Для борьбы с сетевыми атаками используются персональные сетевые экраны. Наиболее известные и зарекомендовавшие себя продукты:

Outpost Firewall; KIS; Jetico Personal Firewall; Norton Personal Firewall; McAfee Firewall; Zone Alarm; Kerio WinRoute Firewall (относится именно к персональным);

Из пакетных сетевых экранов можно отметить Microsoft ISA (Internet Security and Acceleration Server).

Заключение

Интернет-преступность становится еще более сложной и продуманной. Это является результатом консолидации расширяющихся сетевых возможностей и социально-экономических факторов, таких, как экономическое развитие и отсутствие ИТ-занятости. Компьютерные преступники, избегают проблем с законом в тех странах, которые претерпевают серьезные политические проблемы и проблемы безопасности. Очевидно, что проблема надзора за информационными потоками в виртуальном пространстве уже назрела и требует своего решения. В противном случае в ближайшие годы мировому сообществу грозит «шквал» информационных атак, несанкционированных рассылок и даже предполагаются массовые «кибертерракты» как на государственные, так и на корпоративные сети.

Надійшла 16.11.2007р.

УДК 621.391

Дудыкевич В.Б., Томашевский Б.П.

ИССЛЕДОВАНИЕ НЕСИММЕТРИЧНЫХ КРИПТОСИСТЕМ НА АЛГЕБРАИЧЕСКИХ КОДАХ ДЛЯ КАНАЛОВ С АВТОМАТИЧЕСКИМ ПЕРЕСПРОСОМ

Введение

Обеспечение конфиденциальности и целостности передаваемых данных является одной из важнейших задач, стоящих при обмене информации между пользователями. Для ее обеспечения наиболее эффективными являются криптографические методы.

Проведенный анализ [1 - 8] показал, что перспективным направлением в развитии несимметричных криптоалгоритмов для обеспечения конфиденциальности и целостности данных является применение криптосистем с быстрыми (алгебраическими) алгоритмами декодирования, функционирующими в режиме маскирования кодовых слов под случайную последовательность. При этом дешифрование информации для неуполномоченного пользователя (несанкционированный доступ к информационной части сообщения) является NP-полной задачей - декодирование случайного кода. Уполномоченный пользователь, владеющий секретным ключом, расшифровует полученную последовательность быстрыми алгоритмами за полиномиальное время. Такие криптосистемы позволяют, интегрировано обеспечивать защиту и помехоустойчивость информационной части данных в каналах с прямым исправлением ошибок [5-8]. В тоже время большая часть модемных протоколов коррекции ошибок функционирует в режиме автоматического переспроса. Таким образом, актуальным направлением исследований является создание несимметричных кодовых криптосистем с быстрыми алгоритмами шифрования и расшифрования данных для каналов с автоматическим переспросом [7, 8].

Несимметричная кодовая криптосистема Нидеррайтера

В работе [1] впервые предложена кодовая криптосистема, основанная на маскировании проверочной матрицы алгебраического блокового кода. Основное достоинство несимметричной криптосистемы Нидеррайтера состоит в высокой скорости

преобразования информации (относительная скорость кодирования близка к 1). Рассмотрим особенности построения, алгоритмы шифрования и расшифрования данных, а также аппаратную реализацию устройств формирования и расшифрования кодограмм криптосистемы Нидеррайтера.

Пусть H проверочная матрица линейного $(n, к, d)$ кода над $GF(q)$ с полиномиальной сложностью декодирования. Пусть X - невырожденная $r \times r$ -матрица над $GF(q)$, D - диагональная матрица с ненулевыми элементами на диагонали, P - перестановочная матрица размера $n \times n$. Открытым ключом в криптосистеме Нидеррайтера является матрица $H_x = X \cdot H \cdot P \cdot D$ секретным (закрытым) ключом являются матрицы X, P, D. Закрытая информация (кодограмма) S_x представляет собой вектор длины $r = n - к$ и вычисляется по правилу

$$S_x = e \cdot H^T_{X9} \qquad (1)$$

где вектор e - вектор длины n и веса $\le t$, который несет конфиденциальную информацию (информационное сообщение, подлежащее закрытию).

