ПРОТОКОЛ ЭЛЕКТРОННОЙ ТОРГОВЛИ БЕЗ АРБИТРА

Мацук Н. А.

namatsuk@yandex.ru

Московский инженерно – физический институт (государственный университет)

Проблемы товарно – денежного обмена

Дуализм товарно – денежного обмена :

- Заинтересованность обеих сторон в совершении сделки
- Конфликт интересов продавца и покупателя

Конфликт интересов порождает проблемы :

- Одновременность обмена
- «Кот в мешке»

Проблемы товарно – денежного обмена

Дополнительные требования к платежным системам :

- ➢ Анонимность
- ➢ Неотслеживаемость платежей

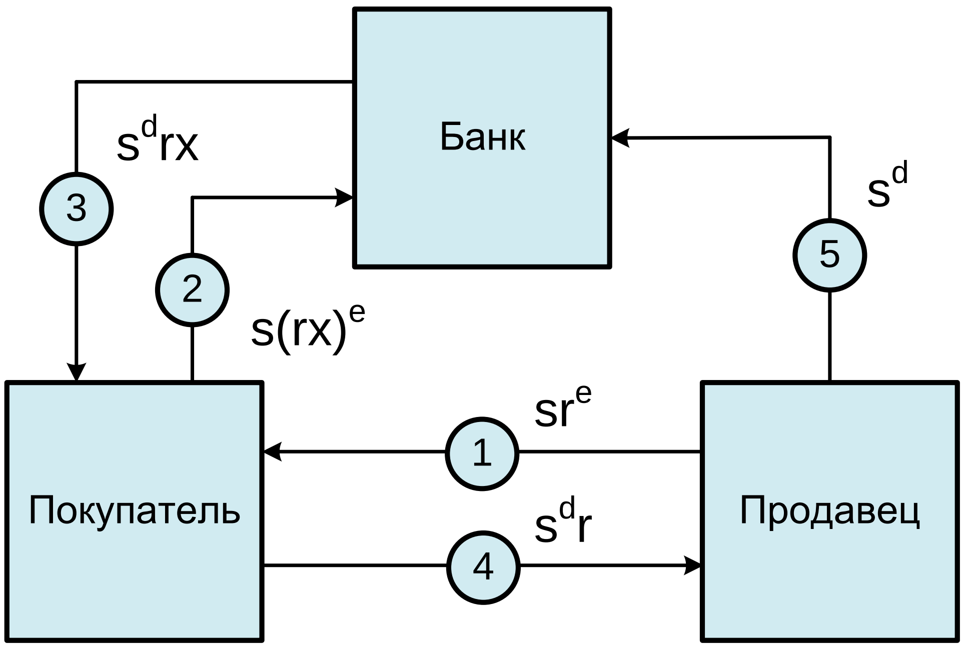
- ✓ Обеспечиваются наличными деньгами
- ✓ Не обеспечиваются прочими традиционными средствами платежа
- ✓ Обеспечиваются только одним видом электронных платежных средств

  - цифровыми деньгами

Схема обращения цифровых денег

Основные поля цифровой банкноты :

