Типы нулевого разглашения

Н. П. Варновский

1. Введение

В данной работе рассматриваются типы протоколов интерактивного доказательства с нулевым разглашением. Слово "доказательство" не включено в заголовок преднамеренно, чтобы подчеркнуть универсальность понятия нулевого разглашения как средства формализации требований к криптографическим протоколам различного рода.

Понятие нулевого разглашения в общем виде и на неформальном уровне можно объяснить следующим образом. Имеется протокол с двумя участниками, которых по традиции, принятой в криптографической литературе, мы будем называть Алисой и Бобом. Выполняя локальные вычисления и обмениваясь сообщениями, Алиса и Боб должны решить некоторую вычислительную задачу. Например, к моменту начала выполнения протокола Алисе известно некоторое значение (входное слово) a, а Бобу — значение b и они должны совместно вычислить значение $f(a,b)$ заданной функции f. Это — типичный пример задачи для распределенных вычислений.

Задача становится криптографической, если, например, Алисе известна некоторая секретная информация k, которая либо совпадает со входным словом a, либо является его частью. Предполагается, что значение k выбрано наудачу из множества K достаточно большой мощности. В этой секретной информации заинтересован противник, в качестве которого могут выступать как Боб, так и третьи лица, подслушивающие диалог между участниками. Обычно делается предположение в пользу противника, что множество K ему известно. Но это — вся информация о значении k, которой он обладает до начала выполнения протокола. Ставится задача построить такой протокол, который удовлетворяет следующим двум основным требованиям.

а). Корректное решение поставленной вычислительной задачи (в нашем примере — правильное вычисление функции f).

б). Сохранение значения k в секрете. Протокол не должен давать противнику никакой полезной для него информации о значении k.

Свойство, неформальным описанием которого является требование б), называется нулевым разглашением, а криптографический протокол, обладающий таким свойством, — протоколом с нулевым разглашением.

Разумеется, не для всякой задачи существует криптографический протокол с нулевым разглашением. Например, если $k = a$ и требуется вычислить функцию $f(a,b) = a$, то в результате выполнения любого корректного протокола противник будет знать значение k. С другой стороны, для некоторых задач свойство нулевого разглашения может оказаться тривиальным, как, например, в случае вычисления функции $f(a,b) = b$.

В протоколе интерактивного доказательства у Алисы и Боба имеется общее входное слово x и Алиса пытается доказать Бобу теорему "$x \in L$", где L — язык, известный обоим участникам. Подчеркнем, что протокол интерактивного доказательства строится отдельно для каждого конкретного языка L. Корректность протокола означает, что если $x \notin L$, то какие бы аргументы не приводила Алиса, Боб наверняка отвергнет доказательство. Из свойства нулевого разглашения следует, что в случае $x \in L$ Боб не получает в результате выполнения протокола никакой информации, которая в дальнейшем помогла бы ему самостоятельно доказывать теорему "$x \in L$" третьим лицам.

Как мы увидим в дальнейшем, понятие корректности криптографического протокола и свойство нулевого разглашения могут быть формализованы различным образом. В результате возникает разнообразие типов нулевого разглашения. Их исследование для протоколов интерактивного доказательства — важнейшее направление соответствующей теории.

Данная работа посвящена следующему более узкому вопросу: что известно о существовании того или иного типа протоколов доказательства с нулевым разглашением для всех языков из класса NP.

2. Основные определения

Пусть $\Sigma = \{0,1\}$. Мы рассматриваем языки в двоичном алфавите, т. е. всякий язык L является подмножеством множества Σ^*.

Всюду ниже мы используем стандартное обозначение $\nu(n)$ для пренебрежимо малой функции. Формально, для функции $f : N \to R$ запись $f(n) = \nu(n)$ означает, что для любого полинома p существует n_0 такое, что для всех $n \geq n_0$, $f(n) \leq 1/p(n)$.

Под противником, который атакует криптографические протоколы или составляющие их примитивы, будет пониматься полиномиальный алгоритм, всюду в данной работе обозначаемый через A. Возможны две формализации. В однородной модели вычислений алгоритм A — это полиномиальная вероятностная машина Тьюринга, а в неоднородной — семейство булевых схем полиномиального размера. Все приводимые ниже определения и результаты могут быть сформулированы в каждой из этих моделей.

