

Федеральное государственное автономное образовательное учреждение высшего образования
Национальный исследовательский ядерный университет «МИФИ»

Кафедра «Криптология и кибербезопасность»

Криптографические протоколы

курс лекций

*Запечников Сергей Владимирович,
профессор кафедры «Криптология
и кибербезопасность» НИЯУ МИФИ*

Москва – 2018

Криптографические протоколы

курс лекций

Лекция 1. **Вероятностные доказательства**

05 февраля 2018 г.

Интерактивные системы доказательства (1)

Интерактивная система доказательства (*interactive proof system*) – протокол, включающий двух участников: *доказывающего* (*prover* – P) и *проверяющего* (*verifier* – V). Предварительно формулируется некоторое утверждение S , например, утверждение о том, что некоторый объект w обладает свойством L : $w \in L$. В ходе протокола P и V обмениваются сообщениями. Каждый из них может генерировать случайные числа и использовать их в своих вычислениях. В конце протокола V должен вынести свое окончательное решение о том, является ли S истинным или ложным.

Цель участника P всегда заключается в том, чтобы убедить участника V в том, что S истинно, независимо от того, истинно ли оно на самом деле или нет. Таким образом, P может мошенничать в протоколе, так как S может быть ложно, т.е. он может быть активным противником. V должен проверять аргументы участника P . Цель участника V заключается в том, чтобы вынести решение, является ли S истинным или же ложным, то есть интересы участников протокола P и V не совпадают.

Интерактивные системы доказательства (2)

Однако участник V имеет полиномиально ограниченные вычислительные возможности, а именно время его работы ограничено некоторым полиномом от длины доказываемого утверждения: $t \leq p(|w|)$. Это предположение является стандартным для моделирования вычислительных возможностей обычных средств вычислительной техники. В силу этого он самостоятельно, без помощи P , не способен распознать истинность утверждения S .

Вычислительные возможности P никак не ограничиваются, что в действительности может соответствовать ситуации, когда P владеет какой-то трудно получаемой информацией (хотя он может и обманывать, утверждая, что такая информация у него имеется).

Программа действий участника V должна быть устроена таким образом, чтобы:

- 1) если S истинно, P смог бы убедить V признать это;
- 2) если S ложно, P не смог бы убедить V в противном, какие бы аргументы он ни выдвигал, т.е. вне зависимости от получаемых от P сообщений.

V может ошибаться, но ставится условие, чтобы вероятность принятия им неправильного решения была бы пренебрежимо мала.

Пример интерактивной системы доказательства, основанной на задаче теории чисел (1)

Зададимся натуральным числом n . Рассмотрим мультипликативную группу $Z_n^* = \{x < n; (x, n) = 1\}$. Обозначим $QR = \{(x, n) \mid x < n, (x, n) = 1, \exists y : y^2 \equiv x \pmod n\}$ – множество квадратичных вычетов числа n . Напомним, что если сравнение $y^2 \equiv x \pmod n$ имеет решение, то x называется квадратичным вычетом числа n . В противном случае x называется квадратичным невычетом. Тогда $L = QNR = \{(x, n) \mid x < n, (x, n) = 1, \nexists y : y^2 \equiv x \pmod n\}$ – множество квадратичных невычетов числа n . P доказывает V утверждение $S : (x, n) \in QNR$.

Задача распознавания квадратичных вычетов не решается за полиномиальное время. В силу этого проверяющий, полиномиально ограниченный в своих вычислительных ресурсах, не может самостоятельно проверить истинность сформулированного утверждения.

Пример интерактивной системы доказательства, основанной на задаче теории чисел (2)

	P		V
1		←	<p>Для $i = \overline{1, k}, k = n$ выбирает:</p> <p>$b_i \in \{0, 1\}$ – случайный бит, $z_i \in Z_n^*$ и вычисляет (w_1, \dots, w_k), где</p> $w_i = \begin{cases} z_i^2 \pmod{n}, & \text{если } (b_i = 1) \\ x \cdot z_i^2 \pmod{n}, & \text{если } (b_i = 0) \end{cases}$
2	<p>Для $i = \overline{1, k}$ вычисляет (c_1, \dots, c_k), где</p> $c_i = \begin{cases} 1, & \text{если } (w_i, n) \in QR \\ 0, & \text{если } (w_i, n) \notin QR \end{cases}$	→	
3			<p>Принимает доказательство тогда и только тогда, когда для $\forall (i = \overline{1, k})$ $c_i = b_i$.</p>

Свойства интерактивной системы доказательства (1)

Утверждение 1. Для $\forall x \in QNR$ если $(x, n) \in QNR$, т.е. $\exists y: y^2 \equiv x \pmod{n}$, то P докажет V утверждение S с вероятностью, равной 1.

