Teori dan Aplikasi *Group Blind Digital Signature*

Maria Helena Iwo-13503088

Program Studi Teknik Informatika
Sekolah Elektro dan Informatika
Institut Teknologi Bandung
40132
Email: if13088@students.if.itb.ac.id

Abstrak

Group blind digital signature merupakan variasi dari tanda tangan dijital yang terdiri dari *group digital signature* dan *blind digital signature*. *Group digital signature* merupakan protokol yang memungkinkan seorang anggota dari suatu kelompok melakukan tanda tangan dijital pada sebuah pesan atas nama seluruh anggota kelompok. Sedangkan *blind digital signature* memungkinkan seseorang menandatangani suatu pesan tanpa mengetahui isi dari pesan tersebut. Jadi, *group blind digital signature* merupakan *group digital signature* dengan menggunakan properti *blind signature*. Konsep *group blind signature* dapat diterapkan untuk menjamin kemanan pada *distributed electronic banking* dan pemilihan umum secara *online.* Pada makalah ini akan membahas berbagai skema *blind signature* dan aplikasinya, protokol *group digital signature*, serta protokol penerapan g*roup blind digital signature* pada *digital cash payment* dan pemilihan umum secara *online*.

Kata kunci: tanda tangan dijital, *group digital signature*, *blind digital signature*, *distributed electronic banking,* pemilihan umum *online*.

---

1. Pendahuluan

Hal yang fundamental di dunia kriptografi adalah mengamankan jalur antara dua belah pihak yang menggunakan jalur komunikasi yang tidak aman. Untuk itu dikembangkan berbagai macam metode kriptografi. Salah satunya adalah tanda tangan dijital. Perkembangan tanda tangan dijital didorong oleh adanya sistem kriptografi kunci publik.

Kriptografi kunci publik mengatasi masalah kesulitan pertukaran kunci privat pada jalur komunikasi yang tidak aman. Ide dari kriptografi kunci publik yang diperkenalkan oleh Diffie dan Hellman adalah menggunakan dua macam kunci untuk melakukan enkripsi/dekripsi [5]. Dua macam kunci tersebut adalah kunci publik dan kunci privat. Kunci publik digunakan untuk melakukan enkripsi sedangkan kunci privat untuk melakukan dekripsi. Kedua macam kunci tersebut harus didesain sedemikian rupa sehingga tidak mungkin mendapatkan kunci privat dari kunci publik. Walaupun kriptografi kunci publik tidak dapat dipecahkan, namun kriptografi kunci publik juga tidak dapat dibuktikan keamanannya secara matematis.

Konsep kriptografi kunci publik mendorong berkembangnya konsep tanda tangan dijital. Tanda tangan dijital adalah analogi elektronis dari tanda tangan tradisional. Tujuan tanda tangan dijital adalah untuk memungkinkan seseorang menandatangani dokumen elektronis secara dijital. Beberapa sifat tanda tangan dijital yang diturunkan dari tanda tangan tradisional adalah mudah dibuat, mudah dicek, dan sulit untuk dipalsukan. Tanda tangan dijital ini menggunakan kunci privat untuk menandatangani dan menggunakan kunci publik untuk memverifikasi. Dengan konsep seperti ini, maka sifat-sifat tersebut dapat terpenuhi.

Salah satu variasi dari tanda tangan dijital adalah *blind digital signature* yang diperkenalkan pertama kali oleh Chaum [4]. *Blind digital signature* memungkinkan si penanda tangan menandatangani suatu dokumen tanpa mengetahui isi dokumen tersebut. Konsep *blind digital signature* ini banyak digunakan pada sistem *digital cash payment* dan pemilihan umum secara *online*.

Variasi lainnya dari tanda tangan dijital adalah *group digital signature*. *Group digital signature* memungkinkan seorang anggota kelompok menandatangani suatu dokumen atas nama seluruh anggota kelompok. Konsep *group digital signature* dapat dipadukan dengan konsep *blind digital signature* menjadi *group blind digital signature*. *Group blind digital signature merupakan group digital signature* yang telah memiliki properti *blindness*. Dengan memanfaatkan konsep *group digital signature*, dapat dilakukan sejumlah modifikasi terhadap aplikasi *blind signature* pada *digital cash payment* dan pemilihan umum secara *online*.

Untuk memudahkan pemahaman akan makalah ini, maka akan dijelaskan terlebih dahulu mengenai beberapa terminologi sebagai berikut:

1. *Electronic cash*
   Merupakan semacam uang dijital yang didapatkan dari bank.
2. Koin
   Merupakan representasi dari *electronic cash*.
3. *Withdrawal*
   Merupakan proses pengambilan koin oleh pelanggan dari bank.
4. *Payment*
   Merupakan proses pembayaran yang dilakukan oleh pelanggan kepada vendor.
5. *Deposit*
   Merupakan penyimpanan koin ke bank yang dilakukan oleh vendor

Makalah ini akan membahas teori dan aplikasi *blind signature* dan *group digital signature*. Kemudian, pada makalah ini diusulkan suatu protokol *group blind digital signature* pada *digital cash payment* dan pemilihan umum secara *online*.

2. Tanda Tangan Dijital

Tanda tangan dijital merupakan tanda tangan untuk data dijital. Tanda tangan dijital bukanlah tulisan tanda tangan yang di-digitisasi (di-*scan*), melainkan suatu nilai kriptografis yang bergantung pada isi pesan dan kunci [10]. Akibatnya, tanda tangan dijital selalu berbeda-beda antara satu isi dokumen dengan dokumen lain. Dengan demikian, maka selain digunakan untuk menjamin integritas data, tanda tangan dijital juga dapat digunakan untuk membuktikan asal pesan (keabsahan pengirim), dan nirpenyangkalan.

Menandatangani pesan dapat dilakukan dengan dua cara, yaitu dengan mengenkripsi pesan atau dengan cara menggunakan fungsi *hash* dan kriptografi kunci publik.

3. *Blind Digital Signature*

Konsep *blind digital signature* diperkenalkan oleh Chaum [4]. *Blind digital signature* ini memungkinkan properti anonimitas seseorang pada sistem *Electronic Cash*. Tanda tangan dijital jenis ini memungkinkan penanda tangan menandatangani sebuah dokumen tanpa mengetahui isi dokumen tersebut. Selanjutnya, jika penanda tangan secara tidak disengaja melihat pasangan dokumen dan tanda tangan, maka ia tidak dapat menentukan kapan dan untuk siapa ia menandatangani dokumen tersebut (meskipun ia dapat memverifikasi bahwa tanda tangan tersebut valid). Hal ini dapat dianalogikan dengan menandatangani suatu dokumen dengan mata tertutup (*blind*). Jika setelahnya, si penandatangan melihat dokumen dan tandatangannya, maka ia akan sangat sulit untuk mengingat kapan atau untuk siapa ia menandatangani dokumen tersebut. Konsep ini terlihat sangat aneh; mengapa seseorang mau menandatangani suatu dokumen tanpa melihatnya terlebih dahulu? Karena itu, penerapan konsep ini hanya ditujukan bagi kepentingan tertentu, misalnya pemilihan umum *online* dan *electronic cash*. Pada pemilihan umum, ketika kertas suara dikumpulkan, kertas suara tersebut harus disahkan oleh petugas yang bersangkutan, tanpa petugas tersebut mengetahui isi dari kertas suara (siapa kandidat yang dipilih). Demikian juga halnya dengan *electronic cash*, pemilik *electronic cash* tidak ingin seseorang mengetahui identitasnya ataupun kapan *electronic cash* tersebut digunakan. Hal ini sama dengan paper cash tradisional, yaitu ketika seseorang melakukan pembelian, si penjual tidak mengetahui identitas si pembeli tetapi si penjual dapat menentukan apakah uang si pembeli legal atau tidak. Pada skenario tersebut, koin elektronis dianalogikan dengan dokumen, dan penandatangan direpresentasikan oleh bank. Pembeli selalu anonim pada setiap transaksi yang melibatkan koin elektronis jika koin-koin tersebut ditandatangani secara *blind*.

