



PROYEK AKHIR
EC-5010 KEAMANAN SISTEM INFORMASI

Identity-Based Encryption

Oleh:
Evelyn
13201019



DEPARTEMEN TEKNIK ELEKTRO
INSTITUT TEKNOLOGI BANDUNG
2004

Abstrak

Identity-Based Encryption merupakan teknik enkripsi dengan menggunakan kunci asimetris yang mempunyai keistimewaan, yaitu *public-key* yang digunakan dapat berupa sembarang *string*. Biasanya, enkripsi menggunakan *public-key* yang rumit dan sulit diingat. *Identity-Based Encryption* menggunakan kunci yang lebih "*user-friendly*". *Public-key* pada *Identity-Based Encryption* ini dapat berupa alamat email, nomor telepon, ataupun suatu kalimat. Kelebihan lain dari teknik enkripsi ini yaitu tidak diperlukannya penentuan pasangan kunci sebelum melakukan enkripsi. Dengan menggunakan *Identity-Based Encryption*, seseorang dapat mengirimkan email yang telah dienkripsi dengan *public-key* walaupun penerima belum mempunyai bahkan belum pernah mendengar *private-key* sekalipun. Pada saat penerima menerima email yang terenkripsi tersebut, penerima akan menghubungi *Private Key Generator*, yang akan melakukan autentikasi dan memberikan *private-key* untuk membaca email tersebut.

DAFTAR ISI

1. Pendahuluan.....	1
2. Sejarah Kriptografi.....	2
2.1 Kriptografi Simetris (1960 – 1970).....	3
2.2 Kriptografi Asimetris (1980 – 1990).....	4
2.3 Identity-Based Encryption (2001 – sekarang).....	5
4. Algoritma <i>Identity-Based Encryption</i>	7
5. Teknik <i>Identity-Based Encryption</i> berdasarkan <i>Pairing</i>	8
5.1 Dasar Matematis.....	8
5.1.1 <i>Bilinear Map</i>	8
5.1.1 <i>Bilinear Diffie-Hellman Problem (BDHP)</i>	8
5.2 Teknik Identity-Based Encryption Boneh-Franklin	8
5.2 Authenticated Identity-Based Encryption.....	11
5.3 Hierarchical Identity-Based Encryption	12
6. Keamanan pada <i>Identity-Based Encryption</i>	14
6.1 Semantic Security.....	14
6.2 Chosen ciphertext security.....	15
7. Perbandingan IBE dengan PKI	15
8. Kelebihan dan Kekurangan IBE.....	20
9. Aplikasi dari <i>Identity-Based Encryption</i>	20
9.1 Revocation of Public Key (Pencabutan Kunci Publik)	20
9.2 Managing User Credentials (Manajemen Pemberian Perintah kepada User).....	21
9.3 Delegations of decryption keys	21
9.4 Forward-secure encryption	22
10. Kesimpulan	22
11. Daftar Pustaka.....	22

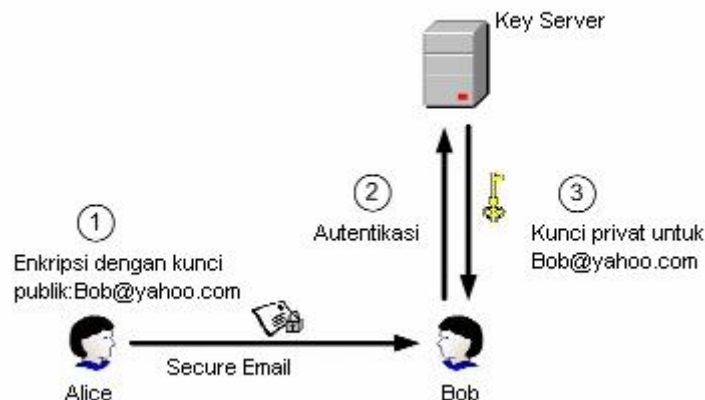
1. Pendahuluan

Pada dasarnya, alasan digunakannya enkripsi adalah untuk mengamankan data sehingga hanya orang tertentu (misalnya, bob@yahoo.com) atau satu mesin (misalnya, www.yahoo.com) saja yang dapat mengakses data tersebut. Sampai sekarang, teknik enkripsi masih mengandalkan kunci acak yang panjang, yang harus dipetakan untuk identitas tertentu dengan menggunakan dokumen yang ditandatangani secara digital (*digitally signed documents*) yang disebut sertifikat. Manajemen sertifikat-sertifikat ini dan perlunya pengambilan sertifikat sebelum melakukan enkripsi ke seseorang atau suatu mesin, menjadi masalah dalam teknik enkripsi.

Identity-Based Encryption (IBE) memberikan pendekatan baru dalam mengatasi masalah pada teknik enkripsi. Dalam IBE, dapat digunakan *string* sembarang sebagai kunci publik sehingga data dapat diamankan tanpa perlu menggunakan sertifikat. Pengamanan dilakukan oleh *key server* yang mengendalikan pemetaan identitas ke kunci dekripsi.

Rancangan sistem IBE telah menjadi masalah terbuka pada dunia kriptografi. Banyak dibuat algoritma untuk mengimplementasikan sistem IBE secara praktis.

IBE secara dramatis telah menyederhanakan proses pengamanan komunikasi yang sensitif sekalipun. Gambar di bawah ini mengilustrasikan bagaimana Alice akan mengirimkan email yang aman untuk Bob menggunakan teknik IBE.



Gambar 1 Teknik *Identity-Based Encryption*

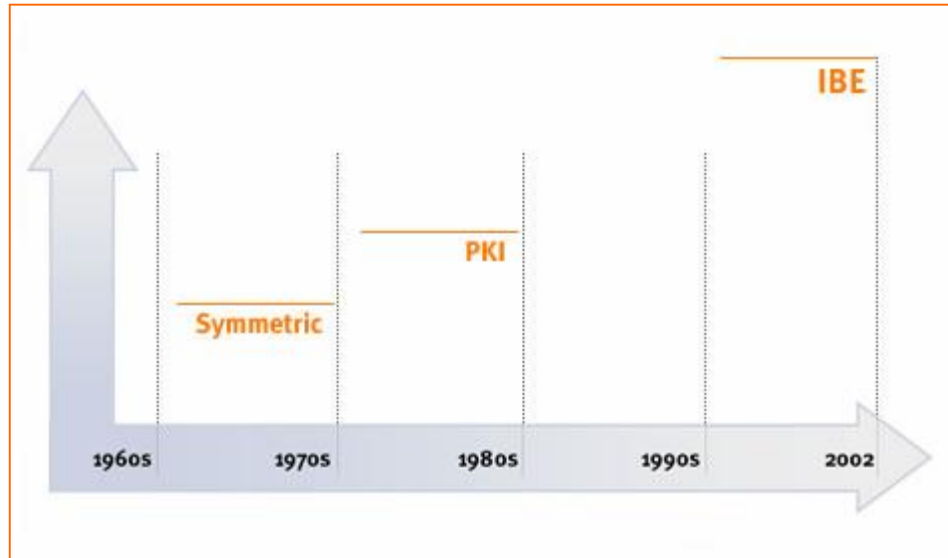
Langkah-langkah pengiriman email dari Alice untuk Bob menggunakan IBE:

1. Alice mengenkripsi email dengan alamat email Bob sebagai kunci publik (bob@yahoo.com).
2. Pada saat Bob menerima pesan tersebut, Bob harus menghubungi *key server*. Kemudian *key server* akan menghubungi direktori atau server domain untuk mengautentikasi identitas Bob dan melakukan beberapa peraturan lainnya.
3. Setelah mengautentikasi Bob, *key server* mengirimkan kunci privatnya untuk mendekripsi pesan. Kunci privat ini dapat digunakan untuk mendekripsi semua pesan/email selanjutnya yang diterima oleh Bob.

