УДК 004.056.55

Н. Н. ПОНОМАРЕНКО, А. Н. СТЕПАНЕНКО

Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Украина

МЕТОД АНОНИМНОГО УПРАВЛЕНИЯ АВТОРСКИМИ ПРАВАМИ С НУЛЕВОЙ ПЕРЕДАЧЕЙ ЗНАНИЙ НА БАЗЕ ШИФРОВАНИЯ С ОТКРЫТЫМ КЛЮЧОМ

Рассматривается задача анонимной регистрации и проверки авторских прав с нулевой передачей знаний. Показано, что эта задача может быть решена на базе шифрования с открытым ключом и использования криптостойких хэш-функций. Предложено использовать сеть доверенных серверов для хранения отметок времени авторских прав и сеть контролирующих серверов для мониторинга и контроля работы доверенных серверов. Перед анонимной публикацией какого-либо материала в открытой печати автор резервирует за собой права на этот материал, не передавая при этом никакой информации ни о себе, ни о публикуемом материале. Регистрация автора на сервере также не требуется. Показано, что использование метода RSA с длиной ключа 4096 бит и одновременно трех хэш-функций MD5, SHA-1 и RIPEMD160 позволяет обеспечить для разрабатываемой системы достаточную криптостойкость.

Ключевые слова: *шифрование с открытым ключом, хэш-функция, защита информации, нулевая передача знаний.*

Введение

Задача обеспечения анонимности или авторизации с нулевой передачей знаний [1, 2] занимает важное место в теории защиты информации [3-6] и решается для разнообразных коммерческих, гражданских и военных применений, например, при безопасной идентификации смарт-карт и их владельцев.

В данной работе рассматривается задача анонимного резервирования авторских прав [7] на какие-либо печатные, видео или иные материалы (в общем случае - данные) перед их публикацией. Очень часто, особенно, когда речь идет о правозащитных организациях, независимых журналистах, блогерах, лицо, публикующее информацию, может подвергаться тем или иным репрессиям и преследованиям за свою разоблачительную деятельность [8]. Поэтому журналист часто вынужден публиковать свой материал на условиях полной анонимности, так как только в этом случае он может сохранить свою безопасность. Однако при этом он не может доказать свои права на опубликованный документ и, как следствие, теряет возможность вносить в него правки, получить гонорар за публикацию, снять документ с публикации и т.д. Другими словами, анонимная публикация в классическом виде не позволяет управлять авторскими правами на документ.

Криптография предоставляет владельцу материала разнообразные инструменты для доказательства подлинности документа или право владельца на документ. Особенно сильно функциональные возможности криптографии расширились с появлением шифрования с открытым ключом, одним из наиболее известных представителей которого является метод RSA [6, 9-11]. Например, цифровая электронная подпись [1] позволяет автору удостоверить подлинность документа. Однако авторское право подразумевает еще и наличие отметки времени, на которую получены права на тот или иной материал. Цифровая электронная подпись не позволяет проверить подлинность такой отметки времени.

На данный момент разработано большое количество протоколов аутентификации пользователей с нулевой передачей знаний [1, 12-14]. Как правило, они предназначены для подтверждения прав доступа пользователя к функциям, доступным большой группе пользователей, внутри которой в результате авторизации данный пользователь остается анонимным. Однако в рассматриваемой задаче авторские права должны быть зарегистрированы на одного конкретного пользователя, а не на группу пользователей, что требует разработки специализированного метода аутентификации.

Для подтверждения отметок времени, на которые регистрируются авторские права, может быть создан специализированный сервер или облачное хранилище данных [15, 16], где хранились бы материалы и отметки времени их размещения. Однако при полной анонимности резервирования прав крайне нежелательно показывать материал кому-либо до его публикации, в том числе и помещать его

на какой-либо сервер. Даже для самого защищенного сервера нельзя исключать утечку информации, в результате которой размещенные на сервере материалы могут оказаться похищенными еще до их опубликования автором. Поэтому на таком сервере должен храниться не сам материал, а, например, значения хэш-функции [6] для данного материала. При этом следует предусмотреть защиту от взлома хэш-функции путем нахождения коллизий [6,17].

