, dan M. Gao, "Quantum Random Number Generator Based on Coherent Optical Receiver," in Proc. IEEE Asia Communications and Photonics Conference (ACP) and International Conference on Information Photonics and Optical Communications (IPOC), 2024, pp. 1–6, doi: 10.1109/ACP/IPOC63121.2024.10809531.

[4] S. Alshareef dan A. B. A. Hassan, "A Digital Signature Architecture for Web Apps," in Proc. 2023 3rd International Conference on Computer, Control and Robotics (ICCCR), Shanghai, China, 2023, pp. 233–238, doi: 10.1109/ICCCR57971.2023.10124439.

[5] I. Darmawan, M. A. Fitri, R. F. Anwar, dan M. R. Yusuf, "An Effective Arithmetic Combined Digital Signature with Digital Watermarking," in Proc. 2023 International Conference on Cybernetics and Intelligent Systems (ICORIS), Yogyakarta, Indonesia, 2023, pp. 215–220, doi: 10.1109/ICORIS58836.2023.10169675.

[6] P. Kumar, A. Mishra, dan S. Srivastava, "A Highly Secure Digital Signature Algorithm Without Modulo Inverse Operations," in Proc. 2022 6th International Conference on Computing, Communication and Security (ICCCS), Kathmandu, Nepal, 2022, pp. 1–6, doi: 10.1109/ICCCS55559.2022.10009163.

[7] F. Halim, Y. Suryadi, dan M. G. Abdullah, "Analysis of Random Number Generated by Quantum Noise Source and Software Entropy Source," in Proc. 2023 International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, Indonesia, 2023, pp. 228–233, doi: 10.1109/iSemantic57873.2023.10169643.

[8] A. S. Mardiana, A. P. Azlina, dan H. H. Hadisoemarto, "Evaluation of Cryptographically Secure Pseudo Random Number Generators for Post Quantum Era," in Proc. 2023 8th International Conference on Computing and Communication Systems (I3CS), 2023, pp. 1–6, doi: 10.1109/I3CS58099.2023.10180087.

[9] S. P. C. Sajimon et al., "Analysis of Post-Quantum Cryptography for Internet of Things," in Proc. 2022 6th Int. Conf. on Intelligent Computing and Control Systems (ICICCS), 2022, pp. 387–392, doi: 10.1109/ICICCS53718.2022.987987.

[10] N. A. Khan et al., "Employing Public Key Infrastructure to Encapsulate Messages During Transport Layer Security Handshake Procedure," in Proc. 2022 IEEE Int. Conf. on Applied Informatics, 2022, doi: 10.1109/ICAI54321.2022.9843872.

[11] R. K. Gupta dan P. Kumar, "Digital Signature Based on ISRSAC," in Proc. 2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2022, pp. 633–637, doi: 10.1109/Confluence52989.2022.9753103.

[12] K. Shah et al., "Advancements in Elliptic Curve Cryptography: A Review of Theory and Applications," in Proc. 2024 Parul Int. Conf. on Engineering and Technology (PICET), 2024, doi: 10.1109/PICET59723.2024.10111938.