Вручение бита на хранение

Битовая схема обязательств (англ. commitment scheme) — это криптографический примитив, который позволяет передать на хранение какое-либо выбранное значение (бит информации), сохраняя его скрытым для других, с возможностью позже раскрыть его значение. Причём схемы обязательств должна быть такой, что сторона не может изменить переданное значение после отправки.

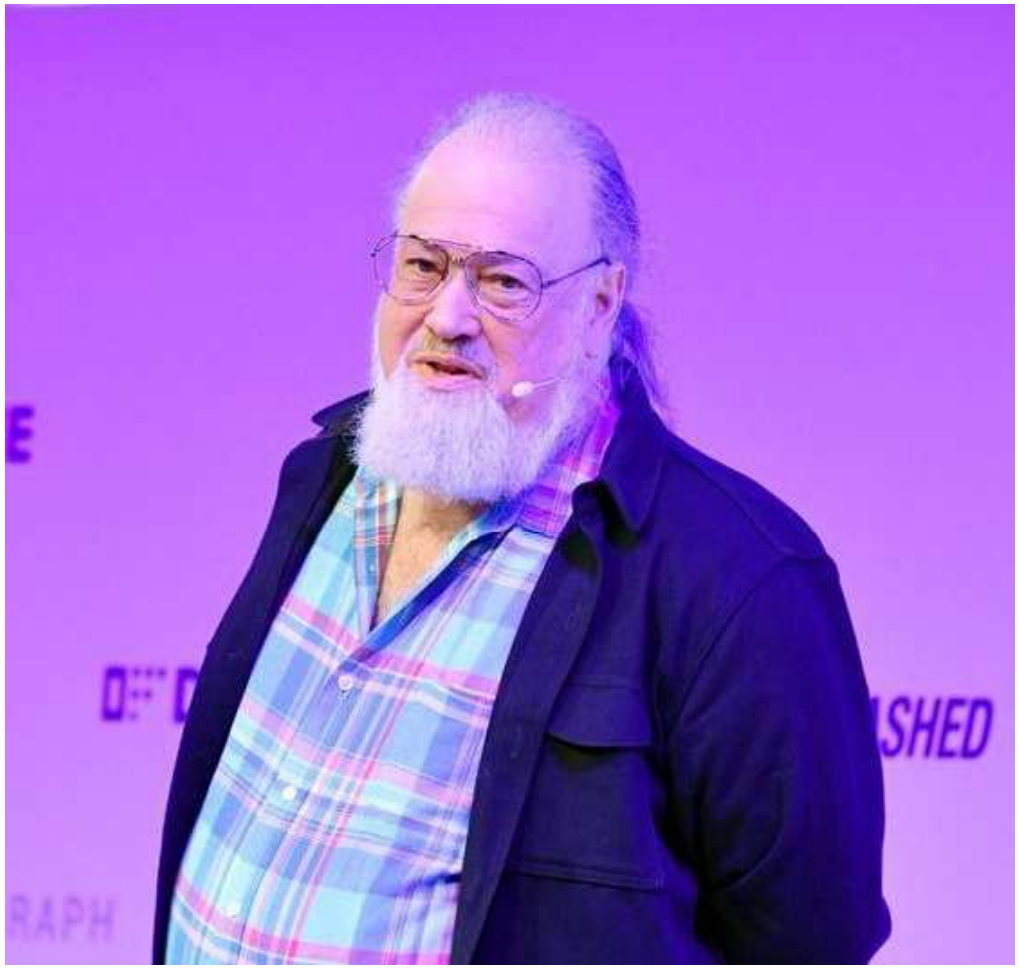
Вручение бита на хранение

Концепция схем обязательств была, возможно, впервые формализована Жилем Брассаром, Дэвидом Чаумом и Клодом Крепо в 1988 году как часть различных протоколов доказательства с нулевым разглашением NP класса, основанных на разных типах схем обязательств. Концепция использовалась и ранее, но без формального рассмотрения. Понятие обязательств появлялось в работах Мануэля Блума.

Жиль Брассар (англ. Gilles Brassard; 1955 г., Монреаль) — канадский физик-теоретик. Известен своими работами по квантовой телепортации, квантовой запутанности, а также квантовой криптографии, в частности созданием протокола BB84.

