Уважаемый пользователь!
Обращаем ваше внимание, что система Антиплагиат отвечает на вопрос, является ли тот или иной фрагмент текста заимствованным или нет. Ответ на вопрос, является ли заимствованный фрагмент именно плагиатом, а не законной цитатой, система оставляет на ваше усмотрение. Также важно отметить, что система находит источник заимствования, но не определяет, является ли он первоисточником.

Уважаемый пользователь!
Появление этого сообщения говорит о том, что нужно внимательнее отнестись к оценке данного документа. Документ содержит признаки, типичные для искусственного завышения процента оригинальности за счет особенностей форматов документов. Что делать: в первую очередь сравнить текст, содержащийся в отчете и в документе, отправленном на проверку. Если, например, в отчете есть текст, не видимый в исходном документе, или слова «склеены» или в слова вставлены посторонние буквы, это означает, что систему и вас пытались обмануть. В то же время, появление данного знака НЕ ОБЯЗАТЕЛЬНО свидетельствует от том, что попытка обмана была. Возможно, текст содержит слишком много иностранных или очень длинных или не найденных в словаре слов. Это часто встречается в работах, где используется много терминов (химия, юриспруденция и т.п.). В заголовке отчета дана информация, по какому критерию показан знак. НЕЛЬЗЯ ОРИЕНТИРОВАТЬСЯ ТОЛЬКО НА ПРОЦЕНТЫ И ПОЯВЛЕНИЕ ДАННОГО ЗНАКА, необходимо открывать отчет и внимательно просматривать его!

Информация о документе:

Имя исходного файла: Диссертация_Синев_123.pdf
Имя компании: ТУСУР
Тип документа: Прочее
Имя документа: Диссертация_Синев_123.pdf
Дата проверки: 19.09.2017 11:17
Модули поиска: Диссертации и авторефераты РГБ, Интернет (Антиплагиат), Университетская библиотека онлайн, Модуль поиска ЭБС "Лань", Модуль поиска ЭБС "Айбукс", Модуль поиска ЭБС БиблиоРоссика

Текстовые статистики:
Индекс читаемости: сложный
Неизвестные слова: в пределах нормы
Макс. длина слова: в пределах нормы
Большие слова: выше нормы!

Источник	Ссылка на источник	Коллекция/ модуль поиска	Доля в отчёте	Доля в тексте
[1] Молдовян, Дмитрий Ни...	http://dlib.rsl.ru/rsl01005000000/rsl01005504000/rsl01005504...	Диссертации и авторефераты РГБ	3,19%	3,19%
[2] Дернова, Евгения Сер...	http://dlib.rsl.ru/rsl01004000000/rsl01004651000/rsl01004651...	Диссертации и авторефераты РГБ	1,38%	2,44%
[3] ko`chirish	http://library.tuit.uz/knigiPDF/107.pdf	Интернет (Антиплагиат)	0,93%	2,27%
[4] Гурьянов, Денис Юрье...	http://dlib.rsl.ru/rsl01004000000/rsl01004919000/rsl01004919...	Диссертации и авторефераты РГБ	0,47%	2,26%
[5] Доронин, Станислав Е...	http://dlib.rsl.ru/rsl01005000000/rsl01005378000/rsl01005378...	Диссертации и авторефераты РГБ	0,45%	2,25%
[6] Диссертация	http://www.spiiras.nw.ru/dissovet/wp-content/uploads/2016/10...	Интернет (Антиплагиат)	0,82%	2,23%
[7] Захаров, Дмитрий Вик...	http://dlib.rsl.ru/rsl01006000000/rsl01006624000/rsl01006624...	Диссертации и авторефераты РГБ	0,3%	2,12%
[8] Горячев, Александр А...	http://dlib.rsl.ru/rsl01006000000/rsl01006589000/rsl01006589...	Диссертации и авторефераты РГБ	0,33%	1,51%
[9] Рамзи Яхья Мохаммед ...	http://dlib.rsl.ru/rsl01006000000/rsl01006567000/rsl01006567...	Диссертации и авторефераты РГБ	0,71%	1,32%
[10] Нашуан Ахмед Касем А...	http://dlib.rsl.ru/rsl01004000000/rsl01004581000/rsl01004581...	Диссертации и авторефераты РГБ	0,07%	1,26%
[11] Куприянов, Иван Алек...	http://dlib.rsl.ru/rsl01006000000/rsl01006610000/rsl01006610...	Диссертации и авторефераты РГБ	0,28%	1,2%
[12] Латышев, Дмитрий Мих...	http://dlib.rsl.ru/rsl01006000000/rsl01006589000/rsl01006589...	Диссертации и авторефераты РГБ	0,13%	1,13%
[13] Труды (13/29)	http://www.spiiras.nw.ru/files/conferences/RI-2010/ri-2010-t...	Интернет (Антиплагиат)	0,23%	1,02%
[14] Механизмы аутентифик...	http://netess.ru/3informatika/536058-1-mehanizmi-autentifika...	Интернет (Антиплагиат)	0,04%	1%

[15] Download	http://i-us.ru/Files/Pdfs/2013_2.pdf	Интернет (Антиплагиат)	0,04%	0,73%
[16] Аникевич, Елена Алек...	http://dlib.rsl.ru/rsl01004000000/rsl01004658000/rsl01004658...	Диссертации и авторефераты РГБ	0,05%	0,72%
[17] Диссертация Биричевс...	http://www.spiiras.nw.ru/dissovet/wp-content/uploads/2015/12...	Интернет (Антиплагиат)	0,02%	0,66%
[18] Расширение функциона...	http://netess.ru/3informatika/387662-1-rasshirenie-funkciona...	Интернет (Антиплагиат)	0,05%	0,64%
[19] pdf	http://www.eltech.ru/assets/files/nauka/dissertacii/2012/Avt...	Интернет (Антиплагиат)	0,05%	0,61%
[20] Хо Нгок Зуй диссерта...	http://dlib.rsl.ru/rsl01005000000/rsl01005435000/rsl01005435...	Диссертации и авторефераты РГБ	0,05%	0,6%
[21] Скачать журнал	http://i-us.ru/Files/Pdfs/2011_2.pdf	Интернет (Антиплагиат)	0,12%	0,59%
[22] 2011(№3) (2/6)	http://www.eltech.ru/assets/files/university/izdatelstvo/izv...	Интернет (Антиплагиат)	0,08%	0,5%
[23] том1 (11/15)	http://www.eltech.ru/assets/files/university/irvc/inmio/tom1...	Интернет (Антиплагиат)	0,27%	0,5%
[24] ПРИМИТИВЫ КРИПТОСИСТ...	http://cyberleninka.ru/article/n/primitivy-kriptosistem-s-ot...	Интернет (Антиплагиат)	0%	0,48%
[25] 2011(№4) (3/8)	http://www.eltech.ru/assets/files/university/izdatelstvo/izv...	Интернет (Антиплагиат)	0,06%	0,44%
[26] Download	http://i-us.ru/Files/Pdfs/2009_1.pdf	Интернет (Антиплагиат)	0,01%	0,43%
[27] Лёвин, Валерий Юрьев...	http://dlib.rsl.ru/rsl01004000000/rsl01004956000/rsl01004956...	Диссертации и авторефераты РГБ	0,02%	0,42%
[28] Михайлов, Александр ...	http://dlib.rsl.ru/rsl01003000000/rsl01003298000/rsl01003298...	Диссертации и авторефераты РГБ	0,08%	0,41%
[29] Источник 29	http://www.znaj.ru/referats/39000/39627.zip	Интернет (Антиплагиат)	0,07%	0,39%
[30] Молдовян, Александр ...	http://dlib.rsl.ru/rsl01002000000/rsl01002802000/rsl01002802...	Диссертации и авторефераты РГБ	0,05%	0,36%
[31] 231673	http://biblioclub.ru/index.php?page=book_red&id=231673	Университетская библиотека онлайн	0,08%	0,35%
[32] 5300	http://e.lanbook.com/books/element.php?pl1_id=5300	Модуль поиска ЭБС "Лань"	0,02%	0,33%
[33] Криптографические и ...	http://ibooks.ru/reading.php?short=1&productid=334362	Модуль поиска ЭБС "Ай��укс"	0%	0,32%
[34] 40849	http://e.lanbook.com/books/element.php?pl1_id=40849	Модуль поиска ЭБС "Лань"	0,03%	0,29%
[35] 232067	http://biblioclub.ru/index.php?page=book_red&id=232067	Университетская библиотека онлайн	0%	0,25%
[36] 3027	http://e.lanbook.com/books/element.php?pl1_id=3027	Модуль поиска ЭБС "Лань"	0%	0,25%
[37] 233689	http://biblioclub.ru/index.php?page=book_red&id=233689	Университетская библиотека онлайн	0%	0,22%
[38] 238045	http://biblioclub.ru/index.php?page=book_red&id=238045	Университетская библиотека онлайн	0,03%	0,21%
[39] Ростовцев, Александр...	http://dlib.rsl.ru/rsl01002000000/rsl01002278000/rsl01002278...	Диссертации и авторефераты РГБ	0%	0,21%
[40] Информационная безоп...	http://ibooks.ru/reading.php?short=1&productid=344097	Модуль поиска ЭБС "Айбукс"	0,01%	0,21%
[41] 50578	http://e.lanbook.com/books/element.php?pl1_id=50578	Модуль поиска ЭБС "Лань"	0%	0,21%
[42] Пылин, Владислав Вла...	http://dlib.rsl.ru/rsl01004000000/rsl01004240000/rsl01004240...	Диссертации и авторефераты РГБ	0%	0,2%
[43] 68466	http://e.lanbook.com/books/element.php?pl1_id=68466	Модуль поиска ЭБС "Лань"	0%	0,19%
[44] Источник 44	http://www.rusdoc.ru/material/raznoe/open_key_crypt.zip	Интернет (Антиплагиат)	0%	0,17%
[45] Математические метод...	http://www.bibliorossica.com/book.html?&currBookId=6793	Модуль поиска ЭБС БиблиоРоссика	0%	0,17%
[46] ko`chirish	http://library.tuit.uz/knigiPDF/79.pdf	Интернет (Антиплагиат)	0%	0,17%
[47] БАНКОВСКИЕ ОПЕРАЦИИ ...	http://www.bibliorossica.com/book.html?&currBookId=6114	Модуль поиска ЭБС БиблиоРоссика	0%	0,17%
[48] Банковские операции ...	http://biblioclub.ru/index.php?page=book_red&id=90798	Университетская библиотека онлайн	0%	0,17%
[49] Банковские микропроц...	http://www.bibliorossica.com/book.html?&currBookId=14696	Модуль поиска ЭБС БиблиоРоссика	0%	0,16%
[50] 209462	http://biblioclub.ru/index.php?page=book_red&id=209462	Университетская библиотека онлайн	0%	0,16%

