УДК 004.9 https://doi.org/10.51301/vest.su.2021.i3.22

Е.Н. Сейткулов*, Р.М. Оспанов, Б.Б. Ергалиева
Евразийский национальный университет им. Л.Н. Гумилева, Нур-Султан, Казахстан
*e-mail: yerzhan.seitkulov@gmail.com

ОБ ОДНОМ МЕТОДЕ ХРАНЕНИЕ ИНФОРМАЦИИ НА ЗАДАННОЕ ВРЕМЯ

Аннотация. Статья посвящена проблеме хранения информации на заданное время. Предложен криптографический протокол, обеспечивающий зашифрование сообщений, расшифрование которых будет возможно не ранее заданного времени. Протокол представляет собой эффективную комбинацию протокола распределенной генерации ключей, протокола проактивного разделения секрета, асимметричного алгоритма шифрования, алгоритма электронной цифровой подписи. На основе такого криптографического протокола можно разработать и внедрить практический сервис шифрования данных на заданное время. Это одно из важных проблем в вопросах обеспечения безопасности функционирования критически важных информационных систем, оперирующие с большими объемами конфиденциальной информации. В частности, в качестве применения, разработанные практические методы и протоколы позволят выработать альтернативную модель функционирования сервиса хранения информации на заданной время. Рассмотрена упрощенная модель функционирования сервиса хранения информации на заданное время на основе этого протокола.

Ключевые слова: хранение, информация, криптографический протокол, шифрование, эллиптические кривые.

Введение. В 1994 году Тимоти Мэй (Timothy C. May) в работе [1, chapter 14.5] впервые ввел в рассмотрение задачу отправки секретного сообщения в будущее. Эта задача заключается в зашифровании сообщений, расшифрование которых возможно только лишь по истечении заданного времени в будущем.

Существуют интересные практические приложения решения этой задачи. Например, можно обеспечить “запечатывание” дневников, записей, других каких-либо данных на какой-нибудь определенный срок, причем таким образом, чтобы даже автор этих данных не смог бы их “распечатать” раньше заданного срока. Полезным практическим приложением может являться защита важных данных, которые были получены в результате каких-нибудь научных исследований или экспериментов, до тех пор, пока они не будут завершены и опубликованы. Это может быть необходимым для предотвращения утечки информации или давления со стороны каких-либо заинтересованных лиц. Например, при проведении торгов можно сокрыть предложения цены участниками торгов до завершения торговой сессии. Другой случай, это когда при голосовании можно обеспечить защиту промежуточных данных голосования до их завершения с целью исключения влияния на ход голосования. Область применения решения задачи отправки секретного сообщения в будущее может быть весьма обширна и включает в себя не только аукционы и голосование, а также электронная коммерция, финансовые рынки и их регулирование, право.

Исследования в этом направлении ведутся с 1994 года. За прошедшее время было получено описание целого ряда интересных подходов к решению задачи шифрования в будущее. Так например, в 1996 году Ривест, Шамир и Вагнер (R. L. Rivest, A. Shamir, D. A. Wagner) в работе [2] для решения этой задачи применили так называемые “шарады” с временным замком (“time-lock puzzles”). В 1997 году Беллар и Голдвассер (M. Bellare, S. Goldwasser) в работе [3] описали схему шифрования с частичным условным депонированием ключей (partial key escrow protocol). В 2005 году Блейк и Чан (I. F. Blake, A. C.-F. Chan) в работе [4] использовали билинейные отображения на GDH группах (Gap Diffie-Hellman groups). В 2006 году Рабин и Торп (M.O. Rabin and C. Thorpe) в работе [5] построили криптографический протокол, который обеспечивает зашифрование сообщений, расшифрование которых будет

