УДК 004.056.2
DOI 10.33764/2618-981X-2022-6-96-100

Предложение о модификации российского стандарта электронной цифровой подписи с целью ликвидации широкополосного скрытого канала

А. А. Клевцов[1]*, *А. Н. Фионов*[1,2]

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[2] Сибирский государственный университет телекоммуникаций и информатики, г. Новосибирск, Российская Федерация
* e-mail: sanek.klevtsov@gmail.com

Аннотация. Большинство алгоритмов цифровой подписи имеют возможность организации скрытых каналов для передачи информации. Их наличие было выявлено после публикации схемы цифровой подписи на базе шифра Эль-Гамаля. Пропускная способность данных каналов от нескольких бит (узкополосные каналы) до 256-512 бит (широкополосные каналы). В литературе описано несколько способов ликвидации широкополосных каналов при помощи надзирателя. Приведен анализ существующих методов ликвидации скрытых каналов в алгоритмах цифровой подписи. Выявлены недостатки существующих схем. Разработан метод модификации российского стандарта электронной цифровой подписи ГОСТ Р 34.10-2012 с целью ликвидации широкополосного скрытого канала. Метод предусматривает наличие надзирателя, который не участвует в образовании подписи и может проверять подписанные сообщения на отсутствие скрытых каналов.

Ключевые слова: ГОСТ Р 34.10-2012, электронная цифровая подпись, скрытые каналы, криптография

Proposal to modify the Russian standard for electronic digital signature in order to eliminate the broadband covert channel

A. A. Klevtsov[1]*, *A. N. Fionov*[1,2]

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
[2] Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian Federation
* e-mail: sanek.kletsov@gmail.com

Abstract. Most digital signature algorithms have the ability to organize hidden channels for transmitting information. Their presence was revealed after the publication of a digital signature scheme based on the El-Gamal cipher. The bandwidth of these channels ranges from a few bits (narrowband channels) to 256-512 bits (broadband channels). The literature describes several ways to eliminate broadband channels with the help of a supervisor. The analysis of existing methods of elimination of hidden channels in digital signature algorithms is given. The shortcomings of the existing schemes are revealed. A method of modification of the Russian standard of electronic digital signature GOST R 34.10-2012 has been developed in order to eliminate the broadband hidden channel. The method provides for the presence of a supervisor who does not participate in the formation of the signature and can check signed messages for the absence of hidden channels.

Keywords: GOST R 34.10-2012, electronic digital signature, covert channels, cryptography

Введение

Рассматривается проблема борьбы со скрытыми каналами в цифровой подписи. Для анализа мы выбрали группу алгоритмов цифровой подписи, которые идентичны DSA. Данная группа включает в себя подписи: Эль-Гамаля, Шнорра, ECDSA, ГОСТы Р 34.10-94, Р 34.10-2011, Р 34.10-2012.

Для подробного рассмотрения будет выбран алгоритм ГОСТ Р 34.10-2012, он аналогичен своим предшественникам, но возведение в степень заменяется операцией композиции точек на эллиптической кривой [2]. Также стоит заметить, что данный алгоритм является стандартом электронной подписи [2] в России и тема ликвидации скрытого канала в алгоритме ГОСТ Р 34.10-2012 является актуальной.

Чтобы проанализировать задачу скрытой передачи данных, мы возьмем стандартную схему взаимодействия. Существуют два участника обмена сообщениями, Алиса и Боб (обозначим их как A и B), и контролёр Венди (W). Венди контролирует все обмены между A и B, разрешая передавать только открытые подписанные сообщения. Предположим, что A хочет передать секретное сообщение таким образом, чтобы W не заподозрила сам факт его наличия (в противном случае любая передача сообщений будет остановлена).

Также следует учесть, что Алиса и Боб могли заранее договорится о секретном ключе *K* до того, как Венди начала контролировать процесс обмена сообщениями. Зная ключ, A и B могут согласованно генерировать любое количество секретных ключей и параметров. Например, $k_i = \text{шифр}_k(i)$, где i – порядковый номер, текущая дата, время и т.п., а шифр – это, например, блочный шифр с секретным ключом *K*.

Наличие скрытых каналов было выявлено [4] после публикации схемы цифровой подписи на базе шифра Эль-Гамаля [9]. Данные каналы сохраняются во всех последующих модификациях схемы. Чтобы прояснить проблему, необходимо рассмотреть особенности алгоритма электронной цифровой подписи ГОСТ Р 34.10-2012.

