На правах рукописи

Синев Валерий Евгеньевич

Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований

Специальность: 05.13.19 –
Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2017

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» (Университет ИТМО)

Научный руководитель: **Молдовян Николай Андреевич**
доктор технических наук, профессор
Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)

Официальные оппоненты: **Александрова Елена Борисовна**
доктор технических наук, доцент, профессор кафедры «Информационная безопасность компьютерных систем» ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого»

Татарникова Татьяна Михайловна
доктор технических наук, доцент, профессор кафедры безопасности информационных систем ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения»

Ведущая организация: Акционерное общество «Научно-исследовательский институт «Вектор» (АО «НИИ «Вектор»)

Защита диссертации состоится “21” декабря 2017 г. в __:__ часов на заседании диссертационного совета Д 002.199.01 при Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН) по адресу: 199178, Россия, Санкт-Петербург, 14 линия, дом 39.

С диссертацией можно ознакомиться в библиотеке и на сайте Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН), www.spiiras.nw.ru.

Автореферат разослан “____” _____ 2017 г.

Ученый секретарь диссертационного совета Д 002.199.01

кандидат технических наук  Зайцева А.А

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Тенденции расширения областей применения информационных технологий, связанных с обработкой, хранением и передачей информации, представленной в цифровом формате, связаны с решением задач обеспечения требуемого уровня информационной безопасности и неотрекаемости (неотказуемости) от содержания электронных сообщений и документов. Решение последней задачи связано с применением электронной цифровой подписи (ЭЦП). Разнообразие информационных технологий, в которых требуется обеспечить неотрекаемость от информации, представленной в электронном виде, определило появление разнообразных типов алгоритмов и протоколов ЭЦП. В случае электронных сообщений и документов, порождаемых коллегиальными органами или коллективами пользователей задача обеспечения неотрекаемости решается с помощью протоколов мультиподписи, которые дают возможность снизить информационную избыточность, связанную с формированием ЭЦП как дополнительного сообщения, присоединяемого к электронному документу. Недостатком известных протоколов мультиподписи является использование нестандартной инфраструктуры открытых ключей и нарушение основополагающего принципа полного недоверия участников протокола ЭЦП друг к другу. Эти недостатки сужают функциональность протоколов ЭЦП, и как следствие, области их применения. Одним из базовых требований к протоколам ЭЦП является их безопасность, т.е. высокая вычислительная сложность подделки цифровой подписи при использовании лучших известных алгоритмов подделки и низкая вероятность появления в обозримом будущем прорывных способов подделки подписи. Для количественной оценки безопасности протоколов ЭЦП используется векторный показатель безопасности в виде пары значений, которые отражают обеспечиваемое значение стойкости и интегральный показатель безопасности, который определяется как отношение обеспечиваемой стойкости к вероятности появления прорывного алгоритма подделки подписи.

Применение алгебраических алгоритмов защитных преобразований для обеспечения информационной безопасности информационно-телекоммуникационных технологий для защиты от атак с принуждением пользователя к раскрытию ключа преобразования требует придания алгоритмам такого типа новых функциональных возможностей. В частности защита от указанных атак потенциально может быть обеспечена разработкой псевдовероятностных алгебраических алгоритмов защитных преобразований позволяющих неоднозначное восстановление преобразованной информации. Тема диссертационного исследования связана с устранением указанных недостатков протоколов обеспечения неотрекаемости и алгоритмов защитных преобразований, что определяет её актуальность.

Степень разработанности темы. В настоящее время теория цифровых подписей является развитой областью современной криптографии и в развитых странах приняты стандарты ЭЦП. Протоколы индивидуальной цифровой

подписи нашли широкое применение в современных информационных технологиях. Достаточно хорошо исследован вопрос построения протоколов мультиподписи (групповых, коллективных, агрегированных подписей и др.), однако для их широкого применения требуется решить задачу построения протоколов таких типов с использованием имеющейся инфраструктуры открытых ключей и стандартов ЭЦП. Вопрос использования алгебраических операций в качестве примитивов защитных преобразований блочного типа и конечных некоммутативных групп в качестве примитива криптосхем с открытым ключом затрагивался различными исследователями, однако вопросы разработки псевдовероятностных алгоритмов защитных преобразований алгебраического типа и вопросы использования задачи скрытого дискретного логарифмирования для построения алгоритмов строгой аутентификации не затрагивались.

Цель и задачи исследования. Цель данной работы состоит в расширении функциональности и повышении уровня безопасности протоколов обеспечения неотрекаемости от электронных сообщений и документов и алгоритмов защитных преобразований. Для достижения этой цели были сформулированы и решены следующие исследовательские задачи:

- Разработка метода и построение протокола утверждаемой групповой ЭЦП, обладающего повышенной безопасностью;
- Разработка метода и построение протокола утверждаемой групповой ЭЦП, свободной от использования вспомогательных открытых ключей;
- Построение протокола утверждаемой групповой подписи, функционирующего с использованием стандартной инфраструктуры открытых ключей;
- Разработка метода построения и протокола коллективной ЭЦП, в котором формируется единая подпись для произвольной совокупности групповых подписантов;
- Построение протокола коллективной ЭЦП, в котором формируется единая подпись для произвольной совокупности групповых подписантов и произвольной совокупности индивидуальных подписантов;
- Выполнение оценивания безопасности алгебраических алгоритмов защитных преобразований;
- Разработка метода и построение псевдовероятностных алгебраических алгоритмов защитных преобразований.

Научная новизна диссертационного исследования заключается в следующем:

1. Разработан протокол утверждаемой групповой ЭЦП, основанный на вычислениях по простому модулю и отличающийся выполнением вспомогательной операции возведения в целочисленную степень по трудно разложимому модулю и вычислением рандомизирующих экспонент, маскирующих открытые ключи подписантов, как значения однонаправленной функции в зависимости от открытых ключей подписантов и секретного ключа

руководителя группы подписантов, за счет чего обеспечивается повышение уровня безопасности, обеспечиваемого протоколом.