Определение 1. Функция $f : \Sigma^* \to \Sigma^*$ называется односторонней, если

1. существует полиномиальная машина Тьюринга M такая, что для всякого $x \in \Sigma^*$, $M(x) = f(x)$;
2. для любого полиномиального алгоритма A $\quad Pr\{f(A(1^n, f(x))) = f(x), x \in_R \Sigma^n\} = \nu(n)$.

Здесь 1^n — число n в унарной записи.

Взаимно однозначная, сохраняющая длину односторонняя функция называется односторонней перестановкой.

Пусть $L \subseteq \Sigma^*$ и $\{D_x\}_{x \in L}$ и $\{E_x\}_{x \in L}$ — два семейства распределений. Для простоты изложения будем предполагать, что для каждого $x \in L$ такого, что $|x| = n$ оба распределения D_x и E_x определены на множестве Σ^n.

Определение 2. Семейства распределений $\{D_x\}_{x \in L}$ и $\{E_x\}_{x \in L}$ называются статистически неразличимыми, если $\sum_{y \in \Sigma^n} |Pr_{D_x}(y) - Pr_{E_x}(y)| = \nu(n)$.

Пусть A — полиномиальный алгоритм, который на входе $y \in \Sigma^n$ выдает либо 1, либо 0.

Определение 3. Семейства распределений $\{D_x\}_{x \in L}$ и $\{E_x\}_{x \in L}$ называются полиномиально неразличимыми, если для любого полиномиального алгоритма A

$$|Pr\{A(y) = 1, y \in_{D_x} \Sigma^n\} - Pr\{A(y) = 1, y \in_{E_x} \Sigma^n\}| = \nu(n).$$

Полиномиальная неразличимость представляет собой естественное ослабление понятия статистической неразличимости: семейства распределений $\{D_x\}_{x \in L}$ и $\{E_x\}_{x \in L}$ могут иметь сильно отличающиеся статистические характеристики. Требуется только, чтобы эти различия были необнаружимы для полиномиальных алгоритмов.

Всюду в дальнейшем те алгоритмы, которые используют Алиса и Боб в процессе выполнения протоколов интерактивного доказательства, будут обозначаться через P и V соответственно. Если участник следует протоколу и выполняет предписанный протоколом алгоритм P (Алиса) или V (Боб), то такой участник называется честным. Нечестный участник может вместо P или V использовать любой другой алгоритм, который будет обозначаться через P^* и V^* соответственно. Для участников протокола интерактивного доказательства в литературе приняты также еще и следующие названия: доказывающий (Алиса) и проверяющий (Боб).

Интерактивный протокол с двумя участниками формализуется посредством интерактивной пары машин Тьюринга (P, V). Такие машины помимо своих обычных лент (входная, рабочая и т. п.) имеют еще дополнительную общую коммуникационную ленту. Интерактивные машины Тьюринга работают по очереди. Если, например, V активна, то P находится в состоянии ожидания. Очередной цикл работы завершается тем, что машина V записывает строку, называемую сообщением, на коммуникационную ленту и переходит в состояние ожидания. При этом активизируется машина P, она читает полученное сообщение, выполняет требуемые вычисления, записывает ответное сообщение на коммуникационную ленту и переходит в состояние ожидания, активизируя тем самым машину V и т. д.

Цикл работы интерактивной пары машин Тьюринга называется раундом. Другими словами, количество раундов в интерактивном протоколе — это количество сообщений, которыми обменялись участники в процессе его выполнения.

В протоколе интерактивного доказательства для языка L общим входом для машин P и V является слово $x \in \Sigma^*$ (всюду ниже чрез n мы будем обозначать его длину). Протокол завершается тем, что машина V выдает либо 1 (доказательство принято), либо 0 (доказательство отвергнуто) и останавливается. Эти события мы будем обозначать следующим образом: $\langle P, V \rangle(x) = \sigma$, $\sigma \in \Sigma$. Машина P не имеет ограничений на используемые вычислительные ресурсы, а V является вероятностной машиной Тьюринга, работающей за полиномиальное (от n) время.