Dengan demikian, kunci privat hanya perlu dihasilkan satu kali saja pada saat penerimaan pesan pertama. Komunikasi selanjutnya dapat didekripsi menggunakan kunci privat yang sama, sehingga dapat dilakukan ketika *user* sedang '*offline*'. Selain itu, oleh karena kunci publik dihasilkan dengan menggunakan alamat email Bob, Alice dapat mengirimkan pesan tanpa Bob harus telah mengetahui kunci privatnya.

2. Sejarah Kriptografi

Banyak usaha telah dilakukan untuk memecahkan masalah keamanan dalam komunikasi, mulai dari kriptografi simetris dan kriptografi kunci publik tradisional sampai teknologi baru masa kini, yaitu *Identity-Based Encryption*.



Gambar 2 Perkembangan Kriptografi

2.1 Kriptografi Simetris (1960 – 1970)

Pada tahun 1970-an, jaringan militer, sistem akademis, protokol interbank, dan ATM merupakan tahap awal adopsi teknologi kriptografi modern yang menggunakan sistem berdasarkan kriptografi simetris. Kriptografi simetris yang terkenal yaitu *Data Encryption Standard (DES)* sangat banyak digunakan pada tahun 1980-an.

Sifat-sifat sistem kriptografi simetris:

- Pengirim dan penerima menggunakan kunci yang sama baik untuk enkripsi maupun dekripsi.
- Autentikasi dilakukan melalui server sentral.
- Kekurangan dari sistem ini yaitu skalabilitasnya rendah, tidak ada enkripsi 'offline', dan tidak ada interkoneksi antar sistem.

Bagaimanapun, kriptografi simetris cocok digunakan untuk jaringan kecil dengan jumlah *user* yang terbatas, dan tidak dapat menangani volume trafik yang besar seperti trafik pada saat *booming* internet pada tahun 1990-an.

2.2 Kriptografi Asimetris (1980 – 1990)

Untuk mengatasi masalah pada kriptografi simetri, dibuat algoritma baru yang disebut kriptografi asimetris atau kriptografi kunci publik. Pada kriptografi kunci publik, setiap *user* mempunyai sebuah pasangan kunci yang terdiri dari kunci publik dan kunci privat. Pasangan kunci ini dapat dihasilkan oleh *user* sendiri maupun oleh suatu sumber sentral. Dengan demikian, kanal komunikasi yang aman sangat diperlukan untuk mengirimkan pasangan kunci ini kepada *user*. Pasangan kunci ini dihasilkan dengan memilih suatu kunci privat secara acak, kemudian dijalankan suatu fungsi satu arah terhadap kunci privat tersebut untuk menghasilkan kunci publik. Oleh karena digunakan fungsi yang searah sebagai penghasil kunci publik, maka kunci privat tidak dapat diperoleh dari kunci publik.

Setelah diperoleh pasangan kunci untuk *user* tersebut, pihak lain dapat menggunakan kunci publik *user* tersebut untuk mengenkripsi pesan yang ditujukan kepadanya. Hal ini dapat dilakukan oleh siapapun apabila kunci publik dipublikasikan. Di lain pihak, untuk mendekripsi *ciphertext* tersebut, harus digunakan kunci privat yang tentunya hanya diketahui oleh *user* tersebut (penerima).

Masalah utama dalam kriptografi kunci publik adalah autentikasi kunci publik. Apabila seorang penjahat dapat meyakinkan seseorang bahwa kunci publik untuk *user* tertentu adalah suatu kunci palsu yang tentunya bukan kunci publik yang benar, maka penjahat tersebut dapat mendekripsi pesan yang ditujukan kepada *user* tersebut. Oleh karena itu, penting bagi seseorang yang akan mengenkripsi pesan menggunakan kriptografi kunci publik untuk memeriksa keaslian dari kunci publik seorang *user* yang akan digunakannya.

Solusi konvensional untuk masalah di atas yaitu penggunaan *Public-Key Infrastructure (PKI)*. Pada PKI, terdapat satu pihak yang dipercaya oleh semua *user* yang disebut *Certification Authority (CA)* yang dapat menjamin kebenaran kunci publik. *User* dapat mengidentifikasi dirinya kepada CA dan mendapatkan kunci publiknya. Kemudian, *user* mengeluarkan ‘bukti kepemilikan’ dari kunci rahasia yang bersesuaian dengan kunci publiknya, yaitu dengan menandatangani sertifikat. Apabila CA yakin bahwa seorang *user* benar-benar mempunyai kunci rahasia yang bersesuaian dengan kunci publiknya, ia akan mempublikasikan suatu sertifikat yang berisi identitas *user*, kunci publiknya, dan informasi lainnya yang diperlukan, serta menandatangani semua informasi ini dengan kunci rahasianya. Dengan demikian, orang yang akan berkomunikasi secara aman dengan

user tersebut harus mencari sertifikat yang telah dikeluarkan oleh CA. Tanda tangan yang sah dari CA akan meyakinkan kebenaran dari kunci publik tersebut.

Sebagai tambahan, PKI juga membuat beberapa alat otorisasi lainnya dengan tugas yang berbeda. Misalnya, *Registration Authority (RA)* yang menangani prosedur autentikasi, *Validation Authority (VA)* yang menjamin validitas sertifikat, dan sebagainya. Semua alat otorisasi di atas digabungkan menjadi bagian dari CA yang dapat menangani semua tugas di atas.

Dengan demikian, sifat-sifat sistem PKI adalah:

- Pengirim dan penerima menggunakan kunci publik yang berbeda.
- Autentikasi dilakukan melalui sertifikat dan *Certificate Authorities (CA)*.
- Kekurangan dari sistem ini yaitu skalabilitasnya rendah, tidak ada enkripsi *offline*, menaikkan biaya administrasi, dan *end-user* tidak suka menggunakannya.

Walaupun PKI telah menggantikan beberapa sistem *server-side*, seperti SSL, PKI telah terbukti tidak sesuai dengan pemakaian antar perusahaan karena beban sertifikat administratif, masalah daftar pembatalan (*revocation list*), dan masalah *cross-certification*. Persyaratan dalam PKI dimana semua penerima harus mendaftarkan diri terlebih dahulu telah membatasi penggunaannya secara luas.

2.3 Identity-Based Encryption (2001 – sekarang)

Konsep IBE ditemukan pada tahun 1984 oleh Adi Shamir dalam rangka mengatasi masalah autentikasi kunci publik. Idennya adalah untuk menghindari kebutuhan autentikasi dengan cara kunci publik yang digunakan berhubungan langsung dengan identitas *user*. Kunci publik *user* dihasilkan langsung dari informasi publik yang tersedia yang dapat mengidentifikasi *user* tersebut secara unik. Informasi ini disebut sebagai identitas digital *user*. Bergantung pada aplikasi, identitas ini dapat berupa (kombinasi dari) nama *user*, nomer kartu identitas, nomer telepon, alamat email, atau informasi yang mungkin lainnya. Dengan demikian, kunci publik *user* telah siap tersedia untuk siapapun yang mengetahui identitasnya sehingga tidak diperlukan lagi pencarian kunci pada basis data. Selain itu, tidak ada lagi keraguan terhadap keaslian dari kunci publik sehingga menghilangkan kebutuhan akan sertifikat seperti pada PKI. Bagaimanapun, realisasi hubungan antara *user* dengan identitas digitalnya cukup sulit.

