Analisis dan Perbandingan Skema *Digital Signature* Spesial

Rachmat Lianda [1)]
1) Jurusan Teknik Informatika ITB, Bandung, email: if14114@students.if.itb.ac.id

Abstract **–** Sejak diperkenalkannya konsep *digital signature* oleh Diffie dan Hellman, telah banyak skema *digital signature* lain yang diajukan untuk memperkaya literatur kriptografi. Secara garis besar skema-skema tersebut dapat dibagi menjadi dua bagian yaitu skema *digital signature* konvensional dan skema *digital signature* spesial.

Pada skema *digital signature* konvensional orang yang memberi *signature* atau tanda tangan mengetahui isi dokumen yg akan ditandatangani serta siapapun yang memiliki kunci public pihak penanda tangan dapat memverifikasi kebenaran tanda tangan tanpa perlu melibat pihak penanda tangan. Kadang kala terdapat hal lain yang diinginkan pengguna seperti misalnya pihak penanda tangan ternyata tidak perlu mengetahui isi dokumen yang akan ditandatangani sehingga isi dokumen ingin disembunyikan. Di sinilah skema *digital signature* spesial berfungsi dengan cara memberikan fitur tambahan yang tidak diperoleh di skema *digital signature* konvensional.

Pada makalah ini penulis ingin melakukan analisis dan perbandingan terhadap beberapa skema digital *signature* spesial yang ada untuk kemudian memberikan penilaian dan saran mengenai skema *digital signature* spesial mana yang paling kuat dan paling baik untuk digunakan berdasarkan hasil penilaian penulis.

Kata Kunci: *digital, signature,* spesial, skema

1. PENDAHULUAN

Digital signature merupakan tanda tangan pada data digital berupa nilai kriptografis yang berfungsi untuk mengotentikasi keaslian suatu dokumen digital. Otentikasi penting karena berguna untuk memastikan keaslian dokumen sehingga diketahui apabila data masih terjaga keasliannya atau telah disalahgunakan oleh pihak yang tidak berwenang.

Pemberian *digital signature* umumnya dilakukan dengan sistem kriptografi kunci publik seperti misalnya RSA. Pada skema ini pihak penanda tangan mengetahui isi dari pesan atau dokumen yang akan ditanda tangani, kemudian siapa pun yang memiliki kunci publik dari pihak penanda tangan dapat memverifikasi keotentikan tanda tangan kapanpun yang dimau tanpa perlu memperoleh persetujuan maupun input dari pihak penanda tangan (disebut *self-authenticating*), dan keamanan didasarkan atas asumsi komplesitas secara teoretis.[1] Namun ada kalanya terdapat hal-hal lain yang ingin diterapkan terhadap dokumen atau pesan seperti misalnya pihak yang akan melakukan verifikasi perlu mendapat persetujuan terlebih dahulu dari pihak penanda tangan atau isi pesan atau dokumen tidak perlu diketahui oleh pihak penanda tangan serta alasan lainnya. Hal tersebut tidak ditangani oleh skema *digital signature* konvensional seperti RSA sehingga diciptakan skema-skema *digital signature* baru yang mampu menangani hal-hal di luar kondisi umum yang ditangani skema *digital signature* konvensional, yang secara umum disebut sebagai skema *digital signature* spesial.

Setiap skema memiliki cara dan metode yang berbeda dari satu dengan lainnya dan memiliki kelebihan serta kekurangan masing-masing sehingga tidak ada skema yang benar-benar dapat dikatakan sempurna. Namun demikian keunggulan yang dimiliki tiap-tiap skema dapat dimanfaatkan untuk menentukan skema digital signature mana yang akan diterapkan untuk pemberian tanda tangan bagi suatu dokumen sesuai dengan keperluan.

