Penggunaan Elliptic Curve Cryptography pada Enkripsi Paket Bluetooth Low Energy

Stefanus Ardi Mulia 13517119[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13517119@std.stei.itb.ac.id

***Abstract*—Dewasa ini, kita dikelilingi oleh banyak alat-alat nirkabel yang saling terhubung. Bluetooth merupakan salah satu protokol yang menjadi primadona untuk alat-alat dengan energi rendah yang perlu dapat terhubung dengan alat lain seperti sensor suhu nirkabel, lampu, telepon genggam pintar, dll. Salah satu iterasi dari Bluetooth merupakan *Bluetooth Low Energi* atau BLE yang di buat untuk Tentunya data yang ditransmisikan oleh alat-alat tersebut menjadi sesuatu yang kita ingin lindungi dari pihak-pihak tidak bertanggung jawab. Spesifikasi awal BLE tidak mendefinisikan cara untuk mengamankan paket-paket data yang ditransmisikan. Makalah ini akan membahas penggunaan *Elliptic Curve Cryptography* untuk mengatasi masalah tersebut.**

***Keywords*—Kriptografi, ECC, Bluetooth.**

I. PENDAHULUAN

Bluetooth banyak digunakan pada berbagai peralatan digital yang perlu terkoneksi dengan alat lain namun memerlukan penggunaan energi yang rendah. Alat-alat ini termasuk telepon genggam pintar, alat-alat *Internet of Things* seperti sensor suhu ruangan, lampu pintar, TV, hingga alat-alat medis nirkabel.

Alat-alat tersebut mungkin saja melakukan transmisi data satu sama lain secara berkala mengenai data-data yang trivial seperti suhu ruangan, terang lampu, dll. Namun bukan tidak mungkin bagi alat-alat tersebut untuk melakukan transmisi data-data yang sensitif seperti nama pengguna, lokasi, hingga data medis pribadi pengguna. Transmisi BLE yang menggunakan gelombang radio antar alatnya bisa saja disadap oleh pihak tidak berwenang. Spesifikasi awal BLE tidak mencantumkan cara yang dapat dilakukan untuk mengamankan data yang ditransmisikan.

Untuk menanggulangi permasalahan tersebut, makalah ini akan membahas penggunaan skema kriptografi kunci publik dengan memanfaatkan algoritma ECC sebagai lapisan keamanan di atas protokol BLE yang sudah ada.

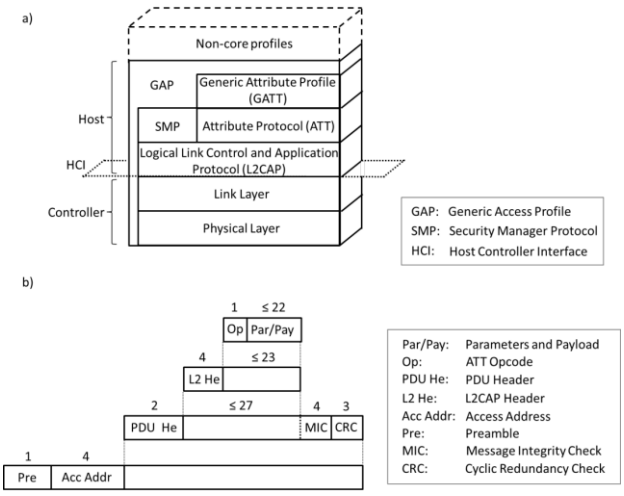
II. DASAR TEORI

A. Bluetooth

Nama Bluetooth berasal dari raja Denmark Haruld Blitund (Bluetooth) yang terkenal terkenal atas keberhasilannya menyatukan orang-orang Skandinavia pada abad ke-10. Demikian pula dengan teknologi nirkabel Bluetooth yang bertujuan untuk menyatukan perangkat-perangkat komputasi pribadi. Nama tersebut dipilih sebagai nama sementara untuk proyek pengembangan yang belum diumumkan pada saat itu. Namun pencarian nama baru tidak pernah membuahkan hasil dan nama sementara tersebut menjadi permanen. Pemilihan nama yang menarik ini dapat dikreditkan dengan sangat baik atas pengakuan dan penerimaan teknologi yang telah diterima sejauh ini. [1]