Целью данной работы является разработка криптографически устойчивого метода, который позволяет без какой-либо авторизации и разглашения информации о публикуемом материале резервировать авторские права на него. Автор, воспользовавшись этим методом, в дальнейшем будет иметь возможность легко доказать свое авторство и наличие отметки времени получения приоритета, причем также с нулевым разглашением информации.

1. Требования к системе анонимного управления авторскими правами

Для успешного функционирования системы должны выполняться основные требования:

- система должна резервировать и подтверждать авторство без передачи сведений об авторе;
- система не должна хранить материал, на который резервируется авторство;
- сервер системы должен хранить отметку времени, на которую было зафиксировано авторство;
- сервер не должен хранить большой объем информации (не больше нескольких кбайт).

Автор должен иметь возможность анонимно опубликовать материал, а при желании доказать свое авторство. В целях обеспечения анонимности система не должна хранить либо передавать информацию об авторе или его работе.

С помощью существующих технологий цифровой электронной подписи [3-6] можно подтвердить, что документ подписан именно этим человеком и целостность документа. Однако данная технология не может подтвердить, что документ подписан именно в тот момент времени, который заявляет автор подписи. При наличии двух авторов, каждый из которых подписал один и тот же документ, невозможно выяснить, кто первым подписал документ.

Для выполнения вышеприведенных требований необходимо создать сервер (или облачное хранилище данных), который не будет хранить материал автора. Вместо этого в данной работе предлагается на сервере хранить хэш-функции, вычисляемые по заданному материалу.

Поскольку длина результатов вычисления хэш-функций составляет всего несколько сотен бит и не требуется большого объема памяти для их хранения, то для повышения криптостойкости системы можно применять одновременно три хэш-функции.

Также сервер не должен хранить какой-либо информации о личности автора. Чтобы обеспечить это требование, в данной работе предлагается хранить на сервере только открытый RSA ключ автора. Доступ к открытому ключу могут получить все желающие, и он применяется для шифрования данных. Закрытый ключ автор должен хранить в секрете. С его помощью он сможет доказать свое право на авторство, расшифровав проверочный текст.

Дайджест, состоящий из даты и времени резервирования, трех хэш-функций и открытого ключа будет храниться в базе сервера.

Генерацию RSA ключей предлагается осуществлять, например, с помощью библиотеки OpenSSL [18, 19].

Автор должен генерировать уникальную пару закрытого и открытого ключа отдельно для каждого материала (текста), для которого он собирается резервировать авторские права. Это необходимо для того, чтобы невозможно было определить, что автором каких-либо двух материалов является один и тот же человек (в случае одинакового открытого ключа, хранимого на сервере для обоих материалов).

2. Схемы резервирования и проверки авторских прав

Резервирование авторских прав (рис. 1) осуществляется в такой последовательности:

1. Пользователь, желающий анонимно зарезервировать авторское право с помощью ПО генерирует открытый и закрытый ключи. Закрытый ключ он хранит в секрете. Открытый ключ он отправляет на сервер.

2. Пользовательское ПО вычисляет для материала значения трех хэш-функций. В данной работе предлагается для этих целей взять хэш-функции MD5 [6], SHA-1 [6] и RIPEMD-160 [20]. Эти значения пользователь также отправляет на сервер.

3. Сервер сохраняет три хеш-функции, открытый ключ, а также текущее время и дату (отметка времени резервирования авторских прав) в базу данных.

По окончании этой процедуры автор может публиковать материал.

Как видно, хранящаяся на сервере информация (открытый ключ и значения хэш-функций) не несут в себе никакой информации о владельце ключа. Материал по значениям хэш-функций также восстановить невозможно из-за их однонаправленности.

