(например, смысловая обработка текстов, графики и т. п.).

Шаг 3. Сглаживание образа одного класса. Поскольку образ представляет собой объединение гармоник, его можно функционально описать огибающей. Процесс сглаживания огибающей должен быть регулируемым. Вначале возможно применить сглаживание Фридмана [3], впоследствии качество сглаживания доводится до нуля (нет сглаживания).

Шаг 4. Повторять шаги 2–3 для объектов одного класса.

Шаг 5. Анализ неоднородности образов одного класса. Регулируемым параметром в данной процедуре является порог близости сглаженных образов огибающих друг к другу. На выходе шага имеем множество кластеров, составляющих данный класс.

Шаг 6. Повторять шаги 2–5 для всех классов выдвинутой классификации.

Шаг 7. Формирование кластерного пространства. Построение пространства начинается с вычисления центрального кластера и упорядочивания кластеров в порядке убывания их взаимосвязи. На этом этапе выбираются 3 любых базовых кластера и относительно них, в полярной системе координат, пересчитывается пространственная формула (метод триангуляции). Использование локальных пространственных формул имеет свойство самоорганизации: при позиционировании триангуляционных лучей в пустоте принимается решение о новом классе классификации (для шага 8).

Шаг 8. Изменение или уточнение классификации. В первом случае повторяются шаги 1–7 для нового классообразования. Во втором случае, в зависимости от целевого признака анализа, корректируются элементы шага 2, 3, 5 (для каждого шага они описаны как изменяющиеся впоследствии). Повторять шаги 1–8 до тех пор, пока качество сглаживания не равно нулю (шаг 3).

Поскольку процедура механизма самоорганизации предполагает использование сглаживающих методов, данная реализация использует качество общности объекта.

IV Выводы

В работе рассмотрена возможность реализации механизмов разграничения доступа и саморазвития операционной системы, построенной на принципах распознавания образов. Показано, что данные механизмы используют диаметрально противоположные характеристики самого образа, точности и общности. Остальные механизмы, не рассмотренные в материале статьи, располагаются в пределах данного диапазона характеристик. Временные рамки описанных механизмов зависят от вычислительных ресурсов субъектов.

Литература: 1. Шелест М. Є., Манухін О. В. Основи побудови автоматизованої системи оперативного аналізу інформації у телекомунікаційних мережах // Спеціальні телекомунікаційні системи та захист інформації, вип. № 1. – К.: СБУ, 2001. – с. 77–83. 2. Розробка технології обліку файлів на об'єктах обчислювальної техніки: Звіт про НДР (заключний) / Військовий інститут НТУУ "КПІ". – № держреєстрації 0101U00798. – К., 2001. – 80 с. 3. Friedman J. H. A variable span scatterplot smoother // Laboratory for Computational Statistics, Stanford University Technical Report, 1984, № 5.

УДК 681.3

ВОЗМОЖНОСТЬ СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ В КРИПТОПРОТОКОЛАХ, ОСНОВАННЫХ НА СВОЙСТВАХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Владислав Мухачев, Михаил Шелест
Служба безопасности Украины

Анотація: **Показано можливість впровадження прихованих каналів передачі інформації у цифровий підпис та протокол пересилки ключів, що побудовані на властивостях еліптичних кривих.**
Summary: **There is shown the possibility of embedding subliminal channels in digital signatures and key transport mechanisms based on elliptic curves.**
Ключові слова: **Прихований канал, стеганографія, цифровий підпис, криптопротокол, еліптична крива, кофактор.**

I Введение

В настоящее время для передачи данных по каналам связи общего пользования все большее применение находят стеганографические методы защиты информации, т. е. методы, основанные на принципах

организации скрытых каналов связи. При реализации подобных методов используются процедуры, естественным образом комбинирующие стеганографию и криптографический подход к защите информации (например, предварительное зашифрование, использование для передачи данных ключевых элементов криптопреобразований либо применение переменных стеганопараметров). Очевидно, скрыть факт передачи сообщения с помощью специфической программы достаточно сложно. Например, программное средство можно идентифицировать по оформлению данных либо другим явным признакам, таким как передача аналогичной информации несколько раз и т. п.

