ПИЛОТНЫЙ ПРОЕКТ
Обоснование и реализация минималистского протокола аутентификации микроэлектронных устройств

Цель проекта. Фактическое доказательство возможности реализации действенной, высокорентабельной и энергоэкономичной встроенной электронной защиты от подделки дешевых микроэлектронных устройств – радиочастотных меток и микросенсоров (кремниевых и органических), в условиях крайнего дефицита ресурсов. Решение этой ключевой задачи, способной привести к далеко идущему инновационному прорыву в области микросенсорных технологий и технологий обеспечения безопасности, осуществляется на основе открытий в области алгебры, развития стохастических систем и технологий – нового научно-технического направления, отличающегося подавляющим превосходством перед всеми другими известными на сегодня в мире подходами.

Особенности технической реализации. Представляемый проект опирается на самые дешевые из всех, промышленно освоенные, неперезаписываемые (типа **RO**) идентификационные радиочастотные метки (RF-метки **ID**), что позволяет при минимальных затратах и в кратчайшие сроки получить максимально значимый практический результат.

Привносимые в проект ноу-хау – односторонний минималистский Протокол аутентификации, с не имеющей сравнительных аналогов высокоэффективной однонаправленной функцией с длиной платформы 2×15 бит и схемотехнические решения позволяют использовать простейший радиочастотный интерфейс (два состояния на входе и выходе метки), с принимаемым и передаваемым сигналом, формально сводимым к логическому нулю и единице. При этом в целом, аппаратная реализация радиочастотного интерфейса и односторонней функции Протокола характеризуется низким энергопотреблением, линейной и простой топологией и очень малым числом логических элементов (30 триггеров и чуть более 300 транзисторов – 75 **GE**).

Согласно предварительному анализу криптографическая стойкость Протокола аутентификации при длине ключа около 65 бит составляет не менее 2^{57}, что по критерию временных и финансовых затрат необходимых для взлома защиты, вполне достаточно для планируемых приложений на основе дешевых RF-меток **ID**. Ко всему, как подтверждает проведенный анализ, криптографическая стойкость указанного Протокола, при незначительно малых дополнительных аппаратных затратах, может быть легко доведена до 2^{64}, на будущее 2^{96} и выше. В свою очередь, как уже не раз говорилось, достижение таких показателей исключительно обязано высокой эффективности привносимых в Проект новой алгебраической базы и стохастических технологий. Между тем, как отмечают эксперты, проведенный криптографический анализ в теоретической части, не касающейся статистического анализа, является не столь убедительным, как того бы хотелось, и в интересах дела требует развития и достижимой на сегодня исчерпывающей полноты.

В дополнение к этому, согласно с Законом, введенным постановлением Правительства РФ от 29.12.2007 № 957, по всем видам деятельности, что вводимые Протоколы аутентификации, как односторонний, так и двухсторонний, ограничены дальностью действия до 400 метров (в нашем случае для пассивных RF-меток, в пределе это 15-20 метров) не подлежат лицензированию. В тоже время, в соответствии с требованиями, предъявляемыми к специальным защитным знакам, утвержденных Правительством РФ от 25.07.1997, снимаются проблемы связанные с сертификацией RF-меток. Ко всему – в продолжение темы, в ответ на беспочвенные заявления в адрес стохастических технологий без должного изучения сути предмета, можно сказать, что неприятие неопровержимо доказанного на известных пакетах статистических тестов (**DICHARD**, **NIST** и их усилении) свойственного им существенно выраженного недетерминированного поведения (в отличие от решений построенных на основе полей Галуа), по сути, ведет к отрицанию предарифметики, а вслед за этим и к совсем абсурдному отрицанию элементарных основ арифметики.

В связи с тем, что требования к считывающим устройствам по стоимости и энергопотреблению не столь критичны и высоки, рассмотрение иных вопросов, касающихся их функционирования, системной поддержки и изготовления, выносится за рамки представляемого Проекта.

