О формализации свойств анонимности участников и конфиденциальности транзакций

Докладчик: **Ахметзянова Лилия**, *зам. начальника отдела криптографических исследований, КриптоПро*

Бабуева Александра, *инженер-аналитик, КриптоПро*

КРИПТОПРО

CTCrypt’2020

Децентрализованная система с конфиденциальными транзакциями как криптографический протокол

Как анализировать стойкость таких протоколов?

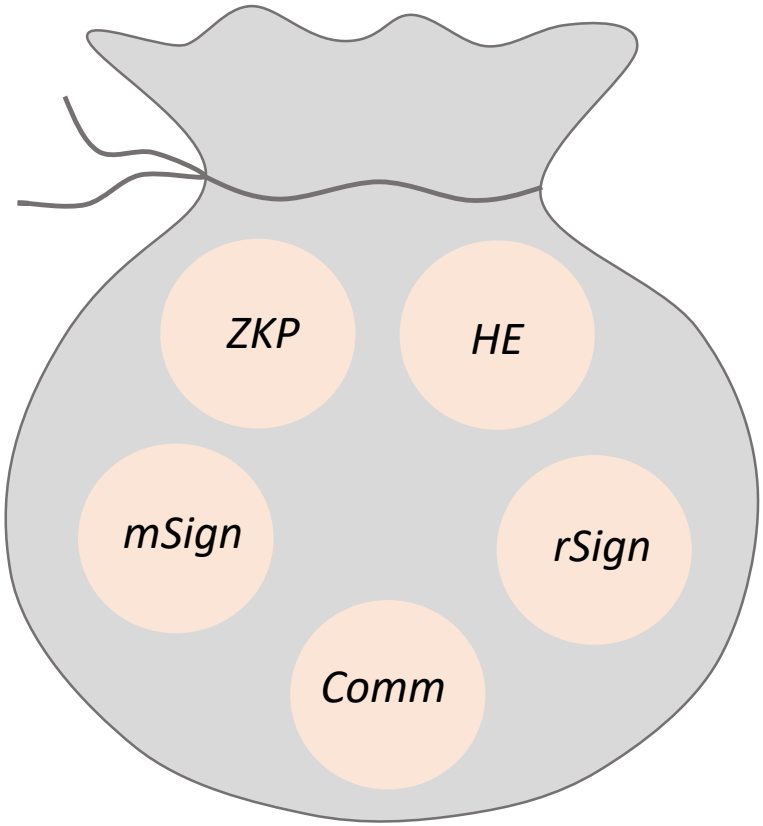
КРИПТОПРО

НЕЛЬЗЯ ПРОСТО ТАК ВЗЯТЬ

И СКАЗАТЬ, ЧТО ПРОТОКОЛ СТОЙКИЙ

КРИПТОПРО

Децентрализованная система с конфиденциальными транзакциями



Сложный протокол, включающий в себя множество базовых криптоалгоритмов

Применение методов анализа, основанных на поиске конкретных атак, не дает достаточной уверенности в стойкости

Необходимо применять другие методы

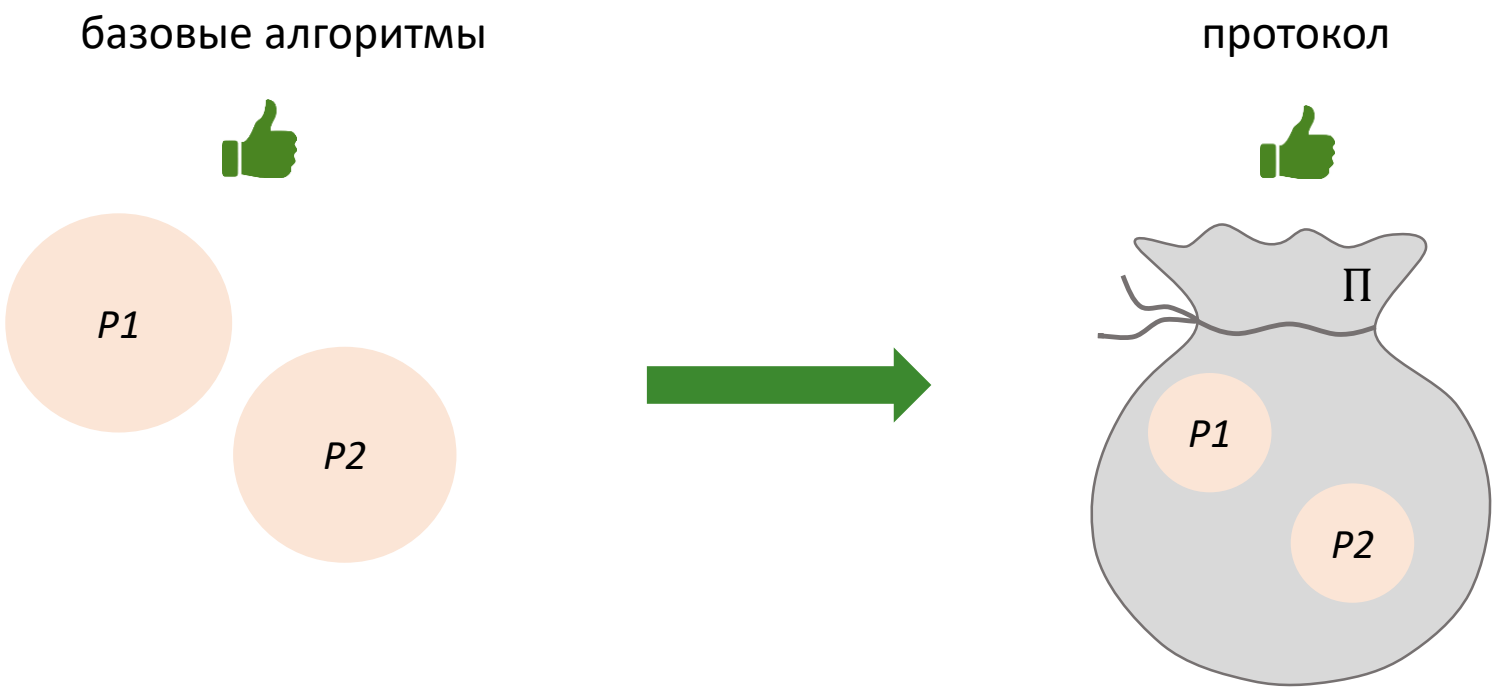
- **криптографические сведения**
- **формальные верификаторы**

