Распределенные реестры и криптометоды. Регистрация фактов доступа к данным

Писковский Виктор Олегович

План

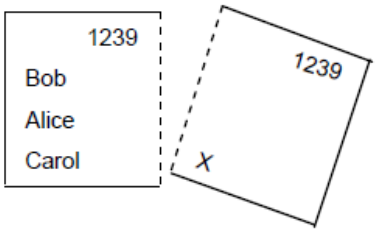
1. История вопроса
2. Цели и задачи
3. Требования
4. Распределенные реестры
5. Криптометоды:
   - доказательство с «нулевым» знанием
   - пороговая подпись
   - гомоморфное шифрование

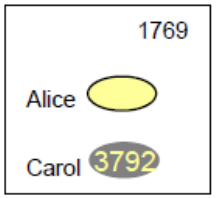
История вопроса

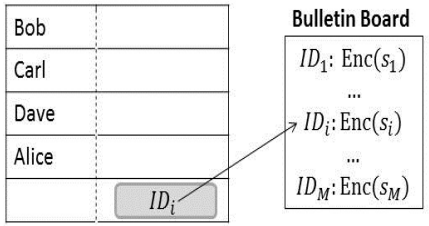
Требования к системе электронного голосования

- Децентрализация хранения и учета
- Невозможность обоснованного подтверждения выбора
- Невозможность локального контроля выборами
- Проверка корректности учёта голосов
- Производительность
- Традиционные требования к ИС

История вопроса







Pret a Voter with re-encryption mixes. P Y A Ryan and S A Schneider
January 2006 Conference: Computer Security - ESORICS 2006, 11th European Symposium on Research in Computer Security, Hamburg, Germany, September 18-20, 2006, Proceedings
https://www.researchgate.net/publication/220270823_Pret_a_Voter_with_Re-encryption_Mixes
Efficient Zero-Knowledge Argument for Correctness of a Shuffle, Stephanie Bayer and Jens Groth, University College London, D. Pointcheval and T. Johansson (Eds.): EUROCRYPT 2012, LNCS 7237, pp. 263–280, 2012. International Association for Cryptologic Research 2012

Схема голосования Бенало

С криптосистемой, гомоморфной относительно сложения:

- Передача участникам открытого ключа системы
- Шифрование данных бюллетеня и отправка выборным представителям
- Агрегация зашифрованных данных без доступа к данным и передача в центр
- Финальная агрегация без доступа к данным и дешифрование полученных результатов

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.760.213&rep=rep1&type=pdf
STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System, Josh Benaloh (Microsoft Research) and others, arXiv:1211.1904v1 [cs.CR] 8 Nov 2012

Регистрация фактов доступа к данным. Цели и задачи

Цель:

Защита от незаконных методов сбора информации

Задачи:

- Регистрация субъектов, осуществивших доступ к информации
- Предоставление услуг по получению исчерпывающей и достоверной информации о том, кто, когда и в какой мере осуществлял доступ к данным

Требования к системе

- Регистрация фактов доступа
- Идентификация субъекта, осуществившего доступ к данным, время, система, место доступа
- Публичность ресурса
- Невозможность локального контроля хранения и учета (децентрализация хранения и учета)
- Обоснованное подтверждение только комиссионно
- Проверка корректности регистрации
- Производительность
- Традиционные требования к ИС

Привлекаемые технологии

Технология	Назначение
Технология распределенных реестров	Невозможность локального контроля хранения и учета (децентрализация хранения и учета)
Доказательство с нулевым разглашением	Возможность подтвердить наличие факта, но не допустить возможности получить содержимое
Конфиденциальное вычисление	Интерактивное вычисления без предоставления к данным источников
Гомоморфное шифрование	Облачные вычисления без знания содержимого
Распределённая схема подписи	Независимость участников при постановке подписи, не интерактивный, асинхронный протокол выдачи проекций секретного ключа, не требует участия дилера. Для проверки достаточно наличия, порогового количества подписантов