Доказательство: Рассмотрим действия участника V на шаге (1) протокола.

Когда $b_i=1$, по условию протокола $\exists z_i: z_i^2 \equiv w_i \pmod{n}$. По определению вычета это означает, что $(w_i, n) \in QR$, т.е. w_i является квадратичным вычетом числа n .

Когда $b_i=0$, по условию протокола $z_i^2 \cdot x \equiv w_i \pmod{n}$. Из доказываемого утверждения известно, что $(x, n) \in QNR$. Может ли w_i быть квадратичным вычетом

числа n ? Для этого должно быть: $\left(z_i \cdot x^{\frac{1}{2}} \right)^2 \equiv w_i \pmod{n}$. Это может быть, только если $x=1$. Но $(1, n) = 1$. Кроме того, $\exists y=1: y^2 \equiv 1 \pmod{n}$. Следовательно, $(1, n) \in QR$ – мы пришли к противоречию с исходным утверждением.

Следовательно, $b_i=0$ тогда и только тогда, когда $(w_i, n) \in QNR$, т.е. мы установили однозначную связь: w_i является квадратичным вычетом числа n только при $b_i=1$. Распознавая QR на шаге (2) протокола (эту задачу нельзя решить за полиномиальное время), доказывающий P будет отвечать битом $c_i=1$ тогда и только тогда, когда $b_i=1$, т.е. на шаге (3) результат проверки всегда будет положительным, и V всегда примет доказательство.

Свойства интерактивной системы доказательства (2)

Утверждение 2. Для $\forall x$ если $(x, n) \notin QNR$, то вероятность ошибки V составляет

$$P_V^{ош} = \frac{1}{2^k}.$$

Доказательство:

Когда $b_i=1$, по условию протокола $\exists z_i : z_i^2 \equiv w_i \pmod{n}$. По определению вычета это означает, что $(w_i, n) \in QR$, т.е. w_i является квадратичным вычетом числа n .

Когда $b_i=0$, по условию протокола $w_i \equiv x \cdot z_i^2 \pmod{n}$. Если $(x, n) \notin QNR$, т.е. $(x, n) \in QR$, то $(x, n) = 1, \exists y : y^2 \equiv x \pmod{n}$. Тогда можно записать, что $w_i \equiv y^2 \cdot z_i^2 \pmod{n}$, или, что то же самое, $w_i \equiv (y \cdot z_i)^2 \pmod{n}$. Значит, $\exists v = y \cdot z_i : v^2 \equiv w_i \pmod{n}$, т.е. $(w_i, n) \in QR$. Итак, w_i – случайный квадратичный вычет числа n .

В любом случае: $b_i=0$ или $b_i=1$ – участник P на шаге (2) протокола всегда будет распознавать число w_i как квадратичный вычет числа n . Следовательно, он может угадать, какой бит $b_i = \{0,1\}$ был выбран, только случайно, с вероятностью $P = \frac{1}{2}$.

Следовательно, все k бит $\{b_1, \dots, b_k\}$ он сможет угадать лишь с вероятностью $P = 2^{-k} \xrightarrow{k \rightarrow \infty} 0$.

Пример интерактивной системы доказательства, основанной на задаче теории графов (1)

Графы G_0 и G_1 называются изоморфными, т.е. $G_0 \approx G_1$, если существует взаимно однозначное соответствие между их вершинами, при котором соединенным ребром вершинам в графе G_0 соответствуют соединенные вершины в графе G_1 .

Задача проверки изоморфности графов не решается за полиномиальное время.

Не упрощая задачи, можно предполагать, что G_0 и G_1 – графы на одном и том же множестве вершин N мощности m : $|N| = m$. $L = GNI = \{(G_0, G_1) \mid \forall G_0 \neq G_1\}$ – множество пар неизоморфных графов. P доказывает V утверждение $S = (G_0, G_1) \in GNI$.

Пример интерактивной системы доказательства, основанной на задаче теории графов (2)

	<i>P</i>		<i>V</i>
1			<p>Для $i = \overline{1, m}$ берет $\alpha_i \in \{0, 1\}$ – случайный бит, создает изоморфную копию $G_{\alpha_i}' \approx G_{\alpha_i}$ путем случайной перестановки вершин:</p> <p style="text-align: center;">←</p> $G_{\alpha_i}' = \{(\pi(u), \pi(v)) \mid (u, v) \in E_{\alpha_i}\}$
2	<p>Для $i = \overline{1, m}$ вычисляет $\beta_i \in \{0, 1\}$ так, что:</p> $\begin{cases} \beta_i = 0, \text{ если } (G_{\alpha_i}' \approx G_0), \\ \beta_i = 1, \text{ если } (G_{\alpha_i}' \approx G_1), \\ \beta_i - \text{случ.}, \text{ если } (G_0 \approx G_1), \\ \beta_i = 0, \text{ если } \begin{pmatrix} G_{\alpha_i}' \neq G_0, \\ G_{\alpha_i}' \neq G_1 \end{pmatrix}, \end{cases}$ <p>травляет β_i проверяющему</p>	→	
3			<p>Принимает доказательство тогда и только тогда, когда все биты совпали: для $\forall \alpha = \overline{1, m} \beta_i = \alpha_i$.</p>