Уполномоченный пользователь (имеющий секретный ключ) находит одно из q^k решений выражения $S_x = c^*_x \cdot H^T_x$ Найденное решение - суть кодовое слово с ошибками $c^*_x = i \cdot G_x + e$. Далее, уполномоченный пользователь строит вектор $\overline{c}^* = c^*_x \cdot D^{-1} \cdot P^{-1}$, декодирует полученное слово и вычисляет кодовое слово $c' = i' \cdot G$, а затем и вектор ошибок $e' = \overline{c}^* - c'$. На последнем шаге производится вычисление вектора $e = e' \cdot P \cdot D$ который несет конфиденциальную информацию.

Таким образом, в кодовой криптосистеме Нидеррайтера основным средством маскировки линейного $(n, к, d)$ кода являются матрицы X, P, D. В работах [2, 3] показано, что перспективным направлением считается использование криптосистемы на алгеброгеометрических кодах (АГК) [3-5].

Недвоичные алгебраические блоковые коды, построенные по алгебраическим кривым (алгеброгеометрические коды) обладают хорошими асимптотическими свойствами. Доказано, что при большой длине эти коды лежат выше границы Варшамова-Гилберта [2-5].

Зафиксируем конечное поле $GF(q)$. Пусть X гладкая проективная алгебраическая кривая в проективном пространстве P^n над $GF(q)$, $g = g(X)$ - род кривой, $X(GF(q))$ - множество ее точек над конечным полем, $N = X(GF(q))$ - их число. Пусть С - класс дивизоров на X степени $a > g - 1$. Тогда C определяет отображение $\varphi : X \to P^{k-1}$, где $k > a - g + 1$. Набор $y_i = \varphi(x_i)$ задает код. Число точек в пересечении $\varphi(X)$ с гиперплоскостью равно a, т.е. $n - d \le a$. Эта конструкция позволяет строить коды с параметрами $к + d \le n - g + 1$, длина n которых меньше либо равна числу точек на кривой X. При $2g < a \le n$ алгеброгеометрический код имеет параметры $(n, a - g + 1, d)$, $d \ge n - a$.

Двойственный к нему код также является алгеброгеометрическим и имеет параметры $(n, n - a + g - 1, d)$, $d^l \ge a - 2g + 2$ [5]. Дадим следующее определение алгеброгеометрического кода.

Определение 1 [6-8]. Пусть X- гладкая проективная алгебраическая кривая в P^n, т.е. совокупность решений однородного неприводимого алгебраического уравнения степени $degX$ с коэффициентами из $GF(q)$, F - однородные одночлены степени $degF$. *Алгеброгеометрический код по кривой X* над $GF(q)$ — это линейный код, состоящий из всех слов $(c_1, c_2, ..., c_n)$ длины $n \le N$, для которых выполняется равенство $d + g - 1$ уравнений

$$\sum_{i=0}^{n-1} c_i F_j(P_i) = 0 \qquad (2)$$

где $c_i \in GF(q)$, $d \geq a - 2g + 2$, $a = degX\, degF$.

Это определение равносильно матричному представлению алгеброгеометрического кода:

$H(c_0, c_1, \ldots, c_{n-1})^T = 0$, где H - проверочная матрица кода

размерности $r \times n, r = n - k = d + g - 2$ $H = \begin{pmatrix} F_0(P_0) & F_0(P_1) & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & F_1(P_{n-1}) \\ F_{r-1}(P_0) & F_{r-1}(P_1) & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,r}$. Схема передачи секретного сообщения от абонента А к абоненту Б в несимметричной кодовой криптосистеме представлена на рис. 1