Blind digital signature dapat dikembangkan dari berbagai algoritma kunci publik, misalnya RSA dan ElGamal. Pada makalah ini hanya membahas *blind digital signature* yang diturunkan dari algoritma RSA. Penurunan *blind digital*

signature dari algoritma ElGamal dapat dilihat pada [9]. Menurut [9], *blind digital signature* yang diturunkan dari algoritma ElGamal memiliki tingkat anonimitas yang lebih tinggi daripada *blind digital signature* yang diturunkan dari algoritma RSA.

a. Skema Tanda Tangan Dijital dengan Algoritma RSA

Algoritma RSA dibuat oleh tiga orang peneliti dari MIT (*Massachussets Institute of Technology*), yaitu Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Kemanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima [10]. Pemfaktoran ini dilakukan untuk memperoleh kunci privat. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin.

Pada algoritma RSA, terdapat besaran-besaran sebagai berikut:

1. p dan q bilangan prima (rahasia)
2. $n=p.q$ (tidak rahasia)
3. $\Phi(n) = (p-1)(q-1)$ (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
5. d (kunci dekripsi) (rahasia)
6. m (plainteks) (rahasia)
7. c (cipherteks) (tidak rahasia)

Keterangan:

- p dan q adalah bilangan prima yang besar.
- e merupakan angka dimana (e, $\Phi(n)$)=1.
- d merupakan angka dimana de = 1 mod $\Phi(n)$.
- Kunci publik penanda tangan adalah (n,e)
- Kunci privat adalah (p,q,d).

Langkah-langkah pemberian tanda tangan dijital dengan algoritma RSA adalah sebagai berikut [10]:

1. Pengirim menghitung nilai *hash* dari pesan *M* yang akan dikirim, misalkan nilai *hash* dari pesan *M* adalah *h*.
2. Pengirim mengenkripsi h dengan kunci privatnya menggunakan persamaan enkripsi RSA, yaitu:
$$S = h^{SK} \bmod n$$
yang dalam hal ini *SK* adalah kunci privat pengirim dan *n* adalah modulus ($n=pq$, p dan q adalah dua buah bilangan prima).
3. Pengirim mentransmisi M + S ke penerima.

Langkah-langkah pemverifikasian tanda tangan dijital dengan algoritma RSA adalah sebagai berikut [10]:

1. Penerima menghitung nilai *hash* dari pesan *M* yang dikirim, misalkan nilai *hash* dari *M* adalah *h'*.
2. Penerima melakukan dekripsi terhadap tanda tangan *S* dengan kunci publik si pengirim menggunakan persamaan dekripsi RSA, yaitu:
$$h = S^{PK} \bmod n$$
yang dalam hal ini PK adalah kunci publik pengirim dan *n* adalah modulus ($n=pq$, p dan q adalah dua buah bilangan prima).
3. Penerima membandingkan *h* dengan *h'*. Jika *h=h'* maka tanda tangan dijital adalah otentik. Jika tidak sama, maka tanda tangan dijital tidak otentik sehingga pesan dianggap tidak asli lagi atau pengirimnya bukanlah orang yang sebenarnya.

Skema pemberian tanda tangan dijital dan pemverifikasiannya dapat dilihat pada Gambar 1. Secara umum, otentikasi tanda tangan dijital dengan menggunakan fungsi *hash* dapat dilihat pada Gambar 2.

b. Skema *Blind Digital Signature* dengan Modifikasi Algoritma RSA

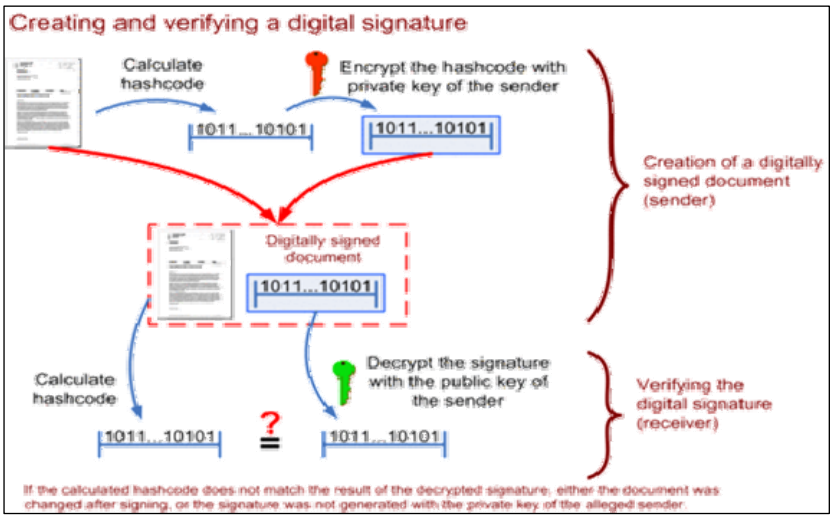
Pada konteks ini, misalkan Bob membutuhkan tanda tangan Alice untuk beberapa dokumen. Akan tetapi, Bob tidak ingin Alice mengetahui isi dokumen-dokumen tersebut. Untuk menyelesaikan masalah tersebut, diperlukan protokol-protokol sebagai berikut [12]:

b.1 Putaran 1 → Bob

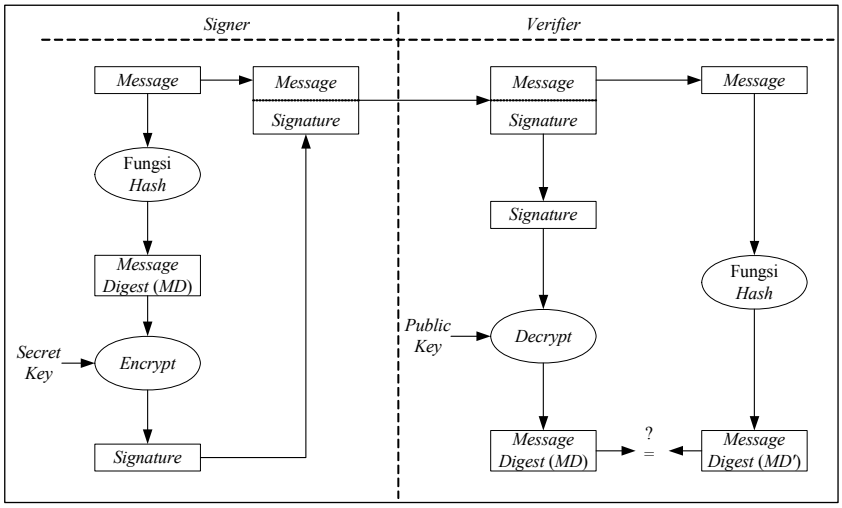
1. Bob ingin sebuah pesan *M* untuk ditandatangani secara "buta" oleh Alice. Bob memberitahukan Alice akan permasalahan tersebut.
2. Bob mengambil suatu angka $r \epsilon_R Z_n^*$ dan menghitung pesan "buta" *M'*:
$$M' = H(M).\ r^e \pmod n$$
dimana n dan e merupakan kunci publik Alice dan Z_n^* merupakan kelompok multiplikatif modulo n. $r \epsilon_R Z_n^*$ berarti mengambil suatu bilangan r secara acak dari suatu kelompok multiplikatif modulo n.

Sedangkan $H(M)$ merupakan fungsi *hash* yang dikenakan terhadap pesan M.