Общие открытые параметры алгоритма:

– эллиптическая кривая *E* над некоторым простым полем;

– простое число q (порядок циклической подгруппы точек на этой кривой);

– точка на кривой *P*, $[q]P = O$;

– хэш-функция *H* в соответствии с ГОСТ Р 34.10-2012.

Каждый пользователь *U* выбирает случайное число x_U (секретный ключ), $0 < x_U < q$, и вычисляет точку на кривой $Y_U = [x_U]G$ (открытый ключ). Параметры кривой и список открытых ключей передаются всем пользователям.

Чтобы подписать сообщение *M*, пользователь *U* делает несколько шагов:

1) генерирует случайное число k, $0 < k < q$;

2) находит точку $C = [k]P = (x, y)$;

3) вычисляет $r = x \bmod q$;

4) вычисляет $s = \big(rd_U + kH(M)\big) \bmod q$.

В итоге пользователь *U* подписывает сообщение парой чисел (*r*,*s*)

В ЭЦП существует широкополосный канал. Он возникает, когда число *k* выбирается не случайно, а содержит некоторое сообщение. Емкость данного канала равна 256–512 бит. Чтобы использовать канал, Боб должен знать ключ подписи Алисы. Для извлечения скрытого сообщения, содержащегося в *k,* Боб выполняет вычисление:

$$k = (s - rd_A)H^{-1}(M) \bmod q.$$

Для борьбы с указанным способом организации скрытого канала была предложена схема Мета-Эль-Гамаля, где контролёр принимает участие в генерации числа *k*. Это позволяет ликвидировать передачу скрытых данных.

Схема Мета-Эль-Гамаля

Для уничтожения скрытого канала подписывающему необходимо запретить выбирать значение k. Но и другие участники не должны иметь возможности выбирать это значение, так как любой, кому будет разрешено выбирать значение k, сможет подделывать подпись.

Единственное и наиболее подходящее решение заключается в том, чтобы подписывающий и контролёр совместно генерировали k. Тогда подписывающий не сможет контролировать биты числа k, а контролёр не сможет определить ни одного бита этого числа. Также у контролёра должна быть возможность проверить, что подписывающий использовал совместно созданное число k. Реализация данного способа была предложена в схеме Мета-Эль-Гамаля [10]:

a) Алиса выбирает k_1, вычисляет $R = [k_1]P$ и отправляет *R* Венди;

b) Венди после получения *R* высылает Алисе k_2;

c) Алиса вычисляет $k = k_1 k_2$ и использует это число для формирования подписи.

В свою очередь, Венди может проверить, что в подписи (*r*,*s*) нет скрытого канала. Для этого она:

– вычисляет $[k_2]R = [k_1 k_2]P = [k]P = (x, y)$;

– проверяет равенство $r = x \bmod q$.

Хотелось бы заметить, что в данной схеме существует два недостатка. Первый недостаток [11] заключается в том, что Венди может создать свой узкополосный скрытый канал путем манипуляции отдельными битам *r* за счет выбора k_2. И второй, наиболее существенный, недостаток – это передача k_2 по открытому каналу. Если Боб узнает k_2, то он может вычислить $k_1 = kk_2^{-1} \bmod q$. Из этого следует, что теперь k_1 может содержать скрытое сообщение. Сразу отметим тот факт, что использование защищенного соединения [12] между Алисой и Венди при помощи протокола TLS не работает. Стоит учесть, что Алиса и Боб в целях передачи скрытой информации могут постоянно получать секретные ключи и параметры. Поэтому, можно предположить, что все секретные параметры, используемые Алисой для установления TLS-соединения с Венди, известны Бобу.

Для устранения выявленных недостатков, нам необходимо пересмотреть указанную схему.

Схема модификации российского стандарта электронной цифровой подписи с целью ликвидации широкополосного скрытого канала

Основная идея заключается в следующем. Пусть Венди будет иметь:

– секретный ключ (ключ подписи) d_W, $z_W = d_W^{-1} \bmod q$;

– открытый ключ $Q_W = [d_W]P$.

Алиса вычисляет:

1) $R = [k_1]Q_W$;

2) $k_2 = H([k_1]P)$;

3) $k = k_1 k_2$.

Следующие шаги происходят по стандартной схеме. Алиса добавляет точку R к подписи.

Чтобы подтвердить метод, сначала заметим, что k_1 – это единственный параметр, который выбирает Алиса. И это единственное место, в котором можно организовать широкополосный канал для передачи скрытого сообщения. Чтобы доказать, что канала не существует и подпись не теряет условие безопасности, необходимо показать, что:

a) Боб не может получить k_2;

b) Венди не знает k (не может получить k_1).