[51] Банковские микропроц...	http://ibooks.ru/reading.php?short=1&productid=339804	Модуль поиска ЭБС "Айбукс"	0%	0,16%
[52] Компьютерные сети. 5...	http://ibooks.ru/reading.php?short=1&productid=344101	Модуль поиска ЭБС "Айбукс"	0,02%	0,15%
[53] 231889	http://biblioclub.ru/index.php?page=book_red&id=231889	Университетская библиотека онлайн	0%	0,15%
[54] 3032	http://e.lanbook.com/books/element.php?pl1_id=3032	Модуль поиска ЭБС "Лань"	0%	0,15%
[55] 240570	http://biblioclub.ru/index.php?page=book_red&id=240570	Университетская библиотека онлайн	0%	0,14%
[56] Теоретико-числовые а...	http://biblioclub.ru/index.php?page=book_red&id=61814	Университетская библиотека онлайн	0%	0,14%
[57] Защита компьютерной ...	http://biblioclub.ru/index.php?page=book_red&id=86475	Университетская библиотека онлайн	0%	0,13%
[58] 1122	http://e.lanbook.com/books/element.php?pl1_id=1122	Модуль поиска ЭБС "Лань"	0%	0,13%
[59] 9303	http://e.lanbook.com/books/element.php?pl1_id=9303	Модуль поиска ЭБС "Лань"	0%	0,12%
[60] Информационная безоп...	http://ibooks.ru/reading.php?short=1&productid=351301	Модуль поиска ЭБС "Айбукс"	0%	0,12%
[61] Защита компьютерной ...	http://www.bibliorossica.com/book.html?&currBookId=5631	Модуль поиска ЭБС БиблиоРоссика	0%	0,11%
[62] Защита компьютерной ...	http://ibooks.ru/reading.php?short=1&productid=26730	Модуль поиска ЭБС "Айбукс"	0%	0,11%
[63] 5114	http://e.lanbook.com/books/element.php?pl1_id=5114	Модуль поиска ЭБС "Лань"	0%	0,11%
[64] Основы сетевой безоп...	http://www.bibliorossica.com/book.html?&currBookId=12070	Модуль поиска ЭБС БиблиоРоссика	0%	0,11%
[65] Алгоритмы шифрования...	http://ibooks.ru/reading.php?short=1&productid=333612	Модуль поиска ЭБС "Айбукс"	0%	0,11%
[66] 71813	http://e.lanbook.com/books/element.php?pl1_id=71813	Модуль поиска ЭБС "Лань"	0%	0,11%
[67] Механизмы аутентифик...	http://www.dslib.net/zaw-informacia/mehanizmy-autentifikacii...	Интернет (Антиплагиат)	0%	0,1%
[68] 59240	http://e.lanbook.com/books/element.php?pl1_id=59240	Модуль поиска ЭБС "Лань"	0%	0,1%
[69] 45571	http://e.lanbook.com/books/element.php?pl1_id=45571	Модуль поиска ЭБС "Лань"	0,01%	0,1%
[70] 270314	http://biblioclub.ru/index.php?page=book_red&id=270314	Университетская библиотека онлайн	0%	0,1%
[71] 275116	http://biblioclub.ru/index.php?page=book_red&id=275116	Университетская библиотека онлайн	0,01%	0,09%
[72] Параллельные алгорит...	http://ibooks.ru/reading.php?short=1&productid=344407	Модуль поиска ЭБС "Айбукс"	0%	0,09%
[73] 63228	http://e.lanbook.com/books/element.php?pl1_id=63228	Модуль поиска ЭБС "Лань"	0%	0,09%
[74] Искусство защиты и в...	http://ibooks.ru/reading.php?short=1&productid=335110	Модуль поиска ЭБС "Айбукс"	0%	0,09%
[75] 252979	http://biblioclub.ru/index.php?page=book_red&id=252979	Университетская библиотека онлайн	0%	0,09%
[76] Иванов, Михаил Алекс...	http://dlib.rsl.ru/rsl01002000000/rsl01002901000/rsl01002901...	Диссертации и авторефераты РГБ	0,02%	0,09%
[77] Инфокоммуникационные...	http://www.bibliorossica.com/book.html?&currBookId=15757	Модуль поиска ЭБС БиблиоРоссика	0%	0,08%
[78] Инфраструктуры откры...	http://www.bibliorossica.com/book.html?&currBookId=12117	Модуль поиска ЭБС БиблиоРоссика	0,02%	0,08%
[79] Информационная безоп...	http://www.bibliorossica.com/book.html?&currBookId=19051	Модуль поиска ЭБС БиблиоРоссика	0%	0,08%
[80] Криптографические ме...	http://ibooks.ru/reading.php?short=1&productid=334031	Модуль поиска ЭБС "Айбукс"	0%	0,07%
[81] Источник 81	http://window.edu.ru/resource/755/66755/files/%D0%9C%D0%B5%D...	Интернет (Антиплагиат)	0%	0,07%
[82] Источник 82	http://window.edu.ru/resource/146/25146/files/nwpi243.pdf	Интернет (Антиплагиат)	0%	0,07%
[83] 45471	http://e.lanbook.com/books/element.php?pl1_id=45471	Модуль поиска ЭБС "Лань"	0%	0,07%
[84] 275627	http://biblioclub.ru/index.php?page=book_red&id=275627	Университетская библиотека онлайн	0%	0,07%
[85] 5193	http://e.lanbook.com/books/element.php?pl1_id=5193	Модуль поиска ЭБС "Лань"	0%	0,07%
[86] Введение в распредел...	http://ibooks.ru/reading.php?short=1&productid=29352	Модуль поиска ЭБС "Айбукс"	0%	0,07%
[87] Нопин, Сергей Виктор...	http://dlib.rsl.ru/rsl01004000000/rsl01004072000/rsl01004072...	Диссертации и	0,04%	0,07%

			авторефераты РГБ		
☑	**[88]** Материалы Второй меж...	http://ibooks.ru/reading.php?short=1&productid=29317	Модуль поиска ЭБС "Айбукс"	0%	0,05%
☑	**[89]** Ходжаев, Александр Г...	http://dlib.rsl.ru/rsl01000000000/rsl01000322000/rsl01000322...	Диссертации и авторефераты РГБ	0%	0,05%
☑	**[90]** 13807	http://e.lanbook.com/books/element.php?pl1_id=13807	Модуль поиска ЭБС "Лань"	0%	0,04%
☑	**[91]** Алгебраические струк...	http://www.bibliorossica.com/book.html?&currBookId=19442	Модуль поиска ЭБС БиблиоРоссика	0%	0,04%
☑	**[92]** Современные тенденци...	http://ibooks.ru/reading.php?short=1&productid=351350	Модуль поиска ЭБС "Айбукс"	0%	0,04%
☑	**[93]** 227774	http://biblioclub.ru/index.php?page=book_red&id=227774	Университетская библиотека онлайн	0%	0,04%
☑	**[94]** Курс алгебры.	http://ibooks.ru/reading.php?short=1&productid=29375	Модуль поиска ЭБС "Айбукс"	0%	0,04%
☑	**[95]** 229582	http://biblioclub.ru/index.php?page=book_red&id=229582	Университетская библиотека онлайн	0%	0,03%
☑	**[96]** Теоретико-численные ...	http://ibooks.ru/reading.php?short=1&productid=343131	Модуль поиска ЭБС "Айбукс"	0%	0,03%
☑	**[97]** Информационная безоп...	http://ibooks.ru/reading.php?short=1&productid=28022	Модуль поиска ЭБС "Айбукс"	0%	0,03%
☑	**[98]** Введение в современн...	http://biblioclub.ru/index.php?page=book_red&id=62989	Университетская библиотека онлайн	0%	0,02%
☑	**[99]** Введение в теорию чи...	http://ibooks.ru/reading.php?short=1&productid=29351	Модуль поиска ЭБС "Айбукс"	0%	0,02%
☑	**[100]** 9368	http://e.lanbook.com/books/element.php?pl1_id=9368	Модуль поиска ЭБС "Лань"	0%	0,02%
☑	**[101]** Организация и технол...	http://ibooks.ru/reading.php?short=1&productid=352907	Модуль поиска ЭБС "Айбукс"	0%	0,02%

Оригинальные блоки: 89,36%

Заимствованные блоки: 10,64%

Заимствование из "белых" источников: 0%

Итоговая оценка оригинальности: **89,36%**

Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики
[8]

Экз. №
На правах рукописи
Синев Валерий Евгеньевич
Методы построения и разработка практичных протоколов
групповой подписи и алгебраических алгоритмов
защитных преобразований
05.13.19 –

методы и системы защиты информации, информационная
безопасность
Диссертация на соискание ученой степени
кандидата технических наук
Научный руководитель
доктор технических наук

профессор [1]Молдовян Н.А.

[2]Санкт-Петербург
2017
2
Оглавление

4
Введение
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 т��ебуемого 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.
5
Применение алгебраических алгоритмов защитных преобразований для обеспечения информационной безопасности информационнотелекоммуникационных 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

6
преобразований. Для достижения этой цели

были сформулированы и решены
следующие исследовательские задачи:
Разработка метода и [6]

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 рандомизируюих экспонент,
маскирующих открытые ключи подписантов, как значения однонаправленной
функции в зависимости от открытых ключей подписантов и секретного ключа
7
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 [1]

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
8
защитных преобразований при решении практических задач информационной
безопасности, а также в учебном процессе.
Методология и

методы исследования. В работе [14]использован аппарат и
методы математической статистики, теории вероятности, алгебры, теории чисел,
[1]

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 повышенние уровня безопасности протоколов данного типа.
2. Метод построения и протокол коллективной ЭЦП, обеспечивающий формирование единой цифровой подписи, разделяемой произвольным числом групповы�? 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 [1]

повышение
производительности алгоритма защитноего преобразования информации.
Степень достоверности и апробация результатов. Обоснованность научных положений, выводов и практических рекомендаций, полученных в диссертационной работе,

обеспечивается анализом состояния исследований в
9

[6]данной [14]области на сегодняшний день, [6]

формальными доказательствами,
вычислительным экспериментом и апробацией результатов на следующих конференциях:

VI Санкт-Петербургской межрегиональной конференции

«Информационная безопасность регионов России (ИБРР-2009)» ([1]СанктПетербург, 28 - 30 октября 2009), [13]XI Санкт-Петербургской международной

конференции «Региональная информатика-2008 (РИ-2008)» ([2]Санкт-Петербург, 22 - 24 октября 2008), Всеармейской научно-практической конференции

«Инновационная деятельность в Вооруженных силах Российской Федерации»

([1]Санкт-Петербург, 25 - 26 ноября 2010), [2]XII [8]Санкт-Петербургской международной

конференции «Региональная информатика (РИ-2010)» ([2]Санкт-Петербург, 20 - 22

октября 2010 г), IX Санкт-Петербургской межрегиональной конференции ([1]

СанктПетербург, 28 - 30 октября 2015 г).
Диссертация включает 5 глав.
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.
10
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 обеспечении 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 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. Описан предложенный способ псевдовероятностного защитного преобразования информации, отличающийся реализацией вычислений в конечных полях, заданных в явной векторной форме.
11
В пятой главе рассматриваются протоколы с открытым ключом, использующие матричное умножение. Показано, что задача поиска сопрягающего элемента в конечном некоммутативном кольце матриц, возникающая при осуществлении криптоанализа двухключевого криптоалгоритма Cayley-Purser, решается

за полиномиальное время путем сведения к решению системы линейных уравнений, [23]

которые легко записываются по значениям параметров открытого ключа данной криптосистемы. Этот результат дает обоснование заключения о том, что алгоритм открытого шифрования Cayley-Purser не удовлетворяет современным требованиям стойкости. При этом достигнуть приемлемого уровня его безопасности не представляется возможным даже при применении секретного и открытого ключа большой разрядности.
12
Глава 1. Примитивы современных алгоритмов защиты и аутентификации электронных документов и сообщений
В настоящее время вопросы обеспечения информационной безопасности современных информационно-вычислительных и телекоммуникационных систем имеют чрезвычайно важное значение для многих областей человеческой деятельности. Эти вопросы связаны как с защитой конфиденциальной информации, так и с реализацией современных систем электронного документооборота, требующего придания юридической значимости сообщениям и документам, представленным в электронной форме. Последнее обеспечивается с помощью электронной цифровой подписи (ЭЦП). Защита информации, передаваемой по открытым каналам связи, связана с применение криптографических преобразований, использующих секретные ключи [1-4]. Для решения задачи распределения секретных ключей практичным является применение протоколов открытого распределения ключей, основанных на двухключевых криптографических алгоритмах. Функционирование последних обеспечивается наличием пары ключей,

связанных между собой, а именно,

личного секретного ключа и открытого ключа. [1]

Процедуры генерации и проверки подписи в протоколах ЭЦП также основаны на двухключевых криптосистемах [57]. В настоящий момент практическое значение криптографии с открытым ключом возросло настолько, что во многих развитых странах внедрена инфраструктура открытых ключей, позволяющая решать задачу проверки подлинности (аутентификации) открытых ключей в достаточно широком масштабе. ⁂ технической точки зрения важным представляется обеспечение высокой стойкости алгоритмов шифрования данных, протоколов открытого распределения ключей и схем ЭЦП. Другим важным обстоятельством, имеющим массовый характер, является распространение мобильной связи, карманных персональных компьютеров и смартфонов. Вычислительные ресурсы таких устройств ограничены для выполнения криптографических преобразований. В последних областях применения необходимы прежде всего алгоритмы, которые
13
бы эффективно использовали память устройств, при этом были более быстрыми и экономичными в потреблении энергии [8-11]. Известно, что криптоалгоритмы открытым ключом работают медленнее по сравнению с симметричными криптоалгоритмами, поэтому при реализации первых в мобильных устройствах следует делать упор на повышении производительности.
Одна из широко применяемых ассиметричных криптосистем, а именно RSA [12,13], низкоэффективна для применения в устройствах с ограниченными вычислительными ресурсами из-за того, что требует оперирования с большими числами, а последнее часто трудно реализовать в виду ограниченности ресурсов. Другими недостатками RSA является довольно медленное выполнение вычислений, особенно при генерации ключей, и необходимость использования более длинных ключей, чем в других криптосистемах с открытым ключом. Это обусловило то, что в мобильных устройствах самая распространенная на данный момент остаются криптоалгоритмы и криптопротоколы, использующие вычисления на эллиптической кривой [14,15], требующие меньше ресурсов, чем RSA. Дальнейшее уменьшение сложности аппаратной реализации и повышение быстродействия криптосхем с открытым ключом все еще остаются направлениями исследований, имеющими важное практическое значение и привлекающими значительный интерес исследователей.
В связи с этим представляет интерес поиск новых примитивов для реализации криптосистемы, которые бы обеспечивали решение поставленной задачи. В качестве таких примитивов представляют интерес конечные