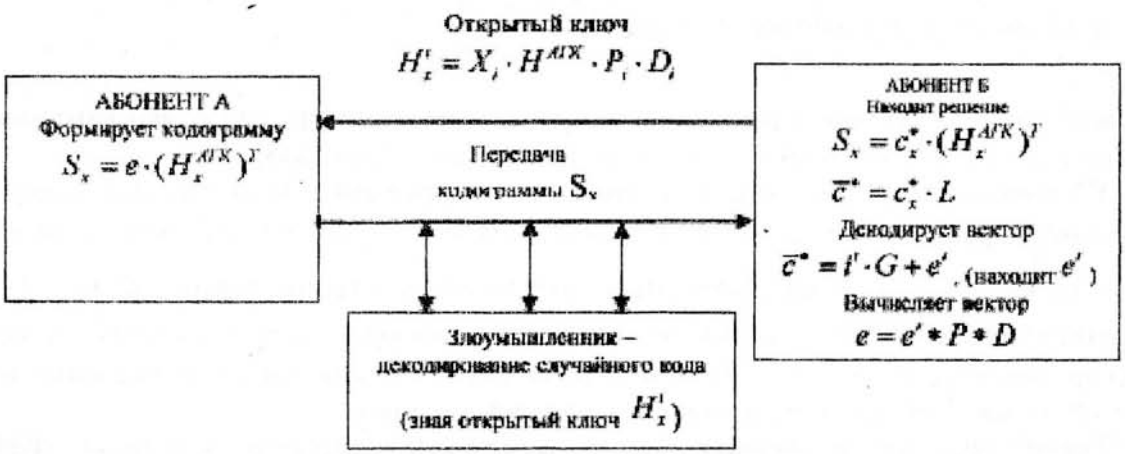

Рис. 1. Схема передачи кодограммы.

Абонент А для отправки секретного сообщения формирует

$$\begin{pmatrix} h_{x0,0} & h_{x0,1} & \cdots & h_{x0,n-1} \\ h_{x1,0} & h_{x1,1} & \cdots & h_{x1,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ h_{xk-1,0} & h_{xk-1,1} & \cdots & h_{xk-1,n-1} \end{pmatrix},$$

криптограмму. $E_j = (S_{x_0}, S_{x_1}, \ldots, S_{x_{n-1}}) = M_j \cdot H'_x = (e_0, e_1, \ldots, e_{n-1}) \cdot$

Ее может сформировать (зашифровать отправляемую информацию) любой пользователь, знающий общедоступный ключ. Секретное сообщение M_j - суть специально подготовленный набор данных, удовлетворяющий следующему ограничению:

$$M_j = (e_0, e_1, \ldots, e_{n-1}), \forall e_j \in GF(q), w(M_j) \leq t = \left[\frac{(d-1)}{2} \right].$$

Таким образом, в формировании сообщения *Mi* участвуют алгоритмы равновесного кодирования, которые, в свою очередь являются алгоритмами избыточного (помехоустойчивого) кодирования. Положим, что контроль ошибок в режиме автоматического переспроса осуществляется на уровне равновесного кодирования. Тогда рассмотренная выше криптосистема позволяет обеспечить комплексную крипто-кодовую защиту передаваемой информации [7].

Рассмотрим алгоритмы формирования и расшифрования кодограммы. Закрытая информация (кодограмма) в несимметричной криптосистеме Нидеррайтера с алгеброгеометрическими кодами представляет собой вектор длины n и вычисляется по правилу (1). Т.е. кодограмма формируется путем вычисления синдрома, соответствующего случайным образом сформированному вектору ошибок e, вес которого не превышает исправляющую способность эллиптического кода. При вычислении значения синдрома

используется проверочная матрица $H_x^{АГК}$. Схема алгоритма формирования кодограммы представлена на рис. 2.

Алгоритм формирования кодограммы представим в виде последовательности следующих шагов:

шаг 1. Ввод информации, подлежащей кодированию. Ввод открытого ключа$H_x^{АГК}$

шаг 2. Формирование вектора ошибок *e*, вес которого не превышает $<t$ - справляющую способность алгеброгеометрического кода.

шаг 3. Формирование кодограммы $S_x = e*(H_x^{АГК})^T$.

Для декодирования кодограммы в криптосистеме Нидеррайтера не обходимо найти одно из возможных решений уравнения $S_x = c_x*(H_x^{АГК})^T$. Затем необходимо снять действие диагональной *D* и перестановочной *P* матриц и декодировать полученный вектор. В результате декодирования нужно выделить вектор ошибок *e'* преобразовав его получить искомую информацию в виде вектора *e* (см. рис. 1). Схема алгоритма снятия кодограммы (раскодирования информации) представлена на рис. 3

Алгоритм декодирования кодограммы представим в виде последовательности следующих шагов:

шаг 1. Ввод кодограммы S_x, подлежащей декодированию. Ввод закрытого ключа - матрицы *X, P, D.*

шаг 2. Нахождение одного из возможных решений уравнения:

$$\overline{c}_x^* = c_x^* \cdot (H_x^{АГК})^T.$$

Рис. 2. Схема алгоритма формирования кодограммы

шаг 3. Снятие действия диагональной и перестановочной матриц:

$$\overline{c}^{\bullet} = c_x^{\bullet} \cdot D^{-1} \cdot P^{-1}.$$

шаг 4. Декодирование вектора $\overline{c}^{\bullet}$. Формирование вектора e\ шаг 5. Преобразование вектора e': $e = e' \cdot P \cdot D$. Формирование искомого информационного вектора e.

