Форма 5Т. Титульная страница отчета в РФФИ

НОМЕР ПРОЕКТА 12-07-31164		Учетная карточка проекта
НАЗВАНИЕ ПРОЕКТА Методы повышения безопасности криптографических механизмов аутентификации и алгоритмов цифровой подписи в технологиях электронного документооборота		
ОБЛАСТЬ ЗНАНИЯ 07	КОД(Ы) КЛАССИФИКАТОРА 07-241, 07-235	
ВИД КОНКУРСА: мол_а Конкурс научных проектов, выполняемых молодыми учеными (Мой первый грант)		
ФАМИЛИЯ, ИМЯ, ОТЧЕСТВО РУКОВОДИТЕЛЯ ПРОЕКТА	ТЕЛЕФОН РУКОВОДИТЕЛЯ ПРОЕКТА	
Новикова Евгения Сергеевна	(812)3283311	
ПОЛНОЕ НАЗВАНИЕ ОРГАНИЗАЦИИ, ГДЕ ВЫПОЛНЯЕТСЯ ПРОЕКТ федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В.И. Ульянова (Ленина)"		
ОБЪЕМ СРЕДСТВ, ФАКТИЧЕСКИ ПОЛУЧЕННЫХ ОТ РФФИ за 2012 г., в руб 350000,00	ОБЪЕМ ФИНАНСИРОВАНИЯ, ЗАПРАШИВАЕМЫЙ НА СЛЕДУЮЩИЙ ГОДИЧНЫЙ ЭТАП (если заявленный ранее срок выполнения проекта не истек), в руб 350000	
ЧИСЛО УЧАСТНИКОВ ПРОЕКТА (включая руководителя) 5	ЧИСЛО УЧАСТНИКОВ, ИМЕЮЩИХ УЧЕНУЮ СТЕПЕНЬ 2	ЧИСЛО МОЛОДЫХ (до 35 лет включительно) УЧАСТНИКОВ 5

ФАМИЛИЯ, ИМЯ, ОТЧЕСТВО ОСНОВНЫХ ИСПОЛНИТЕЛЕЙ 2012г	Подписи исполнителей
Гурьянов Денис Юрьевич	
Демьянчук Анна Алексеевна	
Молдовян Дмитрий Николаевич	
Мондикова Яна Александровна	
ПОДПИСЬ РУКОВОДИТЕЛЯ ПРОЕКТА	ДАТА ПОДАЧИ ОТЧЕТА

Форма 501_мол. КРАТКИЙ НАУЧНЫЙ ОТЧЕТ

1.1. Номер проекта

12-07-31164

1.2. Руководитель проекта

Новикова Евгения Сергеевна

1.3. Название проекта

Методы повышения безопасности криптографических механизмов аутентификации и алгоритмов цифровой подписи в технологиях электронного документооборота

1.4. Вид конкурса

мол_а Конкурс научных проектов, выполняемых молодыми учеными (Мой первый грант)

1.5. Год предоставления отчета

2012

1.6. Вид отчета

2 - Промежуточный

1.7. Аннотация

Важным моментом для практического применения криптографических алгоритмов является их безопасность, которая во многом определяется некоторой вычислительно трудной задачей, лежащей в основе криптографического алгоритма. В настоящем отчете представлен и обоснован подход к построению криптосхем на основе трудности задачи дискретного логарифмирования по трудно разложимому модулю. В работе показано, что в рамках предложенного подхода повышается безопасность криптосхем по сравнению со схемами, использующих ЗФ или ЗДЛ по простому модулю. По сравнению с ранее известными подходами к синтезу криптосхем, основанных на трудности одновременного решения ЗФ и ЗДЛ по простому модулю предложенный подход обеспечивает существенное сокращение размера цифровой подписи и высокую вычислительную эффективность. Показано, что данный подход может быть использован для разработки других типов криптографических протоколов, взлом которых требует одновременного решения ЗФ и ЗДЛ по простому модулю.

