

Электронные платежи

Лекция N 4 курса “Современные задачи криптографии”

Юрий Лифшиц
yura@logic.pdmi.ras.ru

ИТМО

Осень'2005

1 / 28

План лекции

- 1 Классификация электронных платежей
 - Требования к электронным платежам
 - Типы платежей
- 2 Криптографические ингредиенты
 - Цифровые сертификаты
 - Слепая подпись
- 3 Электронные наличные

3 / 28

“И он сделает то, что всем - малым и великим, богатым и нищим, свободным и рабам - положено будет начертание на правую руку их или на чело их, И что никому нельзя будет ни покупать, ни продавать, кроме того, кто имеет это начертание, или имя зверя, или число имени его. Здесь мудрость. Кто имеет ум, тот сочти число зверя, ибо это число человеческое; число его шестьсот шестьдесят шесть.”

Откровение святого Иоанна Богослова, глава 13

2 / 28

План лекции

- 1 Классификация электронных платежей
 - Требования к электронным платежам
 - Типы платежей
- 2 Криптографические ингредиенты
 - Цифровые сертификаты
 - Слепая подпись
- 3 Электронные наличные

4 / 28

Преимущества электронных денег

Мотивация

- Дешевизна банковских операций
- Анонимность
- Защищенность от подделки
- Возможность использования в электронном бизнесе

5 / 28

Характеристики платежных систем

Требования и характеристики платежных систем?

Безопасность

Невозможность подделки
Невозможность превысить кредит
Невозможность двойной траты
Анонимность
Аппаратная/криптографическая основа стойкости

Эффективность

Вычислительная трудоемкость
Коммуникационная сложность
Стоимость банковского обслуживания

6 / 28

Возможности платежных систем

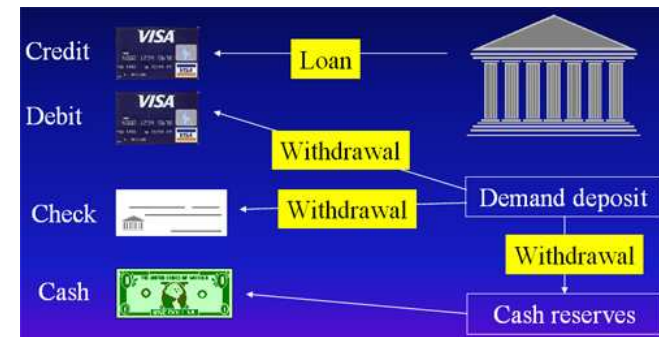
Характеристики использования платежных систем?

Возможности

Переносимость
Делимость
Универсальность
Возможность удаленной оплаты

7 / 28

Типы платежей



8 / 28

Кредитные карты

Дебетные карточки

- Кладем деньги
- Сумма хранится на карточке
- Потраченные деньги вычитаются из баланса карточки

Кредитные карточки

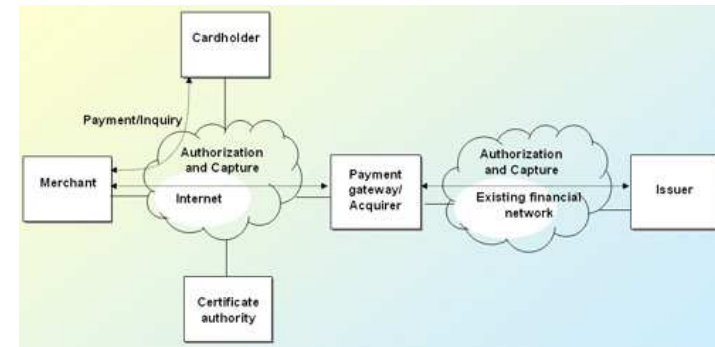
- Заводим счет в банке
- Деньги снимаются со счета

Криптографическая основа

- Протокол SET

9 / 28

Протокол SET



10 / 28

Микроплатежи

Специфика

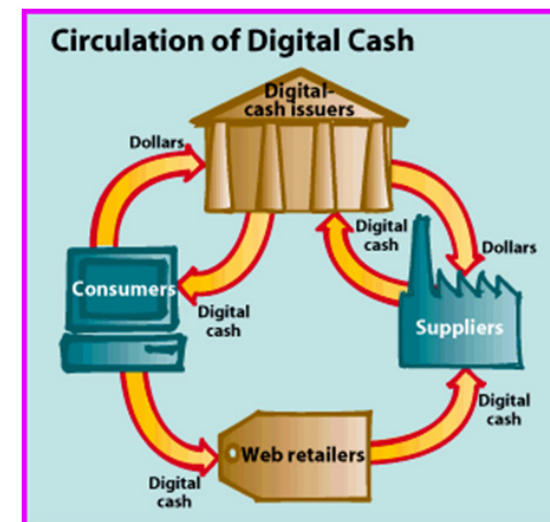
- Не требуется анонимность
- Минимизация криптографических вычислений

Современные решения

- Millicent
- Payword

11 / 28

Электронные наличные



12 / 28

Table 1: Characteristics of digital money, currency, checks, and debit cards

Characteristics	Digital money	Currency	Check	Debit card
Marginal cost per transaction	Low	Medium	High	Medium
Payment finality face-to-face transaction	Yes	Yes	No	No
Payment finality non-face-to-face transaction	Yes	No	No	No
User anonymity	Yes/No*	Yes	No	No

*Many digital money schemes are now being developed. A few of them allow users to remain anonymous.