Вручение бита на хранение

Концепция схем обязательств была, возможно, впервые формализована Жилем Брассаром, Дэвидом Чаумом и Клодом Крепо в 1988 году как часть различных протоколов доказательства с нулевым разглашением NP класса, основанных на разных типах схем обязательств. Концепция использовалась и ранее, но без формального рассмотрения. Понятие обязательств появлялось в работах Мануэля Блума.



Дэвид Ли Чаум (David Chaum, род. 1955 г.) - американский ученый и криптограф. Он также широко известен как изобретатель цифровых денег.

Вручение бита на хранение

Концепция схем обязательств была, возможно, впервые формализована Жилем Брассаром, Дэвидом Чаумом и Клодом Крепо в 1988 году как часть различных протоколов доказательства с нулевым разглашением NP класса, основанных на разных типах схем обязательств. Концепция использовалась и ранее, но без формального рассмотрения. Понятие обязательств появлялось в работах Мануэля Блума.

Клод Крепо (фр. Claude Crépeau, 1962, Монреаль, Квебек, Канада) является профессором в Школе компьютерных наук в Университете Макгилла. Проф. Крепо наиболее известен своими фундаментальными работами в области доказательства с нулевым разглашением, многосторонних вычислений, квантовой криптографии и квантовой телепортации.

Вручение бита на хранение

Концепция схем обязательств была, возможно, впервые формализована Жилем Брассаром, Дэвидом Чаумом и Клодом Крепо в 1988 году как часть различных протоколов доказательства с нулевым разглашением NP класса, основанных на разных типах схем обязательств. Концепция использовалась и ранее, но без формального рассмотрения. Понятие обязательств появлялось в работах Мануэля Блума.

Мануэль Блюм (исп. Manuel Blum; род. 26 апреля 1938, Каракас, Венесуэла) — учёный в области теории вычислительных систем, профессор по информатике в университете Карнеги — Меллон. Награждён в 1995 году премией Тьюринга за достижения в исследовании основ теории сложности вычислений и их применении в криптографии и верификации программ.

Вручение бита на хранение

Итак, идея протокола вручения бита на хранение состоит в следующем. Алисе необходимо передать Бобу бит b так, чтобы тот мог его хранить, не имея возможности узнать его значения до нужного момента. А в нужный момент времени Алиса может объявить значение бита и доказать Бобу, что именно этот бит она ему передала. А у Боба есть возможность проверить, что Алиса не поменяла значение бита в момент его объявления.

Допустим, Алиса может угадывать, какую карту выберет Боб еще до того, как он её выберет. Алиса записывает свое предсказание на клочке бумаги, вкладывает этот клочок бумаги в конверт и отдает запечатанный конверт Бобу. Выбрав карту, Боб показывает её Алисе и зрителям, затем вскрывает конверт и проверяет предсказание. Предсказание, записанное до того, как Боб выбрал карту, не вызывает сомнения.

Взаимодействие двух сторон в схеме обязательства происходит в два этапа:

1. фаза передачи «Commit» — вручение бита (обязательства) на хранение,
2. фаза раскрытия «Reveal» — вскрытие и проверка бита (значения).

Вручение бита на хранение

1. Вручение битов средствами симметричной криптографии

1. Этап вручения бита на хранение:
    1. $B \to A$:$\{R_B\}$, Боб отправляет Алисе своё случайное число;
    2. $A \to B$: $\{E_K(R_B, b)\}$, Алиса шифрует R_B и бит b секретным ключом K, и отправляет Бобу;

Когда для Алисы наступает время раскрыть свой бит, исполнение протокола продолжается.

2. Этап вскрытия бита:
    3. $A \to B$:$\{K\}$, Алиса отправляет Бобу свой секретный ключ K;
    4. Боб расшифровывает сообщение и узнаёт бит. Для проверки достоверности бита Боб проверяет свою случайную строку.

Вручение бита на хранение

2. Вручение битов с использованием однонаправленных функций

1. Этап вручения бита на хранение:
    1. $A \rightarrow B$: $\{H(R_1, R_2, b), R_1\}$, Алиса генерирует два случайных числа R_1, R_2, вычисляет значение однонаправленной функции от R_1, R_2, b, где b вручаемый бит, и отправляет его и R_1 Бобу;

Когда для Алисы наступает время раскрыть свой бит, исполнение протокола продолжается.