1.8. Полное название организации, где выполняется проект

федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В.И. Ульянова (Ленина)"

«Исполнители проекта согласны с опубликованием (в печатной и электронной формах) научных отчетов и перечня публикаций по проекту»

Подпись руководителя проекта _____

Форма 502_мол. КРАТКИЙ НАУЧНЫЙ ОТЧЕТ

(- заполняется на английском языке)

2.1. Номер проекта

12-07-31164

2.2. Руководитель проекта

Novikova Evgenia

2.3. Название проекта

Techniques for Security Enforcement of the Authentication Algorithms and Digital Signature Schemes Used in eDocument Flow

2.4. Год представления отчета

2012

2.5. Вид отчета

2

2.6. Аннотация

The security of the cryptographic protocols is important issue for their usage in practice. The security level of the protocols is determined mainly by the hard problem used in them. In the report an approach to constructing cryptographic protocols based on difficulty of discrete logarithm modulo composite number is presented. It is shown that the usage of the proposed approach allows increasing the security level of the protocols compared to ones based on factorisation or discrete logarithm problem modulo prime. Additionally the suggested approach allows generating short digital signatures and it is characterized by increased performance efficiency when compared to the known digital signature schemes based on factoring and discrete logarithm. The suggested approach facilitates constructing different types of the cryptographic protocols based on factoring and discrete logarithms.

2.7. Полное название организации, где реализуется проект

Saint-Petersburg Electrotechnical University "LETI"

*Форма 503.*РАЗВЕРНУТЫЙ НАУЧНЫЙ ОТЧЕТ

3.1. Номер проекта

12-07-31164

3.2. Название проекта

Методы повышения безопасности криптографических механизмов аутентификации и алгоритмов цифровой подписи в технологиях электронного документооборота

3.3. Код(ы) классификатора

07-241, 07-235

3.4. Объявленные ранее цели проекта на текущий год

В проекте была заявлена следующая цель: расширение набора криптографических средств аутентификации электронной информации, обеспечивающий высокий уровень безопасности. Для этого должны быть получены следующие частные результаты:

1) алгоритмы и протоколы электронной цифровой подписи (ЭЦП), взлом которых требует решения двух трудных задач, обеспечивающих малую длину генерируемой подписи.
2) новые алгоритмы и протоколы групповой ЭЦП, взлом которых требует одновременного решения двух независимых трудных задач;
3) новые алгоритмы и протоколы слепой ЭЦП, взлом которых требует одновременного решения двух независимых трудных задач;
4) рекомендации по выбору параметров в протоколах слепой и групповой подписи

3.5. Степень выполнения поставленных в проекте задач

Заявленные цели на текущий год достигнуты в полной мере.

3.6. Полученные за отчетный год важнейшие результаты (для международных проектов – обязательно описать также и степень участия зарубежного партнера)

Основным результатом, полученным за отчетный год, является разработка подхода к синтезу криптосхем на основе двух трудных задач, основанного на том факте, что задача дискретного логарифмирования по трудно разложимому модулю при соответствующем выборе простых делителей модуля для своего решения требует решения независимых задач факторизации и дискретного логарифмирования по простому модулю. В рамках разработанного подхода, применяя схемы построения ЭЦП, основанные на сложности ЗДЛ по простому модулю и используя в качестве системного параметра трудно разложимый модуль вместо простого, можно построить схемы ЭЦП с более коротким размером ЭЦП (по сравнению с ранее известными схемами ЭЦП, основанными на 2-х этих задачах).

Получены следующие результаты, которые были заявлены на 2012 год:

1) разработаны алгоритмы и протоколы электронной цифровой подписи (ЭЦП), взлом которых требует решения двух трудных задач, обеспечивающих малую длину генерируемой подписи.
2) разработаны новые алгоритмы и протоколы групповой ЭЦП, взлом которых требует одновременного решения двух независимых трудных задач;
3) разработаны новые алгоритмы и протоколы слепой ЭЦП, взлом которых требует одновременного решения двух независимых трудных задач;
4) сформулированы рекомендации по выбору параметров в протоколах слепой и групповой подписи

3.7. Степень новизны полученных результатов

Полученные результаты были представлены на российских и международных конференциях:

1. Международная конференция "Mathematical Methods, Models and Architectures for Computer Network Security 2012" (MMM-ACNS-2012)". Санкт-Петербург, 17–20 октября 2012 г
2. Всеармейская научно-практическая конференция «Инновационная деятельность в Вооруженных силах Российской Федерации». Санкт-Петербург, 29-30 ноября 2012