Свойства интерактивных доказательств

Протокол между участниками P и V называется *интерактивным доказательством* для языка L , если V полиномиально ограничен, и выполнены следующие два условия:

1) для $\forall x \in L$ $P\{(P, V)_{(x)} = 1\} \geq 1 - \frac{1}{2^{n^c}}$, где $C = \text{Const.}$, n – число раундов протокола (т.е. вероятность принятия проверяющим доказательства истинного утверждения стремится к единице);

2) для $\forall x \in L$ и для $\forall P' \neq P$ (для любого другого участника, который действует не так, как честный участник) вероятность принятия проверяющим доказательства ложного утверждения исчезающе мала, т.е. $P\{(P', V)_{(x)} = 1\} \leq \frac{1}{2^{n^c}}$.

Условие 1 называется *полнотой* (completeness), условие 2 – *корректностью* (soundness) доказательства. Класс языков, обладающих интерактивными системами доказательства, обозначается IP .

Теорема. (A. Shamir, A. Shen, 1990) $IP = PSPACE$, т.е. класс задач, обладающих интерактивными системами доказательства, совпадает с классом задач, решаемых с полиномиальным объемом памяти.

Доказательства с нулевым разглашением знания: постановка задачи (1)

Пусть задана интерактивная система доказательства $\langle P, V, S \rangle$. В определении интерактивной системы доказательства ранее не предполагалось, что V может быть противником (предполагалась только возможность существования нечестного участника P'). Но V может оказаться противником, который хочет выведать у P какую-либо новую полезную информацию об утверждении S . В этом случае P может не хотеть, чтобы это случилось в результате работы протокола интерактивной системы доказательства $\langle P, V, S \rangle$. Таким образом приходим к идее протокола доказательства с *нулевым разглашением знания* (zero-knowledge proof). Нулевое разглашение знания подразумевает, что в результате работы протокола интерактивной системы доказательства V не увеличит свои знания об утверждении S , или, другими словами, не сможет извлечь никакой информации о том, почему S истинно.

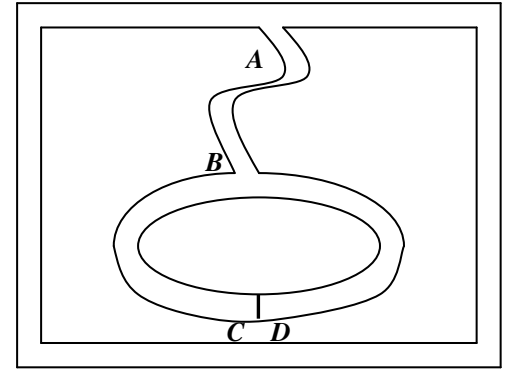
Как и ранее, в протоколе предварительно формулируется некоторое утверждение S , например, о том, что некоторый объект w обладает свойством L : $w \in L$. В ходе протокола P и V обмениваются сообщениями. Каждый из них может генерировать случайные числа и использовать их в своих вычислениях. В конце протокола V должен вынести свое окончательное решение о том, является ли S истинным или ложным.

Доказательства с нулевым разглашением знания: постановка задачи (2)

Цель P всегда состоит в том, чтобы убедить V в том, что S истинно, независимо от того, истинно ли оно на самом деле или нет, т.е. P может быть активным противником, а задача V – проверять аргументы P . Цель участника V заключается в том, чтобы вынести решение, является ли S истинным или же ложным. Как и ранее, V имеет полиномиально ограниченные вычислительные возможности, а именно время его работы ограничено некоторым полиномом от длины доказываемого утверждения: $t \leq p(|w|)$. В силу этого он самостоятельно, без помощи P , не способен распознать истинность высказывания S . Вычислительные возможности P никак не ограничиваются.

«Задача о пещере Али-Бабы»

Это модельная задача, наглядно иллюстрирующая суть доказательств с нулевым разглашением знания. Имеется пещера, план которой показан на рисунке. Пещера имеет дверь с секретом между точками C и D . Каждый, кто знает волшебные слова, может открыть эту дверь и пройти из C в D или наоборот. Для всех остальных оба хода пещеры ведут в тупик.



Пусть P знает секрет пещеры. Он хочет доказать V знание этого секрета, не разглашая волшебные слова. Вот протокол их общения.