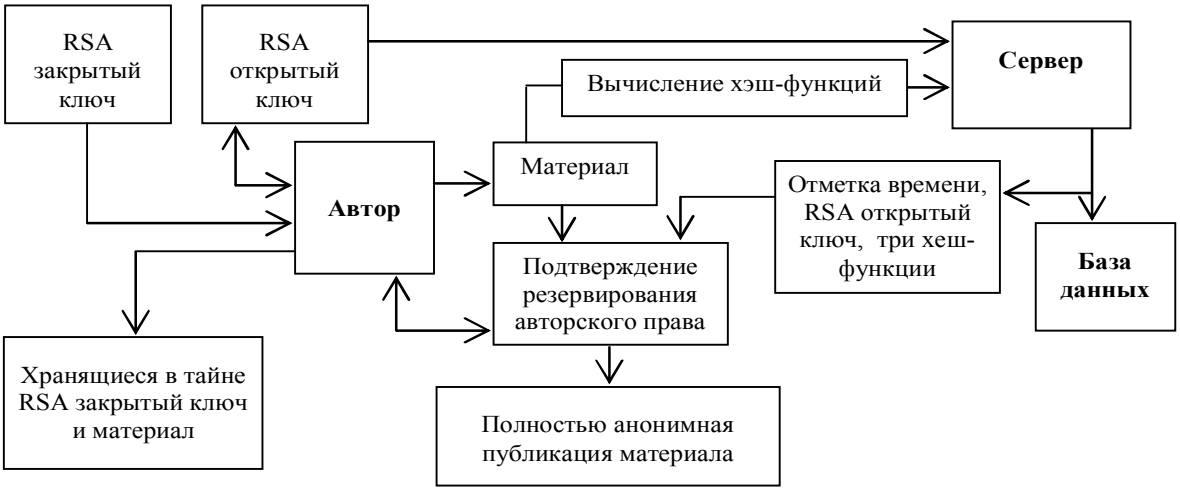

Рис. 1. Резервирование авторского права с нулевой передачей знаний

При желании автор может доказать свое право на авторство (рис. 2). Для этого:

1. Автор посылает материал издателю о просьбе подтвердить авторство.

2. Издательское ПО вычисляет три значения хэш-функций от материала и отправляет их серверу.

3. Сервер по значению хеш-функций находит в базе данных соответствующие открытый ключ, отметку времени и отправляет их издателю.

4. Издательское ПО создает случайное число, шифрует его с помощью полученного открытого ключа и отправляет шифровку автору.

5. Авторское ПО расшифровывает сообщение с помощью закрытого ключа и отправляет результат издателю.

6. Издательское ПО сверяет свое случайное число и полученное от автора. Если они идентичны, то автор доказал свои авторские права на материал. При этом личность автора остается анонимной.

Для обеспечения анонимности местоположения автора его взаимодействие с издателем может осуществляться, например, с помощью сети TOR [21].

Данная схема является неустойчивой к злоупотреблениям администраторов доверенного сервера. Уже после публикации какого-либо материала в открытой печати они задним числом могут вносить в базу данных сервера более ранние отметки времени резервирования прав на этот материал фиктивным автором.

Для решения этой проблемы предлагается разрешить любым серверам (пусть этот будут сервера волонтеров, осуществляющие контроль над доверенным сервером) регулярно копировать все хэш-функции по недавно зарегистрированным авторским правам в свои базы данных. Наличие большого числа таких серверов сделает невозможными любые махинации по внесению данных в доверенный сервер (или сеть доверенных серверов) задним числом.

3. Анализ криптостойкости предложенного метода

Уязвимыми местами предлагаемой системы являются метод шифрования RSA и хэш-функции. Взломав открытый ключ RSA и получив таким образом закрытый ключ, злоумышленник сможет доказать авторское право на документ. Взлом хэш-функций (реконструкция исходного материала по их значениям) также нарушит анонимность авторских прав, так как позволит узнать, на какой именно материал зарегистрированы авторские права.