Поскольку для доказательства использования стеганографических процедур необходимо анализировать программу, а не передаваемую информацию, то задача еще более облегчается. Действительно, при доказанном использовании стеганопрограммы, предположение о применении ее в последующем для скрытой передачи информации достаточно правдоподобно. Очевидно, что это приводит к возможности целенаправленного анализа соответствующих данных, т. е. вероятность раскрытия защищенной информации возрастает. Таким образом, методы, обеспечивающие маскировку применения средств стеганографии, в частности, стеганопрограмм, могут иметь практическое значение. С другой стороны, распространение средств стеганографии предоставляет возможность внедрения скрытых каналов передачи информации в действующую криптосистему. Это может привести к утечке ключевых данных и разрушить систему защиты информации. Следовательно, выявление возможных скрытых каналов в реально действующих системах защиты информации представляется актуальным.

Необходимо признать, что сложившиеся в настоящее время условия позволяют существенно снизить вероятность выявления факта применения стеганопрограмм и, кроме того, аутентично передать скрытую информацию между абонентами линии связи. Подобный вывод основан на следующих соображениях:

- во-первых, очевидно, что скрыть факт использования специфической программы можно с помощью маскировки под другую программу, алгоритм которой используется часто и повсеместно другими пользователями;
- во-вторых, такая возможность реальна, поскольку указанным требованиям соответствуют, например, различные программы наложения цифровой подписи; кроме того, не исключено, что в Украине будет широко распространен национальный стандарт на цифровую подпись (типа Эль Гамаля);
- в-третьих, различные криптопротоколы для согласования и передачи ключей, а также механизмы цифровой подписи (в т. ч. и подписи типа Эль Гамаля) предлагаются и планируются к использованию в ряде международных стандартов (ISO/IEC 9796, ISO/IEC 14888, ISO/IEC 15946).

Использование криптопротоколов для скрытой передачи информации является естественным в том смысле, что скрытая информация маскируется одновременным решением задачи, свойственной данному протоколу. Недостатком такого подхода является короткая длина скрытого сообщения, передаваемого за один сеанс, что обусловлено параметрами цифровой подписи, а также условиями использования секретных ключей для организации скрытого канала связи. Например, цифровая подпись Эль Гамаля, стойкость которой основана на сложности логарифмирования в поле характеристики p, изучалась с точки зрения скрытой передачи данных в работе [1]. Показано, что основные случаи, для которых качество скрытого канала существенно различно, связаны с тем, известен ли секретный ключ подписи каждому из абонентов линии связи или нет. Кроме общих случаев исследовались также конкретные варианты цифровой подписи. В работе [2] рассмотрена схема Онга-Шнорра-Шамира, для которой также показана возможность организации скрытого канала связи.

Поскольку в национальном стандарте предполагается использование криптографической техники, связанной с криптосистемами на эллиптических кривых, то целесообразно рассмотреть аналогичную ситуацию для криптопротоколов подобного типа.

II Исходные данные и постановка задач

Целью данной работы является обоснование возможности организации скрытых каналов в современных средствах криптографической защиты информации.

В настоящее время закончена работа по подготовке к принятию стандарта ISO/IEC 15946, в котором предлагаются механизмы цифровой подписи, согласования и пересылки ключей, основанные на свойствах эллиптических кривых. Многие механизмы, описанные в данном стандарте, построены на основе криптопротоколов, рекомендованных в стандартах ISO/IEC 14888-3, ISO/IEC 11770-3. Следует подчеркнуть, что в стандарте ISO/IEC 14888-3 параметры цифровых подписей типа Эль Гамаля представлены в терминах общего случая коммутативной циклической группы. Там же приводятся конкретные варианты подписей для случая группы точек на эллиптической кривой. Общность достигается использованием т. н. уравнения цифровой подписи вида $Ak+Bd+C=0 \bmod q$, где k – псевдослучайный параметр, d – секретный ключ подписи, q – порядок циклической группы, G – ее порождающий элемент. Для подписи сообщения M, представленной

в виде *(R, C)*, остальные параметры уравнения в произвольном порядке принимают значения *H=Hash(M), R, S*. При этом только *S* заранее неизвестно и определяется из уравнения. Например, эллиптический вариант подписи DSA соответствует выбору *A=S, B=–R, C=–H*.

Мы рассмотрим возможность организации скрытых каналов передачи информации для эллиптических аналогов подобных криптопротоколов. С помощью явного построения покажем, что для соответствующих протоколов возможность внедрения скрытых каналов существует и легко реализуется.

Напомним, что соответствующие криптографические преобразования используют свойства группы точек на эллиптической кривой над полем $F=GF(p^m)$. В группу точек *E=E(F)* на эллиптической кривой над полем *F* входят пары $P=(x,y)\in F\times F$, являющиеся решениями некоторых уравнений [3]. Такие пары называются конечными точками кривой. Например, при $p>3$ уравнение кривой сводится к виду $y^2=f(x)$. Здесь *f(x)* – полином третьей степени с коэффициентами из базового поля *F*, не имеющий кратных корней в алгебраическом замыкании $\overline{F}$.

