Digital Cash

Septia Sukariningrum, Ira Puspitasari, Tita Mandasari

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : if12015@students.if.itb.ac.id , if12059@students.if.itb.ac.id, if12077@students.if.itb.ac.id

Abstrak

Permasalahan keamanan dan privasi saat ini sudah menjadi kebutuhan primer bagi pengguna kartu kredit. Salah satu solusi adalah pemakaian *digital cash*, yaitu sistem pembayaran yang mengandung sebuah tanda tangan digital dan dilengkapi dengan sepasang kunci publik-privat. Dua sistem keamanan tersebut melindungi privasi pemakai kartu dari semua usaha ilegal yang mungkin dilakukan oleh pihak yang tidak berwenang.

***Kata kunci**: digital cash, kriptografi, tugas*

1. Pendahuluan

Salah satu ciri ekonomi modern adalah globalisasi di segala aspek, termasuk perputaran uang yang cepat dan terkontrol. Dengan demikian, pemakaian uang tunai dalam transaksi menjadi tidak efektif dan efisien. Untuk itu telah dikembangkan pemakaian cek dan kartu kredit sehingga transaksi bisa dilakukan dengan cepat, aman, dan dalam nominal yang besar.

Namun, ini bukan tanpa masalah. Di dalam cek dan kartu kredit tersimpan data pribadi pemilik kartu yang memungkinkan pihak tidak berwenang untuk melacak semua transaksi yang pernah dilakukannya. Hal ini tentu saja melanggar privasi si pemilik kartu tersebut.

Salah satu solusi untuk masalah ini adalah pemakaian *digital cash*. *Digital cash*, atau disebut juga *e-cash*, adalah sistem pembayaran yang mengandung sebuah tanda tangan digital (*digital signature*) [1] dan dilengkapi dengan sepasang kunci publik-privat (*public-private keys*)[2]. Tanda tangan digital untuk mengotentikasi pemakai kartu dan sepasang kunci publik-privat untuk mengamankan proses pembayaran. Dua hal ini melindungi privasi pemilik kartu dari segala usaha ilegal.

Dalam praktiknya, *digital cash* dapat dibagi dalam 3 kategori. Pertama adalah pengkategorian *anonymous/identified*. Si pemilik kartu bisa anonim atau teridentifikasi dalam melakukan transaksi. Kedua adalah berdasarkan *online/offline*. Kategori *online* berarti si pemilik harus berkomunikasi dengan bank secara langsung untuk bertransaksi dengan pihak ketiga (misalnya toko); sementara kategori *offline* berarti transaksi bisa dilakukan tanpa melibatkan bank secara langsung. Dan ketiga adalah berdasarkan *smart cards/ purely electronic*. Pemakaian *smart card* seperti kartu kredit layaknya kecuali smart card menyimpan informasi uang di dalam chip yang terdapat pada kartu tersebut; sementara *purely electronic* memakai jaringan atau internet.

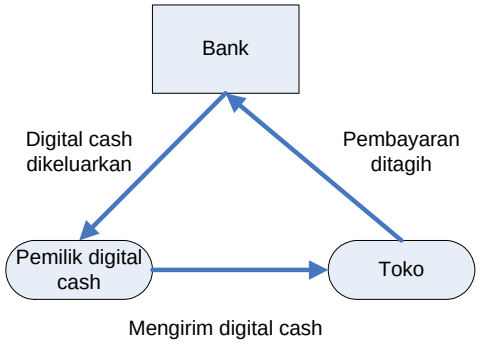
Tulisan ini membahas bagaimana mekanisme kerja dan bagaimana pemakaian *digital cash* ini.

2. Mekanisme kerja

2.1. Umum

Gambar 1 adalah mekanisme kerja umum *digital cash*. Seorang pemilik *digital cash* menginstal sebuah *cyber wallet* di sebuah komputer. Si pemilik *digital cash* dapat mengisi *cyber wallet*-nya dengan cara mengirim pesan terenkripsi ke bank. Pesan tersebut berisi permintaan untuk mengurangi sejumlah uang dari rekening si pemilik dan memasukkannya ke dalam *cyber wallet* si pemilik.