2. Разработан метод построения протоколов коллективной ЭЦП, отличающийся тем, что рандомизирующий параметр подписи формируется несколькими групповыми подписантами, благодаря чему обеспечивается возможность выработки единой ЭЦП, разделяемой несколькими групповыми подписантами, что дает практически важное расширение функциональности протоколов коллективной подписи.

3. Разработан метод построения протоколов комбинированной коллективной ЭЦП, отличающийся тем, что рандомизирующий параметр подписи формируется несколькими групповыми подписантами и несколькими индивидуальными подписантами, благодаря чему обеспечивается возможность выработки единой ЭЦП, разделяемой несколькими групповыми подписантами и несколькими индивидуальными подписантами, что дает практически важное дополнительное расширение функциональности протоколов групповой подписи.

4. Разработан способ повышения производительности алгебраических псевдовероятностных алгоритмов защитных преобразований, отличающийся представлением блоков преобразуемых данных в виде элементов конечного расширенного поля, заданного в явной векторной форме, благодаря чему обеспечивается повышение производительности алгоритма защитного преобразования.

Теоретическая и практическая значимость работы. Теоретическая значимость работы состоит в разработке новых типов мультиподписи – протоколов коллективной ЭЦП с участием групповых подписантов. Практическая значимость состоит в расширении функциональности протоколов мультиподписи и повышением уровня обеспечиваемой безопасности протоколами утверждаемой групповой ЭЦП. Результаты оценивания безопасности алгебраических алгоритмов защитных преобразований представляют интерес для выбора типа защитных преобразований при решении практических задач информационной безопасности, а также в учебном процессе.

Методология и методы исследования. В работе использован аппарат и методы математической статистики, теории вероятности, алгебры, теории чисел, криптографии и вычислительные эксперименты. *Объектом* исследования являются информационные технологии; *предметом* –способы, алгоритмы и протоколы обеспечения неотрекаемости от информации, представленной в цифровом формате.

Положения, выносимые на защиту.

1. Метод построения и протокол утверждаемой групповой ЭЦП, построенный на основе вычислений по модулю простого числа с трудно разложимой функцией Эйлера, обеспечивает повышение уровня безопасности протоколов данного типа.

2. Метод построения и протокол коллективной ЭЦП, обеспечивающий формирование единой цифровой подписи, разделяемой произвольным числом групповых подписантов.

3. Метод построения и протокол коллективной ЭЦП, использующий стандартную инфраструктуру открытых ключей и обеспечивающий формирование единой цифровой подписи, разделяемой произвольным числом групповых подписантов и произвольным числом индивидуальных подписантов.

4. Способ псевдовероятностного защитного преобразования информации, отличающийся реализацией вычислений в конечных полях, заданных в явной векторной форме, благодаря чему обеспечивается повышение производительности алгоритма защитного преобразования информации.

Степень достоверности и апробация результатов. Обоснованность научных положений, выводов и практических рекомендаций, полученных в диссертационной работе, обеспечивается анализом состояния исследований в данной области на сегодняшний день, формальными доказательствами, вычислительным экспериментом и апробацией результатов на всероссийских научно-практических конференциях с международным участием: VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009)» (Санкт-Петербург, 28-30 октября 2009), XI Санкт-Петербургская международная конференция «Региональная информатика-2008 (РИ-2008)» (Санкт-Петербург, 22-24 октября 2008), XII Санкт-Петербургская международная конференция Региональная информатика «РИ-2010» (Санкт-Петербург, 20-22 октября 2010г), IX Санкт-Петербургская межрегиональная конференция (Санкт-Петербург, 28-30 октября 2015 г).

Результаты диссертационной работы использованы в производственной деятельности ООО «Удостоверяющий центр ГАЗИНФОРМСЕРВИС» и внедрены в учебный процесс кафедры информационной безопасности Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» имени В.И.Ульянова(Ленина) на старших курсах обучения студентов по специальности «090900 – Информационная безопасность».

Основные результаты диссертации изложены в 14 публикациях, в том числе, в 5 статьях опубликованы в ведущих рецензируемых журналах, входящих в перечень ВАК.

Структура и объем работы. Диссертационная работа изложена на 166 страницах, включает 5 глав, 11 рисунков, 4 таблицы и список литературы из 126 наименований.

СОДЕРЖАНИЕ РАБОТЫ

Во введении показана актуальность темы диссертации, сформулированы цели исследования и решаемые задачи, определена научная новизна и приведено краткое содержание работы по главам.

В первой главе были рассмотрены известные способы, алгоритмы и протоколы обеспечения неотказуемости от электронных сообщений и документов, используемые в современных информационных технологиях.

Представлены известные схемы и протоколы мультиподписи. Выполнена постановка задач диссертационного исследования.

Вторая глава посвящена разработке протоколов слепой и утверждаемой групповой подписи, обладающих повышенным уровнем безопасности. Для построения протокола слепой подписи был использован ранее известный метод, который состоит в использовании простого модуля p, задаваемого в качестве одного из элементов открытого ключа подписанта и имеющего специальную структуру вида p = 2n + 1, где n = qr, q и r – простые числа, разрядность которых равна или превышает 512 бит и являющиеся элементами личного секретного ключа владельца открытого ключа (подписанта). Известный метод был дополнен механизмом маскирования слепой подписи с использованием операции возведения в степень по модулю n одного из маскирующих параметров. Разработанный протокол слепой ЭЦП включает следующие шаги:

1. Подписант генерирует равновероятное случайное число $k < q$, вычисляет значение $\rho' = \alpha^k \bmod p$ и направляет последнее пользователю А.

2. Пользователь А формирует случайные равновероятные значения маскирующих параметров $\mu, \varepsilon \in \{1, 2, \ldots, n-1\}$, вычисляет значения $\rho = \rho' y^{\mu}\alpha^{\varepsilon} \bmod p$, $R = \rho \bmod n$ и $R' = R/H + \mu \bmod n$, где H–хэш-значение от подписываемого документа, вычисленное по некоторому специфицированному алгоритму хэширования (например, в соответствии с алгоритмом хэширования, заданным стандартом ГОСТ Р 34.11–94). Значение R является неизвестным подписанту и представляет собой первый элемент подлинной цифровой подписи. Число R' представляет собой значение первого элемента слепой подписи.

