С. О. Дорджиев, О. В. Казарин

КРИПТОГРАФИЧЕСКИЕ ПРИМИТИВЫ: ВЛОЖЕНИЯ, ПРИМЕРЫ И ОТКРЫТЫЕ ПРОБЛЕМЫ

Введение

Базовым объектом исследований в современной криптологии наряду с криптосистемами являются *криптографические протоколы*. Криптографические протоколы относятся к сравнительно новому направлению в криптографии, которое в последнее время переживает бурное развитие. Это объясняется, в том числе, переходом информационных систем различных организаций на электронный документооборот, внедрением электронных денег, современных систем электронных платежей и т. п. и связанной с этим необходимостью решения большого пула задач защиты информации.

В то же время криптографические протоколы являются весьма нетривиальным объектом исследований. Даже их формализация на сегодняшний день выглядит весьма затруднительной. Попытки формализации предпринимались во многих работах (см., например: [1—7]). Однако предлагаемые формальные модели описания криптографических протоколов верны лишь для определенных их классов. Все это представляется естественным процессом, так как, по всей вероятности, невозможно создать универсальную логику описания криптографических протоколов и доказательства их стойкости при тех или иных предположениях, условиях и ограничениях.

Неформально под *протоколом* будем понимать распределенный алгоритм, то есть совокупность алгоритмов для каждого из участников вычислений, плюс спецификации форматов сообщений, пересылаемых между участниками, плюс спецификации синхронизации действий участников, плюс описание действий при возникновении сбоев [8, 9]. Можно выделить следующие основные аспекты изучения криптографических протоколов.

Во-первых, в отличие от криптосистем, в основном решающих задачи обеспечения конфиденциальности информации, криптографические протоколы решают задачи обеспечения целостности информации и неотслеживаемости информации и участников протокола. Во-вторых, в отличие от решения проблемы обеспечения конфиденциальности информации посредством криптосистем, при построении криптографических протоколов естественным образом принимается, что участники взаимодействия в протоколе не доверяют друг другу. В-третьих, принимается, что в криптографическом протоколе могут быть два и более участника, протоколы могут быть как интерактивными, так и неинтерактивными.

Общепринятым приемом в теории алгоритмов является построение сложных алгоритмов при помощи более простых. Нечто подобное можно сделать и при построении криптографических протоколов, для которых можно (и, скорее всего, нужно) использовать некоторые простые вычислительные процедуры, корректность которых можно достаточно легко (относительно протокола) доказать.

По существу такие вычислительные процедуры являются «строительным материалом» (их еще называют криптографическими примитивами) для построения более сложных криптографических протоколов, имеющих конкретное прикладное значение. Следовательно, могут наблюдаться определенные иерархические вложения одних криптографических примитивов в другие, и, таким образом, можно говорить о некоторой разновидности иерархической композиции криптографических протоколов.

Естественно принять, что при доказательстве стойкости криптографических протоколов условие стойкости (безопасности) лежащих в их основе криптографических примитивов является необходимым, но не достаточным для доказательства стойкости самих криптографических протоколов на том или ином этапе их построения.

1. Основные понятия и определения

Основные понятия, определения и обозначения будут даваться в соответствии с работой [10]. Здесь отметим лишь следующее. В качестве одного из основных математических объектов в данной работе используются односторонние функции, то есть функции, для которых не существует эффективных алгоритмов инвертирования. Впервые такого рода функцию для конкретного криптографического приложения (открытого распределения ключей) предложили У. Диффи и М. Хеллман в работе [11]. Для функции Диффи–Хеллмана вычисление степеней в мультипликативной группе вычетов над конечным полем является простой задачей с точки зрения состава необходимых вычислений, в то время как извлечение дискретных логарифмов в этом поле — предположительно сложная вычислительная задача. Необходимо отметить, что все предлагаемые сегодня односторонние функции только предположительно являются односторонними.

Пусть $\alpha \equiv \log_g^{(\rho)}\beta$ обозначает, что α является дискретным логарифмом β по основанию g, где g — образующий группы (подгруппы) G вычетов по модулю ρ с порядком $|G|$.