3.8. Сопоставление полученных результатов с мировым уровнем

Полученные результаты являются новыми и оригинальными, они основываются как на результатах, полученные непосредственно исполнителями ранее, так и на современных достижениях двухключевой криптографии. Разработанные криптосхемы отличаются от существующих криптосхем, основанных на сложности решения двух вычислительно трудных задачах, более высоким уровнем быстродействия (в 2,5 и более раз, в зависимости от выбираемой для сравнения известной схемы ЭЦП) и сокращенной длиной подписи (от 5 до 17 раз, в зависимости от выбираемой для сравнения известной схемы ЭЦП).

3.9. Методы и подходы, использованные в ходе выполнения проекта (описать, уделив осо-бое внимание степени оригинальности и новизны)

Подход к синтезу криптосхем на основе двух вычислительно трудных задач

Предлагаемый подход состоит в реализации известных типов криптосхем с открытым ключом, основанных на сложности задачи дискретного логарифмирования (ЗДЛ), над конечным кольцом вычетов по составному модулю $n = rq$, где размер числа r равен 1024 бит, а размер числа q – 512 бит. Известные криптосхемы на основе ЗДЛ реализуются над кольцом вычетов по модулю p размером 1024 бит. Переход от простого модуля к составному означает, что в модифицированных криптосхемах используется трудность ЗДЛ по составному

модулю. Последняя задача принципиально отличается от ЗДЛ по простому модулю. Для решения ЗДЛ по составному модулю можно использовать общие методы дискретного логарифмирования (метод больших и малых шагов, переборный метод, метод Полларда), имеющие экспоненциальную сложность, или метод сведения к ЗДЛ по простому модулю (имеющий субэкспоненциальную сложность) путем факторизации составного модуля и использования китайской теоремы об остатках. Можно также показать, что алгоритм вычисления дискретного логарифма по составному модулю n может быть использован для факторизации числа n. Это подтверждает принципиальное различие ЗДЛ по простому и составному модулям.
Если будут найдены прорывные решения задачи факторизации (ЗФ), то ЗДЛ по составному модулю n потребует решения ЗДЛ по простым модулям q и r. Так как размер числа r в два раза больше размера q, то основной вклад в трудоемкость дискретного логарифмирования в рассматриваемом случае будет вносить ЗДЛ по простому модулю r. При 1024-битовом размере числа r трудоемкость ЗДЛ о модулю r равна 280 операций модульного умножения. Это обеспечит 80-битовую стойкость криптосхем, основанных на трудности ЗДЛ по модулю n даже в случае появления прорывных алгоритмов факторизации. Если будут найдены прорывные решения ЗДЛ по простому модулю, то эти методы смогут быть применены для взлома предлагаемых криптосхем только после решения ЗФ модуля n. Таким образом для взлома предлагаемых криптосхем потребуется решить как ЗФ, так и ЗДЛ по большому простому модулю r.
Следует отметить, что в модифицированных криптосхемах по сравнению с исходными имеет место увеличение временной сложности вычислительных процедур примерно в 2,25 раза, если в исходных схемах не выбираются значения простых модулей со специальной структурой их двоичного представления.
В случае, если в исходных схемах используются простые модули со специальной структурой, то имеет место увеличение сложности в десятки раз. Однако выбор значений модуля, обладающего специальной структурой, в предложенных нами алгоритмах и алгоритмах, известных из литературы и используемых для сравнительной оценки производительности, не может быть использован, поскольку в этом случае не обеспечивается вычислительная сложность нахождения секретных делителей. То есть значение n (в предложенных и используемых для сравнения схемах ЭЦП) не может быть выбрано таким, чтобы устранить операцию арифметического деления при выполнении операции модульного умножения.
Таким образом, в сравнении со схемами [Дернова&Молдовян, 2008; Tahat et.al, 2008; Tahat et al., 2009], основанными на трудности одновременного решения ЗФ и ЗДЛ, в предлагаемых схемах имеет место существенное снижение сложности используемых вычислительных процедур, благодаря уменьшению размера порядка основания, в уравнении проверки подлинности ЭЦП.