Pada sistem kunci publik konvensional, pasangan kunci dihasilkan dengan memilih secara acak sebuah kunci privat dan dengan menggunakan fungsi satu arah diperoleh kunci publik. Pada IBE, pasangan kunci diperoleh dengan cara yang berbeda. Pertama, kunci publik ditentukan berdasarkan identitas *user*. Kemudian kunci privat harus dihasilkan dari kunci publik. Dalam hal ini, pembuatan kunci tidak dapat dilakukan oleh *user* sendiri. Apabila seorang *user* mengetahui bagaimana cara menghasilkan kunci privat yang bersesuaian dengan kunci publiknya, maka ia juga dapat membuat kunci privat untuk *user* lainnya. Oleh karena itu, diperlukan pihak ketiga yang disebut *Privat Key Generator (PKG)*. Setelah melalui suatu prosedur autentikasi, seperti autentikasi kepada CA pada PKI, PKG akan menghasilkan kunci privat *user*. PKG dapat melakukan ini dengan mengetahui suatu informasi rahasia yang disebut *master key*. Informasi yang tersedia untuk umum yang bersesuaian dengan *master key* disebut parameter sistem. Kunci privat dihitung dengan beberapa fungsi satu arah terhadap kunci publik dan *master key*. Dalam hal ini perlu diperhatikan bahwa diperlukan kanal yang aman untuk mengirimkan kunci privat dari PKG ke *user*. Shamir mengusulkan hal ini dilakukan dengan menyimpan kunci privat pada *smart card*.

Dengan konsep IBE, Shamir telah membuat implementasi untuk *Identity-Based Signature*. Implementasi ini mirip dengan RSA yang cukup rumit. Di lain pihak, Shamir melihat bahwa teknik enkripsi RSA tidak dapat dikonversi ke teknik *Identity-Based Encryption*. Hal ini baru terpecahkan pada tahun 2001, dimana Boneh dan Franklin menemukan bahwa sifat bilinear dari *pairing* dapat digunakan untuk mengkonversikan teknik enkripsi ElGamal menjadi IBE. Pada saat yang sama, teknik IBE lainnya juga ditemukan oleh Cocks, yaitu berdasarkan residu kuadratis. Teknik ini kurang populer dan tidak akan dibahas pada makalah ini karena mempunyai kelemahan yaitu tidak efisien, memerlukan *bandwidth* yang besar, dan tidak aman. Oleh karena itu, pada makalah ini akan dibahas teknik IBE berdasarkan *pairing*.

Dengan menggunakan identitas sebagai kunci publik, IBE telah menghilangkan kebutuhan sertifikat yang menjadi masalah pada PKI.

Sifat-sifat sistem IBE:

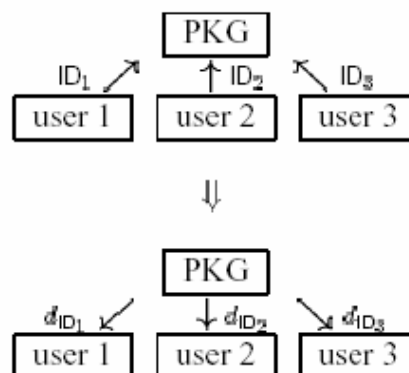
- Kunci publik berdasar pada identitas yang umum, seperti alamat email, dan sebagainya
- Autentikasi dan pelaksanaan kebijaksanaan dilakukan melalui *centrally-administered server*.

- Kelebihan: skalabilitasnya tinggi, enkripsi dapat dilakukan kapanpun dan dimanapun, sekalipun pada saat *offline*, mudah dikelola, dan mudah digunakan.

4. Algoritma *Identity-Based Encryption*

Secara umum, teknik IBE terdiri dari empat algoritma, yaitu:

- *Setup*, yaitu mengambil parameter keamanan sebagai input untuk menentukan parameter sistem dan *master key*. Parameter sistem meliputi deskripsi ruang *plaintext* dan ruang *ciphertext*. Parameter sistem akan dipublikasikan, sedangkan *master key* hanya boleh diketahui oleh PKG. Algoritma ini dijalankan oleh PKG.
- *Extract*, yaitu pembuatan kunci privat d_{ID} yang bersesuaian dengan identitas kunci publik (*string* yang digunakan) dari parameter sistem, *master key*, dan identitas (*string* sembarang) $ID \in \{0,1\}$. Algoritma ini juga dijalankan oleh PKG pada saat *user* meminta kunci privatnya (dengan memberikan *string* yang digunakan untuk menghasilkan kunci publik) untuk mendekripsi pesan. Dalam hal ini, *user* harus membuktikan kepada PKG bahwa dirinya benar-benar pemilik dari identitas atau *string* tersebut.
- *Encrypt*, yaitu mengenkripsi pesan M untuk *user* yang dituju menggunakan kunci publik dan parameter sistem menghasilkan *ciphertext*. Algoritma ini dijalankan oleh *user*.
- *Decrypt*, yaitu mendekripsi *ciphertext* C dengan menggunakan kunci privat d_{ID} dan parameter sistem menghasilkan *plaintext*. Seperti algoritma *encrypt*, algoritma ini juga dijalankan oleh *user*.



Gambar 3 Permintaan kunci privat

Apabila semua algoritma diatas dijalankan dengan benar, maka semua pesan yang dienkripsi dengan algoritma *encrypt* akan terdekripsi dengan benar dengan algoritma *decrypt*.

5. Teknik *Identity-Based Encryption* berdasarkan *Pairing*

5.1 Dasar Matematis

5.1.1 *Bilinear Map*

Bilinear Map merupakan pemetaan $\hat{e} : G_1 \times G_1 \rightarrow G_2$, dimana G_1 dan G_2 merupakan *cyclic group* berderajat p untuk suatu bilangan prima yang besar p . Pemetaan ini harus memenuhi sifat-sifat berikut:

1. Bilinear

Untuk semua $P, Q, R, S \in G_1$, $\hat{e}(P+Q, R+S) = \hat{e}(P, R) \hat{e}(P, S) \hat{e}(Q, R) \hat{e}(Q, S)$.

2. Non-Degenerate

Untuk suatu titik $Q \in G_1$, $\hat{e}(Q, R) = 1_{G_2}$ untuk semua $R \in G_1$ jika dan hanya jika $Q = 0_{G_2}$. Dari sifat ini dan sifat bilinear, jika P adalah penghasil G_1 , maka $\hat{e}(P, P)$ merupakan penghasil G_2 .

3. Computable

Terdapat algoritma yang efisien untuk menghitung $\hat{e}(P, Q)$ untuk setiap $P, Q \in G_1$.

5.1.1 *Bilinear Diffie-Hellman Problem (BDHP)*

BDHP banyak digunakan sebagai dasar keamanan dari IBE. BDHP pada $\langle G_1, G_2, \hat{e} \rangle$ dimana G_1 dan G_2 merupakan *cyclic groups* berderajat p dan $G_1 \times G_1 \rightarrow G_2$ merupakan *bilinear map*, dapat dinyatakan sebagai: diberikan generator P dari G_1 dan tiga elemen $aP, bP, cP \in G_1$ untuk a, b, c acak pada Z_p untuk menghitung $\hat{e}(P, P)^{abc}$.