Если Боб нечестный, то он может вместо предписанной протоколом машины Тьюринга V использовать любую другую полиномиальную вероятностную машину Тьюринга V^*, чтобы получить

как можно больше информации, позволяющей ему в дальнейшем самостоятельно доказывать теорему "$x \in L$". Вся информация, которую получает машина V^* в результате выполнения протокола, описывается распределением вероятностей на множестве векторов $(x, r, m_1, \ldots, m_l)$. Здесь r — случайная строка машины V^*, а $m_1, \ldots, m_l$ — сообщения, которыми обменялись P и V^* в процессе выполнения протокола. Это распределение вероятностей обозначается через $View_{V^*}(x)$.

Определение 4 [GMR]. Интерактивная пара машин Тьюринга (P, V) является доказательством с нулевым разглашением для языка L, если

1. (полнота) Для любого $x \in L$, $\langle P, V\rangle(x) = 1$.

2. (корректность) Для любой машины Тьюринга P^* и любого $x \notin L$, $Pr\{\langle P^*, V\rangle(x) = 1\} = \nu(n)$.

3. (нулевое разглашение) Для любой полиномиальной вероятностной машины Тьюринга V^* существует полиномиальная вероятностная машина Тьюринга M (моделирующая машина), которая на входе x создает распределение вероятностей $M_{V^*}(x)$ такое, что семейства $\{M_{V^*}(x)\}_{x\in L}$ и $\{View_{V^*}(x)\}_{x\in L}$ полиномиально неразличимы.

Подчеркнем, что машина M должна уметь моделировать лишь транскрипции протоколов между P и V^*, а не сами эти протоколы (в интерактивном режиме), и только для слов, принадлежащих языку L.

Если в п. 3 определения вместо полиномиальной неразличимости потребовать, чтобы семейства распределений $\{M_{V^*}(x)\}_{x\in L}$ и $\{View_{V^*}(x)\}_{x\in L}$ были статистически неразличимы, то получим определение доказательства со статистически нулевым разглашением. Чтобы отличать эти два типа протоколов между собой, те доказательства, о которых идет речь в определении 4, называют также доказательствами с вычислительно нулевым разглашением.

Как видно из определения 4, в доказательствах с вычислительно нулевым разглашением присутствует некоторая асимметрия. Безопасность Боба безусловна, т. е. какими бы вычислительными ресурсами Алиса не располагала, она может обманывать лишь с пренебрежимо малой вероятностью. В то же время безопасность Алисы основывается на предположении, что Боб не может решить некоторую гипотетически трудную вычислительную задачу. Возникает вопрос, можно ли и корректность протокола определять в таком же теоретико-сложностном стиле?

Здесь сразу же возникает техническое препятствие, поскольку, как указывалось выше, вычислительные ресурсы машины P предполагаются неограниченными. Но его можно преодолеть, несколько модифицировав модель. Пусть L — язык из класса NP, а P — полиномиальная вероятностная машина Тьюринга, которая на входной ленте, помимо слова x, получает также NP-доказательство (NP-proof — недавно предложенная замена менее удачного термина witness) принадлежности слова x языку L. Например, если L — язык ВЫПОЛНИМОСТЬ и x — булева формула, то NP-доказательством для нее будет набор значений переменных, на котором эта формула принимает значение 1.

Такая модификация позволяет переформулировать требование корректности в следующем виде:

2'. Для любой полиномиальной вероятностной машины Тьюринга P^* и любого $c > 0$ существует $n_0 = n_0(P^*, c)$ такое, что для любого $x \notin L$, $|x| \geq n_0$

$$Pr\{\langle P^*, V\rangle(x) = 1\} \leq 1/|x|^c.$$

Протоколы интерактивного доказательства, в которых корректность определяется требованием 2', получили название аргументов или вычислительно убедительных доказательств [BC], [BCC]. Отметим, что такая терминология появилась с опозданием и в пионерских работах было довольно много путаницы, когда один и тот же термин использовался для протоколов разного типа.

