О. В. Казарин

ИНТЕРАКТИВНАЯ ПРОВЕРЯЕМАЯ СХЕМА РАЗДЕЛЕНИЯ СЕКРЕТА

Введение

Схемы разделения секрета — метод разделения секретной информации (секрета) s между n участниками взаимодействия таким образом, что только участники из заранее заданных разрешенных множеств могут восстановить s, в то время как участники из неразрешенных множеств не имели бы (почти) никакой информации о возможном секрете s. Совокупность заранее заданных разрешенных множеств участников схемы разделения доступа называют еще *ее структурой доступа*.

Схемы разделения секрета основываются, как правило, на (n,t)-*пороговых схемах*. Последние позволяют разделить секретную информацию на n частей таким образом, что по любым t из них она может быть восстановлена, тогда как любая совокупность $t-1$ частей не позволяет этого сделать.

Схемы разделения секрета применяются для обеспечения информационной безопасности в вычислительных системах и сетях, например при организации конференц-связи или для организации хранения резервных наборов ключевой информации в вычислительных сетях [1—3]. В данной работе схемы разделения секрета и их разновидности рассматриваются в рамках исследований моделей и методов теории конфиденциальных вычислений и базового раздела этой теории — моделей и методов *конфиденциального вычисления функции* (см., например: [10, 12, 14]).

Задачу конфиденциальных вычислений, которая решается посредством многостороннего интерактивного протокола, неформально можно описать в следующей постановке. Имеется n участников протокола или n процессоров вычислительной системы, соединенных сетью связи. Изначально каждому процессору известна своя «часть» некоторого входного значения x. Требуется вычислить $f(x)$, f — некоторая известная всем участникам вычислимая функция, таким образом, чтобы выполнились следующие требования:

— *корректности*, когда значение $f(x)$ должно быть вычислено правильно, даже если некоторая ограниченная часть участников произвольным образом отклоняется от предписанных протоколом действий;

— *конфиденциальности*, когда в результате выполнения протокола ни один из участников не получает никакой дополнительной информации о начальных значениях других участников (кроме той, которая содержится в вычисленном значении функции).

Схема разделения секрета, как один из базовых примитивов при конфиденциальных вычислениях, рассматривается в следующей постановке. Пусть имеется конечное множество процессоров вычислительной системы $P = \{p_1,...,p_n\}$. Эти процессоры из центра доверия D получают некоторые доли s_i, $i = 1,...,n$ секрета s. Предположим также, что задан набор подмножеств G_j множества P, называемых *квалифицированными подмножествами*, или *разрешенными коалициями*. Задача центра D при распределении информации состоит в том, чтобы доли s_i любой разрешенной коалиции из P, взятые вместе, давали полную информацию о значении секрета, а любое неразрешенное объединение процессоров F не могло получить никакой информации о секрете. При этом все процессоры из разрешенной коалиции могут корректно восстановить секрет при безусловном обеспечении конфиденциальности своих входов (своих долей секрета).

Схема разделения секрета называется *проверяемой*, если в ней существует дополнительный, возможно интерактивный, алгоритм, позволяющий каждому из участников убедиться в том, что он действительно получил корректную долю секрета.

Основной результат настоящей работы, по мнению автора, заключается в следующем.

Во-первых, в отличие от часто используемых в схемах разделения секрета (n,t)-пороговой схемы Шамира [7] или (n,t)-пороговых схем, основанных на кодах с исправлением ошибок (см., например: [21]), где вычисления производятся с полиномами, определенными над конечным полем, в настоящей работе используется (n,t)-пороговая схема из работы [8], где вычисления производятся с вычетами над таким полем. Следовательно, вся конструкция является более эффективной с точки зрения состава необходимых вычислений.

Во-вторых, в отличие от известных (n,t)-пороговых схем, в данной схеме в формировании, а затем в разделении s принимают участие все абоненты системы. Таким образом, можно рассматривать вопрос о построении стойких проверяемых схем разделения секрета, когда на этапе разделения секрета дилер является нечестным.

В-третьих, так как основной предмет исследования — проверяемые схемы разделения секрета — рассматриваются в рамках исследования методологии конфиденциальных вычислений, они являются еще и основными фундаментальными примитивами указанной методологии. Поэтому исследования и доказательства стойкости схем разделения секрета в данном случае предпочтительно проводить именно в терминах теории конфиденциальных вычислений, что и делается в настоящей работе.