3. Пользователь А передает подписанту значение R'.

4. Подписант вычисляет значение $S' = k + zR' \bmod n$, где z– его секретный ключ, передает значение S' (второй элемент слепой подписи) пользователю А.

5. Пользователь А генерирует случайное число $\delta < n$ и вычисляет значение $D = \delta^e H(S' + \varepsilon) \bmod n$, которое направляет подписанту.

6. Подписант вычисляет значение $D' = D^d \bmod n$, где d является образным значением к e по модулю $\varphi(n)$: $d = e^{-1} \bmod (p-1)(q-1)$. Затем он направляет значение D' пользователю А.

7. Пользователь А вычисляет второй элемент подписи $S = \delta^{-1} D' = H[k + zR' + \varepsilon]^d \bmod n$.

Процедура проверки подлинности ЭЦП (R, S) к документу M выполняется следующим образом:

1. Вычисляется хэш-значение H от документа M и число $R^* = (y^{-R/H}\alpha^{S^e/H} \bmod p) \bmod n$.

2. Если имеет место $R^* = (R, S)$, то подпись (R, S) принимается как подлинная.

В итоге по описанному выше протоколу для генерации подписи вслепую получили ЭЦП с параметрами (R, S). Она является подлинной, если она вместе со значением хэш-функции H от сообщения M проходит уравнение проверки ЭЦП, указанное в п. 1, как верная (подлинная) подпись. Выполнено доказательство корректности протокола.

Для построения протокола УГП, взлом которого требует одновременного решения ЗФ и ЗДЛ, используется простое число p, имеющее вид $p = 2n + 1$, где n – трудно разложимое составное число, и протокол (см. глава 2) в качестве прототипа. Простое число p используется в качестве одного из элементов открытого ключа руководителя, а значит и коллегиального органа, осуществляющего подписывание электронных документов. Таким образом, в предлагаемом протоколе предполагается, что руководитель генерирует случайные 512-битовые сильные простые числа q и r, такие, что число $p = 2n + 1$ также является простым. Затем он вырабатывает число α, имеющее по модулю p порядок, равный n, выбирает случайное число z, имеющее разрядность не менее 256 бит, вычисляет значения $L = \alpha^z \bmod p$ и $\varphi(n) = (q - 1)(r - 1)$, генерирует случайное 32-битовое значение e и вычисляет число $d = e^{-1} \bmod \varphi(n)$. После этого он уничтожает значения q и r и предоставляет четверку чисел (p, α, L, e) как открытый ключ коллегиального органа. Значения z и d составляют личный секретный ключ руководителя. Вычислительная невозможность нахождения значения d по значению e связана с необходимостью факторизации числа n для вычисления значения $\varphi(n)$ и обосновывается также как и в случае криптосистемы RSA.

Каждый j-тый подписант ($j = 1,2, \ldots, g$) генерирует свой личный секретный ключ x_j и вычисляет свой открытый ключ y_j по формуле

$$y_j = \alpha^{x_j} \bmod p .$$

Важно отметить, что платой за повышение уровня безопасности является то, что открытые ключи подписантов оказываются привязанными к открытому ключу руководителя, хотя, естественно, последний не знает личных секретных ключей подписантов. Также существенным отличием предложенного протокола является использование метода формирования рандомизирующей экспоненты λ_i с двукратным вычислением значений хэш-функции от открытого ключа y_i, к которому присоединяется первый раз личный секретный ключ, а второй раз – первое хэш-значение. Этот метод даёт руководителю возможность доказать другим лицам, что идентифицированные при раскрытии некоторой групповой ЭЦП подписанты действительно участвовали в процедуре генерации этой ЭЦП. Процедура формирования групповой подписи к электронному документу M , выполняемая m подписантами, описывается следующими шагами:

1. Руководитель, используя предписанную хэш-функцию F_H вычисляет рандомизирующие экспоненты λ_i по формуле $\lambda_i = F_H(H||P_i||F_H(H||P_i||d))$, где знак $||$ обозначает операцию конкатенации битовых строк ($i = 1,2, \ldots, m$). Затем он направляет каждое значение λ_i (предварительно зашифровав его по открытому

ключу *i*-того подписанта, например с помощью алгоритма открытого шифрования Эль-Гамаля) только *i*-тому подписанту и вычисляет первый элемент групповой ЭЦП в виде значения $U = \prod_{i=1}^{m} y_i^{\lambda_i} \bmod p$.

2. Каждый *i*-ый подписант выбирает случайное $t_i < n$, вычисляет $R_i = \alpha^{t_i} \bmod p$ и отправляет значение R_i руководителю.

3. Руководитель генерирует случайное $T < n$ и вычисляет значения $R' = \alpha^{T} \bmod p$ и $R = R'(R_1 R_2 ... R_m) \bmod p = \alpha^{T+t_1+t_1+..+t_m} \bmod p$ и$E = F_H(M||R||U)$, где E – второй элемент групповой ЭЦП. Руководитель направляет значение R каждому *i*-тому подписанту (i = 1,2, …, m).

4. Каждый *i*-ый подписант вычисляет значение своей доли подписи $S_i = t_i + x_i \lambda_i E \bmod n$, где i = 1,2, …, m, и направляет руководителю значение S_i.

6. Руководитель проверяет корректность каждой из долей S_i (i = 1,2, …, m) путем проверки выполнимости равенства $R_i = y_i^{-\lambda_i E} \alpha^{S_i} \bmod p$. Если все доли S_i вычислены корректно, то руководитель вычисляет свою долю подписи $S' = T + zE \bmod n$ и значение $S = (S' + S_1 + S_2 + ... + S_m)^d \bmod n$ в качестве третьего элемента групповой ЭЦП.

Проверка подлинности групповой ЭЦП (U, E, S) к документу M выполняется следующим образом:

1. Вычислить хэш-значение от документа: $H = F_H(M)$.

2. По открытому ключу (p, α, L, e) и подписи (U, E, S) найти значение

$$\tilde{R} = (UL)^{-E} \alpha^{\left(S^e \bmod \frac{p-1}{2}\right)} \bmod p.$$

3. Вычислить значение $\tilde{E} = F_H\left(M \,\|\, \tilde{R} \| U\right)$.

