УДК 004.056.2
DOI: 10.33764/2618-981X-2021-6-144-148

АНАЛИЗ ПРИМЕНИМОСТИ МЕТОДА ЛИКВИДАЦИИ СКРЫТЫХ КАНАЛОВ В ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Александр Андреевич Клевцов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры информационной безопасности, тел. (913)389-95-98, e-mail: sanek.klevtsov@gmail.com

Андрей Николаевич Фионов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доктор технических наук, профессор кафедры информационной безопасности, тел. (383)269-82-16, e-mail: a.fionov@ieee.org

Приведен способ ликвидации скрытых каналов в алгоритме электронной цифровой подписи ГОСТ Р 34.10-2012. Представлены примеры информационных систем, в которых используются электронные цифровые подписи. Рассмотрена возможность ликвидации скрытых каналов в различных информационных системах.

Ключевые слова: электронная цифровая подпись, ГОСТ Р 34.10-2001, скрытые каналы, криптография

ANALYSIS OF THE APPLICABILITY OF THE METHOD FOR ELIMINATING COVERT CHANNELS IN ELECTRONIC DIGITAL SIGNATURE

Aleksandr A. Klevtsov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Information Security, phone: (913)389-95-98, e-mail: sanek.kletsov@gmail.com

Andrey N. Fionov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, D. Sc., Professor, Department of Information Security, phone: (383)269-82-16, e-mail: a.fionov@ieee.org

A method for eliminating covert (hidden) channels in the GOST R 34.10-2012 electronic digital signature algorithm is presented. Examples of information systems that use electronic digital signatures are presented. The possibility of eliminating hidden channels is considered in various information systems.

Keywords: electronic digital signature, GOST R 34.10-2001, covert channels, cryptography

Введение

Многие алгоритмы электронной цифровой подписи (ЭЦП) имеют особенность, при которой существует возможность передать дополнительную скрытую информацию в подписи, извлекаемую в дальнейшем при помощи дополнительного секрета. Такое свойство впервые обнаружил Симмонс [1] и назвал скрытым каналом.

Среди таких алгоритмов ЭЦП можно выделить: ElGamal, DSA, Ong-Schnorr-Shamir, ESIGN (см., например, [2]), ГОСТ Р 34.10-2012 [3].

По сути, все они являются примерами общей схемы цифровой подписи и обладают свойством, при котором получаемая подпись зависит от некоторого случайного числа. Выбирая это число, подписывающий может определять вид подписи, а также закодировать в ней некоторую информацию.

Симмонс [4] разделил скрытые каналы на две категории:

1) широкополосные – число бит в случайном числе равно количеству бит скрытого сообщения;

2) узкополосные – количество бит случайного числа меньше количества бит в скрытом сообщении (более подробный анализ дан в [5]).

Существует множество информационных систем, в которых применяется цифровая подпись. При передаче сообщений в этих информационных системах существует риск внедрения дополнительной информации в скрытые каналы.

В данной работе приведен анализ метода ликвидации скрытых каналов на примере цифровой подписи ГОСТ Р34.10-2012. Рассмотрены типы информационных систем, в которых указанный метод возможен для применения.

Метод ликвидации скрытых каналов

В большинстве алгоритмов электронной подписи существует случайное число k, которое подписывающий выбирает самостоятельно. 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 контроллер совместно генерировали k. Тогда подписывающий не сможет контролировать биты числа k, а контроллер не сможет определить ни одного бита этого числа. Также должна быть возможность проверить контроллером, что подписывающий использовал совместно созданное число k.

Реализация такого метода ликвидации была предложена Симмонсом для DSA [6–8], этот метод был адаптирован для ЭЦП ГОСТ Р 34.10-2001 в [9, 10]. Мы изложим его применительно к действующему стандарту ГОСТ Р 34.10-2012. Рассматриваемый метод предполагает следующую модификацию алгоритма генерации подписи:

1) подписывающий генерирует число k' и отправляет контроллеру точку

$$U = k'P, \tag{1}$$

где P – генераторная точка на эллиптической кривой;

2) контроллер выбирает случайное число k'' и отправляет его подписывающему;

3) подписывающий использует для создания подписи число

$$k = k'k'' \bmod q, \quad (2)$$

где q – простое число, параметр алгоритма подписи, формируя подпись в виде пары чисел r, s по стандартному алгоритму;

4) контроллер проверяет подпись, а также то, что координата x точки $k''U$ сравнима с r по модулю q.