гарантированно не ранее заданного точного времени, даже если это расшифрование окажется нежелательным для отправителя. В основе этого протокола лежат протокол распределенной генерации ключей Педерсена (Pedersen distributed key generation), протокол проверяемого порогового разделения секрета Фельдмана (Feldman verifiable threshold secret sharing) и алгоритм шифрования Эль-Гамаля. Рабин и Торп отметили различие между существующими протоколами, подобным их, в которых время с момента зашифрования до момента расшифрования фиксировано, и другими протоколами, в которых дается лишь оценка этого времени или находится нижний предел оценки. Разработанное ими решение задачи шифрования в будущее получило название Time-Lapse Cryptography (TLC). Авторы TLC получили патент [6] на свое изобретение. В 2009 году в [7] была представлена реализация TLC на языке Erlang 5.6.5 на серверах под управлением Debian 4.0 Linux на четырехъядерных процессорах Intel Xeon, 2.0 ГГц. В 2015 году Сейткулов Е.Н., Оспанов Р.М., Майманов Е.М. в работе [8] представили криптографический протокол зашифрования данных на заданное время, основанный на TLC. В основе этого протокола вместо протокола распределенной генерации ключей Педерсена, протокола проверяемого порогового разделения секрета Фельдмана и алгоритма шифрования Эль-Гамаля используются, соответственно, протокол распределенной генерации ключей, основанный на дискретном логарифмировании на эллиптических кривых [9], протокол проверяемого порогового разделения секрета Педерсена и алгоритм шифрования Эль-Гамаля на эллиптических кривых. Протокол получил называние Elliptic Curve Time-Lapse Cryptography (ECTLC). Time-Lapse Cryptography (TLC) был также использован в работах [10], [11], [12], [13]. Также в основе протокола шифрования на заданное время возможно применение новых более эффективных алгоритмов и алгоритмов, расширяющих его функциональные возможности. В частности, для обеспечения зашифрования данных на достаточно продолжительное время можно применить протокол проактивного разделения секрета (proactive secret sharing) [14]. К настоящему времени разработаны различные варианты проактивного разделения секрета, такие как, например, в работах [15], [16], [17].

В данной статье рассматривается криптографический протокол, обеспечивающий зашифрование сообщений, расшифрование которых будет возможно не ранее заданного времени. На основе такого криптографического протокола можно разработать и внедрить практический сервис шифрования данных на заданное время. Это одно из важных проблем в вопросах обеспечения безопасности функционирования критически важных информационных систем, оперирующие с большими объемами конфиденциальной информации. В частности, в качестве применения, разработанные практические методы и протоколы позволят выработать альтернативную модель функционирования сервиса хранения информации на заданной время.

Методы. В основе рассматриваемого протокола лежат протоколы TLC и ECTLC. Рассматриваемый протокол осуществляется при помощи Сервиса (Time-Lapse Cryptography Service), состоящего из n участников P1, ..., Pn. Каждый участник Сервиса Pi может быть предстален автономным компьютером (сервером), безошибочно и секретно выполняющим вычисления, предусмотренные протоколом, надежно хранящим все свои секретные данные, имеющим безопасный способ резервного копирования данных для аварийного восстановления. Все участники Сервиса могут приватно и секретно обмениваться информацией между собой, образуя сеть. Предполагается использование в составе Сервиса небольшой сети менеджеров, которые действуют как “команда управления” Сервисом. В задачи этой команды входит создание расписания открытых и соответствующих закрытых ключей, создаваемых Сервисом; ведение внутренней доски объявлений для использования участниками Сервиса; ведение открытой доски объявлений для пользователей Сервиса. Каждый менеджер будет вести собственные копии этих двух досок объявлений. Участники

и пользователи Сервиса будут смотреть на сообщения, размещенные на каждом из копий досок объявлений, и определять правильные значения большинством записей. Каждый участник Сервиса сопровождает каждое сообщение цифровой подписью. Действия всех участников протокола синхронизируются при помощи общедоступных и надежных часов таких, как предоставляемых NIST.

Протокол представляет собой эффективную комбинацию протокола распределенной генерации ключей, протокола проактивного разделения секрета, асимметричного алгоритма шифрования, алгоритма электронной цифровой подписи. Протокол предусматривает использование согласованных параметров асимметричного алгоритма шифрования таких, как, например, простое число p, порождающий элемент g простого порядка q в случае алгоритма шифрования Эль-Гамаля, или модуль эллиптической кривой простое число p, уравнение эллиптической кривой, коэффициенты уравнения a и b из поля Fp, точка эллиптической кривой G простого порядка q в случае алгоритма шифрования Эль-Гамаля на эллиптических кривых. Поэтому необходимо будет осуществить исследование и выбор наиболее эффективных для разрабатываемого протокола указанных выше алгоритмов, протоколов и параметров.