КРИПТОПРО

Криптографические сведения

Основная идея:

(**Неформально**) доказать, что если базовые алгоритмы являются стойкими в некотором смысле, то и протокол, построенный на их основе, является стойким в некоторой модели противника



Криптографические сведения

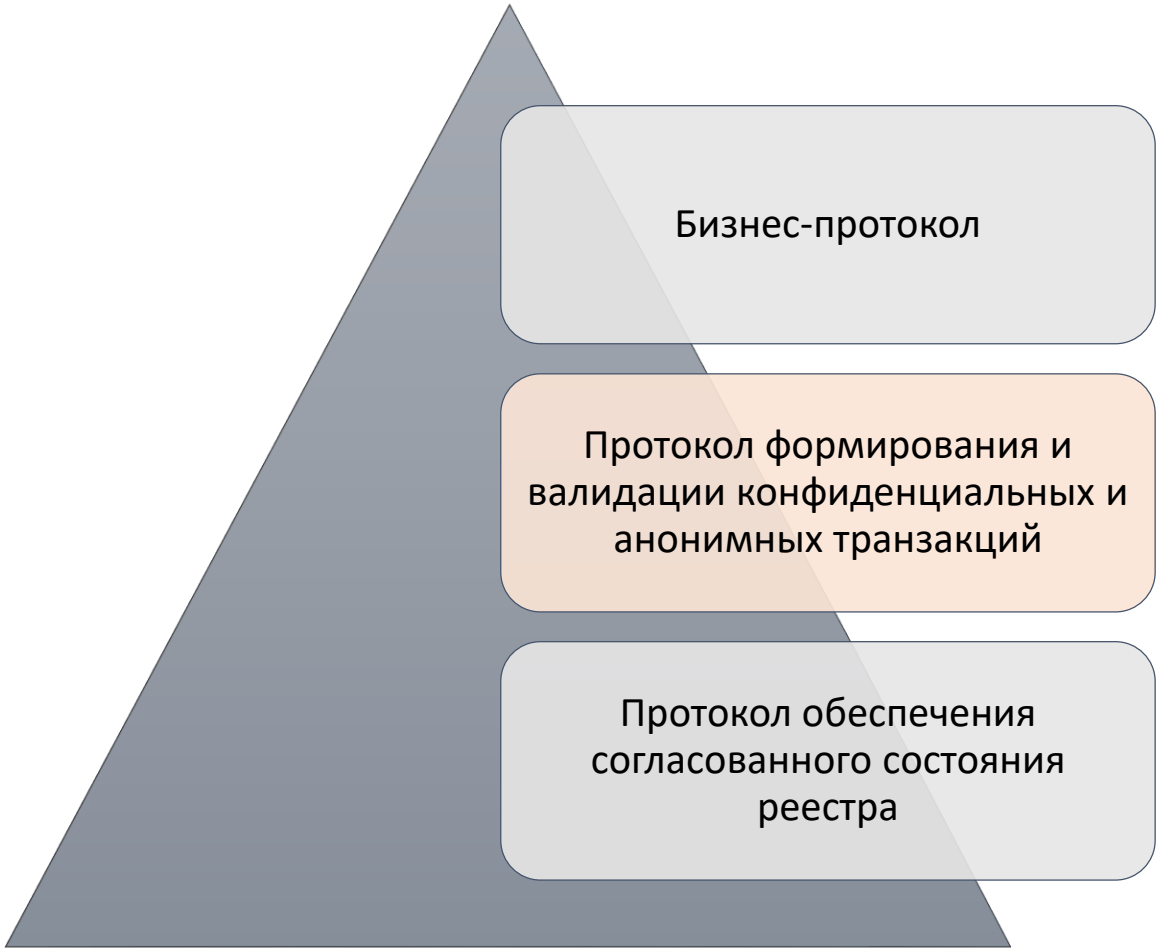
Строгие доказательства невозможны без строгой формализации исследуемых объектов

Необходимо:

- ❑ строго определить объект исследований – протокол
- ❑ сформировать формальную систему оценивания криптографических качеств протокола – модель противника