Предполагаемая общая стоимость работ: 4 млн. руб. ($134 тыс.), из нее 2.5 млн. руб. ($84 тыс.) на обоснование Протокола аутентификации и 1.5 млн. руб. ($50 тыс.) на изготовление промышленного образца, что относительно известных проектов крайне мала, благодаря имеющейся глубокой научно-технической и маркетинговой проработке, а также ограничениям накладываемым на использование и распространение привносимых решений и результатов проекта.

Общая продолжительность работ: 10 месяцев, необходимая для достижения коммерчески значимых результатов, далеко опережающих мировой уровень.

Календарный план выполнения работ, учитывающий указанные особенности технической реализации, а также по имеющимся заключениям экспертов и высокой квалификации исполнителей, гарантирующим получение в указанные сроки заявленных результатов, приведен в Приложении 1.

Результаты реализации Проекта:

1. Подтверждение криптографической стойкости и оптимизация параметров привносимого в проект одностороннего Протокола аутентификации, позволяющего обеспечить действенную, высокорентабельную (**без увеличения себестоимости производства**) и энергоэкономичную (**без уменьшения радиуса действия**) встроенную электронную защиту от подделки RF-меток **ID**.
2. Изготовление промышленных образцов неперезаписываемых (типа **RO**) дешевых защищенных RF-меток **ID**, необходимых для налаживания их массового производства.

Области применения. Защита продукции и изделий от фальсификации и подделки, дистанционная оплата проезда, регламентирование доступа и организация пропускного режима, защита удостоверяющих документов и валюты, маркировка почтовых отправлений, архивных документов, выставочных экспонатов и содержимого библиотечных фондов и прочие.

Потенциальные потребители результатов – ведущие российские и иностранные производители меток RFID (**Ангстрем**, **Ситроникс**, **РосНоноТех**, а также **Hitachi**, **NXP Semiconductors**, **PolyIC**) и крупные системные интеграторы (**EPCglobal**, **Symbol**, **IBM**, **HP**, **Philips**, **Siemens**, **Nokia**, **SAP**, **Microsoft**) и др.

Как видится исходя из анализа потребительного спроса, состояния и динамики развития мирового рынка RFID, при грамотной защите интеллектуальных прав, высококвалифицированной технической поддержке и безукоризненно поставленном маркетинге, результаты Проекта могут быть в различных вариантах легко и быстро адаптированы под нужды Заказчиков, включая интересы торговых гигантов (**Wal-Mart**, **Metro** и др.), транспортных корпораций, государственных ведомств и служб, с большой выгодой проданы владельцами результатов работ, предоставлены по лицензии и/или вложены в производство.

Ближайшие перспективы развития. Распространение решений на реализацию двухстороннего Протокола аутентификации, а также на все остальные однократно (**WORM**) и многократно (**RW**) перезаписываемые промышленно освоенные метки RFID.

Реализация двухстороннего Протокола аутентификации предполагает введение продвинутого радиочастотного интерфейса (четыре независимых состояния на входе и выходе, ориентированного на последующий переход к микросенсорным и помехоустойчивым технологиям), одноразрядного двоичного датчика случайных чисел на подобии встроенного в радиочастотную метку Gen2 EPC, а также элементов памяти типа WORM и RW.

Решение этих задач предполагается в рамках отдельного десятимесячного Развернутого проекта. Работы можно будет начать менее чем через полгода, по ходу подтверждения и получения заложенных в Пилотный проект технических результатов.

Результаты реализации Развернутого проекта способны обеспечить, не приводящую к увеличению себестоимости, действенную, высоко рентабельную и энергоэкономичную встроенную электронную защиту от подделки, всех без исключения промышленно освоенных дешевых меток RFID. В частности таких наиболее распространенных, как Gen2 **EPCglobal**, µ-Chip **Hitachi**, I-Code от разных производителей и аналогичных им кремниевых и перспективных, очень дешевых, но при этом крайне критичных к аппаратным затратам и энергопотреблению – органических меток компаний **PolyIC** и **NXP**, а вслед за ними и недорогие смарт-чипы.

