Второй подход (синтетический) рассматривает лишь реальные системы $\mathbf{A}^*(\mathbf{t})$, близкие к своим оптимальным прототипам $\mathbf{A}_0^*(\mathbf{t})$. Он начинается с синтеза оптимальных моделей $\mathbf{A}_0(\mathbf{t})$, приближающихся к прототипам $\mathbf{A}_0^*(\mathbf{t})$ за счет приближения **L** к $\mathbf{L}^*$ и **F** к $\mathbf{F}^*$.

Аналитический и синтетический подходы используют модели $\mathbf{A}(\mathbf{t})$ и $\mathbf{A}_0(\mathbf{t})$ с **N–L** и **L** степенями свободы, и они тем адекватней в действительности, чем ближе **N** и **L** к $\mathbf{N}^*$ и $\mathbf{L}^*$ соответственно. При $\mathbf{L}^* \ll \mathbf{N}^*$ можно сказать, что $\mathbf{L}^* \ll \mathbf{N}^* - \mathbf{L}^*$ и требуемая адекватность выглядит реальнее достижимой для синтетического подхода, чем для аналитического (реальнее возможность преодоления ситуаций, связанных с системами, имеющими большое количество параметров). Однако использование второго подхода по сравнению с первым усложнено введением параметра оптимальности.

При моделировании реальных компьютерных тренажерных систем, носящих зачастую распределенный характер, наиболее применим синтетический подход, уже хотя бы потому, что приближение **N** к $\mathbf{N}^*$, а **L** к $\mathbf{L}^*$ если и возможно, то достаточно ресурсоемко.

# *РАСПРЕДЕЛЕННАЯ ПОДПИСЬ RSA*

*А.Д. Фомин*

Данная работа посвящена распределенной схеме подписи *RSA*, которая определяется процедурой разделения секретного ключа *RSA* среди участников системы и процедурой совместной постановки подписи подгруппой участников. Одним из важнейших свойств распределенных схем подписи является отсутствие интерактивности процедуры выдачи новой проекции без дилера. Для интерактивного протокола предполагается обмен данными между действующими участниками, что является существенным недостатком, так как растет объем трафика в системе, повышается расход энергии и требуется синхронизация действий узлов. Другим важным свойством распределенных схем подписи является возможность независимой работы участников коалиции при постановке подписи. Данное свойство при изменении состава участников коалиции позволяет не перезапускать протокол постановки подписи, что приводит к сокращению задержки при постановке подписи. Еще одним свойством распределенных схем подписи является возможность самоорганизации, то есть должна быть предусмотрена возможность работы системы без участия дилера после этапа инициализации.

В существующих работах, посвященных распределенной подписи *RSA*, можно выделить три основных подхода к распределению секретного ключа *RSA*.

*При первом подходе* подразумевается, что секретный ключ **d** распределяется по схеме разделения секрета Шамира над кольцом $\mathbf{Z}_{\phi(\mathbf{N})}$ (или $\mathbf{Z}_{\lambda(\mathbf{N})}$), где $\phi(\mathbf{N})$ (или $\lambda(\mathbf{N})$) не опубликованы. Отсутствие информации о $\phi(\mathbf{N})$ (или $\lambda(\mathbf{N})$) делает невозможной работу системы без участия доверенного дилера.

*При втором подходе* предполагается наличие дополнительного уровня в схеме разделения секрета. При этом сначала секрет разделяется между **n** узлами аддитивно, а потом каждая полученная проекция распределяется при помощи пороговой схемы. Подобные схемы интерактивны и неработоспособны без дилера.

*При третьем подходе* предполагается разделение секретного ключа **d** над известным кольцом $\mathbf{Z}_{\mathbf{N}}$ вместо $\mathbf{Z}_{\phi(\mathbf{N})}$ или $\mathbf{Z}_{\lambda(\mathbf{N})}$. Но такое разделение для подписи *RSA* приводит к уязвимости распределенной схемы. Кроме того, данный подход не предполагает возможности независимой работы участников коалиции при постановке подписи.

Таким образом, каждая из упомянутых ранее схем имеет некоторые функциональные ограничения и не отвечает по крайней мере одному из следующих требований:

– процедура постановки подписи должна обеспечивать независимость действий участников коалиции;

– система должна обладать свойством самоорганизации, то есть после инициализации не нуждаться в участии дилера;

– процедура выдачи проекции секрета без дилера должна быть неинтерактивна.