Основные этапы протокола предполагаются следующими:

1) Генерация ключей при помощи протоколов распределенной генерации ключей и проактивного разделения секрета. Сервис может генерировать ключевые структуры на периодической основе; например, каждый день он может создавать ключи со сроком службы 1 неделю, или каждые 30 минут создавать ключи со сроком службы 2 часа. Такое расписание размещается менеджерами на открытой доске объявлений. Кроме того, Сервис может принимать запросы от пользователей генерировать новые ключи с заданным сроком службы; менеджеры принимают эти запросы и размещают их на открытой доске объявлений. Участники Сервиса создают ключи согласно протокола, подписывают их и опубликовывают подписанные ключевые структуры на открытой доске объявлений.

2) Зашифрование данных при помощи открытых ключей, сгенерированных Сервисом, с заданным сроком.

3) Расшифрование данных при помощи закрытых ключей, которые генерируются Сервисом при достижении заданного срока.

Результат. Далее рассмотрим упрощенную модель функционирования сервиса хранения информации на заданное время на основе вышеописанного протокола.

Участники в рассматриваемой модели:

1) Портал приема заявок от клиентов на хранение конфиденциальной информации;

2) Клиент – пользователь портала;

3) Сервис – три распределенных сервера, удаленных друг от друга. Предполагается, что серверы не вступают в сговор между собой, то есть не передают друг другу конфиденциальные информации.

Общее описание модели:

• Клиент осуществляет стандартный вход в портал;

• Клиент отправляет порталу запрос на шифрование данных;

• Портал отправляет запрос Клиента Сервису с указанием идентификатора клиента, времени отправки запроса и времени, раньше которого нельзя расшифровывать данные Клиента.

Шаг 1. Каждый сервер Сервиса получает запрос, генерирует собственный закрытый ключ, вычисляет собственный открытый ключ и отправляет его другим серверам Сервиса (Рис. 1).

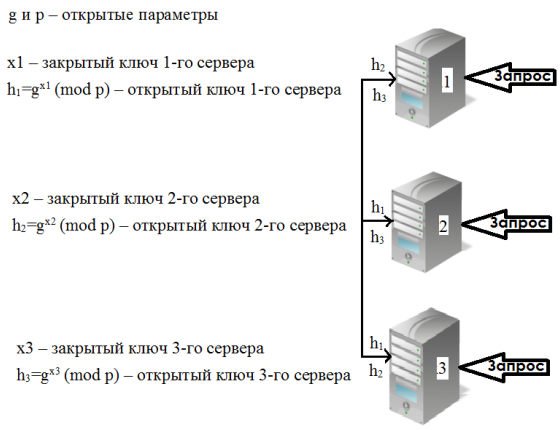

Рисунок 1. Шаг 1.

Шаг 2: Каждый сервер Сервиса получает открытые ключи остальных серверов, вычисляет общий открытый ключ, сохраняет его в своей базе данных с привязкой к указанным в запросе идентификатору Клиента и временным параметрам и отправляет вычисленный общий открытый ключ h порталу (Рис. 2).

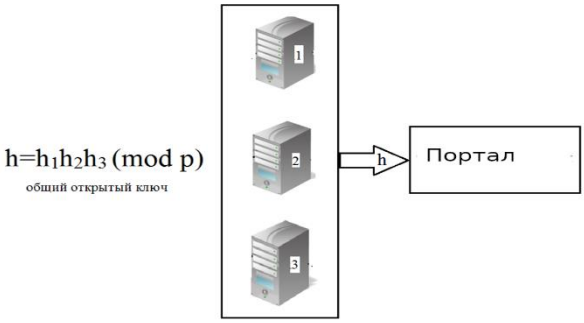

Рисунок 2. Шаг 2.

Шаг 3:

• Портал отправляет полученный открытый ключ h Клиенту;

• Клиент генерирует симметричный ключ s для шифрования данных, зашифровывает свои данные этим ключом, зашифровывает симметричный ключ полученным открытым ключом h по схеме Эль-Гамаля и отправляет зашифрованные данные и зашифрованный симметричный ключ Порталу (Рис. 3).