3. Bob mengirim M' kepada Alice.



Gambar 1. Visualisasi pemberian tanda tangan dijital dan verifikasinya



Gambar 2. Otentikasi tanda tangan dijital yang menggunakan fungsi *hash* satu-arah

b.2 Putaran 2 → Alice

1. Alice mengambil M' dan menghitung tanda tangan dijital terhadap pesan M' tersebut:
   $$\sigma(M')=M'^{d} \pmod n$$
   Perhatikan bahwa:
   $M'^{d} \pmod n=(H(M)r^{e})^{d} \pmod n = H(M)^{d}.r \pmod n$
2. Alice mengirimkan $\sigma(M')$ kepada Bob.

b.3 Putaran 3 → Bob

1. Bob mengambil $\sigma(M')$ yang diberikan Alice. Bob kemudian mengekstrak tanda tangan yang tepat untuk pesan M dengan persamaan:
   $$\sigma(M) = \sigma(M')/r \pmod n$$
2. Pasangan (M, $\sigma(M)$) merepresentasikan pesan dan tanda tangan dijital dengan kunci publik Alice. Hal ini dapat dibuktikan dengan:
   $$\sigma(M') = H(M)^{d}.r \pmod n$$

Pada protokol di atas, dapat dilihat bahwa Alice memberikan tandatangannya tanpa melihat pesan

yang sebenarnya. Hal ini terjadi karena faktor "buta" (*blinding factor*) r^e dimultiplikasi oleh pesan, dan sebagai hasilnya, pesan akhir terlihat seperti elemen acak dari Z_n^* untuk Alice. Kemudian, setelah tanda tangan dikeluarkan oleh Alice, Bob membagi tanda tangan dengan *r* (untuk menghilangkan *blinding factor*). Pasangan pesan dan tanda tangan selanjutnya tidak dapat dikenali oleh Alice. Jika Alice kemudian melihat pesan tersebut, ia dapat dengan mudah memverifikasi bahwa tandatangan tersebut adalah miliknya, namun ia akan sulit memastikan kapan dan untuk siapa ia menandatangani pesan tersebut.

c. Aplikasi *Blind Digital Signature* pada *Digital Cash Payment*

Untuk menjelaskan aplikasi *blind digital signature*, perhatikan skenario di bawah ini. Alice ingin membeli buku Akuntansi seharga Rp 100.000,00 dari suatu toko buku *online*. Alice dan toko buku tersebut menggunakan bank yang sama, yang dinamakan Bank B. Protokol transaksi yang mendukung *blind digital signature* pada skenario di atas dibagi menjadi tiga tahapan, yaitu: penarikan uang si pembeli (*withdrawal*), pembayaran dari pembeli ke penjual (*spending*), dan penyimpanan uang si penjual (*deposit*).

c.1 *Withdrawal*

1. Alice menciptakan selembar mata uang dijital C. Mata uang ini terdiri dari string bit yang menyatakan informasi nomor seri dan jumlah uang, dalam hal ini Rp 100.000,00.
2. Alice mengantar C ke bank B agar dapat ditandatangani secara "buta". Dengan kata lain, Alice dan bank B melakukan protokol *blind signature*.
3. Ketika protokol tersebut telah berhasil dijalankan, bank B mengurangi saldo tabungan Alice sebanyak Rp 100.000,00

c.2 *Spending*

1. Alice meminta sebuah salinan dari buku Akuntansi yang diinginkannya dari toko buku *online*. Alice menyertakan C (yang telah diberi tanda tangan dijital oleh Bank B) kepada toko buku *online*.
2. Toko buku *online* memeriksa validitas C dengan memverifikasi tanda tangan dijital pada C dengan menggunakan kunci publik Bank B. Jika tanda tangan tersebut valid, toko buku *online* dapat mengakhiri protokol.

c.3 *Deposit*

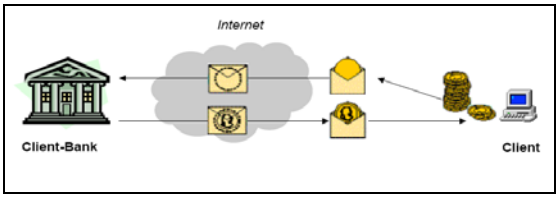
1. Toko buku online mengambil C beserta tanda tangan dari B, kemudian menyerahkannya ke Bank B.
2. Bank B kemudian memverifikasi bahwa tanda tangan dijital pada C valid; memang ditandatangani oleh Bank B. Jika tanda tangan tersebut valid, bank B kemudian harus memeriksa apakah C belum pernah digunakan sebelumnya. Jika C valid dan belum pernah digunakan, maka bank B akan menambahkan saldo toko buku *Online* sejumlah Rp 100.000,00.
3. Jika semua langkah-langkah di atas telah berhasil dilakukan, barulah toko buku *online* memberikan buku yang diminta oleh Alice.

Pada protokol di atas, identitas Alice terjaga anonimitasnya, baik untuk bank maupun untuk toko buku. Hal ini terjadi karena *blind signature* dikeluarkan untuk mata uang tersebut. Karena itu, ketika Alice telah menandatangani mata uang tersebut, toko buku tidak dapat mendeteksi apakah Alice adalah pemilik dari mata uang itu. Selanjutnya, ketika toko buku memberikan uang kepada bank untuk disimpan, bank tidak dapat mendeteksi apakah uang tersebut berasal dari Alice atau tidak serta tidak dapat mendeteksi isinya.

Pada protokol di atas, identitas Alice terjaga anonimitasnya, baik untuk bank maupun untuk toko buku. Keuntungan dari cara ini adalah tidak memerlukan sistem pembayaran dengan menggunakan kartu kredit yang segi keamanannya belum sepenuhnya terjamin. Sistem seperti ini bisa diandaikan dengan memiliki *voucher* dijital.

Pada protokol di atas, terdapat beberapa kelemahan dari segi keamanan pada sistem tersebut. Sebagai contoh, Alice bisa saja memberikan pesan kepada bank sebagai berikut: "Apakah saya telah menandatangani 10 juta dolar untuk Alice?". Kemudian, karena uang elektronik mudah disalin, Alice bisa saja menggunakan uang elektronik yang sama di kemudian hari. Aspek keamanan yang paling berbahaya adalah ketika suatu transaksi selesai dilakukan, tidak ada cara untuk mengecek identitas pemilik uang elektronik.

Secara singkat, aplikasi *blind digital signature* pada *digital cash payment* dapat dilihat pada Gambar 3.



Gambar 3. Aplikasi *blind digital signature* pada *digital cash payment*

d. Aplikasi *Blind Digital Signature* untuk Pemilihan Umum *Online*

Penerapan *blind digital signature* pada pemilihan umum *online* melibatkan dua entitas, yaitu seorang pemilih Alice, dan suatu pusat tabulasi Central Tabulating Facility (CTF). Kita asumsikan bahwa *form* pemungutan berupa "ya" atau "tidak". Protokol pemungutan suara tersebut dibagi menjadi dua tahap, yaitu registrasi dan pemungutan suara.

d.1 Registrasi

1. Alice membuat dua kertas suara elektronik *B1* dan *B2*. Kertas suara tersebut memiliki nomor seri dan beberapa informasi relevan dengan pemungutan suara. *B1* merepresentasikan suara "ya" sedangkan *B2* merepresentasikan suara "tidak".
2. Alice kemudian mengambil kertas suara B1 dan B2 kemudian mem"buta"kannya. Alice kemudian mengirimkan versi "buta" tersebut ke CTF.
3. CTF mengecek basis datanya untuk memastikan bahwa Alice belum pernah melakukan pemilihan sebelumnya. Jika Alice belum melakukan pemungutan, CTF akan menandatangani kertas suara buta tersebut kemudian mengembalikannya kepada Alice.

d.2 Pemungutan Suara

1. Alice mengekstrak kertas suara tersebut dan memiliki dua kertas suara valid yang telah ditandatangani oleh CTF.
2. Alice memilih kertas suara (yang telah diberi tanda tangan oleh CTF) mana yang ingin dipilihnya ("ya" atau "tidak"). Alice kemudian mengenkripsinya dengan kunci publik CTF.
3. Alice mengirim kertas suaranya.
4. CTF mendekripsikan kertas suara, mengecek apakah tanda tangan tersebut valid, dan mengecek basis datanya untuk memastikan nomor seri kertas suara tersebut belum pernah digunakan sebelumnya (hal ini untuk mencegah Alice memilih lebih dari satu kali). Pada akhir pemilihan umum, CTF mengumumkan hasil pemilihan.