С введением двухстороннего Протокола аутентификации, предусматривающего одновременную проверку, как подлинности меток, так и подлинности считывающих их устройств, наряду со снижением эффективности сторонних криптографических атак, ко всему прочему, становится возможным решать такие дополнительные задачи, как – проведение взаимных денежных расчетов и платежей, дистанционная оплата услуг, включая в движении и другие.

Согласно расчетам (см. Приложение 2), предполагаемая общая стоимость работ составляет 7.7 млн. руб. ($257 тыс.), из нее 3.5 млн. руб. ($117 тыс.) на микроэлектронику, и неизмеримо мала по отношению ко всем реализуемым в мире проектам, в частности к многомиллионным Европейским проектам BRIDGE и SToP. Кроме этого, не смотря на усилия, полученные результаты еще и весьма существенно отстают от требований, предъявляемых современным уровнем развития технологий и пока еще далеко неизвестно, когда это отставание будет преодолено.

Отменим, что приводимые согласованные в 2010 году оценки стоимости работ, носят предварительный характер, и в связи с ростом налогов, по всей видимости, будут увеличены.

Дальнейшие перспективы развития. Результаты работ, представляемые этими проектами, в части и в целом, сохраняют преемственность в разработке. Решение следующих за этим задач, предполагает переход от функционально ограниченных технологий RFID к сетевым, защищенным от компрометации и подделки микросенсорным технологиям. Работы в этом направлении планируется проводить поэтапно, в рамках двухгодичного Комплексного проекта.

Приложение № 1
к Соглашению № от __ марта 2010 г.

КАЛЕНДАРНЫЙ ПЛАН ВЫПОЛНЕНИЯ РАБОТ (Пилотный проект)

№ п/п	**Содержание выполняемых работ**	**Перечень документов и технических образцов**	**Сроки проводимых работ**	**Исполнители**	**Оплата работ** (тыс. руб.)
1	**2**	**3**	**4**	**5**	**6**
1	**<u>Первый этап</u>: ЭСКИЗНЫЙ ПРОЕКТ**	Отчетная документация (ОД), Программное обеспечение (ПО), Техническая документация (ТД)	5 месяцев	**Криптоанализ** **Координатор** **Заказчик**	600 250 50
	ИТОГО				900
1.1	Предварительный криптографический анализ привносимого в Проект одностороннего Протокола аутентификации:	ОД, ПО, Экспертное заключение	5 месяцев	**Криптоанализ** **Координатор** **Заказчик**	600 300 50
1.1.1	– Доработка привносимого в Проект специального программного обеспечения, проведение статистического анализа и оценки мощности ключевого пространства. Подготовка промежуточного отчета.	ОД, ПО	5 месяцев	**Координатор**	250
1.1.2	– Проведение криптоанализа, включая доработку привносимых моделей криптографических атак, специального программного обеспечения и подготовка промежуточного отчета, с указанием рекомендаций по технической реализации Проекта.	ОД, ПО	5 месяцев	**Криптоанализ**	600
1.1.3	– Проведение независимой экспертизы по оценке полноты криптографического анализа привносимых решений и проверки их соответствия техническому заданию.	Экспертное заключение	1 месяц	**Заказчик**	50
2	**<u>Второй этап</u>: ТЕХНИЧЕСКИЙ ПРОЕКТ**	Итоговый отчет, ПО, ТД, ОД	5 месяцев	**Электроника** **Криптоанализ** **Координатор**	75 300 475
	ИТОГО				850
2.1	Разработка в соответствии с техническим заданием принципиальной электронной схемы реализации привносимой в Проект однонаправленной функции Протокола аутентификации радиочастотной метки и подготовка технической документации.	ТД	1 месяц	**Координатор**	225
2.2	Разработка радиочастотного интерфейса взаимодействия меток со считывающими устройствами при исполнении одностороннего Протокола аутентификации.	ТД	1 месяц	**Электроника**	75