Для обеспечения конфиденциальности и целостности передаваемых данных с использованием несимметричной криптосистемы Нидеррайтера на алгеброгеометрических кодах разработаны аппаратные средства формирования и раскодирования кодограмм. Устройство формирования кодограммы предваряет следующие операции. Ключевые данные (КД) поступают на вход устройства ввода ключевых данных (УВКД).

Введенные КД преобразуются в коэффициенты $a_1,...,a_n$ однородного многочлена, задающего вид алгебраической кривой над $GF(q)$, $\forall a_i \in GF(q)$. Коэффициенты $a_1,...,a_n$ поступают на вход устройства формирования генераторной матрицы (УФГМ) алгеброгеометрического кода. В УФГМ вычисляются точки алгебраической кривой и по значениям генераторных функций $F_0,...,\ F_{M-1}$ в точках кривой формируется генераторная матрица кода. Функции $F_0,...,\ F_{M-1}$ формируются в устройстве формирования генераторных функций (УФГФ). Структурная схема устройства, основанного на использовании кодера алгеброгеометрических кодов, представлена на рис. 4. Формирование кодограммы осуществляется следующим образом. Информационная последовательность (ИП) поступает на вход кодера равновесного кодирования (КРК), где информационная последовательность преобразуется в равновесный код, в котором информационная последовательность $I_0,...,I_{k-1}$ преобразуется в информационную последовательность равновесного кодирования (ИПРК) $I_0^{\bullet},...,I_{n-1}^{\bullet}$ ИПРК $I_0^{\bullet},...,I_{n-1}^{\bullet}$ поступает на устройство ввода информации (УВИ), где разбивается на блоки по κ символов из $GF(q)$.

Информационные блоки $I_0^{\bullet},...,I_{n-1}^{\bullet}$ поступают на вход устройства формирования кодовых слов (УФКС). В УФКС по считанным из УФГМ элементам генераторной матрицы и поступившему информационному блоку $I_0^{\bullet},...,I_{n-1}^{\bullet}$ формируется кодовое слово алгеброгеометрического кода. В устройстве наложения вектора ошибок (УНВО) к сформированному кодовому слову $c_0,...,c_{n-1}$ добавляется случайный вектор ошибок $c_0,...,c_{n-1}$ в результате чего формируется кодограмма $c_0^{\bullet},...,c_{n-1}^{\bullet}$.

Декодирование кодограмм предваряется операцией ввода ключевых данных в блок УВКД и формированием генераторной матрицы алгеброгеометрического кода в блоках УФГФ и УФГМ. Структурная схема устройства декодирования кодограммы представлена на рис. 5.

Декодирование осуществляется следующим образом. Кодограмма (К) поступает на вход устройства ввода кодограмм (УВК), откуда поступает на вход устройства формирования синдрома (УФС). В УФС формируется синдром $S_0,...,S_{r-1}$ для введенной последовательности (кодограммы). Вычисленный синдром поступает на вход устройства декодирования (УД), где введенная кодограмма декодируется, т.е. выделяется вектор ошибки $e_0,...,e_{n-1}$. С выхода УД считывается кодовое слово без ошибок $c_0,...,c_{n-1}$ и поступает на вход устройства выделения информации, где из кодового слова выделяется информационная последовательность равновесного кодирования $I_0^{\bullet},...,I_{n-1}^{\bullet}$ после чего, с помощью декодера равновесного кодирования (ДРК) ИПРК преобразовывается в информационную последовательность $I_0,...,I_{k-1}$.

Рис. 3. Схема алгоритма декодирования кодограммы

Рис. 4. Структурная схема устройства формирования кодограммы

. Устройство согласования (УС) предназначено для согласования работы УВК, ДРК, УД и УВДИ. Таким образом, разработанный подход как совокупность установленных процедур и правил позволяет обеспечить конфиденциальность и целостность при обмене сообщениями между абонентами информационного обмена с использованием кодовых криптосистем на алгеброгеометрических кодах в -каналах с автоматическим переспросом.