Определение объекта исследований

Определение объекта исследований



Решает конкретные бизнес-задачи

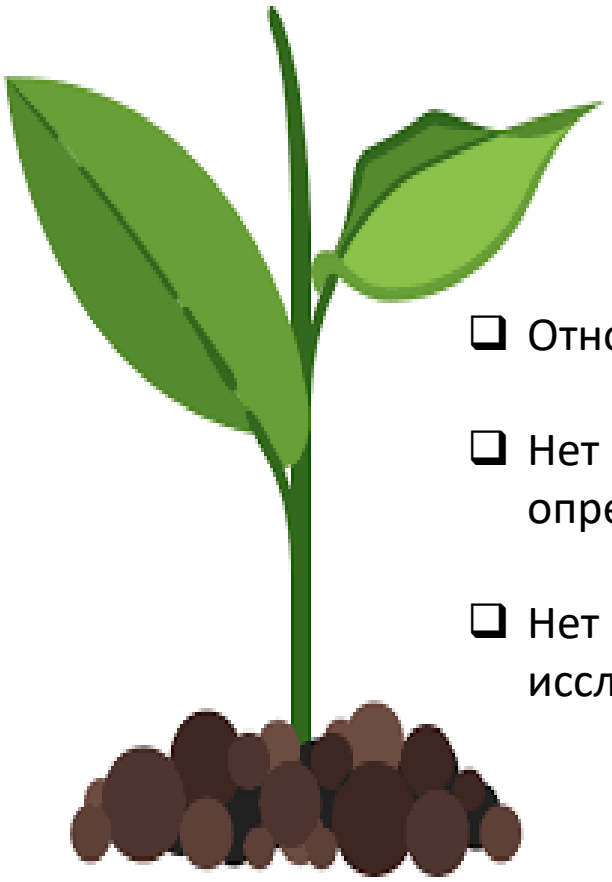
Выполняется локально на узле

Выполняется несколькими валидаторами

Децентрализованная система

КРИПТОПРО

Определение объекта исследований



- Относительно новая область исследований (2010-е — н.вр.)
- Нет устоявшегося понимания объекта исследований – не определено место протокола во всей системе
- Нет универсальных формальных определений объекта исследований

Определение объекта исследований: пример

Определение объекта исследований: пример

Aggregate Cash Systems: A Cryptographic Investigation of Mimblewimble [MOS18]

UTXO-модель (Обозначения)

$\mathbf{pp}$	открытые параметры
$\mathcal{C}_{\mathbf{pp}}, C \in \mathcal{C}_{\mathbf{pp}}$	пространство UTXO, UTXO
$\mathcal{K}_{\mathbf{pp}}, k \in \mathcal{K}_{\mathbf{pp}}$	пространство ключей UTXO, ключ UTXO
$v \in [0, v_{max}]$	количество токенов в UTXO/значение UTXO
Λ	реестр