2.3	Комплексный криптографический анализ привносимого в Проект одностороннего Протокола аутентификации:	ТД, ОД, ПО	4 месяца	**Криптоанализ** **Координатор**	300 150
2.3.1	– Проведение комплексного статистического анализа, включая доработку программного обеспечения, подготовку технической документации и итогового отчета.	ТД, ОД, ПО	4 месяца	**Координатор**	150
2.3.2	– Проведение комплексного криптоанализа, включая доработку моделей криптографических атак, специального программного обеспечения, подготовку технической документации и итогового отчета.	ТД, ОД, ПО	4 месяца	**Криптоанализ**	300
2.4	Подготовка итогового отчета.	ОД	1 месяц	**Координатор**	100
ИТОГО		Итоговый отчет, ПО, ТД, ОД	10 месяцев	**Электроника** **Криптоанализ** **Координатор** **Заказчик**	75 900 725 50
ВСЕГО					1 750

Дополнительные статьи расхода:

Ежемесячные вознаграждения Руководителю работ – 750 тыс. руб., из расчета на 10 месяцев (75 тыс./месяц с учетом налоговых вычетов с физических лиц).

Итого: 750 тыс. руб.

Общая стоимость работ: 2.5 млн. руб. ($84 тыс.), из нее на I этап – 1 275 тыс. руб. ($43 тыс.), на II этап – 1 225 тыс. руб. ($41 тыс.)

Общая продолжительность работ: 10 месяцев.

Примечание. Под ниже условными обозначениями подразумеваются лица, планируемые для привлечения к работе по договорам:

Координатор – Руководитель проекта, ответственный исполнитель работ, **Кулаков И. А**.
Криптоанализ – компания **ЛанКрипто**.
Электроника – ОАО **Ангстрем**.

КАЛЕНДАРНЫЙ ПЛАН ВЫПОЛНЕНИЯ РАБОТ (Заводской проект, для справки)

№ п/п	**Содержание выполняемых работ**	**Перечень документов и технических образцов**	**Сроки проводимых работ**	**Исполнители**	**Оплата работ** (тыс. руб.)
1	**2**	**3**	**4**	**5**	**6**
1	**ТЕХНИЧЕСКИЙ ПРОЕКТ**	ПО, ТД, Фотошаблоны, ОО	6 месяцев	**Электроника** **Электроника-Т**	850 500
1.1	Разработка в соответствии с техническим заданием принципиальной электронной схемы реализации радиочастотной метки (далее RF-метка), исходя из реализации привносимого в Проект одностороннего Протокола аутентификации и его сопряжения с Протоколом идентификации метки. Подготовка технической документации.	ТД	1 месяц	**Электроника**	150
1.2	Создание промышленного образца RF-метки:	ПО, ТД, Фотошаблоны, ОО	5 месяцев	**Электроника** **Электроника-Т**	850 500
1.2.1	– Разработка топологии RF-метки. Проведение стендового моделирования и подготовка технической документации.	ПО, ТД	2 месяца	**Электроника-Т**	500
1.2.2	– Изготовление фотошаблонов и промышленного образца RF-метки. Проведение технической экспертизы и подготовка технической документации.	Фотошаблоны, ОО, ТД	3 месяца	**Ангстрем**	850
ВСЕГО					1 500

Общая стоимость работ: 1.5 млн. руб. ($50 тыс.)

Общая продолжительность работ: 6 месяцев.

Примечание. Под ниже условными обозначениями подразумеваются лица, планируемые для привлечения к работе по договорам:

Электроника-Т (разработка топологии) – ОАО **Ангстрем-М**.

Приложение № 2
к Соглашению № от __ марта 2010 г.