5.2 Teknik *Identity-Based Encryption* Boneh-Franklin

Teknik IBE oleh Boneh dan Franklin merupakan teknik IBE pertama yang efisien dan aman. Untuk mengenkripsi pesan, pengirim menggunakan bilinear map untuk menggabungkan identitas penerima, parameter sistem dari PKG dan *master key* menjadi kunci untuk enkripsi. Penerima pesan dapat menghasilkan kunci untuk dekripsi dengan menggunakan bilinear map untuk menggabungkan kunci privat penerima dan parameter

publik yang dikirimkan bersama *ciphertext*. Secara umum, teknik ini dapat dideskripsikan sebagai berikut:

Setup

Untuk menginisialisasi IBE, PKG mengambil sebuah titik kurva elips, sebuah *master key* s , dan sebuah titik P pada kurva elips menggunakan generator angka acak. Kemudian, parameter publik, yaitu P dan $s \cdot P$ didistribusikan ke semua *user*, biasanya melalui sertifikat server. *Master key* s juga dapat di-*share* secara rahasia sehingga tidak ada server yang dapat berkompromi dengan sistem.

Extract

Pada saat Bob menerima pesan Alice, Bob belum mempunyai kunci k untuk mendekripsi. Untuk memperoleh kunci tersebut, Bob melakukan autentikasi ke PKG. Setelah Bob diautentikasi, server menghitung $s \cdot ID_{Bob}$ dan memberikannya kepada Bob. Nilai ini merupakan kunci privat Bob.

Encrypt

Untuk mengirim pesan ke Bob, Alice memetakan identitas Bob (misalnya bob@yahoo.com) ke suatu titik pada kurva elips ID_{Bob} . Kemudian Alice memilih suatu angka acak r dan menghitung kunci k , sebagai berikut:

$$k = \text{Pair} (r \cdot ID_{Bob}, s \cdot P)$$

Setelah mendapatkan kunci, Alice mengirimkan pesan yang dienkripsi dengan k , $E_k[\text{Pesan}]$, kepada Bob. Selain itu dikirimkan juga hasil perkalian $r \cdot P$.

Decrypt

Setelah menerima pesan beserta hasil perkalian $r \cdot P$, Bob dapat memperoleh kunci k dengan menghitung:

$$k = \text{Pair} (s \cdot ID_{Bob}, r \cdot P)$$

Kunci k di atas, oleh karena sifat *bilinear map*, sama dengan kunci yang digunakan Alice untuk mengenkripsi pesan, yaitu:

$$k = \text{Pair} (r \cdot ID_{Bob}, s \cdot P)$$

Dengan kunci k tersebut, Bob dapat mendekripsi pesan yang diterimanya. Oleh karena hanya Bob yang mengetahui kunci privatnya, yaitu $s \cdot ID_{Bob}$, maka tidak ada orang lain yang dapat menghitung k .

Secara matematis, teknik IBE Boneh-Franklin adalah sebagai berikut:

Setup

Diberikan parameter keamanan k , kemudian

(1) dibuat *cyclic group* G_1, G_2 dari bilangan prima berderajat p bersama dengan bilinear map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ yang bersesuaian dengan parameter keamanan (misalkan p merupakan k -bit bilangan prima). Ambil generator acak $P \in G_1$.

(2) pilih bilangan acak $s \in \mathbb{Z}_p^*$ dan hitung $P_{pub} = sP$

(3) pilih *hash function* kriptografi

$$H_1 : \{0,1\}^* \rightarrow G_1^*$$

$$H_2 : G_2 \rightarrow \{0,1\}^n,$$

$$H_3 : \{0,1\}^n \times \{0,1\}^n \rightarrow \mathbb{Z}_p^*,$$

$$H_4 : \{0,1\}^n \rightarrow \{0,1\}^n \text{ untuk bilangan bulat } n > 0.$$

Ruang *plaintext* adalah $\mathcal{M} = \{0,1\}^n$ dan ruang *ciphertext* adalah $\mathcal{C} = G_1^* \times \{0,1\}^n \times \{0,1\}^n$.

Parameter sistem adalah $\langle G_1, G_2, \hat{e}, p, n, P, P_{pub}, H_1, H_2, H_3, H_4 \rangle$. *Master key* adalah s .

Extract

Diberikan suatu *string* $ID \in \{0,1\}^*$, *master key* s dan parameter sistem untuk menghitung

$$Q_{ID} = H_1(ID) \in G_1^* \text{ dan kunci privat } d_{ID} = sQ_{ID}.$$

Encrypt

Diberikan *plaintext* $M \in \mathcal{M}$, identitas dan parameter publik, kemudian:

(1) hitung $Q_{ID} = H_1(ID)$

(2) pilih secara acak $s \in \{0,1\}^n$ dan hitung $r = H_3(s, M)$

(3) hitung $g = \hat{e}(P_{pub}, Q_{ID})$

(4) *ciphertext* $C = \langle rP, s \oplus H_2(g^r), M \oplus H_4(s) \rangle$

Decrypt

Diberikan *ciphertext* $\langle U, V, W \rangle \in \mathcal{C}$, kunci privat d_{ID} dan parameter sistem, maka:

(1) hitung $g' = \hat{e}(U, d_{ID})$

(2) hitung $s = V \oplus H_2(g')$

(3) hitung $M = W \oplus H_4(s)$

(4) hitung $r = H_3(s, M)$. Apabila $U \neq rP$, maka tolak *ciphertext* dan *plaintext* tidak dapat ditemukan.

Perhatikan bahwa M dienkrpsi sebagai $M = W \oplus H_4(s)$. Persamaan ini dapat digantikan dengan $W = E_{H_4(s)}(M)$, dimana E adalah kriptografi simetris yang aman secara semantik.

Pada teknik ini, keamanan dari *master key* pada PKG sangat penting karena keamanan dari kunci privat lainnya bergantung pada PKG. Salah satu cara untuk meningkatkan keamanan adalah pendistribusian *master key* diantara beberapa PKG menggunakan kriptografi threshold. *Master key* didistribusikan dalam beberapa bagian dengan memberikan setiap PKG satu bagian s_i .

5.2 Authenticated Identity-Based Encryption

Teknik ini merupakan pengembangan dari teknik IBE Boneh-Franklin oleh Lynn yang menemukan bahwa teknik IBE Boneh-Franklin dapat dimodifikasi untuk ditambahkan autentikasi. Pada saat penerimaan pesan, penerima dapat memeriksa identitas pengirim dan memeriksa apakah pesan masih utuh. Hal ini menghilangkan kebutuhan *digital signature* pada saat autentikasi. Tingkat keamanan dalam hal ini adalah sama dengan keamanan pada percakapan pribadi, yaitu komunikasi yang aman tanpa memerlukan pihak ketiga. Untuk penambahan autentikasi ini, bilinear map digunakan untuk menggabungkan identitas dari pengirim dan penerima. Kunci kemudian di-hash dengan nilai acak untuk memperoleh kunci yang berbeda setiap kali enkripsi dilakukan.

Setup

Algoritma ini sama seperti pada IBE Boneh-Franklin kecuali, *hash function* H_2 harus didefinisikan sebagai: $H_2 : \mathbb{Z}_p \times G_2 \rightarrow \{0,1\}^n$ untuk $n > 0$. Ruang *plaintext* adalah $\mathcal{M} = \{0,1\}^n$, dan ruang *ciphertext* adalah $\mathcal{C} = \mathbb{Z}_p \times \{0,1\}^n \times \{0,1\}^n$. Parameter sistem adalah $\langle G_1, G_2, \hat{e}, p, n, H_1, H_2, H_3, H_4 \rangle$. *Master key* adalah s .

Extract

Algoritma ini sama seperti pada teknik IBE Boneh-Franklin.

