К. В. Захарченко

ПОСТРОЕНИЕ СХЕМЫ ОБЯЗАТЕЛЬСТВА С ФУНКЦИЕЙ ТРУДНОГО БИТА

В работе представлено построение схемы криптографического обязательства на основе классической конструкции и криптографии на эллиптических кривых с целью получения схемы, обладающей рядом нестандартных свойств, таких как функция трудного бита и свойство извлекаемости. Необходимость наличия таких свойств возникает при использовании схемы обязательства при построении схем, основывающихся на NP языках и протоколов, требующих наличие симулятора.

I. Схема Обязательства

Схема Обязательства – это криптографический примитив, который позволяет одной стороне интерактивного протокола закрепить себя за каким-то сообщением так, что в дальнейшем эта сторона не может изменить это сообщение [4]. Однако, обязательство в дальнейшем можно раскрыть, тем самым раскрыв исходное сообщение.

Схема Обязательства состоит из двух стадий: *Обязательство* и *Раскрытие*. Стадия *Обязательство* представлена алгоритмом E, вычисляющим обязательство, а стадия *Раскрытие* алгоритмом $CheckE$, позволяющим проверить соответствие обязательства его раскрытию:

1. $E(m, r) \to c$: принимает на вход сообщение m и секретную составляющую r. Результатом будет обязательство c, зависящее от m и r.

2. $CheckE(c, m, r) \to \{1, 0\}$: принимает на вход обязательство c, сообщение m и секретную составляющую r, возвращает 1, если $E(m, r) = c$, и 0 во всех остальных случаях.

Свойство, связывающее эти два алгоритма следующее: для всех пар (m, r), $CheckE(E(m, r), m, r) = 1$.

Схема Обязательства может обладать либо свойством идеального связывания, либо свойством идеального скрытия:

1. **Свойство идеального связывания:** для любой пары (m, r) не существует такой пары (m', r'), что $E(m', r') = E(m, r)$ и $m \neq m'$.

2. **Свойство идеального скрытия:** для любой пары (m, m') существует такая пара (r, r'), что $E(m, r) = E(m', r')$.

Каждое свойство имеет аналогичное, но не с идеальным ограничением, а вычислительным.

1. **Свойство вычислительного связывания:** для любой пары (m, r) вычислительно трудно найти такую пару (m', r'), что $E(m', r') = E(m, r)$ и $m \neq m'$.

2. **Свойство вычислительного скрытия:** для любого c вычислительно трудно найти такую пару (m, r), что $E(m, r) = c$.

Фраза "вычислительно трудно" означает, что любой алгоритм, решающий эту задачу, работает за время пропорциональное экспоненте относительно длины входных данных, или, говоря простым языком, даже при практически допустимом объёме входных данных на решение этой задачи мощнейшим современным компьютерам придётся потратить не одну тысячу лет.

Как можно наблюдать из свойств идеального связывания и скрытия, они противоречат друг другу и не могут присутствовать в одной Схеме Обязательства. Однако, существует варианты схем, обладающих вычислительным скрытием и идеальным связыванием или идеальным скрытием и вычислительным связыванием. Построение последнего варианта Схемы Обязательства приводится в данной работе.

II. Схема обязательства. Первое приближение

Для начального построения схемы обязательства используем классическую схему, основывающуюся на задаче дискретного логарифмирования [4].

Пусть даны g и h – элементы группы G_q. G_q – группа порядка q (q – простое число). g – генератор группы G_q, а h – случайный элемент группы.

Сторона, производящая обязательство относительно сообщения $m \in \mathbb{Z}_q$, выбирает $r \in Z_q$ случайным образом и вычисляет обязательство следующим образом: $E(m, r) = g^m h^r$. Такое обязательство может быть раскрыто в дальнейшем, раскрытием параметров m и r. Свойство идеального скрытия обеспечивается тем, что, функция $E'(r) = E(m, r)$ фиксированная для любого параметра m является инъективной.