В-четвертых, по сравнению с имеющимися даются более строгие определения стойкости (безопасности) проверяемых схем разделения секрета и строятся криптографические протоколы, стойкость которых соответствует таким определениям.

И главное, в настоящей работе демонстрируется так называемая парадигма доказуемой безопасности в криптографии. Если раньше криптографическая схема (криптографическая система, криптографический примитив, криптографический протокол) считалась стойкой (безопасной), пока она не была раскрыта, то сейчас этого недостаточно. Необходимо самому разработчику криптографической схемы математически строго доказать стойкость создаваемой им схемы в условиях выдвинутых гипотез, предположений, определений и модели противника.

1. Основные понятия, определения протоколы и схемы

1.1. Обозначения и определения

Через Z будем обозначать множество целых чисел, а $\mathrm{abs}(x)$ означает, что для двух аргументов x и $-x$ функции abs верно $x = \mathrm{abs}(x) = \mathrm{abs}(-x)$.

Обозначение 1. Пусть $a \in_R M$ обозначает, что элемент a случайно и с равномерным распределением вероятностей выбран из всех элементов множества M.

Обозначение 2. Пусть $a \in_{R^*} M$ обозначает, что элемент a случайно, с равномерным распределением вероятностей и независимо от других событий выбран из всех элементов множества M.

Базовым объектом исследований в теории конфиденциальных вычислений являются многосторонние протоколы взаимодействия участников вычислений.

Обозначение 3. Обозначение $(x_1,x_2,\ldots,x_k)$**Абвг** $= (y_1,y_2,\ldots,y_l)$ означает, что значения выходных параметров протокола (алгоритма, процедуры) **Абвг** равны $y = y_1,y_2,\ldots,y_l$ при инициализации протокола со значениями входных параметров, равными $x = x_1,x_2,\ldots,x_k$.

Обозначение 4. Обозначение

$(y_1,y_2,\ldots,y_l,\cdot,\cdot\ldots)$**Иклм** $= (z_1,z_2,\ldots,z_m) \leftarrow (x_1,x_2,\ldots,x_k)$**Абвг** $= (y_1,y_2,\ldots,y_l)$

означает, что значения выходных параметров протокола (алгоритма, процедуры) **Иклм** равны $z = z_1,z_2,\ldots,z_m$ при инициализации протокола **Иклм** со значениями входных параметров, часть из которых являются значениями $y_1,y_2,\ldots,y_l$; последние, в свою очередь, являются выходными параметрами протокола **Абвг**, работа которого инициирована при значениях входных параметров, равных значениям $x_1,x_2,\ldots,x_k$.

Пусть **Пред**(•,•,…) — предикат, тогда

$\rho r(\textbf{Пред}(\alpha,\beta,\ldots) \leftarrow (a,b,\ldots)\textbf{Алгр} = (\alpha,\beta,\ldots))$

— вероятность того, что **Пред**$(\alpha,\beta,\ldots)$ принимает значение «Истина» после выполнения вероятностного алгоритма (протокола) **Алгр** со входными переменными $a,b,\ldots$

Обозначение 5. $\{(\alpha,\beta,\ldots) \leftarrow (a,b,\ldots)\textbf{Алгр} = (\alpha,\beta,\ldots)\}$ обозначено семейство случайных переменных над $\{(a,b,\ldots)\}$, сгенерированное (индуцированное) после выполнения вероятностного алгоритма **Алгр** со входными переменными $a,b,\ldots$

Обозначение 6.

$\rho r((y_1,y_2,\ldots,y_l,\bullet,\bullet,\ldots)\textbf{Иклм} = (z_1,z_{\_2},\ldots,z_{\_m}) \leftarrow$

$\leftarrow (x_1,x_2,\ldots,x_k)\ \textbf{Абвг} = (y_1,y_2,\ldots,y_l)) > 1\text{-}n^{-c}$

означает, что вероятность того, что протокол **Иклм** закончит свою работу с выходными параметрами $(z_1,z_2,\ldots,z_l)$, больше $1 - n^{-c}$, где $\{y_1,y_2,\ldots,y_l\}$ — семейство случайных переменных, сгенерированных после выполнения (вероятностного) протокола **Абвг** с входными параметрами $(x_1,x_2,\ldots,x_k)$.

