A.V.Beresneva, A.V.Epishkina

Threshold Signature Schemes Application

Keywords: digital signature, threshold signature, elliptic curves, secret sharing, threshold schemes.

This work is devoted to an investigation of threshold signature schemes. The systematization of the threshold signature schemes was done, cryptographic constructions based on interpolation Lagrange polynomial, elliptic curves and bilinear pairings were examined. Different methods of generation and verification of threshold signatures were explored, the availability of practical usage of threshold schemes in mobile agents, Internet banking and e-currency was shown. The topics of further investigation were given and it could reduce a level of counterfeit electronic documents signed by a group of users.

А.В. Береснева, А.В. Епишкина

О ПРИМЕНЕНИИ КРИПТОГРАФИЧЕСКИХ ПРИМИТИВОВ, РЕАЛИЗУЮЩИХ ПОРОГОВУЮ ПОДПИСЬ

Введение

Вопрос о применении электронной подписи является крайне актуальным. Благодаря современному развитию информационных технологий любой бумажный документ заменяется на электронный, который может представлять из себя и электронное письмо, и даже электронные деньги. Во многих из новых форм коммуникации электронная подпись, связывающая хранимый в тайне секретный ключ и цифровые данные подписываемого документа, имеет важное значение.

Электронная подпись [1] используется для подтверждения подлинности, целостности и идентификации автора цифровой информации – например, документов, сообщений электронной почты и макросов – с помощью методов компьютерной криптографии, т.е. с ее помощью возможно обеспечить следующие свойства информации [2]:

- **gодлинность** – электронная подпись осуществляет аутентификацию источника сообщения;
- **целостность** – электронная подпись удостоверяет, что содержимое документа не было изменено и не подделано после формирования подписи;
- **неотрекаемость** – электронная подпись помогает доказать любой из сторон авторство подписанного содержимого.

Поскольку в ряде случаев электронная подпись приравнивается к собственноручной подписи на бумажном документе, необходимо помнить, что данные виды подписи не являются полностью идентичными? и отличия электронной подписи заключаются в следующем [3]:

- не обязательно ставится на документах – любой материал в цифровой форме может быть подписан;
- не переносится на другие документы – электронная подпись не тиражируется и меняется от документа к документу;
- тесно связана с документом – нельзя изменить документ, не меняя подписи;
- не генерируется непосредственно человеком без использования технических средств.

Анализ различных схем электронной подписи

Для реализации электронной подписи необходимы алгоритмы вычисления и проверки подписи, а ее надежность определяется сложностью решения следующих задач [4]:

- подделки подписи, т.е. нахождения значения подписи для данного документа без использования секретного ключа;
- создания подписанного сообщения, т.е. нахождения хотя бы одного сообщения с правильным значением подписи;
- подмены сообщения, т.е. подбора двух различных сообщений с одинаковыми подписями.

В настоящее время существует несколько подходов к созданию схем электронной подписи [5]:

- схемы на основе систем шифрования с открытыми ключами;
- схемы со специально разработанными алгоритмами вычисления и проверки подписи;
- схемы на основе симметричных систем шифрования.

Рассмотрим подробнее виды схем электронной подписи на основе криптосистем с открытым ключом [4, 6]. Схемы различаются по способу формирования секрета подписи:

- мультиподпись;
- подпись «вслепую»;
- составная подпись;
- групповая подпись;
- кольцевая подпись;
- полномочная подпись;
- уникальная подпись;
- пороговая подпись.

В настоящей работе исследуется схема пороговой подписи.

Некоторые свойства схем пороговой подписи

В связи с потребностями современного бизнес-сообщества растет число ситуаций, когда необходимо, чтобы сообщение было подписано группой подписчиков и все они обладали равными правами по отношению к подписи. В этом случае применимо пороговое разделение секрета, а именно пороговая подпись. Пороговая подпись – схема электронной подписи, в которой любые t или более участников подписи в группе, состоящей из n абонентов ($t \leq n$), могут производить подпись от имени группы. Секретная информация распределена среди этих n пользователей, причем любое подмножество из более чем t пользователей может восстановить секрет [7] и никакая подгруппа из менее чем t участников не может вычислить правильную подпись. Пороговая подпись не раскрывает членов группы, которые владеют секретом, а секретный ключ является общим для множества из n участников, для чего может быть использована любая схема порогового разделения секрета. Схема пороговой подписи (t, n) состоит из трех протоколов:

- протокол генерации ключа;
- протокол генерации подписи;

- протокол проверки подписи.

В работе были исследованы различные математические аппараты, применимые для формирования пороговой подписи, среди них можно выделить следующие:

- интерполяционный многочлен Лагранжа [7 – 11];
- эллиптические кривые [10 – 16];
- билинейные спаривания [17 – 19].

Пороговые версии схемы могут быть построены для многих открытых схем шифрования [11, 21]. В настоящее время известны схемы пороговой подписи для следующих алгоритмов электронной подписи:

- RSA [7, 14, 20, 22];
- DSS [20, 23];
- схемы Эль-Гамаля на эллиптических кривых [24 – 26].