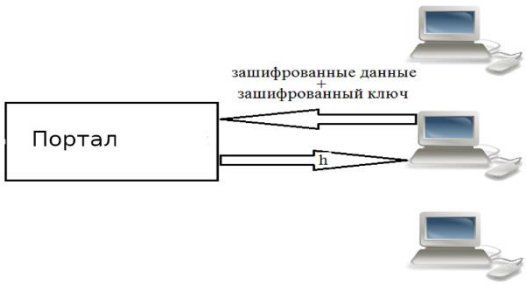

Рисунок 3. Шаг 3.

Шаг 4: Портал сохраняет полученные зашифрованные данные и зашифрованный ключ в своей базе данных с привязкой к указанным в запросе идентификатору Клиента и временным параметрам.

Шаг 5: Портал при достижении времени, раньше которого нельзя расшифровывать данные Клиента, или позже этого времени отправляет запрос Сервису на получение закрытого ключа с указанием идентификатора Клиента, открытого ключа и временных параметров (Рис. 4).

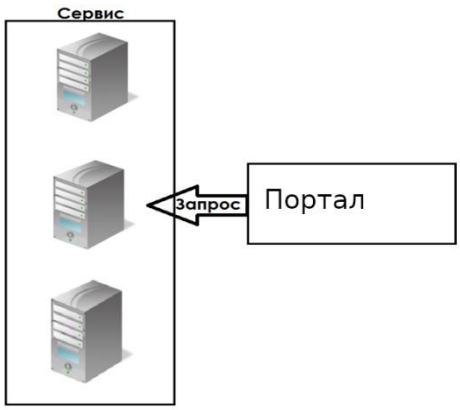

Рисунок 4. Шаг 5.

Шаг 6:

• Каждый сервер Сервиса получает запрос, отправляет собственный закрытый ключ остальным серверам.

• Каждый сервер Сервиса получает закрытые ключи остальных серверов, вычисляет общий закрытый ключ, сохраняет его в своей базе данных с привязкой к соответствующему общему открытому ключу и отправляет закрытый ключ Порталу (Рис. 5).

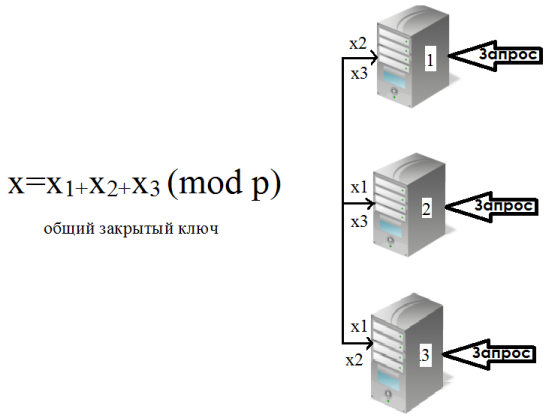

Рисунок 5. Шаг 6.

Шаг 7: Портал получает закрытый ключ, расшифровывает этим ключом симметричный ключ, и расшифровывает данные Клиента.

Обсуждение. В данной работе представлен протокол, обеспечивающий зашифрование сообщений, расшифрование которых будет возможно не ранее заданного времени. В основе его лежит один из подходов к решению задачи отправки секретных сообщений в будущее, известный как Time-Lapse Cryptography (TLC), описанный в [5], [6]. Протокол представляет собой эффективную комбинацию протокола распределенной генерации ключей, протокола

проактивного разделения секрета, асимметричного алгоритма шифрования, алгоритма электронной цифровой подписи. Рассмотрена упрощенная модель функционирования сервиса хранения информации на заданное время на основе представленного протокола. Конечной целью наших исследований является разработка и внедрение практического сервиса шифрования данных на заданное время. Для этого предстоит решить целый ряд задач. Во-первых, нами ведется работа над программной реализацией протокола. Во-вторых, необходимо решить задачу развертывания безопасной и надежной распределенной сети участников сервиса, обеспечивающих генерацию ключей. В-третьих, в перспективе разработать аппаратно-программную реализацию сервиса. В-четвертых, в перспективе рассмотреть возможность использования новых более эффективных алгоритмов и алгоритмов, расширяющих функциональные возможности сервиса. В-пятых, необходимо подробное исследование криптографической стойкости протокола.

