Studi dan Implementasi Kriptografi Berbasiskan Identitas Dengan Mediated RSA

Laksito Anindyo [1)]

1) Jurusan Teknik Informatika ITB, Jln. Ganesha 10 Bandung 40132, email: if141222@students.if.itb.ac.id

Abstract – *Enkripsi kunci public yang berbasiskan identitas memfasilitasi pengenalan terhadap kriptografi kunci publik dengan memungkinkan sebuah entitas kunci public diturunkan dari sebuah hasil arbitrasi value seperti nama atau alamat email. Keuntungan yang utama dari kriptografi berbasiskan identitas adalah dalam mengurangi kebutuhan dan ketergantungan akan sertifikat kunci publik. Sebenarnya teknik berbasiskan identitas telah lama dikembangkan, namun belum ada yang kompatibel dengan algoritma enkripsi kunci publik yang populer. Ini membatasi penggunaan kriptografi berbasiskan identitas sebagai sebuah langkah tradisional untuk diterapkan pada kriptografi kunci publik.*

Mediated RSA (mRSA) adalah sebuah metoda yang simpel dan praktis dalam membagi sebuah kunci privat RSA antara user dan sebuah Security Mediator (SEM). Baik user maupun SEM tidak dapat saling mencurangi satu sama lain karena tiap-tiap operasi kriptografis melibatkan kedua belah pihak. mRSA menawarkan keamanan beserta proses yang singkat dan cepat. Namun, mRSA masih bergantung pada sertifikat kunci publik yang konvensional untuk menyimpan dan mengirimkan kunci publik. Pada makalah ini, akan dibahas mengenai kombinasi mRSA dengan kriptografi berbasis identitas, agar dihasilkan algoritma yang lebih aman, cepat, praktis dan ringkas.

Kata Kunci*: Algoritma kunci publik, kriptografi berbasis identitas, RSA, mediated RSA.*

1. Pendahuluan

Pada infrastruktur kunci public pada umumnya, kunci public pengguna secara eksplisit disandikan dalam sebuah sertifikat kunci public yang mengikat identitas pemegang sertifikat dengan kunci publiknya. Model seperti ini membutuhkan kepercayaan yang universal pada pembuat sertifikat (Certification Authorities atau CA). Hal ini menyebabkan efek samping yang cukup mengganggu seperti kebutuhan untuk mempercayai sumber dari domain yang berbeda, serta pencabutan sertifikat. Permasalahan utamanya terletak pada asumsi dasar bahwa seluruh sertifikat bersifat publik, tersedia dimana-mana, dan oleh karena itu siap tersedia bagi siapa saja. Namun, ternyata asumsi tersebut tidak selamanya realistis, terutama pada jaringan yang memiliki konektivitas kurang baik seperti jaringan nirkabel.

Sedangkan, kriptografi berbasiskan identitas merubah kebiasaan mendapatkan kunci public dengan membangun relasi satu-satu antara identitas dengan kunci public. Secara umum, enkripsi berbasis identitas dan *signatures* atau tanda tangan berbasis identitas merupakan suatau kakas kriptografi yang berguna yang mampu memfasilitasi pengenalan dan konversi yang mudah ke kriptografi kunci public dengan memungkinkan sebuah kunci punlik diturunkan dari identitas seperti alamat email atau nomor telepon. Disamping itu, metoda berbasis identitas ini sangat memperringkas manajemen kunci karena telah mengurangi kebutuhan dan jumlah dari sertifikat kunci public.

Pada makalah ini, penulis mengajukan sebuah metode kriptografi berbasiskan identitas yang dikembangkan pada Mediated RSA (mRSA). mRSA merupakan metoda praktis dalam memecah kunci privat RSA antara pengguna dengan *security mediator* yang disebut SEM. Baik pengguna maupun SEM tidak mengetahui faktorisasi dari modulus RSA dan tidak satupun pula yang dapat mendekripsi atau menandatangani pesan tanpa bantuan yang lain.