- 1 Классификация электронных платежей
Требования к электронным платежам
Типы платежей
- 2 Криптографические ингредиенты
Цифровые сертификаты
Слепая подпись
- 3 Электронные наличные

Используемая криптография

Что используется в электронных платежах?

Аутентификация сообщений

Гарантирует целостность

Шифрование

Гарантирует секретность операций от посторонних

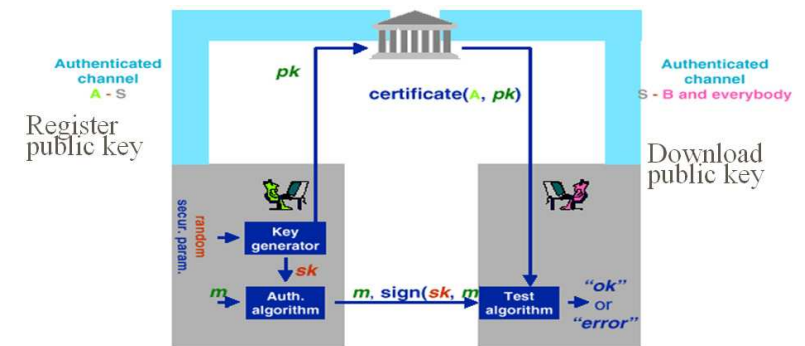
Цифровые сертификаты

Защищают от мошенников

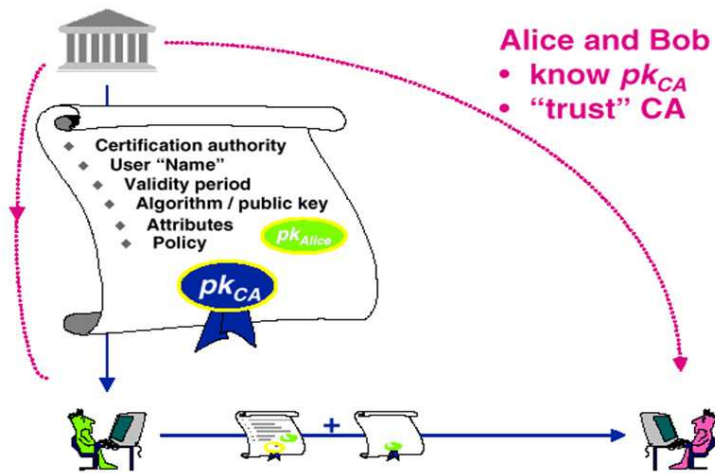
Слепая подпись

Используется для электронных наличных

Цифровые сертификаты



Цифровые сертификаты II



Протокол Шаума

Цифровая подпись RSA:

Сообщение M , секретный ключ d , открытый ключ e

Подпись: $s = M^d$

Проверка подписи: $s^e \stackrel{?}{=} M$

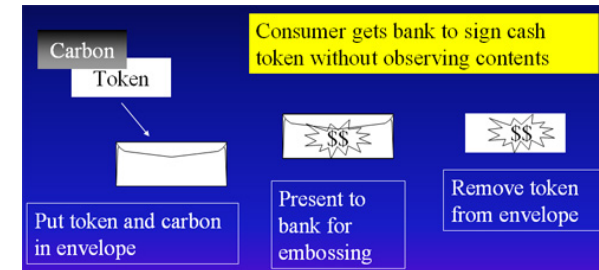
Протокол Шаума

- 1 Боб выбирает случайное r
- 2 Боб посылает Алисе $M' = M \cdot r^e$
- 3 Алиса подписывает M' и посылает $s' = M'^d \cdot r^{ed}$ Бобу
- 4 Боб получает исходную подпись $s = s' \cdot r^{-1}$

Слепая подпись

Обсуждали на прошлой лекции. Напомните смысл?