Kemudian, bank mendekripsi pesan tersebut dengan kunci privat bank dan mengotentikasi pemilik dan pesan memakai tanda tandan digital. Jika pesan sudah didekripsi dan otentikasi berhasil, maka bank membuat nomor seri, mengekripsi pesan, menandatangani dengan tanda tangan digital bank tersebut, dan mengembalikan ke pemilik. Dengan demikian, *cyber wallet* sudah terisi uang sejumlah yang diminta oleh pemilik.



Gambar 1. Skema dasar pemakaian digital cash

Si pemilik *digital cash* sekarang bisa memakai uang di *cyber wallet*-nya untuk berbelanja di toko-toko yang memiliki fasilitas pelayanan *digital cash*. Sebuah toko dengan fasilitas tersebut menerima *digital cash* dalam transaksinya dan memeriksa apakah digital cash tersebut sudah diotorisasi oleh bank yang berwenang. Kemudian toko mengontak pihak bank untuk memastikan bahwa *digital cash* tersebut belum dipakai di tempat lain dan jumlah uang yang dipakai dalam transaksi cukup tersedia di dalam *cyber wallet* si pemilik *digital cash*. Pada tahap akhir, jumlah uang dalam transaksi ditambahkan ke dalam rekening toko.

3. Protokol

Beberapa jenis *digital cash protocol*:

3.1. Protokol 1

1. Alice menyiapkan 100 *anonymous money orders*, yang masing-masing bernilai Rp. 1.000.000
2. Alice memasukkan setiap *money order* yang bernilai Rp. 1.000.000 dan sebuah kertas karbon ke dalam sebuah amplop. Sehingga Alice memiliki 100 amplop yang terdiri dari sebuah *money order* dan sebuah kertas karbon. Kemudian Alice memberikan 100 amplop tersebut ke Bank.
3. Bank membuka 99 amplop dan memeriksa bahwa semuanya bernilai Rp. 1.000.000
4. Bank menandai amplop ke seratus. Karena terdapat kertas karbon didalamnya, maka tanda dari Bank akan mengenai *money order* yang terdapat di dalam amplop. Bank mengembalikan amplop yang sudah ditandai kepada Alice dan memotong jumlah uang yang ada di rekening Alice sebesar Rp. 1.000.000.
5. Alice menggunakan *money order* yang terdapat dalam amplop untuk membeli *handphone*.

6. Penjual *handphone* memeriksa tanda dari Bank untuk menyakinkan bahwa *money order* tersebut asli.
7. Penjual *handphone* membawa *money order* ke Bank.
8. Bank melakukan verifikasi tanda pada *money order* tersebut dan menambahkan uang sebesar Rp. 1.000.000 ke rekening penjual *handphone*.

3.2. Protokol 2

Dengan menggunakan protokol 1, Bank tidak dapat memeriksa jika *money order* di fotocopy dan digunakan lagi oleh Alice. Pada protokol 2 ini terdapat mekanisme untuk mengatasi hal tersebut.

1. Alice menyiapkan 100 *anonymous money orders*, yang masing-masing bernilai Rp. 1.000.000. Pada setiap *money order*, Alice memberikan string acak yang unik dan cukup panjang, sehingga kemungkinan orang lain menggunakan string tersebut sangat kecil.
2. Alice memasukkan setiap *money order* yang bernilai Rp. 1.000.000 dan sebuah kertas karbon kedalam sebuah amplop. Sehingga Alice memiliki 100 amplop yang terdiri dari sebuah *money order* dan sebuah kertas karbon. Kemudian Alice memberikan 100 amplop tersebut ke Bank.
3. Bank membuka 99 amplop dan memeriksa bahwa semuanya bernilai Rp. 1.000.000
4. Bank menandai amplop ke seratus. Karena terdapat kertas karbon didalamnya, maka tanda dari Bank akan mengenai *money order* yang terdapat di dalam amplop. Bank mengembalikan amplop yang sudah ditandai kepada Alice dan memotong jumlah uang yang ada di rekening Alice sebesar Rp. 1.000.000.
5. Alice menggunakan *money order* yang terdapat dalam amplop untuk membeli *handphone*.
6. Penjual *handphone* memeriksa tanda dari Bank untuk menyakinkan bahwa *money order* tersebut asli.
7. Penjual *handphone* membawa *money order* ke Bank.
8. Bank melakukan verifikasi tanda pada *money order* tersebut dan memeriksa pada basisdata apakah string yang terdapat pada *money order* sudah pernah ditukarkan atau belum. Jika belum pernah, maka Bank menambahkan uang sebesar Rp. 1.000.000 ke rekening penjual *handphone* dan menambahkan string tersebut pada basis data.
9. Jika string tersebut telah ada maka Bank tidak menerima *money order* tersebut.