Dibangun diatas mRSA, mRSA berbasis identitas atau IB-mRSA menggabungkan fitur dari kriptografi berbasis identitas dan mediasi. Seperti halnya mRSA, IB-mRSA sepenuhnya kompatibel dengan RSA biasa. Kecuali untuk pemetaan identitas ke kunci publik, IB-mRSA tidak memerlukan perangkat lunak khusus. IB-mRSA juga mengizinkan sertifikat-sertifikat kunci publik opsional yang memudahkan transisi pada suatu *Public Key Infrastructure* (PKI) yang konvensional. Lebih umum lagi, IB-mRSA dapat dipandang sebagai suatu teknik praktis dan sederhana yang dapat dibedah dengan PKI modern yang sudah umum.

2. Enkripsi Berbasis Identitas

Konsep dasar *Identity Based Encription* (IBE) adalah untuk menghindari adanya autentikasi terhadap kunci publik seperti yang terdapat PKI. Satu-satunya autentikasi yang ada hanya autentikasi seorang *user* untuk mendapatkan kunci privatnya.

Jika pada PKI, kunci publik dan kunci privat dibangkitkan sendiri oleh pemilik kunci, maka pada IBE, kunci publik dapat dibangkitkan secara otomatis oleh pihak yang akan mengirimkan pesan. Kunci privat akan dibangkitkan oleh penerima pesan dengan bantuan dari pihak ketiga yang dapat dipercaya atau *Trusted Third Party* (TTP) yang juga dikenal sebagai *Security-Mediator* (SEM) pada IB-mRSA. TTP ini bertanggung jawab untuk membangkitkan kunci privat dari seorang *user.*

Pembangkitan kunci privat dilakukan dengan melakukan serangkaian perhitungan dengan fungsi satu arah yang masukannya adalah kunci publik dan sejumlah parameter tertentu yang hanya diketahui oleh TTP tersebut. Parameter yang hanya diketahui oleh TTP dan digunakan dalam pembangkitan kunci privat disebut sebagai master key. Selain master key yang bersifat rahasia, parameter lain yang digunakan dalam pembangkitan kunci privat dan bersifat umum disebut sebagai parameter sistem.

Secara konsep IBE dapat dibagi menjadi 4 bagian yang masing-masing dapat dianggap sebagai algoritma tersendiri yaitu : [1]

a. *Setup*, yaitu pengambilan parameter-parameter yang diperlukan untuk penentuan parameter sistem dan *master key*.
b. *Extract*, yaitu proses pembuatan kunci privat dengan mengambil masukan dari parameter sistem, master key serta identitas pengguna. Sebelum melakukan proses ini, TTP terlebih dahulu melakukan autentikasi terhadap pengguna yang ingin mendapatkan kunci privatnya.
c. *Encrypt,* yaitu proses enkripsi dengan masukan parameter sistem, identitas dan pesan yang akan dienkripsi.
d. *Decrypt,* yaitu proses dekripsi dengan masukan parameter sistem , ciphertext dan kunci privat yang bersesuaian.

3. Mediated RSA Berbasis Identitas (IB-mRSA)

Fitur utama dari enkripsi yang berbasis identitas adalah kemampuan pengirim untuk mengenkripsi pesan menggunakan kunci publik yang diperoleh dari identitas penerim dan informasi publik yang lain. Identitas tersebut dapat berupa alamat email penerima itu, user id, atau setiap nilai yang unik bagi penerima, yang terpenting berupa sebuah *string* yang sembarang. Untuk menghitung kunci enkripsi, sebuah fungsi pemetaan KG yang efisien dan bersifat publik harus ditetapkan terlebih dahulu. Fungsi ini haruslah berupa suatu pemetaan satu ke satu dari *string*- identitas ke kunci publik.