Beberapa Ekstensi dari Protokol Dasar

Untuk mengatasi berbagai masalah kemanan yang muncul pada sistem *digital cash* dan pemilihan umum *online*, maka dilakukan pengembangan terhadap protokol dasar yang telah dijelaskan. Permasalahan yang utama adalah bagaimana cara mencegah Alice untuk tidak memberikan dokumen yang telah dicurangi kepada bank. Sebagai contoh, apa yang dapat mencegah Alice memberikan pesan kepada bank sebagai berikut: "Tolong berikan Alice uang sebanyak 100 juta". Karena bank menerapkan *blind signature*, maka bank tersebut tidak dapat mengetahui isi dokumen. Untuk mengatasi masalah tersebut, terdapat dua solusi, yaitu:

1. Bank dapat menggunakan kunci publik yang berbeda untuk jumlah uang yang berbeda. Karena itu, jika Alice menginginkan uang 100 juta, maka ia harus mendapatkan tanda tangan dari bank dengan kunci publik yang berkoresponden dengan jumlah uang tersebut. Sebagai hasilnya, Alice tidak dapat menipu siapapun untuk percaya bahwa jumlah uang tersebut melebihi nilai uang yang sebenarnya.

2. Alice dan bank dapat melakukan protokol *cut and choose*. Pada protokol ini, Alice menyiapkan beberapa angka, misalkan 9, yaitu C1,..,C2. Setiap koin seharusnya identik kecuali nomor serinya. Kemudian, Alice mem"buta"kan setiap koin tersebut dan mengirimkannya kepada bank. Bank menerima semua koin tersebut, namun memilih hanya satu dari sejumlah koin itu dan memberitahukan Alice untuk membuka *blinding factor* untuk koin-koin tersebut. Dalam hal ini, bank bertanya pada Alice untuk mendapatkan informasi guna membuka (*unblind*) koin-koin tersebut. Setelah Alice membuka *blinding factor* untuk kedelapan koin lainnya, bank membuka koin-koin tersebut, dan memeriksanya. Jika semua koin berada pada bentuk yang benar, maka Bank memberikan

blind signature pada koin yang tadi dipilih oleh bank dan mengirimkannya kepada Alice. Bank sangat yakin bahwa koin tersebut berada pada format yang benar karena jika Alice menyertakan minimal satu koin yang tidak benar di antara sembilan koin lainnya, maka penipuan tersebut akan ketahuan dengan probabilitas 8/9.

Isu keamanan yang kedua adalah bagaimana seseorang dapat mencegah Alice dari menggandakan uang elektronisnya *C*. Jika telah terjadi tindakan penggandaan, maka bagaimana cara mendeteksi bahwa Alice lah si pelakunya. Solusi standar dari masalah tersebut adalah dengan menerapkan hukuman yang seberat-beratnya bagi pelaku penggandaan uang.

Solusi lain yang dapat diterapkan adalah dengan membuat daftar mengenai koin yang telah digunakan. Daftar ini dikelola oleh bank. Kemudian, pada setiap transaksi, setelah menerima sebuah koin dari vendor, bank akan mengecek untuk melihat apakah koin tersebut telah digunakan. Jika telah digunakan, bank akan menginformasikan vendor mengenai hal tersebut agar vendor tidak memberikan barang tersebut kepada pelanggan Alice. Skema tersebut akurat tetapi mahal karena untuk setiap transaksi, vendor harus menghubungi bank dan menunggu bank memverifikasi koin sebelum memberikan barang kepada pelanggan; vendor harus melakukan hal tersebut karena jika Alice menggandakan uang dan tidak tertangkap secepatnya, maka Alice tidak akan dapat ditangkap karena identitasnya anonim. Hal ini tentu saja sangat mahal. Kekurangan dari cara ini adalah vendor harus mengetahui dengan siapa ia bertransaksi. Jika Alice kedapatan menggandakan uang, tetapi ia berkomunikasi dengan vendor melalui suatu *channel* yang anonim, maka Alice tetap dapat melarikan diri. Selanjutnya, kerugian lainnya dari *channel* ini adalah Alice tetap dapat menggandakan uangnya sebelum daftar diperbaharui.

4. *Group Digital Signatures*

Pada skema *group digital signature*, anggota dari suatu kelompok dapat melakukan tanda tangan dijital pada suatu dokumen atas nama seluruh anggota kelompok. Tanda tangan tersebut dapat diverifikasi dengan menggunakan kunci publik kelompok (*group public key*). Ketika suatu dokumen telah ditandatangani, hanya seorang ketua kelompok yang dapat menentukan siapa anggota yang telah menandatangani dokumen tersebut. Selanjutnya, *group signature* ini harus didesain sehingga tidak ada seorang anggota kelompok pun yang dapat memalsukan tanda tangan anggota kelompok lainnya. Jadi, pada *group digital signature*, terdapat satu kunci publik kelompok dan lebih dari satu kunci privat anggota kelompok. Konsep ini kerap diaplikasikan di perusahaan-perusahaan; dimana *group signature* digunakan untuk memvalidasi daftar harga, *press release*, atau kontrak dijital; pelanggan hanya mengetahui kunci publik tunggal perusahaan untuk memverifikasi tanda tangan. Dengan menggunakan *group digital signature* ini, perusahaan dapat menyembunyikan struktur internalnya sekaligus menentukan karyawan yang mana yang menandatangani dokumen.

Skema *group digital signature* terdiri dari lima prosedur dibawah ini [11]:

1. *Setup*
   Dengan menggunakan parameter kemanan l dan algoritma probabilistik, bangkitkan kunci publik kelompok Y dan sebuah kunci rahasia administrasi S yang ditujukan untuk manajer kelompok.

2. *Join*
   Gabungkan protokol interaktif antara manajer kelompok dan anggota kelompok yang baru, misalnya Bob. Penggabungan ini bertujuan menciptakan kunci rahasia untuk Bob, yaitu χ, dan sertifikat keanggotaannya, yaitu A.

3. *Sign*
   Tanda tangani protokol interaktif antara anggota kelompok, yaitu Bob dan seorang pengguna eksternal, yaitu Alice. Penandatanganan ini melibatkan masukan berupa pesan m dari Alice dan kunci rahasia χ milik Bob. Keluaran yang dihasilkan adalah sebuah tanda tangan s pada pesan m.

4. *Verify*
   Lakukan verifikasi dengan menggunakan algoritma dimana jika terdapat masukan (m,s, Y), tentukan apakah s merupakan tanda tangan yang valid untuk pesan m sesuai dengan kunci publik kelompok Y.

5. *Open*
   Lakukan pengecekan untuk mengetahui identitas anggota kelompok yang

mengeluarkan tanda tangan *s* pada pesan *m* jika terdapat masukan (*m,s,S*).

Implementasi kelima prosedur diatas menjadi suatu skema *group blind signature* membutuhkan komputasi matematis yang rumit serta membutuhkan pengetahuan akan logaritma diskrit. Salah satu implementasi skema *group blind signature* telah dilakukan oleh Camenisch dan Stadler[3]. Selanjutnya perhitungan matematis dari skema tersebut dapat dilihat pada [7][11].

Berikut ini terdapat beberapa syarat (*requirement*) keamanan yang harus dipenuhi oleh suatu skema *group digital signature*:

1. *Unforgeability* (tidak dapat dipalsukan)
   Hanya anggota kelompok yang dapat mengeluarkan tanda tangan yang valid atas nama seluruh anggota kelompok. Atau dengan kata lain, hanya anggota kelompok yang dapat mengeluarkan tanda tangan yang dapat diverifikasi dengan menggunakan kunci publik kelompok.

2. *Conditional Signer Anonymity* (penanda tangan anonim)
   Siapapun dapat mengecek dengan mudah apakah suatu pasangan pesan dan tanda tangan telah ditandatangani oleh beberapa anggota kelompok, tetapi hanya manajer kelompok yang dapat menentukan dengan benar siapakah anggota kelompok yang telah memberikan tanda tangan.

3. *Undeniable Signer Identity* (identitas penanda tangan tidak dapat disangkal)
   Manajer kelompok selalu dapat menentukan identitas dari anggota kelompok yang mengeluarkan tanda tangan. Lebih jauh lagi, manajer kelompok tersebut juga dapat membuktikan kepada entitas lain (misalnya hakim, juri, dan sebagainya) mengenai siapa anggota kelompok yang telah menandatangani suatu dokumen tertentu tanpa membahayakan anonimitas anggota kelompok itu pada pesan-pesan yang telah ditandatangani atau yang mungkin akan ditandatangani oleh anggota kelompok yang bersangkutan.