4. Выполнить проверку равенства значений E и $\tilde{E}$. Если $\tilde{E} = E$, то групповая подпись (U, E, S) принимается как подлинная, иначе подпись отвергается.

Существенное отличие разработанного протокола по сравнению с прототипом является то, что при подстановке значения третьего элемента подписи S в проверочное соотношение последний возводится в степень e по модулю $\frac{p-1}{2} = n$. Поэтому в случае появления прорывного алгоритма решения ЗДЛ по простому модулю и вычислительно эффективной возможности вычисления секретных ключей z и x_j (i = 1,2, …, m) для генерации подписи останется необходимым вычисление корня *e*-ой степени по трудно разложимому модулю n, т.е. для взлома предложенного протокола потребуется решить как ЗДЛ по модулю p, так и задачу факторизации модуля n. Лучшие известные алгоритмы решения этих задач имеют субэкспоненциальную сложность, причем при одинаковом размере чисел p и n трудоемкость этих алгоритмов имеет один порядок.

При одинаковом размере простого модуля p предложенный протокол имеет стойкость в два раза более высокую по сравнению со стойкостью протокола, использованного в качестве прототипа, но это увеличение стойкости не имеет практического значения в повышении уровня интегральной безопасности. Существенный рост значения последнего параметра достигается за счет того, что вероятность появления прорывного алгоритма взлома для предложенного протокола имеет существенно более низкое значение.

Использование двукратного вычисления хэш-функции при формировании маскирующих экспонент обеспечивает возможность доказать без раскрытия личного секретного ключа d любым другим лицам, что руководитель при раскрытии групповой подписи правильно идентифицирует подписантов. Для этого он предъявляет набор маскирующих экспонентλ_i и для каждого из последних – уникальное значение δ_i, такое, что выполняется соотношение $\lambda_i = F_H(H||P_i||\delta_i) \neq F_H(H||P_i)$. В ходе такого доказательства руководителю нет необходимости раскрытия своего секретного ключа d, что потребовалось бы в случае вычисления маскирующих экспонент по формуле $\lambda_i = F_H(H||P_i||d)$. По представленным маскирующим экспонентам вычисляются модифицированные открытые ключи подписантов и их коллективный открытый ключ U, равный соответствующему значению в раскрываемой групповой подписи и зависящий от набора маскирующих коэффициентов в соответствии с формулой

$$U = \prod_{i=1}^{m} y_i^{\lambda_i} \bmod p.$$

Поскольку хэш-функция является вычислительно необратимой, набор маскирующих коэффициентов для данного значения хэш-функции, вычисленной от подписанного документа, могут быть восстановлены руководителем только в случае, если они действительно вычислялись до момента раскрытия подписи, а именно, в ходе формирования раскрываемой групповой подписи. При этом требуется восстановить уникальное значение δ_i. Руководитель и только он имеет возможность это сделать, поскольку последний параметр вычислялся с использованием его секретного ключа по формуле $\delta_i = F_H(H||P_i||d)$. Предоставление руководителем значения δ_i при раскрытии подписи доказывает то, что именно по этому значению вычислялось значение λ_iпри выполнении процедуры формирования групповой подписи.

Процедура идентификации подмножества подписантов включает в себя вычисление коллективных открытых ключей подписантов для всех возможных подмножеств, пока не будет получен коллективный открытый ключ, фигурирующий в значении групповой подписи в качестве одного из ее трех элементов.

Определенным недостатком предложенного протокола по сравнению с протоколом-аналогом является увеличение размера групповой ЭЦП до 2208 бит при обеспечении 80-битовой стойкости. При таком уровне стойкости размер подписи протоколе, использованном в качестве прототипа, размер подписи составляет 1344 бит. Для приложений, в которых первостепенным требованием

является обеспечение высокого уровня безопасности данный недостаток не представляется существенным.

Третья глава посвящена разработке протоколов коллективной подписи для групповых и индивидуальных подписантов. Достаточно реальным случаем является разработка электронного документа несколькими организациями, выступающими в роли групповых подписантов. Использование известных протоколов групповой подписи для этого случая связано с формированием нескольких независимых цифровых подписей. С целью обеспечения возможности формирования единой цифровой подписи, по которой можно доказательно проверить, что все ответственные стороны действительно подписали документ, представляет интерес разработка протокола коллективной ЭЦП для групповых подписантов, в которых размер подписи не зависит от числа индивидуальных подписантов. Изучение схем построения коллективной подписи и утверждаемой групповой подписи (УГП) показало, что эти два типа подписей могут быть объединены в едином протоколе коллективной ЭЦП для групповых подписантов. То есть методом реализации протоколов коллективной ЭЦП для групповых подписантов может служить задание процедур формирования долей подписи, генерируемых каждым групповым подписантом, и объединение всех долей подписи в единую подпись в соответствии с механизмами известных протоколов коллективной ЭЦП.

В соответствии с таким методом протокол коллективной ЭЦП для групповых подписантов может быть построен путем модифицирования известного в литературе протокола УГП, заключающегося в замене в последнем механизма маскирования открытых ключей подписантов, основанного на схеме открытого шифрования RSA, на маскирующий механизм, основанный на вычислении хэш-функции от аргумента, зависящего от секретного ключа руководителя группы подписантов (см. главу 2). Такая замена позволяет использовать один и тот же модуль для различных групповых подписантов при выполнении ими модульных вычислений для генерации ЭЦП и применить модифицированный протокол в качестве основы для протокола коллективной подписи для групповых подписантов.

Применяя такой метод построения, был разработан протокол коллективной ЭЦП для групповых подписантов, который описывается следующим образом. В протоколе используются следующие параметры:

1) достаточно большое простое число p (разрядностью не менее 2464 бит), такое, что число $p - 1$ содержит простой делитель q размером не менее 256 бит;

2) число α, порядок которого по модулю p равен значению q. Каждый представитель группы подписывающих генерирует свой личный секретный ключ в виде случайного числа x размером не менее 256 бит и свой открытый ключ $y = \alpha^x \bmod p$.