Гипотеза 1.1. Любой полиномиальный алгоритм может по заданным g, β и ρ вычислить $\alpha \equiv \log_g^{(\rho)}\beta$ лишь с пренебрежимо малой вероятностью [11].

2. Используемые схемы и протоколы

2.1. Схемы привязки к биту и блобы

Схема привязки к биту позволяет участнику **A** «привязаться» к значению некоторого бита таким образом, чтобы не дать возможности участнику **B** получить какую-либо информацию о значении этого бита без своей помощи, и в то же время такая схема должна гарантировать, что участник **A** не сможет изменить значение рассматриваемого бита в процессе работы схемы.

Схема привязки к биту $\mathbf{П^Б}(r,b)$ состоит из двух протоколов (алгоритмов) — протокола собственно привязки к биту и протокола открытия бита. Пусть далее $r \in_R \{0,1\}^n$, то есть строка r выбрана случайно, с равномерным распределением вероятностей среди всех строк длины n. Для привязки к биту b участник **A** инициирует схему привязки к биту и получает по окончании ее работы пару параметров C и D. Параметр D выдается участнику **B**, в то время как C или C_b (в зависимости от значения бита привязки) хранится участником **A** в секрете. При выполнении протокола открытия бита параметр C становится известным **B**, который может единственным образом открыть бит b, предназначенный для привязки.

Определение 2.1. Схема привязки к биту $\mathbf{П^Б}(r,b)$ представляет собой пару двухсторонних протоколов (**Прив**, **Откр**) — протокола привязки к биту **Прив** и протокола открытия бита **Откр**, при реализации которых выполняются следующие условия безопасности:

Условие полноты. Для любого $b \in \{0,1\}$, любой константы $c > 0$ и для достаточно больших n вероятность

$$\mathrm{P}r((C,D,r)\mathbf{Откр} = b \leftarrow (r,b)\mathbf{Прив} = (C,D)) > 1 - n^{-c}.$$

Условие однозначности. Для всех возможных эффективных алгоритмов **Прот** (возможных действий противника), любой константы $c > 0$ и для всех достаточно больших n вероятность

$$\mathrm{P}r([(C_0,D,r)\mathbf{Откр} = 0 \;\&\; (C_1,D,r)\mathbf{Откр} = 1] \leftarrow (r^*)\mathbf{Прот} = (C_0, C_1, D)) < n^{-c},$$

где $r^* \in_R \{0,1\}^n$ — выбранный противником **Прот** случайный параметр.

Условие неразличимости. Для $\Psi_b(r) = \{(r,b)\mathbf{Прив} = (C,D)\}$ семейства случайных переменных $\{\Psi_0(r) \mid r \in \{0,1\}^*\}$ и $\{\Psi_1(r) \mid r \in \{0,1\}^*\}$ не различимы.

Свойство полноты означает, что если оба участника следуют протоколу, то он корректно завершится с вероятностью, близкой к 1. Свойство однозначности означает, что участник **A** при одном и том же значении D не может одновременно привязаться или к 0, или к 1. Свойство неразличимости говорит о том, что для всех достаточно больших r не существует способа отличить

привязку к 0 от привязки к 1, который был бы лучше, чем простое угадывание. Фактически последнее свойство означает, что мы можем разрешить участнику **B** выбор r по своему усмотрению. Но даже в этом случае вероятность обмана участника **A** участником **B** близка к 0.

Известно, что схемы привязки к биту существуют, если существуют односторонние перестановки. Приведем схему, используемую в данной работе.