некоммутативные группы [16-22]. В таких группах для задания вычислительно трудной задачи дискретного логарифмирования могут выделяться коммутативные подгруппы. Ранее изучались и применялись для построения двухключевых алгоритмов только коммутативные конечные группы. Некоммутативные конечные группы также могут быть применены для синтеза двухключевых алгоритмов, поскольку подгруппы определенного порядка в них являются коммутативными. При этом в силу некоммутативности полной группы можно
14
ожидать, что для них разработка субэкспоненциальных методов дискретного логарифмирования менее вероятна, чем для коммутативных групп. В связи с этим представляет интерес исследовать условия образования некоммутативных групп, а также разработать двухключевые алгоритмы на их основе.
Кроме того, в настоящее время в криптографии сформировалось направление [23-28] поиска двухключевых криптосистем, обладающих экспоненциальной стойкостью к атакам, основанным на использовании квантовых вычислителей, которые позволят решить за полиномиальное время как задачу нахождения разложения целого числа, так и задачу нахождения дискретного логарифма в конечных циклических группах [29]. Указанные две задачи используются в большинстве применяемых на практике двухключевых криптосхемах, поэтому при предполагаемом появлении в будущем практически действующих квантовых компьютеров, которые смогут быть применены для атаки на криптосистемы, стойкость которых станет полиномиальной, что обусловит неприемлемость их практического применения. Это обусловливает интерес к новым типам

вычислительно трудных задач, пригодных для построения криптосистем с открытым ключом, в [16]

частности к трудным задачам
формулируемым над некоммутативными группами [30-33].
1.1. Двухключевые криптосистемы
В настоящее время большую роль для обеспечения информационной безопасности современных информационных технологий и телекоммуникационных систем играют криптосистемы с открытым ключом. Эти криптосистемы предоставляют методы и алгоритмы решения задач открытого распределения секретных ключей между удаленными пользователями и аутентификации информации, представленной в электронной форме. Как и в любой криптосистеме в основе функционирования криптосистем с открытым ключом лежит использование некоторой секретной информации – секретного ключа. Однако в отличие от классических криптосистем, в которых секретный ключ должен быть известным двум или более пользователям, в криптосистемах с
15
открытым ключом секретный ключ известен только одному пользователю, который выработал секретный ключ. С этим секретным ключом связан открытый ключ, значение которого зависит от секретного ключа, причем по известному открытому ключу и алгоритму генерации соответствующих друг другу открытого и секретного ключа вычислительно невозможно за обозримое время вычислить секретный ключ. Пользователь, который выработал для себя пару

секретного и открытого ключей считается владельцем открытого ключа. [10]

Открытый ключ
предоставляется для использования всеми пользователями криптосистемы и фактически является общеизвестным. Возможность решения задач распределения общих секретных ключей удаленными пользователями, аутентификации информации и зашифрования информации обеспечивается корректностью генерации открытого и закрытого ключей и специальными двухключевыми алгоритмами.

Благодаря тому, что личный секретный ключ известен только [78]

пользователю, который является владельцем открытого ключа, имеется возможность построения эффективных схем цифровой подписи, являющихся алгоритмической основой систем придания юридической силы электронным документам.
Криптографические алгоритмы, в которых используются два ключа одновременно – открытый и закрытый (секретный) называют алгоритмами с открытым ключом или двухключевыми криптоалгоритмами. Подход, где один из ключей известен всем пользователям и потенциальному злоумышленнику, т.е. сама идея использования в криптографическом преобразовании открытого ключа представляется фундаментальной, в связи с чем двухключевые криптосистемы часто называют открытыми шифрами, а производимые защитные преобразования по открытому ключу – открытым шифрованием. Выделяют следующие основные направления применения криптографических преобразований с открытым ключом:
выработка общего секрета или обмен ключами;
16
Выработка и проверка электронной цифровой подписи
(аутентификация информации, представленной в цифровом формате);

аутентификация пользователей;
построение систем «электронной наличности»;
построение систем тайного электронного голосования;
защита материальных объектов от подделки и др.
Протоколы электронной цифровой подписи (ЭЦП) способны служить гарантией, что то

или иное сообщение было составлено конкретным абонентом (пользователем) криптосистемы. [1]

Строгая доказательность этого факта

основана
на том, что двухключевые криптосистемы работают при условиях, когда пользователь [10]

не передает свой секретный ключ второй стороне. При выработке подписи к электронному документу использование секретного ключа контролируется с помощью открытого ключа. Но для формирования правильной цифровой подписи открытого ключа недостаточно. При этом владельцу ключа нужно понимать, что сохранение в тайне секретного ключа и соблюдения правил его использования являются его личной зоной ответственности. Секретный ключ дает возможность вычислить сообщение со специфической внутренней структурой, которая связана с открытым ключом и подписываемым документом. Это сообщение и называется ЭЦП. С помощью открытого ключа проверяется, что ЭЦП имеет структуру, которая была сформирована с использованием секретного ключа. Вероятность принятия сообщения от нарушителя, за сообщения от пользователя системы ЭЦП, исключительно низка и составляет менее 10
- 20
.
Таким образом, процедура проверки ЭЦП с использованием открытого ключа даёт высокую степень гарантии, что принятое сообщение было составлено владельцем секретного ключа. Такие свойства двухключевых криптографических систем лежат в основе правовых актов, придающих юридическую силу ЭЦП. При вводе в действие таких правовых актов обеспечивается возможность придания юридической силы электронным документам с помощью протоколов ЭЦП.
17
Поскольку только владелец личного секретного ключа может вычислить цифровую подпись к некоторому сообщению, такую, что она легко может быть проверена любым заинтересованным лицом по открытому ключу владельца, то не возникает трудности в проверке подлинности цифровой подписи. Это дает принципиальную возможность предотвратить отказ от авторства электронного сообщения или документа, т.е.

отрицать [8]свою связь с посланным сообщением.
[2] Например, предотвращение [8]отказа от авторства является [2]

одним из важнейших
требований в технологиях электронной коммерции. Открытый общедоступный ключ вычисляется в зависимости от личного секретного так, что вычисление личного секретного ключа по открытому ключу владельца оказывается вычислительно сложной (практически невыполнимой) задачей.
В основе

криптосистем с открытом ключом лежат различные вычислительно сложные задачи. [7]

Криптосистемы такого типа по определению не
могут являться безусловно стойкими в понимании смысла данного термина в рамках модели нарушителя, обладающего бесконечными вычислительными ресурсами. Применение криптосистем с открытым ключом основано на том, что они облают практической стойкостью, т.е. их взлом с использованием любой известной атаки является вычислительно невыполнимым за обозримое время. Чтобы обеспечить выполнимость требования практической стойкости, параметры вычислительно трудной задачи, лежащей в основе работы двухключевого криптоалгоритма, выбираются достаточно большого размера. При этом с ростом размера (битовой длины, разрядности) используемых параметров снижается производительность (вычислительная эффективность) двухключевых криптосхем. Это обусловливает предпочтительность использования криптоалгоритмов, основанных на задачах, которые обеспечивают достаточно высокий уровень стойкости (криптостойкости) при достаточно низкой вычислительной сложности процедур, выполняемых при осуществления криптографических преобразований. Предпочтительным для построения криптосхем с открытым ключом является выбор вычислительно сложных задачи, для которых зависимость вычислительной сложности криптографических преобразований полиномиально зависит от
18
размера параметров задачи, а сложность решения базовой вычислительной задачи зависит экспоненциально или, по крайней мере, сверхполиномиально (под сверхполиномиальной зависимостью понимается то, что при выборе достаточного размера параметров базовой задачи ее вычислительная сложность растет более быстро по сравнению с любым заранее заданным полиномом).

Наиболее широкое применение для разработки криптографических алгоритмов и протоколов получили следующие

вычислительно трудные задач:

задача факторизации больших целых чисел, [16]

включающих два
множителя, представляющих собой простые числа, удовлетворяющие требованиям «сильной простоты» [13,34];
задача дискретного логарифмирования в конечных ассоциативных алгебраических структурах (полях, циклических группах) [35,36];

задача дискретного логарифмирования на эллиптической кривой (т.е. в циклических группах точек эллиптической кривой) [37-40];

задача [31]извлечения квадратного корня по трудно разложимому модулю [41,42];
[2]

задача извлечения корней большой простой степени в

циклических
группах, порядок которых делится на квадрат степени корня [43-46].

1.2. [4]

Схемы открытого согласования ключей
Под схемой открытого распределения ключей понимают криптографический протокол, в рамках которого используется двухключевой криптоалгоритм и который решает задачу формирования общего секретного ключа для двух или более удаленных пользователей при обмене некоторыми несекретными сообщениями по открытому каналу. Применяются два типа таких схем – протоколы открытого согласования ключей и протоколы открытого распределения ключей, хотя два последних названия часто используются как синонимы. Однако при более строгом использовании данных терминов
19
учитывается то, что эти варианты отличаются тем, как именно формируется и распределяется общий секретный ключ. В схеме открытого согласования ключа ни один из пользователей не знает заранее какое конкретное значение секретного будет сформировано в результате выполнения протокола. Значение секретного ключа зависит от выбора некоторых случайных значений каждой из сторон протокола, причем все стороны, участвующие в протоколе, используя получаемые сообщения вырабатывают одно и то же секретное значение, которое принимается в качестве общего секретного ключа. Нарушитель, перехватывающий все передаваемые данные не может вычислить секретное значение.
В схеме открытого распределения ключей один из пользователей генерирует секретный ключ и, используя открытые ключи других пользователей, участвующих в протоколе, зашифровывает секретный ключ и рассылает полученные криптограммы другим пользователям. Рассмотрим конкретные реализации таких протоколов.
Система открытого согласования ключей Диффи-Хеллмана. Становление и бурное развитие двухключевой криптографии началось с появления статьи Диффи и Хеллмана [36], в которой была предложена криптосхема, основанная на новом подходе к решению задачи распределения секретных ключей. В основу предложенной ими криптосхемы была положена хорошо известная вычислительно трудная задача дискретного логарифмирования в мультипликативной группы конечного простого поля. В предложенной схеме личным секретным ключом, который не подлежит рассылке, является случайное число x достаточно большого размера, а открытый ключ формируется y, путем выполнения операции возведения в степень, равную большому натуральному числу x, по модулю большого простого числа
y =
x
mod p,
где x целое число, такое, что 1< x < p–1, p – простое к-битовое число, примитивный элемент по модулю p [47,48]. Оказалось, что используя данную
20
формулу, имеется

возможность построения практически стойких криптографических систем, в которых не требуется передача секретного ключа.
[8]

Обеспечение удаленных пользователей одинаковым секретным ключом реализуется с применением только открытых несекретных сообщений. Механизм согласования общего секретного ключа двух удаленных абонентов телекоммуникационной системы с открытыми каналами связи реализуется следующим образом. Каждый пользователь генерирует свой личный секретный ключ в виде случайного натурального числа x и по последнему вычисляет свой открытый ключ y, соответствующий выбранному секретному ключу, используя указанную выше формулу. Пользователи A и B формируют общий секретный ключ без передачи каких-либо секретных значений следующим путем. Пользователь A берет из справочника открытых ключей (доступного на

сайте удостоверяющего центра) открытый ключ yB
пользователя B и, используя

свой личный секретный ключ xA

, вычисляет общий секретный ключ:
[18]

ZAB
= (yB
)
x
A
= (
x
B
)
x
A
=
x
B
x
A
mod p.
Аналогичные действия выполняет и пользователь B:
ZAB
= (yA
)
x
B
= (
x
A
)
x
B
=
x
B
x
A
mod p.
В результате этих шагов оба пользователя сформировали одинаковый секретный
ключ ZAB
без использования какого-либо заранее установленного

общего

секретного ключа. Используя сформированный общий секретный ключ в [1]

качестве
ключа шифрования и некоторую одноключевую криптосистему, пользователи
могут зашифровывать направляемые друг другу сообщения, т.е. установить
секретную связь по открытым каналам. Данная процедура согласования общего
секретного ключа имеет достаточно высокую вычислительную эффективность
для достаточно больших длин чисел p, , y и x (например, разрядность этих чисел
может быть тысячи и десятки тысяч бит).
21
Для оценки стойкости данной криптосхемы следует рассмотреть возможные
действия нарушителя. Ему известны значения yB =
x
B
mod p и yA =
x
A
mod p, но
для вычисления значения ZAB
, он должен решить задачу дискретного
логарифмирования и определить либо x
A
, либо x
B
. Это означает. Что нарушитель
должен выполнить операцию, обратную операции возведения в степень, т.е. ему
надо решить задачу дискретного логарифмирования по достаточно большому
простому модулю. Известно, что для достаточно больших простых чисел p, таких,
что в разложении на множители числа p−1 содержится простой делитель q
достаточно большой разрядности, задача дискретного логарифмирования
является вычислительно сложной (практически неосуществимой). На данном
уровне развития вычислительной техники

задача дискретного логарифмирования вычислительно невыполнима за обозримое время [7] при длине числа p более 1536 бит и длине числа q более 240 бит. При данных размерах чисел p и q операция возведение в большую целочисленную степень по модулю p [1] выполняется очень быстро при использовании алгоритма быстрого возведения в степень [41,49], что делает схему открытого согласования ключей Диффи-Хеллмана весьма практичной, поскольку она обладает достаточно высоким быстродействием и высокой криптостойкостью.