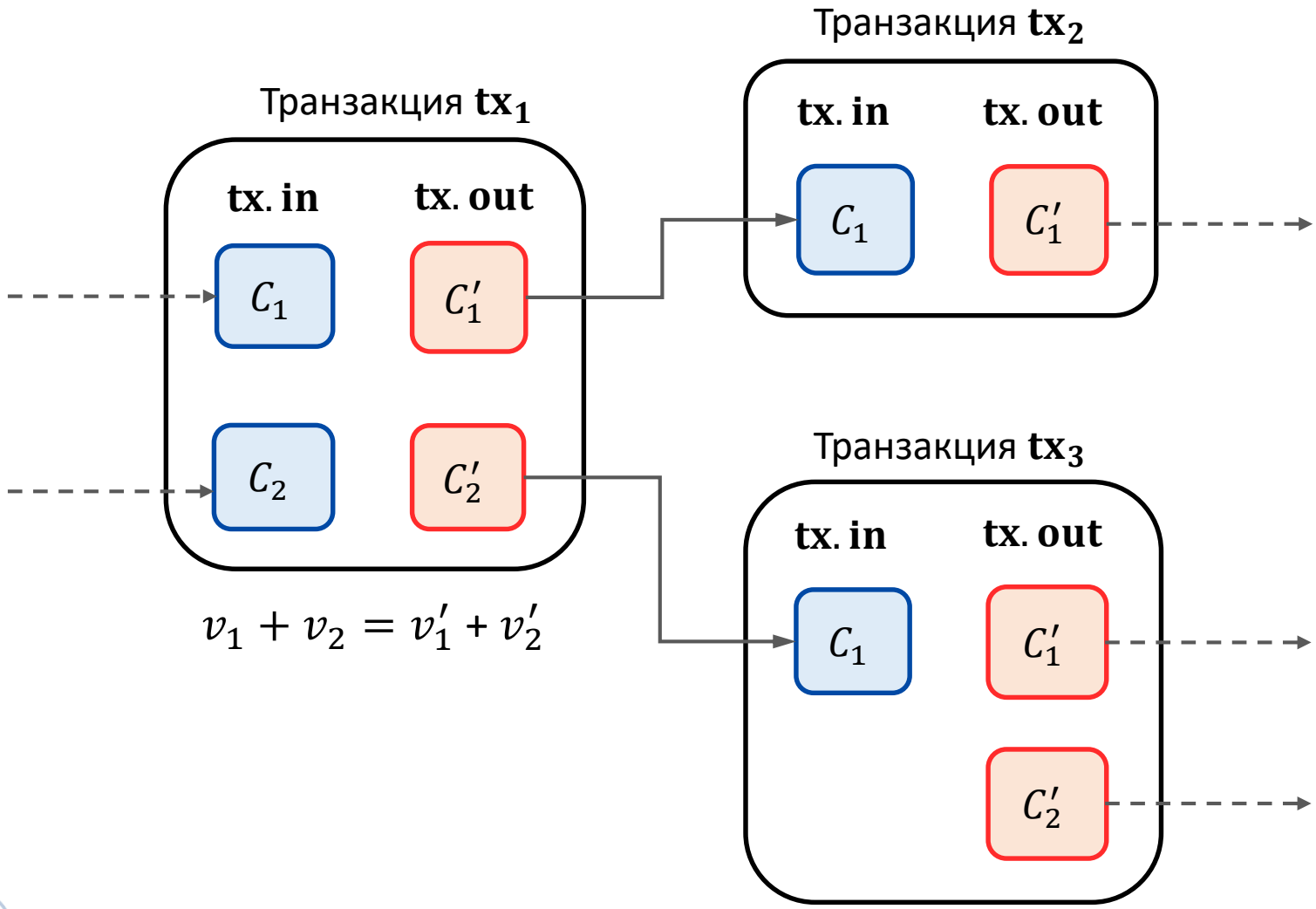
$$(v, k) \xrightarrow{f} C$$

Только тот, кто знает ключ k UTXO C, может тратить v токенов

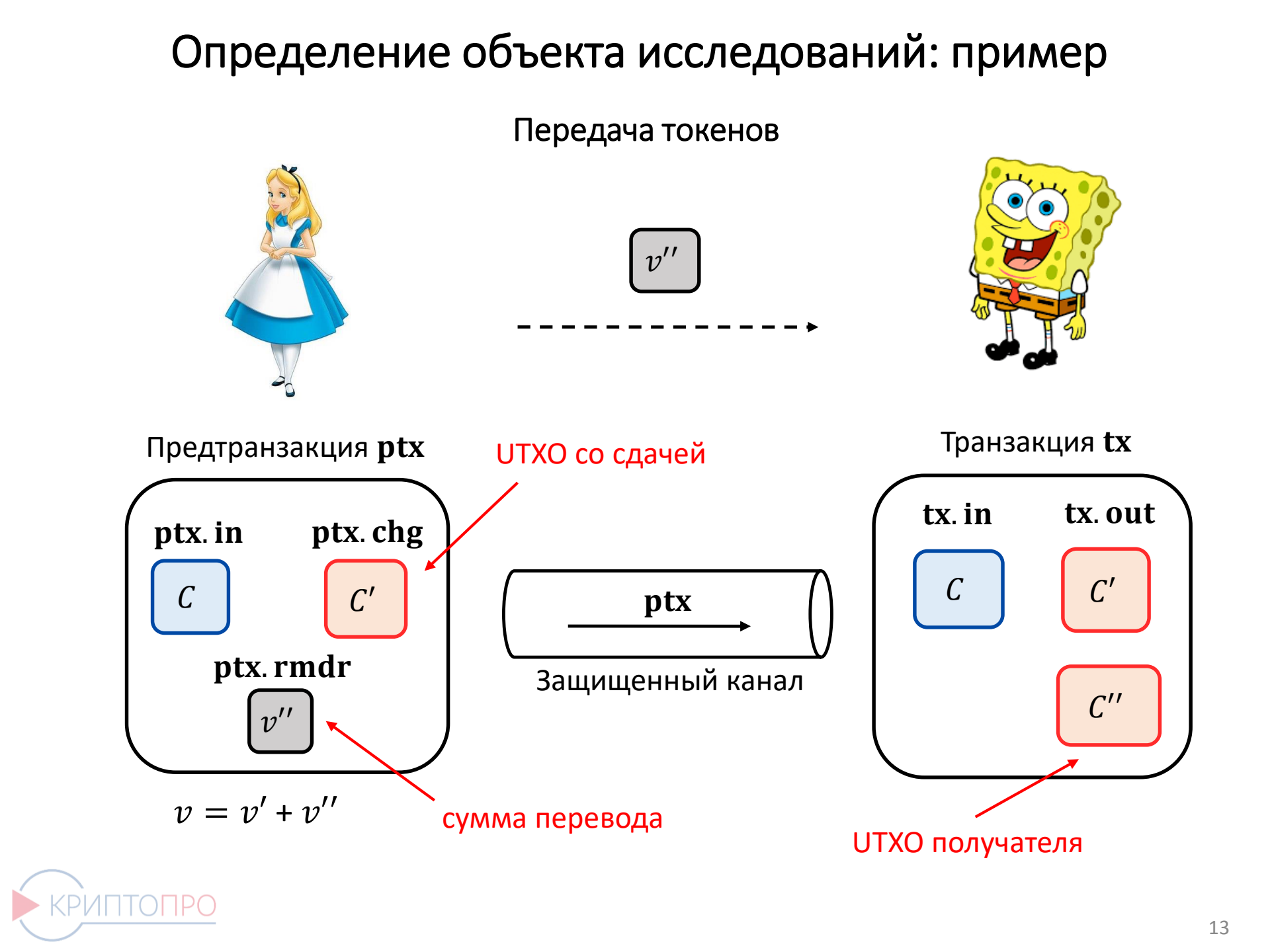
КРИПТОПРО

Определение объекта исследований: пример

Добавление транзакции в реестр



Определение объекта исследований: пример



Определение объекта исследований: пример

Децентрализованная система CASH определяется следующими алгоритмами:

$(\mathbf{pp}, \Lambda) \leftarrow \mathrm{CASH.Setup}(1^{\lambda}, v_{max})$	алгоритм инициализации системы
$(\mathbf{tx}, \mathbf{k}) \leftarrow \mathrm{CASH.Mint}(\mathbf{pp}, \mathbf{v})$	алгоритм выпуска новых токенов
$(\mathbf{ptx}, \mathbf{k}') \leftarrow \mathrm{CASH.Send}(\mathbf{pp}, (\mathbf{C}, \mathbf{v}, \mathbf{k}), \mathbf{v}')$	алгоритм формирования предтранзакции
$(\mathbf{tx}, \mathbf{k}'') \leftarrow \mathrm{CASH.Rcv}(\mathbf{pp}, \mathbf{ptx}, \mathbf{v}'')$	алгоритм формирования транзакции из предтранзакции
$\Lambda' \leftarrow \mathrm{CASH.Ldgr}(\mathbf{pp}, \Lambda, \mathbf{tx})$	алгоритм валидации и добавления транзакции в реестр

$\Lambda.\mathrm{out}$ – список всех непотраченных UTXO в системе
$\Lambda.\mathrm{sply}$ – суммарное количество токенов в системе