Dengan protokol ini, jika Alice mencoba untuk menggunakan hasil fotocopy dari *money order*, atau penjual *handphone* melakukan fotocopy terhadap *money order* yang diberikan Alice, maka Bank akan mengetahuinya.

3.3. Protokol 3

Dengan menggunakan protokol 2, Bank dapat memeriksa jika *money order* di fotocopy dan digunakan lagi oleh Alice. Namun Bank tidak dapat mengetahui apakah Alice yang memfotocopy *money order* tersebut atau penjual *handphone* yang memfotocopy *money order* tersebut. Pada protokol 3 ini terdapat mekanisme untuk mengatasi hal tersebut.

1. Alice menyiapkan 100 *anonymous money orders*, yang masing-masing bernilai Rp. 1.000.000. Pada setiap *money order*, Alice memberikan string acak yang unik dan cukup panjang,

sehingga kemungkinan orang lain menggunakan string tersebut sangat kecil.

2. Alice memasukkan setiap *money order* yang bernilai Rp. 1.000.000 dan sebuah kertas karbon kedalam sebuah amplop. Sehingga Alice memiliki 100 amplop yang terdiri dari sebuah *money order* dan sebuah kertas karbon. Kemudian Alice memberikan 100 amplop tersebut ke Bank.
3. Bank membuka 99 amplop dan memeriksa bahwa semuanya bernilai Rp. 1.000.000.
4. Bank menandai amplop ke seratus. Karena terdapat kertas karbon didalamnya, maka tanda dari Bank akan mengenai *money order* yang terdapat di dalam amplop. Bank mengembalikan amplop yang sudah ditandai kepada Alice dan memotong jumlah uang yang ada di rekening Alice sebesar Rp. 1.000.000.
5. Alice menggunakan *money order* yang terdapat dalam amplop untuk membeli *handphone*.
6. Penjual *handphone* memeriksa tanda dari Bank untuk menyakinkan bahwa *money order* tersebut asli.
7. Penjual *handphone* meminta Alice untuk menulis string identitas pada *money order*.
8. Alice menulis string tersebut.
9. Penjual *handphone* membawa *money order* ke Bank.
10. Bank melakukan verifikasi tanda pada *money order* tersebut dan memeriksa pada basisdata apakah string unik yang terdapat pada *money order* sudah pernah ditukarkan atau belum. Jika belum pernah, maka Bank menambahkan uang sebesar Rp. 1.000.000 ke rekening penjual *handphone* dan menambahkan string unik dan string identitas pada basis data.
11. Jika string unik telah ada maka Bank tidak menerima *money order* tersebut. Kemudian string identitas pada *money order* dibandingkan dengan string identitisa yang terdapat pada basisdata. Jika sama, maka Bank mengetahui bahwa penjual *handphone* yang memfotocopy *money order*, jika berbeda maka orang yang memberikan *money order* kepada penjual *Handphone* yang memfotocopy (dalam kasus ini Alice).

Protokol ini mengasumsikan, penjual *handphone* tidak mengganti string identitas setelah Alice menulisnya.

3.4. Protokol 4

Jika orang yang memberikan *money order* kepada penjual *handphone* yang melakukan fotoocopy dan memberikannya ke penjual *handphone*, maka pihak Bank ingin mengetahui siapakah orang tersebut. Hal ini dapat dilakukan dengan menyembunyikan identitas Alice pada *digital money order*.

1. Alice menyiapkan 100 *anonymous money orders*, yang masing-masing bernilai Rp. 1.000.000. Pada setiap *money order*, Alice memberikan string acak X, yang unik dan cukup panjang, sehingga kemungkinan orang lain menggunakan string tersebut sangat kecil.
   Pada setiap *money order* terdapat n pasang bit string identitas, I_1, I_2,….,I_n. Setiap pasang bit didapatkan dari:
   1) Alice membuat string yang memberikan informasi mengenai nama, alamat, dan informasi lain yang diperlukan oleh Bank mengenai Alice.

