Cyfrowe pieniądze

Łukasz Anforowicz

31 sierpnia 2002

Streszczenie

Ten dokument zawiera opis protokołu kryptograficznego, który pozwala zastąpić papierowe pieniądze ich cyfrowymi odpowiednikami — ciągami bitów o odpowiednich własnościach. Dokument powstał jako zaliczenie wykładu Algorytmiczne Aspekty Kryptografii prowadzonego na Wydziale MIM Uniwersytetu Warszawskiego w roku akademickim 2001/2002.

1 Wprowadzenie

Na codzień mamy do czynienia z elektronicznymi transakcjami przeprowadzanymi przy użyciu kart płatniczych. Do płacenia kartą potrzebny jest specjalny terminal i współpraca on-line z centrum autoryzacji kart.

Przedstawiony poniżej protokół ma dwie cechy, które odróżniają go od płatności przy użyciu kart płatniczych:

- Przekazanie pieniędzy od kupującego do sprzedawcy może się odbywać off-line — bez udziału banku i/lub centrum autoryzacji
- Inaczej niż w przypadku kart, bank nie może stwierdzić kim jest kupujący

Bezpieczeństwo protokołu jest oparte o systemy kryptograficzne z kluczem publicznym. To gwarantuje, że banknotów nie można podrobić — tylko instytucja dysponująca kluczem prywatnym (np. bank) będzie mogła wytworzyć cyfrowy banknot.

Protokół zapewnia, że kopiowanie banknotów będzie nieskuteczne. Ponadto próba ponownego wykorzystania tego samego banknotu będzie wskazywać czy oszukuje kupujący czy sprzedawca.

2 Potrzebne algorytmy

W poniższych sekcjach są opisane podprotokoły, na których oparty jest protokół cyfrowych pieniędzy.

2.1 Ślepy podpis

Ślepy podpis służy do podpisania wiadomości bez możliwości poznania jej zawartości. Prosty przykład zastosowania to poświadczenie przez notariusza, że Alicja jest w posiadaniu pewnego dokumentu, bez ujawniania przez Alicję treści tego dokumentu.

Do generowania ślepych podpisów w poniższym algorytmie jest użyty system RSA. Notariusz ma klucz publiczny $[e, n]$, klucz prywatny $[d, n]$ natomiast wiadomość do podpisania to m. Algorytm składa się z podanych niżej kroków:

1. Alicja wybiera losową liczbę $k < n$ względnie pierwszą z n
2. Alicja *zakrywa* wiadomość m obliczając $t = m \cdot k^e \mod n$
3. Alicja przesyła liczbę t notariuszowi
4. Notariusz szyfruje t swoim kluczem prywatnym $s = t^d \mod n$
5. Notariusz przesyła liczbę s do Alicji
6. Ponieważ $s = t^d = (m \cdot k^e)^d = m^d \cdot k^{ed} = m^d \cdot k \mod n$ więc Alicja może obliczyć podpisaną wiadomość m, czyli $m^d = s \cdot k^{-1} \mod n$

Jak widać po wykonaniu powyższego algorytmu Alicja ma podpisaną wiadomość $m^d \mod n$, przy czym notariusz nie miał możliwości poznania wiadomości m.

Oczywiście notariusz musi używać innej pary kluczy dla normalnych i ślepych podpisów — inaczej Alicja mogła by mu podsunąć do ślepego podpisu wiadomość w której notariusz zrzeka się swojego majątku na rzecz Alicji.

Uwaga Z powyższego algorytmu wynika ważne ostrzeżenie, żeby *nigdy* nie podpisywać wiadomości wyglądających na losowy ciąg bitów — może się okazać, że były one przygotowane zgodnie z powyższym algorytmem.

2.2 Zobowiązanie bitowe

Zobowiązanie bitowe służy do tego, żeby Alicja mogła wybrać bit (0 lub 1), nie mogła go zmienić, a do ujawnienia jej wyboru potrzebna była jej współpraca.

