Общество с ограниченной ответственностью
НАУЧНО-ПРОИЗВОДСТВЕННАЯ ФИРМА
"ПРИБОРЫ"
Адрес: 190103, г. Санкт-Петербург, Дерптский пер, д. 13, лит.А, пом. 1Н
Тел: (812) 370-5530, 575-1777; Факс: (812) 575-1999
http://www.pribory-spb.ru e-mail: info@pribory-spb.ru 3705530@mail.ru
ИНН 7839036441, КПП 783901001, ОКПО 01240597 р/с №40702810732030001722 в ФИЛИАЛ «САНКТ-ПЕТЕРБУРГСКИЙ» АО «АЛЬФА-БАНК», г. Санкт-Петербург, к/с №30101810600000000786, БИК 044030786

ОТЗЫВ

на автореферат диссертационной работы
Синева Валерия Евгеньевича
«Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований»
по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»
на соискание учёной степени кандидата технических наук

Широкое использование современных информационных технологий практически во всех отраслях человеческой деятельности – политической, экономической, финансовой и т.д. – делает проблему обеспечения информационной безопасности весьма острой. Одним из наиболее гибких и эффективных механизмов, используемых для решения комплексной проблемы обеспечения информационной безопасности информационных технологий является аутентификация электронных сообщений и электронных документов. В частности, в последнее время, требуется определение достоверности подписи не конкретного лица, а группы людей, работающих в одной организации, что приводит к созданию общей групповой электронной цифровой подписи (ЭЦП).

Важной научно-технической проблемой в области алгоритмов и протоколов аутентификации информации является разработка методов и протоколов групповой подписи и алгебраических алгоритмов защитных преобразований.

Новизной результатов, полученных автором в результате диссертационной работы над разработкой протоколов и методов групповой ЭЦП, является применение при построении ЭЦП вычислений по простому модулю, отличающееся выполнением вспомогательной операции возведения в целочисленную степень по трудно разложимому модулю и вычислением рандомизирующих экспонент, маскирующих открытые ключи подписантов.

Практическая ценность полученных результатов заключается в расширении функциональности протоколов групповой ЭЦП и повышением уровня обеспечиваемой ими безопасности.

Автореферат даёт хорошее представление о содержании выполненного исследования и полноте изложения основных результатов. Автор имеет 14 публикаций, 5 из которых в рецензируемых изданиях, входящих в перечень ВАК, что говорит о достаточной апробации диссертационной работы.

В качестве замечаний и недостатков автореферата можно отметить:

- отсутствие программного обеспечения, с помощью которого можно было бы провести тестирование разработанных протоколов и алгоритмов;

– по тексту автореферата имеются пропуски букв и опечатки.

Указанные недостатки не являются принципиальными, а выполненное диссертационное исследование является завершенной научно-исследовательской работой, имеющей научную новизну, практическую и теоретическую значимость. Основываясь на материале, изложенном в автореферате, можно заключить, что диссертация соответствует требованиям ВАК РФ, предъявляемым к кандидатским диссертациям, а её автор, Синев Валерий Евгеньевич, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность».

Гурьянов Денис Юрьевич
Кандидат технических наук
советник генерального директора по информационной безопасности
ООО «НПФ «ПРИБОРЫ»
190103, Санкт-Петербург, Дерптский пер., д.13 , лит. А., пом. 1Н
тел.: +7-911-238-39-30
эл. почта: guryanov.dyu@yandex.ru

Советник генерального директора
по информационной безопасности, к.т.н Д.Ю. Гурьянов

Подпись Гурьянова Д.Ю. подтверждаю
Генеральный директор М.П. Соколов