III. Трудный бит схемы обязательства

Трудный бит – понятие, тесно связанное с односторонними функциями. Для односторонней функции f трудным битом называется такая функция h, что для произвольного x, зная только $f(x)$, вычислительно трудно найти $h(x)$ [3]. В данной работе ставится задачей определить функцию трудного бита для Схемы Обязательства. Обозначив пару (m, r), как x и дадим формальное определение. Трудным битом для Схемы Обязательства E назовём такую функцию h, что для произвольного x, зная только обязательство $E(x)$, вычислительно трудно найти $h(x)$. Интуитивно рассуждая, свойство идеального скрытия схемы обязательства должно обес-

печивать трудновычислимость функции трудного бита. Используя схему Педерсена [4] в данной работе, мы построим схему обязательства, основывающуюся на односторонней функции, а именно на возведении в степень в конечном поле. Существуют исследования [3], приводящие доказательства наличия функции трудного бита для задачи дискретного логарифма над полем эллиптической кривой. Используя эти наработки, построим схему обязательства над полем эллиптической кривой. Это обеспечит существование функции трудного бита для этой схемы, что является одной из целей данной работы.

IV. Схема Обязательства. Окончательная версия

Для того, чтобы для схемы обязательства доказуемо присутствовала функция трудного бита, построим схему Педерсена на основе эллиптических кривых. Пусть имеется конечная группа F_p над эллиптической кривой. Пусть G – точка генератор группы. Случайным образом выберем точку на эллиптической кривой $H \in F_p$. Тогда сторона, производящая обязательство относительно сообщения m, случайным образом выбирает целое число $r \in Z_p$ и вычисляет обязательство следующим образом: $E_c(m, r) = mG + rH$.

Такое обязательство в дальнейшем может быть раскрыто, если будут опубликованы параметры m и r. Схема реализует классическую схему Педерсена с единственным отличием в том, что в качестве группы используется группа точек эллиптической кривой.

Как указанно в литературе [3], для подобной схемы трудным битом будет являться любой бит сообщения. Значит, обозначим функцию div, как функцию, изымающую самый младший разряд в двоичном представлении параметра m. То есть, будем подразумевать, что обозначив $x = (m, r)$, $div(x) = b$ тогда и только тогда, когда младший бит числа m в схеме обязательства равен b, где $b \in \{0, 1\}$.

V. Свойство извлекаемости Схемы Обязательства

В полученной схеме Обязательства в качестве односторонней функции используется функция умножения в поле точек эллиптической кривой. Для точек G и H нахождение такого числа k, что $H = kG$ называют задачей дискретного логарифма на эллиптических кривых [3] и считается, что эта задача является вычислительно трудной. Как было показано в литературе [2], для того, чтобы односторонняя функция обладала свойствами извлекаемости, необходимо, чтобы для этой функции выполнялось свойство сложности вычисления задачи Диффи-Хеллмана или задачи Дискретного Логарифма. Следовательно, односторонняя функция, реализованная, как операция умножения в поле точек эллиптической кривой является извлекаемой. Это значит, что имея алгоритм работы стороны, вычисляющей эту одностороннюю функцию, вне зависимости от того, в каком виде представлен этот алгоритм (например обфусцированный код), можно извлечь использованную одностороннюю функцию. Таким образом сторона, обладающая доступом к алгоритму, производящему обязательство имеет возможность нарушить свойство идеального скрытия схемы обязательства. Это можно выгодно использовать при построении некоторых протоколов [5].

VI. Результаты

В работе продемонстрирован вариант построения Схемы Обязательства с функцией трудного бита. Использовав за основу построения конструкции проблему вычисления логорифма в поле эллиптической кривой, получилось создать схему, обладающую помимо трудного бита также свойством извлекаемости, что позволяет использовать схему обязательства наравне с односторонними функциями в различных криптографических конструкциях. Например, такой примитив может использоваться при построении протоколов Нулевого Разглашения [5] или забывчивой передачи, если необходимо иметь свойство идеального скрытия данных принимающей стороны.

1. Boneh D. The decision diffie-hellman problem //International Algorithmic Number Theory Symposium. – Springer, Berlin, Heidelberg, 1998. – С. 48-63.
2. Dakdouk R. R. Theory and application of extractable functions. – Yale University, 2009.
3. Hankerson D., Menezes A. Elliptic curve discrete logarithm problem //Encyclopedia of Cryptography and Security. – Springer US, 2011. – С. 397-400.
4. Pedersen T. P. Non-interactive and information-theoretic secure verifiable secret sharing //Advances in Cryptology—CRYPTO'91. – Springer Berlin Heidelberg, 1991. – С. 129-140.
5. Захарченко К. В. Шифрование с обязательством и сбрасываемое доказательство с нулевым разглашением в два раунда. – 2016.

Захарченко Константин Владимирович, аспирант кафедры Информационных Технологий Автоматизированных Систем Белорусского Государственного Университета Информатики и Радиоэлекстроники, cvzakharchenko@gmail.com.