Анализ различных схем пороговой подписи позволяет указать следующие способы нарушения протокола работы пороговой схемы [5]:

- владелец одной из долей секрета может помешать восстановлению общего секрета, отдав в нужный момент неверную (случайную) долю;
- злоумышленник, не имея собственной доли секрета, может присутствовать при восстановлении секрета.

Пороговая подпись, основанная на алгоритме Эль-Гамаля

Поскольку действующий российский стандарт на алгоритм электронной подписи ГОСТР 34.10-2012 [13] основан на алгоритме Эль-Гамаля, приведем для него схему пороговой подписи [2, 27], состоящую из трех этапов: генерации ключей, генерации подписи и проверки подписи.

Схема генерации ключа. Сервер формирует и публикует системные параметры – открытый ключ, устойчивый к коллизиям алгоритм хэширования H, модуль p, эллиптическую кривую ε_p. Пусть $f(x)$ – (t, n) – пороговая функция, тогда

$$f(x) = a_{t-1}x^{t-1} + \ \ldots + a_1 x + a_0 (\mathrm{mod} n), \qquad (1)$$

где a_i – случайное число, $a_i \in [1, n-1], i = 0, \ldots, t-1$, $f(0) = a_0$ – групповой секретный ключ, $f(x_i)$ – индивидуальный секретный ключ участника U_i, $G \in E\ (GF\ (p))$ – заданная точка эллиптической кривой.

Схема генерации подписи.

Группа, которая должна подписать сообщение, состоит из участников U_1, U_2 – клиента и сервера и может представлять группу для подписи сообщения m. Для генерации результирующей пороговой подписи сообщенияm требуется генерация отдельных электронных подписей, проверка отдельных подписей и последним шагом – генерация пороговой подписи (t, n). Данные действия выполняются поэтапно.

Шаг 1. Сервер отправляет каждому участникуU_i секретный ключ $f(x_i)$. Пользователь использует выбранную им точку на кривой R_i, случайное целое число k_i, $1 \leq k_i \leq n-1$ для расчета своей индивидуальной подписи (r_i, s_i)для сообщения m и дальнейшей ее отправки на сервер.

Шаг 2. После получения электронной подписи (r_i, s_i) всех участников группы сервер проверяет по определенному алгоритму достоверность подписей участников.

Шаг 3. После проверки электронных подписей (r_i, s_i) всех участников сервер вычисляет и публикует групповую подпись (r, s) сообщения m.

Схема проверки подписи. Любой получатель подписи (r, s) может проверить подлинность пороговой подписи сообщения m.

Получатель вычисляет следующее значение:

$$S = \sum_{i=1}^{t} r_i s_i (mod n) \quad (2)$$

и сравнивает его со значением s, в случае выполнения равенства $S = s$ подпись признается подлинной, в противном случае подпись не верна.

Особенности данной схемы заключаются в следующем:

- подпись не является анонимной, т.е. активное подмножество участников подписи должно быть известно проверяющему;
- частичные подписи могут быть проверены посредником, т.е. настоящая схема позволяет обнаружить и скорректировать неисправные частичные подписи.

Сравнительный анализ различных схем пороговой подписи

Помимо схемы пороговой подписи Эль-Гамаля на эллиптических кривых авторами были проанализированы следующие алгоритмы подписи:

- пороговая подпись Шамира;
- пороговая версия схемы DSS;
- пороговая подпись на билинейных спариваниях;
- пороговая версия схемы электронной подписи RSA.

Сравнительные характеристики существующих схем пороговой подписи приведены в табл. 1.

Таблица 1. Сравнительные характеристики схем пороговой подписи

Свойства	Пороговая подпись Шамира	Пороговая подпись Эль-Гамаля на эллиптических кривых	Пороговая подпись на билинейных спариваниях	Пороговая версия схемы DSS	Пороговая версия схемы электронной подписи RSA
Возможность проверки частичных подписей	–	+	–	+	–
Стойкость к атаке заговора $t-1$ участника	+	+	–	+	+

При выборе схемы для дальнейшего исследования учитывалась возможность проверки частичных подписей, т.к. если она не предусмотрена, то итоговая подпись с некоторой вероятностью может быть сформирована неверно. Также во внимание принималась стойкость схем к атаке заговора участников, т.к. успешная атака данного тип может существенно снизить безопасность основанного на схеме протокола.

Области применения пороговой подписи

Распределенная криптография в настоящее время – активно развивающаяся область, и одним из ее наиболее глубоко изученных направлений являются схемы пороговой подписи. Пороговое разделение секрета в схемах электронной подписи на данный момент применяется в различных областях. Наиболее активно такая схема применяется в сфере финансов и, как следствие, сильно распространенного в настоящее время интернет-банкинга. На практике в большинстве случаев для криптографической защиты секретных ключей чаще всего используются пороговые криптосистемы. Механизм разделения секретных ключей применим как для группы участников, так и для одного абонента в том случае, когда он может разделить ключ между несколькими своими устройствами. Данный подход обеспечивает устойчивость процесса обработки и сохранности ключевого материала в условиях неблагоприятных внешних воздействий. Пороговые подписи были также применены в ряде областей, чтобы избежать концентрации ценной информации в единое целое. Например, Oceanstore [31] является крупномасштабной распределенной системой хранения данных. Для обеспечения безопасности информации, хранимой в данной системе, используется пороговая подпись, секрет которой разделен между внутренним кольцом серверов [29, 30]. Таким образом, злоумышленнику будет гораздо сложнее получить доступ к данным. Для системы Oceanstore также разработаны специальные виды онлайн- и оффлайн-схемы пороговой подписи [27, 29], которые предусматривают распределение нагрузок на серверы при вычислении подписи. Преимущество оффлайн-схемы пороговой подписи заключается в том, что все операции для формирования подписи серверы производят заранее, а когда требуется сгенерировать подпись, они просто объединяют уже имеющиеся данные в подпись.