Открытый ключ руководителя L вычисляется по формуле $L = \alpha^X \bmod p$, где X – его секретный ключ. Значение L одновременно является открытым

ключом группы, по которому проверяется подлинность групповой ЭЦП. Предполагается, что открытые ключи всех подписантов и руководителя регистрируются в удостоверяющем центре. Таким образом, они могут подписывать электронные документы не только в рамках протокола УГП, но как индивидуальные подписанты.

Пусть m подписантов, являющихся представителями одной из групп, обладают открытыми ключами $y_i = \alpha^{x_i} \bmod p$, где $i = 1,2, \ldots, m$; x_i – личный секретный ключ i-го подписанта. Формирование групповой подписи указанной группы подписантов к документу M выполняется по следующему алгоритму, входящему составной частью в протокол коллективной ЭЦП для групповых подписантов. Алгоритм вычисления долевого значения отдельного группового подписанта в коллективной групповой подписи включает следующие шаги (Рис. 3.1):

1. Руководитель вычисляет рандомизирующий параметр λ_i для каждого лица, являющегося внутренним подписантом документа M, по формуле $\lambda_i = F_H\left(H \parallel y_i \parallel F_H\left(H \parallel y_i \parallel X\right)\right)$, где $\parallel$ – операция конкатенации; F_H – некоторая специфицированная хэш-функция; $H = F_H(M)$, и передает каждое значение λ_i только i-тому подписанту. Затем руководитель вычисляет первый элемент групповой ЭЦП в виде значения $U = \prod_{i=1}^{m} y_i^{\lambda_i} \bmod p$.

2. Каждый i-ый подписывающий ($i = 1,2, \ldots, m$) генерирует случайное число $k_i < n$ и вычисляет значение $R_i = \alpha^{k_i} \bmod p$ и передает его руководителю.

3. Руководитель формирует случайное число $K < q$ и вычисляет $R' = \alpha^K \bmod p$ и значения $R = R' \prod_{i=1}^{m} R_i \bmod p = \alpha^{K + \sum_{i=1}^{m} k_i}$ и $E = F_H(M||R||U)$,где E – второй элемент групповой ЭЦП.

4. Каждый i-ый подписант ($i = 1,2, \ldots, m$) вычисляет свою долю подписи $S_i = t_i - x_i \lambda_i E \bmod q$, где $i = 1,2, \ldots, m$, и направляет руководителю значение S_i. и направляет ее руководителю.

5. Лидер проверяет корректность каждой доли путем проверки выполнимости равенства $R_i = y_i^{\lambda_i E} \alpha^{S_i} \bmod p$. При условии, что все доли цифровой подписи вычислены корректно, то он вычисляет свою долю подписи $S' = K + XE \bmod q$, а затем – третий элемент групповой подписи $S = S' + \sum_{i=1}^{m} S_i \bmod q$.

В ходе выполнения протокола формирования коллективной групповой ЭЦП данный алгоритм выполняется по частям в следующей последовательности:

1) каждый j-ый (j = 1,2, …, g; g – количество групповых подписантов) групповой подписант выполняет независимо шаги 1–3 алгоритма, за исключением вычисления значения $E = F_H(M||R_j||U_j)$;

2) все групповые подписанты рассылают свое значение параметра R_j и свое значение параметра U_j друг другу, а затем вычисляется произведение R (по mod$p$) всех значений первого параметра $R = R_1R_2...R_g \bmod p$
и произведение всех значений второго параметра: $U = U_1U_2...U_g \bmod p$

3) вычисляется общее значение $E = F_H(M||R||U)$;

4) по общему значению E каждый j-ый групповой подписант вычисляет значение своей доли подписи $S_j = S'_j + \sum_{i=1}^{m} S_{ji} \bmod q$,

где S_{ji} -- доля подписи i-го (i = 1,2, …, m_j) индивидуального подписанта в доле подписи j-го группового подписанта; S'_j -- доля подписи руководителя j-ой группы индивидуальных подписантов;

5) вычисляется общее значение $S = \sum_{j=1}^{k} S_j \bmod q$.

Коллективной групповой ЭЦП является тройка чисел (U, E, S).

При выполнении приводимого далее протокола коллективной ЭЦП для групповых подписантов выполняется проверка корректности долей подписи, генерируемых групповыми подписантами. Проверка подлинности доли S_j в коллективной групповой ЭЦП (U, E, S) к документу M выполняется следующим образом:

1. По открытому ключу L_j заданного группового подписанта и подписи и значениям U_j, E и S_j найти значение $\tilde{R}_j = \left(UL_j\right)^E \alpha^{S_j} \bmod p$.

2. Вычислить значения $\tilde{R}_j$ и R_j.

3. Если $\tilde{R}_j = R_j$, то доля (U_j, E, S_j) в коллективной групповой подписи признается подлинной и это значение используется для генерации значения коллективной групповой подписи, в противном случае эта доля отвергается и j-ый групповой подписант должен скорректировать значение своей доли.

Легко заметить, что значение $D = \sum_{i=1}^{m} S_i \bmod q$, которое является предварительной подписью, утверждаемой руководителем путем сложения по модулю q со значением S', фактически представляет собой коллективную подпись всех подписантов, для формирования которой они использовали модифицированные открытые ключи. В разработанном протоколе схема коллективной подписи используется двояким образом – для формирования предварительной подписи и для формирования коллективной подписи для некоторого числа групповых подписантов.

Предлагаемый протокол коллективной ЭЦП для групповых подписантов описывается следующим образом. Пусть g групповых подписантов, обладающих открытыми ключами $L_j = \alpha^{X_j} \bmod p$, где $j = 1,2, \ldots, k$; X_j – личный секретный ключ руководителя j-й группы подписантов. Формирование коллективной групповой ЭЦП к документу M выполняется следующим образом.

1. В рамках описанного ранее алгоритма вычисления доли в коллективной групповой ЭЦП руководитель каждой j-ой группы подписантов ($j = 1,2, \ldots, g$) организует выработку маскирующих параметров для своих подписантов и j-ой доли в первом элементе коллективной групповой подписи, т.е. значения U_j, а также выработку рандомизирующего параметра $R_j = \alpha^{K_j} \bmod p$. Затем он направляет значения U_j и R_j всем другим руководителям.

