К. В. Захарченко

ШИФРОВАНИЕ С ОБЯЗАТЕЛЬСТВОМ И СБРАСЫВАЕМОЕ ДОКАЗАТЕЛЬСТВО С НУЛЕВЫМ РАЗГЛАШЕНИЕМ В ДВА РАУНДА

В работе представлен новый криптографический примитив – Шифрование с Обязательством, позволяющий производить шифрование пары сообщений относительно Схемы Обязательства таким образом, что только сторона, которая произвела обязательство, способна расшифровать одно из сообщений и только одно. Какое именно сообщение подлежит расшифровке, определяется содержимым обязательства и неизвестно на момент шифрования. Показано возможное применение представленной схемы для реализации протокола сбрасываемого Доказательства с Нулевым Разглашением в минимальное количество раундов.

Введение

Схема Обязательства (СО) – криптографический примитив, используемый во множестве протоколов для того, чтобы одна сторона могла закрепить какое-то сообщение, не раскрывая его, а после продемонстрировать сообщение [6].
Шифрование с Обязательством (ШО) – новый криптографический примитив, представленный в данной работе. ШО представляет из себя возможность зашифровать сообщение относительно произвольной Схемы Обязательства так, что во-первых только участник, способный раскрыть обязательство, способен расшифровать сообщение, а во-вторых расшифрованное сообщение зависит от закреплённого в СО сообщения. Второе свойство представляет большой интерес и будет показано, как его можно применить для построения протокола Доказательства с Нулевым Разглашением с оптимальным количеством раундов.
Доказательство с Нулевым Разглашением (ДНР) – это парадоксальный протокол, который позволяет одному участнику (Доказывающему) убедить другого участника (Проверяющего) в истинности математического утверждения $x \in L$ ($L \in NP$), не раскрывая никакой дополнительной информации Проверяющему. Сбрасываемое ДНР (сДНР) – это более строгое определение протокола, в котором злонамеренный проверяющий может в любой момент "сбросить"Доказывающего в начальное состояние и начать всю процедуру доказательства заново [3]. Такие возможности появляются, если доказывающая сторона реализована в виде смарт-карты или обфусцированного приложения. До сих пор в литературе были предоставлены протоколы сДНР не менее, чем в 4 раунда [4]. Основным достижением данной работы является демонстрация протокола сДНР в 2 раунда, используя более сильное (чем в предыдущих работах) предположение существования схемы Шифрования с Обязательством (ШО). Предоставляется возможная конструкция схемы ШО, основанная на Псевдослучайных Функциях со Свидетельством (ПФС)[7] и Схемах Обязательства (СО)[6]. Для демонстрации нулевого разглашения возможно построение симулятора в модели "белого ящика".

I. Используемые примитивы

Псевдослучайная Функция со Свидетельством состоит из трёх алгоритмов и в упрощённом виде выглядит следующим образом (более подробное определение в [5]):
1. $wprf.gen(L)$: рандомизированный алгоритм, принимает язык $L \in NP$ и генерирует секретный и открытый ключи wsk и wpk соответственно.
2. $wprf.f(x, wsk)$: принимает x и секретный ключ wsk, на выходе имеем y, зависящий от x, неотличимый от случайного. То есть, $wprf.f(x, wsk)$ является псевдослучайной функцией от аргумента x.
3. $wprf.eval(x, w, wpk)$: принимает x, свидетельство w и открытый ключ wpk, вычисляет $wprf.f(x, wsk)$, если w является корректным свидетельством $x \in L$, в обратном случае выводит $\perp$.
Так же, для построения ШО нам понадобится схема симметричного шифрования. Для краткости допустим, что пара алгоритмов (SC, SD) – блочный шифр наподобие AES в режиме CBC такой, что $(\forall m \forall k) SD(SC(m, k), k) = m$. Для удобства допустим, что $(\forall c) SD(c, \perp) = \perp$. Обозначим параметр безопасности системы, как n. Пусть $E : \{0,1\}^{2n} \to \{0,1\}^n$ – Схема Обязательства с идеальным скрытием [4] и div – трудный бит E такой, что относительно x вероятность $P[div(x) = 0] \approx \frac{1}{2}$. Определим язык $L_b := \{com | (\exists w) E(w) = com, div(w) = b\}$ для $b \in \{0,1\}$, тогда w – свидетельство $com \in L$. Напомним, что $(wprf.gen, wprf.f, wprf.eval)$ – схема ПФС. Пусть $(wsk_b, wpk_b) := wprf.gen(L_b)$ для $b \in \{0,1\}$. Предлагаемая схема Шифрования с Обязательством состоит из двух алгоритмов $(ce.enc, ce.dec)$:
1. $ce.enc(m_0, m_1, com)$: принимает обязательство com и два сообщения (m_0, m_1). Пусть $r_b := wprf.f(com, wsk_b)$ для $b \in \{0,1\}$. Тогда результатом функции будет $(c_0, c_1) :=$

$(SC(m_0, r_0), SC(m_1, r_1))$.
2.$ce.dec(c_0, c_1, com, w)$: принимает w, обязательство com и два зашифрованных сообщения (c_0, c_1). Пусть $r_b := wprf.eval(com, w, wpk_b)$ для $b \in \{0, 1\}$. Тогда результатом функции будет $(m_0, m_1) := (SD(c_0, r_0), SD(c_1, r_1))$.
Свойства корректности и надёжности следуют из аналогичных свойств ПФС.