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

Гипотеза 1. Любой полиномиальный алгоритм может по заданным g, β и ρ вычислить $\alpha \equiv \log_g^{(\rho)}\beta$ лишь с пренебрежимо малой вероятностью [6].

Определение 1. Пусть для каждого фиксированного слова x, $A(x)$ и $B(x)$ — это случайные величины, значения которых являются двоичными словами. Семейства случайных величин $\{A(x)\}$ и $\{B(x)\}$ называются *статистически неразличимыми*, если

$\sum_{s\in\{0,1\}^*} |\rho r[A(x) = s] - \rho r[B(x) = s]| < |x|^{-c}$

для любой константы $c > 0$ и всех достаточно длинных $x \in X$.

Семейства случайных величин $\{A(x)\}$ и $\{B(x)\}$ называются *абсолютно неразличимыми* на множестве X, если $\rho r[A(x) = s] = \rho r[B(x) = s]$.

Пусть C_n — это схема (булева схема), $n \in N$ и запись $C_n(s) = 1$ будет означать, что на входной переменной $s = (s_1,\ldots,s_n)$ схема C_n выдает значение 1. Семейство $\{C_n\}$ называется *полиномиально ограниченным*, если для некоторой константы d и всех достаточно больших n количество функциональных элементов в схеме C_n не превосходит n^d.

Определение 2. Семейства случайных величин $\{A(x)\}$ и $\{B(x)\}$ называются *вычислительно неразличимыми* на множестве X, если для произвольного полиномиально ограниченного семейства схем $\{C_n\}$

$|\rho r[C_{|x|}(A(x)) = 1] - \rho rob[C_{|x|}(B(x)) = 1]| < |x|^{-c}$

для любой константы $c > 0$ и всех достаточно длинных $x \in X$.

Предполагается, что случайные величины $A(x)$ и $B(x)$ принимают значения, длина которых совпадает с количеством входных переменных схемы $C_{|x|}$.

Следует заметить, что если семейства случайных величин статистически неразличимы, то они и вычислительно неразличимы.

Определение 3. Матрица пересечений $(S - 1)$ линейно независимых S-мерных векторов $W_1,W_2,\ldots,W_{S\text{-}1}$, обозначаемая как $W_1 \times W_2 \times \ldots \times W_{S\text{-}1}$, имеет вид

$$\left(\begin{vmatrix} W_2^1 & W_3^1 & \ldots & W_S^1 \\ W_2^2 & W_3^2 & \ldots & W_S^2 \\ \ldots & \ldots & \ldots & \ldots \\ W_2^{S-1} & W_3^{S-1} & \ldots & W_S^{S-1} \end{vmatrix}, \begin{vmatrix} W_3^1 & W_4^1 & \ldots & W_S^1 & W_1^1 \\ W_3^2 & W_4^2 & \ldots & W_S^2 & W_1^2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ W_3^{S-1} & W_4^{S-1} & \ldots & W_S^{S-1} & W_1^{S-1} \end{vmatrix}, \ldots, \begin{vmatrix} W_1^1 & W_2^1 & \ldots & W_{S-1}^1 \\ W_1^2 & W_2^2 & \ldots & W_{S-1}^2 \\ \ldots & \ldots & \ldots & \ldots \\ W_1^{S-1} & W_2^{S-1} & \ldots & W_{S-1}^{S-1} \end{vmatrix}\right),$$

где $W_i = (W_1^i, W_2^i, \ldots, W_S^i)$.

Используемая (n,t)-пороговая схема СРС

1. Этап разделения секрета s.

1.1. Дилер получает вектор V при помощи матрицы пересечений в соответствии с определением 3: $V = V_1 \times V_2 \times ... \times V_j \times ... \times V_t$, где $V_j = (v_1^{(j)}, v_2^{(j)}, ..., v_{n-t}^{(j)}) \in {}_{R^*}Z$, Z — множество целых чисел. Каждый элемент v_i вектора V определяется как детерминант $t \times t$ размерной матрицы, состоящей из элементов векторов V_j.

1.2. Определяется $s = \prod_{i=2}^{n-t} \mathrm{abs}(v_i)$, где s — секрет.