Авторы данной схемы ввели понятие справочника открытых ключей и указали на то, что не следует упускать из виду проблему аутентификации открытых ключей. Стойкость схемы открытого согласования ключа может быть обеспечена только в случае, если все открытые ключи в справочнике открытых ключей являются подлинными. Участники протокола должны выполнить процедуру проверки подлинности открытых ключей друг друга. Решение задачи аутентификации открытых ключей решается организационно-техническими мерами.

Обобщенная схема открытого распределения ключей. Об открытом распределении ключей [9] говорят, когда секретный ключ генерируется у одного из

пользователей и потом зашифровывается по открытому ключу получателя и направляется получателю по открытому каналу. Получатель, используя свой личный секретный ключ, расшифровывает полученный шифртекст и тем самым извлекает из шифртекста секретный ключ. В криптосхемах такого типа используется некоторый алгоритм открытого шифрования, название которого связано с тем, что зашифрование сообщений выполняется по открытому ключу получателя сообщения, а расшифрование – по личному секретному ключу получателя. В этом случае имеется возможность направлять секретные сообщения всем пользователям, подлинные открытые ключи которых известны отправителю. Для расшифрования полученных текстов требуются секретные ключи, соответствующие открытым ключам, использованным при зашифровании сообщения. Пусть известен алгоритм открытого шифрования E, такой, что процедуры шифрования по открытому и по соответствующему секретному ключу являются взаимно обратными. Пусть также известен открытый ключ e некоторого пользователя, причем подлинность ключа e подтверждена некоторой выполненной процедурой аутентификации ключа e (например он извлечен из цифрового сертификата, подписанного удостоверяющим центром). Тогда некоторое секретное сообщение Z может быть передано по открытым каналам в виде криптограммы C = Ee
(Z) владельцу открытого ключа e. Значение извлекается
Z, выполняя шифрование по личному секретному ключу d, т.е. осуществляя обратное преобразование:
Ed
(C) = Ee
1
(C) = Ee
1
(Ee
(Z)) = Z.

Поскольку значение d известно только получателю, то только он может извлечь из криптограммы значение Z. В качестве Z может быть направлен получателю некоторый секретный ключ. Получив некоторый секретный ключ, получатель должен убедиться, что он был не был направлен ему от нарушителя, который также может воспользоваться общедоступным открытым ключом e. Для того, чтобы процедура аутентификации значения Z могла быть выполнена следует усилить рассматриваемую криптосхему. Это делается путем добавления шага

шифрования по личному секретному ключу отправителя. В результате этого протокол открытого распределения ключей между пользователями A, B и C приобретает следующий вид.

1. Один из пользователей, например, пользователь A, генерирует секретный ключ Z.
2. Используя открытые ключи пользователей B и C, пользователь A вычисляет криптограммы
A C
C
( )
d e
C E E Z и
A B

B
( )
d e
C E E Z .
3. Пользователь A отправляет криптограмму CB
пользователю B, а
криптограмму CC
пользователю C.
4. Получив криптограмму CB
, пользователь B вычисляет значение
B A
B
( )
d e
E E C Z .
5. Получив криптограмму CC
, пользователь C вычисляет значение
C A
C
( )
d e
E E C Z .
Результатом выполнения этого протокола является появление общего секретного ключа, сгенерированного пользователем A, у пользователей B и C. Причем они уверенны в следующих фактах:
значение Z неизвестно никому другому, кроме пользователя A, если оно было направлено пользователем A;
если значение Z действительно позволяет восстанавливать получаемые сообщения, то ключ Z, был действительно направлен пользователем A.
Некоторым недостатком последней версии протокола открытого распределения ключей является «отложенность» факта подтверждения подлинности отправителя. В следующей версии протокола устраняется этот недостаток.
24
Обобщенный протокол открытого
распределения ключей
1. Один из пользователей, например, пользователь A, генерирует секретный ключ Z.
2. Используя открытые ключи пользователей B и C, пользователь A
вычисляет криптограммы
A C
C A
( ),
d e
C E E Z e и
A B
B A
( ),
d e
C E E Z e .
3. Пользователь A отправляет криптограмму CB
пользователю B, а
криптограмму CC
пользователю C.
4. Получив криптограмму CB
, пользователь B вычисляет значение
A B
B A
( ) ,
e e
E C E Z e ,
убеждается, что правая часть сообщения промежуточного сообщения
B
A
,
e
E Z e представляет собой открытый ключ отправителя (или некоторый другой специфицированный идентификатор), т.е. убеждается в подлинности отправителя, а затем вычисляет секретный ключ Z:
B B
B
( )
d e
E E C Z .
5. Получив криптограмму CC
, пользователь C вычисляет значение
A C
C A
( ) ,
e e

E C E Z e ,
убеждается, что правая часть сообщения
C
A
,
e
E Z e представляет собой
открытый ключ пользователя A (или некоторый другой специфицированный идентификатор), т.е. убеждается в подлинности пользователя A, а затем вычисляет секретный ключ Z:
25
B B
B
( )
d e
E E C Z .
Далее будет рассмотрена криптосистема RSA [12], которая предоставляет конкретную функцию E, которая может быть положена в основу конкретной реализации данного обобщенного протокола распределения секретных ключей по открытым каналам связи.
Двухключевые шифры по сравнению с одноключевыми криптосистемами дают скорость шифрования на несколько порядков ниже. Поэтому наибольшей эффективностью обладают гибридные криптосистемы, которые комбинируют симметричные и асимметричные криптосхемы следующим образом: информационные сообщения шифруются с помощью симметричных (одноключевых) криптоалгоритмов, а распределение ключей симметричного шифрования выполняются по открытому каналу, используя двухключевые криптосхемы . В частности, при использование криптосистемы RSA [12,13], можно выполнить обмен сеансовым ключом с другим пользователем,

зашифровав

сеансовый ключ с помощью его открытого ключа. [3]

При этом безопасно передать
зашифрованный сеансовый ключ по открытому каналу связи, так как секретным ключ необходимым для расшифровки есть только у пользователя, открытый ключ которого использовался для зашифровки. Двухключевые шифры для непосредственного засекречивания информации находят узкое применение.
1.3. Протоколы электронной цифровой подписи
Криптосистема RSA. Данная криптосистема впервые была обнародована в работе [12]. Эта криптосистема является первой широко известной и практически используемой системой цифровой подписи и открытого шифрования. В основе ее работы лежит теорема Эйлера [47], которая утверждает, что для любых двух взаимно простых натуральных чисел n и M < n справедливо соотношение
M
(n)
= 1 mod n,
26
где (n) – функция Эйлера, значение которой определяется как количество чисел, взаимно простых с n и не превосходящих n. Модуль n выбирается таким образом, чтобы его факторизация была вычислительно невыполнимой операцией. Делители n составляют часть личного секретного ключа пользователя, а его открытым ключом значение n и некоторое другое число e, взаимно простое с (n).Значение n генерируется по формуле n = pq, где оба множителя являются сильными простыми числами. Требование сильной простоты делителей p и q [50] обеспечивает практическую невозможность факторизации числа n. Для генерации случайных сильных простых чисел большой разрядности (512, 1024, 2048 бит и более) известны вычислительно эффективные алгоритмы, поэтому пользователи без труда могут сгенерировать значение n, факторизовать которое будет практически невозможно, даже при использовании вычислительных ресурсов всего человечества. Основной операцией преобразования в криптосистеме RSA является операция возведения в степень по модулю n.
Рассмотрим процедуру открытого шифрования. Пусть требуется зашифровать сообщение M (на шифруемые сообщения накладывается требование M < n). Эта процедура выполняется по открытому ключу в виде пары чисел (n, e) по следующей формуле
C = Ee
(M) = M
e
mod n.
Расшифрование криптограммы C состоит в извлечении корня e-ой степени по модулю n. Это выполняется как операция возведения в степень d (ключ расшифрования), равную e
1
mod (n):
Ed
(C) = C
d
mod n = (M
e

mod n)
d
mod n = M
ed
mod n = M.
Непосредственно из теоремы Эйлера следует, что

две процедуры возведения в

степень по модулю n будут [3]

представлять собой взаимно обратные
преобразования, если произведение степеней, используемых в этих процедурах, сравнимо с единицей по модулю, равному функции Эйлера от числа n:
ed 1 mod (n). Если выбрано некоторое значение e, то для расшифрования
27
криптограммы требуется вычислить параметр d = e
1
mod (n). Для вычисления
последнего значения требуется знать разложение числа n, поэтому по открытому ключу зашифрования e никто другой, кроме владельца открытого ключа (n, e), не имеет возможности вычислить секретную экспоненту d. Параметр d является элементом личного секретного ключа того пользователя, который сгенерировал открытый ключ (n, e). Для вычисления экспоненты d владелец открытого ключа поступает следующим образом. Сначала он вычисляет значение функции Эйлера от модуля n. Поскольку для простых значений p и q имеет место (p) = p – 1 и (q) = q – 1, а модуль равен n = pq, то, используя свойство мультипликативности функции Эйлера, владелец открытого ключа (n, e) легко вычисляет значение (n) = (pq) = (p)(q) = (p – 1)(q – 1), а затем для любого числа e определяет требуемую экспоненту расшифрования d = e
1
mod (n), которую сохраняет в
тайне (для последнего он использует расширенный алгоритм Евклида [51,52]).
Таким образом, в криптосистеме RSA предусматривается следующее.
Каждый пользователь выбирает два многоразрядных простых числа p и q, разность которых также является многоразрядным числом, и находит их произведение n = pq. После этого он вычисляет значение функции Эйлера (n) и генерирует случайное число e, такое, что НОД(e, (n)) = 1. Затем он вычисляет обратное (по модулю (n)) к e значение d = e
1
mod (n). После этого он может
уничтожить делители q и p, что будет способствовать сохранению их в тайне.
Секретным ключом является число d.

Пара чисел n и e является открытым

[3]ключом, [12]который предоставляется всем абонентам криптосистемы RSA.