Итак, каждое из требований, корректности и нулевого разглашения, может быть формализовано двумя различными способами. В результате возникают 4 типа протоколов:

доказательства со статистически нулевым разглашением (самый сильный тип);

доказательства с вычислительно нулевым разглашением;

аргументы со статистически нулевым разглашением;

аргументы с вычислительно нулевым разглашением (самый слабый тип).

3. Необходимые и достаточные условия

Нас интересуют вопросы существования доказательств с нулевым разглашением каждого из четырех типов для всех языков из класса NP. При этом основное внимание уделяется следующим аспектам:

— предположение, исходя из которого построен протокол. Доказательства с нулевым разглашением строятся относительно просто, если принять предположение о вычислительной трудности

какой-либо конкретной теоретико-числовой задачи. например. задачи дискретного логарифмирования. Мы же рассматриваем вопрос о возможности построения протоколов исходя из более общего предположения о существовании односторонних функций или односторонних перестановок.

— количество раундов протокола. Этот параметр является важнейшим показателем эффективности протокола и его всегда желательно минимизировать.

— вероятность обмана со стороны нечестной Алисы (см. пп. 2 и 2' определения). Во многих работах описываются доказательства с нулевым разглашением, в которых вероятность обмана ограничена некоторой константой, скажем 1/2. Подразумевается, что такой протокол можно повторить достаточное количество раз, чтобы обеспечить сколь угодно близкую к 0 вероятность обмана. Поскольку, как отмечалось выше, нас интересует минимизация количества раундов, мы рассматриваем только такие протоколы, в которых вероятность обмана со стороны Алисы пренебрежимо мала.

Что известно о необходимых условиях существования протоколов доказательства с нулевым разглашением? Из результатов Импальяццо и Луби [IL] и Островски и Вигдерсона [OW] следует, что для существования доказательств с вычислительно нулевым разглашением, а также обоих типов аргументов с нулевым разглашением, необходимо существование односторонних функций.

Нижняя граница на количество раундов доказана только при дополнительном ограничении технического характера. Моделирующая машина называется универсальной, если она использует алгоритм V^* нечестного проверяющего как "черный ящик", т. е. не анализируя сам этот алгоритм просто подает ему на вход запросы и получает ответы. Поскольку в определении нулевого разглашения стоит квантор всеобщности по алгоритмам V^*, неясно, можно ли строить моделирующие машины, которые анализировали бы внутреннюю структуру всех таких алгоритмов. Во всяком случае, все известные доказательства с нулевым разглашением имеют универсальные моделирующие машины. Гольдрайх и Кравчик доказали следующую теорему.

Теорема 1 [GK]. Трехраундовые протоколы (любого из четырех типов), имеющие пренебрежимо малую вероятность обмана со стороны доказывающего и универсальную моделирующую машину, существуют только для языков из класса BPP.

Из этих результатов следует, что наилучший возможный вариант — это четырехраундовые протоколы, построенные исходя из предположения о существовании односторонней функции. Далее мы рассматриваем состояние исследований отдельно для каждого из четырех типов нулевого разглашения.

Доказательства со статистически нулевым разглашением. Это особый тип; именно он отсутствует в списке протоколов, для существования которых необходимо существование односторонних функций. Доказательства со статистически нулевым разглашением построены для ряда конкретных языков, например, для языков КВАДРАТИЧНЫЕ ВЫЧЕТЫ, ИЗОМОРФИЗМ ГРАФОВ, и доказательства как корректности, так и свойства нулевого разглашения для этих протоколов абсолютны, т. е. не используют никаких недоказанных предположений. Пример протокола для языка ИЗОМОРФИЗМ ГРАФОВ можно найти в [Bap]. Но для всего класса NP такие протоколы наверняка не существуют согласно результату Фортноу.

Теорема 2 [For]. Если для какого-либо NP-полного языка существует доказательство со статистически нулевым разглашением, то полиномиальная иерархия вырождается уже на втором уровне.

Доказательства с вычислительно нулевым разглашением. Такие доказательства были построены для всего класса NP Гольдрайхом, Микали и Вигдерсоном [GMW], первоначально исходя из предположения о существовании семантически стойкой криптосистемы вероятностного шифрования [GM]. В дальнейшем все специалисты стали указывать, что то же самое справедливо и в предположении существования односторонней функции, т. е. верна следующая теорема.