B. Bluetooth Low Energy

Bluetooth Low Energy (BLE) adalah teknologi nirkabel baru yang dikembangkan untuk komunikasi jarak pendek oleh Bluetooth Special Interest Group (SIG). BLE telah dikembangkan sebagai solusi daya rendah untuk aplikasi kontrol dan pemantauan, dibandingkan dengan jenis Bluetooth sebelumnya. BLE adalah fitur khas dari spesifikasi Bluetooth 4.0. Adopsi BLE tergolong cepat diduga disebabkan oleh tingginya penggunaan teknologi Bluetooth (misalnya di ponsel, tablet, kendaraan, dll.) karena pengimplementasian BLE dapat memanfaatkan kesamaan dengan Bluetooth klasik.



Gambar II.1 (a) *Protocol stack* BLE. (b) Struktur unit data BLE (ukuran direpresentasikan dalam byte). [2]

Protocol stack BLE terdiri dari dua komponen utama, seperti pada Bluetooth klasik: *Controller* dan *Host*. *Controller* terdiri dari *Physical Layer* dan *Link Layer*, dan biasanya diimplementasikan dengan radio terintegrasi sebagai *System-on-*

Chip (SoC) kecil. Host berjalan pada prosesor aplikasi dan mencakup fungsionalitas lapisan atas, misalnya, *Logical Link Control and Adaptation Protocol* (L2CAP), *Attribute Protocol* (ATT), *Generic Attribute Profile* (GATT), *Security Manager Protocol* (SMP) dan *Profil Akses Generik* (GAP). Komunikasi antara Host dan Pengontrol distandarkan sebagai Host Controller Interface (HCI). Terakhir, profil non-inti (semisal fungsionalitas lapisan aplikasi yang tidak ditentukan oleh spesifikasi Bluetooth) dapat digunakan di atas Host. *Protocol stack* BLE dapat dilihat pada Gambar I.1 (a).

1. Physical Layer

   BLE beroperasi pada pita radio 2,4 GHz Industrial Scientific Medical (ISM) dan menentukan 40 saluran Frekuensi Radio (RF) dengan jarak saluran 2 MHz. Ada dua jenis *channel* RF BLE: *advertising channel* dan *data channel*. *Advertising channel* digunakan untuk penemuan perangkat, pembentukan koneksi dan transmisi siaran, sedangkan *data channel* digunakan untuk komunikasi dua arah antara perangkat yang terhubung.

2. *Link Layer*

   Di BLE, ketika perangkat hanya perlu menyiarkan data, ia mengirimkan data dalam paket *advertising* melalui saluran periklanan. Perangkat apa pun yang mengirimkan paket iklan disebut pengiklan. Transmisi paket melalui *advertising channel* terjadi dalam interval waktu yang disebut peristiwa periklanan. Dalam *advertising*, *advertiser* secara berurutan menggunakan setiap *advertising channel* untuk melakukan transmisi paket. Perangkat yang hanya bertujuan menerima data melalui iklan.

   Komunikasi data dua arah antara dua perangkat memungkinkan mereka untuk terhubung satu sama lain. Pembentukan koneksi antara dua perangkat adalah proses asimetris di mana *advertiser* menyatakan bahwa itu adalah perangkat yang dapat dihubungkan melalui *advertising channel*, sementara perangkat lain mendengarkan *advertising* semacam itu (disebut sebagai inisiator).

   Saat *advertiser* terdeteksi oleh inisiator, pesan *Connection Request* dapat dikirim ke *advertiser*, memberikan sambungan *point-to-point* antara kedua perangkat. Dengan menggunakan saluran data fisik, kedua perangkat kemudian dapat berkomunikasi. Kode akses 32-bit yang dibuat secara acak akan mengidentifikasi paket untuk koneksi ini.

