Studi mengenai Blind Signature dan Blind Unanticipated Signature Makalah IF5054 Kriptografi

Dyah Saptanti Perwitasari
Teknik Informatika ITB, Bandung 40135, email: if14017@students.if.itb.ac.id

Abstract – *Tanda tangan digital (Digital Signature) digunakan untuk menandatangani pesan dengan kunci privat pengirim atau penandatangan pesan. Pada tanda tangan digital biasa, penandatangan mengetahui isi pesan terlebih dahulu sebelum memberikan tanda tangan. Berbeda dengan konsep Blind Signature dan Blind Unanticipated Signature. Pada kedua skema tanda tangan jenis ini, pesan ditandatangani si pemberi tanda tangan tanpa mengetahui isi pesan yang akan ditandatangani terlebih dahulu. Pada makalah ini akan dibahas mengenai skema Blind Signature dan Blind Unanticipated Signature.*

Kata Kunci*: Signature, Blind, Unanticipated, kunci publik, blinding, eksponen*

1. PENDAHULUAN

Digital Signature adalah tanda tangan digital yang berbasis kunci asimetri yang digunakan untuk menandatangani pesan digital. Tanda tangan digital digunakan untuk otentikasi, yaitu terhadap pengirim atau penandatangan pesan dan keaslian pesan. Proses pengiriman dan otentikasi pada tanda tangan digital adalah sebagai berikut:

a. Melakukan komputasi terhadap pesan digital sehingga mendapatkan *hash* dari pesan yang bersangkutan.
b. Dari nilai *hash* tersebut, pesan digital ditandatangani dengan menggunakan kunci privat pengirim pesan.
c. Penerima pesan menghasilkan *hash* dari pesan yang dikirim
d. Dengan menggunakan kunci publik, tanda tangan digital didekripsi sehingga menghasilkan nilai *hash* sebelum dienkripsi dengan kunci privat pengirim.
e. Jika nilai *hash* sama dengan nilai dekripsi, maka pesan asli dan pengirim asli.

Pada tanda tangan digital identitas pengirim jelas tertulis pada tanda tangan pesan. Untuk sistem tertentu, semua pihak tidak perlu mengetahui identitas pengirim dan isi pesannya, kecuali si pengirim pesan yang bersangkutan. Karena itulah dibutuhkan suatu mekanisme untuk merealisasikannya.

2. PEMBAHASAN

2.1. Blind Signature

Blind Signature adalah penandatanganan pesan yang dibuat oleh si pengirim pesan, dan ditandatangani oleh penerima pesan. Pada Blind Signature, pesan ditandatangani si penandatangan tanpa mengetahui isi pesan yang akan ditandatangani terlebih dahulu.

Mekanisme Blind Signature adalah sebagai berikut:

1. Pihak pengirim pesan membangkitkan faktor *blinding* secara acak terhadap dokumen yang bersangkutan, kemudian mengirimkan dokumen yang telah disamarkan tersebut ke pihak penerima.
2. Pihak penerima menerima pesan dan langsung menandatanganinya.

Pengirim pesan mengeluarkan faktor *blinding* dari dokumen sehingga yang tertinggal pada dokumen tersebut adalah isi pesan yang sebenarnya dan tanda tangan penerima pesan

Sebenarnya mekanisme ini dapat dimanfaatkan oleh pihak-pihak tertentu untuk kepentingan sepihak yang mungkin dapat merugikan si pemberi tanda tangan, misalnya untuk menandatangani bukti bahwa si pemberi tanda tangan berhutang kepada seseorang, dan sebagainya. Karena itu untuk mencegah dampak negatif yang ditimbulkan dari adanya Blind Signature ini adalah dengan menerapkan konsep probabilitas, yaitu dengan mengambil sampel dokumen. Jika sampel dokumen yang dipilih berisi pesan yang wajar menurut penerima pesan, maka pesan lainnya dianggap sama wajarnya. Mekanismenya adalah sebagai berikut:

1. Pengirim mengirimkan *n* pesan yang telah disisipkan faktor *blinding* di dalamnya kepada penerima, kemudian penerima memilih pesan sejumlah *n-1*.
2. Penerima meminta faktor *blinding* dari sejumlah *n-1* dokumen yang dipilihnya ke pengirim.
3. Penerima dapat membuka pesan tersebut setelah menghilangkan faktor *blinding*. Setelah memastikan bahwa isi *n-1* pesan benar menurut pandangan penerima, kemudian seluruh dokumen ditandatangani oleh penerima pesan.