Номер счета покупателя	Номинал	Серийный номер



e - открытый ключ банка

d - секретный ключ банка

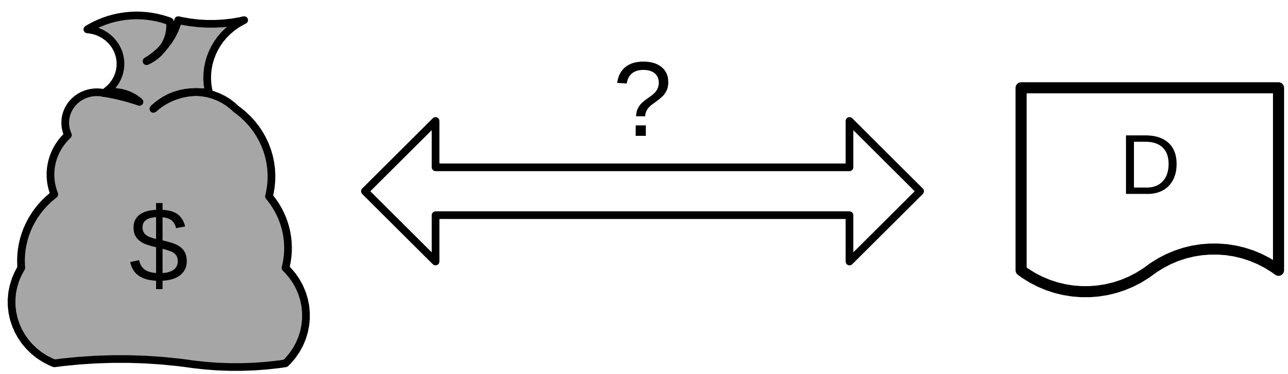
Операции выполнятся по mod n

r - затемняющий множитель продавца

x - затемняющий множитель покупателя

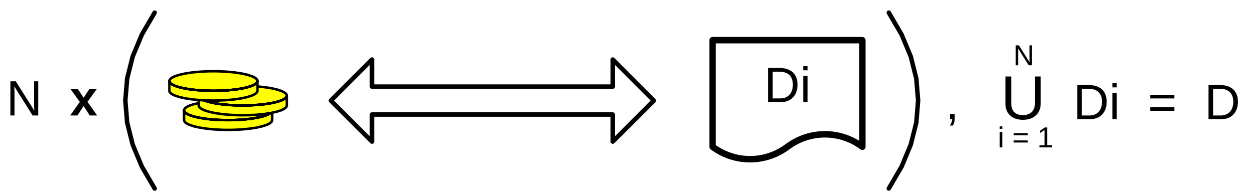
Решение проблем товарно – денежного обмена

Как сделать так, чтобы и продавец и покупатель находились в равных условиях ?

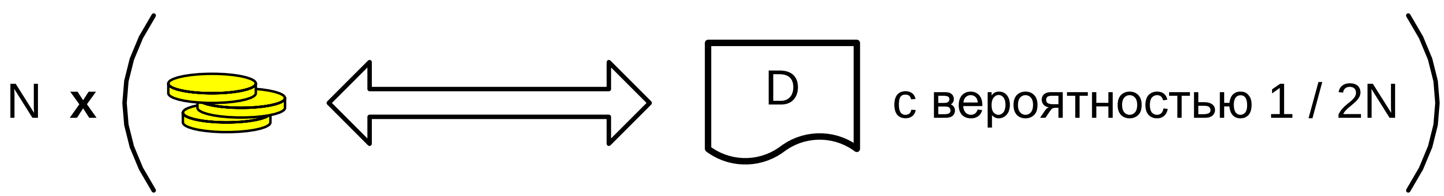


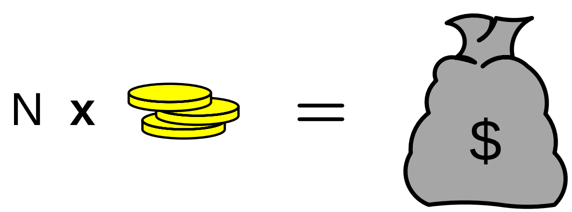
Решение проблем товарно – денежного обмена