КАЛЕНДАРНЫЙ ПЛАН ВЫПОЛНЕНИЯ РАБОТ (Развернутый проект, для потенциальных инвесторов)

№ п/п	**Содержание выполняемых работ**	**Перечень документов и технических образцов**	**Сроки проводимых работ**	**Исполнители**	**Оплата работ** (тыс. руб.)
1	**2**	**3**	**4**	**5**	**6**
1	**<u>Первый этап</u>: ЭСКИЗНЫЙ ПРОЕКТ**	Отчетная документация (ОД), Программное обеспечение (ПО), Опытные образцы (ОО), Техническая документация (ТД)	5 месяцев	**Электроника** **Радиотехника** **Криптоанализ** **Криптоанализ-М** **Координатор**	1 800 350 250 350 400
	ИТОГО				3 150
1.1	Предварительный криптографический анализ привносимого в Проект двухстороннего Протокола аутентификации:	ОД, ПО	5 месяцев	**Криптоанализ** **Криптоанализ-М** **Координатор**	250 350 150
1.1.1	– Доработка привносимого в Проект специального программного обеспечения, проведение статистического анализа и оценки мощности ключевого пространства. Подготовка промежуточного отчета.	ОД, ПО	5 месяцев	**Координатор**	150
1.1.2	– Проведение криптоанализа двухстороннего Протокола аутентификации, включая доработку моделей криптографических атак, специального программного обеспечения и подготовка промежуточного отчета.	ОД, ПО	5 месяцев	**Криптоанализ**	250
1.1.3	– Разработка методики комплексного криптографического анализа решений предоставляемых стохастическими технологиями и подготовка промежуточного отчета, с указанием рекомендаций по технической реализации Проекта.	ОД	5 месяцев	**Криптоанализ-М**	350
1.2	Разработка радиочастотного интерфейса взаимодействия меток со считывающими устройствами при исполнении двухстороннего Протоколов аутентификации, с перспективой перехода к помехоустойчивым технологиям приема и передачи сигналов.	ТД	2 месяца	**Радиотехника**	225
1.3	Разработка одноразрядного двоичного датчика случайных чисел, на основе прототипа встроенного в радиочастотную метку Gen2 EPC.	ТД	1 месяц	**Радиотехника**	125
1.4	Разработка в соответствии с техническим заданием принципиальной электронной схемы, распространяющаяся на реализацию всех типов RF-меток и привносимого в Проект двухстороннего Протокола их аутентификации:	ТД	1 месяц	**Электроника** **Координатор**	300 250

1.4.1	– Разработка принципиальной электронной схемы реализации привносимой в Проект однонаправленной функции двухстороннего Протокола аутентификации RF-метки и подготовка технической документации.	ТД	1 месяц	**Координатор**	250
1.4.2	– Разработка принципиальных электронных схем реализации RF-меток типа RO, WORM, RW, с учетом реализации одностороннего и двухстороннего Протокола аутентификации и подготовка технической документации.	ТД	5 месяцев	**Электроника**	300
1.5	Разработка на основе ПЛИС имитационных прототипов RF-меток типа RO, WORM, RW с привносимым в Проект встроенным односторонним и двухсторонним Протоколом аутентификации и проведение их стендовых испытаний:	ПО, ОО, ОД	5 месяцев	**Электроника**	1 500
1.4.1	– Создание демонстрационно-испытательного стенда.	ОО	2 месяца	**Электроника**	450
1.4.2	– Разработка на основе ПЛИС имитационных прототипов RF-меток указанных типов с односторонним и двухсторонним Протоколом аутентификации. Проведение стендового моделирования и доработка решений.	ПО, ОО	4 месяца	**Электроника**	850
1.4.3	– Оценка основных характеристик реализации на кристаллах опытных образцов RF-меток указанного типа, для различных топологических норм.	ОД	1 месяц	**Электроника**	200
2	**<u>Второй этап</u>: ТЕХНИЧЕСКИЙ ПРОЕКТ**	Итоговый отчет, ПО, ТД, ОД, Демонстрационный стенд, ОО	5 месяцев	**Электроника** **Криптоанализ** **Криптоанализ-М** **Координатор**	1 700 350 550 300
	ИТОГО				3 600
2.1	Комплексный криптографический анализ привносимого в Проект одностороннего и двухстороннего Протокола аутентификации:	ТД, ОД, ПО	5 месяцев	**Криптоанализ** **МИФИ** **Координатор**	350 550 200
2.1.1	– Проведение комплексного статистического анализа, включая доработку програм-много обеспечения, подготовку технической документации и итогового отчета.	ТД, ОД, ПО	4 месяца	**Координатор**	200
2.1.2	– Проведение комплексного криптоанализа, включая доработку моделей криптографических атак, специального программного обеспечения, подготовку технической документации и итогового отчета.	ТД, ОД, ПО	4 месяца	**Криптоанализ**	350
2.1.3	– Доработка методики комплексного криптографического анализа, разработка программного обеспечения и проведение общей криптографической экспертизы, подготовка технической документации и итогового отчета.	ТД, ОД, ПО	5 месяцев	**Криптоанализ-М**	550
2.2	Доработка имитационных прототипов RF-меток типа RO, WORM, RW с привносимым в Проект встроенным односторонним и двухсторонним Протоколом аутентификации и проведение их стендовых испытаний:	ПО, ОО, ТД, ОД	5 месяцев	**Электроника**	1 700
2.2.1	– Доработка имитационных прототипов RF-меток указанных типов, необходимая для последующей разработки топологии и изготовления опытных образцов. Проведение стендового моделирования, технической экспертизы и подготовка технической документации.	ПО, ТД, ОО	5 месяцев	**Электроника**	900
2.2.2	– Доработка демонстрационно-испытательного стенда и изготовление мобильного Демонстрационного стенда.	ОО	5 месяцев	**Электроника**	450