Источник финансирования. Данная работа выполнена при финансовой поддержке грантового финансирования МЦРИАП, No AP06850817.

ЛИТЕРАТУРА

[1] May, T.C. (1994) *The Cyphernomicon: Cypherpunks FAQ and More*, v. 0.666, September 10, 1994.

[2] Rivest, R. L., Shamir, A., Wagner, D. A. (1996) “Time-lock puzzles and timed-release crypto”, *Technical Report MIT/LCS/TR-684*, MIT.

[3] Bellare, M., Goldwasser, S. (1997) “Verifiable partial key escrow”, *ACM Conference on Computer and Communications Security*, pp. 78–91.

[4] Blake, I. F., Chan, A. C.-F. (2005) “Scalable, server-passive, user-anonymous timed release public key encryption from bilinear pairing”, *Proceedings of 25th IEEE International Conference on Distributed Computing Systems*, pp. 504 – 513.

[5] Rabin, M.O., Thorpe, C.A. (2006) “Time-lapse cryptography”, *Technical report TR-22-06*, Harvard University School of Engineering and Computer Science.

[6] Rabin, M.O., Thorpe, C.A. (2007) “Method and apparatus for time-lapse cryptography”, *U.S. Patent 8,526,621*.

[7] Thorpe, C.A., Barrientos, M., Rabin, M.O. (2009) “Implementation of A Time-Lapse Cryptography Service”, *IEEE Symposium on Security and Privacy*, Oakland.

[8] Сейткулов Е.Н., Оспанов Р.М., Майманов Е.М. Сервис шифрования данных на заданное время // “Информационная безопасность в свете Стратегии Казахстан-2050”: сборник трудов III международной научно-практической конференции (15-16 октября 2015г., Астана). - Астана, 2015. - 400 с. - С. 308-317.

[9] Tang, C., Chronopoulos, A.T. (2005) “An Efficient Distributed Key Generation Protocol for Secure Communications with Causal Ordering”, *Proceedings of IEEE ICPADS 2005, The 11th International Conference on Parallel and Distributed Systems*, 20-22 July 2005, Volume 2, Fukuoka, Japan, pp. 285 - 289.

[10] Doku, R., Rawat, D. B., Liu, C. (2020) "On the Blockchain-Based Decentralized Data Sharing for Event Based Encryption to Combat Adversarial Attacks", I*EEE Transactions on Network Science and Engineering*, doi: 10.1109/TNSE.2020.2987919.

[11] Alvarez, R., Nojoumian, M. (2019) “Comprehensive Survey on Privacy-Preserving Protocols for Sealed-Bid Auctions”, *Computers and Security* (C&S), *Elsevier*, vol 88, pp. 101502-101515.

[12] Sun, J, Liu, N. (2017) “Incentivizing Verifiable Privacy-Protection Mechanisms for Offline Crowdsensing Applications”, *Sensors*. 2017; 17(9):2024. https://doi.org/10.3390/s17092024

[13] Luong, N. C., Hoang, D. T., Wang, P., Niyato, D., Han, Z. (2017) “Applications of Economic and Pricing Models for Wireless Network Security: A Survey”, *IEEE Communications Surveys and Tutorials*, vol. 19, no. 4, 7994586, pp. 2735-2767. https://doi.org/10.1109/COMST.2017.2732462

[14] Herzberg, A., Jarecki, S., Krawczyk, H., Yung, M. (1995) “Proactive secret sharing or: How to cope with perpetual leakage”, In: Coppersmith D. (eds) *Advances in Cryptology* — CRYPT0’ 95. CRYPTO 1995. Lecture Notes in Computer Science, vol 963. Springer, Berlin, Heidelberg. pp. 339–352. https://doi.org/10.1007/3-540-44750-4_27

[15] Baron, J., ElDefrawy, K., Lampkins, J., Ostrovsky, R. (2015) “Communication-Optimal Proactive