4. *Unlinkability*
   Secara komputasi, setiap orang kecuali manajer kelompok tidak dapat membuktikan jika terdapat dua tanda tangan berbeda telah dilakukan oleh seorang anggota kelompok yang sama.

5. *Security Against Framing Attacks* (keamanan terhadap serangan *framing*)
   Serangan *framing* merupakan serangan terhadap *group digital signature* dimana seorang anggota kelompok dapat menandatangani suatu dokumen atas nama anggota kelompok yang lain. Sehubungan dengan kasus tersebut, suatu skema *group digital signature* yang aman hendaknya dapat mengatasi serangan *framing*; yaitu tidak ada sekumpulan anggota kelompok, termasuk manajer kelompok yang dapat menandatangani suatu pesan atas nama anggota kelompok yang lain. Hal ini dapat dijamin dengan melakukan prosedur *open*.

6. *Coalition Resistance*
   Tidak ada sekumpulan anggota kelompok, termasuk manajer kelompok yang dapat bersekongkol dan membangkitkan tanda tangan dijital yang valid namun tidak dapat dilacak. Secara khusus, aspek keamanan ini bertujuan untuk mencegah serangan dimana suatu koalisi antara anggota kelompok berkumpul, dan mengumpulkan informasi, serta membangkitkan tanda tangan dijital yang lolos dari prosedur *Verify* tetapi tidak dapat ditentukan siapa penandatangannya oleh prosedur *Open*.

Untuk membuat suatu skema *group digital signature* yang baik, diperlukan efisiensi terhadap beberapa parameter di bawah ini:
1. Ukuran (jumlah bit) kunci publik kelompok *Y*.
2. Ukuran (jumlah bit) *group digital signature* yang sebenarnya pada pesan.
3. Efisiensi dari protokol *Sign, Verify, Setup, Open,* dan *Join.*

5. *Group Blind Digital Signature*

Group blind digital signature mengkombinasikan properti *group signature* dan *blind signature*. Penggunaanya lebih ke penggunaan *blind signature*. Beberapa aplikasi *group blind digital signature* adalah pada sistem *electronic cash* yang melibatkan banyak bank dan pemilihan umum *online* yang melibatkan banyak server.

Syarat (*requirement*) keamanan pada skema *group blind digital signature* sama seperti syarat

keamanan pada *group digital signature*. Satu-satunya tambahan adalah adanya properti kebutaan (*blindness*) pada tanda tangan dijital. Karena itu, syarat-syarat kemanan pada *group blind digital signature* adalah *blindness of signatures, unforgeability, conditional signer anonymity, undeniable signer identity, unlinkability, security against framing attacks,* dan *coalition resistance.*

Properti *blindness of signatures* berarti penandatangan tidak dapat melihat pesan yang ditandatanganinya. Lebih jauh lagi penanda tangan tidak memiliki ingatan apakah ia telah menandatangani pesan tersebut. Walaupun demikian, ia dapat memverifikasi bahwa tanda tangannya memang valid.

Seperti halnya syarat keamanan pada *group blind digital signature,* protokol atau prosedur pada *group blind digital signature* pun sama persis seperti protokol pada *group digital signature*. Untuk mengingatkan, protokol-protokol tersebut antara lain: *setup, join, sign, verify,* dan *open*.

6. Aplikasi *Group Blind Digital Signature* pada *Digital Cash Payment* dan Pemilihan Umum secara *Online*

Pada bagian ini akan membahas aplikasi *group blind digital signature* pada *electronic cash* dan pemilihan umum *online*.

a. Aplikasi *Group Blind Digital Signature* pada *Digital Cash Payment*

Penerapan *group blind digital signature* pada *electronic cash* hampir sama dengan penerapan *blind signature* pada *electronic cash*. Namun, pada bagian ini, terdapat perbedaan dalam hal model bank yang digunakan. Model bank yang digunakan adalah bank elektronik yang terdistribusi (*distributed electronic banking*).

a.1 Bank Elektronik yang Terdistribusi (*Distributed Electronic Banking*)

Pada model ini, terdapat sekumpulan besar bank yang diawasi oleh sebuah bank sentral negara, misalnya Bank Indonesia. Setiap bank dalam kumpulan tersebut dapat mengeluarkan *electronic cash*. Agar bank elektronik yang terdistribusi tersebut dapat berjalan dengan baik, maka dibutuhkan properti-properti sebagai berikut:

1. Tidak ada bank yang dapat melacak *electronic cash* yang telah dikeluarkan oleh bank yang bersangkutan. Jika suatu bank mengeluarkan sebuah *electronic cash* kepada seorang pelanggan, dan jika kemudian bank itu melihat lagi *electronic cash* yang telah dikeluarkannya, maka bank yang bersangkutan tidak dapat menentukan identitas pelanggan mana yang menggunakan *electronic cash* tersebut. Jika pelanggan menggunakan beberapa *electronic cash*, maka ketika bank melihat *electronic cash*- *electronic cash* tersebut, bank tidak dapat mengidentifikasi bahwa *electronic cash*- *electronic cash* tersebut digunakan oleh pelanggan yang sama. Karena itu, sama seperti uang kertas tradisional, setiap orang dapat menggunakan *electronic cash*-nya dalam mode yang anonim.

2. Sebuah vendor hanya diharuskan untuk melakukan prosedur verifikasi universal yang tunggal berdasarkan kunci publik kelompok. Prosedur ini dimaksudkan untuk memastikan validitas tanda tangan bank pada berbagai *electronic cash* yang diterima oleh vendor. Prosedur ini dapat berjalan tanpa harus mengetahui bank yang mana yang mengeluarkan *electronic cash.* Hal ini memudahkan pekerjaan vendor karena vendor hanya membutuhkan informasi mengenai kunci publik kelompok yang hanya ada satu. Skema ini mengadopsi skema *group signature*. Perhatikan bahwa, walaupun tanda tangan pada *electronic cash* valid, tetap ada kemungkinan *electronic cash* tersebut tidak digunakan dengan benar, misalnya jika *electronic cash* tersebut sudah pernah digunakan sebelumnya.

3. Terdapat satu kunci publik untuk seluruh bank yang tergabung dalam bank elektronik yang terdistribusi. Ukuran kunci publik ini tidak tergantung dari jumlah bank yang tergabung dalam kumpulan bank elektronik yang terdistribusi. Hal ini berdampak positif karena tidak perlu memodifikasi kunci publik jika ada penambahan maupun pengurangan jumlah bank yang tergabung dalam kumpulan bank elektronik yang terdistribusi. Akibatnya, skema ini masih aplikatif pada kumpulan dengan jumlah bank yang sangat banyak.

4. Hanya bank sentral yang dapat menentukan bank yang mana yang mengeluarkan suatu *electronic cash* tertentu. Hal ini sesuai dengan properti *conditional signer anonymity*. Restriksi ini memberikan lapisan ekstra dalam hal anonimitas karena baik identitas pengguna *electronic cash* maupun identitas bank yang mengeluarkan *electronic cash* tidak diketahui.

5. Tidak ada sekumpulan bank, termasuk bank sentral dapat mengeluarkan *electronic cash* atas nama bank yang lain. Dengan kata lain, tidak ada bank atau entitas yang lain yang dapat melakukan serangan *frame*.

6. Berbagai koalisi bank (tidak termasuk bank sentral) tidak dapat membangun *electronic cash* yang tidak dapat dilacak. Dengan kata lain, tidak ada koalisi yang dapat mengeluarkan *electronic cash* yang tidak dapat dilacak pembuatnya oleh bank sentral.

Selanjutnya, akan dijelaskan bagaimana mengimplementasikan suatu skema *group blind digital signature* yang memenuhi properti-properti di atas.

a.2 Penerapan *Group Blind Digital Signature* pada Bank Elektronik yang Terdistribusi

Pada bagian ini akan dijelaskan modifikasi terhadap protokol penerapan *blind signature* pada *digital cash payment* yang telah dijelaskan di Bab 3 bagian c. Aplikasi *blind signature* pada *digital cash payment.* Pihak-pihak yang terlibat dalam protokol ini adalah Alice, Bob, Bank A, dan Bank B, dan Bank Indonesia. Alice adalah pelanggan Bank A. Alice ingin membeli beberapa item dari vendor, yaitu Bob. Bank yang digunakan oleh Bob adalah Bank B. Sedangkan Bank Indonesia berfungsi sebagai bank sentral.