Распределенные реестры

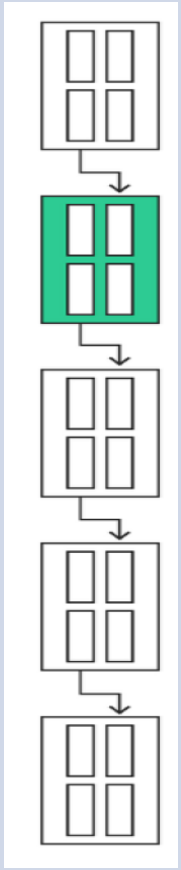
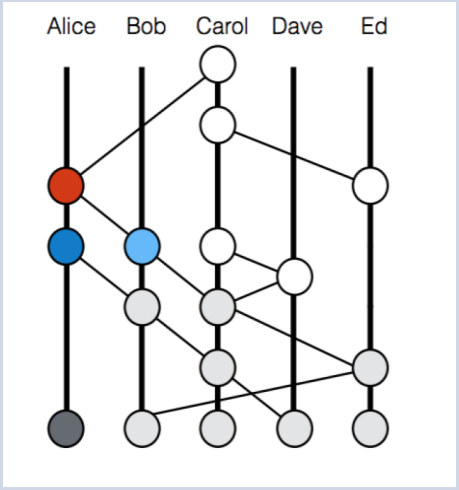
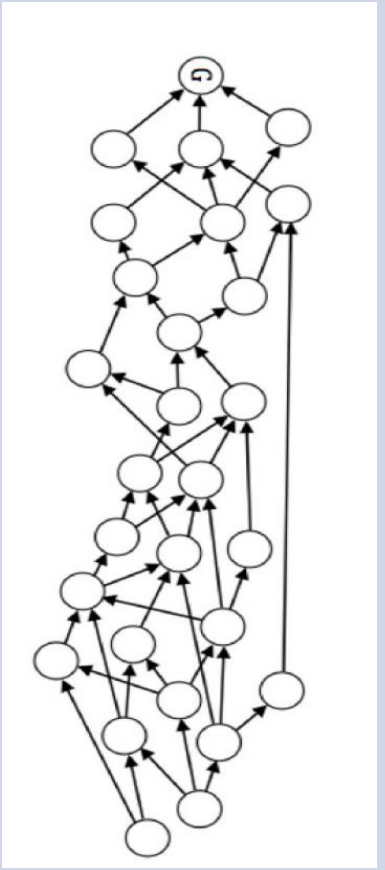
№	Модель DLT	Протокол достижения консенсуса	Производительность (TPS)	Примечание
1	BlockChain	Proof of Work (PoW)	10	Регулируется соглашением
2		Proof of Storage (PoSt)	100-200	
3		Proof of Stake (PoS)	100-200	
4		Byzantine Fault Tolerance (BFT)	1 тыс	Отдельные решения до 1 млн
5	HashGraph	Asynchronous BFT (ABFT)	250 - 350 тыс.	SWIFT-VISA (50 тыс. TPS)
6	DAG	BlockDAG/TxDAG	> 1 млн	
7	Holochain	Proof-of-Service	неограничена	Ceptr, LLC Определение распределенных систем

https://holochain.org
https://hbarprice.com/hashgraph-vs-holochain/
https://ceptr.org

Модель DLT

Технология	Модель DLT	Комментарий
Связный список	Blockchain	Связный список вытянутых в цепочку блоков, связанных соотношением один к одному
Направленный ациклический граф	HashGraph	Каждый узел хранит свою историю "событий“. Протокол "слухов" (gossip protocol)
	blockDAG	Каждая вершина содержит набор транзакций (аналог блока). Каждый блок хеш-ориентирован на несколько родительских блоков
	txDAG	Каждая вершина содержит уникальную транзакцию. Ветви содержат непересекающиеся транзакции
	Holochain	Распределенные «git-архивы», объединяемые с помощью BitTorrent-подобной технологии распределенной таблицы хешей (DHT). Протокол "слухов" (gossip protocol)

Модели DLT

Blockchain	Hashgraph	DAG
		

https://cryptor.net/kriptovalyuty/different-types-of-dlts

Доказательство с нулевым разглашением

1. Полнота. Если доказывающий знает утверждение, то он сможет убедить в этом проверяющего.
2. Корректность. Если доказывающий не знает утверждение, то он может обмануть проверяющего только с пренебрежимо малой вероятности.
3. Нулевое разглашение. Проверяющий, даже если он ведет себя нечестно, не узнает ничего кроме самого факта, что утверждение известно доказывающему

