ОТЗЫВ

официального оппонента на диссертацию
Березина Андрея Николаевича
на тему: «Методы повышения уровня безопасности защитных преобразований информации» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»
на соискание ученой степени кандидата технических наук

1. Актуальность избранной темы

Защитные преобразования информации являются одним из основных средств обеспечения её безопасности, в частности конфиденциальности, аутентичности и подлинности выполнения различных протоколов. Некоторые из этих преобразований используют ассиметричные криптосистемы с открытым ключом, стойкость которых (т.е. устойчивость к преднамеренному нарушению безопасности) основывается на сложности решения так называемых трудных задач, к которым относятся, прежде всего, задача факторизации и дискретного логарифмирования.

К настоящему времени не известно (а возможно эти задачи, вообще не имеют решения) как выбрать защитные преобразования и их параметры так, чтобы гарантированно обеспечить неизменность заданной сложности вычислений для взлома этих преобразований. Возможность открытия в будущем «продвинутых» методов решения задач факторизации и дискретного логарифмирования ставят под угрозу применение многих защитных преобразований по защите информации.

Поэтому тема диссертационной работы Березина А.Н., предлагающая исследовать повышение уровня безопасности защитных преобразований, безусловно, является актуальной. Однако следует заметить, что при формулировке темы не был конкретизирован ключевой момент исследований, который следовало бы сформулировать как «усовершенствование защитных преобразований на основе одновременного использования двух трудных задач, обеспечивающих сохранение стойкости при дальнейшем прогрессе выполнения алгоритмов факторизации и логарифмирования».

Именно эта задача, в основном, и решается в диссертации, и она является, безусловно, актуальной.

2. Степень обоснованности научных положений, выводов и рекомендаций

Обоснованность полученных результатов достигается путём корректного использования математического аппарата, а так же апробированных другими авторами частных результатов. Корректность и применимость метода демонстрируется путём разработки достаточно широкого круга протоколов защитных преобразований различного типа.

Основные результаты апробированы на 8 международных и национальных конференциях и опубликованы в 6 работах, 5 входят в перечень журналов, рекомендованных ВАК РФ.

Корректность разработанных протоколов показана с помощью формальных математических доказательств.

3. Новизна и достоверность, полученных результатов, выводов и рекомендаций

Основная новизна работы состоит в предложении использовать для защиты информации такие преобразования, которые для нарушения их безопасности требуют решения задачи дискретного логарифмирования по составному модулю, состоящему из произведения двух, специально выбранных больших простых чисел. Такой подход приводит к необходимости решения одновременно двух трудных задач: факторизации и дискретного логарифмирования по простому модулю. То, что такой подход лучше, чем общепринятый с использованием известных простых модулей при логарифмировании, подтверждается тем соображением, что появление продвинутых алгоритмов факторизации и дискретного логарифмирования являются независимыми событиями. Хотя эта гипотеза не может пока быть доказана, но, тем не менее, выбор двух независимых защитных процедур, безусловно, повышает безопасность системы.

Заметим, что хотя предложение использовать составные модули с секретными простыми множителями и рассматривались ранее (см., например, статью K.McCurley "The Discrete Logarithm Problem"), однако, в диссертационной работе более подробно исследован выбор простых множителей, а также применение данного подхода не только для обеспечения конфиденциальности сообщений, но и для выполнения цифровой подписи, распределения ключей и некоторых протоколов. Таким образом, обеспечивается универсальность метода, что ранее отсутствовало в известных работах.

Значительной новизной обладает также исследование коммутативного шифрования, которое не использует для своей реализации вообще никакого обмена открытыми или закрытыми ключами, но требует аутентификации корреспондентов, что может быть обеспечено обменом секретными ключами.

Достоверность полученных результатов не вызывает сомнений. Все выводы и рекомендации были получены на основе строгих математических доказательств и подкреплены поясняющими примерами. Частные результаты и выводы совпадают с известными из литературы.

4. Значимость полученных автором результатов

В теоретическом плане разработанный метод представляет новое направление обеспечения вычислительной трудности задачи дискретного логарифмирования по трудно

разложимому модулю n для построения алгоритмов и протоколов защитных преобразований информации и решает задачу всестороннего оценивания ее вычислительной сложности в условиях, когда известно значение порядка генератора группы.