1. *Setup*

Aktivitas-aktivitas yang dilakukan pada tahap ini meliputi pembentukan kelompok bank yang terdistribusi. Setiap bank melakukan protokol *join* dengan manajer kelompok, yaitu bank sentral. Setiap bank juga dapat menandatangani dokumen atas nama seluruh bank dalam kelompok.

2. Withdrawal

Untuk melakukan penarikan uang, maka harus dilakukan protokol sebagai berikut:

1. Alice menciptakan koin elektronik *C*. Koin ini memiliki nomor seri dan berbagai informasi terkait dengan mata uang, misalnya nilai uang.
2. Alice meminta Bank A untuk memberikan *group blind digital signature* pada koin *C*.
3. Bank A memberikan *group blind digital signature* pada koin *C* dan mengurangi sejumlah uang (sesuai yang tertera pada koin C) dari *account* milik Alice. Sekarang Alice telah memiliki suatu koin *C* beserta tanda tangan dijital yang valid.

3. *Spending*

Protokol untuk menggunakan uang adalah sebagai berikut:

1. Alice memberikan koin *C* beserta tanda tangan dijital dari bank pada koin tersebut kepada vendor, yaitu Bob.
2. Bob mengecek apakah tanda tangan dijital pada koin *C* tersebut otentik atau tidak. Hal ini dapat dilakukan dengan mudah melalui kunci publik kelompok.
3. Jika tanda tangan dijital tersebut valid, maka Bob memberikan koin tersebut kepada bank-nya, yaitu Bank B untuk disimpan. Bob kemudian menunggu tanggapan dari Bank B.

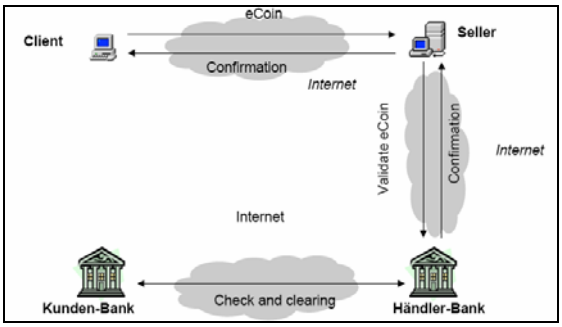
4. *Deposit*

Protokol untuk melakukan penyimpanan adalah sebagai berikut:

1. Bob mengambil koin *C* beserta tanda tangan dijital dari Bank A pada koin tersebut, dan memberikannya kepada Bank B.
2. Bank B memverifikasi koin tersebut dengan cara mengecek tanda tangan dijital pada koin itu. Untuk melakukan pengecekan, Bank B tidak perlu mengetahui siapakah Bank A Pengecekan dapat dilakukan dengan mudah dengan menggunakan kunci publik kelompok.
3. Bank B kemudian mengecek apakah koin tersebut pernah digunakan sebelumnya. Untuk itu, semua bank harus me-*maintain* suatu daftar global dari koin-koin yang sudah pernah digunakan.
4. Jika pengecekan terhadap penggandaan penggunaan koin telah selesai dilakukan, maka Bank B menambahkan sejumlah uang yang tertera pada koin ke dalam *account* Bob.
5. Bob memberikan item yang dibeli oleh Alice.

Jika dicermati lebih lanjut, skema di atas memiliki masalah utama, yaitu skema di atas hanya bisa dijalankan pada kondisi *online*. Maksudnya, vendor Bob harus benar-benar memastikan apakah koin yang diterimanya benar-benar valid dan belum pernah digunakan sebelumnya sebelum memberikan item barang yang diinginkan pelanggan. Satu-satunya cara untuk memastikan bahwa koin yang diterima oleh vendor belum pernah digunakan sebelumnya adalah dengan melibatkan bank dalam melakukan pengecekan. Hal ini berarti harus terdapat suatu hubungan *online* antara vendor dan bank. Untuk mengatasi masalah tersebut, maka dibuatlah skema *offline electronic cash*.

Secara singkat, penerapan *group blind digital signature* pada *digital cash payment* dapat dilihat pada Gambar 4.



Gambar 4. Aplikasi *group blind signature* pada *digital cash payment*

a.3 Skema *Offline Electronic Cash*

Salah satu solusi yang mungkin dari masalah di atas disebut *anonymity-revoking trustee,* yaitu melibatkan pihak ketiga yang dipercaya. Pihak ketiga ini dapat membatalkan jika dideteksi adanya penipuan. Skema *electronic cash* dengan menggunakan pihak ketiga yang anonim ini pertama kali diperkenalkan oleh Maurer Camenisch dan Stadler [2][8]. Skema yang diperkenalkan oleh Maurer Camenisch dan Stadler ternyata hanya dapat diterapkan pada model bank tunggal. Namun, skema yang diajukan pada makalah ini melibatkan lebih dari satu bank dan membutuhkan pihak ketika setiap kali seorang pengguna membuka *account*-nya. Sehubungan dengan hal tersebut,maka ide yang diajukan adalah dengan membuat kelompok pelanggan dan seorang manajer kelompok sebagai pihak ketiga. Pelanggan dapat menggabungkan tanda tangan dijital kelompoknya ke koin elektronik selama fase *spending*, dan sebagai hasilnya, identitas kelompok pelanggan tersebut dapat dikodekan selama transaksi berlangsung. Selanjutnya, hanya pihak ketiga yang dipercaya, yaitu manajer kelompok pelanggan yang dapat menentukan identitas pelanggan.

Skema di atas direpresentasikan dalam lima buah fase, yaitu *setup, withdrawal, spending, depositing,* dan *anonymity revocation*.

1. *Setup*

Aktivitas-aktivitas yang dilakukan pada tahap ini meliputi pembentukan kelompok bank yang terdistribusi. Setiap bank melakukan protokol *join* dengan manajer kelompok, yaitu bank sentral. Setiap bank juga dapat menandatangani dokumen atas nama seluruh bank dalam kelompok. Sebagai tambahan, dibentuk pula kelompok yang terdiri dari para pelanggan. Ketika seorang pelanggan membuka *account* baru, maka secara otomatis pelanggan tersebut didaftarkan ke dalam kelompok pelanggan. Pihak ketiga yang dapat dipercaya adalah manajer kelompok dari kelompok pelanggan ini. Asumsi yang digunakan pada skema ini adalah semua vendor merupakan bagian dari *Public-Key Infrastructure* (PKI). Maksudnya, semua vendor memiliki kunci publik dan kunci privat yang berasosiasi dengan PKI tersebut.

2. *Withdrawal*

Protokol pada fase ini sama seperti protokol pada fase *withdrawal* di bagian skema *online* sebelumnya.

3. *Spending*

Protokol untuk menggunakan *electronic cash* adalah sebagai berikut:

1. Alice memberikan koin *C* beserta tanda tangan dijital dari bank pada koin tersebut kepada vendor, yaitu Bob.
2. Bob kemudian mengecek apakah tanda tangan dijital pada koin *C* valid atau tidak. Hal ini dapat dilakukan dengan menggunakan kunci publik kelompok bank. Jika tanda tangan dijital tersebut valid, maka Bob melakukan langkah-langkah di bawah ini:
   (a) Bob membangkitkan urutan bit secara acak, yang disebut *nonce*.

(b) Bob membuat pesan yang berisi identitasnya, *nonce*, serta waktu sekarang (*current time*).
(c) Bob memberikan tanda tangan dijital pada pesan tersebut dengan menggunakan kunci privatnya yang berasosiasi dengan PKI.
(d) Bob mengirimkan pesan beserta tanda tangannya kepada Alice.