Теорема 3. Если существуют односторонние функции, то для всякого языка $L \in NP$ существует протокол доказательства с вычислительно нулевым разглашением.

Это утверждение стало частью "криптографического фольклора"; по-видимому ни в одной работе нет его полного доказательства. Однако, такое доказательство нетрудно получить, объединив доказательство из работы [GMW] с результатами Хостада [H], Импальяццо и др. [ILL] и Наора [Naor]. Несколько подробнее об этом говорится в следующем разделе. Что же касается количества раундов, то оно в протоколе из работы Гольдрайха и др. полиномиально от n. И снизить его, исходя хотя бы даже из предположения о существования односторонней перестановки, до сих пор никому не удалось.

Аргументы со статистически нулевым разглашением. Здесь имеется единственная работа Наора и др. [NOVY], в которой доказана следующая теорема.

Теорема 4 [NOVY]. Если существуют односторонние перестановки, то для всякого языка $L \in NP$ существует аргумент со статистически нулевым разглашением.

Количество раундов в протоколе из работы [NOVY] полиномиально от n.

Аргументы с вычислительно нулевым разглашением. Это — самый слабый из всех типов нулевого разглашения и естественно ожидать наибольшего прогресса исследований именно здесь. И в самом деле, еще в 1990 г. Файге и Шамир [FS], исходя из предположения о существовании односторонней функции, построили для любого языка из NP 5-раундовый аргумент с вычислительно нулевым разглашением. Оставался нерешенным только один вопрос, можно ли сократить количество раундов еще на единицу. Этот вопрос был решен положительно Белларом и др. [BJY].

Теорема 5 [BJY]. Если существуют односторонние перестановки, то для всякого языка $L \in NP$ существует 4-раундовый аргумент с вычислительно нулевым разглашением.

4. Доказательства и аргументы

В дальнейшем нас будут интересовать те два типа протоколов, для которых ответ на поставленный выше вопрос до сих пор неясен: доказательства с вычислительно нулевым разглашением и аргументы со статистически нулевым разглашением, которые ниже для краткости будем иногда называть просто доказательствами и аргументами соответственно.

Доказательство упоминавшейся выше теоремы Гольдрайха и др. [GMW], как и теоремы 3, состоит из двух частей. Сначала показывается, что если доказательство с нулевым разглашением существует для какого-либо NP-полного языка, то такие доказательства существуют и для всего класса NP. Это утверждение технического характера и доказывается несложно (см. [GMW]). Более интересна вторая часть теоремы, в которой предъявляется доказательство с нулевым разглашением для NP-полного языка 3-РАСКРАСКА ГРАФА.

Пусть $G = (V, E)$, $|V| = m$, — граф, для которого существует 3-раскраска. Будем считать, что каждой вершине $v \in V$ соответствует число $\phi(v) \in \{1, 2, 3\}$, ее цвет. Алиса выбирает случайную перестановку π из S_3, вычисляет $\pi(\phi(v))$ для каждой вершины $v \in V$ и посылает все числа $\pi(\phi(v))$ Бобу, но не в открытую, а в зашифрованном виде. Боб выбирает $e \in_R E$ и передает e Алисе. Тем самым он требует от нее расшифровать значения $\pi(\phi(v_1))$ и $\pi(\phi(v_2))$ для вершин v_1 и v_2, инцидентных ребру e. Если Алиса правильно отвечает на запрос, т. е. $\pi(\phi(v_1)), \pi(\phi(v_2)) \in \{1, 2, 3\}$ и $\pi(\phi(v_1)) \neq \pi(\phi(v_2))$, то Боб принимает доказательство в данном элементарном трехраундовом протоколе.

Корректность этого протокола, по существу, вытекает из следующих рассуждений. Если граф G не является 3-раскрашиваемым, то либо хотя бы одно из зашифрованных Алисой чисел не принадлежит множеству $\{1, 2, 3\}$, либо хотя бы для одного ребра $e \in E$ для инцидентных ему вершин v_1 и v_2 выполняется $\pi(\phi(v_1)) = \pi(\phi(v_2))$. В любом случае вероятность обнаружения обмана будет не меньше, чем $1/m^2$. Нетрудно показать, что полиномиального от m количества повторений данного трехраундового протокола достаточно, чтобы обеспечить пренебрежимо малую вероятность обмана со стороны нечестной Алисы.