1.3. Определяется $S^* = \begin{vmatrix} S_1 \\ S_2 \\ \dots \\ S_n \end{vmatrix} = \begin{vmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,t} \\ a_{2,1} & a_{2,2} & \dots & a_{2,t} \\ \dots & \dots & \dots & \dots \\ a_{n,1} & a_{n,2} & \dots & a_{n,t} \end{vmatrix} \cdot \begin{vmatrix} V_1 \\ V_2 \\ \dots \\ V_t \end{vmatrix}$,

где A — сгенерированная случайным образом матрица. Т. е. $A \in {}_R S^{nt}$, где S^{nt} — пространство возможных долей секрета.

1.4. Значение v_1 делается общедоступным для всех участников схемы. Каждому участнику j, $j = 1,...,n$ конфиденциально выдается вектор $S_j = (s_1^{(j)}, s_2^{(j)}, ..., s_{n-t}^{(j)})$.

2. Этап восстановления секрета s.

2.1. Пусть B — множество участников схемы, желающих восстановить секрет, где $t \le |B| \le n$. Любой участник из B получает $S = S_{j \in B} \times ... \times S_{j \in B}$.

2.2. Секрет s восстанавливается следующим образом: $s = \prod_{i=2}^{n-t} \mathrm{abs}(s_i/h)$, где $h = s_1/v_1$.

Обсуждение безопасности схемы можно найти в работах [1, 8].

В данной работе будет использоваться интерактивная система доказательств с абсолютно нулевым разглашением из работы [9, 22], где участник **Р** доказывает участнику **V** равенство двух дискретных логарифмов $\log_g^{(\rho)} M \equiv \log_e^{(\rho)} L \equiv H$, где g — образующий группы вычетов по модулю ρ, e — любой элемент этой группы, без разглашения самого значения H. Пусть $M \equiv g^H (\mathrm{mod}\ \rho)$, $L \equiv e^H (\mathrm{mod}\ \rho)$ общеизвестны, а логарифм H известен только участнику **Р**.

Используемый Протокол ДНР(H,(M,g)(L,e),ρ)

1. Участник **V** выбирает $a,b \in {}_R Z_q$, вычисляет $\delta \equiv e^a g^b (\mathrm{mod}\ p)$ и посылает δ участнику **Р**.

2. Участник **Р** выбирает $t \in {}_R Z_q$, вычисляет $h_1 \equiv \delta g^t (\mathrm{mod}\rho)$, $h_2 \equiv h_1^H (\mathrm{mod}\rho)$и посылает h_1 и h_2 участнику **V**.

3. Участник **V** высылает **Р** параметры a и b.

4. Если $\delta \equiv e^a g^b (\mathrm{mod}\ p)$, то участник **Р** посылает **V** параметр t; в противном случае — останавливается.

5. Участник **V** проверяет выполнение равенств $h_1 \equiv^? e^a g^{b+t} (\mathrm{mod}\ p)$ и $h_2 \equiv^? L^a M^{b+t} (\mathrm{mod}\rho)$.

6. Если проверка завершена успешно, то $\log_g^{(\rho)} M \equiv \log_e^{(\rho)} L$.

Стойкость этого протокола определяется следующей теоремой.

Теорема 0. Протокол **ДНР** является протоколом доказательства с абсолютно нулевым разглашением.

Подробности доказательства данной теоремы можно найти в работе [9].

Для некоторых задач, решаемых в рамках методологии конфиденциальных вычислений, достаточно введения определения *конфиденциального вычисления функции* [10].

Пусть в сети N, состоящей из n процессоров $P_1, P_2, ..., P_n$ со своими секретными входами $x_1, x_2, ..., x_n$, необходимо корректно (т. е. даже при наличии t сбоящих процессоров) вычислить значение функции $(y_1, y_2, ..., y_n) = f(x_1, x_2, ..., x_n)$ без разглашения информации о секретных аргументах функции, кроме той информации, которая содержится в вычисленном значении функции.