   BLE mendefinisikan dua peran perangkat untuk koneksi di *Link Layer*: master dan slave. Ini adalah perangkat yang berfungsi sebagai pemrakarsa dan mengiklankan masing-masing selama pembuatan koneksi. Beberapa koneksi simultan dengan budak berbeda dapat dikelola oleh satu master, sementara setiap budak hanya dapat dihubungkan ke satu master. Jadi, jaringan yang disusun oleh master dan budaknya, yang disebut piconet, mengikuti topologi bintang. Saat ini, perangkat BLE hanya dapat berada pada satu piconet.

3. L2CAP

   L2CAP yang digunakan di BLE adalah protokol yang dioptimalkan dan disederhanakan berdasarkan L2CAP Bluetooth klasik. Dalam BLE, tujuan utama L2CAP adalah untuk melakukan *multiplexing* di atas koneksi Link Layer dari tiga protokol lapisan yang lebih tinggi, ATT, SMP dan pensinyalan kontrol Layer Link. L2CAP mengelola data untuk layanan ini dengan pendekatan upaya terbaik dan tanpa menggunakan transmisi ulang dan sistem kontrol aliran yang termasuk dalam implementasi Bluetooth lainnya. Kemampuan segmentasi dan *reassembly* tidak digunakan karena unit data yang sesuai dengan ukuran *payload* L2CAP maksimum, yang dalam BLE setara dengan 23 byte, diberikan oleh protokol lapisan atas.

4. ATT

   ATT mendefinisikan komunikasi di atas *channel* L2CAP khusus antara dua perangkat yang masing-masing menjalankan peran sebagai server serta klien. Kumpulan atribut disimpan oleh server. Atribut adalah sistem data yang menyimpan informasi yang ditangani oleh protokol yang berjalan di atas ATT, GATT. GATT memutuskan peran klien atau server dan tidak bergantung pada peran *slave* atau *master*.

   Dengan mengirimkan permintaan yang memicu pesan respons dari server, klien dapat mengakses atribut server. Untuk kinerja yang lebih baik, server juga dapat mengirim dua jenis pesan yang tidak diminta ke klien yang berisi atribut: (i) *notification*, yang belum dikonfirmasi; dan (ii) *indication*, yang mengharuskan klien untuk mengirimkan konfirmasi. Untuk menulis nilai atribut, klien juga dapat mengirim perintah ke server. Transaksi *request*/*response* dan *indication*/*confirmation* mengikuti skema *stop-and-wait*.

5. GATT

   GATT mendefinisikan kerangka kerja yang menggunakan ATT untuk menemukan layanan dan untuk pertukaran fitur antar perangkat. Karakteristik adalah kumpulan data yang berisi nilai dan properti. Data dan fungsionalitas terkait layanan terdapat dalam atribut. Misalnya, server yang menjalankan layanan "sensor suhu" mungkin memperhitungkan karakteristik "suhu" yang menggunakan atribut untuk mendeskripsikan sensor, atribut lain untuk menyimpan nilai pengukuran suhu, dan atribut lebih lanjut untuk menentukan unit pengukuran.

C. Kriptografi

Kriptografi adalah praktik dan studi teknik untuk komunikasi yang aman di hadapan pihak ketiga yang disebut musuh. Secara lebih umum, kriptografi adalah tentang membangun dan menganalisis protokol yang mencegah pihak ketiga atau publik membaca pesan pribadi; berbagai aspek dalam keamanan informasi seperti kerahasiaan data, integritas data, otentikasi, dan *non-repudiation* adalah inti dari kriptografi modern.

Kriptografi modern berada di persimpangan disiplin ilmu matematika, ilmu komputer, teknik elektro, ilmu komunikasi, dan fisika. Aplikasi kriptografi meliputi perdagangan elektronik, kartu pembayaran berbasis chip, mata uang digital, sandi komputer, dan komunikasi militer.

D. Public Key Cryptography

Kriptografi kunci publik, atau kriptografi asimetris, adalah sistem kriptografi yang menggunakan pasangan kunci: kunci publik, yang dapat disebarluaskan, dan kunci privat, yang hanya diketahui oleh pemiliknya. Pembangkitan kunci tersebut bergantung pada algoritma kriptografi berdasarkan masalah matematika untuk menghasilkan fungsi satu arah. Keamanan yang efektif hanya membutuhkan kerahasiaan kunci privat; kunci publik dapat didistribusikan secara terbuka tanpa mengorbankan keamanan.