Ide dasar dibalik mRSA berbasis identitas adalah penggunaan modulus RSA tunggal *n* untuk semua pengguna di dalam suatu sistem atau domain. Untuk melakukan enkripsi sebuah pesan untuk penerima tertentu (Bob), pengirim (Alice) terlebih dahulu menghitung *eBob = KG (IDBob)* di mana *IDBob* adalah nilai identitas penerima seperti alamat *e-mail* dan *KG*() adalah suatu fungsi pemetaan satu ke satu yang biasanya merupakan fungsi hash seperti MD5 atau SHA. Selanjutnya pasangan nilai (*eBob*,*n*) dianggap sebagai kunci publik RSA biasa dan dilakukan proses enkripsi RSA secara umum.

Pada IB-mRSA terdapat sedikit perubahan pada konsep IBE karena dibutuhkan *Certificate Authority* (CA) yang menentukan dan menyimpan nilai modulus *n* RSA yang berlaku publik. Hal ini mirip dengan konsep CA yang terdapat dalam PKI. IB-mRSA sebenarnya dapat dianggap gabungan dari IBE dan PKI (dengan RSA).

Berikut rincian skema IBE-mRSA untuk tiap bagian dalam IBE :[3]

a. Setup

Pada fase ini, TTP dalam hal ini adalah CA memilih suatu nilai *p'* dan *q'* yang merupakan bilangan prima dan memenuhi $p=2p' + 1$ dan $q = 2q'+1$ dimana *p* dan *q* juga bilangan prima. Hasil perkalian *p* dan *q* yaitu *n* merupakan parameter sistem yang didistribusikan pada tiap *user* dalam *domain* CA tersebut. Sedangkan nilai *p'* dan *q'* merupakan *master key* yang bersifat rahasia. Setelah itu juga ditentukan
suatu nilai acak ganjil *Zn* yang juga merupakan *master key*. Selanjutnya proses pembentukan kunci privat *user* Alice adalah sebagai berikut :

(a) s = k - |KG()| - 1
(b) eAlice = 0s||KG(IDAlice)||1
(c) dAlice = 1/eAlice mod Φ (n)
(d) dAlice,u = Zn – {0}
(e) dAlice,sem = (dAlice – dAlice,u) mod Φ (n)

dAlice,u akan diserahkan pada *user* Alice, sedangkan *dAlice,sem* akan diserahkan pada SEM yang bersangkutan.

b. Extract

Proses ekstraksi kunci pada IB-mRSA telah tergabung dengan proses dekripsi.

c. Encrypt

Untuk melakukan enkripsi, pengirim terlebih dahulu harus memiliki nilai modulus *n*, *k*, dan *KG* yang digunakan. Nilai – nilai tersebut bersifat publik dan disebarkan oleh CA.

Berikut algoritma enkripsi IB-mRSA :
(1) s = k - |KG()| - 1
(2) *e = 0s||KG(ID)||1*
(3) lakukan enkripsi pesan m dengan menggunakan kunci publik (*e,n*) seperti pada RSA standar.

d. Decrypt
Untuk melakukan dekripsi, user harus melakukan kontak dengan SEM.
Berikut algoritma proses dekripsi :
1. *USER* : *m'* = pesan terenkripsi
2. *USER* : kirim *m'* ke SEM
3. secara bersamaan :
   3.1 SEM
   (a) jika *user* tidak terdaftar *return (ERROR)*
   (b) PDSem = m'dsem mod n
   (c) Kirim PDSem ke *user*
   3.2 *USER*
   Pdu = m'du mod n
4. *USER : M = (PDSem * PDu) mod n*
5. *USER : m = OAEP Decoding* dari M
6. *USER* : jika sukses, kembalikan (m)

4. Perbandingan Dengan Boneh-Franklin Identity Based Encryption

BF-IBE merupakan skema usulan Dan Boneh dan Matthew Franklin pada tahun 2001. Skema BF-IBE mendasarkan kekuatan keamanannya pada *Bilinear Diffie Hellman Problem* (BDHP).