2. Каждый j-ый руководитель вычисляет значения $U = \prod_{j=1}^{g} U_j \bmod p$, $R = \prod_{j=1}^{g} R_j \bmod p = \alpha^{\sum_{j=1}^{g} K_j} \bmod p$ и $E = F_H(M||R||U)$, где U и E – первый и второй элементы коллективной групповой ЭЦП, соответственно.

3. Каждый j-ый руководитель ($j = 1,2, \ldots, g$) вычисляет свою долю подписи S_j и рассылает значение S_j остальным руководителям. При этом для правильно вычисленной доли S_j выполняется соотношение $R_j = \left(U_j L_j\right)^E \alpha^{S_j} \bmod p$ (по которому выполняется проверка корректности доли подписи предоставленной j-ым руководителем). Затем он рассылает значение S_j остальным пользователям, которые могут проверить правильность значения по последней формуле.

4. Если проверка всех долей S_j подтвердила их правильность, то вычисляется третий элемент групповой подписи по формуле $S = \sum_{j=1}^{g} S_j \bmod q$.

Проверка подлинности групповой ЭЦП (U, E, S) к документу M выполняется следующим образом:

1. Вычисляется коллективный открытый ключ как произведение открытых ключей всех групповых подписантов:

$$L = \prod_{j=1}^{g} L_j \bmod p = \alpha^{\sum_{j=1}^{g} X_j} \bmod p.$$

2. Вычислить значение $\tilde{R} = (UL)^E \alpha^S \bmod p$

3. Вычислить значение $\tilde{E} = F_H(M \parallel \tilde{R} \parallel U)$.

4. Сравнить значения E и $\tilde{E}$. Если $\tilde{E} = E$, то коллективная групповая подпись (U, E, S) признается подлинной, в противном случае подпись отвергается.

В предложенном протоколе коллективной групповой подписи восстановление лиц, участвовавших в формировании некоторой заданной коллективной подписи (идентификация индивидуальных подписантов) в одной или всех группах подписывающих требует участия всех руководителей. Процедура идентификации (раскрытие групповой подписи) выполняется по аналогии с процедурой раскрытия групповой подписи в протоколе УГП, описанном во второй главе.

Также достаточно реальным случаем является разработка электронного документа несколькими индивидуальными подписантами и несколькими организациями, выступающими в роли групповых подписантов. Построение протокола коллективной ЭЦП для данного случая может быть выполнено в полном соответствии с протоколом коллективной ЭЦП для групповых подписантов, описанным в разделе 3.1 диссертации. В качестве метода преобразования протокола коллективной ЭЦП для групповых подписантов в протокол комбинированной коллективной ЭЦП предлагается принятие соглашения о том, что для индивидуальных подписантов значение доли в первом элементе коллективной подписи равно единице, т.е., если j-ый подписант является индивидуальным, то имеем $U_j = 1$.

Впервые разработаны протоколы коллективной цифровой подписи для групповых и индивидуальных подписантов, независимо от соотношения первых и вторых. В случае, когда все подписанты являются индивидуальными, разработанные протоколы вырождаются в протоколы коллективной подписи, подобные протоколам, описанным в работах (см. Глава 3).

Достоинствами протоколов коллективной подписи для групповых подписантов и комбинированной коллективной подписи являются следующие:

- возможность реализации на основе процедур формирования и проверки подлинности ЭЦП на основе стандарта ГОСТ Р 34.11–2012;
- фиксированный размер подписи независимо от числа групповых и индивидуальных подписантов;
- для практического применения протокола можно использовать имеющуюся на практике инфраструктуру открытых ключей.

В четвертой главе рассматриваются вопросы разработки алгебраических алгоритмов защитных преобразований для обеспечения информационной безопасности информационных технологий.

Рассмотрены достоинства и недостатки ряда алгебраических операций при их использовании в качестве примитивов защитных преобразований, включая матричное и векторное умножения. Для разработки алгебраических алгоритмов защитных преобразований блочного типа предложен метод

комбинирования алгебраических операций из различных алгебраических структур. В качестве последних может быть использована операция умножения в конечных полях и кольцах. Например, умножение в простых конечных полях представляет собой умножение чисел по модулю простого числа, а в расширенных конечных полях – умножение многочленов по модулю неприводимого многочлена. Для снижения вычислительной сложности матричного умножения предложен метод задания матриц над конечными полями, заданными в явной векторной форме. Данный метод представляет особый интерес при аппаратной реализации алгебраических алгоритмов защитных преобразований, когда имеется возможность легкого распараллеливания вычислительного процесса.

Для защиты от атак с принуждением раскрытия ключа шифрования разработан алгебраический алгоритм псевдовероятностного шифрования, в котором выполняется совместное шифрование секретного и фиктивного сообщения так, что формируемый шифртекст является вычислительно неразличимым от шифртекста формируемого путем вероятностного шифрования фиктивного сообщения по некоторому фиктивному ключу, который предоставляется атакующему в качестве ключа шифрования. Разработанный алгоритм описывается следующим образом.

Шифруемые секретные сообщения будем разбивать на блоки размером 1024 бит. Битовую строку некоторого блока сообщения обозначим переменной *M*, которую будем рассматривать как вектор $M = (m_1, m_2, ..., m_h)$, координаты которого заданы над простыми конечным полем *GF*(*p*).Фиктивное сообщение разбивается аналогичным образом. Пусть вектор $D = (d_1, d_2, ..., d_h)$ обозначает 1024-битовый блок фиктивного сообщения и операция умножения векторов определена так, что множество всех возможных значений векторов размерности *h* образуют расширенное поле GF(p^h), порядок мультипликативной группы которого делится на многоразрядное (256 бит) простое число. Каждый из используемых ключей K_Q и K_W представляет собой пару векторов и пару чисел (*e*, *d*): $K_Q = (Q_1, Q_2, e_1, d_1)$ и $K_W = (W_1, W_2, e_2, d_2)$. В качестве числа *e* выбирается случайное число *e*, взаимно простое со значением $p^h - 1$, где *h*– разрядность векторов. Второе число *d* вычисляется как значение, обратное к числу *e* по модулю $p^h - 1$. Алгоритм псевдовероятностного защитного преобразования включает следующие шаги:

1. Генерация вектора R_1 по формуле $R_1 = M^{e_1}$.