Dengan adanya mekanisme baru seperti ini kemungkinan pengirim pesan untuk melakukan kecurangan kecil, yaitu *1* banding *n*, karena pengirim tidak pernah tahu pesan mana yang dipilih oleh penerima.

Dengan skema Blind Signature, seseorang dapat mendapatkan tanda tangan pada sebuah pesan dari si penandatangan yang tidak mengetahui isi pesan dan tidak dapat mengekstrak pesan. Skema Blind Signature mempunyai properti *blindness* dan *untraceability*, untuk menjamin kerahasiaan pengirim dan menghilangkan keterhubungan antara pesan dengan tanda tangan. Karena itu Blind Signature biasanya digunakan untuk memfasilitasi kerahasiaan pengguna sistem.

Berdasarkan prinsip yang dimilikinya, Blind Signature dapat digunakan di aplikasi seperti Sistem Cash Payment dan Sistem Voting Elektronik. Misalnya pada Sistem Voting setiap kotak suara harus disahkan oleh pihak yang berwenang terhadap pemilihan sebelum diperhitungkan. Di luar sistem pihak ini seharusnya mengecek apakah pemilih memang memenuhi syarat sebagai pemilih dan tidak memilih lebih dari satu kali dengan memasukkan ke kotak suara yang lain. Dalam hal ini penghitung suara tidak mengetahui bahwa subjek S dipilih pemilih mana saja, atau bahkan apakah subjek S dipilih oleh pemilih P. Informasi keterhubungan seperti ini tidak ada sehingga tidak mungkin menelusuri kotak suara tersebut (unblinded).

Bentuk pesan yang telah mengalami *blinding* pada Blind Signature adalah sebagai berikut:

$$M' = B(M,R) \quad \text{..... (1)}$$

Keterangan:
M = pesan semula
R = kunci *blinding* yang dipilih
M' = pesan setelah dikenakan fungsi Blinding

Penandatangan mengembalikan pesan S' untuk di unblind oleh pengguna, pengguna melakukan komputasi terhadap tanda tangan S pada pesan awal M dengan menggunakan fungsi Unblinding U dengan menerima S' dan R sebagai input. S' adalah tanda tangan dari si penandatangan pada pesan M'.

Sedangkan fungsi Blinding dan Unblinding pada skema Blind Signature adalah sebagai berikut:
Fungsi Blinding:

$$B(M,R) = R^E M \pmod N \quad \text{..... (2)}$$

Fungsi Unblinding:

$$U(S',R) = R^{-1} S' \pmod N \quad \text{..... (3)}$$

RSA-Signature adalah modifikasi skema RSA yang di ajukan oleh Chaum. Algoritma RSA hasil modifikasi yang untuk seterusnya disebut sebagai skema Chaum adalah sebagai berikut:

$$S^E = M \pmod N$$

Keterangan:
E = eksponen publik
N = p.q
p, q = bilangan prima yang relatif besar
M = pesan yang ditandatangani
S = tanda tangan RSA dari pesan M

Proses *blinding* pada Blinding Signature membutuhkan komputasi untuk mengantisipasi seluruh kemungkinan jenis tanda tangan. Untuk sebuah jenis kurang lebih ada sekitar lebih dari satu tanda tangan yang harus diantisipasi. Untuk itu dicetuskan skema Blind Unanticipated Signature. Skema ini membutuhkan komputasi sejumlah tertentu saja selama *blinding* untuk mengantisipasi berbagai kemungkinan tanda tangan yang diberikan pengguna yang berjumlah tak terhingga.

