Skema Boneh-Franklin Identity-Based Encryption dan Identity-Based Mediated RSA

Dedy Sutomo, A.Ais Prayogi dan Dito Barata

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : if11022@students.if.itb.ac.id , if11035@students.if.itb.ac.id, if11055@students.if.itb.ac.id

Abstrak

Identity-Based Encryption (IBE) adalah salah satu teknik enkripsi yang menggunakan kunci asimetris. Keistimewaan IBE dibanding teknik enkripsi kunci asimetris yang lainnya adalah autentikasi yang relatif mudah, tidak seperti mekanisme otentikasi *Public Key Infrastructure* (PKI) yang rumit dan harus dilakukan bertingkat-tingkat, mekanisme otentikasi pada IBE hanya dilakukan sekali, yaitu pada saat user membangkitkan kunci *privat* seseorang. Dalam paper kami ini, akan kami bahas 2 varian IBE yaitu Boneh-Franklin Identity-Based Encryption (BF-IBE) dan Identity-Based Mediated RSA (IB-mRSA).

***Kata kunci**: Teknik enkripsi kunci asimetris, Identity-Based Encryption, Boneh-Franklin Identity-Based encryption, Identity-Based Mediated RSA, kunci privat*

1. Pendahuluan

Identity Based Encryption (IBE) merupakan salah satu dari banyak varian dalam teknik kriptografi kunci publik. IBE pertama kali diusulkan oleh Shamir tahun 1984. Pada IBE, kunci publik seseorang merupakan *string* yang didapatkan dari fungsi terhadap identitas orang tersebut. Identitas yang digunakan sendiri dapat berupa nomor kartu identitas, *username* pada lingkungan Linux, alamat *e-mail*, nomor telepon, alamat rumah atau informasi lainnya yang dapat mewakili secara unik identitas suatu entitas dalam hal ini seseorang.

Penggunaan identitas seseorang sebagai kunci publik, secara signifikan akan mengurangi kerumitan yang diperoleh dibandingkan jika menggunakan sistem kunci publik konvesional atau *Publik Key Infrastructure* (PKI).

2. Ruang lingkup

Makalah ini membahas tentang cara kerja dua skema IBE yaitu skema Boneh-Franklin Identity-Based Encryption (BF-IBE) dan Identity-Based Mediated RSA (IB-mRSA).

3. *Identity Based-Encryption* (IBE)

Konsep dasar 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 *Private Key Generator* (PKG) pada BF-IBE atau *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.

Hingga saat ini telah cukup banyak skema yang diajukan untuk implementasi IBE. Namun hanya ada sedikit skema yang dapat diimplemtasikan dan mempunyai tingkat keamanan yang cukup kuat. BF-IBE dan IBE-mRSA adalah dua di antaranya.

4. *Boneh-Franklin Identity-Based Encryption* (BF-IBE)

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 $s \bullet p$.

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 $s \bullet ID_{user}$, 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 titika pada kurva elips. Setelah itu, pengirim memilih satu nilai acak **r** dan melakukan penghitungan kunci *k* sebagai berikut :
$k = Pair (\mathbf{r} \bullet ID_{penerima} , s \bullet p)$
Dengan menggunakan kunci *k* tersebut, pengirim mengenkripsi pesan dan mengirimkan hasil enkripsi beserta nilai $\mathbf{r} \bullet p$

d. *Decrypt*
Setelah penerima pesan yang telah dienkripsi dan nilai $\mathbf{r} \bullet p$, maka penerima pesan kemudian menghitung kunci *k* sebagai berikut :
$k = Pair (s \bullet ID_{penerima} , r \bullet p)$
Asumsi : $s \bullet ID_{penerima}$ telah didapatkan oleh penerima dari PKG.
Dengan kunci *k* tersebut, penerima dapat melakukan dekripsi terhadap ciphertext.

5. Identity-Based Mediated RSA (IB-mRSA)

Ide dasar dari IB-mRSA adalah penggunaan sebuah modulus *n* RSA yang bersifat publik dan digunakan oleh sejumlah RSA dalam satu sistem IBE tertentu yang berada dalam *domain* tertentu. Untuk melakukan enkripsi sebuah pesan untuk penerima tertentu (Bob), pengirim (Alice) terlebih dahulu menghitung $e_{Bob} = KG (ID_{Bob})$ di mana ID_{Bob} 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 (e_{Bob},*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). Konsep SEM sendiri agak berbeda dengan PKG pada BF-IBE, karena SEM pada IBE-mRSA lebih condong pada fungsi mediator.

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 $q = 2q'+1$ di mana *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 Z_n yang juga merupakan *master key*. Selanjutnya proses pembentukan kunci privat *user* Alice adalah sebagai berikut :
(a) $s = k - |KG()| - 1$
(b) $e_{Alice} = 0^s||KG(ID_{Alice})||1$
(c) $d_{Alice} = 1/e_{Alice} \bmod \Phi (n)$
(d) $d_{Alice,u} = Z_n - \{0\}$
(e) $d_{Alice,sem} = (d_{Alice} - d_{Alice,u}) \bmod \Phi (n)$
$d_{Alice,u}$ akan diserahkan pada *user* Alice, sedangkan $d_{Alice,sem}$ 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) $e = 0^s||KG(ID)||1$

(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) $PD_{Sem} = m'^{dsem} \bmod n$

   (c) Kirim PD_{Sem} ke *user*

   3.2 *USER*

   $Pdu = m'^{du} \bmod n$
4. *USER* : $M = (PD_{Sem} * PD_u) \bmod n$
5. *USER* : *m = OAEP Decoding* dari M
6. *USER* : jika sukses, kembalikan (m)

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* sembarangan 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.

Perbandingan antara skema BF-IBE dengan IB-mRSA terlihat pada beberapa aspek, yaitu: kemudahan, penarikanan, keamanan dan biaya dari pembangkitan kunci. [3]

(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.

[1] D. Boneh, M. Franklin, *Identity-Based Encryption from the Weil Pairing*, Advances in Cryptology – Crypto2001, Springer LNCS 2139
[2] D. Boneh, *et al. Identity-Based Mediated RSA,* http://pollux.usc.edu/~xuhuad/publications/wisa.pdf, diakses tanggal 10 Januari 2005.
[3] X. Ding, G. Tsudik, *Simple Identity-Based Cryptography with Mediated RSA*, 2001
[4] Evelyn, *Identity-Based Encryption*, http://budi.insan.co.id, diakses tanggal 05 Januari 2005