Свойство нулевого разглашения зависит от весьма нетривиальных свойств того, что мы выше назвали "шифрованием" раскраски. Здесь, на самом деле, используется специальный криптографический примитив, называемый протоколом привязки к биту (bit commitment). В этом протоколе у Алисы изначально имеется некоторый бит b и она передает Бобу "привязку" $BC(b)$, называемую блобом (blob). Это — первый этап протокола, называемый этапом привязки. На втором этапе, этапе открытия, Алиса передает Бобу некоторую информацию, позволяющую открыть блоб, т. е. извлечь из него значение бита b. Протокол привязки к биту должен удовлетворять следующим, сформулированным пока неформально, требованиям:

1. Алиса может открыть блоб с двумя различными исходами, т. е. и как 0 и как 1, лишь с пренебрежимо малой вероятностью.

2. Боб без помощи Алисы, используя полиномиальные вероятностные алгоритмы, может самостоятельно открыть блоб лишь с пренебрежимо малой вероятностью.

Ясно, что эти требования можно формализовать. Для соответствующего определения протокола привязки к биту Наор доказал следующую теорему.

Теорема 6 [Naor]. Если существуют псевдослучайные генераторы, то существуют стойкие протоколы привязки к биту.

В работах Импальяццо и др. [ILL] и Хостада [H] псевдослучайные генераторы построены исходя из произвольной односторонней функции. Отсюда получается доказательство теоремы 3.

Сформулированные выше требования к протоколу привязки к биту асимметричны. Уверенность Боба в том, что его не обманут, безусловна, в то время как безопасность Алисы основывается на предположении, что Боб не может решить некоторую вычислительно трудную задачу, например, инвертировать одностороннюю функцию.

Существует и двойственный тип протокола привязки к биту, в котором уже безопасность Алисы безусловна, а уверенность Боба в том, что его не обманывают, основывается на некотором недоказанном предположении. Приведем для этого типа протокола формальное определение.

Пусть n — параметр безопасности и S и R — полиномиальные (от n) вероятностные алгоритмы Алисы и Боба соответственно. Алгоритмы, используемые нечестными участниками, будем обозначать через S^* и R^*. Алгоритм S^* по-прежнему полиномиальный, в то время как на вычислительные ресурсы алгоритма R^* никаких ограничений не накладывается.

На этапе привязки Алиса и Боб выполняют протокол, вообще говоря интерактивный. Если его выполнение завершается успешно, то выходом для алгоритма R будет блоб $BC(b)$. На этапе открытия блоба Алиса посылает Бобу строку $r \in \Sigma^*$ такую, что $R(BC(b), r) = b$.

Определение 5. Протокол привязки к биту называется стойким, если

1. Для любого алгоритма R^*, $Pr\{R^*(BC(b)) = b\} = 1/2 + \nu(n)$.

2. Для любого полиномиального алгоритма S^* справедливо следующее. Предположим, что этап привязки завершился успешно и к моменту его завершения алгоритм R выдал строку s, а алгоритм S^* — дополнительную строку $Hist$ (историю выполнения этого этапа). Тогда

$$Pr\{S^*(Hist, s) = (r_0, r_1) : R(s, r_0) = 0 \ \& \ R(s, r_1) = 1\} < \nu(n).$$

Подчеркнем, что алгоритм которым пользуется Боб в процессе выполнения протокола, должен быть полиномиальным. Но создаваемый при этом блоб должен быть стойким против атак противника, обладающего неограниченными вычислительными ресурсами.

Протоколы привязки к биту, стойкие в смысле этого определения, легко строятся исходя из предположений о вычислительной трудности теоретико-числовых задач, например, задачи дискретного логарифмирования. Пусть p и q — простые числа, $q|p-1$ и $g \in Z_p$ таково, что $g^q = 1 \bmod p$. Этап привязки состоит из двух шагов:

— Боб выбирает $x \in_R Z_q$, вычисляет $y = g^x \bmod p$ и посылает y Алисе.