1. V находится в точке A .
2. P заходит в пещеру и добирается либо до точки C , либо до точки D .
3. После того, как P исчезает в пещере, V приходит в точку B , не зная, в какую сторону пошел P .
4. V зовет P и просит его выйти либо из левого, либо из правого коридора пещеры согласно желания V .
5. P выполняет это, открывая при необходимости дверь, если, конечно, он знает волшебные слова.
6. P и V повторяют шаги (1) – (5) n раз.

Если P не знает секрета двери, вероятность того, что V попросит его выйти из того же коридора, в который он вошел, равна $\frac{1}{2}$. После n раундов вероятность сократится до $\frac{1}{2^n}$.

Протокол доказательства изоморфизма графов

P хочет доказать V изоморфизм графов G_0 и G_1 . Пусть $G_1 = \varphi(G_0): G_0 \approx G_1$, где φ - преобразование изоморфизма. m – мощность множества N вершин графов.

	P		V	
1	π - случайная перестановка вершин, вычисляет $H = \pi G_1$	\rightarrow		} m раз
2		\leftarrow	$\alpha = \{0,1\}$ -случ.	
3	Посылает преобразование ψ , такое что: $\psi = \begin{cases} \pi, & \text{если } (\alpha = 1), \\ \pi \circ \varphi, & \text{если } (\alpha = 0). \end{cases}$	\rightarrow		
4			Вычисляет граф ψG_α и сравнивает: $H \stackrel{?}{=} \psi G_\alpha$.	
5			Принимает доказательство тогда и только тогда, когда для $\forall m \ H^{(m)} = \psi G_\alpha^{(m)}$.	

Протокол доказательства знания дискретного логарифма

Перед началом работы протокола задаются открытые величины: p, q – простые числа, такие, что $q|(p-1)$, элемент $g \in Z_p^*$, число X . Доказывающему P известна секретная величина $x: x \in Z_q, g^x = X$, знание которой он должен доказать V , не разглашая самой секретной величины.

	P		V
1	$r \in_R Z_q$ $M = g^r \pmod{p}$	\rightarrow	
2		\leftarrow	$R \in_R Z_q$
3	$m = r + xR \pmod{q}$	\rightarrow	
4			$g^m \stackrel{?}{=} X^R \cdot M \pmod{p}$

Протокол доказательства знания представления числа в базисе

Перед началом работы протокола задаются открытые величины, известные всем участникам: простые числа p, q , элементы $y, g_1, g_2, \dots, g_k \in G_q$. Доказывающему P известны секретные величины $\alpha_1, \alpha_2, \dots, \alpha_k \in Z_q : y = g_1^{\alpha_1} \cdot g_2^{\alpha_2} \dots \cdot g_k^{\alpha_k}$, знание которых он должен доказать V , не разглашая самих этих величин.

	P		V
1	$r_1, r_2, \dots, r_k \in_R Z_q$ $M = g_1^{r_1} \cdot g_2^{r_2} \cdot \dots \cdot g_k^{r_k}$	→	
2		←	$R \in_R Z_q$
3	$m_i = r_i + \alpha_i R, i = \overline{1, k}$	→	
4			$g_1^{m_1} \cdot g_2^{m_2} \cdot \dots \cdot g_k^{m_k} \stackrel{?}{=} y^R \cdot M$

Доказательство знания представления множества чисел в соответствующих базисах

Перед началом работы протокола задаются открытые величины, известные всем участникам: простые числа p, q , элементы $y^{(j)}, g_1^{(j)}, g_2^{(j)}, \dots, g_k^{(j)} \in G_q$ для некоторых (j) . Доказывающему P известны секретные величины $\alpha_1, \alpha_2, \dots, \alpha_k \in Z_q$, такие, что для $\forall j$ $y^{(j)} = (g_1^{(j)})^{\alpha_1} \cdot (g_2^{(j)})^{\alpha_2} \cdot \dots \cdot (g_k^{(j)})^{\alpha_k}$, знание которых он должен доказать V , не разглашая самих этих величин.