Для взлома RSA нужно разложить известное число n на простые сомножители [22].

При длине ключа n = 4096 бит количество операций на факторизацию составит:

$$\exp\left(\sqrt[3]{\frac{64}{9}}\,n^{\frac{1}{3}}(\ln n)^{\frac{2}{3}}\right) = 7{,}17\cdot 10^{54}.$$

При взломе хэш-функций методом «грубой силы» количество операций на перебор всех возможных значений пропорционально 2^n (для MD5 n = 128 бит, для SHA-1 и RIPEMD-160 n = 160 бит) и составит:

$$2^{128}\cdot 2^{160}\cdot 2^{160} = 7{,}28\cdot 10^{134}.$$

При использовании атаки «дней рождения» для RIPEMD-160 для обнаружения коллизий потребуется в среднем 2^{80} операций, для SHA-1 - 2^{69} операций, для MD5 - 2^{39} операций. В конечном итоге потребуется: $2^{80}\cdot 2^{69}\cdot 2^{39} = 3{,}92\cdot 10^{56}$ операций.

Рассматривать атаку «дней рождения» в данном случае можно применительно к хэш-функциям всех публикаций, хранящихся на сервере (к этим данным имеют доступ контролирующие сервера и все желающие).

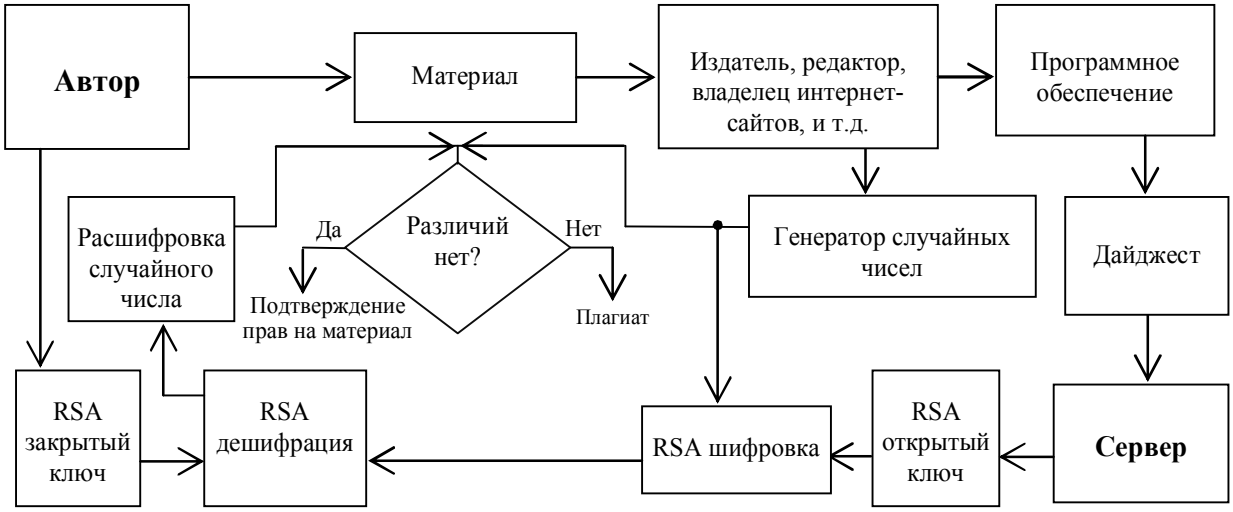

Рис. 2. Проверка авторских прав с нулевой передачей знаний

Злоумышленникам, чтобы доказать свой приоритет на какой-либо материал, достаточно найти коллизию лишь с одним из хранящихся на сервере значений хэш-функций (не важно, для какого материала) с подходящими отметками времени.

Именно поэтому в данной работе предлагается дополнительно защитить хэш-функции, используя сразу три из них. При этом, как показано выше, обеспечивается криптостойкость не меньше, чем у метода RSA. Таким образом, у предлагаемой системы нет каких-либо компонент, существенно более уязвимых, чем остальные, что обеспечивает ее сбалансированность с точки зрения криптостойкости.