3. Alice mengecek apakah tanda tangan dijital Bob pada pesan valid atau tidak. Kemudian Alice memeriksa waktu yang dicantumkan pada pesan. Alice lalu membuat pesannya sendiri yang berisi konkatenasi dari koin *C*, tanda tangan dijital bank pada *C,* dan pesan yang baru saja diterimanya dari Bob beserta tanda tangan dijital Bob. Pada pesan yang baru tersebut, Alice juga menyertakan tanda tangan dijital kelompok pelanggan. Alice lalu mengirimkan pesan tersebut beserta tanda tangan dijital kepada Bob.
4. Bob mengecek apakah Alice telah memberikan pesan dalam format yang benar dan apakah pesan asal beserta tanda tangan dijitalnya merupakan bagian dari pesan yang baru dikirim oleh Alice. Bob kemudian mengecek apakah tanda tangan dijital kelompok pelanggan yang diberikan oleh Alice valid atau tidak. Hal ini untuk memastikan agar pihak ketiga akan mampu mencabut anonimitas Alice jika sewaktu-waktu perlu dilakukan.
5. Setelah semua pengecekan dilakukan, Bob memberikan item yang dibeli oleh Alice.

Pada fase ini, terdapat pesan yang dibuat oleh Bob. Hal ini dimaksudkan untuk mencegah serangan yang bersifat *transferable* (dapat dioperkan) berikut ini. Misalkan, pada protokol di atas, hanya terdapat tanda tangan dijital kelompok pelanggan yang dikeluarkan oleh Alice pada koin *C*; tanpa adanya *nonce* atau pesan ekstra. Selanjutnya, andaikan Alice sendiri adalah seorang vendor maka Alice dapat terlibat ke dalam dua protokol transaksi pada saat yang bersamaan (konkuren). Pada protokol yang pertama, Alice berperan sebagai pelanggan dan Bob sebagai vendor. Pada protokol yang kedua, Alice bertindak sebagai vendor dan Charles sebagai pelanggan. Jika tidak terdapat pesan dan tanda tangan dijital dari Bob kepada Alice, maka Alice dapat dengan mudah meneruskan semua tanggapan yang didapatkannya dari Bob kepada Charles. Dengan kata lain, Alice dapat berpura-pura sebagai Bob ketika ia berkomunikasi dengan Charles. Akibatnya, pada akhir transaksi, Alice dapat mengambil koin milik Charles dan memberikannya secara langsung pada Bob. Dengan demikian, identitasnya tidak akan ketahuan selama melakukan protokol tersebut. Identittas Alice tidak adan pernah dikaitkan dengan koin. Karena itu, jika mekanisme *anonymity-revocation* diterapkan pada koin elektronik, nama Charles lah satu-satunya yang akan ketahuan, sedangkan Alice dapat "melarikan diri" dengan bebas setelah melakukan penipuan.

Jika terdapat tanda tangan dijital vendor, maka jika Alice mencoba untuk meneruskan respon Bob kepada Charles, maka Charles dapat mengecek tanda tangan dijital pada pesan dan memutuskan apakah pesan tersebut berasal dari Alice atau tidak. Jika sebaliknya, Alice mencoba untuk menghilangkan tanda tangan dijital milik Bob, dan menggantinya dengan tanda tangan dijital miliknya, maka hasil koin elektronik yang diperolehnya dari Charles akan mengandung tanda tangan dijital miliknya. Selanjutnya, jika Alice mencoba memberikan koin elektronik yang sama kembali kepada Bob, maka Bob akan segera menyadari bahwa tanda tangan dijital pada *nonce* telah berubah.

Kerugian kecil dari skema di atas adalah diketahuinya identitas vendor. Hal ini juga yang membedakan dari skema sebelumnya. Meskipun vendor tidak keberatan pelanggan anonim, tetapi pembeli mungkin ingin mengetahui identitas vendor jika item yang dibelinya rusak di kemudian hari.

4. *Deposit*

Protokol untuk melakukan penyimpanan *electronic cash* ke bank adalah sebagai berikut:

1. Bob mengambil koin *C* beserta tanda tangan dijital dari Bank A pada koin tersebut, dan memberikannya kepada Bank B.
2. Bank B memverifikasi koin tersebut dengan cara mengecek tanda tangan dijital pada koin. Untuk melakukan pengecekan, Bank B tidak perlu mengetahui siapakah Bank A Pengecekan dapat dilakukan dengan mudah dengan menggunakan kunci publik kelompok bank dan kunci publik kelompok pelanggan.
3. Bank B kemudian mengecek apakah koin tersebut pernah digunakan sebelumnya. Untuk itu, semua bank harus me-*maintain* suatu daftar global dari koin-koin yang sudah pernah digunakan. Jika koin sudah

pernah digunakan sebelumnya, maka pihak ketiga harus dipanggil untuk melakukan protokol *anonymity revocation*.

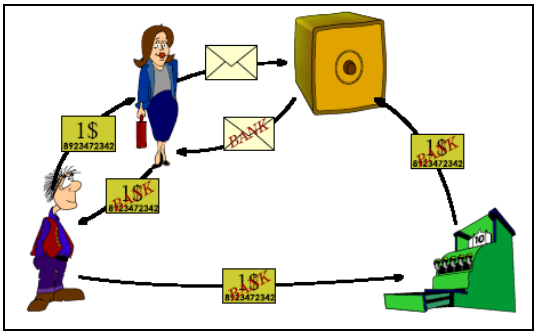
4. Jika pengecekan terhadap penggandaan penggunaan koin telah selesai dilakukan, maka Bank B menambahkan sejumlah uang yang tertera pada koin ke dalam *account* Bob.
6. Bob memberikan item yang dibeli oleh Alice.

5. *Anonymity Revocation*

Jika terdapat alasan yang dapat dipercaya bahwa suatu koin telah dicurangi, maka identitas dari pengguna koin tersebut dapat dilacak sebagai berikut:

1. Koin *C* beserta tanda tangan dijital milik bank pada *C,* dan tanda tangan dijital milik pelanggan pada *C* diberikan kepada pihak ketiga.
2. Karena pihak ketiga adalah manajer kelompok pelanggan, maka ia dapat menggunakan algoritma *open* untuk menentukan identitas sebenarnya dari penandatangan.

Secara singkat, penerapan *group blind digital signature* pada *digital cash payment* dengan melibatkan pihak ketiga yang dapat dipercaya dapat dilihat pada **Error! Reference source not found.**.



Gambar 5. *Group blind digital signature* pada *digital cash payment* dengan melibatkan pihak ketiga

b. Aplikasi *Group Blind Digital Signature* pada Pemilihan Umum secara *Online*

Skema aplikasi *group blind digital signature* pada pemilihan umum secara *online* mirip dengan skema aplikasi *blind digital signature* pada pemilihan umum secara *online* yang telah dibahas di Bab 3 bagian d. Aplikasi *Blind Digital Signature* pada Pemilihan Umum secara *Online*. Yang membedakan adalah pada aplikasi kali ini, terdapat pemungutan suara secara online yang terdistribusi.

Pada skema pemungutan suara secara online yang terdistribusi ini, terdapat tiga entitas yang terlibat, yaitu pemilih (Alice), Badan Registrasi Lokal (BRL), dan Badan Pengiriman Suara (BPS). Terdapat banyak BRL dan setiap pemilih hanya dapat mendaftarkan diri pada satu BRL; hal ini berkoresponden dengan keadaan di dunia nyata dimana seorang pemilih hanya dapat terdaftar di suatu pusat pemungutan suara lokal. Jadi, terdapat banyak BRL yang membentuk kelompok dan diatur oleh beberapa badan pusat. Asumsi yang digunakan adalah kertas suara direpresentasikan dengan "Ya" dan "Tidak".

Protokol pemungutan suara secara online yang terdistribusi ini dibagi menjadi dua tahap, yaitu registrasi (*registration*) dan pemungutan suara (*voting*).

1. Registrasi (*registration*)

Protokol registrasi adalah sebagai berikut:

1. Alice membuat dua kertas suara elektronik *B1* dan *B2*. Kertas suara tersebut memiliki nomor seri dan beberapa informasi relevan dengan pemungutan suara. *B1* merepresentasikan suara "ya" sedangkan *B2* merepresentasikan suara "tidak".
2. Alice kemudian mengambil kertas suara B1 dan B2 kemudian mem"buta"kannya. Alice kemudian mengirimkan versi "buta" tersebut ke BRL.
3. BRL mengecek basis datanya untuk memastikan bahwa Alice belum pernah melakukan pemilihan sebelumnya. Jika Alice belum melakukan pemungutan, BRL akan menandatangani kertas suara buta tersebut kemudian mengembalikannya kepada Alice.