[Дернова&Молдовян, 2008] Дернова Е.С., Молдовян Н.А. Протоколы коллективной цифровой подписи, основанные на сложности решения двух трудных задач // Безопасность информационных технологий. 2008 №2. С 79-85.
[Tahat et.al, 2008] Tahat N.M.F., Shatnawi S.M.A., Ismail E.S. New Partially Blind Signature Based on Factoring and Discrete Logarithms. Journal of Mathematics and Statistics.2008. Vol. 4 (2): P. 124-129.
[Tahat et al., 2009] Tahat N.M.F., Ismail E.S., Ahmad R.R. A New Blind Signature Scheme Based On Factoring and Discrete Logarithms. International Journal of Cryptology Research. 2009. Vol.1 (1): P.1-9.

3.10.1.1. Количество научных работ, опубликованных в ходе выполнения проекта (цифрами; для итоговых отчетов – за весь отчетный период)

4

3.11.1.2. Из них включенных в перечень ВАК

0

3.11.1.3. Из них включенных в системы цитирования

0

3.11.2. Количество научных работ, подготовленных в ходе выполнения проекта и принятых к печати в текущем году (цифрами)

1

3.11. Участие в научных мероприятиях по тематике проекта, которые проводились при финансовой поддержке Фонда (указать только количество мероприятий – цифрами)

0

3.12. Участие в экспедициях по тематике проекта, проводимых при финансовой поддержке Фонда (указать только количество экспедиций – цифрами)

0

3.13. Финансовые средства, полученные от РФФИ

350000

3.14.1. Вычислительная техника и научное оборудование, приобретенные на средства Фонда

0

3.15.1. Адреса (полностью) ресурсов в Интернете, подготовленных авторами по данному проекту

-

3.16. Библиографический список всех публикаций по проекту за весь период выполнения проекта, предшествующий данному отчету, в порядке значимости: монографии, статьи в научных изданиях, тезисы докладов и материалы съездов, конференций и т.д.

3.17. Приоритетное направление развития науки, технологий и техники РФ, которому, по мнению исполнителей, соответствуют результаты данного проекта

Информационно-телекоммуникационные системы

3.18. Критическая технология РФ, которой, по мнению исполнителей, соответствуют результаты данного проекта

Технологии обработки, хранения, передачи и защиты информации

3.19. Основное направление технологической модернизации экономики России, которому, по мнению исполнителей, соответствуют результаты

Стратегические информационные технологии, включая вопросы создания суперкомпьютеров и разработки программного обеспечения.

Подпись руководителя проекта _____

Форма 506. ФИНАНСОВЫЙ ОТЧЕТ ПО ПРОЕКТУ №12-07-31164

(Отчет должен соответствовать утвержденной в Фонде смете расходов по проекту.
В случае несоответствия необходимо приложить разъяснение за подписью руководителя проекта и главного бухгалтера)

I.

№ пункта	Код	Наименование показателя	Всего на 2012г. (в целых руб.)
6.1.		Объем финансирования, полученный от РФФИ в 2012 г.	350000,00
6.2.	**211**	Заработная плата	228495,00
6.3.	**212**	Прочие выплаты	-
6.4.	**213**	Начисления на выплаты по оплате труда	69005,00
6.5.	**221**	Услуги связи	-
6.6.	**222**	Транспортные услуги	-
6.7.	**224**	Арендная плата за пользование имуществом	-
6.8.	**225**	Работы, услуги по содержанию имущества	-
6.9.	**226**	Прочие работы, услуги	-
6.10.	**290**	Прочие расходы	-
6.11.	**310**	Увеличение стоимости основных средств	-
6.12.	**340**	Увеличение стоимости материальных запасов	-
6.13.	**900**	ИТОГО РАСХОДОВ (сумма пунктов 6.2 – 6.12)	297500,00
6.14.		Организационно-техническое сопровождение проекта (до 15%)*	52500,00
6.15.		Фактические расходы по проекту в 2012 г. (сумма пунктов 6.13 и 6.14)	350000,00
6.16.		Остаток (если таковой имеется)	-

*С показателя «Увеличение стоимости основных средств» средства на организационно-техническое сопровождение проектов не исчисляются.