— Алиса выбирает $r \in_R Z_q$, вычисляет блоб $BC(b) = g^r y^b \bmod p$ и посылает его Бобу.

На этапе открытия Алиса просто посылает Бобу значение r. Боб не получает на этапе привязки никакой информации о значении b, поскольку и $BC(0)$ и $BC(1)$ являются случайными элементами группы, порождаемой g. Алиса же может обманывать Боба, но только в том случае, если она вычислит дискретный логарифм числа y.

Если этот протокол использовать для построения блобов в приведенной выше общей конструкции доказательства для языка 3-РАСКРАШИВАЕМЫЕ ГРАФЫ, то в результате будет получен аргумент со статистически нулевым разглашением. Но напомним, что нас интересует возможность построения такого протокола при более общих предположениях, чем предположение о вычислительной трудности задачи дискретного логарифмирования. Эта проблема представляет интерес не только с академической точки зрения. Рассмотрим в качестве примера криптографическую задачу интерактивной аутентификации.

Для протокола аутентификации фиксируется некоторый язык L и всякий желающий, скажем Алиса, может выбрать пару (w, x), где $x \in L$, а w — NP-доказательство для x, и поместить x в общедоступный сертифицированный справочник. Слово x называется обычно открытым ключом Алисы, а слово w — ее секретным ключом. Поскольку априори известно, что все открытые ключи, хранящиеся в справочнике, принадлежат языку L, доказывать утверждение "$x \in L$" бессмысленно. На самом деле, если Алисе нужно доказать свою аутентичность Бобу, то последний выбирает из справочника открытый ключ Алисы x и требует от нее доказательство, что она знает соответствующий секретный ключ w. Такие интерактивные протоколы называются доказательствами знания (prooofs of knowledge); их отличия от рассматривавшихся до сих пор доказательств принадлежности входного слова языку L, несущественны для обсуждаемых в данной статье вопросов.

Если в протоколе аутентификации используются блобы, стойкость которых основывается на задаче дискретного логарифмирования, то, как легко понять, такой протокол не будет иметь никаких преимуществ по сравнению с протоколом доказательства знания дискретных логарифмов. В последнем протоколе Алиса выбирает пару (w, x) такую, что $x = g^w \bmod p$ и доказывает Бобу, что она

знает секретный ключ w, соответствующий данному открытому ключу x. Для доказательства знания дискретных логарифмов существуют весьма эффективные протоколы, например, протокол Шнорра, описание которого можно найти в [Вар].

Одно из важнейших направлений исследований в теоретической криптографии состоит в поиске ответа на следующий вопрос: если прогресс в области методов факторизации и дискретного логарифмирования в конце концов сделает все криптографические протоколы, основанные на этих задачах, нестойкими, то каким образом можно будет обеспечивать криптографическую защиту информации? В частности, на какой математической основе будут строиться протоколы аутентификации?

Рассматривая доказательства с нулевым разглашением как протоколы аутентификации, легко проследить принципиальные различия между доказательствами с вычислительно нулевым разглашением и аргументами со статистически нулевым разглашением. Оба типа протоколов основываются на какой-либо вычислительно трудной задаче, но используют ее по разному. В доказательствах на вычислительной сложности основывается свойство нулевого разглашения. Выполнив один раз протокол аутентификации, Боб получает транскрипцию этого протокола и в дальнейшем может автономно выполнить достаточно большой объем вычислений, пытаясь извлечь из этой транскрипции секретный ключ Алисы. В случае аргумента никакие вычислительные ресурсы не помогут Бобу это сделать. Правда в этом протоколе может обманывать Алиса, но только в том случае, если она умеет решать вычислительно трудную задачу в оперативном режиме (on-line). Аргумент может быть построен таким образом, что Боб прерывает его выполнение, если Алиса "задумалась", скажем, более, чем на 20 секунд. Таким образом, с практической точки зрения аргументы представляются более привлекательным типом протокола.

Как было указано выше, доказательство существования аргументов со статистически нулевым разглашением для всего класса NP сводится к построению протокола привязки к биту, стойкого в смысле определения 5. Долгое время сделать это, исходя из общих предположений, не удавалось, пока в 1992 г. Наор и др. не доказали следующую теорему.