Заключение

В работе предложен метод управления авторскими правами без авторизации и сообщения какой-либо информации об авторе и публикуемом материале. Предлагаемый метод был протестирован на реальном сервере (соответствующие подпрограммы были реализованы на языках программирования PHP и JavaScript; в качестве базы данных использовалась СУБД MySQL).

Литература

1. Feige, U. Zero-knowledge proofs of identity [Text] / U. Feige, A. Fiat, A. Shamir // Journal of cryptology. – 1988. – T. 1, №. 2. – P. 77-94.

2. Рябко, Б. Криптографические методы защиты информации [Текст] / Б. Рябко, А. Фионов. – М. : Горячая Линия – Телеком, 2012. – 230 с.

3. Мельников, Д. Информационная безопасность открытых систем [Текст] / Д. Мельников. – М. : Флинта, 2014. – 448 с.

4. Романьков, В. Введение в криптографию [Текст] / В. Романьков. – М. : Форум, 2012. – 240 с.

5. Платонов, В. Программно-аппаратные средства защиты информации [Текст] / В. Платонов. – М. : Академия, 2014. – 336 с.

6. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] / Б. Шнайер. – М. : Триумф, 2002. – 816 с.

7. Kwall, R. The soul of creativity: forging a moral rights law for the United States [Text] / R. Kwall. – Stanford University Press, 2010. – 272 p.

8. A Research Agenda for the Protection of Human Rights Defenders [Text] / A. M. Nah [et al.] // Journal of Human Rights Practice. – 2013. – T. 5, №. 3. – P. 401-420.

9. Жилин, А. В. Использование RSA алгоритма для обеспечения задач криптографической защиты информации в современных информационно-телекоммуникационных системах [Текст] / А. В. Жилин, А. В. Корнейко, В. В. Мохор // Захист інформації. – 2013. – №. 15, № 3. – С. 225-231.

10. Lin, X. J. Fully Deniable Mutual Authentication Protocol Based on RSA Signature [Text] / X. J. Lin, L. Sun // IACR Cryptology ePrint Archive. – 2013. – T. 2013. – C. 750.

11. Nagalakshmi, V. Improve Security with RSA and Cloud Oracle 10g [Text] / V. Nagalakshmi, V. Devi // ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India. –Vol. I. – Springer International Publishing, 2014. – P. 497-503.

12. Camenisch, J. A framework for practical universally composable zero-knowledge protocols [Text] / J. Camenisch, S. Krenn, V. Shoup // Advances in Cryptology–ASIACRYPT 2011. – Springer Berlin Heidelberg, 2011. – C. 449-467.

13. Cayrel, P. L. A zero-knowledge identification scheme based on the q-ary syndrome decoding problem [Text] / P. L. Cayrel, P. Véron, S. Alaoui // Selected

Areas in Cryptography. – Springer Berlin Heidelberg, 2011. – P. 171-186.

14. Groth, J. New techniques for noninteractive zero-knowledge [Text] / J. Groth, R. Ostrovsky, A. Sahai // Journal of the ACM (JACM). – 2012. – T. 59, №. 3. – P. 11.

15. Задірака, В. Сучасні методи розв'язання задач інформаційної безпеки [Текст] / В. Задірака // Вісник Національної академії наук України. – 2014. – №. 5. – С. 65-69.

16. Bhagat, S. K. An Analysis on Cloud Data Security and Accountability [Text] / S. K. Bhagat, G. P. Bhole // International Journal of Current Engineering and Technology. – 2014. – Vol. 1, №. 4. – P. 2464-2467.

17. Kumar, Raghuvanshi K. Study and Comparative Analysis of Different Hash Algorithm [Text] / Raghuvanshi K. Kumar, P. Khurana, P. Bindal // Journal of Engineering Computers & Applied Sciences. – 2014. – T. 3, №. 9. – P. 1-3.