Что касается Венди, то у нее та же информация, что и в схеме Мета-Эль-Гамаля и она не сможет получить k_1 по причине сложности задачи дискретного логарифмирования. Также можно заметить, что Венди не участвует в образовании подписи, а это значит, что Венди не может создать какой-либо канал.

Обращаем внимание на то, что Венди, как и в схеме Мета-Эль-Гамаля, может получить:

$$[z_W]R = [z_W][k_1]Q_W = [z_W k_1 d_W]P = [k_1]P.$$

В результате Боб не может узнать k_1 и $[k_1]P$.

В последствии модификация алгоритма ЭЦП ГОСТ Р 34.10-2012 будет реализована следующим образом. Чтобы подписать сообщение M, пользователь U:

1) генерирует случайное число k, $0 < k < q$;

2) находит точку $R = [k_1]Q_W$;

3) находит точку $[k_1]P$ и вычисляет $k_2 = H([k_1]P)$;

4) вычисляет $k = k_1 k_2$:

a) находит точку $C = [k]P = (x, y)$;

b) вычисляет $r = x \bmod q$;

c) вычисляет $s = \big(rd_U + kH(M)\big) \bmod q$.

В итоге пользователь U подписывает сообщение парой чисел (r, s, R).

Венди проверяет подпись на предмет отсутствия скрытого канала:

1) находит точку $T = [z_W]R$;

2) вычисляет $k_2 = H(T)$;
3) находит точку $[k_2]T = (x, y)$;
4) проверяет равенство $r = x \bmod q$.

Выводы

Разработан метод модификации российского стандарта электронной цифровой подписи с целью ликвидации широкополосного скрытого канала. Данный метод конкурентоспособен по отношению к ранее известным схемам [10] и [13]. Метод позволяет обнаружить широкополосный скрытый канал в бесконечном количестве подписей по принципу «один за другим». Он не требует взаимодействия с контролёром при образовании подписи, а, следовательно, не даст сбоев, если получатель скрытых сообщений (Боб) имеет доступ к каналу между отправителем (Алисой) и контролёром (Венди).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Шнайер Б. Прикладная криптография: протоколы, алгоритмы и исходный код на С: учеб. пособие. – М.: Диалектика, 2019. – 1040 с.

2. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи – М.: Стандартинформ, 2018. – 33 с.

3. Simmons G.J. The Subliminal Channel and Digital Signatures // Advances in Gryptology: Proceedings of CRYPTO ’83, Plenum Press, 1984, P. 51-67.

4. Simmons G.J. The Subliminal Channel and Digital Signatures // Advances in Gryptology: Proceedings of EUROCRYPT ’84, Springer-Verlag, 1985, P. 364-378.

5. Simmons G.J. The Subliminal Channel: Past and Present // European Transactions on Telecommunications, 1994, Vol. 4, No. 4, P. 459-473.

6. Simmons G.J. The Subliminal Channel of the U.S. Digital Signature Algorithm (DSA) // Proceedings of the Third Symposium on: State and Progress of Research in Cryptography, Rome: Fondazone Ugo Bordoni, 1993, P. 33-54.

7. Kobara K., Imai H. On The Channel Capacity of Narrow-band Subliminal Channels // In Proc. Of ICICS ’99, 1999, Vol. 1726, P. 309-323.

8. Simmons G.J. Subliminal Communication is Easy Using the DSA // Advances in Cryptology – EUROCRYPT ’93 Proceedings. Springer-Verlag, 1994, P. 218-232.

9. ElGamal A. A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE Trans. On Inform. Theory, Vol. IT-31, July 1985, No. 4, P. 469-72.

10. Horster P., Michels M., Petersen H., Subliminal channels in discrete logarithm based signature schemes and how to avoid them, 1994, P. 198-203.

11. Атамашкин М.И., Белим С.В. Скрытые каналы передачи информации в алгоритме электронной цифровой подписи ГОСТ Р 34.10-2001// Математические структуры и моделирование, 2011, Вып. 22, С. 101-113.

12. Rescola E. The transport layer security (TLS) protocol version 1.3, RFC 8446, 2018

13. Choi J., Golle P., Jakobsson M., Tamper-evident digital signature protecting certification authorities against malware// IEEE Int, Symp. On Dependable, Automatic and Secure Computing, Indianapolis, IN, 2006, P. 37-44.