1. Покупатель и продавец получают равную выгоду



2. Покупатель и продавец подвергаются равному риску

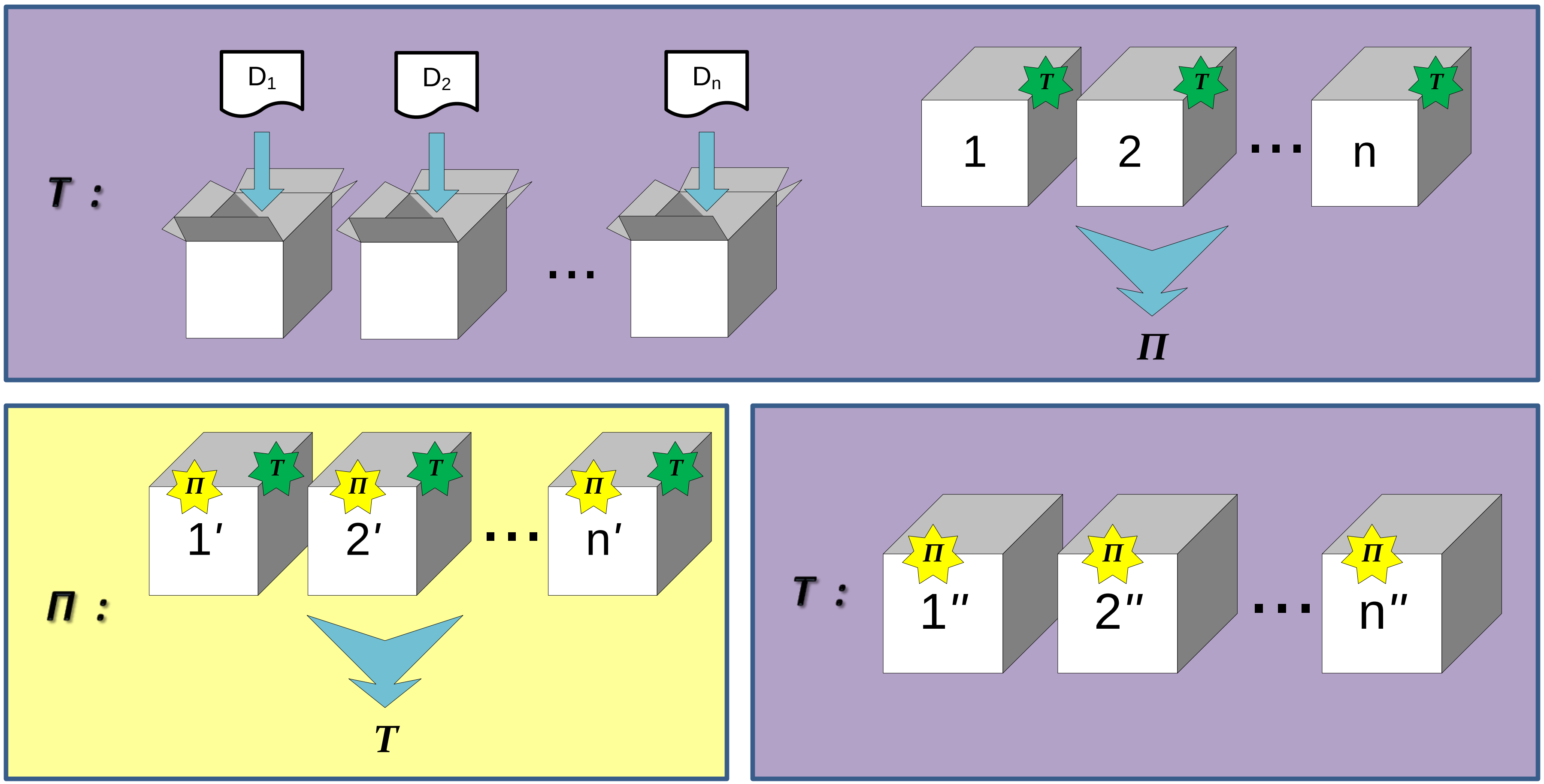




Первый вариант протокола

В протоколе принимают участие покупатель ***П*** и торговец ***Т***.