2. Этап вскрытия бита:
    2. $A \rightarrow B$: $\{(R_1, R_2, b)\}$;
    3. Боб вычисляет значение однонаправленной функции от полученного сообщения, сравнивает со значениями, полученными на первом этапе. Их совпадение подтверждает достоверность врученного бита.

Вручение бита на хранение

3. Вручение битов с помощью генераторов псевдослучайных последовательностей

1. Этап вручения бита на хранение:
   1. $B \rightarrow A$:$\{R_B = x_1x_2x_3\ldots x_n\}$, Боб отправляет Алисе своё случайное число;
   2. $A \rightarrow B$: $\{Z = z_1z_2z_3\ldots z_n\}$, где $z_i = \begin{cases} y_i & \text{, если } x_i = 0 \\ y_i \oplus b, & \text{если } x_i = 1 \end{cases}$ и $G(R_A) = y_1y_2y_3\ldots y_n$ результат действия генератора псевдослучайных битов G от случайного числа Алисы R_A, $\oplus$ означает операцию XOR.

Когда для Алисы наступает время раскрыть свой бит, исполнение протокола продолжается.

2. Этап вскрытия бита:
   3. $A \rightarrow B$:$\{R_A, b\}$, Алиса отправляет Бобу своё число и бит;
   4. Боб выполняет вычисления шага 2, результат сравнивает с сообщением, полученным на том же шаге.

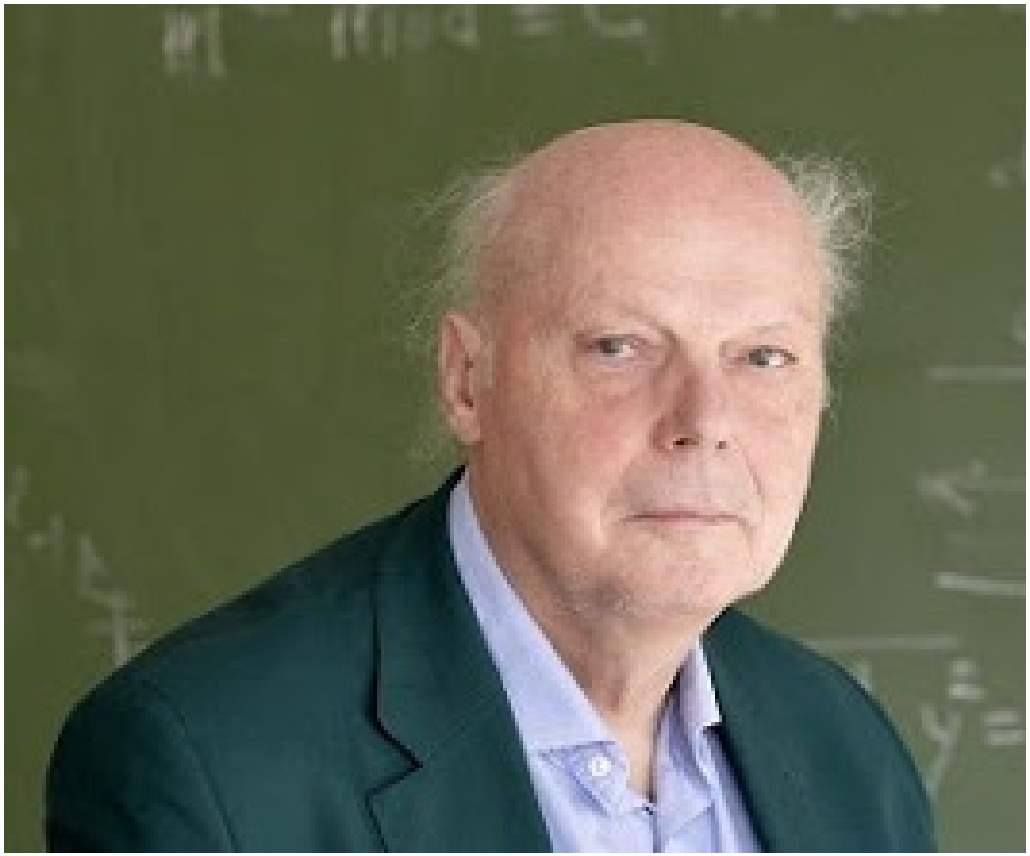
Вручение бита на хранение

Те строки, которые Алиса посылает Бобу для вручения бита, иногда называют *блобами* (blob). Блоб не несёт никакой информации и представляет собой тот необходимый избыток информации, который позволяет провести аутентификацию вручаемого бита. Но, кроме того, блоб позволяет и скрыть значение бита до того момента, когда вручающий захочет его раскрыть. То есть блоб полноценно играет роль конверта.