В практическом плане предложенный метод позволяет существенно расширить типы алгоритмов и протоколов защитных преобразований информации, взлом которых требует одновременного решения двух вычислительно сложных задач – факторизации и дискретного логарифмирования по простому модулю, что обеспечивает повышение уровня безопасности, обеспечиваемого протоколами. В частности метод, позволяет решить проблему разработки практичных протоколов открытого согласования ключа, открытого шифрования, бесключевого шифрования, аутентификации удаленных пользователей информационно-телекоммуникационных систем, индивидуальной, коллективной и групповой ЭЦП, обладающих повышенным уровнем безопасности.

5. Конкретные рекомендации по использованию результатов

Разработанный метод и протоколы предполагаются для использования при разработке современных средств обеспечения информационной безопасности в организациях, деятельность которых охватывает область информационной безопасности, в частности в следующих организациях: СПИИРАН, СПбГЭТУ «ЛЭТИ», ФГБОУ ВО ПГУПС, ФГБОУ ВО "ГУМРФ ИМЕНИ АДМИРАЛА С.О. МАКАРОВА", УНИВЕРСИТЕТ ИТМО, СПбПУ, СПбГУТ, ГУАП, АО "НИИ "ВЕКТОР" и др. Это подтверждается актами о внедрении в СПИИРАН, СПбГЭТУ «ЛЭТИ», ФГБОУ ВО "ГУМРФ ИМЕНИ АДМИРАЛА С.О. МАКАРОВА".

6. Оценка содержания диссертации, ее завершенность

Полученные автором основные научные результаты достаточно полно опубликованы в научных изданиях. Оформление диссертации соответствует требованиям для работ, направляемых в печать. Содержание автореферата корректно отражает основные результаты диссертации.

Диссертация написана хорошим языком, достаточно структурирована, имеет внутреннее единство, что свидетельствует о личном вкладе автора в науку и представляет собой законченное научное исследование.

Основное содержание диссертации, ее положения и результаты соответствуют паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» по пп. 5, 11, 13: «Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет»; «Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа»; «Принципы и решения (технические, математические, организационные и др.) по созданию

новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

7. Замечания

1. Как уже отмечалось ранее, предположение о независимости появления продвинутых алгоритмов факторизации и дискретного логарифмирования является слабо обоснованным. Более того, вообще не имеет смысл рассматривать вероятность появления «многокубитного» квантового компьютера, так как это «единичное событие» и вероятностные методы к нему не применимы.
2. В диссертации (даже в обзоре) не рассматриваются такие криптосистемы с открытым ключом, как Мак-Элис и криптосистема на решётках (LWE), которые, как известно, не могут быть взломаны даже при появлении «многокубитового» квантового компьютера.
3. В диссертации (даже в обзоре) не рассмотрены также методы распределения ключей с обеспечением секретности на «физическом уровне» (см., например, статью A.Mukherjee, et al. “Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey”, 2014), где не требуется решения никаких трудных вычислительных задач для обеспечения информационной безопасности.
4. В диссертации отсутствует место, где бы была чётко сформулирована задача, по преимуществу использования составных модулей при дискретном логарифмировании. Этот вопрос рассредоточен по 1-ой и 2-ой главам.
5. Некоторые предложенные протоколы (например, коллективная ЭЦП) требуют наличие «доверенной стороны», которая должна сформировать некоторые параметры защитных преобразований, что является определенным недостатком, вносящим ограничения при практическом использовании.
6. Не уточнена степень личного вклада автора в совместных публикациях, которые подкрепляют положения, выносимые на защиту.
7. К диссертации не приложены акты о внедрении полученных в ней результатов.
8. Замечания по оформлению работы:
   - нечётко изложены научная задача и цель работы (стр. 10);
   - нет определения, что такое «теория информационной безопасности»;
   - не используются принятая терминология (симметричные, несимметричные криптосистемы, криптосистема с открытым ключом);
   - выводы по главам 2, 3, 4 не конкретизированы;

Отмеченные выше недостатки не являются, однако, принципиальными и не ставят под сомнение основные результаты работы, поскольку относятся либо к расширению области их применения, либо к оформлению работы.

Представляется, что в целом, выполнена интересная в теоретическом плане и, весьма важная, в практическом отношении работа.

8. Заключение

Таким образом, диссертация А.Н. Березина является научно-квалификационной работой, в которой содержится решение задачи разработки универсального и практически реализуемого метода построения протоколов защитного преобразования информации, обладающих повышенным уровнем безопасности, имеющей значение для развития средств и систем обеспечения информационной безопасности информационно-телекоммуникационных технологий, что соответствует требованиям п. 9 «Положения о порядке присуждения ученых степеней», утвержденного постановлением Правительства Российской Федерации от 24.09.2013 г. № 842, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, а ее автор заслуживает присуждения искомой ученой степени.

Официальный оппонент,
профессор, доктор технических наук