	P		V
1	$r_1, r_2, \dots, r_k \in_R Z_q, \text{ для } \forall j$ $M^{(j)} = (g_1^{(j)})^{r_1} \cdot (g_2^{(j)})^{r_2} \cdot \dots \cdot (g_k^{(j)})^{r_k}$	→	
2		←	$R \in_R Z_q$
3	$m_i = r_i + \alpha_i R, i = \overline{1, k}$	→	
4			для $\forall j$ $(g_1^{(j)})^{m_1} (g_2^{(j)})^{m_2} \cdot \dots \cdot (g_k^{(j)})^{m_k} \stackrel{?}{=} \stackrel{?}{=} (y^{(j)})^R \cdot M^{(j)}$

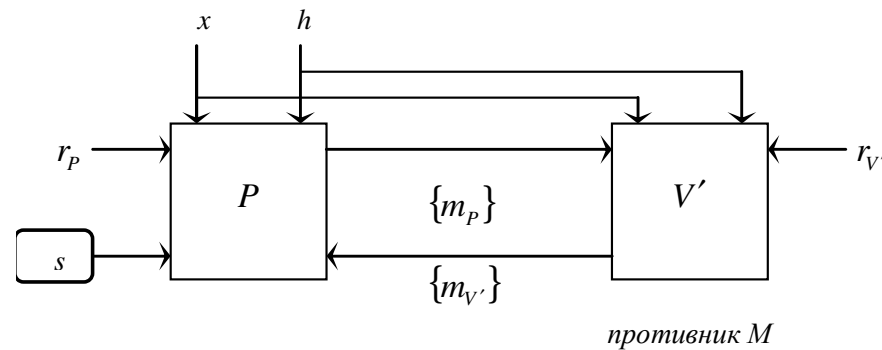
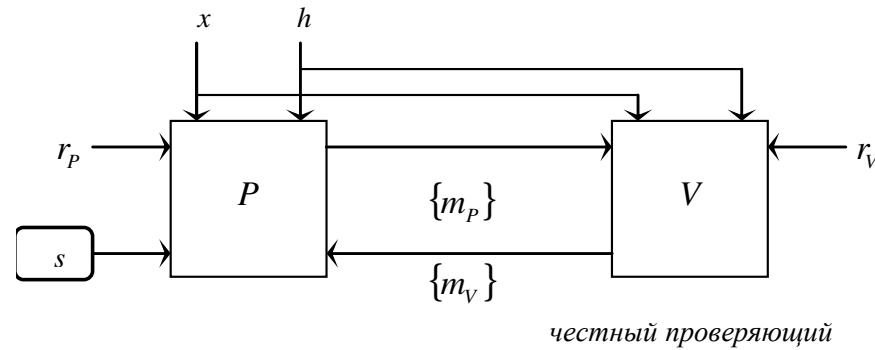
Структура протоколов доказательства с нулевым разглашением

В общем виде протокол интерактивного доказательства с нулевым разглашением состоит из четырех шагов:

- доказывающий передает проверяющему W – результат вычисления однонаправленной функции от секретной величины, знание которой он доказывает;
- проверяющий посылает ему случайный запрос;
- доказывающий отвечает на этот запрос, причем ответ зависит как от случайного запроса, так и от секретной величины, но из него вычислительно невозможно получить эту секретную величину;
- получая ответ, V проверяет его соответствие величине, переданной на первом шаге.

	P	$S : x \in L$ – доказываемое утверждение, h – др. общедоступные параметры и величины, s – секретные данные доказывающего о том, почему S истинно, r – случ. число	V
1	r_P – случ., $W = f_1(x, r_P)$	\rightarrow	
2		\leftarrow	r_V – случ., $C = f_2(r_V)$
3	$R = f_3(C, x)$	\rightarrow	
4			? $R \approx W$

Свойства доказательств с нулевым разглашением знания (1)



Пусть $\{m_P\}, \{m_V\}$ – совокупность всех сообщений, передаваемых от P к V (соответственно от V к P), каждое из которых является случайной величиной, и таким образом, $\{x, h, r_V, \{m_P\}, \{m_V\}\} = \text{view}_{P,V}(x, h)$ – это ансамбль случайных величин протокола, наблюдаемых извне (внешним наблюдателем), $\{x, h, r_{V'}, \{m_P\}, \{m_{V'}\}\} = M_{V'}(x, h)$ – это ансамбль случайных величин, получаемых в результате работы полиномиального моделирующего алгоритма (simulator), который выполняется внешним наблюдателем (противником) самостоятельно.

Свойства доказательств с нулевым разглашением знания (2)

Если величины $view_{P,V}(x,h) \stackrel{c}{\approx} M_{V'}(x,h)$ вычислительно неразличимы за полиномиальное время (т.е. не существует никакого алгоритма, который за полиномиальное время мог бы распознать эти два ансамбля случайных величин), то говорят, что протокол обеспечивает **вычислительно нулевое разглашение знания** (computationally zero-knowledge).

Если величины $view_{P,V}(x,h) \approx M_{V'}(x,h)$ одинаково распределены над множеством случайных величин, то говорят, что протокол обеспечивает **абсолютно нулевое разглашение знания** (perfect zero-knowledge).

Система $\langle P, V, S \rangle$ называется **интерактивной системой доказательства с нулевым разглашением знания** для языка L , если она:

- 1) является интерактивной системой доказательства для языка L (т.е. обладает свойствами полноты и корректности);
- 2) обладает свойством нулевого разглашения знания.