Схема привязки к биту $\mathbf{П^{Б}}(\rho,b)$

Пусть ρ — простое число и q — большой простой делитель $\rho - 1$. Пусть также $g^q \equiv 1 (\mathrm{mod}\ \rho)$, $g \neq 1$. Это условие при построении в дальнейшем схемы привязки к биту является обязательным по следующей причине. В терминах теории групп каждый элемент β подгруппы G (простого порядка) группы вычетов по модулю ρ с образующим g и элементом α $(1 < \alpha < q)$, то есть элемент $\beta \equiv g^{\alpha} (\mathrm{mod}\ \rho)$, может сам служить образующим подгруппы, то есть $\beta^q \equiv 1 (\mathrm{mod}\ \rho)$. Следовательно, функцию $\beta \equiv g^{\alpha} (\mathrm{mod}\ \rho)$ следует считать односторонней перестановкой.

Протокол **Прив**

1. Участник **B** выбирает $t \in {}_{R*}Z_q$ $(t \neq 1)$ и отправляет его участнику **A**.

2. Участник **A** выбирает случайный параметр $\rho \in {}_{R*}Z_q$ и вычисляет $\beta \equiv g^{\rho} t^{b} (\mathrm{mod}\ \rho)$, где $b \in \{0,1\}$ есть выбранный для привязки бит.

3. Участник **A** отправляет β участнику **B**.

Параметры протокола: $(b)\mathbf{Прив} = (C,D)$, $C = \rho$, $D = \beta$.

Протокол **Откр**

1. Для того чтобы участник **B** убедился, что значение β действительно было привязано к биту b, он выдает запрос участнику A о передаче ему значения ρ, которое, по существу, является свидетельством правильных действий **A**.

2. Участник **A** выдает участнику **B** свидетельство ρ.

3. Участник B проверяет, выполняется ли сравнение $\beta \equiv {}^{?} g^{\rho} t^{b} (\mathrm{mod}\ \rho)$.

Параметры протокола: $(C,D)\mathbf{Откр} = (b,\{\text{«Да»},\text{«Нет»}\})$.

Чтобы доказать безопасность схемы привязки к биту, необходимо доказать, что лежащий в ее основе вычислительный примитив, именуемый *блоб* [8], обладает следующими свойствами:

1. При привязке участника **A** к блобу он фактически привязывается к биту b.

2. Нет такого блоба, посредством которого участник **A** мог бы одновременно открыть либо 0, либо 1 (или, по крайней мере, для криптографических протоколов блоб с привязкой к 0 вычислительно трудно отличить от блоба с привязкой к 1).

3. Участник **B** не получает никакой информации о том, как **A** может открыть любой неоткрытый блоб.

4. Блоб не должен нести в себе никакой информации о любом другом секрете, который желает скрыть участник **A** от участника **B**.

Безопасность схемы привязки к биту, а следовательно, и выполнение свойств блоба определяются следующей теоремой.

Теорема 2.1. В соответствии с гипотезой 1.1 и в условиях определения 2.1 схема $\mathbf{П^{Б}}$ является безопасной.

Доказательство теоремы 2.1. Для доказательства теоремы необходимо доказать выполнение условий полноты, однозначности и неразличимости.

Полнота. Условие полноты выполняется для данной схемы очевидно. В процессе выполнения протокола **Прив** участник **A** безусловно привязывается к биту b, а если оба участника следуют протоколу, то он корректно завершится с вероятностью 1.

Однозначность. Условие однозначности выполняется тогда и только тогда, когда справедлива гипотеза 1.1. В противном случае, если **A** может

извлечь логарифм ω такой, что $t \equiv g^{\omega} (\mathrm{mod}\ \rho)$, то он может найти такие ρ_0 и ρ_1, что $\rho_0 \equiv \rho_1 + \omega (\mathrm{mod}\ q)$. Таким образом, участник **A** при одном и том же значении β может по своему усмотрению открыть участнику **B** или 0, или 1 из-за того, что $t^0 g^{\rho_0} \equiv t^1 g^{\rho_1} (\mathrm{mod}\ \rho)$.