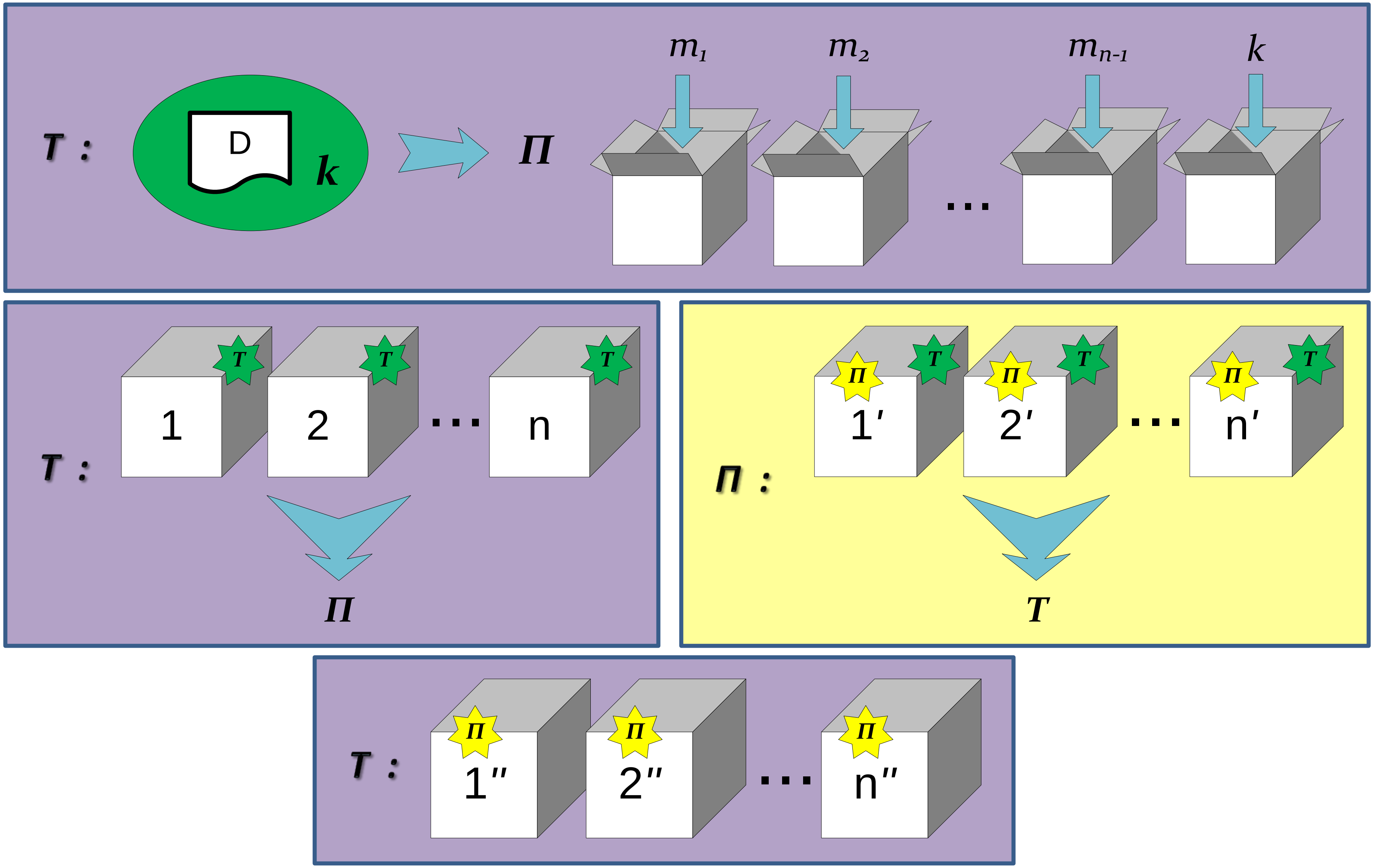
Покупатель подготавливает цифровые деньги по обычной схеме.