В большинстве известных работ рассматривается схема разделения секрета Шамира. В схеме Шамира предполагается заданным полином $\mathbf{f}(\mathbf{x}) = \mathbf{f}_0 + \mathbf{f}_1\mathbf{x} + \ldots + \mathbf{f}_{\mathbf{t}-1}\mathbf{x}^{\mathbf{t}-1} \bmod \mathbf{P}$, в котором $\mathbf{f}_0 = \mathbf{S}$ – секрет; $\mathbf{f}_1, \ldots, \mathbf{f}_{\mathbf{t}-1}$ – случайные значения; **P** – простое число. Каждый участник протокола получает проекцию секрета в виде $\mathbf{ss} = \mathbf{f}(\mathbf{id})$, где **id** – идентификатор участника. Любая коалиция **K** из **t** участников сможет восстановить секрет $\mathbf{f}_0 = \mathbf{f}(0)$,

используя интерполяцию по Лагранжу: $\mathbf{f(0)} = \mathbf{\sum_{u\in K} ss_u l_u(0) (mod\, P)}$, где $\mathbf{l_u(x)}$ – коэффициенты Лагранжа.

Чтобы использовать схему Шамира для распределенной подписи *RSA*, необходимо выбрать секрет **S** и модуль **P**. Для распределенной подписи *RSA* секретом является секретный ключ **d**. Относительно модуля **P** имеется две возможности: либо сделать его публичным, например **P=N**, либо секретным, положив $\mathbf{P = \phi(N)}$ или $\mathbf{P = \lambda(N)}$. Если **P** всем известно (например модуль *RSA*), это приведет к утечке информации и взаимозависимости действий участников коалиции во время выполнения процедуры постановки распределенной подписи. Если **P** – секретное значение (например $\mathbf{P = \lambda(N)}$ или $\mathbf{P = \phi(N)}$), то это приведет к невозможности самоорганизации системы. Следовательно, для устранения вышеуказанных недостатков необходимо отказаться от использования модуля **P**. Однако процедура выдачи проекций без дилера остается интерактивной. Кроме того, отказ от **P** приводит к росту размера проекций, а следовательно, и к сложности постановки подписи. Для размера проекции секрета **R** легко получить верхнюю оценку: $\mathbf{R \le log(N) + (t-1)k + 1}$, где **N** – модуль *RSA*; **t** – размер коалиции; **k** – длина идентификатора узла.

Опишем схему разделения секрета, для которой процедура выдачи проекции без дилера становится неинтерактивной, а размер проекции секретного ключа, используемой для постановки подписи, не превышает $\mathbf{log(N) + t + k}$.

Введем в рассмотрение простое число $\mathbf{Q > max(id_i)}$ и будем вычислять проекции секрета по формуле:

$$\mathbf{f(x,y) = \sum_{i=0}^{t-1}\sum_{j=0}^{t-1} f_{i,j}(x^i \bmod Q)(y^j \bmod Q)}.$$

При таком задании функции разделения секрета нельзя использовать интерполяцию по Лагранжу. Вместо этого необходимо решать систему линейных уравнений.

Для восстановления секрета каждый участник коалиции **u** вычисляет значение своей функции в точке **x=0**, получая $\mathbf{f(0, id_u) = f_0 + f_1(y \bmod Q) + \ldots + f_t(y^t \bmod Q)}$ в точке $\mathbf{y = id_u}$. При этом $\mathbf{f_0 = f_{0,0}}$. Имея **t** значений данной функции, можно восстановить секрет, решив следующую систему уравнений:

$$\mathbf{\left[f_0\ f_1\ \ldots f_{t-1}\right] G = \left[f(x_{i_1})\, f(x_{i_2})\, \ldots f(x_{i_t})\right]}, \text{ где}$$

$$\mathbf{G} = \begin{bmatrix} (x_{i_1})^0 \bmod Q & (x_{i_2})^0 \bmod Q & \ldots & (x_{i_t})^0 \bmod Q \\ (x_{i_1})^1 \bmod Q & (x_{i_2})^1 \bmod Q & \ldots & (x_{i_t})^1 \bmod Q \\ & & \vdots & \\ (x_{i_1})^{t-1} \bmod Q & (x_{i_2})^{t-1} \bmod Q & \ldots & (x_{i_t})^{t-1} \bmod Q \end{bmatrix}.$$