Доказательство с нулевым разглашением. Протокол Фиата-Шамира

$n = p \bullet q, s \in [1, n-1], НОД\ (s, n) = 1$

$v = s^2 \bmod(n)$

$s - ?$

N

Верификация:

1. Алиса: $r \in [1, n-1], x = r^2 \bmod(n)$, где *r - не повторяется (!)*
2. Боб: выбирает случайный бит e (0 или 1)
3. Алиса: вычисляет $y = r \bullet s^e \bmod(n)$
4. Боб: $F(y^2 \equiv x \bullet v^e \bmod(n))$

- Алиса знает секрет: $F = True$
- Алисе не знает секрет: $y = \frac{r^2}{v} \bmod(n) : e = 0 \rightarrow True\ ; e = 1 \rightarrow ?.$

$$P_{True} = O(\frac{1}{2^N})$$

Конфиденциальное вычисление

Требования: конфиденциальность, корректность, изоляция (гарантия, отсутствие возможности помешать другим участников получить выходные данные)

Пример решения проблемы миллионеров

Алиса: $i \in (1, L-1]$, Боб: $j \in (1, L-1]$

a – открытый ключ Алисы

E_a – шифрование с открытым ключом a

D_a – дешифрование с закрытым ключом для открытого ключа a

Протокол:

1. Боб: отправляет Алисе $m = E_a(x) - j + 1$, где x - случайное число, N бит,
2. Алиса отправляет Бобу L-1 значений

$$\begin{bmatrix} y_n = \{D_a(m+n-1) \bmod(p), n \le i < L \\ y_n = \{D_a(m+n-1) \bmod(p) + 1, i < n < L \end{bmatrix}$$

p – простое число из N/2 бит

3. Боб сравнивает число x и j и результат сообщает Алисе.

Если x=j, то Алиса «испортила» значения «дальше» и i > j

Гомоморфное шифрование

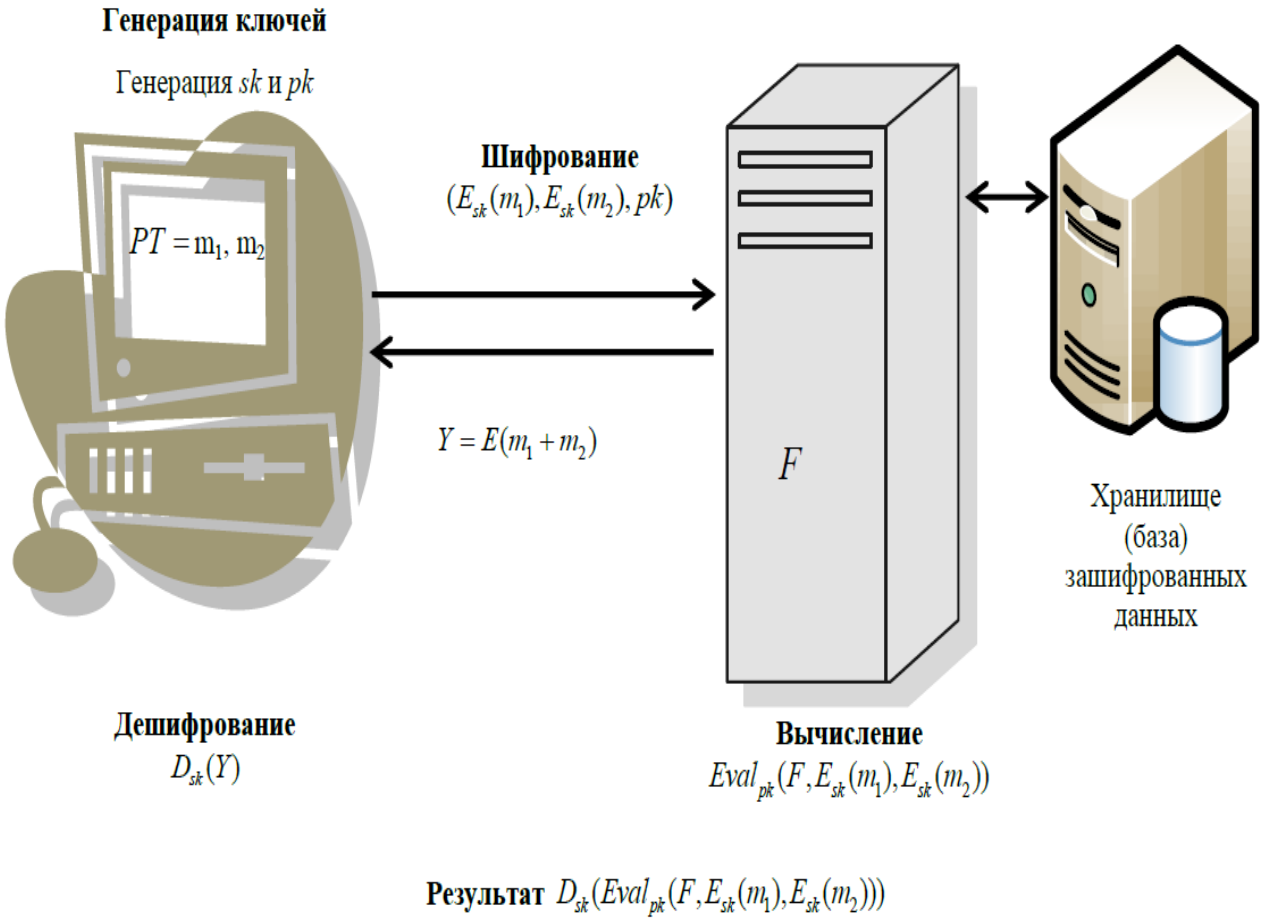
Полностью гомоморфное шифрование – особый тип криптосистемы, который позволяет проводить произвольно сложные вычисления с зашифрованными данными