Доказательство с нулевым разглашением

Жан-Жак Кискате (Jean-Jacques Quisquater) и Луи Гилу (Louis Guillou) поясняют суть доказательства с нулевым разглашением (Zero-Knowledge Proof) с помощью аналогии с пещерой.

Жан-Жак Кискатер (Jean-Jacques Quisquater, родился 13 января 1945 г. Уккел, Бельгия) - криптограф и профессор Лувенского университета (UCLouvain). Вместе с Клаусом Шнорром он получил награду RSA за выдающиеся достижения в области математики в 2013 г. и премию ESORICS за выдающиеся исследования в 2013 г.



Доказательство с нулевым разглашением

В пещере (см. Рис. 9) есть секрет — потайная дверца между C и D, открыть которую может только тот, кто знает волшебные слова. Для остальных же оба хода заканчиваются тупиком.

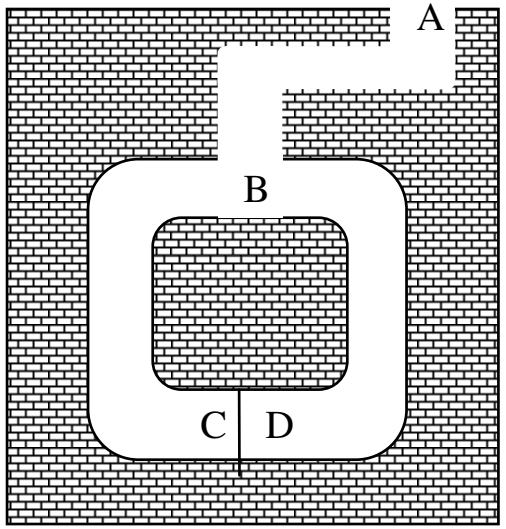


Рис. 9. Пещера с нулевым разглашением

Допустим, Пегги знает секрет пещеры. Свое знание она хочет доказать Виктору, но не хочет открывать ему волшебных слов. Вот как она его убеждает:

1) Виктор стоит в точке A.
2) Пегги проходит либо к точке C, либо к точке D пещеры .
3) Как только Пегги исчезнет в пещере, Виктор переходит в точку B.
4) Виктор кричит Пегги, предлагая ей:
   a. Выйти из левого прохода или
   b. Выйти из правого прохода
5) Пегги выполняет просьбу, используя, если необходимо, волшебные слова для открытия двери.
6) Пегги и Виктор *n* раз повторяют этапы 1—5.

Доказательство с нулевым разглашением

Метод, используемый в этом протоколе, напоминает классический протокол честного дележа, называемый «разделяй и выбирай»:

1) Алиса разрезает пополам какую-либо вещь.
2) Боб выбирает одну половину себе.
3) Алиса забирает оставшуюся половину.

Честный дележ на этапе 1 в интересах Алисы, поскольку Боб на этапе 2 выберет любую половину, которая ему понравится. Технику «разделяй и выбирай» в криптографии впервые предложил Майкл Рабин (Michael Rabin).

Михаэль Озер Рабин (нем. *Michael Oser Rabin*, род. 1 сентября 1931, Вроцлав) — израильский учёный в области теории вычислительных систем, математик, лауреат премии Тьюринга и многих других премий. Его дочь, Таль Рабин, руководит научной группой *Cryptography and Privacy Research Group* в компании IBM.