Berikut rincian skema BF-IBE untuk tiap bagian dalam IBE :[1,4]
a. Setup
Inisialisasi IBE dilakukan dengan pemilihan sebuah titik *p* pada kurva elips, pemilihan suatu nilai *master key s*. Yang menjadi parameter sistem dan didistribusikan pada tiap pengguna IBE adalah nilai *p* dan *s* • *p*.
b. Extract
Proses ekstraksi pada BF-IBE dilakukan pada saat pengguna yang ingin mendapatkan kunci privatnya melakukan autentikasi dirinya pada PKG. Jika autentikasi berhasil maka, PKG kemudian melakukan proses penghitungan kunci publik sebagai *s* • ID*user*, dengan *s* adalah *master key* yang hanya diketahui oleh PKG dan ID*user* adalah string berisi identitas yang
disediakan oleh *user.*
c. Encrypt
Sebelum melakukan proses enkripsi, pengirim terlebih dahulu melakukan pemetaan identitas penerima ke suatu titik pada kurva elips. Setelah itu, pengirim memilih satu nilai acak **r** dan melakukan penghitungan kunci *k* sebagai berikut :
*k = Pair (***r** *• IDpenerima, s • p)*
Dengan menggunakan kunci *k* tersebut, pengirim mengenkripsi pesan dan mengirimkan hasil enkripsi beserta nilai **r** • *p*
d. Decrypt
Setelah penerima pesan yang telah dienkripsi dan nilai **r** • *p*, maka penerima pesan kemudian menghitung
kunci *k* sebagai berikut :
k = Pair (s • IDpenerima ,r • p)
Asumsi : *s • IDpenerima* telah didapatkan oleh penerima dari PKG.
Dengan kunci *k* tersebut, penerima dapat melakukan dekripsi terhadap ciphertext.

Perbandingan antara skema BF-IBE dengan IB-mRSA terlihat pada beberapa aspek, yaitu: kemudahan, penarikanan, keamanan dan biaya dari pembangkitan kunci
(a) Kemudahan
Walaupun BF-IBE dan IB-mRSA memiliki kesamaan arsitektur, tetapi keduannya memiliki dasar kriptografi
yang berbeda. IB-mRSA lebih mudah dibangun karena RSA sudah menjadi kunci publik kriptografi yang populer.
(b) Penarikan kunci
IB-mRSA menyediakan penarikan peroperasi (*pre-operation revocation*) sedangkan BF-IBE menyediakan penarikan secara periodik (*periodic revocation*)
(c) Keamanan
SEM pada IB-mRSA dan PKG pada BF-IBE keduanya merupakan pihak ketiga yang dipercaya, perbedaannya terletak pada tingkat kepercayaan. SEM sangat dipercaya (*fully trusted*) karena untuk mendapatkan kunci seluruh user diperlukan penggabungan SEM dengan salah satu *user*, sedangkan jika kita mengetahui *master-key* PKG, kita dapat langsung mengetahui keseluruhan kunci.

5. Implementasi

Implementasi IB-mRSA dimaksudkan untuk tujuan percobaan dan validasi. Pengkodean perangkat lunak implementasi ini dibangun di atas pustaka OpenSSL. OpenSSL menyertakan banyak fungsi-fungsi kriptografi dan sejumlah besar primitif aritmatika. Sebagai tambahan untuk menjadikannya efisien dan tersedia di berbagai platform perangkat keras dan perangkat lunak, OpenSSL bertahan pada patokan-patokan PKCS yang umum dan terletak pada domain publik.

Pada tahap inisialisasi, suati CA menginisialisasi pengaturan kriptografis untuk seluruh domain, yang dinamakan (*n,p,q,p',q'*) dan memilih fungsi mapping untuk seluruh klien dari domain (secara default diset pada MD5). Proses selanjutnya mengikuti langkah-langkah IB-mRSA seperti yang telah dijelaskan

sebelumnya. Untuk masing-masing pengguna, dua buah struktur di-export, bundel SEM yang mencakup setengah dari kunci SEM d_i^{SEM}, dan bundel pengguna yang mencakup d_i " dan keseluruhan bundel server.