В [3]

этой криптосхеме процедуры зашифрования и расшифрования являются симметричными, поэтому, если выполнить расшифрования некоторого сообщения, то это даст некоторое значение, из которого можно восстановить исходное сообщение по открытому ключу, что может сделать любой желающий, используя открытый ключ. С точки зрения обеспечения секретности пересылаемых сообщений возведение сообщения в секретную степень не имеет смысла (поскольку обратное преобразование выполняется по открытому ключу),
28
однако значение которое даст такое преобразование не может быть получено по открытому ключу. При этом по открытому ключу можно легко проверить, что некоторое значение было получено путем возведения некоторого сообщения в секретную степень d. Легко понять, что это свойство может быть использовано для аутентификации источника сообщения по открытому ключу. Другими словами, криптосхема RSA реализует не только возможность выполнения открытого шифрования, но и возможность вычисления некоторых чисел, которые фактически представляют собой цифровую подпись к сообщениям, представленным в цифровом виде. При этом подлинность подписи может быть проверена любым лицом, используя открытый ключ подписанта.
Процедура генерации ЭЦП. Пусть требуется сформировать ЭЦП к некоторому заданному сообщению M < n. Цифровая подпись может быть вычислена путем возведения числа M в степень d по модулю n в соответствии с формулой
S = M
d
mod n.
Значение S есть ЭЦП, которую для заданного сообщения M

может выработать

только владелец секретного ключа.

Процедура проверки [3]

подлинности ЭЦП. Подлинности цифровой подписи S
к сообщению M проверяется как возведение числа S в

степень открытого ключа e
по модулю n по формуле
M = S
e
mod n.
[1]

Если результат этой операции дает значение M равное заданному сообщению M, то ЭЦП S признается подлинной.
Криптостойкость схемы RSA основана на сложности факторизации модуля. Если эту задачу решить, то тогда можно вычислить функцию Эйлера от модуля и затем

определить секретный ключ по открытому. Однако до настоящего времени не [3]

предложены алгоритмы решения вычислительно сложной задачи
29
факторизации модуля рассматриваемого вида, имеющие полиномиальную сложность при использовании имеющихся вычислительных ресурсов, если размер модуля равен 1536 бит и более и если делители модуля p и q представляю собой сильные простые числа примерно одинаковой длины.
В системе RSA необходимо учитывать также возможность экзистенциальной подделки подписи [53,54], которая состоит в выборе произвольного значения в качестве цифровой подписи и формировании по этой подписи сообщения. На самом деле, взяв некоторое произвольное число S, можно легко вычислить значение M , удовлетворяющее условию M = S
e
, т. е.
произвольное значение можно попытаться выдать за цифровую подпись к некоторому случайному сообщению. Обычно случайные сообщения подписывать нет смысла в большинстве практических случаях использования протоколов ЭЦП. Однако, в ряде приложений иногда требуется подписывать случайные значения.
Для устранения возможности экзистенциальной подделки ЭЦП и обеспечения возможности вычисления подписи к сообщениям произвольного размера в практически применяемых вариантах криптосхемы RSA подпись формируется не непосредственно по значению сообщения, а по значению хэш-функции, которая вычисляется от сообщения по некоторому алгоритму хэширования, который специфицируется как элемент протокола ЭЦП.
В настоящее время наибольшее распространение получили криптосхемы, основанные на трудности задачи дискретного логарифмирования. Впервые эта задача была применена в схеме цифровой подписи Эль-Гамаля [55].
Схема ЭЦП Эль-Гамаля [55] включает следующую процедуру генерации ключей.
1. Выбрать случайное достаточно большое простое число p, такое, что задача дискретного логарифмирования в конечном простом поле GF(p) является практически нерешаемой.
30
2. Вычислить примитивный элемент α поля GF(p), т.е. число для которого имеет место α
(p 1)
≡ 1mod p, причем для всех нетривиальных делителей
r|
p 1 не выполняется неравенство α
(p 1)/r
mod p 1.
3. Сформировать случайное натуральное число x < p 1, x – личный секретный ключ.
4. Используя значение x, вычислить значение открытого ключа y по следующей формуле: y = α
x
mod p.
5. В качестве открытых параметров криптосхемы используются

числа
α и p. Секретный ключ x необходимо хранить в тайне.

Генерация подписи [8]

включает следующие шаги:
1. Сгенерировать случайное секретное число к, удовлетворяющее условию 0 < к < p – 1 и НОД(к, p –1) = 1 (к играет роль разового секретного ключа).
2. Вычислить параметр рандомизации цифровой подписи R = α
к
mod p (R
играет роль разового открытого ключа и не является секретным).
3. Вычислить значение S из следующего уравнения:
1 mod 1 mod
p
к

xR M
S p kS xR M
4. В качестве цифровой подписи к сообщению M берется пара
натуральных чисел (R, S).
Процедура проверки подлинности ЭЦП осуществляется в соответствии со
следующей процедурой:
. mod и если ,)) , (, (
) , , (
p R y p r True S R м Verify
M S R
p y
31
Корректность схемы ЭЦП Эль-Гамаля доказывается подстановкой
сгенерированной ЭЦП в проверочное уравнение процедуры верификации ЭЦП:
. mod) ( ) (p R y
M xR M xR
к
xR M
к R x S R M
Для того, чтобы обеспечить возможность вычисления второго элемента
подписи, а именно, значения S, необходимо обеспечить условие взаимной
простоты чисел к и p – 1 (данное требование вытекает из известной теоремы из
теории сравнений о существовании обратного элемента). В связи с этим при
генерации числа к требуется обеспечить выполнимость условия НОД(к, p –1) = 1.
Число к должно уничтожаться после формирования значения подписи, поскольку
по известному к и известной подписи не составляет труда вычислить секретный
ключ.
После опубликования статьи Эль-Гамаля, в которой был представлен
алгоритм

цифровой подписи, основанный на задаче дискретного

логарифмирования, [1]

было предложено множество вариаций реализации его идеи
использования рандомизирующего значения в процедуре генерации подписи.

Наиболее значительными из них является схема цифровой подписи Шнорра [56].
[8]

Также представляют интерес схемы ЭЦП на основе трудности дискретного
логарифмирования в конечных простых полях, в которых нет возможности
выделения одного из элементов подписи как параметра рандомизации,
предложенные в работах [57-59].
Схема ЭЦП Шнорра [56] имеет существенные особенности по сравнению с
алгоритмом цифровой подписи Эль-Гамаля. Важным достоинством схемы
Шнорра является достаточно малый размер подписи (320 бит при обеспечении 80битового уровня стойкости, т.е. трудоемкости взлома не
менее 2
80
операций
модульного умножения), что представляется важным для многих практических
применений. Для обеспечения 80-битовой стойкости ЭЦП в схеме Эль-Гамаля
требуется использовать 1024-битовый модуль, что дает размер ЭЦП, равный 2048
32
бит. Теоретически важной особенностью схемы Шнорра является то, что значение
хэш-функции вычисляется принудительно только после генерации параметра
рандомизации R. Благодаря этой особенности для схемы Шнорра может быть
формально доказано, что существование эффективных алгоритмов подделки
подписи означает существование эффективных алгоритмов решения задачи
дискретного логарифмирования [60], т.е. имеется возможность теоретического
доказательства ее стойкости в смысле доказательства того, что сложность взлома
не проще решения трудной задачи дискретного логарифмирования, положенной в
основу криптосхемы.
Более компактное представление значения ЭЦП достигается в схеме
Шнорра с помощью конструирования поля Fp
, содержащего намного подгруппу
заданного простого порядка q. В схеме ЭЦП Эль-Гамаля безопасной длиной
параметра p считается 1024 бит, что определяется возможностью решения задачи
дискретного логарифмирования методом вычисления индексов [49], имеющим
субэкспоненциальную сложность. Поскольку трудоёмкость этого метода
определяется размером характеристики поля и практически не зависит от размера
порядка основания логарифма, то имеется возможность уменьшения размера
порядка до |q| ≈ 160 бит. При росте размера |p| потребуется увеличит размер |q|,
чтобы обеспечить рост стойкости, однако при этом отношение размера |p| к
размеру |q| будет возрастать, т.е. схема Шнорра при усилении требований по
стойкости будет еще более предпочтительна. Рассмотрим схему ЭЦП Шнорра.
Схема ЭЦП Шнорра [61] включает следующую процедуру генерации
ключей.
1. Сгенерировать простые числа p, q, такие что q| p 1; |p| ≈ 1024 бит, |q| ≈
160 бит.
2. Сгенерировать элемент) (p GF порядка q, т.е. α
q

1 mod p.
3. Выбрать криптографически стойкую функцию хэширования Fh
.
33
4. Сгенерировать случайное число x (секретный ключ) такое, что для него
выполняется соотношение 1 < x < q.
5. Вычислить y = a
x
mod p.
Личным секретным ключом является x, а открытым ключом – значение y.
Системными параметрами схемы Шнорра являются значения p, q и a.
Генерация цифровой подписи к сообщению M
1. Вырабатывается случайное натуральное число к, удовлетворяющее
условию 1 < к < q.
2. Вычисляется значение параметра рандомизации R = a
к
mod p.
3. К подписываемому сообщению M присоединяется параметр
рандомизации и вычисляется значение хэш-функции Fh
от аргумента M||R:
E = H (M||R) – первый элемент ЭЦП.
4. Вычисляется значение S, которое представляет собой

второй элемент
ЭЦП:
S = к + xE mod q.

Процедура проверки подлинности [22]

подписи подписи включает следующие шаги:
1. Вычисляется значение R’: p y R
E S
mod '
2. К сообщению M присоединяется число R’ (т.е. получаем аргумент M||R’)
и вычисляется значение хэш-функции Fh
(M||R’): E’ = Fh
(M||R)
3. Проверяется равенство значений E’ и E. Если последние два значения
равны, то подпись признается подлинной.
Корректность работы схемы Шнорра показывается следующим образом.
Пусть к сообщению M приложена подпись (S, E), полученная по правильному
значению секретного ключа и в соответствии с процедурой генерации подписи,
специфицированной для схемы Шнора. Тогда имеем:
p R p y R
к xE xE к E S
mod mod '
.
34
Так как R’ = R E’, то E’ = E, т.е. процедура проверки ЭЦП подтвердит подлинность
подписи. Аналогично крипто схеме Эль-Гамаля, параметр к фактически
используется в качестве разового секретного ключа и поэтому должен
генерироваться как равновероятное случайное число, которое должно
уничтожаться непосредственно после вычисления значения ЭЦП.
Одним из ключевых моментов при реализации схем ЭЦП является
применение хэш-функций, которые служат для обеспечения контроля
целостности подписываемых сообщений и документов [62]. Наиболее полно
требованиям, предъявляемым к криптографически стойким методам хэширования
информации, отвечают однонаправленные хэш-функции без секрета [52].
Различные виды хэш-функций описаны в международном стандарте ISO/IEC
10118, ряде национальных стандартов и криптографической литературе. Хэшфункция предназначена для сжатия подписываемого документа в
криптографически стойкую контрольную сумму размером от 160 бит до 512 бит,
причем для данного алгоритма вычисления значения хэш-функции размер ее
значения является фиксированным (чем больше размер значения хэш-функции
тем более высокая стойкость может быть достигнута).
В качестве аргумента хэш-функция Fh
(M) могут браться сообщения
произвольной длины M, а результатом вычисления хэш-значения является
битовая строка h фиксированной длины Fh
(M) = h. Значение хэш-функции Fh
(M)
зависит от каждого бита хэшируемого сообщения M и практически не позволяет
получить два или более сообщений с одинаковым значением хэш-функции.
Хэш-функция должна удовлетворять ряду условий [63]:
ее значение должно зависеть от каждого бита сообщения-аргумента M по
псевдослучайному закону, т.е. она должна изменяться при удалении,
исправлении, вставки и перестановки любых битов, слов, предложений и т.п.;
35
должна обладать свойством вычислительной необратимости, т.е. задача
вычисления документа M, который обладал бы заданным наперед случайным
значением хэш-функции, должна быть вычислительно невыполнимой;

должна удовлетворять требованию коллизионной стойкости, которое состоит в том, что вычислительно неосуществимо нахождение каких-либо двух сообщений, обладающих одинаковыми значениями хэш-функции; вероятность того, что значение хэш-функции двух различных документов совпадут, должна быть ничтожно мала.

1.4. Постквантовая криптография и трудные задачи над некоммутативными группами

В большинстве современных продуктов и стандартов криптографии применяются методы с открытым ключом, основанные на проблеме факторизации больших чисел (RSA) [13] и дискретного логарифмирования (стандарты DSA [64], ECDSA [65], ГОСТ Р 34.10-94 [66] и ГОСТ Р 34.10-2001 [67]). Подход [68,69,115] к синтезу двухключевых криптосистем на основе эллиптических кривых (используется трудность

задачи дискретного

логарифмирования на эллиптической кривой (ЭК), т.е. в [2]

конечной группе точек

ЭК) обеспечивает эквивалентную защиту при меньшем числе разрядов открытого ключа и других параметров криптосхемы по сравнению с ранее разработанными протоколами. Сложность атаки, как правило, связывают с зависимостью количества операций, необходимых для решения трудной задачи, положенной в основу криптосхемы. По виду функции, описывающей нарастание сложности решения трудных задач, различают полиномиальную, субэкспоненциальную и экспоненциальную сложность. Под видом функции здесь понимается формула, описывающая зависимость роста вычислительной сложности трудной задачи от размера задачи [70] (размера параметров, входящих в формулировку вычислительной задачи).