2.2. Blind Unanticipated Signature

Blind Unanticipated Signature adalah tanda tangan yang ditentukan setelah *blinding*. Skema Chaum bukan merupakan Blind Unanticipated Signature karena hasil *blinding* (B) dapat ditentukan langsung berdasarkan besar eksponen (E), nilai B tergantung E. Pada skema Chaum Blind Unanticipated Signature, fungsi Blinding dan Unblinding didefinisikan sebagai berikut:

Fungsi Blinding

$$B(M,R) = (M.g_1)^{k1}. \ldots g_u^{ku} \pmod N \quad \text{..... (4)}$$

Fungsi Unblinding

$$U(i,S',R) = S' x \, (S_{1)\,i}{}^{-k1} \, x \ldots x \, (S_u)_i{}^{-ku} \pmod N \quad \text{..... (5)}$$

Keterangan:
g (g_1,..,g_u) = generator
R = (k_1, ..., k_u) = kunci *blinding* acak
$S_{i,j}$ = tanda tangan pada generator g dan berkoresponden dengan eksponen E. Sebelumnya telah dipublish oleh penandatangan.
S' = tanda tangan yang dipilih penandatangan

Langkah pengiriman dan penerimaan pesan adalah sebagai berikut:

a. Untuk setiap generator g_i , tanda tangan digital S yang mempunyai koresponden dengan setiap eksponen publik dipublikasikan. Pengrim lalu mengambil kunci blinding kemudian mengirimkan pesan M' yang telah dikenai proses *blinding* dari persamaan (4).
b. Pesan M' kemudian diberikan kepada penandatangan yang kemudian memilih sebuah tandatangan, misalnya tanda tangan tertentu yang berkoresponden dengan eksponen E_i, misalnya tanda tangan S'. Kemudian tanda tangan S' beserta informasi E_i kemudian dikirim kepada

pengirim pesan. Dari tanda tangan S' tersebut, pengirim akan mendapatkan tanda tangan S dengan menggunakan persamaan (5).

Tanda tangan pada algoritma ini dikatakan *unanticipated* karena pengirim pesan tidak mengetahui jenis tanda tangan, misalnya eksponen publik, ketika mengirim pesan yang telah dilakukan *blinding* kepada penandatangan, yang mempunyai koresponden dengan tanda tangan tertentu.

Kelemahan metode ini adalah bahwa jumlah tanda tangan yang dihasilkan semakin mengurangi tingkat *unanticipatability* karena jumlah tanda tangan menjadi dibatasi. Selain itu metode ini masih mempunyai kekurangan, yaitu kemungkinan error masih ada ketika menghasilkan tanda tangan serta jumlah tanda tangan berbanding terbalik dengan laju pembuatan tanda tangan. Semakin banyak jenis tanda tangan, semakin lama waktu yang diperlukan untuk menghasilkan tanda tangan. Hal ini disebabkan karena keharusan untuk melakukan *unblinding* dengan bantuan data. Padahal data akan selalu bertambah seiring dengan jenis tanda tangan. Karenanya data membutuhkan sumber daya dan waktu tambahan untuk penyimpanan dan pemrosesan data. Selain itu metode ini tingkat *untraceability* kurang karena data yang dikirimkan oleh penandatangan diverifikasi oleh pihak ketiga terlebih dahulu sebelum kepada pengirim pesan semula.

Dengan adanya kelemahan pada metode ini, perlu dikembangkan solusi untuk menjamin *unanticipatability* dan *untraceability* tanda tangan dan pesan. Karena itu dimunculkan skema 1 dan 2 yang merupakan perbaikan dari metode sebelumnya. Untuk selanjutnya akan dibahas skema Blind Unanticipated RSA Signature, yaitu skema 1 dan 2.

1.3.1 SKEMA 1

Pada skema ini fungsi Blinding yang digunakan berbasis pangkat. Keuntungan skema 1 adalah dalam hal lebih beragamnya jenis tanda tangan jika dibandingkan dengan skema-2 maupun skema Chaum. Bahkan properti data untuk menjamin *untraceability* dapat dicek oleh pengguna individu.