II. Схема сДНР в два раунда

Покажем в неформальном виде возможность применения схемы ШО для построения протокола сДНР в два раунда. Во время выполнением протокола общей информацией для двух сторон является схема обязательства E, её трудный бит div, параметр безопасности n, открытые параметры схемы ШО, а так же непосредственно доказываемое математическое утверждение x. Проверяющий отдельно получает случайное значение r_v. Доказывающий получает случайный параметр r_p и свидетельство w истинности x.
1. Первый раунд. Проверяющий выбирает параметр k, соответствующий количеству раундов классического[1] ДНР, которые позволяют достичь желаемого уровня убедительности. Значение r_v используется, чтобы инициализировать генератор псевдослучайных чисел (ГПСЧ). После чего Проверяющий рандомизированным образом с помощью E производит k обязательств и отправляет их Доказывающему.
2. Второй раунд. а) Доказывающий получает от проверяющего k обязательств. Значение r_p вместе с полученными обязательствами используется для инициализации ГПСЧ. После чего Доказывающий генерирует k пар аргументов доказательства классического[1] протокола ДНР используя w и x. Каждая пара зашифровывается с помощью Шифрования со Свидетельством. Доказывающий отправляет Проверяющему k пар зашифрованных аргументов. б) Проверяющий получает k пар зашифрованных аргументов и для каждой пары расшифровывает один из аргументов в зависимости от обязательства. Если каждый аргумент верен, то проверяющий принимает доказательство, если существует неверный аргумент, то проверяющий отвергает доказательство.
Представленный протокол действительно является сбрасываемым, так как сообщение, отправляемое Доказывающим, зависит исключительно от сообщения, отправленного Проверяющим. Чтобы скомпрометировать Доказывающего необходимо найти такую пару (x_0, x_1), что $E(x_0) = E(x_1)$. Нахождение такой пары является вычислительно трудной задачей.
Построение модели симулятора основывается на существовании ансамблей необфусцируемых функций[5]. В таком случае симулятор в модели белого ящика может получать на вход исходный код проверяющей стороны и извлекать параметр r_v. Имея данный параметр симулятор сможет восстановить поведение проверяющей стороны и скомпроментировать его.

III. Выводы

Таким образом, в данной статье представлена схема Шифрования со Свидетельством, позволяющая реализовать сбрасываемое Доказательство с Нулевым Разглашением с симулятором в модели белого ящика. Фактически, ШО эквивалентно схеме Забывчивой Передачи с идеальным скрытием и вычислительным связыванием и является первой конструкцией этого примитива. Представленная схема, насколько известно автору, является первой схемой сДНР в два раунда.
На данный момент открытым вопросом является возможность реализации более строгой модели симулятора. Другое направление дальнейших исследований состоит в ослаблении используемых предположений. Схема ПФС по своей природе схожа с Ограниченными Псевдослучайными Функциями[2] – схемой которые используют более слабые предположения.

1. Blum M. How to prove a theorem so no one else can claim it //Proceedings of the International Congress of Mathematicians. – 1986. – Т. 1. – С. 2.
2. Boneh D., Waters B. Constrained pseudorandom functions and their applications //Advances in Cryptology-ASIACRYPT 2013. – Springer Berlin Heidelberg, 2013. – С. 280-300.
3. Canetti R. et al. Resettable zero-knowledge //Proceedings of the thirty-second annual ACM symposium on Theory of computing. – ACM, 2000. – С. 235-244.
4. Chung K. M. et al. 4-round resettably-sound zero knowledge //Theory of Cryptography. – Springer Berlin Heidelberg, 2014. – С. 192-216.
5. Bitansky N., Paneth O. From the impossibility of obfuscation to a new non-black-box simulation technique //Foundations of Computer Science (FOCS), 2012 IEEE 53rd Annual Symposium on. – IEEE, 2012. – С. 223-232.
6. Pedersen T. P. Non-interactive and information-theoretic secure verifiable secret sharing //Advances in Cryptology—CRYPTO'91. – Springer Berlin Heidelberg, 1991. – С. 129-140.
7. Zhandry M. How to avoid obfuscation using witness PRFs //Theory of Cryptography. – Springer Berlin Heidelberg, 2016. – С. 421-448.

Захарченко Константин Владимирович, магистрант кафедры информационных технологий автоматизированных систем Белорусского государственного университета информатики и радиоэлекстроники, c.v.zakharchenko@gmail.com.