Неразличимость. Так как функция $\beta \equiv g^{\alpha} (\mathrm{mod}\ \rho)$ при указанных криптографических соглашениях является односторонней перестановкой, любой элемент из группы G может успешно использоваться как для привязки к 0, так и для привязки к 1. Это объясняется еще и тем, что параметр ρ выбран случайно, равновероятно и независимо от других событий. Поэтому участник **B** не может отличить привязку к 0 от привязки к 1. То есть неразличимость рассматривается здесь в теоретико-информационном смысле — противнику «просто не хватает» информации для нахождения отличий между привязкой к 0 и привязкой к 1. Теорема доказана.

2.2. Интерактивные системы доказательств с нулевым разглашением

В данной работе будет использоваться *интерактивная система доказательств с абсолютно нулевым разглашением* из работ [12, 13], где участник **P** доказывает участнику **V** неравенство двух дискретных логарифмов: $\log_g^{(\rho)} w \neq \log_r^{(\rho)} \gamma$, где g — образующий группы вычетов по модулю ρ.

Протокол **ДНЛ**$((w,g)(\gamma,r),\rho)$

В данном протоколе **P** доказывает, что $\log_g^{(\rho)} w \neq \log_r^{(\rho)} \gamma$. Следующие шаги выполняются в цикле l раз.

1. Участник **V** выбирает $d,e \in {}_R Z_q$, $d \neq 1$, $\beta \in {}_R\{0,1\}$. Вычисляет $a \equiv g^e\ (mod\ \rho)$, $b \equiv w^e (\mathrm{mod}\ \rho)$, если $\beta = 0$, и $a \equiv r^e\ (mod\ \rho)$, $b \equiv \gamma^e (\mathrm{mod}\ \rho)$, если $\beta = 1$. Посылает **S** значения a, b, d.

2. Участник **P** проверяет соотношение $a^u\ (mod\ \rho) \equiv b$. Если оно выполняется, то $\alpha = 0$, в противном случае $\alpha = 1$. Выбирает $R \in {}_R Z_q$, вычисляет $c \equiv d^{\alpha} g^R (mod\ \rho)$ и посылает **V** значение c.

3. Участник **V** посылает участнику **P** значение e.

4. Участник **P** проверяет, что выполняются соотношения из следующих двух их пар: $a \equiv g^e\ (mod\ \rho)$, $b \equiv w^e (\mathrm{mod}\ \rho)$ и $a \equiv r^e\ (mod\ \rho)$, $b \equiv \gamma^e (\mathrm{mod}\ \rho)$. Если да, то посылает **V** значение R. Иначе останавливается.

5. Участник **V** проверяет, что $d^{\beta} g^R (mod\ \rho) \equiv c$.

Если во всех l циклах проверка в п. 5 выполнена успешно, то участник **V** принимает доказательства участника **P**.

Безопасность этого протокола определяется следующей теоремой.

Теорема 2.2. Протокол **ДНЛ** является протоколом доказательств с абсолютно нулевым разглашением.

Доказательство теоремы 2.2. См. работы [12, 13].

2.3. Схема подписи с верификацией по запросу

В работах Д. Шаума (см., например: [14, 15]) впервые была предложена *схема подписи с верификацией по запросу*, в которой участник **V** (проверяющий подпись) не может осуществить верификацию подписи без помощи участника **S** (проставляющего подпись). Такие схемы могут эффективно использоваться в том случае, когда фирма-изготовитель поставляет потребителю некоторый информационный продукт (например, программное обеспечение) с проставленной на нем подписью указанного вида. Однако проверить эту подпись, которая гарантирует подлинность программы или отсутствие ее модификаций, можно, только уплатив за нее. После факта оплаты фирма-изготовитель дает разрешение на верификацию корректности полученных программ.

Схема состоит из трех этапов (протоколов), к которым относятся непосредственно этап генерации подписи, этап верификации подписи с обязательным участием подписывающего (протокол верификации) и этап оспаривания, если подпись или целостность подписанных данных подверглась

сомнению (отвергающий протокол **ОП**). В последнем **S** доказывает **V**, что $\log_g^{(\rho)} w \neq \log_r^{(\rho)} \gamma$. Это делается при помощи доказательства неравенства двух логарифмов, приведенного выше [12, 13].