Wybranie bitu:

1. Bob generuje losowy ciąg bitów R i przesyła go Alicji
2. Alicja wybiera bit b
3. Alicja losuje klucz K
4. Alicja oblicza zaszyfrowaną wiadomość $E_K(R, b)$ i przesyła ją do Boba

Odkrycie bitu:

1. Alicja przesyła klucz K Bobowi
2. Bob deszyfruje $E_K(R, b)$ i sprawdza czy otrzymał podane przez siebie R
3. Jednocześnie Bob po odszyfrowaniu $E_K(R, b)$ poznaje bit b

Bezpieczeństwo algorytmu zależy od tego czy można w rozsądnym czasie znaleźć klucz K', taki żeby $E_K(R, b) = E_{K'}(R, \not b)$.

3 Cyfrowe pieniądze

3.1 Wydawanie banknotu

Poniższe kroki służą do wydania Alicji banknotu, przez bank, w którym ma ona konto.

1. Alicja ustala kwotę y, na jaką chce otrzymać banknot
2. Alicja przygotowuje 100 wiadomości; każda wiadomość składa się z
   - kwoty y
   - losowego identyfikatora x (każda wiadomość ma inny identyfikator)
   - 100 ciągów I_j identyfikujących Alicję. I_j nie są zapisane bezpośrednio — Alicja wybiera najpierw losowy ciąg R_j oblicza $L_j = I_j \oplus R_j$ i umieszcza w wiadomości zobowiązania bitowe dla ciągów R_j i L_j
3. Alicja zakrywa każdą ze 100 wiadomości tak jak do ślepego podpisu i przekazuje je do banku
4. Bank losuje liczbę $s < 100$ i prosi Alicję o odkrycie pierwszych s wiadomości i ujawnienie ich zobowiązań bitowych.

   Ten krok służy sprawdzeniu czy Alicja nie próbuje oszukiwać np. umieszczając w różnych wiadomościach różne kwoty y
5. Bank podpisuje na ślepo s-tą wiadomość, przekazuje ją Alicji i jednocześnie zmniejsza stan konta Alicji o kwotę y
6. Alicja usuwa czynnik zakrywający wiadomość do ślepego podpisu.

Po powyższych krokach Alicja dysponuje podpisaną przez bank wiadomością zawierającą

- identyfikator banknotu — x
- kwotę na jaką opiewa banknot — y
- zobowiązanie bitowe dla pary ciągów L_j oraz R_j które ujawnione razem (ale tylko wtedy) pozwolą zidentyfikować Alicję

Powyższa wiadomość jest cyfrowym banknotem na kwotę y.

3.2 Zapłata cyfrowym banknotem

Wykonanie poniższych kroków służy Alicji do przekazania banknotu sprzedawcy i umożliwienia mu dostępu w banku do kwoty y.

1. Alicja przekazuje sprzedawcy banknot
2. Sprzedawca generuje losowy ciąg 100 bitów r_j
3. Alicja ujawnia sprzedawcy zobowiązanie bitowe dla R_j jeśli $r_j = 0$, w przeciwnym przypadku ujawnia zobowiązanie bitowe dla L_j

3.3 Złożenie banknotu w banku

Te kroki służą sprzedawcy do dostępu w banku do kwoty na którą wystawiono banknot.

1. Sprzedawca przekazuje bankowi
   - banknot cyfrowy
   - ujawnioną przez Alicję część ciągów identyfikacyjnych
2. Bank sprawdza, czy już nie został zdeponowany banknot o takim samym identyfikatorze

   Jak okaże się w następnej sekcji, jeśli banknot jest składany dwukrotnie to bank może stwierdzić czy oszukuje Alicja czy sprzedawca.
3. Jeśli nie zdeponowano jeszcze banknotu o takim identyfikatorze to bank dopisuje do konta sprzedawcy kwotę y

3.4 Ujawnienie podwójnego użycia banknotu

Jeśli podczas deponowania przez sprzedawcę banknotu, bank stwierdzi, że ten sam banknot jest wykorzystywany drugi raz, to może stwierdzić kto oszukuje — Alicja czy sprzedawca.