Множество конечных точек эллиптической кривой расширяется до (абелевой) группы *E*, если присоединить особый элемент, называемый бесконечно удаленной точкой *O*. Порядок (число элементов) группы *E* обозначается через #*E*. Бесконечно удаленная точка является нейтральным элементом группы и не имеет представления в виде пары координат, удовлетворяющих данному уравнению.

Для построения схемы цифровой подписи (ЦП) необходимо выбрать эллиптическую кривую так, чтобы число #*E* содержало простой делитель $n>4\sqrt{p^m}$. Кроме того, необходимо определить точку *G=G(x,y)* на кривой, порядок которой в группе *E* равен *n*. Размер двоичного представления *n* составляет, примерно, 180 – 400 битов [4]. Механизм ЦП использует свойства циклической подгруппы $E(G)\subset E$ с элементами вида $G_0=G$, $G_1=G+G$, $G_2=G+G+G$ и т. д. Если записывать подобное *k*-кратное сложение на кривой в виде *[k]G*, положив *[0]G=0*, то коэффициент *k* можно приводить по модулю *n* и рассматривать выражения вида *[u]P+[v]Q* и *[u]([v]P)*. Операция *[k]G* называется скалярным умножением на *k*.

В эллиптических аналогах, как правило, секретный и открытый ключи подписи представляют собой соответственно псевдослучайное число $d\in[1, n-1]$ и точку на кривой вида *P=[d]G*. Естественно, механизм цифровой подписи использует также псевдослучайный параметр *k*. Подпись представляет собой пару чисел *(R, S)*, которые связаны с координатами точки *[k]G* секретным ключом подписи и друг с другом. Вторая часть подписи *S* зависит от подписываемого сообщения *M*, например, через функцию хэширования *H=H(M)*.

Механизмы пересылки ключей реализуются в ходе обмена данными между абонентами, на основе которого они могли бы безопасным образом построить общие секретные параметры и убедиться в том, что обмен данными не навязан третьим лицом. Иными словами, механизмы должны обеспечивать безопасные криптопротоколы при взаимном недоверии между абонентами. С этой целью в соответствующих протоколах используются т. н. функции генерации производных ключей (*kdf*), а также алгоритм выработки кодов аутентификации сообщений (MAC), который представляет собой аналог хэш-функции с секретным параметром (ключом).

Спецификой эллиптических кривых обусловлено применение преобразования $G\to\pi(G)$ точки на кривой в целое число. Это преобразование является функцией от координат точки *G*, например, хэш-функцией от ее первой координаты. Кроме того, используются дополнительные параметры, связанные с реализацией мер против использования в качестве точки *G* элемента (другой) подгруппы кривой малого порядка. Соответствующая процедура основана на использовании т. н. кофактора *c=#E/n* в качестве дополнительного множителя для точек вида *[k]G* (см. ниже).

В третьем разделе будет показано, что возможности, присущие классическим подписям типа Эль Гамаля, сохраняются и для их аналогов, основанных на эллиптических кривых. Кроме того, будет показано, что использование в механизмах ключевого обмена умножения на кофактор позволяет легко организовать скрытую передачу данных. Эти результаты без труда распространяются на класс криптопротоколов, корректность выполнения которых взаимно однозначно связана с истинностью значения некоторого (несекретного) глобального параметра. Тем не менее, мы будем рассматривать возможность организации скрытого канала для конкретных механизмов цифровой подписи и пересылки ключей.

III Скрытые каналы в цифровой подписи и протоколе пересылки ключей

Рассмотрим, как наиболее простой, механизм наложения цифровой подписи (ECNR), состоящий в следующем.

Пусть, как обычно, *(d,P=dG)* – ключевая пара владельца подписи для криптосистемы на эллиптических кривых, *n* – порядок базовой точки *G*. Выбираем псевдослучайное число $k\in[1, n-1]$ и вычисляем точку $[k]G=(x,y)$ на эллиптической кривой. Перешифровываем значение *H=H(M)* с помощью первой координаты

точки $[k]G$ сложением по модулю n, получаем значение первой части подписи $R=H+x \bmod n$. Вторая часть подписи равна $S=k–dR \bmod n$.

