где a – исходный информационный объект; $/i_k/$ – множество информационных каналов распределения информации мощности n; $/p_j/$ – множество физических каналов передачи информации мощности m.

$method(/i_k/\rightarrow/p_j/)$ – способ распределения информационных каналов по физическим каналам.

Для модели (II.11.1) справедлив общий протокол функционирования:

Начало

A: $a\uparrow si_4(t, t_0, t_{00})$; $f(a) \rightarrow /i_k a_k/\ si_4(t, t_1, t_2)$; $method(/i_k/ \rightarrow /p_j/) \rightarrow (/ia_k/\rightarrow/pa_j/\ si_4(t, t_3, t_4)) \rightarrow$ B

B: $method^{-1}(/i_k/\rightarrow/p_j/) \rightarrow (/pa_j/\rightarrow/ia_k/\ si_4(t, t_5, t_6)) \rightarrow f(a)$; $a = f^{-1}(/ia_k/\ si_4(t, t_7, t_8)$

Конец

Здесь

$f(a) \rightarrow /i_k a_k/\ si_4(t, t_1, t_2)$ – процесс шифрования и разделения информации на множество информационных каналов;

$/ia_k/\rightarrow/pa_k/\ si_4(t, t_3, t_4)$ – процесс распределения множества информационных каналов по множеству физических каналов;

$si_4(t, t_1, t_2)$ – селектирующая функция интервала [3].

Причем в зависимости от методов преобразования информации справедливо неравенство

$$L(a) \le \sum_k L(i_k). \qquad \textbf{(2)}$$

где L – длина информации в некоторых единицах.

Соотношение (2) подразумевает разбиение информации на информационные каналы и распределение информационных каналов по физическим каналам передачи. Эти два действия будут называться манипулированием информацией. В общем случае, во времени любой информационный канал может подвергаться вторичному преобразованию (1), используя новые физические каналы.

Таким образом, представление (1) может генерировать большое число вариантов многоканальных информационных систем с временной координатой t, варьируя количеством информационных и физических каналов.

3 Модели систем $S_{m+n+1}s_{m+n+1}$ (m – количество физических каналов; n – количество информационных каналов)

Рассмотрены некоторые варианты построения систем: S_{2+3+1}; S_{2+4+1}; S_{4+4+1} и ряд других.

Построение таких систем нашло применение в массовых технологиях современного рынка: LABEL, LABEL DOC (защита интеллектуальной и материальной собственности), SEMAIL (двухканальная электронная почта).

Литература:

1. Мищенко, В.А. Ущербные тексты и многоканальная криптография / В.А. Мищенко, Ю.В. Виланский. – Минск: Энциклопедикс, 2007. – 291 с.

2. Мищенко, В.А. Криптографический алгоритм MV2 / В.А. Мищенко, Ю.В. Виланский, В.В. Лепин. – Минск: Энциклопедикс, 2007. – 177 с.

3. Мищенко, В.А. Теория селектирующих функций в практических приложениях / В.А. Мищенко. – Минск: Медисонт, 2012. – 247 с.

О СОВЕРШЕННЫХ МОДУЛЯРНЫХ СХЕМАХ РАЗДЕЛЕНИЯ СЕКРЕТА

Т.В. Галибус, Г.В. Матвеев,
БГУ, г. Минск

Разделение секрета является широко используемым криптографическим примитивом. Схема модулярного разделения секрета, предложенная Миньоттом, оказалась несовершенной, т.е. частичные секреты (ключи) участников дают возможность получить некоторую информацию о секрете, даже если группа участников не является полномочной, т.е. не имеет доступа к конфиденциальной информации. Для устранения указанного недостатка Асмут и Блюм предложили усовершенствование исходного модулярного подхода, которое затем было исследовано Пренелем и другими авторами, с целью качественного улучшения модулярных пороговых схем, построенных в кольце целых чисел. Напомним, что семейство подмножеств произвольного множества участников P называется структурой доступа, если оно обладает свойством монотонности, т.е.

$$A \in \Gamma,\ A \subset B \subset P \Rightarrow B \in \Gamma.$$

Реализацией структуры доступа или схемой разделения секрета называется такой алгоритм, который позволяет вычислить некоторый секрет лишь группам участников, образующих подмножества из множества P.

Принципиально иной подход был предложен нами в работе [1]. Он заключается в замене кольца целых чисел на кольцо многочленов от одной переменной $F_q[x]$ над конечным полем. Оказалось, что в этом кольце можно реализовать не только совершенно, но даже идеально любую пороговую структуру доступа. Сразу же возникла задача об обобщении этого результата на случай кольца многочленов от многих переменных $F_q[x_1, x_2, \ldots, x_n]$. В этой связи, в работе [2] было сформулировано условие на модули участников совершенной схемы.

В работе [3] было показано, что для совершенной реализации общих структур доступа нужны специальные идеалы $I_1, I_2, \ldots, I_k$ в кольце $F_q[x_1, x_2, \ldots, x_n]$. Они были названы равноостаточными, потому что должны удовлетворять условию:

$$RP(I_{i_1} I_{i_2} \ldots I_{i_m}) = RP(I_{j_1} I_{j_2} \ldots I_{j_m}),$$

где $i_1, i_2, \ldots, i_m$; $j_1, j_2, \ldots, j_m$ – произвольные m-выборки из 1, 2, ..., k, а RP означает множество приведенных мономов.