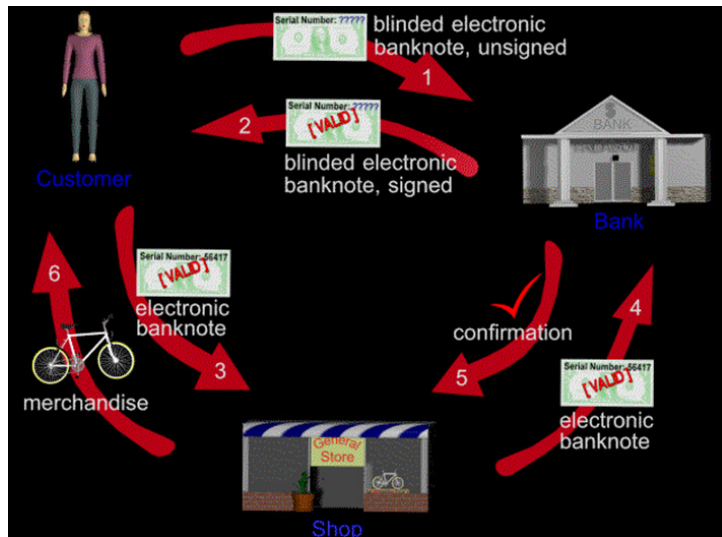
Протокол слепой подписи — протокол обмена сообщениями между Алисой и Бобом, в результате которого Боб получит подпись Алисы на нужном ему сообщении, а Алиса не узнает, что она подписала.



План лекции

- 1 Классификация электронных платежей
Требования к электронным платежам
Типы платежей
- 2 Криптографические ингредиенты
Цифровые сертификаты
Слепая подпись
- 3 Электронные наличные

Общий вид схемы



21 / 28

Наивный протокол

Обналичивание

- 1) Участник просит Банк выдать 100\$
- 2) Банк присылает счет на 100\$:
 $\{ \text{Я счет на } 100\$ \#4257 \}_{SK_B}$
- 3) Участник проверяет подпись и признает счет

Оплата

- 1) Участник посылает продавцу счет
- 2) Продавец проверяет подпись и признает счет

Получение денег

- 1) Продавец посылает счет в Банк
- 2) Банк проверяет свою подпись и переводит деньги продавцу

22 / 28

Недостатки

Какие недостатки у наивного протокола?

- 1) Можно тратить дважды
- 2) Нет анонимности

23 / 28

Построение анонимности

Обналичивание - новый вариант

- 1) Участник просит Банк выдать 100\$
- 2) Участник готовит счет:
 $\{ \text{Я счет на } 100\$ \#4257 \}$
- 3) Участник вслепую подписывает счет
- 4) Участник проверяет подпись и признает счет

Остались проблемы:

- 1) Двойной траты
- 2) Банк подпишет 1000\$ вместо 100\$

24 / 28

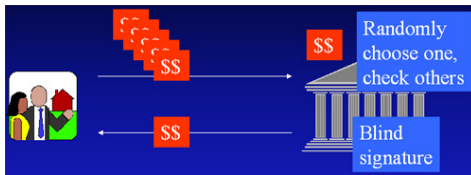
Проверка выдаваемой суммы

Выборочная проверка

- 1) Участник посылает Банку 1000 счетов
- 2) Банк проверяет (открывая) 999 и подписывает 1000-ый счет

Система ключей:

- 1) У банка есть набор секретных ключей $SK_1, SK_{10}, SK_{100}, \dots$
- 2) Каждая подпись годится только для фиксированной суммы



25 / 28

Контроль двойной траты

On-line контроль

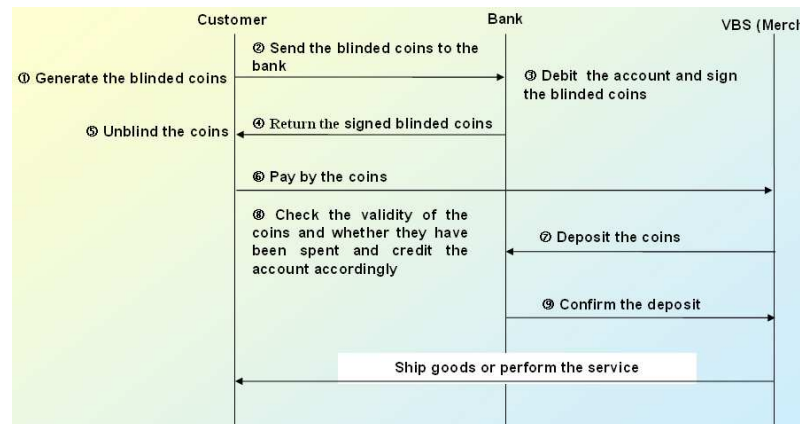
Продавец высылает запрос Банку
"Была ли уже потрачена купюра 4257?"

Off-line контроль:

- 1) Участник генерирует $x_1, \dots, x_k, y_1, \dots, y_k$ так, что $ID = x_i \oplus y_i$
- 2) Участник посылает Банку хэш-функции от этих значений
- 3) К каждой электронной купюре добавляется набор из k значений, по одному из пары по выбору Продавца
- 4) Два раза потратили \Rightarrow с вероятностью $1 - 2^{-k}$ можно установить нарушителя

26 / 28

Последовательность шагов



27 / 28

Последний слайд

Если не запомните ничего другого:

- Типы платежей: кредитные карты, электронные наличные, микроплатежи
- Электронные наличные основаны на слепой подписи
- Два метода борьбы с двойной тратой — on-line и off-line методы

Вопросы?

28 / 28