Fungsi Blinding:

$$B(M,R) \equiv M^R \pmod N \quad \text{..... (6)}$$

Fungsi Unblinding:

$$U(S',R) \equiv (S')^A.M^B \pmod N \quad \text{.....(7)}$$

Keterangan:
R = kunci *blinding* acak
E = eksponen publik
A, B = integer yang dapat memenuhi AR + BE = 1
Fungsi Unblinding dapat dihitung jika GCD(R,E) = 1. GCD(R,E) adalah faktor persekutuan terbesar dari kunci blinding acak dan eksponen publik. Nilai properti ini ditentukan setelah dilakukan pemilihan kunci *blinding* R oleh pengguna. Himpunan nilai E bersifat tetap yang telah ditentukan sejak awal. Fungsi Blinding tidak memungkinkan *untraceability* terhadap tanda tangan karena ada beberapa metode yang memungkinkan pesan awal M terhubung dengan pesan M' yang telah disamarkan.

1.3.1.1 Metode 1

Misalnya, M adalah pesan awal yang merupakan pesan pangkat ke-L modulo P, L membagi P - 1. Maka M' pun merupakan pesan pangkat ke-L modulo P juga. Karena itu pihak penandatangan mendapatkan informasi mengenai keterhubungan pengguna yang mendapatkan tanda tangan ke-L

1.3.1.2 Metode 2

L adalah faktor persekutuan terbesar dari P-1 dan Q-1.
f,g : $(Z/NZ)^* \rightarrow Z/L$
f = komposisi proyeksi pada $(Z/PZ)^*$ dan simbol pangkat ke-L
g = komposisi proyeksi pada $(Z/QZ)^*$ dan simbol pangkat ke-L

Jika f (M') / g (M') = f (M) / g (M), maka penandatangan dapat mendapatkan informasi tentang keterhubungan. *Untraceability* masih belum terjamin. Untuk menjamin *untraceability* pada kedua metode ini diperlukan suatu cara untuk menghilangkan keterhubungan. Langkah yang dibutuhkan adalah dengan memperbanyak kunci *blinding* R menjadi sekian kali faktor masking G. Properti G harus memenuhi kondisi. Jika G dapat membagi R maka blinded message merupakan milik grup

$$Z(G) = \{a^G \mid a \in (Z/NZ)^*\}$$

Untuk mengecek *untraceability* digunakan tingkat *blinding* W, yaitu probabilitas bahwa variabel acak X terdapat pada $(Z/NZ)^*$ dan untuk variabel acak Y1 dan Y2, yang tidak berhubungan satu sama lain, yang kedua variabel ini terdapat pada Z(G), probabilitas bahwa Y1 didapat oleh *blinding* X berbeda dengan Y2 yang didapat oleh *blinding* X.

Jika $W \approx 1$, maka setiap pesan yang telah dikenakan *blinding* dapat berkoresponden pada pesan awal manapun. Hal ini menyebabkan *untraceability* tanda tangan hampir terjamin seluruhnya. Misalnya $W \approx 1/3$, makan untuk pesan awal yang banyak, penandatangan dapat menghubungkan pesan awal dengan salah satu dari tiga himpunan pesan yang dikenakan *blinding*. Pada setiap himpunan, semua koresponden antara pesan awal dan pesan yang dikenakan *blinding* akan mempunyai peluang yang sama.

Dengan tingkat *blinding*, probabilitas bahwa untuk data awal acak X yang dibagikan kepada semua sisa modulo N, dan semua data acak Y1 dan Y2 yang dibagikan kepada semua sisa modulo N yang

berpangkat G, maka kemungkinan untuk mendapatkan Y1 dengan melakukan *blinding* terhadap X sama dengan probabilitas mendapatkan Y2 dengan melakukan *blinding* terhadap X. Jika tingkat *blinding* tertentu, setiap pesan yang dikenakan *blinding* berkoresponden dengan setiap pesan awal yang mempunyai probabilitas yang sama. Semakin kecil nilai tingkat *blinding*, semakin mengurangi tingkat *untraceability*

Untuk menjamin *untraceability*, ambil faktor masking G yang merupakan bilangan relatif prima terhadap eksponen publik E dan memenuhi kondisi di bawah ini:

1. G dapat dibagi dengan GCD(P-1,Q-1), yaitu faktor persekutuan terbesar dari P-1 dan Q-1.
2. G dapat dibagi oleh semua D<U, D dapat membagi P-1 atau Q-1, U adalah batas yang bersesuaian.