II. Финансово-экономическое обоснование расходов по проекту (необходимо обосновать и расшифровать каждый использовавшийся показатель)

Основной статьей расходов в смете по проекту является статья 211 – фонд оплаты труда участников проекта. В проекте участвует 5 человек:

1. Гурьянов Денис Юрьевич (исполнитель)
2. Демьянчук Анна Алексеевна (исполнитель)
3. Молдовян Дмитрий Николаевич (исполнитель)
4. Мондикова Яна Александровна (исполнитель)
5. Новикова Евгения Сергеевна (руководитель)

Остальная часть делегированной суммы по проекту направляется на социальные начисления на фонд оплаты труды (статья 213) и на организационно-техническое сопровождение проекта (15 % от делегированной суммы).

Подпись руководителя проекта _____

Подпись главного бугалтера, заверенная печатью _____

*Форма 510_мол_а.*ЗАЯВКА НА 2013 год

10.1. Номер проекта

12-07-31164

10.2.1. Основной код классификатора

07

10.2.2. Дополнительные коды классификатора

07-241, 01-217

10.3. Ключевые слова

Аутентификация информации, электронная цифровая подпись, вычислительно трудная задача, теория групп и полей

10.4. Цели очередного годичного этапа, связь с основной задачей проекта

Выполнение исследований по разработке в рамках предложенного на первом этапе подхода новых криптографических протоколов, обладающих повышенным уровнем безопасности, за счет того, что из взлом требует одновременного решения двух независимых вычислительно трудных задач.

1) Разработка протоколов слепой коллективной цифровой подписи, основанных на трудности одновременного решения задачи факторизации и дискретного логарифмирования по простому модулю.

2) Разработка протоколов аутентификации удаленных абонентов телекоммуникационной системы с нулевым разглашением секрета, основанных на трудности одновременного решения задачи факторизации и дискретного логарифмирования по простому модулю.

3) Разработка алгоритма коммутативного шифрования на основе двух трудных задач -- факторизации и дискретного логарифмирования.

4) Разработка протокола открытого шифрования на основе двух трудных задач -- факторизации и дискретного логарифмирования.

10.5. Ожидаемые в конце 2013 г. научные результаты

Основным результатом данного исследования будет расширение набора криптографических средств аутентификации и защиты электронной информации, обладающих повышенным уровнем безопасности, за счет того, что из взлом требует одновременного решения двух независимых вычислительно трудных задач. Будут представлены оценки их стойкости и вычислительной эффективности.

Будут получены следующие частные результаты:

1) Протокол слепой коллективной цифровой подписи, основанный трудности одновременного решения задач факторизации и дискретного логарифмирования по простому модулю.

2) Протоколы с нулевым разглашением на основе трудности одновременного решения задач факторизации и дискретного логарифмирования по простому модулю.

3) Способ построения алгоритмов коммутативного шифрования, основанный трудности одновременного решения задач факторизации и дискретного логарифмирования по простому модулю.

3) Способ построения алгоритмов открытого шифрования, основанный трудности одновременного решения задач факторизации и дискретного логарифмирования по простому модулю.

10.6.1. Объем финансирования на 2013 г. запрашиваемый в РФФИ

350000,00

10.6.2. Финансово-экономическое обоснование предполагаемых расходов

Основной статьей расходов в смете по проекту является статья 211 – фонд оплаты труда участников проекта. В проекте участвует 5 человек:

1. Гурьянов Денис Юрьевич (исполнитель)
2. Демьянчук Анна Алексеевна (исполнитель)
3. Молдовян Дмитрий Николаевич (исполнитель)
4. Мондикова Яна Александровна (исполнитель)
5. Новикова Евгения Сергеевна (руководитель)

Остальная часть делегированной суммы по проекту направляется на социальные начисления на фонд оплаты труды (статья 213) и на организационно-техническое сопровождение проекта (15 % от делегированной суммы).