Encrypt

Diberikan *plaintext* $M \in \mathcal{M}$, kunci privat A d_{ID_A} , kunci publik (identitas) B ID_B dan parameter sistem,

- (1) pilih bilangan acak $s \in \{0,1\}^n$
- (2) hitung $r = H_3(s, M)$
- (3) hitung $g = \hat{e}(d_{ID_A}, H_1(ID_B))$
- (4) *ciphertext* menjadi $C = \langle r, s \oplus H_2(r, g), M \oplus H_4(s) \rangle$

Decrypt

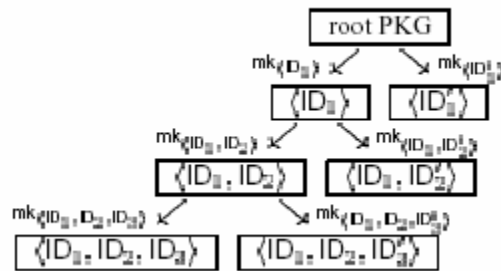
Diberikan *ciphertext* $\langle U, V, W \rangle \in \mathcal{C}$, kunci publik (identitas) A ID_A , kunci privat B d_{ID_B} dan parameter sistem,

- (1) hitung $g = \hat{e}(H_1(ID_A), d_{ID_B})$
- (2) hitung $s = V \oplus H_2(U, g)$
- (3) hitung $M = W \oplus H_4(s)$
- (4) hitung $r = H_3(s, M)$. Apabila $U \neq r$, maka tolak *ciphertext* dan *plaintext* tidak dapat ditemukan.

Seperti pada sebelumnya, $M = W \oplus H_4(s)$ dapat digantikan dengan $W = E_{H_4(s)}(M)$, dimana E adalah kriptografi simetris yang aman secara semantik.

5.3 Hierarchical Identity-Based Encryption

Salah satu kelemahan dari kedua teknik IBE sebelumnya adalah bahwa pada jaringan yang besar, PKG akan memperoleh pekerjaan yang sangat banyak. Salah satu solusi untuk masalah ini adalah membuat sistem dengan adanya hirarki pdari PKG. Dengan demikian, PKG hanya akan menghitung kunci privat dari entitas yang ada dibawahnya pada hirarki. Pada sistem ini, *user* tidak lagi direpresentasikan dengan *string* identitas, melainkan dengan deretan identitas yang terdiri dari identitas 'nenek moyangnya' pada hirarki. Contohnya, $\langle ID_1, \dots, ID_i \rangle$ akan menjadi parent dari $\langle ID_1, \dots, ID_{i+1} \rangle$. Pada sistem ini, identitas dari setiap entitas pada hirarki kecuali root dapat dijadikan kunci publik.



Gambar 4 Hirarki PKG

Root Setup

Diberikan parameter keamanan k

- (1) buat *cyclic group* G_1, G_2 dari bilangan prima berderajat p bersama dengan bilinear map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ yang bersesuaian dengan parameter keamanan (misalkan p merupakan k -bit bilangan prima). Ambil generator acak $P_e \in G_1$.

(2) Pilih bilangan acak $s_e \in Z_p^*$ dan hitung $Q_e = s_e P_e$

(3) Pilih *hash function* kriptografi

$$H_1 : \{0,1\}^* \rightarrow G_1^*,$$

$$H_2 : G_2^* \rightarrow \{0,1\}^*,$$

$$H_3 : \{0,1\}^n \times \{0,1\}^n \rightarrow Z_p^* \text{ dan}$$

$$H_4 : \{0,1\}^n \rightarrow \{0,1\}^n \text{ untuk bilangan bulat } n > 0.$$

Ruang *plaintext* adalah $M = \{0,1\}^n$ dan ruang *ciphertext* adalah $C = G_1^{*l} \times \{0,1\}^n \times \{0,1\}^n$.

Parameter sistem adalah $\langle G_1, G_2, \hat{e}, p, n, P_e, Q_e, H_1, H_2, H_3, H_4 \rangle$. *Master key root* adalah s_e .

Lower-level Setup

Diberikan parameter sistem, setiap entitas $E_{\overline{ID}(i)}$ selain root memilih secara acak $s_{\overline{ID}(i)} \in Z_p^*$ dan menghitung $Q_{\overline{ID}(i)} = s_{\overline{ID}(i)} P_e$ yang kemudian dirahasiakan.

Extract

Diberikan $\langle ID_1, \dots, ID_l \rangle$ dari salah satu anak, kunci privatnya $mk_{\overline{ID}(i-1)} = \langle S_{\overline{ID}(i-1)}, Q_e, Q_{\overline{ID}(1)}, \dots, Q_{\overline{ID}(i)} \rangle$, *master keynya* $s_{\overline{ID}(i-1)}$ dan parameter sistem. Kemudian PKG dari $E_{\overline{ID}(i-1)}$ menghitung kunci privat sebagai berikut:

(1) hitung $P_{\overline{ID}(i)} = H_1(\overline{ID}(i))$

(2) hitung $S_{\overline{ID}(i)} = S_{\overline{ID}(i-1)} + s_{\overline{ID}(i-1)} P_{\overline{ID}(i)}$

(3) kunci privat *user* adalah $\langle S_{\overline{ID}(i)}, Q_e, Q_{\overline{ID}(1)}, \dots, Q_{\overline{ID}(i-1)} \rangle$ (*user* telah mengetahui $Q_{\overline{ID}(i)}$)

Encrypt

Diberikan *plaintext* $M \in M$, $\langle ID_1, \dots, ID_l \rangle$ dan parameter sistem,

(1) hitung $P_{\overline{ID}(i)} = H_1(\overline{ID}(i))$ untuk $1 \leq i \leq l$

(2) hitung $g = \hat{e}(Q_e, P_{\overline{ID}(1)})$

(3) pilih secara acak $S \in \{0,1\}^n$ dan hitung $r = H_3(S, M)$

(4) *ciphertext* $C = \langle rP_e, rP_{\overline{ID}(2)}, \dots, P_{\overline{ID}(l)}, S \oplus H_2(g^r), M \oplus H_4(S) \rangle$

Decrypt

Diberikan *ciphertext* $C = \langle U_0, U_2, \dots, U_l, V, W \rangle \in C$, kunci privat $\langle S_{\overline{ID}(i)}, Q_e, Q_{\overline{ID}(1)}, \dots, Q_{\overline{ID}(i-1)} \rangle$ dan parameter sistem,

(1) hitung

$$g' = \frac{\hat{e}(U_0, S_{\overline{ID}(l)})}{\prod_{i=2}^l \hat{e}(Q_{\overline{ID}(i-1)}, U_i)}$$

- (2) hitung $s = V \oplus H_2(g')$
- (3) hitung $M = W \oplus H_4(s)$
- (4) hitung $r = H_3(s, M)$. Apabila $U \neq rP_e$, maka tolak *ciphertext* dan *plaintext* tidak dapat ditemukan.

Seperti pada sebelumnya, $M = W \oplus H_4(s)$ dapat digantikan dengan $W = E_{H_4(s)}(M)$, dimana E adalah kriptografi simetris yang aman secara semantik.

6. Keamanan pada *Identity-Based Encryption*

Ada beberapa konsep keamanan pada enkripsi kunci publik, antara lain *semantic security* dan *chosen ciphertext security*. *Chosen ciphertext security* cukup sesuai untuk banyak aplikasi sehingga cocok sebagai keamanan untuk enkripsi kunci publik konvensional. Berikut akan dijelaskan masing-masing konsep keamanan di atas.