18. Viega, J. Network Security with OpenSSL: Cryptography for Secure Communications [Text] / J. Viega, M. Messier, P. Chandra. – "O'Reilly Media, Inc.", 2002. – 386 p.

19. McAndrew, A. Introduction to Cryptography with open-source software [Text] / A. McAndrew. – CRC Press, Inc., 2011. – 461 p.

20. Dobbertin, H. RIPEMD-160: A strengthened version of RIPEMD [Text] / H. Dobbertin, A. Bosselaers, B. Preneel // Fast Software Encryption. – Springer Berlin Heidelberg, 1996. – P. 71-82.

21. Колисниченко, Д. Анонимность и безопасность в Интернете [Текст] / Д. Колисниченко. – БХВ-Петербург, 2012. – 229 с.

22. Integer factorization algorithm [Электронный ресурс]. – Режим доступа: http://www.connellybarnes.com/documents/factoring.pdf. – 22.09.2014.

Поступила в редакцию 6.11.2014, рассмотрена на редколлегии 18.11.2014

Рецензент: д-р техн. наук, проф., проф. каф. «Приема, передачи и обработки сигналов» В. В. Лукин, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Харьков.

МЕТОД АНОНІМНОГО УПРАВЛІННЯ АВТОРСЬКИМИ ПРАВАМИ З НУЛЬОВОЮ ПЕРЕДАЧЕЮ ЗНАНЬ НА БАЗІ ШИФРУВАННЯ З ВІДКРИТИМ КЛЮЧЕМ

М. М. Пономаренко, О. М. Степаненко

Розглянуто задачу анонімної реєстрації та перевірки авторських прав з нульовою передачею знань. Показано, що ця задача може бути вирішена на базі шифрування з відкритим ключем і використання криптостійких хеш-функцій. Запропоновано використовувати мережу довірених серверів для зберігання відміток часу авторських прав та мережу контролюючих серверів для моніторингу і контролю роботи довірених серверів. Перед анонімною публікацією будь-якого матеріалу у відкритій пресі автор резервує за собою права на цей матеріал, не передаючи при цьому жодної інформації ні про себе, ні про матеріал, що публікується. Реєстрації користувача на сервері також не потрібно. Показано, що використання методу RSA з довжиною ключа 4096 біт і одночасно трьох хеш-функцій MD5, SHA-1 і RIPEMD160 дозволяє забезпечити для запропонованої системи достатню криптостійкість.

Ключові слова: шифрування з відкритим ключем, хеш-функція, захист інформації, нульова передача знань.

METHOD OF ANONYMOUS MANAGEMENT OF MORAL RIGHTS WITH ZERO KNOWLEDGE TRANSFER BASED ON PUBLIC KEY CRYPTOGRAPHY

N. N. Ponomarenko, A. N. Stepanenko

The problem of anonymous registration and verification of moral rights with zero knowledge transfer is considered. It is shown that the problem can be solved based on public key cryptography and by using of cryptographically strong hash functions. Proposed to use a network of trusted servers to store timestamps of moral rights and network of control servers for monitoring of the trusted servers. Before an anonymous publication of any material the author reserves the moral rights to this material without transmitting any information about themselves or about the published materials. Author registration on trusted server is not required too. It is shown that the use of the 4096-bit RSA key with hash functions MD5, SHA-1 and RIPEMD160 allows to provide good cryptographic strength for the proposed system.

Key words*:* public key cryptography, hash function, information security, zero knowledge transfer.

Пономаренко Николай Николаевич - д-р техн. наук, доцент, доцент каф. «Приема, передачи и обработки сигналов», Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», Харьков, Украина, e-mail: nikolay@ponomarenko.info.

Степаненко Александр Николаевич – магистрант каф. «Приема, передачи и обработки сигналов», Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», Харьков, Украина, e-mail: stepanenko.alexander@gmail.com.