К настоящему времени равноостаточные идеалы удалось построить лишь для обратного лексикографического упорядочения.

Литература:

1. Galibus, T. Some structural and security properties of the modular secret sharing / T. Galibus, G. Matveev, N. Shenets // SYNASC'08. – California: IEEE Comp. Soc. CPC, 2009. – P. 197–200.

2. Шенец, Н.Н. Об информационном уровне модулярных схем разделения секрета / Н.Н. Шенец // Докл. Нац. акад. наук Беларуси. Сер. физ.-мат. наук. – 2010. – Т. 54, №6. – С. 9–12.

3. Галибус, Т.В. Идеалы симметрических отношений и разделение секрета / Т.В. Галибус // Вестн. Белорус. гос. ун-та. Сер. 1, Физика. Математика. Информатика. – 2011. – № 2. – С. 141–143.

СИСТЕМА МАРКИРОВКИ И КОНТРОЛЯ ДВИЖЕНИЯ МАТЕРИАЛЬНЫХ ОБЪЕКТОВ НА ОСНОВЕ АЛГОРИТМОВ КРИПТОГРАФИЧЕСКОГО РАЗБИЕНИЯ СЕКРЕТА

В.В. Захаров,
Институт современных знаний имени А.М. Широкова

Массовый поток контрафактных товаров на мировом рынке является вызовом для международных организаций, союзов и отдельных государств. Объем контрафакта в отдельных отраслях сравним с объемом легального производства, а зачастую и превышает его, что ведет к существенным потерям для бюджета государства.

Всемирная таможенная организация (ВТО) и международная торговая палата (МТП) по данным 2012 года, считают, что подделки ежегодно вынимают около 600 млрд евро из мировой экономики, что эквивалентно потере оригинальными товарами по всему миру примерно 5–7 % рынка. Ожидается, что к 2015 году эта сумма достигнет 1,7 трлн долл. США.

Однако, если подделка одежды, бытовой техники и других товаров народного потребления может привести только к потере денег и (или) времени потребителя, то подделка лекарств несет угрозу здоровью и жизни покупателя.

До сих пор меры по борьбе с поддельными лекарствами включали: меры, принимаемые регулятивными органами в области лекарств, и инициативы по сотрудничеству между различными органами правопорядка; нанесение простых, легко интерпретируемых и недорогих маркеров подлинности; координацию на международном уровне надзора за поддельными и некачественными лекарствами и просвещение пациентов и работников здравоохранения.

В настоящее время некоторые страны уполномочивают компании подтверждать подлинность их продукции путем создания «родословной», которая заверяет происхождение лекарства и дальнейшее обращение с ним.

Управление США по контролю качества пищевых продуктов и лекарственных препаратов рекомендовало фармацевтическим компаниям перейти к использованию технологии радиочастотной идентификации (РЧИ) для лучшего отслеживания лекарств. Некоторые фармацевтические компании экспериментально применяют РЧИ и оптически изменяющиеся устройства или, по крайней мере, используют штрих-коды или другие технологии, такие как веб-порталы, которые помогают отслеживать и идентифицировать лекарства.

Используют голограммы, чернила, изменяющие цвет, и водяные знаки, которые способствуют подтверждению подлинности упаковок и таблеток. Экспериментируют с использованием чернил и красителей, предлагают для некоторых продуктов специальную упаковочную пленку в целях предотвращения подделок.

Однако такой подход к применению современных средств защиты, на первый взгляд, позволяющих отличить подделку от оригинала, на самом деле лишь увеличивает время изготовления подделки и стоимость единовременных затрат преступника на приобретение специального оборудования и материалов, и, следовательно, уменьшает вероятность подделки, но незначительно.

Возможным решением этой проблемы является создание системы, в которой проверка маркировки (ярлыка) производится удаленно, непосредственно у производителя (или у его доверенного представителя), а результат поступает пользователю по каналам связи.

Уникальность ярлыка, монтируемого на товар, является необходимым требованием обеспечения возможности дистанционной проверки. Действительно, современный опыт показывает, что для современного промышленного «пирата», осуществляющего массовое производство поддельного товара, не существует препятствий для воспроизведения любого массового, не являющегося уникальным защитного элемента. Одной из возможных компрометаций систем с обратной связью является продажа партии подделок до начала продажи подлинного товара. Для такой операции злоумышленник должен иметь возможность предвидеть проверочные значения, наносимые на ярлык. Соответственно, для реализации надежной системы проверки с обратной связью с производителем необходимо для каждой единицы товара обеспечить уникальные, непредсказуемые проверочные данные. Если товар массовый и не дорогой, то необходимо также обеспечить дешевизну ярлыка, содержащего такие проверочные данные. Кроме того, необходимо иметь недорогие, достаточно надежные устройства для считывания этих данных для ввода в систему. Одним из самых дешевых и распространенных носителей иденти-