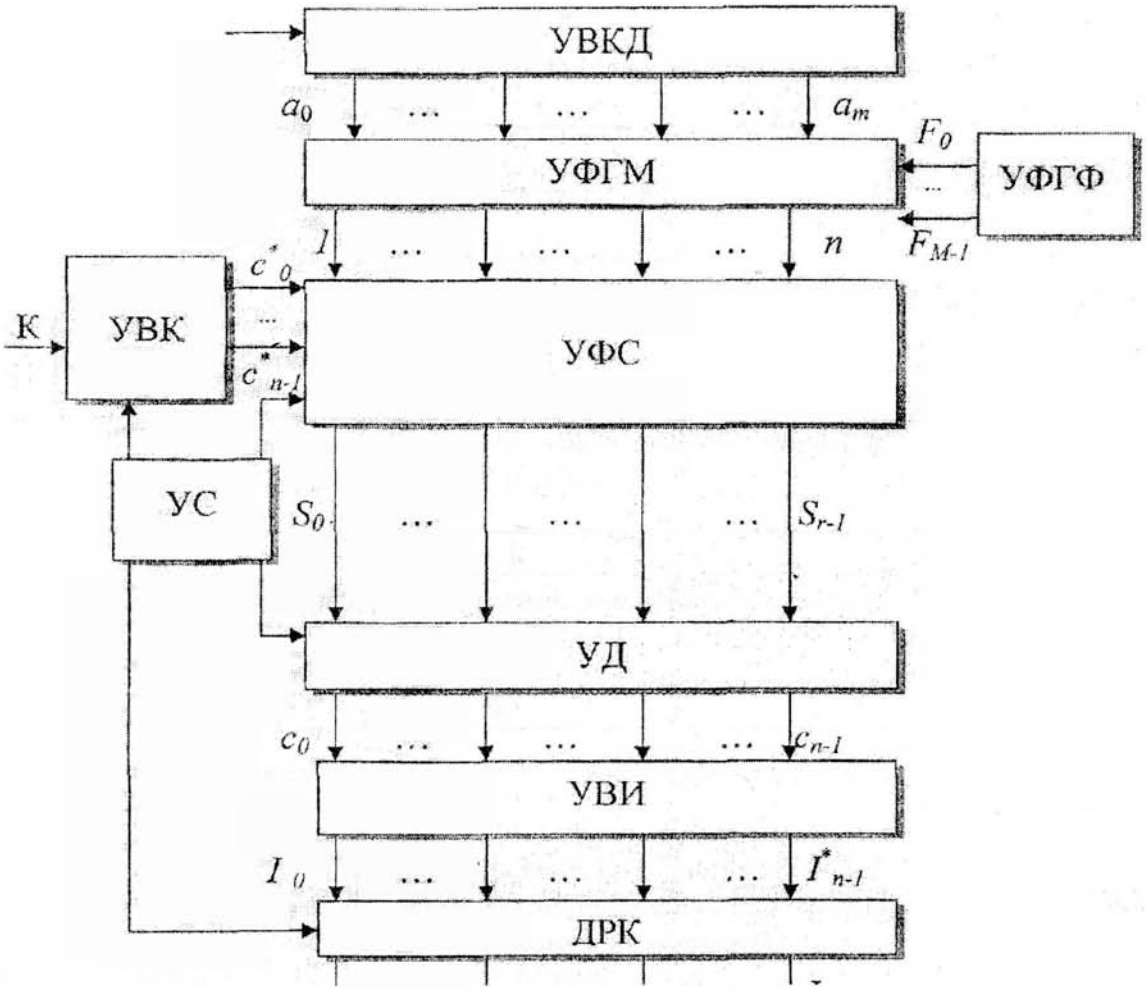

Рис.5. Структурная схема устройства декодирования кодограммы

Выводы

В ходе проведенных исследований рассмотрены криптосистемы, построенные с использованием алгебраических блоковых кодов, стойкость которых обосновывается сложностью декодирования случайного кода. Предложенные алгоритмы формирования и расшифрования информационных данных, их аппаратная реализация криптосистемы Нидеррайтера на алгеброгеометрических кодах, функционирующей в режиме маскирования кодовых слов под случайную последовательность, позволяют обеспечить безопасность и достоверность передачи данных в каналах с автоматическим переспросом.