36

Стойкость криптосхем на основе специально выбранных ЭК экспоненциально связана с длиной ключа. Стойкость же RSA, основанной на сложности факторизации – субэкспоненциальная. Это позволяет использовать открытые ключи и другие открытые параметры криптосхем на основе ЭК значительно меньшей длины, чем для криптосхемы RSA. Размер параметров, равный 160 бит в первом случае, обеспечивает примерно такой же уровень безопасности, как RSA с параметрами размером 1024 бит. Кроме того, увеличение длины ключа для схем на основе ЭК в два раза приводит к значительно большему увеличению криптостойкости, чем увеличение в два раза длины параметров RSA, поэтому в будущем преимущества алгоритмов и протоколов эллиптической криптографии еще более только возрастут. Также увеличение длины ключа и уменьшение разрядности процессора приводит к увеличению преимущества по производительности криптосхем на основе ЭК. При этом аналогичная сравнительная картина имеет место при сопоставлении криптосхем, заданных над конечными полями (схема Эль-Гамаля [55], схема Шнорра [56]), по сравнению со схемами эллиптической криптографии. Однако, если давать сравнение стойкости различных схем к атакам, основанным на предполагаемой возможности использований квантового компьютера, то все перечисленные в данном параграфе криптосхемы окажутся нестойкими, т.е. непригодными для практического использования ни при каких размерах параметров, так как квантовый компьютер решает задачу факторизации и задачу дискретного логарифмирования в циклической подгруппы любого типа за полиномиальное время при использовании алгоритма Шора [29].

Последнее обстоятельство, а также ожидание, что в ближайшем будущем появятся реально действующие квантовые вычислители, а значит и возможность их применения для выполнения криптоанализа двухключевых криптосистем, обусловило большой интерес к другим типам задач, на основе которых могут быть разработаны протоколы ЭЦП [17,24,28], открытого распределения ключей [24], алгоритмы открытого и коммутативного шифрования [25,26,28], которые

37

основаны на вычислительно трудных задачах, имеющих экспоненциальную сложность при выполнении вычислений на квантовом компьютере.

Большое внимание разработчиков привлекают трудные задачи, формулируемые над некоммутативными группами. Заслуживают внимание вычислительная задача поиска сопрягающего элемента в некоммутативных группах кос (группах переплетения) [21-23], а также вычислительно трудная задача дискретного логарифмирования в маскируемой циклической подгруппе, которая представляет собой

комбинирование [11]задачи дискретного

логарифмирования и задачи поиска сопрягающего элемента и задается над

конечными некоммутативными группами [1]

матриц и векторов [26,28].

Задача поиска сопрягающего элемента состоит в следующем. Пусть известно значение Y = X

G

X

1

, где X – неизвестный элемент некоммутативной группы и

G – элемент заданный элемент, принадлежащий , Причем X принадлежит

некоторой заданной подгруппе группы , а элемент G имеет достаточно большой порядок. Задача состоит в том, чтобы найти значение X, который называется элементом, сопрягающим элементы Y и G. Трудность задачи поиска сопрягающего элемента используется в ряде протоколов открытого распределения ключей [17], ряде алгоритмов открытого шифрования [22], а также в схемах ЭЦП различного типа [30].

При этом ожидается, что использование трудности задачи поиска сопрягающего элемента в [1] группах кос позволит построить криптосхемы, обладающих высокой (сверхполиномиальной) стойкостью к атакам с использованием вычислений на квантовом компьютере [25].

Вопрос появления реально действующего многокубитового квантового компьютера в обозримом будущем является дискуссионным и в настоящее время с целью построения протоколов цифровой подписи для их построения используется подход, состоящий в комбинировании в единой криптосхеме двух вычислительно сложных задач, а именно, задачи факторизации и задачи дискретного логарифмирования. При этом протокол ЭЦП строится таким

образом, что для его взлома требуется одновременно решить обе эти задачи. В связи с этим вероятность взлома протокола за счет появления в ближайшем будущем прорывного непредвиденного алгоритма решения вычислительно трудной задачи, положенной в основу протокола, существенно снижается.

Для реализации данного подхода повышения уровня безопасности, обеспечиваемого протоколом ЭЦП предложен метод, использующий трудность разложения составного модуля специального вида [71,72], а также метод использующий вычислительную трудность нахождения дискретного логарифма по трудно разложимому модулю [73-76].

1.5. Протоколы коллективной и групповой цифровой подписи

На практике потребность в протоколах коллективной ЭЦП имеет место при разработке документации для крупных проектов, требующими привлечения достаточно большого числа специалистов различного профиля. Каждый из них готовит, например, отдельный раздел документации. При этом отдельные разделы проектной документации или вся их совокупность должны быть подписаны всеми разработчиками. Для сокращения размера совокупной цифровой подписи и снижения вычислительной сложности проверки подлинности ЭЦП могут быть применены протоколы коллективной ЭЦП, предложенные и разработанные в работах [77-79]. Построение протоколов коллективной подписи оказалось весьма удачным, что позволило по аналогии с построением протоколов слепой индивидуальной подписи разработать протоколы слепой коллективной ЭЦП [8082].

В отличии от мультиподписей других типов протоколы коллективной ЭЦП ориентированы на использовании имеющейся на практике инфраструктуры открытых ключей, причем оказалось возможным реализация таких протоколов на основе процедур генерации и проверки ЭЦП, которые специфицируются стандартами ЭЦП России, Беларуси и Украины [83-86]. Также перечисленные стандарты ЭЦП могут быть использованы для построения протоколов слепой и

слепой коллективной ЭЦП, т.е. функциональность данных стандартов может быть существенно расширена. Последнее потенциально обеспечивает более широкое применение этих стандартов и имеющейся инфраструктуры открытых ключей в практически используемых информационных технологиях.

Коллективная подпись обладает важным для практики свойством внутренней целостности, которое состоит в том, что по коллективной подписи вычислительно невозможно вычислить подпись, относящуюся к другой совокупности подписантов. Целостность означает, что подпись едина и неделима: либо все подписанты подписали электронный документ, либо никто из них не подписывал этот документ. Размер такой подписи равен размеру одной обычной (индивидуальной) ЭЦП. Рассмотрим, как функционирует обобщённый протокол коллективной ЭЦП (КЭЦП). В

нём вводится понятие коллективного открытого ключа некоторого [2] произвольного задаваемого множества подписантов, например, включающего м субъектов. Коллективный открытый ключ Y представляет собой значение, вычисляемое по всем открытым ключам $y_1, y_2, \ldots y_м$ заданного множества: $Y = f(y_1, y_2, \ldots, y_м)$. Обобщенная

схема формирования КЭЦП
представлена на рис. 1.1.
Рис. 1.1 [14]

Схема формирования коллективной подписи по протоколам [78,79]
При формировании КЭЦП каждый i-й подписант генерирует свой разовый
личный секретный ключ к
i
, и вычисляет по последнему свой разовый открытый
40
ключ r
i
(фактически параметр r
i
представляет собой значение, через которое i-й
подписант участвует в рандомизизации подписи). Все разовые открытые ключи r
i
рассылаются каждому участнику протокола, после чего по ним вычисляется
разовый коллективный открытый ключ R по формуле R = f(r
1
, r
2
,…, rm
), который
по своей сути является интегральным параметром рандомизации, маскирующим
все

личные секретные ключи подписантов. При формировании коллективной
подписи к [1]

электронному документу M произвольного размера используется
типовой приём представления документа M значением хэш-функции H = FH
(M),
где FH
– некоторая специфицированная функция хэширования. Значение R может
быть взято в качестве первого элемента КЭЦП. Вторым элементом КЭЦП
является число S, представляющее собой сумму долей S
i
, i = 1, 2,…, м,
вычисляемых каждым подписантом индивидуально. Число S
i
зависит от значения
параметра R, значения хэш-функции H, значения личного секретного ключа
подписанта x
i
и его разового секретного ключа к
i
. Если кто-либо из подписантов,
участвовавших в формировании параметра рандомизации R, не предоставит
правильно вычисленную долю подписи S
i
, то нахождение правильного значения
второго элемента КЭЦП вычислительно нереализуемо. Допустим все доли S
i
вычислены правильно. Они рассылаются всем подписантам и любой из них может
вычислить по всем долям их интегральное значение S, представляющее собой
второй элемент КЭЦП. Полученное корректным способом значение КЭЦП в виде
пары чисел (R, S) может быть использовано для доказательства того, что каждый
из заданного множества подписантов действительно подписал электронный
документ M.
Обобщенная схема процесса проверки подлинности КЭЦП представлена
на рис. 1.2. Для проверки подлинности КЭЦП (R, S) к электронному документу M
проверяющий считывает из справочника открытых ключей открытые ключи y
i
подписантов (или из цифровых сертификатов подписантов). Коллективный
открытый ключ Y для указанного множества подписантов вычисляется по
формуле Y = f(y
1
, y
2
,…, ум
). Затем коллективный открытый ключ Y и коллективная
41
подпись (R, S) подставляются в обычное проверочное уравнение, которое в
частном случае м = 1 полностью совпадает с проверочным уравнением в
протоколе индивидуальной ЭЦП.
Рис. 1.2 Схема проверки подлинности коллективной ЭЦП по протоколам
[78,79]
Важными преимуществами такого общего построения протоколов
коллективной цифровой подписи является сравнительно малая длина подписи и

использование имеющейся на практике инфраструктуры открытых ключей.
Другим интересным для практических приложений протоколов мультиподписи является групповая ЭЦП [87], который реализует возможность формирования ЭЦП от имени некоторого органа – группы подписантов, причем в группе подписантов выделяется лидер (руководитель). Предполагается, что протокол групповой подписи предоставляет следующие возможности: 1) подписать документ имеет возможность любой подписант или несколько подписантов из рассматриваемой группы; 2) руководитель и только он по значению ЭЦП и подписанному документу может идентифицировать подписантов, сформировавших данную подпись. Предложены различные варианты протоколов групповой ЭЦП [87], различающиеся дополнительными требованиями, использованными как критерии их разработки. Определенный интерес представляют протоколы пороговой групповой ЭЦП, спецификой которых является то, что для выработки групповой ЭЦП требуется участие не
42
менее чем t подписантов, т.е. никакое их подмножество из t – 1 субъектов вычислить правильное значение групповой подписи к какому-либо электронному документу не смогут. Существенными недостатками многих известных протоколов пороговой групповой ЭЦП являются следующие: 1) требуется участие в протоколе некоторой доверенной стороны, которой подписанты передают свои личные секретные ключи; 2) для практической реализации протоколов требуется создание специфической инфраструктуры ключей.
В работе [88] предложен протокол утверждаемой групповой ЭЦП, который удовлетворяют следующим требованиям:
1) неразглашение личных секретных ключей подписывающих;
2) формирование групповой ЭЦП осуществляется путем вычисления предварительной цифровой подписи, после чего лидер по предварительной подписи вычисляет значение групповой ЭЦП (последнюю процедуру можно назвать утверждением подписанного документа);
3) предварительная подпись потенциально может быть создана каждым из подписывающих и произвольным их подмножеством;
4) руководитель и только он имеет возможность раскрыть групповую подпись к заданному документу без использования какой-либо дополнительной информации, т.е. используя значение подписи и сам электронный документ, к которому относится ЭЦП.
В работе [88] данный набор требований к протоколу групповой ЭЦП обосновывается тем, свойства протокола обеспечивают близкую аналогию с процедурой подписывания и утверждения бумажных документов, которая реализуется на практике. Такая аналогия обусловливает практическую востребованность проколов утверждаемой групповой подписи, однако конкретный протокол такого типа, предложенный в работе [88] и использующий вычислительную трудность задачи дискретного логарифмирования в простом поле ставил открытыми следующие задачи:
43
1) реализация протокола утверждаемой групповой подписи с использованием вычислений на эллиптических кривых;
2) реализация протокола утверждаемой групповой подписи с использованием процедур формирования и проверки подлинности, регламентируемых российским стандартом ЭЦП ГОСТ Р 34.10-2012;
3) устранение использования внутренней инфраструктуры открытых ключей;
4) утверждение электронного документа двумя и более групповыми подписантами (например, документации к проекту, разработанного несколькими организациями) с помощью единой цифровой подписью при использовании имеющейся на практике инфраструктурой открытых ключей;
5) утверждение электронного документа единой подписью, подтверждающей, что документ подписан некоторой совокупностью групповых подписантов и некоторой группой индивидуальных подписантов.
Решение четвертой задачи означает разработку протоколов коллективной ЭЦП для групповых подписантов, что является построением нового типа протоколов мультиподписи, а решение пятой задачи – разработку протоколов комбинированной коллективной ЭЦП, что также относится к разработке протоколов мультиподписи нового типа.
Выводы к главе 1. Постановка задачи исследования
В современных технологиях электронного документооборота применение протоколов электронной цифровой подписи (ЭЦП) обеспечивает неотрекаемость от электронных сообщений и электронных документов. Применение таких протоколов лежит в основе придания юридической силы электронным документам и сообщениям. Огромное практическое значение протоколов ЭЦП обусловило принятие закона об электронной подписи и стандартов ЭЦП ГОСТ Р 34.10-1994, ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, а также создание развитой
44
инфраструктуры открытых ключей, функционирующей в России. Все упомянутые стандарты специфицируют протоколы цифровой подписи формируемой индивидуальным подписантом, однако практика выдвигает новые задачи, для решения которых требуется формирование цифровых подписей некоторой совокупностью индивидуальных подписантов (коллективная ЭЦП) или некоторым коллегиальным органом (групповая ЭЦП). Также востребована поддержка сценариев формирования единой ЭЦП со стороны нескольких