КРИПТОПРО

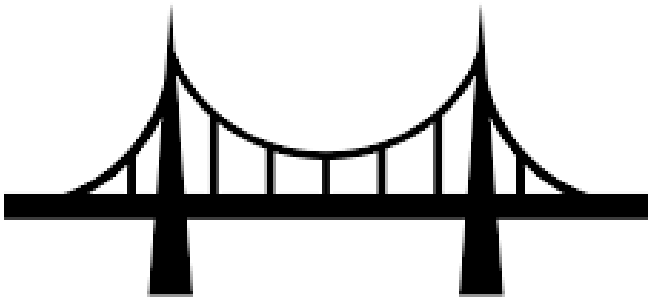
Формализация модели противника

Модель противника

релевантное моделирование

Реальность

Противник не должен узнать какую-либо конфиденциальную информацию о транзакции



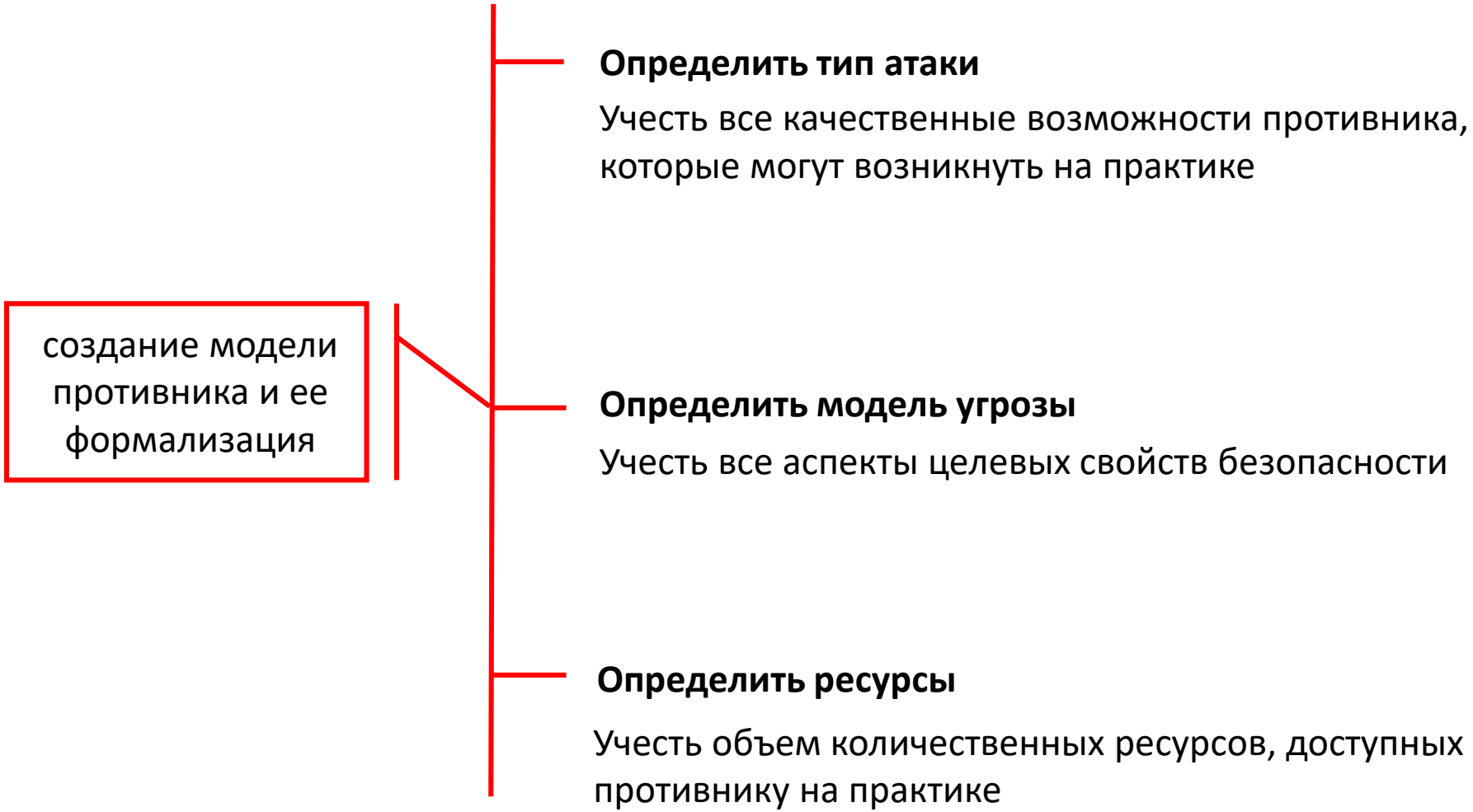
Модель

Преимущество противника в модели M должно быть пренебрежимо малым

некоторые гарантии безопасности на практике

КРИПТОПРО

Модель противника



Модель противника для децентрализованных систем с конфиденциальными транзакциями

Нет универсальных формальных определений протоколов

- Нет общих формальных моделей противника
- Соотношения между ними почти не исследованы

КРИПТОПРО

Модель противника для децентрализованных систем с конфиденциальными транзакциями

Отсутствие единой системы оценивания криптографических качеств протоколов приводит к снижению качества криптоанализа и увеличению риска использования уязвимых решений

Создание такой системы оценивания является одной из основных задач в этой области

КРИПТОПРО

Формализация модели противника: пример

Формализация модели противника: пример

Aggregate Cash Systems: A Cryptographic Investigation of … [MOS18]

Рассмотрены и формализованы три свойства безопасности:

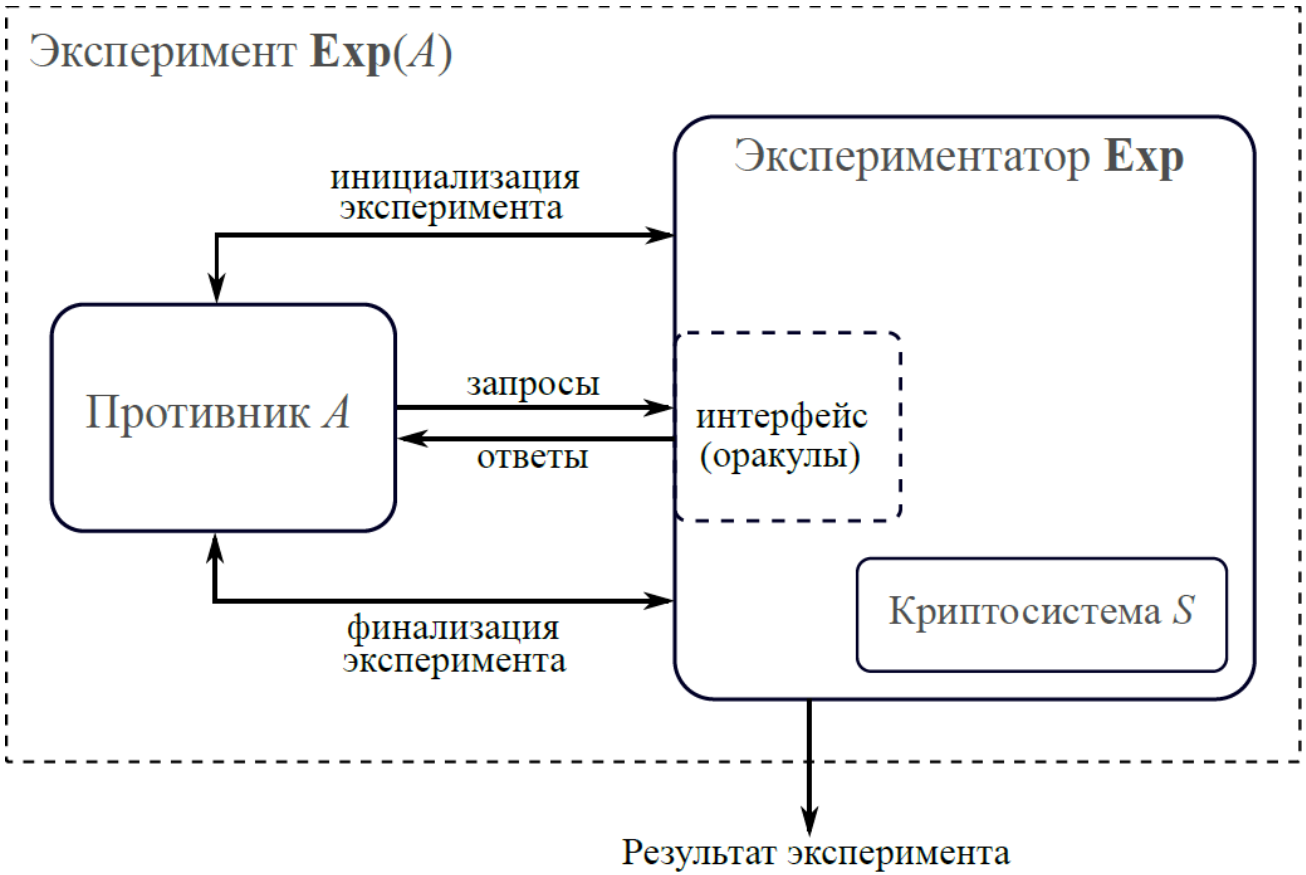
- **невозможность неполномочного создания новых токенов** – единственным способом создания токенов является транзакция выпуска;
- **невозможность неполномочного перевода токенов** – тратить токены может только легитимный обладатель соответствующего секретного ключа;
- **конфиденциальность содержимого транзакций** – количество токенов, участвующих в транзакции, должны быть известны только отправителю и получателю.

Доказано, что система Mimblewimble обеспечивает данные свойства.

КРИПТОПРО

Формализация модели противника: пример

Используется game-based подход:



Формализация модели противника: пример

Невозможность неполномочного создания новых токенов

Угроза

Неформально: противник создает денежные средства, не имея полномочий.

Формально: противник создает предтранзакцию, в которой переводимых токенов v больше, чем токенов в системе $\Lambda.\mathrm{sply}$, и соответствующая транзакция является валидной.

Формализация модели противника: пример

Невозможность неполномочного создания новых токенов

$\underline{\text{Game } \mathrm{INFL}_{\mathsf{CASH},\mathcal{A}}(\lambda, v_{\max})}$

$(\mathsf{pp}, \Lambda) \leftarrow \mathsf{CASH.Setup}(1^\lambda, v_{\max})$

$(\Lambda, \mathsf{ptx}, \mathbf{v}) \leftarrow \mathcal{A}(\mathsf{pp}, \Lambda)$

$(\mathsf{tx}, \mathbf{k}) \leftarrow \mathsf{CASH.Rcv}(\mathsf{pp}, \mathsf{ptx}, \mathbf{v})$

$\mathbf{return}\ \bot \notin \mathsf{CASH.Ldgr}(\mathsf{pp}, \Lambda, \mathsf{tx})\ \mathbf{and}\ \Lambda.\mathsf{sply} < \sum \mathbf{v}$

Definition 10 (Inflation-resistance). *We say that an aggregate cash system* CASH *is secure against inflation if for any* $v_{\max}$ *and any p.p.t. adversary* $\mathcal{A}$*,*

$$\mathsf{Adv}^{\mathrm{infl}}_{\mathsf{CASH},\mathcal{A}}(\lambda, v_{\max}) := \Pr\left[\mathrm{INFL}_{\mathsf{CASH},\mathcal{A}}(\lambda, v_{\max}) = \mathbf{true}\right] = \mathsf{negl}(\lambda)\ ,$$

КРИПТОПРО

Формализация модели противника: пример

Невозможность неполномочного перевода токенов

Угроза

Неформально: противник тратит «чужие» денежные средства.

***Формально*:** противник создает следующую ситуацию: UTXO, которые легитимный пользователь считает своими, отсутствуют в списке непотраченных UTXO всей системы $\mathcal{L}.\mathrm{out}$.