Теорема 1. (Goldreich O., Krawchuk H.) Последовательное выполнение двух протоколов с нулевым разглашением знания является протоколом с нулевым разглашением знания.

Теорема 2. (Goldreich O., Krawchuk H.) Параллельное выполнение протоколов с нулевым разглашением знания не обязательно приводит к протоколу с нулевым разглашением знания.

Другие виды вероятностных доказательств

Среди всех протоколов доказательства с нулевым разглашением знания выделяют класс протоколов *доказательства знания* (*proof of knowledge*).

Например, доказательство знания чисел p , q , таких, что $p \cdot q = n$ есть доказательство знания, но доказательство того, что n – составное число, доказательством знания не является – это так называемое *доказательство обладания* (*proof of possession*).

Но доказательство знания не обязательно должно быть доказательством с нулевым разглашением знания, так как можно просто сообщить секрет другой стороне протокола: при этом сообщивший докажет знание секрета, но тем самым разгласит секрет. В различных приложениях криптографии, в частности, в протоколах аутентификации и в схемах электронных платежей, встречаются протоколы *доказательства знания с нулевым разглашением знания* (*zero-knowledge proof of knowledge* – *ZKPK*). Существуют специальные разновидности протоколов доказательства знания с нулевым разглашением знания: протоколы группового и «скрытого» доказательства знания и др.

Неинтерактивные доказательства с нулевым разглашением (*non-interactive zero-knowledge proofs*) – однораундовые протоколы доказательства с нулевым разглашением, в которых доказывающий формирует, а проверяющий проверяет доказательство, пользуясь общей ссылочной строкой (*common reference string*), которая служит заменой случайного запроса проверяющего к доказывающему на шаге (2) обычного интерактивного протокола.

**Протоколы аутентификации, основанные
на доказательствах с нулевым разглашением
знания**

Цель и требования к протоколам аутентификации

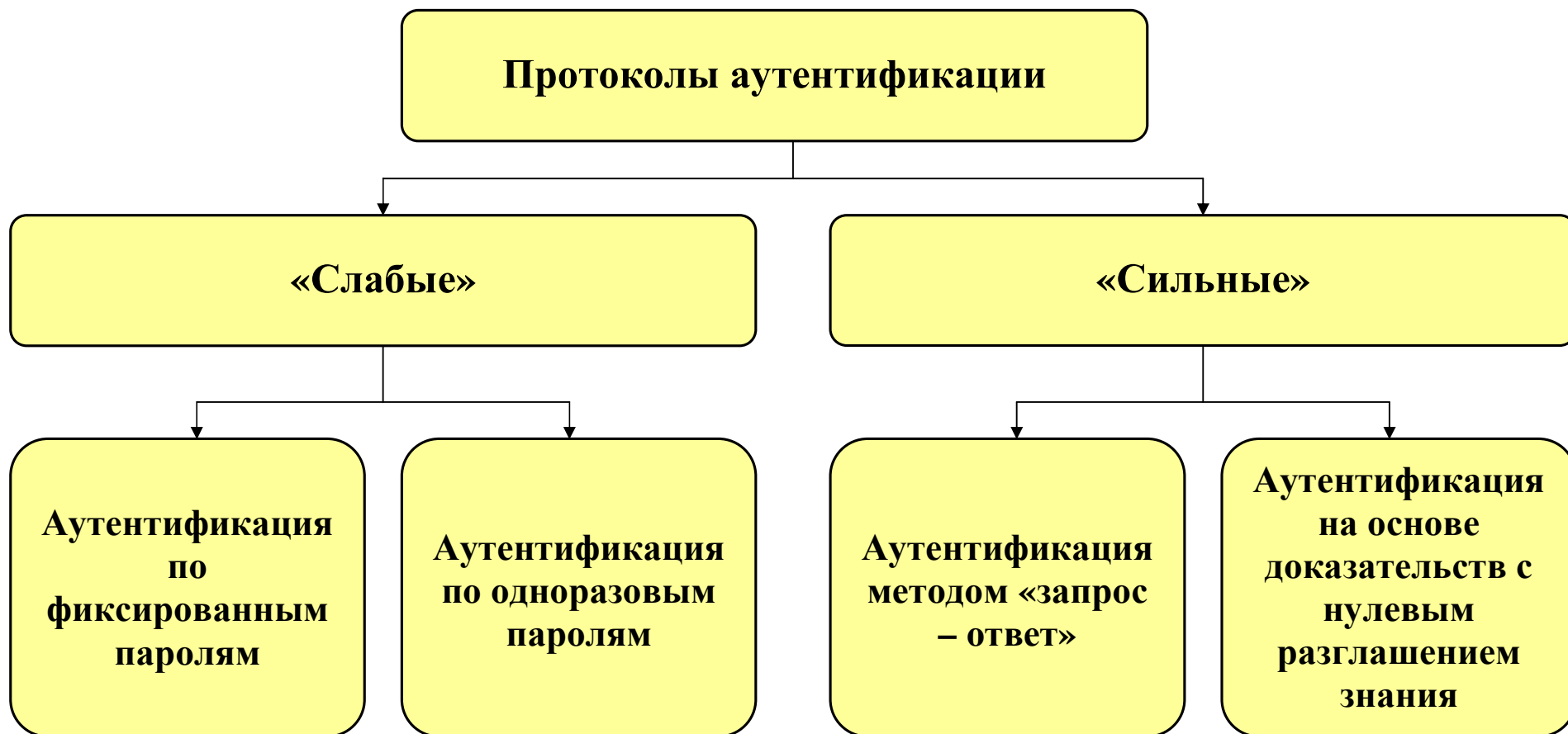
Участники протокола: *претендент* P и *проверяющий* V .