групповых подписантов (коллективная ЭЦП для групповых подписантов). Также востребовано обеспечение возможности формирования единой цифровой подписи со стороны нескольких индивидуальных и нескольких групповых подписантов (комбинированная коллективная ЭЦП). Протоколы такого типа относятся к так называемым протоколам мультиподписи. В настоящее время предложены и исследованы протоколы групповой и коллективной ЭЦП, однако открытым остался вопрос разработки протоколов коллективной ЭЦП для групповых подписантов и комбинированной коллективной ЭЦП. При этом известные протоколы групповой подписи не удовлетворяют основополагающему принципу известности секретного ключа единственному субъекту и не позволяют использовать имеющуюся на практике инфраструктуру открытых ключей в неизменном виде.

Важным практическим вопросом информационной безопасности является обеспечение конфиденциальности информации, передаваемой по открытым каналам, реализуемое с помощью защитных преобразований информации. При этом в ряде практических случаях требуется разработка программных и программно-аппаратных модулей, реализующих такие преобразования на основе типовых алгебраических операций, что обеспечивает снижение затрат на реализацию таких модулей и упрощает их интеграцию в существующие информационно-телекоммуникационные технологии.

Учитывая перечисленные моменты в данной диссертационной работе были поставлены следующие задачи:

45

1. Разработать метод повышения уровня информационной безопасности протоколов утверждаемой групповой подписи, предложенной впервые в работе [88].
2. Разработать метод повышения уровня информационной безопасности протокола слепой подписи
3. Разработать метод реализации протоколов утверждаемой групповой подписи с использованием вычислительной трудности задачи дискретного логарифмирования на эллиптической кривой.
4. Разработать метод построения протоколов утверждаемой групповой подписи с использованием процедур генерации и проверки подлинности ЭЦП, специфицируемых российским стандартом ГОСТ Р 34.10-2012.
5. Разработать метод реализации протоколов коллективной групповой подписи.
6. Разработать метод построения протоколов комбинированной коллективной подписи.
7. Разработать метод устранения необходимости использования внутренней инфраструктуры открытых ключей для обеспечения возможности раскрытия групповой подписи руководителем.
8. Разработать метод построения безопасных защитных преобразований информации с использованием алгебраических операций.
9. Разработать метод псевдовероятностных защитных преобразований, стойкий к атакам с принуждением отправителя и получателя сообщений к раскрытию ключа шифрования.

46

Глава 2. Построение протоколов слепой и групповой подписи, обладающих повышенным уровнем безопасности

Распространены протоколы слепой подписи, основанные на вычислительной трудности задачи разложения на множители составных чисел вида n = qr, где q и r – два сильных простых числа [5,13,42] и на задаче дискретного логарифмирования в конечной циклической группе большого простого порядка [5,36,55]. Для усложнения задачи взлома протоколов слепой подписи, имеет смысл разработать такого протокола слепой подписи, чтобы при попытке взлома пришлось одновременно решать две различные трудные вычислительные задачи.

В настоящей главе протоколы слепой подписи строятся по аналогии с протоколами обычной ЭЦП, основанными на двух различных трудных вычислительных задачах [89].

2.1. Метод построения и протокол слепой подписи, базирующийся на вычислительной сложности одновременного решения задачи разложения целого числа на множители и дискретного логарифмирования

Обеспечение повышенного уровня безопасности протоколов слепой подписи может быть достигнуто за счет того, чтобы задать необходимость

одновременного решения задачи дискретного логарифмирования в простом поле и задачи факторизации [3]

при попытках взлома протокола. Для этой цели протокол слепой ЭЦП можно построить на основе конструктивной схемы ЭЦП, сочетающей механизмы, используемые в схеме ЭЦП Шнорра [56] и в схеме ЭЦП, предложенной в работе [90]. Метод построения такого протокола связан с использованием в качестве модуля простого числа p, имеющего структуру вида p = 2n + 1,

где n = qr, q и r – большие простые числа размером не менее 512 бит [1]

являющиеся элементами личного секретного ключа подписанта. При этом число p
47
задается в качестве одного из элементов открытого ключа подписанта и в качестве второго элемента открытого ключа задается значения параметра , имеющего секретное значение порядка (по модулю p), благодаря чему подпись требуемой длины может быть сгенерирована только владельцем открытого ключа, причем в ходе формирования ЭЦП предполагается использование ослепляющих параметров для обеспечения анонимности пользователя, предоставляющего документ для подписывания. В основу протокола цифровой подписи [90] положено следующее проверочное уравнение
r = F(
HSr
mod p),
где три числовых значения (p, ,) представляют собой открытый ключ, а два числа (r, S) – это цифровая подпись, при этом разрядность числа S удовлетворяет условию |S| ; параметр H – это значение хэш-функции, вычисляемое от документа M; F – это некоторая специфицированная однонаправленная сжимающая функция (например, в качестве F можно использовать хэш-функцию
FH
, используемую для нахождения хэш-значения H =FH
(M) от подписываемого
сообщения); – это число, порядок которого по модулю p равен простому числу q, где q – личный секретный ключ. Параметр представляет собой битовую разрядность числа q, а q - простой делитель числа n. При таком соглашении уравнение генерации параметра S принимает следующий вид
S = к(Hr)
1
mod q.
В последнем выражении предполагается, что число r предварительно вычисляется по формуле r = F(
к
mod p) по значению к которое является разовым
секретным ключом. При выборе 1024-битового простого значения p и сжимающей функции F, значение разрядности которой равно 160 битам, битовая разрядность цифровой подписи примерно равна |F| + |q| 160 + 512 672 бит.
Проверка выполнимости условия |S| является одним из достаточно важных шагов верификации подлинности ЭЦП. Это связано с тем, что цифровая подпись с параметрами (r, S) при разрядности |S | 1024 бит (при |p| 1024 бит) может
48
быть достаточно просто вычислена по открытому ключу, т.е.

без знания

секретного числа q. Несмотря на то, что [7]

подпись (r, S) и будет удовлетворять
проверочному соотношению, добиться выполнения условия |S | настолько вычислительно сложно, насколько вычислительно сложна задача разложения на множители модуля n.
Алгоритм ЭЦП, предложенный в работе [90], может быть использован в качестве прототипа схемы ЭЦП, для взлома которой необходимо решения двух трудных задач – факторизации числа n и дискретного логарифмирования в простом поле характеристики p. Отметим, что в последнем случае мы делаем отличие между задачами дискретного логарифмирования в конечном поле, решаемой методом вычисления индексов, который имеет субэкспоненциальную сложность [5] и задачей дискретного логарифмирования в подгруппе этого поля, решаемой общими методами дискретного логарифмирования, которые имеют экспоненциальную сложность. Разберём следующую схему ЭЦП с открытым ключом, представленную в виде чисел (p, , ,y). Первые три числа задаются по аналогичной схеме ЭЦП [90], а параметр y вычисляется по формуле y =
x
mod p,
где x – еще один элемент секретного ключа. Разработанный протокол ЭЦП создан по принципу алгоритма ЭЦП Шнорра, где подпись к сообщению M формируется по следующей процедуре:
1. Сгенерировать R =
к
mod p, где к - случайно генерируемое значение,
при условии к <q.
2. Вычислить E = FH
(M||R).
3. Вычислить S = к + xE mod q, обеспечивающее выполнение условия
R =
S
y
E
mod p. Пара параметров (R, S) принимают в качестве значения ЭЦП.
Проверка подлинности подписи (R, S):
1. Если |S| > , то подпись отклоняется как неверная. В
противоположном случае вычисляется R
*

=
S
y
E
mod p.
49
2. Вычисляется значение м-функции от сообщения M, к которому
присоединили значение E
*
= FH
(M||R
*
).
3. Если значения E
*
и E равны, то подпись считается подлинной.
На основе алгоритма представленного выше генерация ЭЦП использует
случайные ослепляющие параметры и , и выполняется следующим образом.
1. Подписант генерирует значение R =
к
mod p, , где к - случайно
генерируемое значение, при условии к <q.
2. Пользователь A генерирует случайные значения и , разрядность
которых бит. Потом он вычисляет значения R = R
y
mod p, E = H
(M
||R
) и
E = E
, после чего передает подписывающему вычисленное значение E.
3. Подписант вычисляет значение S = к + xE mod q, обеспечивающее
условия R =
S
y
E
mod p. Пользователю A пересылает S (в данном случае
параметрам слепой подписи являются (R, S)).
4. Пользователь A вычисляет значение S = S + . И в итоге получает
подлинную подпись подписанта к сообщению M, представленную парой чисел
(R, S).
Сгенерированная подпись (R , S) должна успешно пройти проверку на
достоверность, тем самым будет доказана корректность описанного протокола
слепой подписи.
Для этого из R =
S
y
E
mod p => R
y
=
S +
y
(E+)
mod p и
R =
S
y
E
mod p. При этот вопрос об авторстве отпадает, так как любую тройку
чисел (R, S, E), сформированную подписывающим, можно сопоставить с
подписью (E, S
) для данного документа M. В итоге:
R =
S
y
E
mod p и R =
S
y
E
mod p} {R/R
SS
y
E+E
y
mod p,
отсюда при условии случайном равновероятном выборе «ослепляющих»
слагаемых и , считается, что подпись (E, S

) была создана одной из троек,
50
которые были сформированы подписывающим при вычислении параметров слепой подписи.
Стоит отметить, что на первом шаге функции проверки подлинности подписи, одним из важных условий является требование к размеру подписи, которое состоит в том, что размер подлинной подписи не превышает размер секретного ключа |q| = . Важность этого требования связана с тем, что после потенциально возможного появления прорывного решение вычислительно трудной задачи нахождения дискретного логарифма по модулю p у потенциального нарушителя появится возможность вычислить значение подписи, для которой выполняется условие |S| |n| и которая удовлетворяет проверочному соотношению. Для этого параметр S вычисляется нарушителем по формуле S = к xE mod n. При условии, что для решения задачи дискретного логарифмирования в конечном поле найден прорывной полиномиальный алгоритм и вычисление секретного значения x становится осуществимым практически, формирование элемента подписи S длины |S| всё ещё является вычислительно трудной задачей, поскольку для выполнения последнего неравенства необходимо решить задачу факторизации целого числа n.
При взломе описанной схемы подписи требуется решить две задачи одновременно: факторизации, позволяющую найти значение q, необходимое для вычисления значения параметра S, размер которого не превысит число = |q|, и дискретного логарифмирования, позволяющего найти закрытый (секретный) ключ x. Следует отметить, что одновременное решение двух выше обозначенных сложных задач не является обязательным условием для осуществления взлома. Секретные параметры системы можно получить, решив одну только задачу дискретного логарифмирования. Для этого можно воспользоваться следующим алгоритмом:
1. Произвольно выбирается число t, при условии, что его битовая длина не превышает 1.
51
2. Вычисляется значение Z =
t
mod p.
3. Методом вычисления индексов находится = log
. Это значение T,
вычисленное по модулю n = p 1. Размер этого значения с вероятностью почти равной единицы: |T| |n| > |t|. Так как