Теорема 7 [NOVY]. Если существуют односторонние перестановки, то существуют протоколы привязки к биту, стойкие в смысле определения 5.

Протокол, предложенный Наором и др. имеет $O(n)$ раундов и вопрос о возможности существенного уменьшения количества раундов остается открытым. Более того, справедлива следующая теорема.

Теорема 8. Существует оракул, относительно которого существуют односторонние перестановки, но нет двухраундовых протоколов привязки к биту, стойких в смысле определения 5.

Доказательство этой теоремы основано на методах доказательства основной теоремы из работы Саймона [Sim] (утверждающей существование оракула, относительно которого существуют односторонние перестановки, но нет семейств хэш-функций с трудно обнаружимыми коллизиями) и в данных тезисах опущено.

Мы также выдвигаем гипотезу, что утверждение теоремы 8 верно для протоколов, у которых количество раундов ограничено произвольной константой.

Литература

[Вар] Варновский Н. П. Криптографические протоколы. В кн. Введение в криптографию. Ященко В. В. ред., М., МЦНМО, ЧеРо, 1998, 1999, 2000

[BC] Brassard G., Crépeau C. Non-transitive transfer of confidence: a perfect zero-knowledge interactive protocol for SAT and beyond. Proc. 27th Annual IEEE Symposium on Foundations of Computer Science, 1986, 188–195

[BCC] Brassard G., Chaum D., Crépeau C. Minimum disclosure proofs of knowledge. J. of Computer and System Sciences, Vol. 37, No 2, 1988, 156–189

[BJY] Bellare M., Jakobsson M., Yung M. Round-optimal zero-knowledge arguments based on any one-way function. EUROCRYPT'97, Lecture Notes in Computer Science, Vol 1233, 280–305

[For] Fortnow L. The complexity of perfect zero-knowledge. Proc. 19th Annual ACM Symposium on the Theory of Computing, 1987, 204–209

[FS] Feige U., Shamir A. Witness indistinguishable and witness hiding protocols. Proc. 22nd Annual ACM Symposium on the Theory of Computing, 1990, 416–426

[GK] Goldreich O., Krawczyk H. On the composition of zero knowledge proof systems. SIAM J. on Computing, Vol 25, No 1, 1996, 169–192

[GM] Goldwasser S., Micali S. Probabilistic encryption. J. of Computer and System Sciences, Vol 28, 1984, 270–299

[GMR] Goldwasser S., Micali S., Rackoff C. The knowledge complexity of interactive proof systems. SIAM J. on Computing, Vol. 18, No 1, 1989, 186–208

[GMW] Goldreich O., Micali S., Wigderson A. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. J. of ACM, Vol 38, No 1, 1991, 691–729

[H] Håstad J. Pseudorandom generators under uniform assumptions. Proc. 22nd Annual ACM Symposium on the Theory of Computing, 1990, 395–404

[IL] Impagliazzo R., Luby M. One-way functions are essential for complexity-based cryptography. Proc. 30th IEEE Symposium on Foundations of Computer Science, 1989, 230–235

[ILL] Impagliazzo R., Levin L., Luby M. Pseudorandom number generation from one-way functions. Proc. 21st Annual ACM Symposium on the Theory of Computing, 1989, 12–24

[Naor] Naor M. Bit commitment using pseudo-randomness. J. of Cryptology, Vol. 4, 1991, 151–158

[NOVY] Naor M., Ostrovsky R., Venkatesan R., Yung M. Perfect zero knowledge arguments for NP can be based on general compexity assumptions. Crypto'92, Lecture Notes in Computer Science, Vol 740, 1992, 196–214

[OW] Ostrovsky R., Wigderson A. One-way functions are essential for non-trivial zero-knowledge. Proc. 2nd Israel Symposium on Theory of Computing and Systems, IEEE Computer Society Press, 1993, 3–17

[Sim] Simon D. Finding collisions on a one-way street: can secure hash functions be based on general assumptions? EUROCRYPT'98, Lecture Notes in Computer Science, Vol. 1403, 334–345