Список литературы

1. *H. Niederreiter.* Knapsack-Type Cryptosystems and Algebraic Coding Theory. // Probl. Control and Inform. Theoty. - 1986. - V.15. -P. 19-34.

2. *Сидельников В.М., Шестаков С.О.* О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона.//Дискретная математика.-1992.-ТА№3.-С.57-63.

3. *Сидельников В.М.* Криптография и теория кодирования. Материалы конференции «Московский университет и развитие криптографии в России», МГУ. - 2002. - 22с.

4. *Гоппа В.Д.* Коды и информация // Успехи математических наук, 1984. -Т.30, вып. 1(235).-С. 77-120.

5. *Кузнецов А.А., Евсеев С.П., Томашевский Б.П., Жмурко Ю.И.* Исследование протоколов и механизмов защиты информации в компьютерных системах и сетях. // Збірник наукових праць ХУ ПС. - Харків: ХУПС. - 2007. - Вил. 2(14).-

С. 102-111.

6. Кузнецов А.А., Евсеев СП. Разработка теоретико-кодовых схем с использованием эллиптических кодов. // Системи обробки шформацп. - Харюв: ХВУ. -2004 - Вип. 5. - С 127-132.

7. Евсеев СП. Несимметричные криптосистемы на ЭК для каналов с автоматическим переспросом. // Збірник наукових праць ХУ ПС. - Харків: ХУПС. - 2007. - Вип. 5 (63). - С 134-137.

8. Евсеев СП. Криптографическое преобразование информации в кодовых криптосистемах на эллиптических кодах для каналов с автоматическим переспросом. // Збірник наукових праць ХУ ПС - Харків: ХУПС. - 2007. - Вип. 8 (66).-С. 29-32.

Надійшла 3.12.2007р.

УДК 004.7.056.5

Нетров А.С., Минин А.В.

ОСОБЕННОСТИ ОПТИМИЗАЦИИ СТЕГОАЛГОРИТМОВ ДЛЯ ВИДЕОКОНТЕЙНЕРА

Прогресс в области компьютерной стеганографии позволяет сильно изменить существующие подходы к проблеме информационной безопасности. В связи с этим актуальной является задача построения цифровых контейнеров, в которых можно скрывать данные, не подлежащие огласке. Каждый месяц появляются новые стегоалгоритмы и алгоритмы стегоанализа. На данном этапе основное внимание в стеганографии уделено цифровым статическим изображениям и цифровым аудиофайлам. Методы стеганографии для встраивания скрытой информации в видеофайлы в настоящее время пока еще находятся на стадии исследований и носят фрагментарный характер.

Информационная последовательность, в которую встраивается сообщение, принято называть контейнером. В нашем случае это видеоконтейнер. Пока видеофайл не попал в стегокодер - это пустой видеоконтейнер, после стегокодера - заполненный видеоконтейнер, или стегофайл. Стегофайл должен быть визуально неотличим от пустого видеоконтейнера. Различают два основных типа видеоконтейнеров: потоковый и фиксированный.

Потоковый видеоконтейнер представляет собой непрерывно следующую последовательность бит. Сообщение вкладывается в него в реальном масштабе времени, так что стегокодеру заранее неизвестно, поместится все сообщение в видеоконтейнер или нет. В один видеоконтейнер большого размера может быть встроено и несколько сообщений. Интервалы между встраиваемыми битами определяются генератором псевдослучайной последовательности с равномерным распределением интервалов между отсчетами. Основная трудность заключается в осуществлении синхронизации, определении начала и конца последовательности. Если в данных контейнера имеются биты синхронизации, заголовки пакетов и т.д., то скрываемая информация может располагаться сразу после них. Трудность обеспечения синхронизации превращается в достоинство с точки зрения обеспечения скрытности передачи. На практике востребованность стегоалоритмов для работы с потоковым видеоконтейнером очевидна: представьте себе, например, стегоприставку к обычному компьютеру или мобильному телефону с встроенной веб-камерой. Вы проводите веб-конференцию или видеозвонок, разговариваете на отвлеченные темы, а параллельно передаете секретную информацию. Не удивительно, что работ в этом направлении практически не встречается.