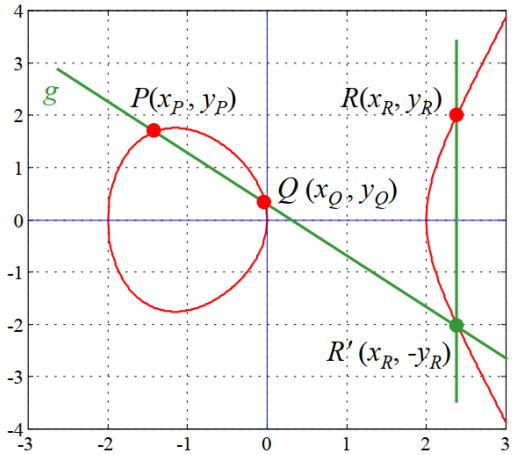
E. Elliptic Curve Cryptography

Elliptic Curve Cryptography atau ECC merupakan salah satu pendekatan kriptografi kunci publik yang berbasis pada struktur aljabar suatu kurva eliptis pada suatu bidang terbatas atau bidang Galois. Penggunaan kurva eliptis pada kriptografi bermula dari kesuksesan H.W. Lentra dalam melakukan faktorisasi bilangan bulat pada kurva eliptis [3].

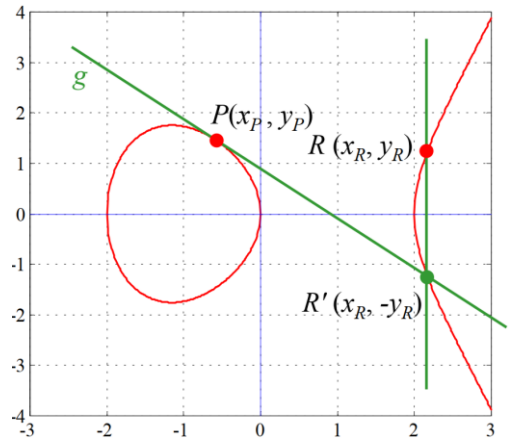
Rumus dasar yang dipakai dalam merepresentasikan sebuah kurva eliptis pada ECC adalah sebagai berikut.

$$y^2 = x^3 + ax + b \tag{1}$$

Variasi pada implementasi ECC dilakukan dengan mengubah nilai a dan b yang digunakan sebagai dasar rumus kurva. Dengan melakukan perubahan pada nilai tersebut didapatkan kurva yang berbeda-beda. Pada gambar II.2 dan II.3 dapat dilihat bagaimana proses penjumlahan titik pada kurva eliptis ini.



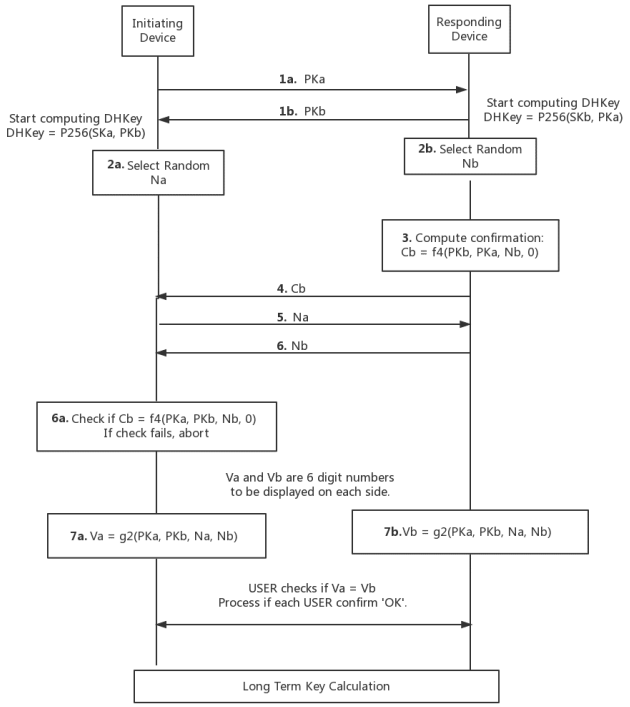
Gambar II.2 Penjumlahan dua titik pada kurva. [4]



