СОВРЕМЕННАЯ КРИПТОЛОГИЯ: EUROCRYPT 2012 И SIBECRYPT 2012. НАУЧНАЯ ПРОБЛЕМАТИКА И ЛИЧНЫЕ ВПЕЧАТЛЕНИЯ

Коренева Алиса Михайловна
Компания Pointlane, Москва, ведущий специалист отдела ИБ
alisa.koreneva@gmail.com

Криптология – наука, которая еще совсем недавно была открыта только спецслужбам, в наши дни доступна для изучения каждому человеку, имеющему к ней интерес. Возможности криптологии широко используются во многих современных приложениях – шифрование личных данных на носителях и при передаче информации по каналам связи, криптовалюта, системы аутентификации, сертификаты для организации доверенной переписки по электронной почте. Не удивительно, что интерес молодых специалистов к данной науке растет. В настоящее время конференции по криптологии ежегодно проходят в Европе, Америке, Азии и России. В 2012 году мне довелось выступить с докладами на международной конференции Eurocrypt (Англия, Кембридж) и на российской конференции Sibecrypt (Иркутск) в рамках темы научной работы «Криптографические свойства блочных шифров регистрового типа, построенных на основе обобщения раундовой функции Фейстеля» [1,2].

Цель научного исследования – развить математический аппарат анализа блочных шифров на основе регистров сдвига произвольной длины, обобщающих шифры Фейстеля. Шифры Фейстеля позволяют обеспечить ряд хороших криптографических свойств, в том числе, инволютивность алгоритма шифрования – полезное технологическое свойство шифрующих подстановок, при котором зашифрование и расшифрование реализуются одним и тем же алгоритмом [3]. Увеличение длины базового регистра позволяет рассчитывать на улучшение некоторых характеристик шифра. Например, использование регистра сдвига большей длины дает возможность увеличить размер входного блока данных без существенного усложнения реализации алгоритма, что актуально для шифрования больших объемов информации, а также предоставляет разработчику богатое множество вариантов при построении раундовой функции и ключевого расписания.

В ходе исследований блочных шифров регистрового типа доказан критерий инволютивности и оценены перемешивающие свойства. В математическом плане исследования относятся в основном к теории графов: получены новые результаты в виде оценок экспонентов и диаметров определенного класса ориентированных графов, моделирующих перемешивание данных регистровыми блочными шифрами [2,4,5].

Результаты исследований были представлены в рамках конференций – европейской и российской. Несмотря на различие в масштабах интересно сравнение этих научных форумов: обе конференции похожи по своей структуре и атмосфере. Но есть и существенные различия, особенно в научных направлениях: работы на Eurocrypt 2012 посвящены математическому аппарату эллиптических кривых, разработке протоколов, анализу асимметричных криптоалгоритмов. Выступление с докладом про симметричные блочные шифры выглядело там довольно необычно, но, тем не менее, было одобрено со стороны председателей и участников конференции.

Участников на Eurocrypt было в десятки раз больше, чем на Sibecrypt. Это во многом связано с тем, что западные ВУЗы широко финансируют участие студентов и аспирантов в подобных мероприятиях, чем мотивируют молодых людей к научной деятельности. Также в рамках Eurocrypt состоялись интересные личные знакомства с видными учеными: У. Диффи, Б. Пренелем, А. Шамиром и др.

На Sibecrypt 2012 доклад также был одобрен председателем Оргкомитета. Научная проблематика докладов, представленных на Sibecrypt, была в меньшей степени связана с развитием асимметричной криптографии или ее математического аппарата. Однако на конференции выступил молодой ученый из Канады (российского происхождения), что можно расценить как наличие интереса к российской криптографической конференции. Благодаря прекрасным способностям организаторов и крайне дружественной обстановке пребывание на Sibecrypt было очень приятным. Российскую конференцию во многом отличает по-домашнему теплая атмосфера, а сибирская природа просто несравненна по своей красоте.

Обобщая бесценный личный опыт участия в Eurocrypt и Sibecrypt, стоит отметить, что результатом можно считать совершенствование собственных знаний, знакомство и общение с уникальными людьми, выступление перед крупной аудиторией.

Такого рода опыт доступен каждому из нас – молодых ученых, студентов и аспирантов российских ВУЗов, которые, занимаясь различными исследованиями, успешно развиваются в современных научных направлениях. К сожа-

лению, часто случается, что молодому человеку не хватает времени, терпения или определенных условий, и он перестает заниматься своей научной работой, теряет к ней интерес, расставляет другие приоритеты в жизни. Чтобы избежать больших потерь в научных кадрах, необходимо продумать меры морального и материального стимулирования перспективных молодых ученых со стороны заинтересованных организаций. Сделать это надо пока еще не поздно, пока нашей стране есть чем гордиться.

Студентам и молодым ученым не стоит упускать свой шанс или просто ждать, как проходит время. Все-таки есть возможность проявить себя и продемонстрировать свои личные достижения. Помните, что в научном обществе Вас окружают единомышленники, люди с которыми не трудно завести знакомство и с которыми есть большое количество тем для общения.

Хотелось бы пожелать успехов каждому, кто работает или начинает работать в области научных исследований. Безусловно, это большой человеческий труд, но ведь нет ничего сильнее, чем желание целеустремленного человека. Каждый из нас заслуживает своей личной победы.

Список источников

1. Alisa Koreneva and Vladimir Fomichev One Little Cipher Story [Электронный ресурс]: Rump Session EuroCrypt 2012. – Режим доступа к статье: http://www.cs.bris.ac.uk/eurocrypt2012/Rump/koreneva.pdf

2. А.М. Коренева, В.М. Фомичев. Об одном обобщении блочных шифров Фейстеля // Томский государств. университет. Прикладная дискретная математика, №3 (17), 2012. – С. 34-40.

3. Фомичев В.М. Методы дискретной математики в криптологии. - М.: Диалог-МИФИ, 2010. – 424 с.

4. Коренева А.М. Систематизация теоретико-графовых моделей в криптологии // М.: НИЯУ МИФИ. Безопасность информационных технологий. – 2011. – №3. – С. 47-49.

5. Коренева А.М. Применение теоретико-графового подхода для определения значения экспонента матрицы существенной зависимости // М.: НИЯУ МИФИ. Безопасность информационных технологий. – 2011. –№4. – С. 126-129.