2. HASIL DAN PEMBAHASAN

Skema *digital signature* spesial yang akan dibandingkan antara lain *blind signature scheme*, *designated confirmer scheme*, *fail-stop signature scheme*, *group signature scheme*, *one-time signature scheme*, *Merkle tree signature scheme*, dan *undeniable signature scheme*.[2]

Blind Signature Scheme

Blind signature scheme pertama kali diperkenalkan oleh Chaum. Penggunaan *blind signature scheme* memungkinkan seseorang untuk meminta orang atau pihak lain untuk menandatangani dokumen tanpa memberikan informasi apapun mengenai isi pesan dalam dokumen tersebut kepada orang atau pihak yang akan melakukan penandatanganan.

Implementasi dari konsep ini dapat dimisalkan sebagai berikut:
Misalkan Alice memiliki sebuah pesan *m* dan ia ingin pesan tersebut ditandatangani oleh Bob namun ia tidak ingin Bob mengetahui apapun mengenai pesan *m* tersebut. Bob memiliki kunci publik *(n,e)* dan kunci privat *(n,d)*. Alice akan menciptakan sebuah nilai acak *r* yang memenuhi persamaan $gcd(r, n) = 1$ dan kemudian mengirimkan $x = (r^e m) \bmod n$ kepada Bob.

Nilai dari x akan ditutupi oleh nilai acak dari r sehingga Bob tidak dapat memperoleh informasi dari situ. Bob kemudian akan mengembalikan nilai penandatanganan $t = x^d \bmod n$ kepada Alice. Karena $x^d \equiv (r^e m)^d \equiv r m^d \bmod n$ maka Alice dapat memperoleh tanda tangan sebenarnya dari pesan m dengan menghitung $s = r^{-1} t \bmod n$.

Sekarang pesan Alice telah memiliki tanda tangan yang tidak dapat diperoleh dengan sendirinya. Skema *digital signature* ini aman dengan anggapan pemfaktoran dan pengakaran nilai sulit untuk dilakukan. Namun demikian, dengan mengabaikan permasalahan tersebut, skema ini masih tetap dapat dikatakan 'buta' karena nilai r yang acak. Nilai r yang acak tersebut tidak memungkinkan pihak penandatangan untuk mengetahui isi pesan meskipun pihak penandatangan dapat memecahkan persoalan sulit sebelumnya yang berkaitan dengan pemfaktoran dan pengakaran angka.

Berdasarkan penilaian penulis, kelebihan skema ini yaitu pemilik dokumen lebih memiliki kontrol atas dokumen dan isi pesan karena isi pesan dapat disembunyikan namun hal tersebut dapat menimbulkan ketidakpercayaan dari pihak penandatangan karena yang dapat mengakibatkan pihak penandatangan keberatan untuk memberikan tanda tangannya.

Designated Confirmer Scheme

Designated confirmer scheme hampir mirip dengan skema *digital signature* konvensional yang bersifat *self-authenticating* atau otentikasi langsung. Yang membedakannya adalah pada *designated confirmer scheme* ditambahkan aspek *zero-knowledge proof,* yaitu pihak yang melakukan verifikasi tidak mengetahui apapun mengenai fakta yang sedang dibuktikan (kecuali bahwa fakta itu benar) dari pihak pembukti yang tidak dapat diperoleh sebelumnya tanpa pihak pembukti, sehingga skema ini tidak sepenuhnya bersifat *self-authenticating*.

Kondisi pertama (*self-authenticating*) memungkinkan siapapun untuk memverifikasi tanda tangan namun kondisi kedua (*zero-knowledge proof*) hanya memungkinkan satu penerima pada suatu waktu untuk mengotentikasi dokumen bersangkutan dan hanya melalui interaksi dengan pihak penanda tangan.

Designated confirmer signature memungkinkan pihak tertentu yang telah ditetapkan untuk mengonfirmasi keotentikan dokumen tanpa memerlukan input atau masukan dari pihak penanda tangan namun pada saat bersamaan tanpa bantuan dari baik pihak penanda tangan maupun pihak tertentu yang telah ditetapkan, tidak mungkin memverifikasi keotentikan dari dokumen bersangkutan.