Формализация модели противника: пример

Невозможность неполномочного перевода токенов

Экспериментатор

выпусти новые токены

переведи мне токены

прими от меня токены

добавь транзакцию в реестр

Mint

Send

Rcv

Ledger

КРИПТОПРО

Формализация модели противника: пример

Невозможность неполномочного перевода токенов

Game $\text{STEAL}_{\mathsf{CASH},\mathcal{A}}(\lambda, v_{\max})$

$(\mathsf{pp}, \Lambda) \leftarrow \mathsf{CASH.Setup}(1^\lambda, v_{\max})$
$\mathsf{Hon}, \mathsf{Val}, \mathsf{Key}, \mathsf{Ptx} := ()$
$\mathcal{A}^{\text{MINT},\text{SEND},\text{RECEIVE},\text{LEDGER}}(\mathsf{pp}, \Lambda)$
return $(\mathsf{Hon} \not\subseteq \Lambda.\mathsf{out})$

Aux function $\mathsf{Store}(\mathbf{C}, \mathbf{v}, \mathbf{k})$

$\mathsf{Val}(\mathbf{C}) := \mathbf{v}$; $\mathsf{Key}(\mathbf{C}) := \mathbf{k}$

Oracle $\text{MINT}(\mathbf{v})$

$(\mathsf{tx}, \mathbf{k}) \leftarrow \mathsf{CASH.Mint}(\mathsf{pp}, \mathbf{v})$
$\Lambda \leftarrow \mathsf{CASH.Ldgr}(\mathsf{pp}, \Lambda, \mathsf{tx})$
$\mathsf{Hon} := \mathsf{Hon} \,\|\, \mathsf{tx.out}$
$\mathsf{Store}(\mathsf{tx.out}, \mathbf{v}, \mathbf{k})$
return tx

Oracle $\text{SEND}(\mathbf{C}, \mathbf{v}')$

if $\mathbf{C} \not\subseteq \mathsf{Hon}$ **or** $\bigcup_{\mathsf{ptx} \in \mathsf{Ptx}} \mathsf{ptx.in} \cap \mathbf{C} \neq ()$
  return $\perp$ // only honest coins never sent can be queried
$(\mathsf{ptx}, \mathbf{k}') \leftarrow \mathsf{CASH.Send}(\mathsf{pp}, \mathbf{C}, \mathsf{Val}(\mathbf{C}), \mathsf{Key}(\mathbf{C}), \mathbf{v}')$
$\mathsf{Store}(\mathsf{ptx.chg}, \mathbf{v}', \mathbf{k}')$; $\mathsf{Ptx} := \mathsf{Ptx} \,\|\, (\mathsf{ptx})$
return ptx

Oracle $\text{RECEIVE}(\mathsf{ptx}, \mathbf{v})$

$(\mathsf{tx}, \mathbf{k}) \leftarrow \mathsf{CASH.Rcv}(\mathsf{pp}, \mathsf{ptx}, \mathbf{v})$
$\Lambda' \leftarrow \text{LEDGER}(\mathsf{tx})$ // updates Hon
if $\Lambda' = \perp$ **then return** $\perp$
$\mathsf{Hon} := \mathsf{Hon} \,\|\, (\mathsf{tx.out} - \mathsf{ptx.chg})$
$\mathsf{Store}(\mathsf{tx.out} - \mathsf{ptx.chg}, \mathbf{v}, \mathbf{k})$
return tx

Oracle $\text{LEDGER}(\mathsf{tx})$

$\Lambda' \leftarrow \mathsf{CASH.Ldgr}(\mathsf{pp}, \Lambda, \mathsf{tx})$
if $\Lambda' = \perp$ **then return** $\perp$ **else** $\Lambda := \Lambda'$
for all $\mathsf{ptx} \in \mathsf{Ptx}$ **do**
  if $\mathsf{ptx.chg} \subseteq \mathsf{tx.out}$
  // if all change of ptx now in ledger
    $\mathsf{Ptx} := \mathsf{Ptx} - (\mathsf{ptx})$
    $\mathsf{Hon} := (\mathsf{Hon} - \mathsf{ptx.in}) \,\|\, \mathsf{ptx.chg}$
    // consider input of ptx consumed
return Λ

Definition 11 (Theft-resistance). *We say that an aggregate cash system* CASH *is* secure against coin theft *if for any* $v_{\max}$ *and any p.p.t. adversary* $\mathcal{A}$,

$$\mathsf{Adv}^{\text{steal}}_{\mathsf{CASH},\mathcal{A}}(\lambda, v_{\max}) := \Pr\left[\text{STEAL}_{\mathsf{CASH},\mathcal{A}}(\lambda, v_{\max}) = \mathbf{true}\right] = \mathsf{negl}(\lambda) \ ,$$

Формализация модели противника: пример

Конфиденциальность содержимого транзакций

Угроза

Неформально: противнику стало известно сколько денежных средства было переведено.

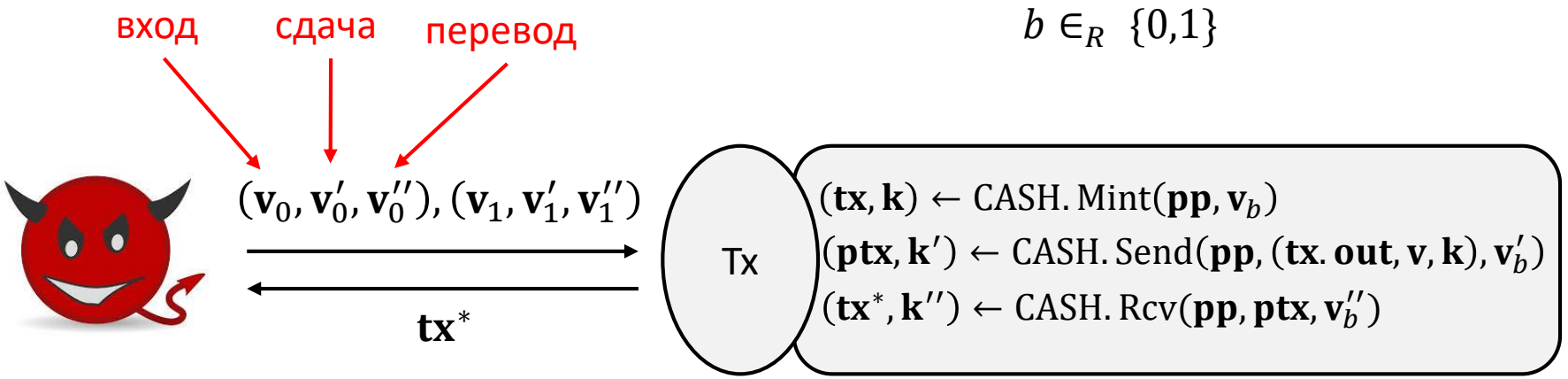
***Формально*:** противник успешно решает следующую задачу различения.