Первый вариант протокола

- Если *n* велико, то стоимостью одной части можно пренебречь
- Ни продавец, ни покупатель не определяют, какие части и в каком порядке выкупаются
- Если покупатель перемешал фрагменты в случайном порядке, то документ должен выкупаться равномерно
- Продавец может раскрыть несколько частей до начала торгов
- Торги могут быть прерваны в любой момент без ущерба для обоих сторон

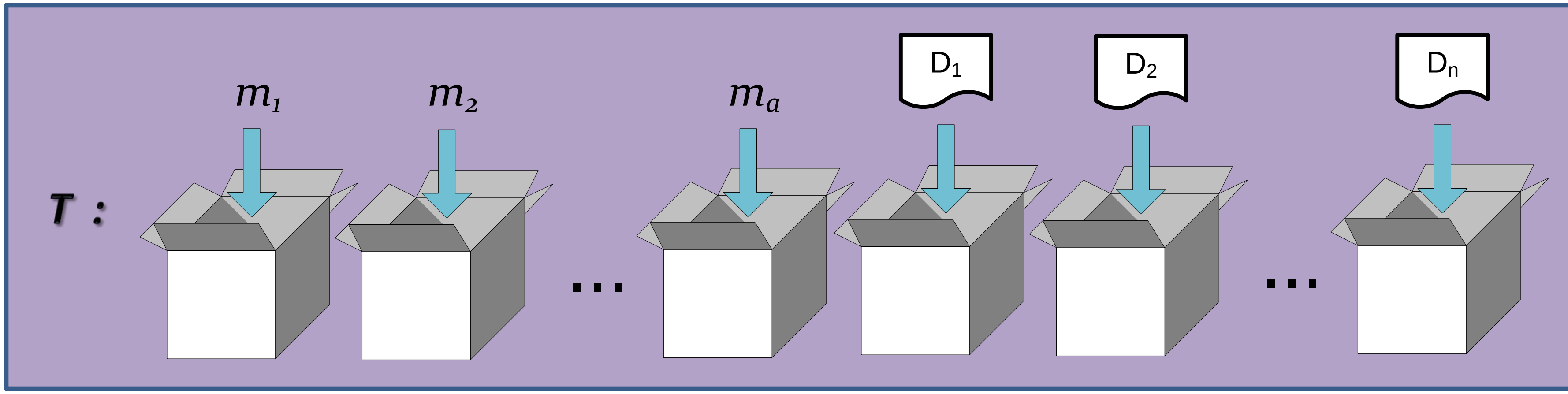
Второй вариант протокола



Второй вариант протокола

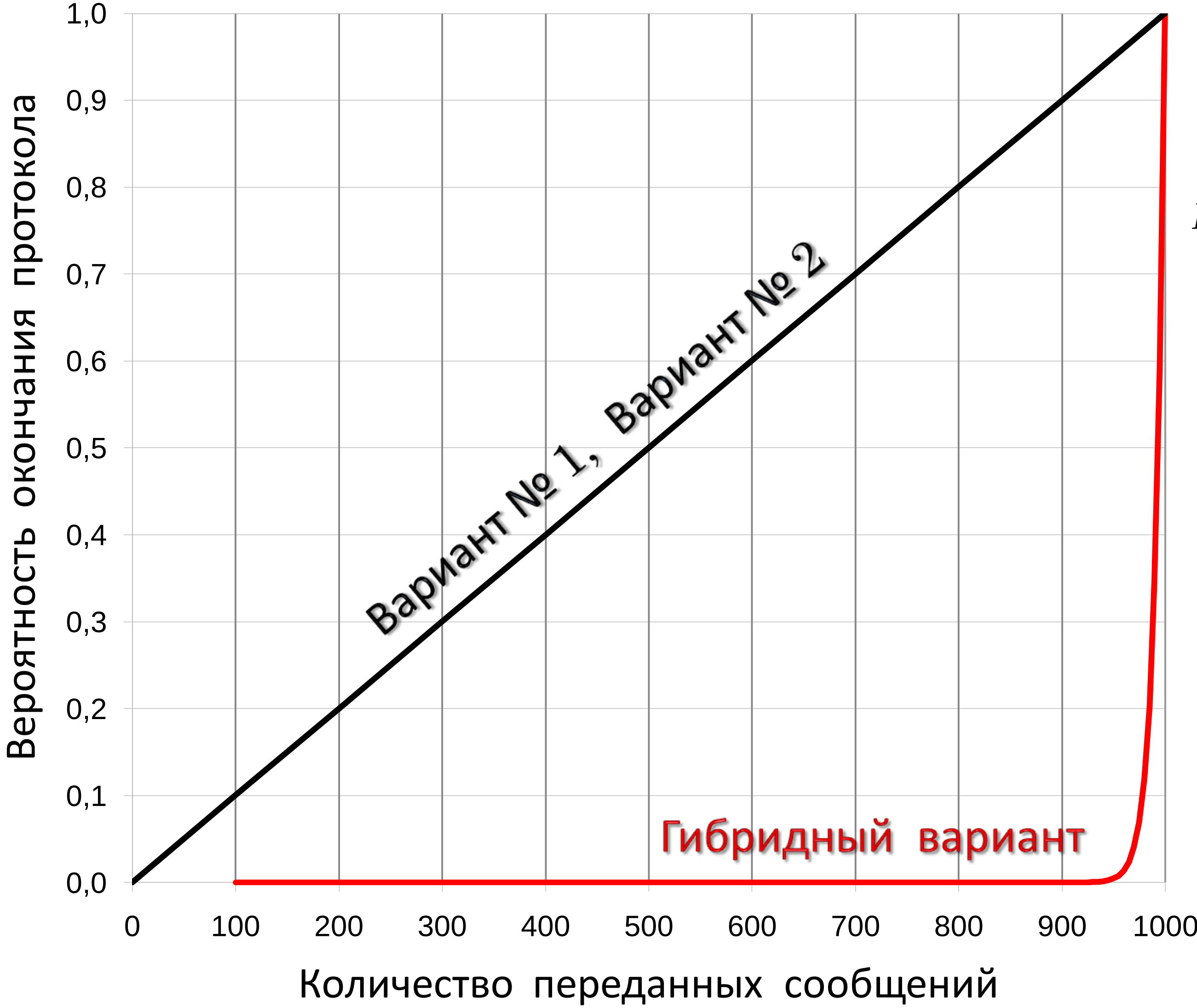
- Ни продавец, ни покупатель не могут повлиять на то, когда будет выкуплен ключевой конверт
- Покупатель может с одинаковой вероятностью как недоплатить, так и переплатить
- Покупателю выгодно участвовать в протоколе до тех пор, пока он не получит свой товар
- Если продавец попытается подменить пакеты, то покупатель обнаружит это и выйдет из протокола
- Проблема «кота в мешке» не решена

Гибридный вариант протокола



- Комбинируются сильные и слабые стороны обоих вариантов
- Прибыль продавца более предсказуема
- Мошенничество продавца выявляется намного раньше

Ожидаемое число итераций протокола



Гипергеометрическая функция :

$$P(k) = f\,(k, n, b, a+b) = \frac{C_b^k \cdot C_a^{n-k}}{C_{a+b}^n}$$

Вариант № 2 вырожден:

a = 999

b = k = 1

Гибридный вариант :

a = 900

b = 100

Ожидаемое число итераций протокола

Для завершения протокола достаточно узнать 90% секрета

Криптографическая реализация

На практике все несколько сложнее, чем в теории :

- Продавец может скомпрометировать протокол, воспользовавшись знанием сообщений m_i

- Покупатель может подменить зашифрованные сообщения их произведением и выделить ключ из первого же пакета

Существующая криптографическая реализация решает эти и некоторые другие проблемы.

Криптографическая реализация

В протоколе принимают участие покупатель ***П*** и торговец ***Т***.