по модулю p число имеет порядок q

получаем T = t mod q, поэтому число q делит нацело [25]

на разность T t. Отсюда
возможно вычислить параметр q для этого достаточно выполнить факторизацию числа T t. При этом достаточно высока вероятность, что задача разложения числа T t будет иметь достаточно низкую вычислительную сложность. Поэтому если выполнить несколько раз данную процедуру можно найти легко значение T t, которое может быть сравнительно легко разложено на простые множители. Поэтому требуется модифицированная схема ЭЦП, для взлома которой требуется решение двух трудных задач одновременно. Рассмотрим следующую модифицированную схему для осуществления взлома которой нужно решение двух сложных задач – факторизации числа n и логарифмирования в конечном поле характеристики p. Для этого при создания схемы ЭЦП выбирается параметр с порядком n, а в уравнение проверки значения S вводится S
2
. Теперь подпись к
сообщению M формируется по следующему алгоритму.
1. Сгенерировать R =
к
mod p, где к - случайно генерируемое значение,
при условии к <q.
2. Вычислить E = FH
(M||R).
3. Вычислить S
2
= к xE mod n, при условии R =
S
2
y
E
mod p. Значение
(R, S) принимается в качестве ЭЦП.
Проверка подлинности подписи (R, S):
1. Если |S| > , то подпись отклоняется как неверная. В
противоположном случае вычисляется R
*
=
S
y
E

mod p.
2. Вычисляется значение хэш-функции от сообщения M, к которому присоединили значение E
*
= FH
(M||R
*
).
52
3. Если значения E
*
и E равны, то подпись считается подлинной.
Для взлома модифицированной схемы нельзя обойтись только решением задачи нахождения дискретного логарифма по простому модулю. Для подделки подписи после модифицирования криптосхемы потребуется знание разложения числа n. Решение задачи дискретного логарифмирования в итоге дает возможность вычисления

секретного ключа x и возможности вычислить значение к [3]xE [25]mod n. Однако для вычисления элемента подписи S необходимо также извлечь квадратный корень из последнего значения, [3]

что не менее сложно, чем разложение модуля n на простые множители.
Представленный алгоритм ЭЦП использует две вычислительно трудные задачи. Его можно использовать в качестве основы для алгоритма построения слепой подписи, по подобной схеме, основанной на алгоритме ЭЦН Шнорра, представленного в работе [7]. Попытка найти лазейку для взлома системы слепой подписи, когда одновременно требуется решение двух сложных задач, пока не имела успеха, так как пользователь, готовящий документ для получения к нему подписи вслепую, может факторизовать число n за счет того, что извлечение квадратного корня по модулю n дает четыре различных значений. Поэтому было принято решение в проверочном уравнении выполнять возведение параметра ЭЦП S в степень e, значение которого является взаимно простым со значением функции Эйлера по модулю.
Последний механизм был использован для разработки протокола слепой подписи с использованием схемы слепой подписи, описанной в работе [208] и включающей следующие шаги (рис. 2.1):
1. У подписывающего имеется открытый ключ y =
к
mod p. Он генерирует случайное значение к < q, вычисляет число =
к
mod p и передает его пользователю A. Пользователь A обладает некоторым электронным сообщением M и намерен получить для него слепую ЭЦП подписывающего, из которого пользователь A будет иметь возможность самостоятельно найти
53
значение подписи, которое удовлетворяет проверочному уравнению, используемому в стандарте ГОСТ Р 34.1094 (данная схема слепой подписи предложена в [208] как вариант потенциального расширения функциональности указанного стандарта).
2. Пользователь A вырабатывает случайные равновероятные числа , {1, 2, …, q 1}, вычисляет значения = y

mod p, R = mod q и
R = R/H + mod q, где H хэш-значение от подписываемого документа, [21]

вычисляемое в соответствии со стандартом ГОСТ Р 34.11–94. Значение R неизвестно подписанту и представляет собой первый элемент подлинной ЭЦП, а R – первый параметр слепой подписи.
3. Пользователь A направляет число R подписанту. По значению R нельзя вычислить R, ввиду случайного выбора неизвестных для подписанта значений параметров и , которые связывают значение R с числом R.
4. Подписант вычисляет второй параметр слепой подписи S = к + zR mod q (z – его секретный ключ) и передаёт его пользователю A.
5. Пользователь A вычисляет второй элемент подлинной цифровой подписи S = H(S +) mod q.
54
Рис. 2.1 Протокол слепой ЭЦП
Этот протокол использует в качестве проверочного соотношения уравнение проверки ЭЦП, специфицируемое стандартом ЭЦП ГОСТ Р 34.1094:
R = (
S/H
y
R/H
mod p) mod q (1).
Полученная в соответствии с описанным протоколом генерации подписи

(R, S) вслепую последняя является подлинной, если она удовлетворяет уравнению проверки подлинности ЭЦП, указанному в п. 1. Для того, чтобы взлом схемы ЭЦП с таким уравнением потребовал

одновременного решения двух разных
Подписывающий
Пользователь А
Генерирует случайное
число: <
=
[25]

Вычисляет число:
Генерирует случайные
равновероятные значение
, {1, 2, …, n 1}
Вычисляет:
= y
mod p
Первый элемент цифровой
подписи:
R= mod n
R = R/H + mod n
Вычисляет:
S = к + zR mod n
Генерирует случайное
значение: < n
Вычисляет значение
D =
e
H(S +) mod n
Вычисляет: D = D
d
mod n
D

Вычисляет второй элемент
подписи:
S =
1
D
e
= H[к + zR +]
d
mod n.
D
55

вычислительно сложных задач - нахождения дискретного логарифма **[1]**

по простому
модулю и разложения числа специального вида, в качестве модуля следует взять простое число, обладающее следующей

структурой p = 2n + 1, где n = qr, q и r –
сильные простые числа размером не менее 512 бит. **[1]**

При этом в качестве
проверочного уравнения выбирается следующее
R = (
S
e
/H
y
R/H
mod p) mod n , (2).
где значение e – число, взаимно простое с произведением (p 1)(q 1)=(n).
Значение e является элементом открытого ключа подписанта, которое выбирается им и по которому он вычисляет секретное значение d = e
1
mod (n). При этом
число имеет порядок по модулю p, равный n.
С учетом указанных модификаций протокол слепой подписи имеет
следующий вид (рис. 2.1):
1. Подписант генерирует равновероятное случайное число к < q, вычисляет значение =
к
mod p и направляет последнее пользователю А.
2. Пользователь А формирует случайные равновероятные значения маскирующих параметров , {1, 2, …, n 1}, вычисляет значения
= y

mod p, R= mod n и R = R/H + mod n, где H хэш-значение от подписываемого документа, вычисленное по [21]

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 A передает подписанту значение R.
4. Подписант

вычисляет значение S = к + [21]zR mod n, где z его секретный ключ, передает значение S (второй элемент слепой подписи) пользователю A.
56
5. Пользователь A генерирует случайное число < n и вычисляет значение
D =
e
H(S +) mod n, которое [3]

направляет подписанту.
6. Подписант вычисляет значение D = D
d
mod n, где d является образным
значением к e по модулю (n): d = e
1
mod (p 1)(q 1). Затем он направляет
значение D пользователю A.
7. Пользователь A вычисляет второй элемент подписи S =
Полученная в
соответствии с описанным
1
D
e
= H[к + zR +]
d
mod n.
Процедура проверки подлинности ЭЦП (R, S) к документу M выполняется следующим образом (Рис 2.2):
1. Вычисляется хэш-значение H от документа M и число
R* = (y
R/H
S
e
/H
mod p) mod n.
2. Если имеет место R* = (R, S), то подпись (R, S) принимается как подлинная.
Рис. 2.2 Процедура проверки подлинности ЭЦП (R, S) к документу M
Вычисляется значение хэшфункции H от документа M
Вычисляется:
R* = (y
R/H
S
e
/H
modля p) mod n
R* = (R, S)
Подпись (R, S) признается подлинной
Подпись (R, S) не признается подлинной
Да Нет
57
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, [21]

указанное в п. 1, как верная (подлинная) подпись. Корректность работы протокола слепой ЭЦП для взлома которой необходимы решения одновременно двух вычислительно сложных задач дискретного логарифмирования в простом поле и факторизации можно доказать.
На шаге 4 вычисляет второй элемент слепой подписи S = к + zR mod n. Из данной формулы с учетом, что порядок числа (по модулю p) равен n, следует справедливость сравнения
S
к
zR

mod p, из которого вытекает следующее
сравнение
к
S
zR
mod p. Поскольку R = H(R) mod q, то при
вычислении правой части проверочного соотношения (2) для значения подписи
(R, S) и значения хэш-функции H получаем следующее:
. * *
mod
*
) ( ) (
R R
p y
y y y y y
y y
R к R R z к R
H
R z к H
H
R H
H
S
H
R
e
d e
(3)
Последнее равенство означает, что подпись (R, S) к сообщению M успешно
проходит процедуру проверки ЭЦП, т.е. является корректной.
Данный протокол создаёт условия анонимности пользователя, который
предоставляет сообщения для получения подписи вслепую, т.е. точно определить
пользователя приславшего данное сообщения для формирования слепой ЭЦП
подписывающий не может (число подписанных сообщений с помощью протокола
слепой подписи данным подписывающим N > 1). При наличии у подписывающего
подлинной подписи (R, S) к сообщению M он не сможет идентифицировать
пользователя, приславшего ему

документ на подпись с вероятностью выше
58
значения d/N, где N – количество документов, подписанных (данным
подписывающим) с помощью протокола слепой подписи; d– число документов,
[3]

представлявшихся данным пользователем, так как любая подлинная подпись
(R, S) с равной вероятностью может быть отнесена к каждой из N вычисленных
значений слепой ЭЦП.
Подписывающему известны все тройки значения (, R, S), из ��ыполненных
им N процедур, когда он подписывал сообщение вслепую. Любые из строек
можно ассоциировать с произвольной подлинной (R, S), относящейся к
некоторому сообщению, которая представлена значением хэш-функции H. Так
как тройки подлинной ЭЦП (, R, S) и формируемая слепой подписи описанным
(R, S, H) связаны сгенерированными равновесными значениями и , в
соответствии с описанным ранее протоколом между подписывающим и
пользователем, предоставляющим сообщение для получение слепой подписи.
Поэтому тройка элементов подлинной ЭЦП (R, S, H) с

равной вероятностью
могла бы быть вычислена из любой тройки **[21]**

значений (, R, S), которые
формировались в ходе каждой из N процедур генерации слепой ЭЦП.
Если подписант фиксирует и хранит значение D, сформированное
пользователем A, то для идентификации пользователя A подписант не может
воспользоваться соотношением
n
S H
D
d
d
mod
) (
или, что тоже самое, соотношением
, mod
) (
n
S H
D e
поскольку любые наборы переменных, входящих в правую часть последних двух
формул, соответствуют некоторому случайному значению , которое неизвестно

подписанту.

59

2.2. Метод повышения уровня безопасности протокола групповой подписи, основанного на маскировании открытых ключей подписантов

Криптографические алгоритмы и протоколы с открытым ключом широко применяются в современных информационно-телекоммуникационных системах для защиты информации и формирования электронных цифровых подписей (ЭЦП) к электронным документам, что предопределяет пристальное внимание к безопасности их использования. Понятие безопасности криптографических протоколов предполагает выполнение двух требований: 1) взлом протокола с помощью лучшего известного алгоритма взлома является вычислительно невыполнимым (это определяет стойкость протокола) и 2) вероятность появления прорывного алгоритма взлома в обозримом будущем является достаточно малой (это определяет возможность безопасного использования протокола).

Таким образом, высокая стойкость является только одним из двух основных требований, предъявляемых к протоколам с открытым ключом. Значение стойкости количественно выражается вычислительной трудоемкостью W лучшего известного алгоритма взлома протокола и измеряется в количестве операции определенного типа.

Вторым важным условием является значение вероятности P появления прорывного алгоритма взлома. В работах [74,75] предложено внедрить в криптосхему в качестве элемента безопасности соотношение W/P.