10.7. Планируемая численность участников проекта в 2013 году (указать ФИО и должность)

5

1. Гурьянов Денис Юрьевич (ассистент, исполнитель)
2. Демьянчук Анна Алексеевна (аспирант, исполнитель)
3. Молдовян Дмитрий Николаевич (н.с., исполнитель)
4. Мондикова Яна Александровна (аспирант, исполнитель)
5. Новикова Евгения Сергеевна (ассистент, руководитель)

Подпись руководителя проекта _____

Форма 512. ДАННЫЕ О РУКОВОДИТЕЛЕ И ОСНОВНЫХ ИСПОЛНИТЕЛЯХ - КАК О ТЕХ, КТО ФАКТИЧЕСКИ ПРИНИМАЛ УЧАСТИЕ В ВЫПОЛНЕНИИ ПРОЕКТА В 2012 г., ТАК И О ТЕХ НОВЫХ ИСПОЛНИТЕЛЯХ, КОТОРЫЕ БУДУТ УЧАСТВОВАТЬ В РАБОТЕ ПО ПРОЕКТУ В 2013 г

12.1.1. Фамилия, имя, отчество *(полностью)*
Гурьянов Денис Юрьевич

12.1.2. Фамилия, имя, отчество *(на английском языке)*
Gurianov Denis Y

12.2.1. Дата рождения *(цифрами - число.месяц.год)*
20.11.1984

12.2.2. Пол *(1-мужской, 2-женский)*
1

12.3.1. Учёная степень *(сокращённое название)*
ктн

12.3.2. Год присуждения ученой степени
2011

12.4.1. Учёное звание
б/з

12.4.2. Год присвоения ученого звания

12.5.1. Полное название организации – места работы
федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В.И. Ульянова (Ленина)"

12.5.2. Сокращенное название организации – места работы
СПбГЭТУ

12.6. Должность *(сокращенное название)*
асс.

12.7.1. Область научных интересов - ключевые слова

12.7.2. Область научных интересов – коды классификатора
01-217

12.8. Общее число публикаций *(исключая тезисы докладов)*

12.9.1. Почтовый индекс
198332

12.9.2. Почтовый адрес
пр. Кузнецова, д. 17, кв. 117

12.10. Телефон для связи
(812)2341543

12.12. Факс
(812) 3462758

12.13. Адрес электронной почты
rightx@gmail.com

12.14. Участие в проекте *(Р - руководитель; И - исполнитель)*
И

12.15. Участие в других проектах, поддерживаемых РФФИ или другими организациями *номера грантов и вид участия в них (Р - руководитель; И - исполнитель)*

12.16. Номер страхового свидетельства государственного пенсионного страхования *(для граждан РФ)*
139-573-647 04

12.17. Год участия в проекте
2012

Личная подпись участника, на которого заполнена форма _____

Форма 512. ДАННЫЕ О РУКОВОДИТЕЛЕ И ОСНОВНЫХ ИСПОЛНИТЕЛЯХ - КАК О ТЕХ, КТО ФАКТИЧЕСКИ ПРИНИМАЛ УЧАСТИЕ В ВЫПОЛНЕНИИ ПРОЕКТА В 2012 г., ТАК И О ТЕХ НОВЫХ ИСПОЛНИТЕЛЯХ, КОТОРЫЕ БУДУТ УЧАСТВОВАТЬ В РАБОТЕ ПО ПРОЕКТУ В 2013 г

12.1.1. Фамилия, имя, отчество *(полностью)*
Демьянчук Анна Алексеевна

12.1.2. Фамилия, имя, отчество *(на английском языке)*
Demyanchuk Anna Alexeevna

12.2.1. Дата рождения *(цифрами - число.месяц.год)*
01.12.1987

12.2.2. Пол *(1-мужской, 2-женский)*
2

12.3.1. Учёная степень *(сокращённое название)*
б/с

12.3.2. Год присуждения ученой степени

12.4.1. Учёное звание
б/з

12.4.2. Год присвоения ученого звания

12.5.1. Полное название организации – места работы
Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук

12.5.2. Сокращенное название организации – места работы
СПИИРАН

12.6. Должность *(сокращенное название)*
мнс

12.7.1. Область научных интересов - ключевые слова

12.7.2. Область научных интересов – коды классификатора
01-217

12.8. Общее число публикаций *(исключая тезисы докладов)*

12.9.1. Почтовый индекс

12.9.2. Почтовый адрес

12.10. Телефон для связи
(812)3283311

12.12. Факс
3284450

12.13. Адрес электронной почты
vleti@ya.ru

12.14. Участие в проекте *(Р - руководитель; И - исполнитель)*
И

12.15. Участие в других проектах, поддерживаемых РФФИ или другими организациями *номера грантов и вид участия в них (Р - руководитель; И - исполнитель)*