Для выдачи проекции новому участнику без дилера каждый участник коалиции **u** вычисляет значение своей функции в точке $\mathbf{x = id_{new}}$, получая $\mathbf{f(id_{new}, id_u) = s_{new}(id_u) = s_0 + s_1(y \bmod Q) + \ldots + s_{t-1}(y^{t-1} \bmod Q)}$ в точке $\mathbf{y = id_u}$. Проекция секрета $\mathbf{(s_0, s_1, \ldots, s_{t-1})}$ для нового абонента находится из системы уравнений:

$$\mathbf{\left[s_0\ s_1\ \ldots s_{t-1}\right] G = \left[s_{new}(x_{i_1})\, s_{new}(x_{i_2})\, \ldots s_{new}(x_{i_t})\right]}.$$

На основе описанной модифицированной схемы разделения секрета можно предложить следующую схему распределенной подписи *RSA*.

**1. Инициализация схемы.**

(a) Дилер генерирует простое число $\mathbf{Q > max(id_i)}$.

(b) Дилер генерирует публичный ключ *RSA* $\mathbf{N = pq}$ и $\mathbf{e > Q}$ – простое число и вычисляет секретный ключ $\mathbf{d : ed = 1 \bmod \Phi(N)}$.

(c) Дилер генерирует функцию $\mathbf{f(x,y) = \sum_{i=0}^{t-1}\sum_{j=0}^{t-1} f_{i,j}(x^i \bmod Q)(y^j \bmod Q)}$, где $\mathbf{f_{0,0} = d}$, а коэффициенты $\mathbf{f_{i,j} \in Z_N}$ выбраны случайным образом с соблюдением условия $\mathbf{f_{i,j} = f_{j,i}}$.

(d) Каждый узел **u** в качестве проекции секретного ключа получает функцию $\mathbf{s_u(x) = f(x, id_u)}$.

**2. Распределенная постановка подписи.**

(a) Выбирается коалиция **K** из **t** участников. Каждый участник коалиции вычисляет частичную подпись по формуле $\mathbf{S_u(m) = m^{s_u(0)} \bmod N}$, где **m** – значение хэш-функции от подписываемого сообщения и $\mathbf{u \in K}$.

(b) После получения **t** частичных подписей сборщик подписи составляет матрицу **G** для членов коалиции **K** и обращает ее над полем рациональных чисел.

(c) Сборщик подписи вычисляет $\mathbf{G' = \lambda \cdot G^{-1}}$, где $\mathbf{\lambda}$ – наименьшее общее кратное знаменателей всех элементов матрицы $\mathbf{G^{-1}}$.

(d) Используя матрицу $\mathbf{G'}$, он вычисляет:

$$\mathbf{S'(m) = \left( \prod_{j=1}^{t} \left( S_{u_j}(m) \right)^{g'_{1j}} \right) \bmod N}.$$

(e) Сборщик находит **x,y** такие, что $\mathbf{x\lambda + ye = 1}$.

(f) Подпись вычисляется как $\mathbf{S(m) = \left( (S'(m))^x \cdot m^y \right) \bmod N}$.

**3. Выдача проекции ключа новому узлу.**

(a) Для получения проекции секретного ключа новый узел **u** должен найти коалицию **K** из **t** уже проинициализированных узлов и сообщить им свое $\mathbf{id_{new}}$.

(b) Каждый участник коалиции **u** вычисляет значение своей функции в точке $\mathbf{x} = \mathbf{id}_{\mathbf{new}}$, получая $\mathbf{f}(\mathbf{id}_{\mathbf{new}}, \mathbf{id}_{\mathbf{u}}) = \mathbf{s}_{\mathbf{new}}(\mathbf{id}_{\mathbf{u}}) = \mathbf{s}_0 + \mathbf{s}_1(\mathbf{y} \bmod \mathbf{Q}) + \ldots + \mathbf{s}_{\mathbf{t}-1}(\mathbf{y}^{\mathbf{t}-1} \bmod \mathbf{Q})$ в точке $\mathbf{y} = \mathbf{id}_{\mathbf{u}}$, и посылает его новому узлу.