6.1 *Semantic Security*

Teknik enkripsi kunci publik sudah aman secara semantik apabila seseorang yang diberi *ciphertext* yang telah dienkripsi dengan beberapa kunci publik tidak dapat mempelajari apapun mengenai *plaintext* yang bersesuaian. Hal ini dapat diilustrasikan dengan sebuah permainan antara penantang dengan lawannya. Misalkan penantang memberikan lawannya suatu kunci publik secara acak. Kemudian lawan diberi dua pesan, dimana salah satu pesan dipilih secara acak dan yang lainnya merupakan pesan yang dienkripsi oleh penantang dengan kunci publik tersebut. Apabila lawan dapat menebak pesan mana yang dienkripsi dengan kunci publik tersebut, maka lawan memenangkan permainan. Sistem dapat dikatakan aman secara semantik apabila lawan tidak dapat memenangkan permainan dengan probabilitas yang tidak dapat diabaikan lebih dari setengah.

Gagasan keamanan di atas harus diperkuat agar memenuhi kebutuhan keamanan pada IBE yang setiap nilai dapat digunakan sebagai kunci publik, khususnya, kunci publik yang tidak acak. Oleh karena itu, seseorang dapat mempunyai akses ke beberapa kunci privat yang bersesuaian dengan kunci publik yang dipilihnya. Selain itu, teknik IBE harus aman terhadap serangan pada enkripsi kunci publik yang dipilih sendiri, bukan kunci publik yang dipilih secara acak. Berikut akan dijelaskan bagaimana gagasan *semantic security* diperbaiki sehingga dapat memenuhi situasi yang baru.

Untuk mengilustrasikan *semantic security* dalam IBE, misalkan seorang penantang dan lawannya yang bermain seperti pada permainan di atas. Hanya dalam hal ini, lawan dapat memilih kunci publik yang diinginkan untuk ditebak kunci privatnya. Lawan juga

diberi kesempatan tambahan untuk mengeluarkan beberapa pertanyaan mengenai pembuatan kunci kepada penantang. Lawan mengeluarkan kunci publik pilihannya dan penantang meresponnya dengan kunci privat yang bersesuaian. Tetapi lawan tidak boleh menanyakan kunci privat untuk kunci publik yang diberikan oleh penantang. IBE dapat dikatakan aman secara semantik apabila lawan tidak dapat memenangkan permainan dengan probabilitas lebih dari setengah.

6.2 *Chosen ciphertext security*

Chosen ciphertext security, dapat diilustrasikan dengan permainan yang mirip seperti di atas, hanya pada permainan ini, lawan diberi kesempatan tambahan untuk mengeluarkan beberapa pertanyaan kepada penantang. Lawan mengeluarkan *ciphertext* yang dipilihnya dan penantang merespon dengan hasil dekripsi *ciphertext* tersebut dengan kunci privat yang bersesuaian dengan kunci publik yang diberikan kepada lawan. Lawan hanya tidak boleh mengeluarkan pertanyaan untuk *ciphertext* yang dikeluarkan oleh penantang. Sistem kunci publik standar dapat dikatakan aman dengan *chosen ciphertext* apabila lawan tidak dapat memenangkan permainan dengan probabilitas lebih dari setengah. *Chosen ciphertext security* secara tidak langsung menyatakan bahwa apabila diberikan sebuah *ciphertext* dan sebuah kunci publik, seseorang tidak dapat mempelajari apapun mengenai pesan asli (*plaintext*)nya walaupun ia mengetahui hasil dekripsi dari beberapa *ciphertext* lainnya.

Berikut akan dijelaskan bagaimana *chosen ciphertext security* diperbaiki untuk IBE. Seperti pada permainan sebelumnya, pada *chosen ciphertext security* lawan dapat memilih kunci publik yang diinginkan untuk ditebak kunci privatnya. Selain itu, lawan juga diberi kesempatan untuk menanyakan hasil deskripsi dari suatu *ciphertext* yang dienkripsi menggunakan suatu kunci publik kepada penantang. IBE dapat dikatakan aman dengan *chosen ciphertext* apabila lawan tidak dapat memenangkan permainan dengan probabilitas lebih dari setengah.

7. Perbandingan IBE dengan PKI

Sistem IBE dan PKI keduanya adalah asimetris. Oleh karena itu, protokol untuk enkripsi, dekripsi, penandatanganan dan pemeriksaan tanda tangan mempunyai fungsi yang mirip untuk kedua sistem. Perbedaan utama antara keduanya adalah manajemen kunci. IBE pertama kali diusulkan untuk menghindari kebutuhan sertifikat untuk autentikasi kunci publik. Pada kenyataannya, sistem IBE memenuhi sifat-sifat sebagai berikut:

- *User* hanya perlu mengetahui identitas *user* yang diinginkan untuk berkomunikasi

- Tidak diperlukan basis data untuk menyimpan kunci publik atau sertifikat
- Layanan PKG hanya diperlukan selama *set-up* sistem.
- Berikut akan dibandingkan IBE dengan PKI dalam hal autentikasi parameter sistem, pendaftaran pada *authority*, *key escrow*, *key revocation* dan *key rollover*, pendistribusian kunci, keamanan *master key*, skalabilitas dan *commercial maturity*.

⊕ Autentikasi sistem parameter

Misalkan penyerang pada IBE membuat *master key* sendiri dan parameter sistem yang bersesuaian dengan kunci tersebut. Kemudian ia membohongi *user* bahwa parameter sistem yang palsu tersebut adalah benar. Untuk kunci publik apapun, ia dapat membuat kunci privat yang bersesuaian dengan menggunakan *master key*nya. Dengan demikian ia dapat mendekripsi pesan yang dienkripsi dengan parameter sistem yang palsu tersebut. Selain itu, ia juga dapat membuat *signature* atas nama siapapun, yang akan diterima oleh *user* yang mempercayai parameternya. Penyerang juga mungkin dapat berpura-pura menjadi PKG dan mengeluarkan kunci privat yang diminta oleh *user*. Dengan demikian, sangat penting bahwa PKG menjamin keaslian dari parameter sistem.

Masalah serupa juga terjadi pada sistem PKI, dimana *user* harus diyakinkan mengenai keaslian kunci publik dari CA. Apabila penyerang dapat meyakinkan *user* bahwa kunci publik tertentu merupakan kunci publik asli dari CA, ia dapat membuat sertifikat yang berisi kunci publik palsu yang telah diketahui kunci privatnya. Konsekuensinya, penyerang dapat membaca pesan yang terenkripsi dengan kunci publik palsu tersebut dan membuat *signature* yang terlihat sah untuk kunci tersebut. Perbedaan dengan IBE yaitu bahwa penyerang tidak dapat berpura-pura menjadi CA sehingga *user* dapat terperingati bahwa sertifikat yang dimintanya berisi kunci publik yang salah.

⊕ Pendaftaran pada *authority*

Pada kedua sistem, *user* yang ingin berpartisipasi harus mendaftar pada RA yang merupakan bagian dari CA atau PKG. Setelah melakukan prosedur autentikasi, RA mengeluarkan identitas digital yang unik untuk *user*. Pada sistem PKI, *user* dapat memberikan identitas digital dan kunci publiknya kepada CA dengan bukti kepemilikan kunci privat yang bersesuaian. CA kemudian mengeluarkan sertifikat yang menggabungkan identitas digital dan kunci publiknya. Pada IBE, *user* memberikan identitas digitalnya kepada PKG. RA bertanggung jawab untuk keunikan identitas digital dan hubungan antara identitas dengan *user* secara fisik. Kemudian PKG menghitung

kunci privat yang bersesuaian dengan kunci publik yang diperoleh dari identitas digitalnya.

Sistem IBE mempunyai kelemahan yaitu kunci privat harus dikirimkan dari PKG kepada *user*. Oleh karena itu, kanal yang aman diperlukan untuk menjamin kerahasiaan dan keaslian kunci tersebut. Oleh karena itu, sistem IBE akan bekerja sangat baik pada aplikasi dimana mudah membuat suatu kanal yang aman (misalkan pada sistem kecil) atau dimana *user* jarang meminta kunci privat.