Berdasarkan penilaian penulis kelebihan dari skema ini yaitu pihak-pihak yang akan melakukan verifikasi dokumen dapat ditentukan oleh pihak penanda tangan karena keterlibatan pihak penanda tangan dalam otentikasi dokumen, dengan demikian akses terhadap dokumen dapat lebih dibatasi sesuai kehendak pemilik dokumen. Yang menjadi kekurangan dari skema ini adalah tidak adanya penangan terhadap masalah jika misalnya terjadi penyangkalan oleh pihak penanda tangan.

Fail-stop Signature Scheme

Fail-stop signature scheme dirancang oleh van Heyst dan Pederson untuk melindungi dokumen dari kemungkinan bahwa pihak lawan dapat memalsukan tanda tangan seseorang. Skema ini merupakan variasi dari *one-time signature* yang akan dijelaskan kemudian, yaitu hanya satu pesan yang dapat ditanda tangan dan dilindungi oleh kunci yang diberikan pada satu waktu. Yang melandasi skema *fail-stop signature* ini adalah logaritma diskrit. Jika pihak lawan ternyata dapat memalsukan tanda tangan maka pihak penanda tangan yang asli dapat membuktikan bahwa permalsuan terjadi dengan memberikan pemecahan dari permasalahan sulit yang dimiliki dengan demikian kemampuan pemalsu untuk memecahkan masalah tersebut berpindah ke pihak penanda tangan asli.

Kata '*fail-stop*' berarti pihak penanda tangan dapat mendeteksi dan menghentikan kegagalan yang dalam konteks ini adalah pemalsuan. Yang perlu diperhatikan adalah apabila pihak lawan memperoleh duplikat dari kunci privat milik pihak penanda tangan maka pemalsuan tidak dapat dibuktikan. Apa yang skema ini deteksi adalah pemalsuan berdasarkan kriptanalisis.

Berdasarkan penilaian penulis, kekuatan skema ini terletak pada kemampuannya mendeteksi salah satu bentuk penyalahgunaan yaitu pemalsuan. Namun hal ini berarti bahwa pemalsuan masih dapat dilakukan karena penanganan yang dilakukan oleh skema ini tidak bersifat mencegah. Akan lebih baik jika skema ini digunakan bersama skema lain untuk memperkuat keamanan dan kerahasiaan dokumen.

Group Signature Scheme

Group signature scheme diperkenalkan oleh Chaum dan van Heist. Skema *digital signature* ini memungkinkan salah satu anggota dari suatu grup untuk memberi tanda tangan digital pada suatu dokumen yang dapat dibuktikan oleh pihak yang melakukan verifikasi bahwa tanda tangan berasal dari grup tersebut namun tanpa mengetahui anggota yang mana yang menandatanganinya.

Protokol memungkinkan identitas dari penanda tangan untuk diketahui, jika misalkan terjadi pembantahan, oleh otoritas grup yang telah ditetapkan yang memiliki sejumlah informasi tambahan untuk mendukung pembuktian.

Yang menjadi kekuatan dari skema ini adalah pihak penanda tangan leibh memiliki keleluasaan dalam pemberian tanda tangan karena tidak harus orang yang telah ditetapkan yang harus memberi tanda tangan. Asalkan masih anggota kelompok yang berwenang memberi tanda tangan maka tanda tangan dapat dikatakan asli. Hal ini dapat menanggulangi masalah apabila wakil yang diharuskan memberi tanda tangan berhalangan. Sementara itu yang menjadi kelemahan dari skema ini adalah karena setiap kali salah satu anggota grup memberi tanda tangan, pasangan kunci yang baru harus diciptakan untuk si penanda tangan. Penciptaan pasangan kunci baru ini mengakibatkan panjang dari baik kunci rahasia dari anggota grup maupun informasi tambahan bagi otoritas grup yang telah ditetapkan yang akan digunakan untuk melakukan pembuktian jika terjadi pembantahan bertambah, Hal ini cenderung mengakibatkan skema ini menjadi susah dipakai jika digunakan oleh grup untuk menandatangani sejumlah pesan atau saat digunakan untuk periode waktu yang lama.