Теорема 2.3. Отвергающий протокол **ОП** является протоколом доказательства с абсолютно нулевым разглашением.

Доказательство теоремы 2.3. См. работы [12, 13].

2.4. Конвертируемая и селективно конвертируемая схемы подписи с верификацией по запросу

В работе [16] показано, как строить *конвертируемую и селективно конвертируемую схемы подписи с верификацией по запросу*, а в работе [13] предложены такие схемы для отечественного стандарта ГОСТ Р 34.10-94.

В таких схемах открытие определенного секретного параметра некоторой схемы подписи с верификацией по запросу позволяет трансформировать последнюю в обычную схему электронной подписи. При этом открытие секретного параметра в конвертируемой схеме подписи с верификацией по запросу дает возможность верифицировать все имеющиеся и сгенерированные в дальнейшем подписи, в то время как в селективно конвертируемых схемах подписи с верификацией по запросу можно верифицировать лишь какую-либо одну подпись [16].

2.5. Конвертируемая и селективно конвертируемая схемы подписи с верификацией по запросу с распределенными доказывающими

Протокол с распределенными доказывающими — система доказательств, в которой полиномиально ограниченный доказывающий заменяется многими доказывающими, каждый из которых имеет лишь частичную информацию о доказываемом свидетельстве, принадлежащем оригинальному доказывающему. Применение таких протоколов возможно в сценарии, когда подписывающий может распределить часть своего секретного ключа подписи среди n участников так, чтобы любые t ($t < n$) из них могли в дальнейшем ее проверить.

Почти во всех областях применения схем подписи с верификацией по запросу значительной проблемой является обязательное присутствие подписывающего при верификации подписи. Следовательно, для проверяющего важно, чтобы либо подписывающий, либо агент, уполномоченный подписывающим, всегда присутствовал при этом событии. Такой агент может оказывать помощь подписывающему, так как, если последний подписывает очень много сообщений, он быстро может быть «перегружен», каждый раз верифицируя подписи. В схемах подписи с верификацией по запросу подписывающий может доверить агенту верификацию всех подписей, а если подписи являются селективно конвертируемыми, тогда агент может быть уполномочен проверять только отдельные подписи. В любом случае требуется, чтобы подписывающий безусловно доверял этому агенту.

Если подписывающий не хочет доверять одному человеку, тогда он может разрешить осуществлять процесс верификации подписи n агентам так, чтобы проверка потребовала сотрудничества, по крайней мере, t из них друг с другом. Для этого подписывающий должен распределить ключи подписи так, чтобы каждый агент мог проверить, что он получил корректные доли этих ключей, а затем дать агенту возможность проверить или оспорить подписи.

Описание конвертируемой и селективно конвертируемой схем подписи с верификацией по запросу с распределенными доказывающими и доказательство ее безопасности рассматривается в работе [17], где схема разделения секрета (и ее вариант — проверяемая схема разделения секрета) основывается на интерполяционных полиномах Шамира [18].

3. Вложения примитивов

Все приведенные выше схемы и протоколы определенным образом взаимосвязаны. Каждый из них является одним из основных элементов построения следующей в иерархии схемы или

протокола. Условно назовем их *нижестоящим* и *вышестоящим* протоколами в *иерархической композиции криптографических протоколов*. Можно также отметить, что стойкость вышестоящего протокола определенным образом зависит от стойкости нижестоящего.

Рассмотрим следующие вложения описанных в разделе 2 криптографических протоколов (схем): *Блоб* → *схема привязки к биту* → *протокол доказательства неравенства двух дискретных логарифмов* → *отвергающий протокол* → *схема подписи с верификацией по запросу* → *конвертируемая и селективно конвертируемая схема с верификацией по запросу* → *конвертируемая и селективно конвертируемая схема с верификацией по запросу с распределенными доказывающими*.

Основные элементы данных криптографических протоколов (схем).

Блоб

Протокол (параметр): параметр β протокола **Прив** схемы привязки к биту – $\mathbf{П^{Б}}$.