Введем понятия «реальное и идеальное вычисления функции f» [12]. Пусть множество входов и выходов обозначается как X и Y соответственно, размерности этих множеств $|X|=\chi$ и $|Y|=\mu$. Множество случайных параметров, используемых всеми процессорами сети, обозначается через R, размерность — $|R|=\nu$. Кроме того, через W обозначим рабочее пространство параметров сети. Через $T^{(r)}$ обозначается трафик в r-раунде, через $t_i^{(r)}$ — трафик для процессора i в r-м раунде, r_0 и r_k — инициализирующий и последний раунды протокола соответственно и r^* — заданный неким произвольным образом раунд выполнения протокола ρ.

Пусть функцию f можно представить как композицию d функций (функций от двух аргументов-векторов) $g_1 \circ ... \circ g_\eta \circ g_{\eta+1} \circ ... \circ g_d$:

$f(x_1,...,x_n) = g_1((w_1,...,w_n),(t_1^{(r_o)},..., t_n^{(r_o)})) \circ ... \circ g_d((w_1,...,w_n),(t_1^{(r^*)},..., t_n^{(r^*)}))$.

Аргументы функции g_η являются рабочими параметрами $w_1,...,w_n$ участников протокола с трафиком $(t_1,...,t_n)$ в r раунде. Значения данной функции g_η являются аргументами (рабочими параметрами протокола с трафиком $(t_1,...,t_n)$ в $r+1$ раунде) для функции $g_{\eta+1}$.

Из сказанного выше следует, что функция $f:(X^n \times R^n \times W^n) \to Y$, где $\times$ — декартово произведение множеств, реализует:

$f(x_1,...,x_n) = g_d((w_1,...,w_n),(t_1^{(r^*)},..., t_n^{(r^*)})) = ((y_1,...,y_n),(t_1^{(r_k)},..., t_n^{(r_k)}))$.

Далее введем понятие моделирующего устройства M. Здесь можно проследить некоторые аналогии с моделирующей машиной в интерактивных системах доказательств с нулевым разглашением (см., например: [4, 9, 14, 15]).

Пусть ${}_{\rho}\Theta^{\Pi\text{рот}}$ — распределение вероятностей над множеством историй нечестных участников во время выполнения протокола ρ [12]. Моделирующее устройство M, взаимодействующее с нечестными участниками, осуществляет свое функционирование в рамках идеального сценария и создает распределение вероятностей параметров взаимодействия ${}_{и}\Theta^{\Pi\text{рот}}$ между M и нечестными участниками.

Определение 4. Протокол ρ *конфиденциально вычисляет* функцию $f(x)$, если выполняются следующие условия:

Условие корректности. Для всех несбоящих процессоров P_i функция

$f(x_1,...,x_n) =$

$= g_1((w_1,...,w_n),(t_1^{(r_o)},..., t_n^{(r_o)})) \circ ... \circ g_\eta((w_1,...,w_n),(t_1^{(r^*)},..., t_n^{(r^*)})) \circ$

$\circ g_{\eta+1}((w_1,...,w_n),(t_1^{(r^*)},..., t_n^{(r^*)})) \circ ... \circ g_d((w_1,...,w_n),(t_1^{(r^*)},..., t_n^{(r^*)})) =$

$= ((y_1,...,y_n),(t_1^{(r_k)},..., t_n^{(r_k)}))$

вычисляется с вероятностью ошибки, близкой к 0.

Условие конфиденциальности. Для заданной тройки $(x,r,w) \in (X^n \otimes R^n \otimes W)$ распределения ${}_{\rho}\Theta^{\Pi\text{рот}}$ и ${}_{и}\Theta^{\Pi\text{рот}}$ являются статистически неразличимыми.

Определение 5. Функция f, удовлетворяющая условиям определения 4, называется *конфиденциально вычислимой*.

Более подробно определения и понятия из теории конфиденциального вычисления функции рассмотрены в работах [12, 13, 22].

Схема привязки к значению некоторого параметра является одним из часто используемых вычислительных примитивов, применяемых в различных криптографических конструкциях.

Определение 6. *Схема привязки* **Пр**(r,z) с рабочими параметрами привязки (C,D) представляет собой пару двухсторонних протоколов (**Прив**,**Откр**), при реализации которых выполняются следующие условия безопасности:

Условие полноты. Для любого z, любой константы $c > 0$ и для достаточно большого $|\rho|$ вероятность

$\text{Prob}((C,D,r)\textbf{Откр} = z \leftarrow (r,z)\textbf{Прив} = (C,D)) > 1 - |\rho|^{-c}$.