✦ *Key escrow*

IBE mempunyai pihak ketiga yang menangani kunci, yaitu PKG. Oleh karena PKG mempunyai *master key*, maka PKG dapat menghasilkan kunci privat. Bergantung pada aplikasinya, pihak ketiga dalam sistem belum tentu hal yang buruk. Pihak ketiga dapat memungkinkan penemuan kembali kunci yang hilang. Adanya pihak ketiga pada PKI memang memungkinkan terjadinya penipuan. Di lain pihak, apabila *user* menghasilkan pasangan kunci sendiri dan *central authority* tidak menyimpan kunci tersebut, maka kunci yang hilang tidak dapat ditemukan kembali. Hal ini bertentangan dengan IBE dimana PKG dapat menghasilkan kembali kunci yang hilang.

Teknik IBE oleh Boneh dan Franklin memberikan cara untuk mengatasi masalah di atas yaitu dengan pembuatan beberapa PKG. Masing-masing PKG mempunyai *master key* sendiri. *User* memberikan kunci publiknya kepada masing-masing PKG dan akan mendapatkan bagian-bagian kunci privatnya dari setiap PKG. Kunci privat dapat diperoleh dengan menggabungkan semua bagian kunci privat tersebut. Dalam kasus ini, pembuatan kembali kunci privat terdistribusi ke semua PKG. Secara praktis, membuat sistem dengan banyak PKG sangatlah kompleks. Selain itu, beban pekerjaan menjadi beberapa kali lipat lebih besar karena setiap PKG harus melakukan pekerjaan yang sama seperti pada sistem dengan satu PKG. Oleh karena itu, IBE akan bekerja dengan baik pada aplikasi dimana pihak ketiga tidak menjadi masalah atau dimana jumlah *user* cukup kecil untuk memungkinkan sistem dengan banyak PKG.

✦ *Key revocation dan key rollover*

Pada waktu sertifikat dicabut pada PKI, *user* lain diberitahukan dengan *Certificate Revocation List (CRL)*. Hal ini terjadi pada saat *user* meninggalkan kelompoknya atau suatu kunci privat terbongkar. Pada saat kunci privat terbongkar atau pada saat pasangan kunci harus diganti setelah sertifikatnya kadaluarsa, *user* dapat menghasilkan pasangan kunci baru dan memperoleh sertifikatnya. Daftar pencabutan yang memungkinkan *user*

memeriksa validitas kunci publik, dapat juga digunakan pada IBE. Tetapi, karena kunci publik *user* dihasilkan dari identitasnya, *user* tidak dapat memperoleh pasangan kunci yang baru dengan mudah setelah pencabutan seperti pada PKI karena tidak mungkin mengubah identitas setiap kali diperlukan pembaharuan kunci.

Solusi untuk masalah ini adalah dengan membuat kunci publik bukan semata-mata dari identitas, tetapi dengan merangkaikan identitas dengan informasi lainnya. Contohnya, apabila tahun dimasukkan ke dalam identitas, *user* hanya dapat menggunakan kunci privatnya selama tahun tersebut. Dengan demikian, kunci privat akan kadaluarsa setiap tahunnya dan setiap *user* harus meminta kunci baru setiap tahun. Tidak seperti pada PKI, *user* tidak harus memperoleh sertifikat baru *user* lain karena kunci publik tetap unik dan mudah diketahui (karena tahun merupakan informasi yang umum). Tetapi terdapat kemungkinan bahwa kunci privat terbongkar pada pertengahan tahun yang menyebabkan *user* harus menunggu sampai akhir tahun sebelum mendapatkan kunci yang baru. Situasi ini dapat diatasi dengan merangkaikan identitas dengan tanggal sehingga interval waktunya lebih pendek. Kelemahan dari solusi ini adalah tidak efisien dimana setiap *user* harus memperbaharui kuncinya setiap hari.

Solusi lain yaitu dengan merangkai identitas dengan beberapa informasi khusus. Contohnya, informasi yang sederhana seperti nomer indeks, atau tanggal pengeluaran kunci. Dalam kasus ini, apabila kunci terbongkar, *user* dapat meminta kunci baru dengan menaikkan indeks atau mengubah tanggal pengeluaran kunci. Hal ini akan menghilangkan sifat unik dari IBE dimana kunci publik dapat dihasilkan dari identitas (digabungkan dengan informasi yang umum) semata-mata. Dengan demikian, *user* lain harus mencari nomer indeks atau tanggal pengeluaran kunci pada tempat penyimpanan tertentu. Hal ini akan membawa pada masalah autentikasi seperti pada kriptografi kunci publik.

✚ Pendistribusian kunci

Penyederhanaan distribusi kunci merupakan alasan diperkenalkannya IBE yang kunci publiknya dihasilkan dari identitas *user*. Dengan demikian, prosedur memperoleh kunci publik seseorang untuk enkripsi menjadi sederhana dan transparan. Sebaliknya pada PKI, seseorang harus mencari sertifikat, memeriksa *signature* CA dan tanggal kadaluarsa sertifikat. Selain itu, seseorang juga harus memeriksa keaslian sertifikat yang dapat dilakukan dengan melihat CRL atau memeriksa secara online pada *Validation Authority*.

⊕ Keamanan *Master key*

PKG dalam IBE mempunyai satu kelemahan. Penyerang yang dapat memperoleh *master key* PKG dapat menghasilkan semua kunci privat dan oleh karena itu dapat membaca semua pesan dan memalsukan *signature* atas nama siapapun. Oleh karena itu, sangat penting untuk menjaga *master key* tetap rahasia. Untuk mencegah *master key* disimpan pada satu tempat, *master key* dapat didistribusikan ke beberapa PKG seperti pada pencegahan *key escrow*. Pada tingkat yang lebih kecil, CA pada PKI merupakan suatu kelemahan. Apabila kunci privat CA terbongkar, penyerang dapat membuat sertifikat atas nama CA untuk suatu kunci publik baru untuk membohongi *user* lain agar mempercayai keaslian kunci publik tersebut. Tetapi, pengetahuan mengenai kunci privat CA tidak memungkinkan penyerang mendapatkan kunci privat yang telah ada sebelumnya. Jadi penyerang tidak dapat membaca pesan yang dienkripsi dengan kunci publik yang telah ada sebelumnya atau memalsukan *signature* dengan kunci privat tersebut.

⊕ Skalabilitas

Pada IBE, PKG harus melakukan pemeriksaan keaslian dan menghitung kunci privat untuk setiap permintaan kunci. Hal ini dapat mengakibatkan beban kerja yang berat untuk PKG terutama apabila jumlah permintaan kunci besar seperti pada sistem yang masa kadaluarsanya pendek. Solusi dari masalah ini adalah dengan menyebar pekerjaan ke beberapa PKG. Solusi ini tidak dapat digunakan untuk mencegah *key escrow* atau meningkatkan keamanan karena pendistribusian *master key*. Dalam kasus ini, setiap PKG harus melakukan beban pekerjaan yang sama dengan sistem dengan satu PKG. Dari sini terlihat bahwa IBE akan baik jika digunakan dalam skala kecil.