Jika faktor masking G memenuhi kedua kondisi di atas, maka:

$$W > (1 - \log(N) / [U-\log (U+1)])^2$$

Skema 1 versi A dan B mempunyai cara pemilihan faktor masking G yang memenuhi kondisi 1 dan 2 berbeda. Misalnya sebagai berikut:

- **Versi A**
  Untuk kasus G = 2 dan P,Q memenuhi kondisi:
  (A1) 2<D<U, P - 1 tidak mempunyai pembagi D.
  (A2) 2<D<U, Q - 1 tidak mempunyai pembagi D.
  (A3) GCD(P-1, Q-1) = 2.
  Penandatangan dapat menggunakan *cut-and-choose protocol* untuk meyakinkan pengguna bahwa faktor rahasia memiliki properti di atas

- **Versi B**
  G adalah pembagi terbesar dari N-1 yang relatif prima terhadap eksponen e dan:
  (B1) N adalah perkalian P dan Q
  (B2) 2<D<U, P - 1 tidak mempunyai pembagi D
  (B3) 2<D<U, Q - 1 tidak mempunyai pembagi D

  Versi ini memenuhi kondisi 1, yaitu bahwa G dapat dibagi oleh GCD(P-1,Q-1). GCD(P-1,Q-1) membagi N-1 karena N-1 = P(Q-1) + (P-1). Karena itu fakta bahwa G sama dengan pembagi terbesar N-1 prima terhadap setiap eksponen dan kondisi B1 menyebabkan G dapat dibagi oleh GCD(P-1,Q-1), sehingga memenuhi kondsi 1. Pada versi B, properti N, P, dan Q dapat dites oleh pengguna dengan menggunakan bantuan penandatangan.

1.3.2 SKEMA 2

Fungsi Blinding berbasis perkalian. Seperti halnya Chaum, skema ini tidak selalu *untraceable*. Padahal *unantraceable* adalah properti yang harus dijamin pada skema Blind Unanticipated Signature, bahkan Blind Signature.

Pada skema ini eksponen berupa $E = E_1^{K1} ... E_k^{Kk.}$
$K_1,..,K_k$ adalah integer positif, $K_i<L_i$ untuk i=1,..,k.
Nilai L dapat dipilih oleh pengguna sebelum menerapkan fungsi Blinding atau ditentukan terlebih dahulu.
Fungsi Blinding:

$$B(M,R) = R^U.M(\text{mode } N)$$
$$U = E_1^{L1} \text{ x } ... \text{ x } E_k^{Lk}$$

Fungsi Unblinding:

$$U(S',R) = S'.R^{(-V)}(\text{mod } N)$$
$$V = E_1^{(L1 - K1)} \text{ x } ... \text{ x } E_k^{(Lk - Kk)}$$

K1,..,Kk dipilih oleh penandatangan. Derajat *unanticipatability* skema ini adalah banyaknya tanda tangan, ditentukan oleh angka k dari eksponen publik dan oleh batas multiplisit L. Misalnya untuk k = 3 dan semua batas multiplicit adalah 1000, maka banyak tanda tangan adalah 10^9

Modifikasi terhadap skema di atas tidak semudah itu dapat direalisasikan. Misalnya pada skema 1 dapat dipilih P, Q, dan G sehingga G memenuhi salah satu kriteria tidak dapat dibagi dengan GCD(P-1,Q-1) atau tidak dapat dibagi dari pembagi P-1 dan Q-1 yang bernilai lebih kecil dari batas. Misalnya plih G=1. Meski pilihan ini tidak memungkinkan dapat menutup kemungkinan tingkat *blinding* adalah 1, namun untuk situasi tertentu *untraceability* dapat dijamin.