Стойкость: основывается на доказательстве теоремы 2.1.

Схема привязки к биту

Протокол (схема): схема привязки к биту $\mathbf{П^{Б}}$.

Стойкость: доказательство теоремы 2.1.

Протокол доказательства неравенства двух дискретных логарифмов

Протокол (схема): протокол **ДНЛ**.

Стойкость: доказательство теоремы 2.2.

Отвергающий протокол

Протокол (схема): протокол **ОП**.

Стойкость: доказательство теоремы 2.3.

Схема подписи с верификацией по запросу

Протокол (схема): схема подписи с верификацией по запросу.

Стойкость: доказательство теоремы 2.3 и других теорем из работ [12, 13].

Конвертируемая и селективно конвертируемая схема подписи с верификацией по запросу

Протокол (схема): конвертируемая схема подписи с верификацией по запросу и селективно конвертируемая схема подписи с верификацией по запросу.

Стойкость: сводится к доказательству корректности схем из работ [12, 13].

Конвертируемая и селективно конвертируемая схемы подписи с верификацией по запросу с распределенными доказывающими

Протокол (схема): схема из работы [17].

Стойкость: там же.

Таким образом, одним из приемов доказательства стойкости при построении достаточно сложных криптографических протоколов является их декомпозиция на более простые, доказательство стойкости которых может являться более простым.

4. Открытые вопросы и замечания

Если рассматривать криптографические протоколы как иерархические вложения нижестоящих протоколов в вышестоящие, то один из основных вопросов, возникающих при таком подходе, может быть следующим: «*Что является достаточным условием для доказательства стойкости криптографических протоколов (схем), в основе которых лежат более простые криптографические примитивы?*». Кроме того, естественно, встает вопрос: «*Насколько унифицированным должен быть математический аппарат описания криптографических схем (протоколов) и их вложений?*».

Например, все рассмотренные в данной работе протоколы (схемы) основаны на вычислениях в мультипликативной группе (подгруппе) вычетов по модулю большого простого числа, а стойкость предложенных схем основывается на гипотезе о существовании односторонней функции дискретного экспоненцирования. В то же время проверяемая схема разделения секрета, используемая для построения схемы подписи с верификацией по запросу с распределенными доказывающими, основывается на вычислениях над полиномами в поле вычетов по модулю большого простого числа.

И, наконец, остается открытым и следующий вопрос: «*Каковы вообще пути доказательства стойкости сложных криптографических протоколов, кроме доказательства стойкости при их декомпозиции на более простые, и, в целом, является ли декомпозиция неким универсальным приемом при таком доказательстве?*».

Заключение

В данной работе предпринята попытка исследования некоторых аспектов построения криптографических протоколов. Реализация принципа иерархической композиции/декомпозиции (иерархических вложений) криптографических протоколов может стать хорошим инструментом как для их эффективного построения, так и для доказательства стойкости протоколов и безопасности криптографических схем в целом.

В работе приводятся криптографические протоколы, реализующие идею схем подписи с верификацией по запросу и их разновидностей. Лежащие в их основе криптографические примитивы, такие как блоб, схема привязки к биту, интерактивные системы доказательств с нулевым разглашением и др., имеют свое самостоятельное значение и свой достаточно развитый математический аппарат для доказательства их стойкости. Это значит, что при построении новых криптографических протоколов с использованием известных примитивов может не понадобиться «изобретать велосипед» для доказательства их стойкости, а значит, можно существенно сократить время и избежать многих ошибок, типовых и рутинных процедур при доказательстве безопасности различных криптографических конструкций.

Для решения проблемы доказательства стойкости произвольной композиции протоколов, по мнению авторов, можно использовать модель с *определениями безопасности симуляцией в неизвестном окружении*, например *гибридную модель Канетти – hybrid UC-модель* (*universally composable model*) [19]. В данной модели изначально заложен модульный принцип доказательства стойкости протоколов [20], а само доказательство проводится через доказательство эквивалентности идеальной и реальной функциональности (см., например, аналог из работы [21]).