Secret Sharing for Dynamic Groups", *Cryptology ePrint Archive*, Report 2015/304, 2015, Available at: https://eprint.iacr.org/2015/304 (Accessed: 1 June 2021)

[16] Brendel, J., Demirel, D. (2017) "Efficient Proactive Secret Sharing", *Cryptology ePrint Archive*, Report 2017/719, 2017, Available at: https://eprint.iacr.org/2017/719 (Accessed: 1 June 2021)

[17] Low, A., Krishna, D., Zhang, F., Wang, L., Zhang, Y., Juels, A., Song, D. (2019) "Proactive Secret Sharing in Dynamic Environments", EECS Department University of California, *Berkeley Technical Report No. UCB/EECS-2019-62,* May 17, 2019, Available at: http://www2.eecs.berkeley.edu/Pubs/TechRpts/2019/EECS-2019-62.pdf (Accessed: 1 June 2021)

REFERENCES

[1] May, T.C. (1994) *The Cyphernomicon: Cypherpunks FAQ and More*, v. 0.666, September 10, 1994.

[2] Rivest, R. L., Shamir, A., Wagner, D. A. (1996) "Time-lock puzzles and timed-release crypto", *Technical Report MIT/LCS/TR-684*, MIT.

[3] Bellare, M., Goldwasser, S. (1997) "Verifiable partial key escrow", *ACM Conference on Computer and Communications Security*, pp. 78–91.

[4] Blake, I. F., Chan, A. C.-F. (2005) "Scalable, server-passive, user-anonymous timed release public key encryption from bilinear pairing", *Proceedings of 25th IEEE International Conference on Distributed Computing Systems*, pp. 504 – 513.

[5] Rabin, M.O., Thorpe, C.A. (2006) "Time-lapse cryptography", *Technical report TR-22-06*, Harvard University School of Engineering and Computer Science.

[6] Rabin, M.O., Thorpe, C.A. (2007) "Method and apparatus for time-lapse cryptography", *U.S. Patent 8,526,621*.

[7] Thorpe, C.A., Barrientos, M., Rabin, M.O. (2009) "Implementation of A Time-Lapse Cryptography Service", *IEEE Symposium on Security and Privacy*, Oakland.

[8] Sejtkulov E.N., Ospanov R.M., Majmanov E.M. Servis shifrovanija dannyh na zadannoe vremja // "Informacionnaja bezopasnost' v svete Strategii Kazahstan-2050": sbornik trudov III mezhdunarodnoj nauchno-prakticheskoj konferencii (15-16 oktjabrja 2015g., Astana). - Astana, 2015. - 400 s. - S. 308-317.

[9] Tang, C., Chronopoulos, A.T. (2005) "An Efficient Distributed Key Generation Protocol for Secure Communications with Causal Ordering", *Proceedings of IEEE ICPADS 2005, The 11th International Conference on Parallel and Distributed Systems*, 20-22 July 2005, Volume 2, Fukuoka, Japan, pp. 285 - 289.

[10] Doku, R., Rawat, D. B., Liu, C. (2020) "On the Blockchain-Based Decentralized Data Sharing for Event Based Encryption to Combat Adversarial Attacks", I*EEE Transactions on Network Science and Engineering*, doi: 10.1109/TNSE.2020.2987919.

[11] Alvarez, R., Nojoumian, M. (2019) "Comprehensive Survey on Privacy-Preserving Protocols for Sealed-Bid Auctions", *Computers and Security* (C&S), *Elsevier*, vol 88, pp. 101502-101515.

[12] Sun, J, Liu, N. (2017) "Incentivizing Verifiable Privacy-Protection Mechanisms for Offline Crowdsensing Applications", *Sensors*. 2017; 17(9):2024. https://doi.org/10.3390/s17092024

[13] Luong, N. C., Hoang, D. T., Wang, P., Niyato, D., Han, Z. (2017) "Applications of Economic and Pricing Models for Wireless Network Security: A Survey", *IEEE Communications Surveys and Tutorials*, vol. 19, no. 4, 7994586, pp. 2735-2767. https://doi.org/10.1109/COMST.2017.2732462