(c) Новый узел находит свою проекцию секрета $(\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{\mathbf{t}-1})$, решая систему уравнений:

$$\left[\mathbf{s}_0\ \mathbf{s}_1\ \ldots\ \mathbf{s}_{\mathbf{t}-1}\right]\mathbf{G} = \left[\mathbf{s}_{\mathbf{new}}(\mathbf{x}_{\mathbf{i}_1})\ \mathbf{s}_{\mathbf{new}}(\mathbf{x}_{\mathbf{i}_2})\ \ldots\ \mathbf{s}_{\mathbf{new}}(\mathbf{x}_{\mathbf{i}_t})\right].$$

Таким образом, выдача проекции секретного ключа новому узлу не требует участия дилера и является неинтерактивной.

В заключение отметим, что предложенная схема распределенной подписи *RSA* обладает следующими достоинствами: действия участников коалиции при постановке подписи независимы, протокол выдачи проекций секретного ключа неинтерактивен и не требует участия дилера после инициализации системы.

# *РАСПРЕДЕЛЕННАЯ ВЕРИФИКАЦИЯ РЕЗУЛЬТАТА АГРЕГАЦИИ ДАННЫХ В СЕНСОРНЫХ СЕТЯХ*

*Е.А. Крук, А.Д. Фомин*

В современном мире беспроводные сенсорные сети помогают решать всевозможные задачи, связанные с мониторингом различных процессов и территорий. Сенсорные сети состоят из множества сенсоров, распределенных по исследуемой поверхности, и базовой станции, с помощью которой осуществляется контроль и управление сетью. Сенсоры являются автономными устройствами, обладают низкопроизводительным процессором, небольшим объемом памяти и маломощным передатчиком. Задачей каждого сенсора является сбор определенной информации и последующая ее передача на базовую станцию.

Использование агрегации в сенсорной сети позволяет значительно повысить экономичность и живучесть сети. В том случае, когда базовой станции требуется определить интегральную характеристику для какого-либо участка сети, один из узлов этого участка назначается агрегатором. Он собирает с остальных узлов этого участка частные значения определяемой характеристики, вычисляет агрегатную функцию от них (среднее, минимум, максимум и т.д.) и передает это значение базовой станции. При этом общие затраты на передачу информации существенно ниже, чем при отсутствии агрегатора. Если количество сенсоров в сети достаточно велико, сеть обычно разбивается на кластеры и агрегация выполняется в каждом кластере независимо.

Так как сенсорные сети часто разворачиваются на открытой и легкодоступной территории, необходимо использовать специальные процедуры для защиты передаваемой информации от возможных случайных или преднамеренных искажений. Обеспечение надежности агрегированного результата наиболее важно, так как его искажение может привести к более сильному искажению информации о контролируемых параметрах, чем искажение данных отдельных сенсоров.

Известны два способа обеспечения надежной агрегации. Первый основан на распределенности процесса агрегации путем вовлечения в него дополнительных сенсоров. Второй способ основан на усложнении протокола взаимодействия между базовой станцией и агрегатором. В рамках этого протокола агрегатор должен доказать базовой станции корректность представленного результата.

Так, в рамках первого подхода известна схема, основанная на использовании древовидной маршрутизации. Корнем дерева является базовая станция. Направление агрегации – от листьев к корню. При этом в каждом узле вычисляется агрегатная функция от значений, полученных от потомков, и вычисленное значение вместе со значениями аргументов передается узлу-родителю. В этом случае узел-родитель может проверить правильность агрегации, выполненной дочерними узлами. Однако данная схема не обладает достаточной надежностью: в частности, результат агрегации может оказаться некорректным при неправильной работе двух соседних узлов в дереве. Более того, в данном протоколе ограничено число вычисляемых функций агрегации, например, невозможно вычислить медиану.

Другое решение основано на использовании так называемых узлов-свидетелей, которые фактически дублируют действия агрегатора. Если результат агрегации, полученный свидетелями, совпадает с результатом агрегатора, то они подписывают результат. После этого агрегатор отправляет результат и подписи свидетелей на базовую станцию. Недостатком данного решения является то, что объем передаваемых сенсорами данных ли-