2. Pemungutan Suara (*voting*)

Protokol pemungutan suara adalah sebagai berikut:

1. Alice mengekstrak kertas suara tersebut dan memiliki dua kertas suara valid yang telah ditandatangani oleh BRL.
2. Alice memilih kertas suara (yang telah diberi tanda tangan oleh BRL) mana yang

ingin dipilihnya ("ya" atau "tidak"). Alice kemudian mengenkripsinya dengan kunci publik BPS.

3. Alice mengirim kertas suaranya kepada BPS.
4. BPS mendekripsikan kertas suara, mengecek apakah tanda tangan tersebut valid, dan mengecek basis datanya untuk memastikan nomor seri kertas suara tersebut belum pernah digunakan sebelumnya (hal ini untuk mencegah Alice memilih lebih dari satu kali). Pada akhir pemilihan umum, BPS mengumumkan hasil pemilihan.

Variasi lain dari protokol ini adalah dengan mengirimkan kertas suara kepada setiap pemilih dengan menggunakan *email*. Aplikasi pemungutan suara itu sendiri merupakan suatu aplikasi berbasis *web* dengan menggunakan *applet*. Penerapan aplikasi ini telah dilakukan di Universitas Cambridge [1]. Penerapan lainnya dari aplikasi ini juga dapat dilihat pada [6].

7. Kesimpulan

Beberapa kesimpulan dan saran pengembangan yang dapat diambil dari penjelasan mengenai teori dan aplikasi *group blind digital signature*, antara lain:

1. Penemuan kriptografi kunci publik telah membawa banyak hal baru dan perkembangan dalam dunia kriptografi; salah satunya adalah tanda tangan dijital.

2. *Blind digital signature* memungkinkan seseorang menandatangani suatu dokumen tanpa mengetahui isinya.

3. *Blind digital signature* dapat dikembangkan dari berbagai algoritma kunci publik, misalnya RSA dan ElGamal. Penambahan properti *blindness* terhadap sejumlah algoritma dasar kunci publik tersebut memiliki kelebihan dan kekurangan masing-masing.

4. Properti *blindness* pada *blind digital signature* sangat mendukung penerapannya pada *digital cash payment* dan pemilihan umum secara *online.*

5. Properti *blindness* pada aplikasi *digital cash payment* menimbulkan kerugian utama, yakni sulit untuk melacak pelaku, jika terjadi penggandaan atau pemalsuan *electronic cash*.

6. *Group digital signature* memungkinkan seorang anggota kelompok menandatangani suatu dokumen atas nama seluruh anggota kelompok.

7. Perpaduan antara *group digital signature* dan *blind digital signature* memungkinkan penerapan *digital cash payment* dan pemilihan umum secara *online* pada dunia nyata. Karena selain aplikasi tersebut membutuhkan properti *blindness*, juga membutuhkan kolaborasi lebih dari satu entitas sejenis yang terlibat di dalamnya, misalnya berbagai bank.

8. Penggunaan *group blind digital signature* pada *digital cash payment* mengatasi masalah kemanan yang sering dijumpai pada berbagai sistem pembayaran online yang dijumpain pada *e-commerce*. Masalah keamanan yang diatasi adalah si pembeli tidak perlu memeberikan nomor kartu kreditnya kepada vendor.

9. Implementasi *group blind digital signature* pada *digital cash payment* yang dilakukan dengan mempertimbangkan semua aspek keamanan akan dapat menggantikan sistem pembarayan *online* saat ini yang menggunakan kartu kredit. Oleh karena itu diharapkan suatu saat aplikasi-aplikasi yang menerapkan *group blind digital signature* pada *digital cash payment* akan digunakan secara luas pada *e-commerce*.

10. Penerapan *group blind signature* pada *digital cash payment* masih menyisakan masalah efisiensi pada saat pengecekan apakah suatu *electronic cash* sudah pernah digunakan sebelumnya atau tidak. Masalah ini mengundang banyak riset untuk mengatasinya.

11. Terdapat berbagai macam skema *group blind digital signature* [11][12] yang masing-masing mengimplementasikan protokol setup*, join, sign, verify,* dan *open* dengan menambahkan properti *blindness*. Pembuktian efisiensi dan kemanan dari implementasi berbagai skema tersebut masih berupa pengujian secara teoritis dengan menggunakan berbagai notasi matematis yang rumit.

12. Permasalahan seputar skema yang paling efisien pada group blind digital signature merupakan masalah yang masih membutuhkan kajian lebih lanjut.

13. Pemanfaatan *group blind digital signature* pada pemilihan umum secara *online* lebih stabil daripada pemanfaatan *group blind digital signature* pada *digital cash payment.* Hal ini dapat dilihat dari banyaknya implementasi aplikasi berbasis web untuk melakukan pemilihan umum secara online [1][6].

Daftar Pustaka

[1] Anderson, Ross. *The Dancing Bear-A New Way of Composing Chipers*, Cambridge University.
http://www.cl.cam.ac.uk/~rja14/Papers/grizzle.pdf
TanggalAkses: 27 Oktober 2006 pukul 09:57

[2] Camenisch, Jan, Ueli Maurer, Markus Stadler. *Digital Payment Systems with Passive Anonymity-Revoking Trustees*.
http://www.ubilab.org/publications/print_versions/pdf/esorics96.pdf
TanggalAkses: 27 Oktober 2006 pukul 16:07

[3] Camenisch, Jan, dan Markus Stadler. *Efficient Group Signatures for Large Groups*
http://www.springerlink.com/index/BXQFMWUF90MKH86D.pdf
TanggalAkses: 27 Oktober 2006 pukul 16:07

[4] Chaum, David. *Blind Signatures for Untraceable Payments*,1983.
http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C82/199.pdf
Tanggal Akses: 27 Oktober 2006 pukul 17:38

[5] Diffie,W, dan M.E.Hellman. *New Direction in Cryptography*,1976.
http://crypto.csail.mit.edu/classes/6.857/papers/diffie-hellman.pdf
Tanggal Akses: 27 Oktober 2006 pukul 17:42

[6] Kofler, Robert, Robert Krimmer, Alexander Prosser, dan Martin-Karl Unger. *The Role of Digital Signature Cards in Electronic Voting*, Proceedings of the 37th Hawaii International Conference on System Sciences, 2004.
http://csdl.computer.org/comp/proceedings/hicss/2004/2056/05/205650116a.pdf
TanggalAkses: 27 Oktober 2006 pukul 16:30

[7] Lysyanskaya, Anna dan Zulfikar Ramzan. *Group Blind Signatures: A Scalable Solution to Electronic Cash*, Massachusetts Institute Of Technology, 1998.
http://www.cs.brown.edu/research/pubs/pdfs/1998/Lysyanskaya-1998-GBD.pdf
TanggalAkses: 27 Oktober 2006 pukul 16:34

[8] Messerschmitt, David G. *Anonymous Digital Cash Protocol*s, University of California, 1999.
http://www.eecs.berkeley.edu/~messer/netappc/Supplements/14-adcash.pdf
TanggalAkses: 27 Oktober 2006 pukul 17:58

[9] Mohammed, Elsayed, A.E.Emarah, dan Kh.El-Shenway. *A Blind Signature Scheme Based On ElGamal Signature*.
http://ieeexplore.ieee.org/iel5/7031/18937/00874771.pdf
TanggalAkses: 26 Oktober 2006 pukul 10:10

[10] Munir, Rinaldi. Diktat Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung

[11] Popescu, Constantin. *A Secure and Efficient Group Blind Signature Scheme*. University Of Oradea. A-List Publishing, 2003.
http://www.q2s.ntnu.no/publications/open/2003/Journal/2003_popescu_SEG.pdf
TanggalAkses: 27 Oktober 2006 pukul 17:00

[12] Ramzan, Sulfikar Amin. *Group Blind Digital Signatures: Theory and Applications*, Massachusetts Institute Of Technology, Mei 1999.
http://theory.lcs.mit.edu/~cis/theses/ramzanms.pdf

TanggalAkses: 27 Oktober 2006 pukul 17:45