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

$\rho\text{rob}([(C_{z'},D,r)\textbf{Откр} = z' \ \&\ (C_{z''},D,r)\textbf{Откр} = z''] \leftarrow (r)\textbf{Прот} = (C_{z'},D,r)) < |\rho|^{-c}$.

Условие неразличимости. Для $\Psi_z(r) = \{(r,z)\textbf{Прив} = (D)\}$ семейства случайных переменных $\{\Psi z'(r) \leftarrow r \in \{0,1\}^*\}$ и $\{\Psi z''(r) \leftarrow r \in \{0,1\}^*\}$ вычислительно неразличимы.

В данной работе мы будем использовать следующую схему привязки.

Схема привязки Пр(r,z)

Пусть ρ — простое число и q — большой простой делитель $\rho - 1$. Пусть также $g^q \equiv 1 (\mathrm{mod}\ \rho)$, $g \neq 1$.

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 $r \in_{R^*} Z_q$ и вычисляет $\beta \equiv g^z t^r (\mathrm{mod}\ \rho)$, где z — параметр, выбранный для привязки.

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

Параметры протокола: $(z)\textbf{Прив} = (C,D)$, $C = r$, $D = \beta$.

Протокол Откр

1. Для того чтобы участник **B** убедился, что значение β действительно было привязано к параметру z, он выдает запрос участнику **A** о передаче ему значений r и z, которые, по существу, являются свидетельством правильных действий **A**.

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

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

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

Безопасность схемы привязки к биту определяется следующей теоремой.

Теорема 1. Схема **Пр** является безопасной.

Доказательство теоремы 1. Для доказательства теоремы необходимо доказать выполнения условий полноты, однозначности и неразличимости.

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

Однозначность. Доказательство проведем от противного. Пусть $z' \neq z'' (\mathrm{mod}\ q)$ и абонент **A** нашел z' и z'' такие, что $g^{z'} t^{r'} (\mathrm{mod}\ \rho) \equiv g^{z''} t^{r''} (\mathrm{mod}\ \rho) \equiv \beta$. Тогда $r' \neq r'' (\mathrm{mod}\ q)$ и $\log_g^{(\rho)} t \equiv \frac{z'-z''}{r''-r'} (\mathrm{mod} q)$. В этом случае несправедлива гипотеза 1, так как противник (например, участник **A**) может вычислять дискретные логарифмы в группе G.

Неразличимость. Так как функция $\beta \equiv g^{\alpha} (\mathrm{mod}\ \rho)$ при указанных криптографических соглашениях является односторонней перестановкой, то для любого z и для $t \in_{R^*} Z_q$ значение $\beta \equiv g^z t^r (\mathrm{mod}\ \rho)$ равномерно распределено среди всех элементов группы G. Таким образом, учитывая гипотезу 1, семейства случайных переменных $\{g^{z'} t^{r'} (\mathrm{mod}\ \rho) \equiv \beta'\}$ и $\{g^{z''} t^{r''} (\mathrm{mod}\ \rho) \equiv \beta''\}$ вычислительно неразличимы.

Статистическая же неразличимость вытекает из следующего факта. Предположим, что противник (например, участник **B**, который пытается узнать что-либо о значении z) может вычислять дискретный логарифм l такой, что $\beta'/\beta'' \equiv t^l (\mathrm{mod}\ \rho)$, где $\beta' \equiv g^z t^{r'} (\mathrm{mod}\ \rho)$, $\beta'' \equiv g^z t^{r''} (\mathrm{mod}\ \rho)$ и $r' \neq r'' (\mathrm{mod}\ q)$. Противник, знающий l, может открыть β' как привязку к z тогда и только тогда, когда он может открыть β'' как привязку к z. Так как $l = r' - r'' (\mathrm{mod}\ q)$, то можно доказать равенство двух параметров привязки.

В то же время значение $r' - r'' \pmod q$ не дает никакой информации о значении параметра z. Таким образом, противник, даже умея извлекать дискретные логарифмы, не может отличить привязку к z' от привязки к z''. Таким образом, вероятность успеха противника в этих условиях не превышает $1/q$.