12.16. Номер страхового свидетельства государственного пенсионного страхования *(для граждан РФ)*
126-419-742 62

12.17. Год участия в проекте
2012

Личная подпись участника, на которого заполнена форма _____

Форма 512. ДАННЫЕ О РУКОВОДИТЕЛЕ И ОСНОВНЫХ ИСПОЛНИТЕЛЯХ - КАК О ТЕХ, КТО ФАКТИЧЕСКИ ПРИНИМАЛ УЧАСТИЕ В ВЫПОЛНЕНИИ ПРОЕКТА В 2012 г., ТАК И О ТЕХ НОВЫХ ИСПОЛНИТЕЛЯХ, КОТОРЫЕ БУДУТ УЧАСТВОВАТЬ В РАБОТЕ ПО ПРОЕКТУ В 2013 г

12.1.1. Фамилия, имя, отчество *(полностью)*
Молдовян Дмитрий Николаевич

12.1.2. Фамилия, имя, отчество *(на английском языке)*
Moldovyan Dmitriy Nikolaevich

12.2.1. Дата рождения *(цифрами - число.месяц.год)*
04.09.1986

12.2.2. Пол *(1-мужской, 2-женский)*
1

12.3.1. Учёная степень *(сокращённое название)*
б/с

12.3.2. Год присуждения ученой степени

12.4.1. Учёное звание
б/з

12.4.2. Год присвоения ученого звания

12.5.1. Полное название организации – места работы
Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук

12.5.2. Сокращенное название организации – места работы
СПИИРАН

12.6. Должность *(сокращенное название)*
мнс

12.7.1. Область научных интересов - ключевые слова
криптография, шифры, криптографические протоколы, цифровая подпись, аутентификация, защита информации, трудные задачи, криптосистемы с открытым ключом

12.7.2. Область научных интересов – коды классификатора
07-241, 01-217, 07-235

12.8. Общее число публикаций *(исключая тезисы докладов)*
35

12.9.1. Почтовый индекс

12.9.2. Почтовый адрес

12.10. Телефон для связи
(812)3283311

12.12. Факс
3284450

12.13. Адрес электронной почты
mdn.spectr@mail.ru

12.14. Участие в проекте *(Р - руководитель; И - исполнитель)*
И

12.15. Участие в других проектах, поддерживаемых РФФИ или другими организациями *номера грантов и вид участия в них (Р - руководитель; И - исполнитель)*
государственный контракт №П635 от 19.05.2010

гранты РФФИ № 08-07-00096-а и № 08-07-90100-Мол_а

12.16. Номер страхового свидетельства государственного пенсионного страхования *(для граждан РФ)*
126-748-289 91

12.17. Год участия в проекте
2012

Личная подпись участника, на которого заполнена форма _____

Форма 512. ДАННЫЕ О РУКОВОДИТЕЛЕ И ОСНОВНЫХ ИСПОЛНИТЕЛЯХ - КАК О ТЕХ, КТО ФАКТИЧЕСКИ ПРИНИМАЛ УЧАСТИЕ В ВЫПОЛНЕНИИ ПРОЕКТА В 2012 г., ТАК И О ТЕХ НОВЫХ ИСПОЛНИТЕЛЯХ, КОТОРЫЕ БУДУТ УЧАСТВОВАТЬ В РАБОТЕ ПО ПРОЕКТУ В 2013 г

12.1.1. Фамилия, имя, отчество *(полностью)*
Мондикова Яна Александровна

12.1.2. Фамилия, имя, отчество *(на английском языке)*
Mondikova Yana

12.2.1. Дата рождения *(цифрами - число.месяц.год)*
10.11.1989

12.2.2. Пол *(1-мужской, 2-женский)*
2

12.3.1. Учёная степень *(сокращённое название)*
б/с

12.3.2. Год присуждения ученой степени

12.4.1. Учёное звание
б/з

12.4.2. Год присвоения ученого звания

12.5.1. Полное название организации – места работы
федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В.И. Ульянова (Ленина)"

12.5.2. Сокращенное название организации – места работы
СПбГЭТУ

12.6. Должность *(сокращенное название)*
студ.

