Бекенов М.И., Оспанов Р.М.

О ПРОТОКОЛАХ ИНТЕРАКТИВНОГО ДОКАЗАТЕЛЬСТВА С НУЛЕВЫМ РАЗГЛАШЕНИЕМ

Евразийский национальный университет им. Л.Н.Гумилева, Казахстан, Астана

Данная работа посвящена одному из важнейших понятий современной криптографии – понятию протокола интерактивного доказательства с нулевым разглашением.

В математической криптографии исследование криптографических протоколов является одним из основных направлений. Под протоколом (protocol) понимают распределенный алгоритм, определяющий последовательность шагов, точно специализирующих действия, которые требуются от двух или более участников для решения некоторой задачи. Протокол, в котором используются криптографические алгоритмы и который служит для решения некоторой криптографической задачи, называют криптографическим протоколом (cryptographic protocol). В основе выбора и/или проектирования криптографического протокола лежит условие обеспечения криптографической стойкости, свойства протокола, характеризующее его способность противостоять атакам противника и/или нарушителя, а также оценка сложности (вычислительной, коммуникационной или раундовой) протокола. Последние 30 лет важным предметом изучения теории криптографических протоколов и теории сложности является понятие доказательства с нулевым разглашением, основанного на понятии системы (протокола) интерактивного доказательства.

Протокол интерактивного доказательства или IP-протокол (interactive proof) – протокол с двумя участниками, в котором один участник (доказывающий) доказывает другому участнику (проверяющему) истинность утверждения, не раскрывая сущности доказательства. Протокол интерактивного

доказательства должен обладать следующими двумя свойствами.

Свойство полноты (completeness property) [1] – свойство криптографического протокола, означающее, что при выполнении честными участниками протокол решает ту задачу, для которой он создан.

Свойство корректности (soundness property) [1] - способность протокола противостоять угрозам со стороны противника и/или нарушителя, не располагающего необходимой секретной информацией, но пытающегося выполнить протокол за участника, который по определению должен такой информацией владеть.

В случае обладания еще одним свойством, а именно свойством нулевого разглашения (zero-knowledge property) [1] (свойство протокола , обеспечивающее такое его выполнение, что никакая информация о доказываемом утверждении, кроме факта его истинности, не может быть получена нечестным проверяющим из переданных сообщений за время полиномиально зависящее от суммарной длины этих сообщений), получаем:

Протокол доказательства с нулевым разглашением или ZK-протокол (zero-knowledge proof) – протокол интерактивного доказательства, в ходе работы которого проверяющая сторона не может получить никакой информации о доказываемом утверждении, кроме факта его истинности.

Существует другой вариант свойства нулевого разглашения. А именно нулевое разглашение относительно честного проверяющего (honest-verifier zero-knowledge) [1] — ослабленный вариант разглашения нулевого, при котором требуется, чтобы протокол интерактивного доказательства не давал никакой дополнительной информации о доказываемом утверждении лишь честному проверяющему, т.е. выполняющему действия, предписанные протоколом. С криптографической точки зрения данное свойство защищает доказывающего не от нечестного проверяющего, а от противника, который подслушивает сеанс выполнения протокола.

Известными примерами протоколов с нулевым разглашением являются [2], [3], [4], [5], [6]:

1) «Задача о пещере Али-Бабы»;
2) Доказательство изоморфизма графов;
3) Доказательство неизоморфизма;
4) Доказательство знания дискретного логарифма;
5) Доказательство знания представления числа в базисе;
6) Доказательство знания представления множества чисел в соответствующих базисах;
7) Доказательство знания мультипликативной связи «депонированных» величин;
8) Доказательство принадлежности подгруппе;
9) Протокол идентификации Шнорра;
10) Доказательство принадлежности числа множеству квадратичных вычетов;
11) Доказательство принадлежности числа множеству квадратичных невычетов;
12) Доказательство знания разложения числа на два простых множителя;
13) Доказательство знания гамильтонова цикла;
14) Доказательство 3-раскрашиваемости графа.

Существуют различные математические модели понятия интерактивного доказательства с нулевым разглашением. Одним из подходов к математическому определению основан на использовании так называемых интерактивных машин Тьюринга. Другой подход рассматривает протокол интерактивного доказательства как игру с двумя участниками. Недавно появились работы, предлагающие протоколы с нулевым разглашением, основанными на технике протоколов Яо (протоколов конфиденциальных вычислений). Это связано с тем фактом, что протоколы интерактивного доказательства являются частным случаем двусторонних протоколов конфиденциальных вычислений. Такой подход позволяет проектировать протоколы с нулевым разглашением для языков, не обязательно с некоторой

алгебраической структурой. Например, протокол, в котором доказывается утверждение вида “Я знаю x такой, что y=SHA-256(x)” [7].

Теория протоколов с нулевым разглашением активно развивается усилиями ученых из разных стран. Существует множество различных практических приложений, в том числе, интелектуальные карты, web-приложения с нулевым разглашением и др. Однако публикаций и разработок отечественных авторов пока нами не обнаружено.

Литература

1. Погорелов Б.А., Сачков В.Н. (ред.) Словарь криптографических терминов. - М.: МЦМНО, 2006.
2. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: Учебное пособие для вузов. - М.: Горячая линия - Телеком, 2007.
3. Bruse Schneier, Applied Cryptography, Second edition: Protocols, Algorthms and Source Code in C, Wiley Computer Publishing, John Wiley & Sons, Inc.,1996,666p., - P.95-96
4. Венбо Мао Современная криптография: теория и практика.: Пер. с англ. - М.: Издательский дом “Вильямс”, 2005
5. S.Goldwasser, S.Micali and C.Rackoff. The Knowledge Complexity of Interactive Proof System. In Proceeding of 17th ACM Symposium on the Theory of Computing, pages 291-304, 1985
6. O.Goldreich Foundations of cryptography. Basic tools. Cambridge University Press, 2004
7. M.Jawurek, F.Kerschbaum, C.Orlandi Zero-Knowledge Using Garbled Circuits or How To Prove Non-Algebraic Statements Efficiently , Cryptology ePrint Archive: Report 2013/073