Gambar II.3 Penjumlahan titik yang sama pada kurva. [4]

F. Elliptic Curve Diffie Hellman

Elliptic-curve Diffie – Hellman (ECDH) adalah protokol pertukaran kunci yang memungkinkan dua pihak, masing-masing memiliki pasangan kunci publik-privat kurva eliptis, untuk membangkitkan kunci rahasia bersama melalui saluran yang tidak aman. Rahasia bersama ini dapat langsung digunakan sebagai kunci, atau untuk mendapatkan kunci lain. Kunci, atau kunci turunan, kemudian dapat digunakan untuk mengenkripsi komunikasi berikutnya menggunakan sandi kunci simetris. Ini adalah varian dari protokol Diffie – Hellman yang menggunakan kriptografi kurva eliptik. Gambar II.4 menjelaskan bagaimana ECDH bekerja pada pertukaran kunci algoritma ECC yang menggunakan kurva P-256.



Gambar II.4 Proses Elliptic Curve Dilfie Hellman menggunakan kurva P-256.

III. Analisis Permasalahan

BLE banyak digunakan pada berbagai peralatan digital yang perlu terkoneksi dengan alat lain namun memerlukan penggunaan energi yang rendah. Alat-alat ini termasuk telepon genggam pintar, alat-alat *Internet of Things* seperti sensor suhu ruangan, lampu pintar, TV, hingga alat-alat medis nirkabel.

Alat-alat tersebut mungkin saja melakukan transmisi data satu sama lain secara berkala mengenai data-data yang trivial seperti suhu ruangan, terang lampu, dll. Namun bukan tidak mungkin bagi alat-alat tersebut untuk melakukan transmisi data-data yang sensitif seperti nama pengguna, lokasi, hingga data medis pribadi pengguna. Transmisi BLE yang menggunakan gelombang radio antar alatnya bisa saja disadap oleh pihak tidak berwenang. Spesifikasi awal BLE tidak mencantumkan cara yang dapat dilakukan untuk mengamankan data yang ditransmisikan. Makalah ini akan membahas salah satu solusi yang dapat dilakukan untuk meningkatkan keamanan dari suatu transmisi data pada BLE.

IV. Usulan Solusi

Untuk menanggulangi permasalahan tersebut, makalah ini mengusulkan penggunaan sebuah skema kriptografi kunci publik dengan memanfaatkan algoritma *ECC* sebagai lapisan keamanan di atas protokol BLE yang sudah ada. Solusi ini dipilih karena banyak alat-alat yang memanfaatkan protokol BLE sebagai protokol komunikasinya merupakan alat-alat dengan kekuatan komputasi yang rendah. ECC, dibandingkan dengan beberapa algoritma kriptografi kunci publik lainnya seperti RSA ataupun Elgamal menggunakan sumber daya komputasi yang lebih rendah. Selain itu ECC juga menawarkan keamanan yang lebih kuat dibandingkan algoritma yang disebutkan sebelumnya untuk panjang kunci yang sama sehingga dapat dipilih untuk menggunakan panjang kunci yang sama untuk mendapatkan keamanan yang lebih atau menggunakan panjang kunci yang lebih pendek untuk keamanan yang sama dengan algoritma RSA maupun Elgamal.