Цель проверяющего V в протоколе аутентификации заключается в том, чтобы подтвердить идентичность претендента, т.е. что он в самом деле является P , а не кем-то иным. Выбор происходит из конечного множества лиц – зарегистрированных участников системы.

Требования к протоколу аутентификации:

- 1) если P и V являются честными, V завершит протокол, приняв идентичность P ;
- 2) V не может повторно использовать протокол, совершенный с P , для того, чтобы успешно деперсонифицировать P в протоколе с третьей стороной M ;
- 3) вероятность того, что любая сторона M , отличная от P , проведя протокол и играя роль P , может заставить V завершить протокол с принятием идентичности P , пренебрежимо мала;
- 4) предыдущие свойства остаются справедливыми, даже если между P и V совершено большое, но полиномиально ограниченное число сеансов протокола аутентификации, противник M участвовал в предыдущих сеансах выполнения протокола, и несколько сеансов могли выполняться одновременно.

Классификация протоколов аутентификации



Общие положения

Общая идея протоколов аутентификации, основанных на доказательствах с нулевым разглашением знания, состоит в том, что законный пользователь P , имеющий открытый и секретный ключи, и проверяющий V выполняют совместный криптографический протокол интерактивного доказательства, в процессе которого P , выступающий в роли претендента, должен доказать свою подлинность. Для этого он должен продемонстрировать знание секретного ключа, но не разгласить его для проверяющего V , т.е. из информации, полученной V , ему вычислительно невозможно получить секретный ключ P .

Все протоколы имеют два этапа: *предварительный* и *рабочий*. На предварительном, который выполняется однократно, специфицируются некоторые параметры и вырабатываются величины, участвующие в рабочем этапе протокола, в частности, открытые и секретные ключи P . На рабочем этапе собственно выполняется доказательство аутентичности P .

Протокол аутентификации Фиата – Шамира

Предварительный этап			
	<i>P</i>	<i>Центр доверия</i>	<i>V</i>
	$s: (s, n) = 1, 1 \leq s \leq n - 1$ $v = s^2 \pmod{n}$	p, q – большие простые числа, $n = pq$	
n, v			
Рабочий этап			
	<i>P</i>		<i>V</i>
1	$r \in_R \{1, 2, \dots, n - 1\}$ $x = r^2 \pmod{n}$	→	
2		←	$e \in_R \{0, 1\}$
3	$y = rs^e \pmod{n}$	→	
4			Если ($y=0$), отклоняет доказательство, так как $r=0$. В противном случае: $y^2 \stackrel{?}{\equiv} xv^e \pmod{n}$

Стойкость протокола

Рассмотрим подробнее структуру этого протокола. Запрос e на шаге (2) требует, чтобы P был способен ответить на два вопроса: один из них нужен для того, чтобы продемонстрировать знание s , другой – чтобы предотвратить обман честного претендента нечестным проверяющим.

Соответственно запросу претендент отвечает на шаге (3) либо $y=r$, либо $x = rs(\text{mod } n)$. Ни тот, ни другой ответ не несет никакой информации об s : в первом случае он от s вообще не зависит, во втором – замаскирован случайной величиной r , которая известна только P , так как на шаге (1) тоже была замаскирована при помощи ОНФ.

Противник, пытающийся деперсонифицировать P , может стремиться обмануть проверяющего, выбрав произвольное r , вычислив $x = \frac{r^2}{v}(\text{mod } n)$ и ответив $y=r$ при $e=1$, но не сможет ответить при $e=0$, так как это требует знания $\sqrt{x}(\text{mod } n)$.