Доказательство с нулевым разглашением

Формальное описание интерактивного протокола с нулевым разглашением

1) Пегги, используя свою информацию и случайное число, преобразует одну трудную задачу в другую (новую) задачу, изоморфную оригинальной задаче. Затем с помощью своей информации и случайного числа она решает новую трудную задачу.
   Пегги передает решение новой задачи, используя схему вручения бита.
2) Виктор предлагает Пегги сделать одно из двух:
   a. доказать изоморфность новой и исходной задачи (т.е. два различных решения для двух родственных задач), либо
   b. раскрыть решение, врученное ею на этапе 2, и доказать, что это решение новой задачи.
3) Пегги выполняет предложение Виктора.
4) Пегги и Виктор повторяют *n* раз этапы 1—3.

Доказательство с нулевым разглашением

Изоморфизм графов

Допустим, Пегги знает, что графы G_1 и G_2 изоморфны. Это знание Пегги может доказать с помощью следующего протокола:

1) Пегги в произвольном порядке переставляет вершины графа G_1, получая другой граф, H, изоморфный G_1. Поскольку Пегги знает об изоморфности графов H и G_1, ей известна также изоморфность графов H и G_2. Однако для всех остальных установление изоморфизма графов H и G_1 или H и G_2 задача столь же трудная, как доказательство изоморфизма графов G_1 и G_2.
   Пегги отсылает Виктору граф H.
2) Виктор предлагает Пегги либо
   a. доказать изоморфность графов H и G_1 либо
   b. доказать изоморфность графов H и G_2.
3) Пегги подчиняется. Она либо:
   a. доказывает изоморфность графов H и G_1, не доказывая изоморфности графов H и G_2, либо
   b. доказывает изоморфность графов H и G_2, не доказывая изоморфности графов H и G_1.
4) Пегги и Виктор повторяют n раз этапы 1—3.

Доказательство с нулевым разглашением

Гамильтоновы циклы (Мануэль Блюм, 1986 г.)

Пегги знает гамильтонов цикл графа G. Пегги доказывает Виктору своё знание, не сообщая самого цикла.

1) Пегги произвольно переставляет граф G, создавая новый граф H, изоморфный графу G. Если Пегги знает гамильтонов цикл графа G, она без труда найдет гамильтонов цикл графа H.
   Пегги посылает граф H Виктору.
2) Виктор предлагает Пегги либо:
   a. доказать, что граф H – это изоморфная копия графа G, либо
   b. показать гамильтонов цикл графа H.
3) Пегги подчиняется. Она либо:
   a. доказывает, что граф H – это изоморфная копия графа G, раскрывая с этой целью перестановки, но не показывая гамильтонов цикл графов G или H, либо
   b. показывает гамильтонов цикл графа H, но не доказывая изоморфность графов G и H.
4) Пегги и Виктор n раз повторяют этапы 1—3.

Доказательство с нулевым разглашением

Неинтерактивные доказательства с нулевым разглашением

Кэрол (третье лицо) невозможно убедить в верности предыдущих доказательств, потому что протокол интерактивный, а она в нем не участвует. Чтобы убедить Кэрол и других заинтересованных лиц, следует использовать неинтерактивный протокол.

Протоколы неинтерактивных доказательств с нулевым разглашением не требуют никакого взаимодействия участников. Пегги может опубликовать их и тем самым доказать свое знание всем, у кого найдется время проверить достоврность доказательства.

Доказательство с нулевым разглашением

Неинтерактивные доказательства с нулевым разглашением

Базовый протокол вместо Виктора использует однонаправленную хэш-функцию:

1) Пегги, используя свою информацию и *n* случайных чисел, преобразует трудную задачу в *n* различных изоморфных задач. Затем с помощью своей информации и случайных чисел Пегги решает *n* новых трудных задач.
2) Пегги вручает решение *n* новых трудных задач.
3) Пегги использует все вручения как единый вход для однонаправленной хэш-функции. Затем она сохраняет первые *n* битов значения хэш-функции.
4) Пегги берет *n* битов, сгенерированных на этапе 3, и поочередно берет *i-й* бит для каждой трудной задачи *i*:
   a. если *i-й* бит равен 0, она доказывает изоморфность исходной и новой задач, либо
   b. если *i-й* бит равен 1, она открывает решение, врученное на этапе 2, и доказывает, что оно служит решением новой задачи *i*.
5) Пегги публикует все решения, врученные на этапе 2, и все доказательства, полученные на этапе 4.
6) Виктор, Кэрол и все прочие заинтересованные лица проверяют корректность исполнения этапов 1—5.