Т вырабатывает пару ключей RSA (*e,d*), соответствующих модулю *n*.

П формирует a сообщений m_i.

$$T: \quad k^e mod\ n \to \Pi$$

П затемняет сообщения случайным множителем r_n, а ключ - r.

$$\Pi: \quad \begin{pmatrix} m_1^e r_n^e \ mod\ n \\ \dots \\ m_a^e r_n^e \ mod\ n \\ k^e r^e r_n^e \ mod\ n \end{pmatrix} \to T$$

Криптографическая реализация

T расшифровывает сообщения, подписывая их «вслепую». ***T*** не знает в каком из сообщений скрыт ключ *k*.

$$T: \begin{pmatrix} \cdots \\ m_i r_n \ mod\ n \\ \cdots \\ krr_n \ mod\ n \\ \cdots \end{pmatrix}, \quad i \in [1, a]$$

T зашифровывает сообщения по схеме Полига-Хеллмана. ***T*** сообщает *p* своему клиенту.

$$T: \begin{pmatrix} \cdots \\ (m_i r_n \ mod\ n)^q \ mod\ p \\ \cdots \\ (krr_n \ mod\ n)^q \ mod\ p \\ \cdots \end{pmatrix}, \quad i \in [1, a]$$

Криптографическая реализация

T производит случайное число $r_m < p$ и затемняет им каждое сообщение. Затем к массиву добавляется r_m, все сообщения перемешываются и передаются ***П***.

$$T: \begin{pmatrix} \dots \\ (m_i r_n \ mod\ n)^q r_m^q \ mod\ p \\ \dots \\ (krr_n \ mod\ n)^q r_m^q \ mod\ p \\ \dots \\ r_m \\ \dots \end{pmatrix} \to \Pi, \quad i \in [1, a]$$

П зашифровывает сообщения по схеме Полига-Хеллмана. Результаты перемешиваются и вместе с r_n отсылаются ***T***.

$$\Pi: \begin{pmatrix} \dots \\ (m_i r_n \ mod\ n)^{sq} r_m^{sq} \ mod\ p \\ \dots \\ (krr_n \ mod\ n)^{sq} r_m^{sq} \ mod\ p \\ \dots \\ r_m^s \ mod\ p \\ \dots \end{pmatrix} \to T, \quad i \in [1, a]; \quad r_n \to T$$

Криптографическая реализация

T снимает затемнение со значений, полученных им ранее, и проверяет достоверность $m_1 \ldots m_a$.

T просит ***П*** раскрыть расположение сообщения $r_m{}^s \ mod\, p$ в полученном множестве.

$$T: \begin{pmatrix} \cdots \\ (m_i r_n \ mod\ n)^{sq} r_m^{sq} \ mod\ p \\ \cdots \\ (krr_n \ mod\ n)^{sq} r_m^{sq} \ mod\ p \\ \cdots \end{pmatrix} \cdot r_m^{-sq} \ mod\ p = \begin{pmatrix} \cdots \\ (m_i r_n \ mod\ n)^{sq} mod\ p \\ \cdots \\ (krr_n \ mod\ n)^{sq} mod\ p \\ \cdots \end{pmatrix}, \quad i \in [1, a]$$

Криптографическая реализация

T находит ключ q^{-1} *mod p* и расшифровывает на этом ключе каждое сообщение. В итоге ***T*** получает массив сообщений *{ x }*, выступающих в качестве товара.

$$T: \begin{pmatrix} \cdots \\ (m_i r_n \ mod\ n)^s \ mod\ p \\ \cdots \\ (krr_n \ mod\ n)^s \ mod\ p \\ \cdots \end{pmatrix} = \begin{pmatrix} x_1 \\ \cdots \\ x_{a+1} \end{pmatrix}, \quad i \in [1, a]$$

Спасибо за внимание

Мацук Н. А.

namatsuk@yandex.ru