Рассмотрим случай, когда обоим абонентам известен секретный ключ цифровой подписи d. Воспользуемся тем, что в подписях типа Эль Гамаля параметр k, очевидно, может быть определен из S при знании ключа d. Напомним, что, кроме того, при проверке подписи получатель всегда имеет возможность явно получить точку $[k]G$.

Предположим, что между абонентами A и B существует линия связи, по которой передаются сообщения с цифровой подписью. Допустим, что между абонентами согласован некоторый долговременный ключ $K \in GF(n)$. Пусть необходимо передать сообщение $M^* \neq 0$ по скрытому каналу от A к B, обеспечив аутентичность источника.

Сначала абонент A формирует сообщение $M=M^*||r$, где r – псевдослучайное число (размером, скажем, 80 битов) и определяет число k из равенства $M=Kk$ (операции рассматриваются в поле $GF(n)$). Далее A выбирает произвольное сообщение $M_1 \neq 0$, $M_1 \neq M$, вычисляет его цифровую подпись (R, S) и отправляет абоненту B подписанное сообщение.

Абонент B проверяет ЦП, убеждается в аутентичности источника сообщения и, зная ключ d, определяет из S параметр k. Затем, используя ключ K, вычисляет сообщение M.

Использование параметра r связано с необходимостью исключить возможность подписи разных сообщений M_1 с одним и тем же значением k при повторной передаче M^*. В этом случае k и d могут быть определены по двум подписям (для любого механизма ЦП типа Эль Гамаля).

Рассмотрим ситуацию, когда значение d получателю неизвестно. В этом случае, очевидно, для передачи одного бита можно использовать передачу одного сообщения. Действительно, выбирая k псевдослучайным образом, можно добиться того, чтобы очередной бит сообщения M^* совпал, скажем, с последним битом числа $\pi([Kk]G)$. Поскольку при проверке подписи легко вычислить точку $[K][k]G=[Kk]G$, то получатель в состоянии принять бит, переданный по скрытому каналу.

Можно усложнить выбор k, требуя, чтобы очередные несколько битов сообщения M^* совпадали с числом $\pi([Kk]G) \bmod t$ для небольшого простого числа t. Таким образом, преимущество в вычислительной мощности приводит к лучшему качеству скрытого канала.

Покажем теперь возможность организации скрытого канала в механизме пересылки ключей типа Эль Гамаля (Key transport of ElGamal type). Механизм использует кофактор c и дополнительный параметр v. Он обеспечивает однопроходной протокол пересылки ключа K от абонента A к абоненту B и заключается в следующем.

Для аутентификации ключа K абоненты используют алгоритм вычисления кода аутентификации сообщений (MAC). Для этого алгоритма вырабатывается свой псевдослучайный ключ K_1. Кроме того, для перешифровки ключа K формируется блок Z гаммы по модулю два. Ключи K_1 и Z вырабатываются с помощью функции генерации производных ключей (kdf), которая использует значения вторых аргументов, связанные с параметрами пользователей и параметрами алгоритма (MAC).

Пусть для абонентов с идентификаторами A и B ключевые пары для криптосистем на эллиптических кривых соответственно равны (d_1, P_1) и (d_2, P_2).

Абонент A выбирает псевдослучайное число $u \in \{1,\ldots,n-1\}$, вычисляет точку uG и гамму $Z=kdf(\pi(uvcP_2, par1))$. Затем перешифровывает подлежащий пересылке ключ: $D=(A||K) \oplus Z$ и вырабатывает промежуточный ключ $K_1=kdf(\pi(uvcP_2, par2))$.

Поясним роль дополнительных параметров. При выборе $v=c^{-1} \bmod n$ общий секретный параметр не зависит от кофактора и криптопротокол доступен в рамках исходной группы пользователей. Если $v=1$, то криптопротокол доступен только для пользователей, использующих умножение на кофактор. Кроме того, если порядок точки G не равен n, то $[c]G=0$, что позволяет пользователю обнаружить нарушение протокола.

Абонент A использует K_1 для получения кода аутентификации сообщения $\mathrm{MAC}(K_1, D)$ и пересылает абоненту B сообщение $M=D||uG||\mathrm{MAC}(K_1, D)$. Абонент B в состоянии вычислить первый аргумент функции kdf, исходя из секретного ключа d_2 и переданной ему точки uG, т. к. $uP_2=d_2uG$ и $\pi(uvcP_2)=\pi(uvcd_2G)$.

Далее он снимает гамму Z, получает D, проверяет совпадение идентификатора A с реальным идентификатором абонента, вырабатывает ключ $K_1=K(c, d_2, u, v)$ и вычисляет заново $\mathrm{MAC}(K_1, D)$. Если значение вновь вычисленного кода MAC совпадает с кодом, хранящимся в M, то абонент B признает ключ K истинным.