2) String tersebut dibagi menjadi dua bagian dengan menggunakan *secret splitting protocol* (tidak dibahas pada makalah ini). Kemudian Alice melakukan mensahkan *money order* dengan menggunakan *bit-commitment protocol*.

2. Alice menandatangani semua *money order* dengan menggunakan *blind signature protocol*. Kemudian Alice memberikan 100 amplop tersebut ke Bank.
3. Bank membuka 99 amplop dan memeriksa bahwa semuanya bernilai Rp. 1.000.000, memeriksa string unik, dan meminta Alice untuk memberikan string identitas.
4. Jika Bank sudah yakin bahwa Alice tidak berusaha untuk melakukan kecurangan makan Bank menandai amplop ke seratus. Karena terdapat kertas karbon didalamnya, maka tanda dari Bank akan mengenai *money order* yang terdapat di dalam amplop. Bank mengembalikan amplop yang sudah ditandai kepada Alice dan memotong jumlah uang yang ada di rekening Alice sebesar Rp. 1.000.000.
5. Alice menggunakan *money order* yang terdapat dalam amplop untuk membeli *handphone*.
6. Penjual *handphone* memeriksa tanda dari Bank untuk menyakinkan bahwa *money order* tersebut asli.
7. Penjual *handphone* meminta Alice untuk menulis sebagian string identitas yang bagain kiri atau bagian kanan pada *money order*. Kemudian penjual *Handphone* memberikan Alice string selector b_1, b_2,…. *Bn*. Alice membuka bagian kiri atau bagian kanan dari I_i, berdasarkan apakah b_i bernilai 0 atau 1.
8. Alice menulis string tersebut.
9. Penjual *handphone* membawa *money order* ke Bank.
10. Bank melakukan verifikasi tanda pada *money order* tersebut dan memeriksa pada basisdata apakah string yang terdapat pada *money order* sudah pernah ditukarkan atau belum. Jika belum pernah, maka Bank menambahkan uang sebesar Rp. 1.000.000 ke rekening penjual *handphone* dan menambahkan string tersebut pada basis data.
11. Jika string unik telah ada maka Bank tidak menerima *money order* tersebut. Kemudian string identitas pada *money order* dibandingkan dengan string identitisa yang terdapat pada basisdata. Jika sama, maka Bank mengetahui bahwa penjual *handphone* yang memfotocopy *money order*, jika berbeda maka orang yang memberikan *money order* kepada penjual *Handphone* yang memfotocopy (dalam kasus ini Alice). Karena penjual kedua yang menerima *money order*, memberikan Alice string selektor yang berbeda dari penjual yang pertama, sehingga pihak Bank dapat mencari posisi bit dari para penjual yang menyebabkan Alice membuka bagian kiri dan bagian kanan. Kemudian Bank melakukan XOR dari dua bagian tersebut dan mendapatkan identitas Alice.

4. Pemakaian

4.1. Digital Cash Praktis

Sebuah perusahaan Belanda, DigiCash, memiliki sebagian besar hak paten *digital cash* dan telah mengimplementasikan protokol-protokol *digital cash* dalam berbagai produk. Pihak yang tertarik dapat menghubungi

DigiCash BV, Kruislaan 419, 1098 VA Amsterdam, Belanda.

4.2. Protokol *Digital Cash* Lainnya

Sebenarnya masih banyak protocol *digital cash* lain selain yang telah disebutkan sebelumnya. Beberapa diantaranya melibatkan matematika yang cukup rumit. Secara umum, berbagai macam protokol *digital cash* dapat dibagi menjadi beberapa kategori, yaitu:

1. *On-line*

Dalam sistem *on-line merchant* akan berkomunikasi dengan bank setiap kali terjadi transaksi, mirip seperti protokol kartu kredit masa kini. Jika terjadi masalah maka bank tidak akan menerima transaksi dan pemilik *digital cash* tidak dapat curang.