СПИСОК ЛИТЕРАТУРЫ:

1. *Backes M., Pfitzmann B., Waidner M.* A universally composable cryptographic library. URL: http://citeseer.ist.psu.edu (дата обращения: 17.12.13).
2. *Berger R., Kannan S., Peralta R.* A framework for study of cryptographic protocols // Lecture Notes in Computer Science. Advances in Cryptology – CRYPTO'85. V. 218. P. 87–103.
3. *Boulton P. I. P., Lee E. S., Thompson B., Soper R. E.* Authentication in secure local area network // Decentralized Systems. M. Cosnant & C. Girault. Elsevier Sciences Publishers B. V. (North-Holland). 1990. P. 41–53.
4. *Burrows M., Abadi M., Needham R. M.* A logic of authentication // Proc. R. Soc. Lond. A 426. 1989. P. 233–271.
5. *Lincoln P., Mitchell J., Mitchell M., Scedrov A.* Probabilistic polynomial-time equivalence and security analysis. URL: http://citeseer.ist.psu.edu (дата обращения: 17.12.13).
6. *Mateus P., Mitchell J., Scedrov A.* Composition of cryptographic protocols in a probabilistic polynomial-time process calculus. URL: http://citeseer.ist.psu.edu (дата обращения: 17.12.13).

7. *Needham R. M., Schroeder M. D.* Using encryption for authentication in large networks of computers // Commun. ACM. 1978. V. 21. № 12. P. 993–999.
8. *Варновский Н. П.* Криптографические протоколы // Введение в криптографию / Под общ. ред. В. В. Ященко. М.: МЦНМО, 2012. С. 44–88.
9. *Казарин О. В.* Методология защиты программного обеспечения. М.: МЦНМО, 2009. – 464 с.
10. *Казарин О. В.* Интерактивная проверяемая схема разделения секрета // Безопасность информационных технологий. 2010. № 3. С. 35–40; 2011. № 1. С. 61–67.
11. *Diffi W., Hellman M. E.* New direction in cryptography // IEEE Transactions on Information Theory. 1976. V. IT-22. № 11. P. 644–654.
12. *Казарин О. В.* О доказательстве безопасности схемы подписи с верификацией по запросу // Безопасность информационных технологий. 1997. № 1. С. 58–62.
13. *Казарин О. В.* Конвертируемые и селективно конвертируемые схемы подписи с верификацией по запросу // Автоматика и телемеханика. 1998. № 6. С. 178–188.
14. *Chaum D.* Zero-knowledge undeniable signatures // Lecture Notes in Computer Science. Advances in Cryptology – EUROCRYPT'91. V. 547. P. 458–464.
15. *Chaum D., van Antverpen H.* Undeniable signature // Lecture Notes in Computer Science. Advances in Cryptology – CRYPTO'89. V. 435. P. 212–216.
16. *Boyar J., Chaum D., Damgard I., Pedersen T.* Convertible undeniable signature // Lecture Notes in Computer Science. Advances in Cryptology – CRYPTO'90. V. 537. P. 189–205.
17. *Pedersen T. P.* Distributed provers with applications to undeniable signatures // Advances in Cryptology – EUROCRYPT'91. Proceedings. Springer-Verlag LNCS. V. 547. P. 221–242.
18. *Shamir A.* How to share a secret // Communication of ACM. 1979. V. 22 (11). P. 612–613.
19. *Canetti R.* Universally composable security: a new paradigm for cryptographic protocols // Lecture Notes in Computer Science. 42nd Foundation of Computer Sciences Conference. 2001. P. 136–145.
20. *Прокопьев С. Е.* Поиск упрощенной модели протоколов инфраструктуры цифровой подписи с использованием верификаторов моделей // Прикладная дискретная математика. 2009. № 1 (3). С. 79–92.
21. *Казарин О. В.* Разработка моделей и методов проактивной защиты информационных систем на основе конфиденциальных вычислений // Вопросы защиты информации. 2013. № 3. С. 68–80.