3. KESIMPULAN

Beberapa kesimpulan yang dapat diambil terkait studi mengenai Blind Signature dan Blind Unanticipated Signature adalah sebagai berikut:

1. Skema ini hanya diperuntukkan bagi pengguna dengan jumlah dan jenis tetap. Untuk kasus pengguna yang berubah-ubah, dibutuhkan algoritma lain yang tentu lebih kompleks untuk tetap dapat mengantisipasi tanda tangan.

2. Algoritma RSA cocok untuk diterapkan pada Blind Signature meski konsep RSA sebelumnya muncul pada Digital Signature. Sedangkan algoritma Digital Signature lain seperti ElGamal yang meskipun sama-sama berbasis logaritma kurang cocok untuk diterapkan. Pada ElGamal kejelasan si penandatangan justru diperlukan, berbeda dengan konsep Blind Signature yang memungkinkan kerahasiaan keterhubungan tanda tangan dan isi pesan.

3. Dibandingkan dengan Blind Signature, Blind Unanticipated lebih fleksibel terhadap tanda tangan. Tanda tangan dapat berubah-ubah karena tanda tangan dihasilkan setelah proses *blinding.* Pada kasus transaksi keuangan misalnya, dibutuhkan penentuan tanda tangan secara

berulang-ulang, tanda tangan tidak selamanya dipakai pada transaksi yang berbeda-beda. Karena itu Blind Unanticipated Signature lebih cocok diterapkan pada kasus yang membutuhkan tanda tangan yang tidak tetap.

4. Skema Blind Signature dan Blind Unanticipated Signature memang memberikan manfaat di beberapa hal untuk menjamin kerahasiaan keterhubungan tanda tangan dan pesan. Untuk beberapa kasus yang lain, kedua skema ini dapat digunakan untuk melakukan tindak kriminal. Misalnya mengirimkan cek dengan nominal yang tidak seperti seharusnya atau mengirimkan pesan bahwa seseorang berhutang padahal pesan telah tersamarkan sehingga pihak penandatangan menandatangani tanpa mengetahui isi pesan. Karena itu tetap dibutuhkan suatu mekanisme di di dalam sistem yang menggunakan skema ini untuk mengantisipasi semua kasus khusus tak terduga yang mungkin muncul.

DAFTAR PUSTAKA

[1] Schneier, Bruce. *Applied Cryptography*, John Wiley & Sons, 1994

[2] Khamitov, I.M.; Tavrichesky, Bank; Moshonkin A.G.; Smirnov, A.L.; Steklov Mathematical, Institute. *Blind Unanticipated RSA Signature Schemes*. http://www.paycashwallet.com/merchant/AboutPayCash/blind_rsa_signature.pdf Tanggal akses : 10, 12, dan 13 Januari 2008

[3] Khamitov, I.M. *Pay Cash: A Secure Efficient Internet Payment System*. http://www.paycashwallet.com/merchant/AboutPayCash/paycash_payment_system.pdf Tanggal akses : 10, 12, dan 13 Januari 2008

[4] Cheng, chi Lee; Wei, Pang Yang; Min, Shiang Hwang. *Untraceable Blind Signature Schemes Based on Discrete Logarithm Problem*. http://portal.acm.org/citation.cfm?id=958775.958779&dl=GUIDE&dl=GUIDE Tanggal akses: 13 Januari 2008

[5] Chaum, David. *Undeniable Signature System*. http://gauss.ffii.org/PatentView/EP318097 Tanggal akses: 13 Januari 2008

[6] Zolotarev, O.A; Khamtov, I.M.; Kuznetsov, I.V.; Moshonkin, A.G.; Smirnov, A.L. *Method form The Blind Generation of A Digital RSA Signature and Device for Realising The Same* http://www.freepatentsonline.com/EP1128599.html Tanggal akses: 10, 12, dan 13 Januari 2008