Мы построим скрытый канал связи в случае, когда используется механизм умножения на кофактор ($v=1$). Заметим, что использование кофактора в данном протоколе приводит к тому, что обнаружение нарушения корректности преобразований в ходе его выполнения не является однозначно свидетельством попытки

несанкционированных действий. По этой причине некорректность преобразований, вызванная использованием кофактора, для системы критичной не является.

Очевидно, при качественных криптографических преобразованиях, задействованных для реализации протокола, можно считать, что его корректное завершение практически достоверно свидетельствует об использовании истинного значения кофактора. Иными словами, по отношению к кофактору абонент *B* обладает некоторым проверочным соотношением *T*. Таким образом, корректность криптопротокола взаимно однозначно зависит от глобального (несекретного) параметра *c*. Исходя из этого, скрытую передачу сообщения *M** от *A* к *B* (*t* битов информации) можно осуществить следующим образом.

Абоненты заранее согласовывают долговременный ключ *Y* (случайное число, не превосходящее *n*), а также стеганографический параметр *W*, состоящий из *t* чисел, указывающих на номера различных разрядов в двоичной записи *c* (необходимого размера). Для передачи данных абонент *A* поразрядно сложением по модулю два модифицирует соответствующими битами сообщения *M** разряды кофактора *c*, перечисленные в списке *W*. Затем результат умножается на *Y*. В итоге получается модифицированный кофактор $c_1=Y(c\oplus M^*(W)) \bmod n$. Далее при использовании протокола пересылки ключа *K* абонент *A* действует стандартно, за исключением того, что использует модифицированный кофактор вместо исходного.

Абонент *B*, обнаруживая нарушение корректности преобразований в ходе протокола, строит модифицированный кофактор перебором с критерием истинности *T*. Затем вычисляет $Y^{-1}c_1\oplus c=M^*(W) \bmod n$.

Очевидно, реальные значения $t\approx 30$, т. е. *t* пренебрежимо мало по сравнению с *n*, следовательно, ключ *K* может быть принят абонентом *B* практически с исходной надежностью.

Заметим также, что аутентичность информации, передаваемой по скрытому каналу, в принципе, может быть обеспечена стандартными методами.

IV Выводы

В работе рассмотрена возможность скрытой передачи данных в криптопротоколах, основанных на свойствах эллиптических кривых. Показано, что механизмы цифровых подписей типа Эль Гамаля и механизмы пересылки ключей, внедряемые в настоящее время, допускают организацию скрытых каналов передачи информации, в том числе новых. Таким образом, существует угроза внедрения скрытых каналов связи в распространенные средства криптографической защиты информации. Качество скрытых каналов зависит от вычислительных ресурсов абонентов.

Литература: 1. Simmons G. J. Subliminal Communication is Easy Using the DSA // Advances in Cryptology. Proceedings of EUROCRYPT'93. – Springer-Verlag, 1995. – P. 219–232. 2. Simmons G. J. The Subliminal Channel and Digital SignaturesDSA // Advances in Cryptology. Proceedings of EUROCRYPT'84. – Springer-Verlag, 1985. – P. 364–378. 3. Silverman J. The Arithmetic of Elliptic Curves. – New York: Springer, 1986, – 400 p. 4. Кочубинский А. И. Эллиптические кривые в криптографии. // Безопасность информации. – 2, – 2000. с.18–31.

УДК 681.3.067:681.3.016

МЕТОДИКА ВЫЯВЛЕНИЯ В ДВОИЧНЫХ ВЕРОЯТНОСТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ ДЕТЕРМИНИРОВАННЫХ СОСТАВЛЯЮЩИХ НА ОСНОВЕ МЕТОДА БИНОМИАЛЬНОГО ПРЕОБРАЗОВАНИЯ

Виктор Куценко, Тарас Левченко
Научно-технический комплекс "Импульс", г. Киев

Аннотация: **При помощи известного метода биномиального преобразования проведен анализ двоичной вероятностной последовательности (ДВП) после наложения на нее трех типов детерминированных составляющих. Предложена методика выявления в ДВП детерминированных составляющих. Методика дает необходимые доказательства наличия в ДВП детерминированной составляющей и может быть применена как составная часть системы информационной безопасности.**

Summary: **The analysis of a binary probabilistic sequence (BPS) after queued superposition of three types of determined components made using of known method of binomial transformation. The technique is**