12.7.1. Область научных интересов - ключевые слова

12.7.2. Область научных интересов – коды классификатора
01-103

12.8. Общее число публикаций *(исключая тезисы докладов)*

12.9.1. Почтовый индекс

12.9.2. Почтовый адрес

12.10. Телефон для связи
(812)2341543

12.12. Факс
(812) 3462758

12.13. Адрес электронной почты
MondikovaY@gmail.com

12.14. Участие в проекте *(Р - руководитель; И - исполнитель)*
И

12.15. Участие в других проектах, поддерживаемых РФФИ или другими организациями *номера грантов и вид участия в них (Р - руководитель; И - исполнитель)*

12.16. Номер страхового свидетельства государственного пенсионного страхования *(для граждан РФ)*
116-631-790 52

12.17. Год участия в проекте
2012

Личная подпись участника, на которого заполнена форма _____

*Форма 512.*ДАННЫЕ О РУКОВОДИТЕЛЕ И ОСНОВНЫХ ИСПОЛНИТЕЛЯХ - КАК О ТЕХ, КТО ФАКТИЧЕСКИ ПРИНИМАЛ УЧАСТИЕ В ВЫПОЛНЕНИИ ПРОЕКТА В 2012 г., ТАК И О ТЕХ НОВЫХ ИСПОЛНИТЕЛЯХ, КОТОРЫЕ БУДУТ УЧАСТВОВАТЬ В РАБОТЕ ПО ПРОЕКТУ В 2013 г

12.1.1. Фамилия, имя, отчество *(полностью)*
Новикова Евгения Сергеевна

12.1.2. Фамилия, имя, отчество *(на английском языке)*
Novikova Evgenia

12.2.1. Дата рождения *(цифрами - число.месяц.год)*
18.09.1984

12.2.2. Пол *(1-мужской, 2-женский)*
2

12.3.1. Учёная степень *(сокращённое название)*
ктн

12.3.2. Год присуждения ученой степени
2009

12.4.1. Учёное звание
б/з

12.4.2. Год присвоения ученого звания

12.5.1. Полное название организации – места работы
Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук

12.5.2. Сокращенное название организации – места работы
СПИИРАН

12.6. Должность *(сокращенное название)*
снс

12.7.1. Область научных интересов - ключевые слова
защита информации, аутентификация данных, двухключевая криптография

12.7.2. Область научных интересов – коды классификатора
01-217, 07-241

12.8. Общее число публикаций *(исключая тезисы докладов)*
30

12.9.1. Почтовый индекс
197183

12.9.2. Почтовый адрес
ул. Школьная, д.5, кв. 5

12.10. Телефон для связи
(812)3283311

12.12. Факс
3284450

12.13. Адрес электронной почты
evgeshka19@mail.ru

12.14. Участие в проекте *(Р - руководитель; И - исполнитель)*
Р

12.15. Участие в других проектах, поддерживаемых РФФИ или другими организациями *номера грантов и вид участия в них (Р - руководитель; И - исполнитель)*
№ 08-07-90100-Мол_а "Новые алгоритмы аутентификации электронной информации и криптографические схемы с разделением секрета" "РФФИ"; № 08-07-00096-а "Новые протокол аутентификации информации в автоматизированных системах" "РФФИ"; №10-07-90403-Укр_а "Протоколы обеспечения неотслеживаемостии аутентификации информации в автоматизированных информационных системахи расширение функциональности стандартов цифровой подписи" "РФФИ";
"Методы повышения безопасности криптографических механизмов аутентификации и алгоритмов цифровой подписи в технологиях электронного документооборота" Мой первый грант РФФИ № 12-07-311064 мол_а (2012-2013 гг.)

12.16. Номер страхового свидетельства государственного пенсионного страхования *(для граждан РФ)*
130-697-163 59

12.17. Год участия в проекте
2012

Личная подпись участника, на которого заполнена форма _____