One-time Signature Scheme

One-time signature scheme memungkinkan penandatanganan sebuah pesan dengan menggunakan potongan informasi privat atau public yang diberikan. Keunggulan dari skema ini adalah secara umum bersifat cepat. Namun skema cenderung menjadi sulit dipakai jika digunakan untuk mengotentikasi banyak pesan karena data tambahan perlu diciptakan untuk menanda tangan dan untuk memverifikasi setiap pesan baru. Kebalikannya, skema *digital signature* konvensional seperti RSA membolehkan penggunaan pasangan kunci yang sama untuk mengontentikasi banyak dokumen. Terdapat implementasi *one-time signature* yang cukup efisien yang dilakukan oleh Merkle yang diberi nama *Merkle Tree Signature Scheme*, yang tidak mengharuskan pasangan kunci baru untuk setiap pesan melalui skema yang menyerupai pohon.

Merkle Tree Signature Scheme

Merkle Tree Signature Scheme secara umum menyerupai *one-time signature scheme*. Yang membedakannya adalah skema ini tidak mengharuskan pasangan kunci baru untuk setiap pesan. Hal itu dicapai melalui penggunaan skema yang menyerupai pohon.

Setiap pesan yang akan ditandatangani berkoresponden dengan simpul pada pohon, dengan isi pada simpul mencakup parameter verifikasi yang digunakan untuk menandatangani pesan dan untuk mengotentikasi parameter verifikasi simpul berikutnya. Walaupun jumlah pesan yang dapat ditandatangani dibatasi oleh besarnya pohon, pohon dapat dibuat berukuran besar untuk dapat menangani jumlah pesan yang banyak sehingga hal ini tidak terlalu menjadi masalah. Skema *digital signature* ini cukup efisien karena hanya membutuhkan aplikasi fungsi hash.

Undeniable Signature Scheme

Undeniable signature scheme yang dirancang oleh Chaum dan van Antwerpen merupakan skema *digital signature* yang bersifat *non-self-authenticating* di mana tanda tangan hanya dapat diverifikasi dengan persetujuan pihak penanda tangan. Namun jika tanda tangan hanya dapat diverifikasi dengan bantuan pihak penanda tangan, mungkin saja pihak penanda tangan tidak jujur dan menolak untuk mengotentikasi dokumen asli. Skema ini mengatasi masalah tersebut dengan menambahkan komponen yang bernama *disavowal protocol* atau protokol penyangkalan untuk melengkapi komponen normal seperti tanda tangan dan verifikasi.

Skema ini diimplementasi dengan menggunakan kriptografi kunci publik yang didasarkan atas logaritma diskrit. Bagian tanda tangan dari skema umumnya serupa dengan skema lain yang juga menggunakan logaritma diskrit. Verifikasi dijalankan dengan *challenge-response protocol* atau protokol respon-tantangan di mana pihak yang akan melakukan verifikasi mengirimkan ‘tantangan’ kepada pihak penanda tangan dan memperlihatkan jawabannya untuk memverifikasi tanda tangan. Proses penyangkalan dapat dikatakan serupa, pihak yang akan melakukan verifikasi mengirimkan ‘tantangan’ dan respon dari pihak penanda tangan akan menunjukkan apakah tanda tangan tersebut merupakan asli kepunyaan penanda tangan. Kemungkinan

seorang penanda tangan yang tidak jujur berhasil mengelabui pihak yang akan melakukan baik verifikasi maupun penyangkalan adalah *1/p* di mana *p* merupakan bilangan prima pada kunci privat milik pihak penanda tangan.