Формализация модели противника: пример

Конфиденциальность содержимого транзакций

Экспериментатор

$b \in_R \{0,1\}$



Задача противника понять, какому набору соответствует транзакция $\mathbf{tx}^*$

Сокрытие количества UTXO в транзакции (**in, out**) не обеспечивается. Является ли данный аспект нарушением конфиденциальности?

КРИПТОПРО

Формализация модели противника: пример

Конфиденциальность содержимого транзакций

Game $\text{IND-TX}_{\mathsf{CASH},\mathcal{A}}(\lambda, v_{\max})$

$b \leftarrow\$ \{0,1\}$
$(\mathsf{pp}, \Lambda) \leftarrow \mathsf{Setup}(1^\lambda, v_{\max})$
$b' \leftarrow \mathcal{A}^{\mathrm{Tx}}(\mathsf{pp})$
return $b = b'$

Oracle $\mathrm{Tx}((\mathbf{v}_0, \mathbf{v}'_0, \mathbf{v}''_0), (\mathbf{v}_1, \mathbf{v}'_1, \mathbf{v}''_1))$

if not $(\mathbf{v}_0, \mathbf{v}'_0, \mathbf{v}''_0, \mathbf{v}_1, \mathbf{v}'_1, \mathbf{v}''_1 \in [0, v_{\max}]^*)$
  return $\bot$
if $|\mathbf{v}_0| \neq |\mathbf{v}_1|$ **or** $|\mathbf{v}'_0| + |\mathbf{v}''_0| \neq |\mathbf{v}'_1| + |\mathbf{v}''_1|$
  return $\bot$ // as number of coins is not hidden
if $\sum \mathbf{v}_0 \neq \sum(\mathbf{v}'_0 \,\|\, \mathbf{v}''_0)$ **or** $\sum \mathbf{v}_1 \neq \sum(\mathbf{v}'_1 \,\|\, \mathbf{v}''_1)$
  return $\bot$ // as transactions must be balanced
$(\mathsf{tx}, \mathbf{k}) \leftarrow \mathsf{Mint}(\mathsf{pp}, \mathbf{v}_b)$
$(\mathsf{ptx}, \mathbf{k}') \leftarrow \mathsf{Send}(\mathsf{pp}, (\mathsf{tx.out}, \mathbf{v}_b, \mathbf{k}), \mathbf{v}'_b)$
$(\mathsf{tx}^*, \mathbf{k}'') \leftarrow \mathsf{Rcv}(\mathsf{pp}, \mathsf{ptx}, \mathbf{v}''_b)$
return tx^*

Definition 12 (Transaction indistinguishability). *We say that an aggregate cash system* CASH *is* transaction-indistinguishable *if for any* $v_{\max}$ *and any p.p.t. adversary* $\mathcal{A}$*,*

$$\mathsf{Adv}^{\text{tx-ind}}_{\mathsf{CASH},\mathcal{A}}(\lambda, v_{\max}) := 2 \cdot \left| \Pr\left[\text{TX-IND}_{\mathsf{CASH},\mathcal{A}}(\lambda, v_{\max}) = \mathbf{true}\right] - \tfrac{1}{2} \right| = \mathsf{negl}(\lambda) \ ,$$

КРИПТОПРО

Формализация модели противника: пример

А что с анонимностью?

Отсутствие в Mimblewimble каких-либо идентификаторов в транзакциях могут сформировать ощущение, что анонимность обеспечивается by design (в отличие от account-based модели).

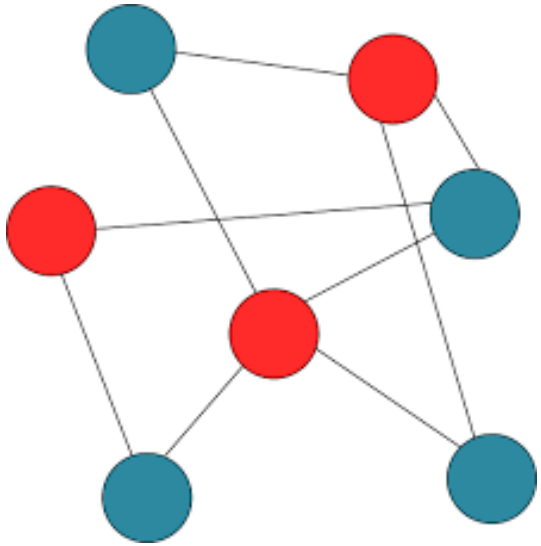
В работе не приведены никакие формальные модели, анонимность протокола строго не исследовалась.

Формализация модели противника: пример

А что с анонимностью?

Однако недавние результаты показали, что анонимность в протоколе все-таки может нарушаться.

https://medium.com/dragonfly-research/breaking-mimblewimble-privacy-model-84bcd67bfe52



Открытые задачи

- Систематизация существующих моделей противника для различных типов систем и выявление соотношений между ними
- Анализ существующих моделей на предмет их релевантности
- Разработка/расширение моделей противника и их формализация

КРИПТОПРО

Спасибо за внимание!

Вопросы?

lah@cryptopro.ru
babueva@cryptopro.ru