Bundel server yang pada dasarnya merupakan suatu amplop RSA yang ditandatangani oleh CA dan dienkripsi dengan kunci publik SEM itu. Bundel klien merupakan suatu amplop kunci yang dibagi bersama yang juga ditandatangani oleh CA dan dienkripsi dengan pengguna menyediakan kunci yang dapat merupakan suatu kunci yang telah ditetapkan lebih dulu, suatu kata sandi atau suatu passphrase.

Setelah pengeluaran bundel, masing-masing bundel pengguna dibagi-bagikan kepada pengguna yang sesuai. Sebelum mencoba transaksi IB-mRSA, pengguna itu harus terlebih dahulu mendekripsi dan memverifikasi bundel. Suatu program yang terpisah disediakan untuk tujuan ini. Dengan program tersebut, bundel itu didekripsi dengan kunci yang disediakan pengguna, tandatangan CA itu dibuktikan, dan, akhirnya separuh kunci pengguna itu diekstraksi dan disimpan pada tempat itu.

Untuk mendekripsi suatu pesan, pengguna harus mengirimkan suatu permintaan IB-mRSA, dengan bundel SEM. SEM lalu mengecek status dari klien. Hanya ketika klien itu dianggap sebagai pengguna yang sah, SEM memproses permintaan menggunakan bundel yang terdapat di tempat itu. Sebagaimana disebutkan sebelumnya, untuk mengenkripsi suatu pesan untuk satu IB-mRSA, sertifikat domain pengguna itu perlu untuk diperoleh. Distribusi dan manajemen sertifikat-sertifikat domain diasumsikan untuk dilaksanakan di suatu cara serupa dengan sertifikat normal, misalkan dengan melalui LDAP.

6. Kesimpulan

Identity Based Encryption (IBE) mengatasi masalah yang terdapat pada teknik kriptografi tradisional seperti kebutuhan keamaanan yang belum dapat diatasi dan masalah penanganan sertifikat. IBE telah mengatasi ini dengan suatu sistem dimana dapat digunakan *string s*embarangan sebagai kunci publik. IBE telah menghilangkan sistem sertifikat yang kompleks dengan menggunakan identitas sebagai kunci publik.

Aplikasi IBE secara praktis telah memberikan solusi yang mudah untuk mengimplementasikan dan mudah diatur. Teknik IBE menggunakan pemetaan satu-satu yang merupakan salah satu teknik yang menjanjikan karena mempunyai model keamanaan yang kuat.

Identity Based mediated RSA (IB-mRSA) merupakan salah satu penerapan IBE yang praktis dan aman. IB-mRSA kompatibel dengan enkripsi RSA standard dan menawarkan kontrol yang baik pada keutamaan keamanan dari penggunanya.

Jika dibandingkan dengan BF-IBE, IB-mRSA relatif lebih mudah dibangun karena RSA sudah menjadi kunci publik kriptografi yang populer. IB-mRSA juga menyediakan penarikan peroperasi *(pre-operation revocation)* sedangkan BF-IBE menyediakan penarikan secara periodik *(periodic revocation)*. SEM pada IB-mRSA dan PKG pada BF-IBE keduanya merupakan pihak ketiga yang dipercaya, namun SEM lebih dipercaya karena untuk mendapatkan kunci seluruh user diperlukan penggabungan SEM dengan salah satu user, sedangkan jika kita mengetahui *master-key* PKG, kita dapat langsung mengetahui keseluruhan kunci.

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Kriptografi*, Institut Teknologi Bandung, 2006.

[2] Ding, Xuhua dan Gene Tsudik, *Simple Identity-Based Cryptography with Mediated RSA*, University Of California.