3.4.1 Alicja wykorzystuje banknot dwukrotnie

Podczas przekazywania banknotu drugiemu sprzedawcy Alicja musi ujawnić część identyfikujących ją ciągów. Prawdopodobieństwo, że ciągi r_j u obu sprzedawców będą takie same jest bardzo małe. Wynika z tego, że z dużym prawdopodobieństwem Alicja ujawni jednemu sprzedawcy L_j, a drugiemu odpowiadające R_j.

Po drugim złożeniu banknotu x bank jest w stanie stwierdzić tożsamość Alicji ($I_j = L_j \oplus R_J$) i oskarżyć ją o oszustwo.

3.4.2 Sprzedawca wykorzystuje banknot dwukrotnie

Sprzedawca nie może zmodyfikować banknotu, bo banknot był przy jego wydawaniu podpisany przez bank. Z tego też powodu nie może manipulować ujawnionymi przez Alicję ciągami identyfikacyjnymi — byłyby one niezgodne ze zobowiązaniami bitowymi na banknocie.

Po otrzymaniu dwóch identycznych banknotów bank wie z dużym prawdopodobieństwem, że oszukiwał sprzedawca. Sprzedawca może być niesłusznie oskarżony tylko gdy wygenerowany przez niego ciąg r_j jest taki sam jak przy poprzedniej próbie wykorzystania banknotu — jest to bardzo mało prawdopodobne.

3.5 Potencjalne słabości protokołu

Zaprezentowany protokół opiera się na solidnych teoretycznych podstawach. Jednakże realizacja tego protokołu na rzeczywistym sprzęcie niesie za sobą pewne niebezpieczeństwa (w większości wspólne dla innych protokołów kryptograficznych)

- programy realizujące protokół mogą zostać zarażone przez wirusy
- korzystanie z protokołu wymaga użycia zaufanego sprzętu
- w pewnym stopniu można podsłuchać wymianę informacji (np. przez badanie pola elektromagnetycznego generowanego przez monitor)

Pewnym rozwiązaniem powyższych problemów jest zaimplementowanie protokołu na karcie procesorowej. Jest to kosztowniejsze ale znacznie bezpieczniejsze.

W opinii autora tego dokumentu istnieją jeszcze dwa potencjalne niebezpieczeństwa związane z przedstawionym protokołem.

- prawdopodobieństwo, że Alicja oszuka bank podczas ślepego podpisu (krok 4 w sekcji 3.1) jest niewielkie (wynosi 0.01), ale niewystarczająco małe
- zawsze istnieje możliwość zdobycia kontroli nad kluczem prywatnym banku przez niepowołane osoby (np. pracowników technicznych banku)

4 Niektóre konsekwencje ewentualnego wdrożenia protokołu

Jakkolwiek pieniądze cyfrowe oferują dużo korzyści (przede wszystkim wygodę płacenia na odległość), to część konsekwencji ich wprowadzenia jest negatywna. Poniższe paragrafy opisują jak cyfrowe pieniądze mogłyby służyć światu przestępczemu.

Pełna anonimowość płatności stwarza możliwość wykorzystania cyfrowych banknotów do transakcji sprzecznych z prawem, bez obawy o wykrycie kupca.

Ponieważ banknot po zaszyfrowaniu nie jest rozróżnialny od losowego ciągu bitów, więc możliwy jest niekontrolowany, międzynarodowy transfer pieniędzy.

Przekazanie banknotu może polegać na zaszyfrowaniu go kluczem publicznym odbiorcy i opublikowaniu w prasie. To może wyeliminować newralgiczny dla porywaczy moment przekazywania okupu.

5 Bibliografia

Wszystkie przedstawione w tym dokumencie algorytmy pochodzą z książki
Mirosław Kutyłowski, Willy Strothmann — „Kryptografia”