A FULLY HOMOMORPHIC ENCRYPTION SCHEME

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE
AND THE COMMITTEE ON GRADUATE STUDIES
OF STANFORD UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

Craig Gentry
September 2009

Схема гомоморфного шифрования



А.И. Трубей. Гомоморфное шифрование: безопасность облачных вычислений и другие приложения (обзор) // Информатика. – 2015. – № 1.

Операции гомоморфного шифрования

1. Система гомоморфна относительно умножения

$$D(E(m_1) \otimes E(m_2)) = m_1 \bullet m_2$$

2. Система гомоморфна относительно сложения

$$D(E(m_1) \oplus E(m_2)) = m_1 + m_2$$

3. Система полностью гомоморфна, если выполнены 1 и 2

А.И. Трубей. Гомоморфное шифрование: безопасность облачных вычислений и другие приложения (обзор) // Информатика. – 2015. – № 1.

Применение гомоморфного шифрования

- ✓ Облачные вычисления,
- ✓ Электронное голосование,
- ✓ Защищенный поиск информации,
- ✓ Защита децентрализованных сетей связи,
- ✓ Аутсорсинговые услуги для смарт-карт,
- ✓ Системы с обратной связью,
- ✓ Обфускация для защиты программных продуктов

А.И. Трубей. Гомоморфное шифрование: безопасность облачных вычислений и другие приложения (обзор) // Информатика. – 2015. – № 1.

Распределённая схема подписи

Требования:

- Отсутствие интерактивности
- Независимость участников при постановке подписи
- Работа без участия дилера
- Для восстановления секрета достаточно k и больше сторон.
- Никакие k и меньше сторон не смогут получить никакой информации о секрете.

Схема интерполяционных полиномов Лагранжа (схема разделения секрета Шамира или схема Шамира) — схема разделения секрета, широко используемая в криптографии.

$$F(x) = \sum_i l_i(x)\, y_i \bmod(p)$$

$$l_i = \prod_{i \neq j} \frac{x - x_j}{x_i - x_j} \bmod(p)$$

https://ru.wikipedia.org/wiki/Схема_разделения_секрета_Шамира

Распределенная подпись RSA, А.Д. Фомин, Программные продукты и системы, №2, 2007