Противник, выступающий в роли проверяющего, может смоделировать пары сообщений (x,y) самостоятельно. Действительно, можно выбирать случайные y , задаваться случайными

битами $e=\{0/1\}$ и вычислять в зависимости от этого $x = y^2(\text{mod } n)$ либо $x = \frac{y^2}{v}(\text{mod } n)$.

Распределение вероятностей пар (x,y) не будет отличаться от распределения вероятностей тех величин, что сгенерировал бы P в реальном протоколе. Таким образом, протокол действительно обладает свойством нулевого разглашения знания.

Протокол аутентификации Файге – Фиата – Шамира

Предварительный этап			
	<i>P</i>	Центр доверия	<i>V</i>
	$s_i: (s_i, n) = 1,$ $1 \leq s \leq n - 1$ $v_i = s_i^2 \pmod{n}$ $v = (v_1, v_2, \dots, v_k)$ $s = (s_1, s_2, \dots, s_k)$	p, q – большие простые числа, $n = pq$	
n, v_1, v_2, \dots, v_k			
Рабочий этап			
	<i>P</i>		<i>V</i>
<i>for</i> ($i=1, 2, \dots, t$)			
1	$r_i \in_R \{1, 2, \dots, n-1\},$ $x_i = r_i^2 \pmod{n}$	→	
2		←	$(e_{i1}, e_{i2}, \dots, e_{ik}) \in_R \{0, 1\}^k$
3	$y_i = r_i (s_1^{e_{i1}} s_2^{e_{i2}} \dots s_k^{e_{ik}}) \pmod{n}$	→	
4			$x_i \stackrel{?}{=} y_i^2 (v_1^{e_{i1}} v_2^{e_{i2}} \dots v_k^{e_{ik}}) \pmod{n}$

Протокол аутентификации Гиллу - Кискатра (Guillou – Quisquater)

Предварительный этап			
	<i>P</i>	<i>Центр доверия</i>	<i>V</i>
	I_P, B, J	p, q — простые числа, $n=pq$, $I_P, J = H(I_P)$, $JB^v \equiv 1(\text{mod } n)$	
	n, J		
Рабочий этап			
	<i>P</i>		<i>V</i>
1	$r \in_R (1; n-1)$ $T = r^v(\text{mod } n)$	→	
2		←	$d \in_R (0; v-1)$
3	$D = rB^d(\text{mod } n)$	→	
4			$T' = D^v J^d \text{ mod } n$ $T \stackrel{?}{\equiv} T'(\text{mod } n)$

Протокол аутентификации Шнорра

Предварительный этап			
	<i>P</i>	<i>Центр доверия</i>	<i>V</i>
	$s \in_R \{1, \dots, q-1\}$ $v = a^s \pmod p$	p, q — простые числа, $q p-1$, $a \in \mathbb{Z}_p: a^q \equiv 1 \pmod p$	
p, q, a, v			
Рабочий этап			
	<i>P</i>		<i>V</i>
1	$r \in_R \{1, \dots, q-1\}$ $x = a^r \pmod p$	→	
2		←	$e \in_R \{0, \dots, 2^{t-1}\}$
3	$y = r + se \pmod q$	→	
4			$?$ $x = a^y v^e \pmod p$

Протокол аутентификации Брикелла – МакКарли

Предварительный этап			
<i>P</i>	<i>Центр доверия</i>	<i>V</i>	
$s < p$ – секр. ключ $v: v = a^{-s} \pmod{p}$	p, q, w – простые числа, $q w \mid p - 1; q^2 \nmid p - 1; q, w \geq 2^k$ $a: a^q \equiv 1 \pmod{p}$		
p, a, v			
Рабочий этап			
	<i>P</i>		<i>V</i>
1	$r \in_R \{1, \dots, p-1\}$ $x = a^r \pmod{p}$	→	
2		←	$e \in_R \{0, \dots, 2^t\}$
3	$y = r + se \pmod{p-1}$	→	
4			$?$ $x = a^y v^e \pmod{p}$

Сравнение схем цифровой подписи и протоколов аутентификации

- в схемах цифровой подписи сообщение имеет время жизни – тем самым, обеспечивается невозможность отказа от факта создания документа и возможность разрешения конфликтных ситуаций, связанных с принадлежностью цифровой подписи, в то же время в протоколах аутентификации проверка и принятие решений происходят немедленно, в режиме реального времени;
- содержание сообщений, подписываемых цифровой подписью, может быть произвольным, в то время как в протоколах аутентификации содержание всех передаваемых сообщений фиксировано;
- цифровая подпись служит для аутентификации сообщений, в то время как основная цель протокола аутентификации – аутентификация субъекта компьютерной системы (чаще всего это пользователь, взаимодействующий с системой через некоторый комплекс аппаратно-программных средств).