2.Генерация вектора R_2 по формуле $R_2 = M^{e_2}$.

3. Вычисление блока криптограммы в виде пары векторов $C = (C_1, C_2)$, которая представляет собой решение системы уравнений следующего вида

$$\begin{cases} Q_1 C_1 + Q_2 C_2 = R_1 \\ W_1 C_1 + W_2 C_2 = R_2 \end{cases}.$$

Алгоритм расшифровывания криптограммы $C = (C_1, C_2)$ по ключу $K_Q = (Q_1, Q_2, e_1, d_1)$ состоит в выполнении следующих шагов:

1. Вычисление значения R по формуле $R = Q_1 C_1 + Q_2 C_2 = R_1$.

2. Вычисление блока сообщения N по формуле $N = R^{d_1} = R_1^{d_1} = M$.

Расшифровывание криптограммы $C = (C_1, C_2)$ по ключу $K_W = (W_1, W_2, e_2, d_2)$ состоит в выполнении следующих шагов:

1. Вычисление значения R по формуле $R = W_1 C_1 + W_2 C_2 = R_2$.

2. Вычисление блока сообщения N по формуле $N = R^{d_2} = R_2^{d_2} = D$.

Таким образом, одна и та же криптограмма расшифровывается в различные сообщения в зависимости от использованного ключа. При этом процесс расшифровывания выполняется в единообразной манере, в которой каждый бит криптограммы преобразуется одинаковым способом независимо от значения ключа расшифровывания, т.е. криптограмма неотличима от криптограммы, полученной с помощью процесса вероятностного шифрования, в котором используются случайные параметры Q_1, Q_2, R_1.

В пятой главе рассматриваются протоколы с открытым ключом, использующие матричное умножение.

Для построения стойких протоколов с открытым ключом, основанных на вычислениях в конечных группах невырожденных матриц предложено использовать вычислительную трудность задачи дискретного логарифмирования в скрытой подгруппе. На основе данной задачи разработаны новые протоколы строгой аутентификации удаленных абонентов.

Пусть заданы некоторые элементы $G \in \Gamma$ и $U \in \Gamma$, порядок каждого из которых является достаточно большим простым числом, причем элементы G и U неперестановочны. В качестве секретного ключа выбирается пара чисел (w, x). Открытым является элемент группы Г, вычисляемый по формуле $Y = U^w \circ (G^x) \circ U^{-w}$. При наличии у пользователей аутентичных открытых ключей, вычисленных по последней формуле, протокол взаимной аутентификации двух удаленных пользователей выглядит следующим образом. Знак «$\circ$» обозначает групповую операцию в используемой конечной некоммутативной группе Г.

1. Первый пользователь генерирует случайный элемент R_1 группы Г и направляет R_1 второму пользователю.

2. Второй пользователь, используя полученный элемент R_1, вычисляет следующее: элемент $K = Q^{w_2} \circ Y_1^{x_2} \circ Q^{-w_2}$, значения $h_1 = F_h(R_1), h_2 = F_h(K), h_3 = F_h(KR_1)$ и элемент $Z = K^{h_1} \circ R_1^{h_2} \circ K^{h_3}$. Затем он генерирует случайный элемент R_2 группы Г и отправляет элементы Z и R_2 первому пользователю.

3. Первый пользователь, используя сгенерированный им случайный элемент R_1 группы Г, вычисляет следующее: элемент $K = Q^{w_1} \circ Y_2^{x_1} \circ Q^{-w_1}$, значения $h_1 = F_h(R_1), h_2 = F_h(K), h_3 = F_h(KR_1)$ и элемент $Z' = K^{h_1} \circ R_1^{h_2} \circ K^{h_3}$. Затем он сравнивает элементы Z и Z'. Если выполняется равенство $Z = Z'$, то он делает вывод о подлинности второго пользователя.

4. Первый пользователь, используя полученный элемент R_2 и уже вычисленный элемент $K = Q^{w_1} \circ Y_2^{x_1} \circ Q^{-w_1}$, находит следующее: значения $h_1' = F_h(R_2), h_2' = F_h(K), h_3' = F_h(KR_2)$ и элемент $Z'' = K^{h_1'} \circ R_2^{h_2'} \circ K^{h_3'}$. Затем он и отправляет элементы Z'' второму пользователю.

5. Второй пользователь, используя сгенерированный им случайный элемент R_2 группы Г и уже вычисленный элемент $K = Q^{w_2} \circ Y_1^{x_2} \circ Q^{-w_2}$, находит значения $h_1' = F_h(R_2), h_2' = F_h(K), h_3' = F_h(KR_2)$ и элемент $Z^* = K^{h_1'} \circ R_2^{h_2'} \circ K^{h_3'}$. Затем он сравнивает элементы Z'' и Z^*. Если выполняется равенство $Z'' = Z^*$, то он делает вывод о подлинности второго пользователя.

Из протокола видно, что секретные значения не отправляются по открытому каналу связи, т.е. он относится к типу протоколов строгой аутентификации. При этом аутентификация выполняется по открытым ключам, поэтому не требуется предварительное использование защищенных каналов для обмена секретными значениями.

В заключении сформулированы результаты выполненного диссертационного исследования:

1. Разработан метод повышения уровня информационной безопасности и протокол утверждаемой групповой подписи, отличающийся использованием вычислений в конечном поле $GF(p)$, где число $p-1$ является трудно факторизуемым, что обеспечивает безопасность протокола при появлении прорывного решения одной из следующих двух трудных вычислительных задач: дискретного логарифмирования по простому модулю и факторизации. На основе метода разработан

2. Разработан метод повышения уровня информационной безопасности и протокол слепой подписи, отличающийся использованием вычислений в конечном поле $GF(p)$, где число $p-1$ является трудно факторизуемым

3. Разработан метод реализации и протокол утверждаемой групповой подписи, основанный на вычислительной сложности задачи нахождения дискретного логарифма на эллиптической кривой и отличающийся вычислением открытого ключа в виде суммы точек эллиптической кривой и генерацией маскирующих коэффициентов в виде криптографической контрольной суммы зависящей от секретного ключа руководителя группы подписантов.