Однако, данный метод с участием контроллера для создания подписей возможен не во всех информационных системах, соответственно полностью ликвидировать скрытые каналы не представляется возможным.

Информационные системы с применением ЭЦП

Электронная подпись применяется для контроля целостности передаваемого сообщения, а также для подтверждения авторства.Эти свойства позволяют использовать подпись, например, для:

– взаимодействия граждан с органами государственной власти;

– применения в различных системах на основе блокчейн-технологий;

– электронной коммерции;

– подачи судебных исков;

– оформления онлайн заявлений для регистрации программ для ЭВМ.

В России, для взаимодействия с различными видами информационных систем, существует классификация ЭЦП. Всего их три вида:

1) простая электронная подпись – используется для получения госуслуг, заверения документов, внутреннего корпоративного документооборота;

2) усиленная неквалифицированная электронная подпись – используется для внутреннего и внешнего электронного документооборота по предварительной договоренности обеих сторон;

3) усиленная квалифицированная подпись – используется для сдачи отчетности, участия в торгах, работы с ГИС, проведения электронного документооборота.

Рассмотрим возможность применения метода ликвидации скрытых каналов в нескольких информационных системах.

Bitcoin. Технология блокчейн

Сеть Bitcoin [11] хранит всю информацию в цепочке блоков, называемой блокчейном. Особенность данной технологии в том, что изменить информацию в цепи можно только в конце блоков. Например, если Алиса заплатит Бобу биткоин, то эта информация появится в конце цепи, а в блоках до этого будет информация о том, что Бобу заплатил Трент.

Вся информация о транзакциях доступна любому участнику цепи. Каждая транзакция внутри блока подписывается электронной подписью, это сделано для того, чтобы информацию внутри транзакции нельзя было подделать.

В уже существующем алгоритме блокчейна реализовать метод ликвидации скрытых каналов невозможно, так как нельзя существенно изменить алгоритм их

работы. При создании своего блокчейна метод противодействия скрытым каналам можно учесть. Но необходимо условие недоступности канала, по которому контроллер передает число k'' автору подписи. В противном случае любой участник цепи, а, следовательно, и получатель скрытого сообщения, может узнать k'', восстановить k' и получить скрытое сообщение.

Регистрация программы для ЭВМ с ЭЦП заявителя

Регистрация программы для электронных вычислительных машин с цифровой подписью заявителя может быть реализована при помощи сайта Федерального института промышленной собственности (ФИПС) [12] и портала государственных услуг Российской Федерации. В данном случае протокол противодействия скрытым каналам реализовать возможно. В качестве контроллера могут выступать:

1) ФИПС;

2) портал «Госуслуги».

Получатель скрытого сообщения не сможет получить информацию, так как будет внедрен метод противодействия скрытым каналам и число k будет совместно сгенерировано отправляющим и контроллером.

Подача обращения через портал ГАС РФ «Правосудие»

При помощи электронной подписи также можно запрашивать и направлять документы в суд. Для этого существует онлайн-система запросов и подачи документов – Государственная автоматизированная система (ГАС) РФ «Правосудие» [13]. В этом случае в качестве контроллера может выступить сама онлайн-система, которая принимает заявку. ГАС РФ «Правосудие» сформирует число k'' и отправит подписывающему.

Заключение

Популярность электронных цифровых подписей увеличивается с каждым годом, информационные системы, в которых применяется подпись, расширяются. Но и риск внедрения дополнительной информации в скрытые каналы увеличивается.

Представленный в статье способ ликвидации скрытых каналов может решить проблему предотвращения скрытой передачи информации в различных информационных системах с применением цифровой подписи.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

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

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

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

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

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

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

7. 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.

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

9. Белим С.В., Федосеев А.М. Исследование скрытых каналов передачи информации в алгоритме цифровой подписи ГОСТ Р 34.10-2001 // Известия Челябинского научного центра. – 2007, вып. 2. – С. 55–57.

10. 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.

11. Интернет-энциклопедия: [Электронный ресурс] – Режим доступа: URL: http://ru.wikipedia.org/wiki/Bitcoin/. (Дата обращения: 15.04.2021).

12. Официальный сайт ФИПС: [Электронный ресурс] – Режим доступа: URL: https://new.fips.ru/ (Дата обращения: 15.04.2021).

13. Официальный сайт ГАС РФ «Правосудие»: [Электронный ресурс] – Режим доступа: URL: https://sudrf.ru/ (Дата обращения: 15.04.2021).

© А. А. Клевцов, А. Н. Фионов, 2021