2. *Off-line*

Dalam sistem *off-line*, yang mirip dengan protokol #4, tidak dibutuhkan komunikasi antara *merchant* dan bank sampai transaksi antara *merchant* dan *costumer* selesai. Sistem ini tidak mampu mencegah pemilik *digital cash* dari berbuat curang, tetapi sistem ini mampu mendeteksi kecurangan yang dilakukan oleh pemilik *digital cash*. Protokol #4 mendeteksi kecurangan yang dilakukan dengan mengetahui identitas pemilik *digital cash*.

3. *Observer*

Cara lain adalah dengan menciptakan *smart card* khusus yang mengandung chip anti-rusak yang disebut dengan *observer*. Chip *observer* berisi basis data mengenai bagian dari *digital cash* yang digunakan oleh *smart card*. Jika pemilik *digital cash* berniat menduplikat *digital cash* dan menggunakannya dua kali, maka *observer* yang berada dalam *smart card* akan mendeteksi menggunakan *digital cash* yang sama lebih dari satu kali dan *smart card* tidak akan mengijinkan transaksi terjadi. Karena chip *observer* bersifat anti-rusak, maka pemilik *digital cash* tidak dapat menghapus basis data tanpa merusak *smart card* secara permanen. Saat *cash* didepositkan maka bank dapat mengecek *cash* tersebut dan menentukan siapa, jika ada, yang melakukan kecurangan.

Protokol *digital cash* bisa juga dibagi berdasarkan bentuknya, yaitu:

1. *Electronic coins*

Electronic coins memiliki nilai yang tetap dan pihak yang menggunakan sistem ini akan membutuhkan beberapa koin dalam nominal yang berbeda.

2. *Electronic checks*

Electronic checks dapat digunakan dalam jumlah berapapun sampai pada suatu nilai maksimum dan kemudian dikembalikan untuk mengambil cash yang tidak digunakan.

Tatsuaki Okamoto dan Kazuo Ohta telah mendaftar enam properti mengenai sistem *digital cash* yang ideal, yaitu:

1. *Independence*. Keamanan *digital cash* tidak bergantung kepada lokasi fisik. *Cash* bisa dikirimkan melalui jaringan komputer.
2. *Security*. *Digital cash* tidak dapat diduplikat dan digunakan kembali.
3. *Privacy (untraceability).* Kerahasiaan user harus dilindungi, tidak ada siapapun bisa melacak hubungan antara user dan transaksi yang dilakukan user tersebut.
4. *Off-line payment*. Saat user membayar barang-barang yang dibelinya menggunakan *electronic cash*, protokol antara user dan *merchant* dieksekusi secara *off-lin*e. Artinya, toko tidak perlu terhubung dengan *host* untuk memproses pembayaran user.
5. *Transferability*. *Digital cash* dapat diserahterimakan kepada user lainnya.
6. *Divisibility*. Bagian dari *digital cash* dengan nilai tertentu dapat dibagi menjadi bagian yang lebih kecil dengan nilai yang lebih kecil.

Protokol-protokol yang telah dibicarakan sebelumnya memenuhi properti 1,2,3, dan 4, tetapi tidak 5 dan 6. beberapa *digital cash* dengan sistem *on-line* memenuhi semua properti kecuali properti 4.

5. Kesimpulan

Digital cash dapat menggantikan fungsi uang tunai, cek, dan kartu kredit. Lebih daripada itu, digital cash menyediakan tingkat keamanan yang lebih baik daripada tiga bentuk pembayaran lainnya, karena digital cash menghilangkan kemungkinan pelacakan transaksi oleh pihak yang tidak berwenang.

[Kesimpulan kedua adalah mekanisme kerja digital cash tentang protokolnya. Kesimpulan bisa dimulai dengan kalimat: “Mekanisme kerja digital cash tidaklah begitu rumit.” Kemudian dijelaskan dalam dua atau tiga kalimat dan ditutup dengan: Namun, semakin tinggi kebuutuhan sekuriti maka semakin rumit protokol yang dibutuhkan.]

6. Referensi

[1] Amit et. al., *Digital Cash*, a presentation in http://www.cs.bham.ac.uk/~mdr/ diakses tanggal 4 Januari 2006 pukul 09.00

[2] Miller, J., *Digital Cash Mini-FAQ*, http://ntrg.cs.tcd.ie/mepeirce/ diakses tanggal 4 Januari 2006 pukul 09.00