4. Разработан метод построения и протокол утверждаемой групповой подписи, отличающийся использованием процедур генерации и проверки подлинности ЭЦП, специфицируемых российским стандартом ГОСТ Р 34.10-2012.

5. Разработан метод реализации и протокол коллективной групповой подписи.

6. Разработан метод построения и протокол комбинированной коллективной подписи.

7. Разработан метод устранения необходимости использования внутренней инфраструктуры открытых ключей для обеспечения возможности раскрытия групповой подписи руководителем, отличающийся тем, что параметры, маскирующие открытые ключи подписантов, вычисляются с использованием двухкратного вычисления хэш-функции, зависящей от секретного ключа руководителя группы подписантов.

8. Разработан метод построения безопасных защитных преобразований информации с использованием алгебраических операций, отличающихся комбинированием операций из конечных алгебраических структур различного типа и разбиением входного блока данных на подблоки различного размера.

9. Разработан метод псевдовероятностных защитных преобразований, стойкий к атакам с принуждением отправителя и получателя сообщений к раскрытию ключа шифрования, отличающийся реализацией вычислений в конечных полях, заданных в явной векторной форме, благодаря чему обеспечивается повышение производительности.

Перспективы развития выполненного исследования состоят в разработке протоколов групповой ЭЦП, коллективной ЭЦП для групповых подписантов, в которых подпись свободна от включения третьего дополнительного параметра U, что упростит строение этих протоколов, их реализацию и использование имеющейся на практике инфраструктуры открытых ключей при практическом применении протоколов данных типов. Дальнейшее развитие направления разработки способов алгебраических алгоритмов защитных преобразований можно связать с их построением на основе некоммутативных конечных ассоциативных алгебр размерности 3, что позволит повысить производительность алгоритмов защитного преобразования алгебраического типа.

Список работ, опубликованных автором по теме диссертации в журналах, входящих в перечень ВАК

1. Синев В.Е. Повышение уровня безопасности протокола групповой цифровой подписи, основанного на механизме маскирования открытых ключей // Известия СПбГЭТУ «ЛЭТИ». 2016. № 6. С. 21-25.
2. Молдовян А.А., Галанов А.И., Синев В.Е. Утверждаемая групповая подпись: новые протоколы // Вопросы защиты информации. 2016. № 2. С. 44-50.
3. Галанов А.И., Захаров Д.В., Молдовян Д.Н., Синев В.Е. Протоколы слепой подписи на основе двух вычислительно трудных задач // Вопросы защиты информации. 2009. № 4. С.2-7.
4. Доронин С.Е., Молдовян Н.А., Синев В.Е. Конечные расширенные поля для алгоритмов электронной цифровой подписи // Информационно-управляющие системы. 2009. № 1. С. 33-40.
5. Доронин С.Е., Молдовяну П.А., Синев В.Е. Векторные конечные поля: задание умножения векторов большой четной размерности // Вопросы защиты информации. 2008. № 4(83). С.2-7.

Другие публикации

6. Дернова Е.С., Костина А.А., Синев В.Е. Выбор характеристики и степени расширения конечных полей для схем цифровой подписи на основе конечных групп матриц // Материалы

VI Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2009)». Санкт-Петербург, 28-30 октября. СПб.: СПОИСУ, 2009. С.96

7. Дернова Е.С., Костина А.А., Молдовяну П.А., Синев В.Е. Примитивы алгоритмов цифровой подписи: конечные группы матриц над векторными полями // XIC-Петербургская международная конф. «Региональная информатика-2008 (РИ-2008)» СПб, 22-24 октября 2008 г. / Материалы конференции. СПб, 2008. с. 96-97.
8. Дернова Е.С., Костина А.А., Синев В.Е. Выбор параметров задания конечных групп матриц для построения алгоритмов электронной цифровой подписи // Научно-технические проблемы в промышленности. СПб, 12-14 ноября 2008 г. Материалы конференции. СПб, 2008. с. 40-41.
9. Костина А.А., Аль-Рахми Р.Я., Синев В.В. Подходы к разработке шифров на основе операций матричного умножения // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции. 25-26 ноября 2010, г. Санкт-Петербург. СПб.: ВАС, 2010. С. 57-62.
10. Борков П.В., Костина А.А., Аль-Рахми Р.Я., Синев В.В. Блочное шифрование с использованием некоммутативных операций // XII Санкт-Петербургская международная конференция Региональная информатика «РИ-2010» СПб, 20-22 октября 2010г. Материалы конференции. СПб, 20. сс. 94-95
11. Дернова Е.С., Костина А.А., Синев В.Е. Выбор параметров задания конечных групп матриц для построения алгоритмов электронной цифровой подписи // Труды конф. «Научно-технические проблемы в промышленности», Санкт-Петербург, 12-14 ноября 2008 г. СПб., 2008. С. 291-295.
12. Гурьянов Д. Ю., Мирин А.Ю., Синев В.Е. Метод решения задачи дискретного логарифмирования в конечных группах двухмерных векторов // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции. 10-11 декабря 2009 г., Санкт-Петербург. СПб.: ВАС, 2009. С. 228-233.
13. Дернова Е.С., Костина А.А., Синев В.Е. Выбор порождающего элемента в схемах цифровой подписи на основе конечных групп матриц и векторов // Материалы VI Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2009)». Санкт-Петербург, 28-30 октября. СПб.: СПОИСУ, 2009. С.96-97.
14. Галанов А.И., Березин А.Н., Синёв В.Е. Протокол утверждаемой групповой цифровой подписи на основе двух трудных задач // IX Санкт-Петербургская международная конференция Информационная безопасность регионов России «ИБРР-2015» СПб, 28-30 октября 2015г. Материалы конференции. СПб, 2015. сс. 101-102.

Подписано в печать "20" октября 2017 г.
Формат 60x84 1/16. Бумага офсетная. Печать офсетная.
Усл.печ.л. 1,0. Тираж 100 экз.
Заказ №