[14] Herzberg, A., Jarecki, S., Krawczyk, H., Yung, M. (1995) "Proactive secret sharing or: How to cope with perpetual leakage", In: Coppersmith D. (eds) *Advances in Cryptology* — CRYPT0' 95. CRYPTO 1995. Lecture Notes in Computer Science, vol 963. Springer, Berlin, Heidelberg. pp. 339–352. https://doi.org/10.1007/3-540-44750-4_27

[15] Baron, J., ElDefrawy, K., Lampkins, J., Ostrovsky, R. (2015) "Communication-Optimal Proactive Secret Sharing for Dynamic Groups", *Cryptology ePrint Archive*, Report 2015/304, 2015, Available at: https://eprint.iacr.org/2015/304 (Accessed: 1 June 2021)

[16] Brendel, J., Demirel, D. (2017) "Efficient Proactive Secret Sharing", *Cryptology ePrint Archive*, Report 2017/719, 2017, Available at: https://eprint.iacr.org/2017/719 (Accessed: 1 June 2021)

[17] Low, A., Krishna, D., Zhang, F., Wang, L., Zhang, Y., Juels, A., Song, D. (2019) "Proactive Secret Sharing in Dynamic Environments", EECS Department University of California, *Berkeley Technical Report No. UCB/EECS-2019-62,* May 17, 2019, Available at: http://www2.eecs.berkeley.edu/Pubs/TechRpts/2019/EECS-2019-62.pdf (Accessed: 1 June 2021)

Е.Н. Сейткұлов*, Р.М. Оспанов, Б.Б. Ергалиева
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан, Қазақстан
*e-mail: yerzhan.seitkulov@gmail.com

БЕРІЛГЕН УАҚЫТТА АҚПАРАТТЫ САҚТАУ БІР ӘДІС ТУРАЛЫ

Аннотация. Мақала белгілі бір уақытқа ақпаратты сақтау мәселесіне арналған. Хабарламалардың шифрлануын қамтамасыз ететін криптографиялық протокол ұсынылды, олардың шифрын ашу берілген уақыттан ерте мүмкін болмайды. Протокол - бұл таратылған кілттерді құру хаттамасының, құпияны проактивті бөлу протоколының, асимметриялық шифрлау алгоритмінің, электрондық цифрлық қолтаңба алгоритмінің тиімді үйлесімі. Осындай криптографиялық протоколдың негізінде белгілі бір уақытқа деректерді шифрлаудың практикалық қызметін жасауға және енгізуге болады. Бұл құпия ақпараттың үлкен көлемімен жұмыс істейтін аса маңызды ақпараттық жүйелердің жұмыс істеу қауіпсіздігін қамтамасыз ету мәселелеріндегі маңызды проблемалардың бірі. Атап айтқанда, қолдану ретінде әзірленген практикалық әдістер мен протоколдар белгілі бір уақытқа ақпаратты сақтау қызметі жұмысының балама моделін жасауға мүмкіндік береді. Осы протокол негізінде белгілі бір уақытқа ақпаратты сақтау қызметі жұмысының жеңілдетілген моделі қарастырылады.

Негізгі сөздер: сақтау, ақпарат, криптографиялық протокол, шифрлау, эллиптикалық қисықтар.

Y.N. Seitkulov*, R.M. Ospanov, B.B. Yergaliyeva
L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan
*e-mail: yerzhan.seitkulov@gmail.com,

ON ONE METHOD OF STORING INFORMATION FOR A SPECIFIED TIME

Abstract. The article is about the problem of storing information for a specified time. A cryptographic protocol is proposed that provides encryption of messages, the decryption of which will be possible no earlier than a specified time. The protocol is an effective combination of a distributed key generation protocol, a proactive secret sharing protocol, an asymmetric encryption algorithm, and an electronic digital signature algorithm. On the basis of such a cryptographic protocol, you can develop and implement a practical data encryption service for a specified time. This is one of the most important problems in ensuring the security of the operation of critical information systems that operate with large amounts of confidential information. In particular, as an application, the developed practical methods and protocols will allow us to develop an alternative model for the operation of the information storage service at a specified time. A simplified model of the operation of the information storage service for a specified time based on this protocol is considered.

Keywords: storage, information, cryptographic protocol, encryption, elliptic curves.