СПИСОК ЛИТЕРАТУРЫ:

1. *Казарин О. В., Ухлинов Л. М.* Использование свойств эллиптических кривых в криптографических протоколах // Автоматика и вычислительная техника. 1992. № 3. С. 23–32.
2. *Ухлинов Л. М.* Распределение ключей защиты данных и проблема аутентификации // Автоматика и вычислительная техника. 1990. № 5. С. 11–17.
3. *Ухлинов Л. М.* Метод оптимального размещения ключевой информации в информационно-вычислительных сетях // Автоматика и вычислительная техника. 1989. № 3. С. 3–8.
4. *Варновский Н. П.* Криптографические протоколы // Введение в криптографию / Под общ. ред. В. В. Ященко. М.: МЦНМО, «ЧеРо», 1998. – 272 с.
5. *Казарин О. В., Ухлинов Л. М.* К вопросу о создании безопасного программного обеспечения на базе методов конфиденциального вычисления функции // Тез. докл. Международной конференции IP+NN'97. 1997. С. 3–6.
6. *Diffi W., Hellman M. E.* New Direction in Cryptography // IEEE Transactions on Information Theory. 1976. V.IT-22. № 11. P. 644–654.
7. *Shamir A.* How to Share a Secret // Communication of ACM. 1979. Vol. 22 (11). P. 612–613.
8. *Lain C. S., Lee J. Y.* A New Threshold Scheme and Its Application in Designing the Conference Key Distribution Cryptosystem // Information Processing Letters. 1989. Vol. 32. P. 95–99.
9. *Казарин О. В.* Конвертируемые и селективно конвертируемые схемы подписи с верификацией по запросу // Автоматика и телемеханика. 1998. № 6. С. 178–188.
10. *Yao A. C.* Protocols for Secure Computations (extended abstract) // Proc. of 23rd IEEE Symp. on Foundations of Computer Science. 1982. P. 160–164.
11. *Ben-Or M., Goldwasser S., Wigderson A.* Completeness Theorems for Non-cryptographic Fault-tolerant Distributed Computation // Annual ACM Symposium of Computing – STOC'88, Proceedings. 1988. P. 1–10.
12. *Micali S., Rogaway Ph.* Secure Computation // Advances in Cryptology – CRYPTO'91, Proceedings. Springer-Verlag LNCS. V. 576. 1992. P. 392–404.
13. *Ben-Or M., Canetti R., Goldreich O.* Asynchronous Secure Computation // Annual ACM Symposium of Computing – STOC'93, Proceedings. 1993. P. 52–61.
14. *Варновский Н. П.* Криптография и теория сложности // Введение в криптографию / Под общ. ред. В. В. Ященко. М.: МЦНМО, «ЧеРо», 1998. – 272 с.
15. *Казарин О. В., Ухлинов Л. М.* Интерактивная система доказательств для интеллектуальных средств контроля доступа к информационно-вычислительным ресурсам // Автоматика и телемеханика. 1993. № 11. С. 167–175.
16. *Кабатянский Г. А.* Математика разделения секрета // Введение в криптографию / Под общ. ред. В. В. Ященко. М.: МЦНМО, «ЧеРо», 1998. – 272 с.
17. *Desmedt Y., Frankel Y.* Shared Generation of Authenticators and Signatures // Advances in Cryptology – CRYPTO'91, Proceedings. Springer-Verlag LNCS. V. 576. 1992. P. 457–469.
18. *Pedersen T. P.* Distributed Provers with Applications to Undeniable Signatures // Advances in Cryptology – EUROCRYPT'91, Proceedings. Springer-Verlag LNCS, V. 547. 1991. P. 221–242.
19. *Казарин О. В., Ухлинов Л. М.* Новые схемы цифровой подписи на основе отечественного стандарта // Защита информации. 1995. № 5. С. 52–56.
20. *Казарин О. В.* О доказательстве безопасности схемы подписи с верификацией по запросу // Безопасность информационных технологий. 1997. № 1. С. 58–62.
21. *Gennaro R., Micali S.* Verifiable Secrete Sharing as Secure Computation // Advances in Cryptology – EUROCRYPT'95, Proceedings/ Springer-Verlag LNCS, V. 921. 1996. P. 168–182.
22. *Казарин О. В.* Методология защиты программного обеспечения. М.: МЦНМО, 2009. – 464 с.