2.2.3	– Уточнение оценок основных характеристик реализации на кристаллах опытных образцов RF-меток указанного типа, для различных топологических норм.	ОД	5 месяцев	**Электроника**	350
2.3	Подготовка итогового отчета.	ОД	1 месяц	**Координатор**	100
ИТОГО		Итоговый отчет, ПО, ТД, ОД, Демонстрационный стенд, ОО	10 месяцев	**Электроника** **Радиотехника** **Криптоанализ** **Криптоанализ-М** **Координатор**	3 500 350 600 900 700
ВСЕГО **из нее, на разработку:** – имитационных прототипов RF-меток на ПЛИС (из нее на оценку основных характеристик опытных образцов - 550 тыс. руб.); – мобильного Демонстрационного стенда; – радиочастотного интерфейса; – принципиальной электронной схемы; – специального программного обеспечения (1250 тыс. руб.) и проведение криптографического анализа (600 тыс. руб.).					6 050 2 400 900 350 550 1 850

Дополнительные статьи расхода:

1. Ежемесячные вознаграждения Руководителю работ – 1150 тыс. руб., из расчета на 10 месяцев (115 тыс./месяц с учетом налоговых вычетов с физических лиц).
2. Приобретение ноутбука, принтера, сканера и расходных материалов для организационно-технического сопровождения Проекта и последующего обслуживания мобильного Демонстрационного стенда – 125 тыс. руб.
3. Модернизация стационарного компьютера Координатора, для проведения статистических расчетов, адаптации специального криптографического обеспечения и подтверждения результатов реализации Проекта – 25 тыс. руб.
4. Участие автора в международных конференциях и симпозиумах по проблемам безопасности технологий RFID, в целях маркетингового продвижения результатов Проекта, включая расходы на референта свободно владеющего английским языком – 350 тыс. руб.

Итого: 1 650 тыс. руб.

Общая стоимость работ: 7.7 млн. руб. ($257 тыс.), без учета оплаты работ за подготовку материалов на английском языке.

Общая продолжительность работ: 10 месяцев.

Примечание. Под ниже условными обозначениями подразумеваются лица, планируемые для привлечения к работе по договорам:

Криптоанализ-М (разработка комплексной методики) – Руководитель группы, доктор технических наук, профессор, **Иванов М.А.**
Радиотехника – ОАО **Ангстрем**.