Berdasarkan penilaian penulis kekuatan skema ini terletak pada penjagaan keamanan dengan hanya mengizinkan verifikasi dilakukan atas persetujuan pihak penanda tangan. Selain itu dengan adanya penanganan terhadap masalah penyangkalan oleh pihak penanda tangan semakin menambah kekuatan skema ini.

3. KESIMPULAN

Dari beberapa skema *digital signature* spesial yang telah penulis berikan di atas, penulis berkesimpulan bahwa *undeniable signature scheme* lebih kuat dari skema *digital signature* konvensional dan lebih unggul dibanding skema digital signature lainnya. Kesimpulan ini penulis ambil setelah melakukan penilaian dan perbandingan antar skema *digital signature*.

One-time signature dan skema pengembangannya, *Merkle tree signature*, memiliki keunggulan yaitu cepat jika dibandingkan dengan skema lainnya namun keamanannya tidak sebaik skema lain karena tidak memberikan metode penanganan masalah atau penyangkalan. *Fail-stop signature* memiliki keunggulan dalam pendeteksian serta pembuktian masalah berupa pemalsuan namun karena penanganannya berupa pembuktian, masalah masih tetap dapat terjadi.

Beberapa skema *digital signature* spesial seperti *designated confirmer signature* dan *group signature* telah berusaha meningkatkan aspek keamanan seperti yang dilakukan *undeniable digital signature*, yaitu melibatkan pihak penanda tangan dalam proses verifikasi. Namun terdapat kelemahan pada *designated confirmer signature* dan pada *group signature*. Pada *designated confirmer signature* tidak ada penanganan terhadap masalah jika misalnya pihak penanda tangan melakukan penyangkalan, yang akan berujung pada kesulitan pelaksanaan proses verifikasi sedangkan pada *group signature* masalah yang dihadapi adalah telah ada metode penyangkalan namun karena diberlakukannya penggunaan kunci baru untuk setiap pesan yang ditanda tangani, proses penyangkalan menjadi sulit dilakukan karena panjangnya informasi yang dibutuhkan dan akan terus bertambah seiring dilakukannya penandatanganan dokumen baru. Pada *undeniable signature* masalah tersebut tidak ditemui dalam proses penyangkalan sehingga skema tersebut menjadi lebih unggul dibandingkan dengan dua skema lainnya yang telah disebutkan tersebut.

Terdapat skema yang memiliki fitur yang tidak dimiliki oleh skema *undeniable signature*, seperti misalnya fitur penyembunyian isi pesan atau dokumen yang dimiliki oleh skema *blind signature* namun penulis beranggapan hal tersebut tidak menjadikan keunggulan skema *undeniable signature* berkurang. Pada umumnya sebagai pihak yang akan memberikan tanda tangan, penanda tangan perlu atau memiliki hak untuk melihat isi pesan atau dokumen agar tindakannya dapat dipertanggungjawabkan. Mungkin saja terdapat kasus-kasus khusus di mana hal tersebut menjadi sesuatu yang dihindari namun itu tidak menjadi keharusan bahwa skema *digital signature* wajib memiliki fitur tersebut sehingga berdasarkan penilaian penulis, skema *undeniable signature* masih tetap lebih unggul.

Saran yang penulis berikan untuk lebih memperkuat keamanan pesan atau dokumen yang penggabungan atau penggunaan bersamaan skema *fail-stop signature* dan *undeniable signature*. Skema *fail-stop signature* akan menangani upaya pemalsuan tanda tangan dan skema *undeniable signature* akan menjaga agar dokumen tidak digunakan oleh pihak yang tidak berwenang dan tidak disalahgunakan.

DAFTAR REFERENSI

[1] Munir, Rinaldi, “Tandatangan Digital”, *slide kuliah IF5054 Kriptografi*

[2] RSA Laboratories, http://www.rsa.com, diakses tanggal 12 Desember 2007, 3 Januari 2008, dan 13 Januari 2008