⊕ *Commercial Maturity*

Realisasi IBE dengan *pairing* merupakan teknologi yang sangat baru. Walaupun kriptografi IBE menjanjikan, terdapat beberapa kekurangan pada saat diimplementasikan pada aplikasi praktis. Selain itu, teknologi sekarang kebanyakan muncul dengan teori dan sulit untuk diimplementasikan. Sebaliknya, teknologi PKI telah muncul dan tersebar sejak beberapa tahun yang lalu. Selain itu, tidak seperti IBC, PKI telah distandarisasi secara luas. Melihat sifat konservatif dari organisasi yang menggunakan PKI, IBE akan sulit untuk menggantikan PKI dalam waktu dekat.

8. Kelebihan dan Kekurangan IBE

Kelebihan utama dari IBE adalah kesederhanaannya. Dengan menggunakan pengidentifikasi yang sudah banyak dikenal, seperti alamat email, sebagai kunci publik, IBE memudahkan mekanisme pengamanan komunikasi, dimana pesan secara langsung dapat dienkripsi dan di autentikasi. Dengan kesederhanaannya, IBE dapat digunakan untuk membangun sistem keamanan yang lebih dinamis, kecil, dan berskalabilitas tinggi.

Kelebihan-kelebihan IBE secara lebih rinci antara lain:

- Pada sistem kriptografi kunci publik yang sudah ada (PKI), diperlukan sertifikat untuk memperoleh kunci publik. Tidak seperti pada PKI, pada IBE pengirim dapat mengenkripsi pesan ke penerima tanpa perlu adanya sertifikat karena kuncinya adalah identitas. Dengan demikian IBE telah menghilangkan kebutuhan akan sertifikat yang tidak praktis. Hal ini merupakan fitur yang sangat penting untuk membuat produk email yang terpisah-pisah atau bagi perusahaan yang menyebarkan solusi keamanan email secara bertahap. Dengan menghilangkan kebutuhan akan sertifikat, IBE telah membuang kesulitan pada PKI, yaitu pencarian sertifikat, manajemen *lifecycle*, daftar pencabutan sertifikat (*Certificate Revocation List*), dan masalah *cross-certification*.
- Sekali klien mendapatkan parameter publik dari “*security district*” penerima, pengirim email (klien) tersebut dapat mengenkripsi pesan untuk seluruh anggota pada “*security district*” tersebut, sekalipun pada waktu *offline*. Pada PKI (*Public Key Infrastructure*) tradisional, setiap penerima email mempunyai sertifikat digital yang unik yang harus ada sebelum percakapan yang aman dapat dilakukan. Dengan IBE, pengirim tetap memerlukan parameter publik penerima, tetapi apabila pengirim berkomunikasi dengan sejumlah orang yang termasuk di dalam domain tertentu, pengirim dapat menggunakan parameter publik yang telah diperoleh sebelumnya untuk satu penerima, untuk menghasilkan kunci untuk penerima lainnya yang masih dalam “*security district*” yang sama.

9. Aplikasi dari *Identity-Based Encryption*

9.1 *Revocation of Public Key* (Pencabutan Kunci Publik)

Pada sertifikat kunci publik terdapat tanggal kadaluarsa. Pada IBE, kunci publik dapat dibuat kadaluarsa dengan mengenkripsi pesan menggunakan kunci publik “alamat penerima || tanggal”, dimana tanggal dapat berupa hari, minggu, bulan ataupun tahun,

bergantung pada periode yang ditentukan dimana *user* harus memperbaharui kunci publiknya. Tidak seperti pada PKI tradisional, pada IBE pengirim tidak perlu memperoleh sertifikat baru setiap kali kunci privat diperaharui, sedangkan penerima harus menghubungi PKG untuk memperoleh kunci privat barunya. Dengan demikian, IBE sangat efisien dalam mengimplementasikan sistem kunci publik.

Aplikasi ini sangat berguna, dimana apabila kunci privat disimpan pada laptop yang kemudian dicuri, kunci privat pada periode waktu itu saja yang terbongkar, sedangkan *master key* tetap terjaga. Aplikasi ini juga dapat digunakan untuk mengirim pesan untuk tanggal tertentu. Dengan menggunakan tanggal yang diinginkan dan identitas penerima sebagai kunci publik untuk enkripsi, penerima tidak dapat mendekripsi pesan tersebut sampai ia memperoleh kunci privatnya dari PKG pada tanggal yang telah ditentukan oleh pengirim.

9.2 *Managing User Credentials (Manajemen Pemberian Perintah kepada User)*

Aplikasi ini dapat digunakan untuk memberi suatu persyaratan yang harus dipenuhi sebelum pesan yang terenkripsi tersebut dapat dibaca. Hal ini dapat dilakukan dengan mengenkripsi pesan menggunakan “alamat penerima || tanggal || kondisi”. Penerima dapat mendekripsi pesan tersebut apabila kondisi telah dipenuhi. Dalam hal ini, PKG dapat digunakan untuk memberikan perintah kepada *user* (penerima). Untuk mencabut perintah ini, PKG akan menghentikan pemberian kunci privat tersebut pada periode waktu selanjutnya.

9.3 *Delegations of decryption keys*

Misalkan seorang manajer mempunyai beberapa asisten yang masing-masing mempunyai kewajiban yang berbeda. Manajer dapat bertindak sebagai PKG dan memberi kunci privat kepada asisten-asistennya sesuai dengan kewajibannya masing-masing. Dalam hal ini, kunci publik merupakan kewajiban masing-masing asisten. Dengan demikian, setiap asisten dapat mendekripsi pesan yang sesuai dengan kewajibannya tetapi tidak dapat mendekripsi pesan yang ditujukan untuk asisten lainnya. Sedangkan manager dapat mendekripsi semua pesan menggunakan *master key*nya.

9.4 *Forward-secure encryption*

Pada aplikasi ini, kunci privat penerima berubah setiap periode waktu tertentu, sehingga apabila kunci privat dari suatu periode waktu terbongkar, semua pesan yang dienkripsi pada periode sebelumnya tetap aman.

Ada teknik lain yang disebut *key-insulated encryption* dimana kunci privat dibagi menjadi dua bagian. Kedua bagian ini juga berubah setiap interval waktu dan harus digabungkan untuk memperoleh kunci privat untuk dekripsi. Kunci ini dapat diketahui orang lain hanya apabila keduanya terbongkar pada periode waktu yang sama.

10. Kesimpulan

Identity-Based Encryption merupakan teknik kriptografi yang dapat mengatasi masalah-masalah yang terjadi pada teknik kriptografi tradisional, antara lain kebutuhan keamanan yang belum dapat diatasi dengan teknik kriptografi tradisional dan masalah penanganan sertifikat. IBE telah mengatasi masalah ini dengan suatu sistem dimana dapat digunakan *string* sembarang sebagai kunci publik.

Dengan menggunakan identitas sebagai kunci publik, IBE telah menghilangkan sistem sertifikat yang kompleks dan infrastruktur lainnya. Aplikasi IBE secara praktis telah memberikan solusi yang mudah untuk diimplementasikan dan mudah diatur. Teknik IBE berdasarkan bilinear map merupakan salah satu teknik yang menjanjikan antara lain karena mempunyai model keamanan yang kuat.

11. Daftar Pustaka

Dan Boneh, Matthew Franklin . *Identity-Based Encryption from the Weil Pairing*. <http://crypto.stanford.edu/~dabo/papers/ibe.pdf> . 2001.

www.voltage.com/technology/ibe.htm

Ran Canetti, Shai Halevi . *Chosen-Ciphertext Security From Identity-Based Encryption* . 2004.

H. Tanaka . *A Realization Scheme for the Identity-based Cryptosystem* . Kobe University. Japan.

M. Baldwin . *Identity Based Encryption from the TatePairing to Secure Email Communications* . University of Bristol. 2002.

Martin Mass . *Pairing-Based Cryptography* . 2004.