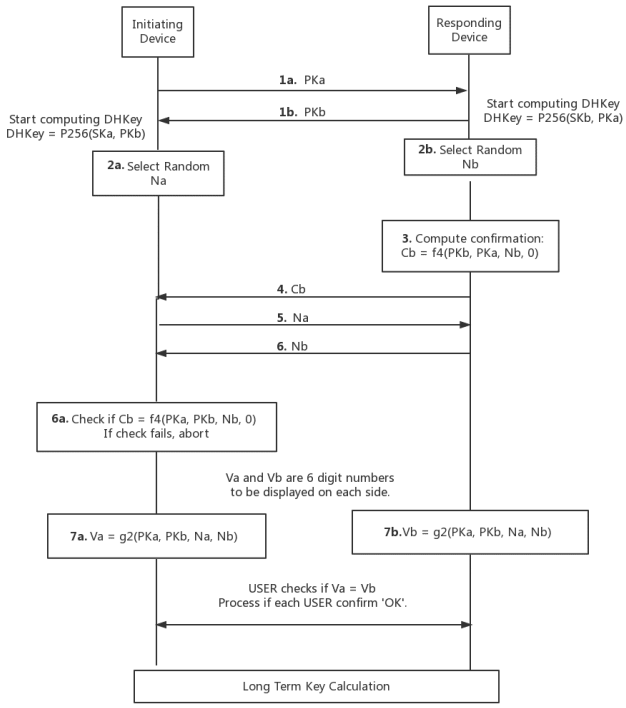
Secara garis besar skema yang digunakan adalah sebagai berikut.

1. Inisiasi koneksi dengan melakukan ECDH.
2. Paket dienkripsi dengan kunci yang didapatkan dari ECDH.

A. Inisiasi Koneksi

Dilakukan ECDH untuk pertukaran kunci yang aman dan pembangkitan kunci bersama. Karena batasan dari protokol BLE sendiri, ukuran dari suatu paket adalah 20 byte atau 160 bit. Oleh karena itu dipilih panjang kunci 160 bit. Salah satu standar yang dapat digunakan untuk pembangkitan kunci ini adalah standar SECP160k2 dengan variabel sebagai berikut.

A = 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFAC70
B = 0xB4E134D3FB59EB8BAB57274904664D5AF50388BA
P = 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFAC73
G = (0x52DCB034293A117E1F4FF11B30F7199D3144CE6D, 0xFEAFFEF2E331F296E071FA0DF9982CFEA7D43F2E)
n = (0x0100000000000000000000351EE786A818F3A1A16B)
h = 1



Gambar IV.1 Proses Elliptic Curve Dilfie Hellman menggunakan kurva P-256.

B. Inisiasi Koneksi

Berdasarkan kunci yang dibangkitkan pada tahap sebelumnya maka dapat dilakukan enkripsi terhadap paket-paket yang hendak dikirim. Untuk meningkatkan keamanan dari skema ini maka digunakan mode CBC atau *Cipher Block Chaining* dengan setiap paket yang berukuran 20 byte dianggap sebagai satu blok pesan.

V. Kesimpulan

BLE melakukan transmisi data secara tidak aman secara default. Untuk data-data yang sensitif diperlukan cara untuk mengamankannya. Oleh karena itu makalah ini mengusulkan penggunaan ECC sebagai skema enkripsi data yang ditransmisikan melalui paket-paket BLE. Dengan kebutuhan komputasi ECC yang lebih rendah dibandingkan algoritma kunci publik lain diharapkan skema ini dapat bekerja dengan baik pada perangkat berdaya rendah yang cenderung menggunakan BLE.

VII. Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Tuhan YME atas penyertaannya selama menuliskan makalah ini. Penulis juga mengucapkan terima kasih kepada orang tua penulis atas dukungannya dalam menulis makalah ini. Tak lupa penulis mengucapkan terima kasih kepada Bapak Rinaldi Munir sebagai dosen mata kuliah Kriptografi yang mengajarkan pengetahuan yang dibutuhkan agar penulis mampu menuliskan makalah ini.

Terakhir, penulis mengucapkan terima kasih kepada teman-teman penulis atas dukungannya selama menuliskan makalah ini.

REFERENCES

[1] Bisdikian, C. (2001). An overview of the Bluetooth wireless technology. IEEE Communications magazine, 39(12), 86-94.
[2] W.-K. Chen, *Linear Networks and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135. Gomez, C., Oller, J., & Paradells, J. (2012). Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. Sensors, 12(9), 11734-11753.
[3] Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of computation, 48(177), 203-209.
[4] Steffen, A. (2002). Elliptic Curve Cryptosystem. Group, 3, 4.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 21 Desember 2020

Stefanus Ardi Mulia 13517119