Исследование вопросов, связанных с применением электронной валюты, позволяет говорить о том, что здесь также важная роль при обеспечении информационной безопасности отводится пороговой подписи. Из-за использования такой схемы электронной подписи организация может осуществлять совместный контроль при переводе электронной валюты, распределяя части секретного ключа между устройствами нескольких работников. В некоторых случаях для перевода электронной валюты необходимо подтверждение нескольких лиц, причем при использовании обычной мультиподписи нарушаются анонимность и конфиденциальность. А пороговую подпись получатель не сможет отличить от подписи, сформированной одним абонентом. По этой причине пороговые подписи, применяемые для электронных кошельков, также называют «хитрыми мультиподписями».

Помимо рассмотренных вариантов практического использования пороговой подписи существует еще один способ ее применения, благодаря которому становится возможным разделить хранилище ключей одного пользователя. Вместо того чтобы размещать секретный ключ на одном компьютере, части ключа находятся на двух устройствах, например, на персональном компьютере и на смартфоне. Для формирования подписи необходимо взаимодействие сразу двух устройств, так как ни одно из них не содержит секретный ключ целиком. Пользователь инициирует транзакцию на компьютере, а затем подтверждает действие с помощью смартфона, после чего формируется пороговая подпись. Чтобы украсть электронные деньги из личного кабинета пользователя, защищенного подобным способом, злоумышленнику придется одновременно перехватить управление сразу двумя устройствами. Такой способ защиты применяют многие крупные компании, занимающиеся электронными денежными транзакциями.

Данное применение пороговой подписи не предполагает наличие других участников схемы – абонент может сам воспользоваться распределенным секретом.

Рассмотрим также такую область применения пороговых подписей, как безопасность мобильных агентов [20]. В последние годы многие исследования были посвящены проблеме безопасности программного обеспечения и данных мобильных агентов, которую обычно разделяют на две части:

- защита платформы, на которой работает мобильный агент, от вредоносного программного обеспечения и несанкционированного доступа;
- защита мобильного агента от вредоносных платформ.

Рассмотрим подробнее вопрос о разделении задачи между несколькими агентами для повышения уровня доверия в коллективных операциях агентов. При установке нового мобильного агента необходимо воспользоваться помощью уже существующих агентов. Их задача – провести исследование в этой области и выяснить, какой агент обладает рациональным соотношением цены и качества. В процессе поиска существует ненулевая вероятность того, что некоторые из запущенных агентов могут подвергнуться изменению вредоносными узлами.

Когда искомое программное обеспечение найдено, пользователю необходимо приобрести его, и тут как раз может быть использована схема пороговой подписи. Пользователь выступает в ней доверенным лицом между мобильными агентами, среди которых происходит разделение секретного ключа. Когда подпись сформирована, пользователь обеспечивает разделение секрета между мобильными агентами. Третье лицо, например, продавец программного обеспечения, получает части подписи и собирает из них действующую подпись. Полученная подпись является эквивалентом подписи пользователя. Это распределение доверия между множеством агентов снижает угрозу от вредоносных узлов, которые могут внести изменения в вычислительные программные части агентов.

Кроме того, пороговые подписи применяются в протоколах электронного голосования, групповой электронной подписи, помехоустойчивом кодировании [6, 20].

Таким образом, пороговые подписи являются развивающимся криптографическим примитивом, применимым во многих сферах деятельности человека. Однако все существующие схемы основаны на зарубежных алгоритмах электронной подписи, поэтому весьма актуальна разработка пороговой схемы подписи для алгоритма ГОСТ Р 34.10-2012.

Заключение

Основными результатами проделанной работы являются следующие:

- систематизированы различные способы формирования и проверки пороговой подписи;
- проанализированы различные виды электронной подписи, приведены иллюстрирующие примеры;
- исследован математический аппарат, положенный в основу различных типов пороговой подписи;
- приведены примеры практического применения схем пороговой подписи.

В рамках дальнейшего исследования по данной тематике предполагается предложить схему пороговой подписи, основанную на российском стандарте ГОСТ Р 34.10-2012, обосновать ее стойкость и разработать программный комплекс, реализующий указанный алгоритм пороговой подписи.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон Российской Федерации от 10.01.2002 № 1-ФЗ (ред. от 08.11.2007) «Об электронной цифровой подписи».
2. Фомичев В.М. Дискретная математика и криптология. М.: Диалог-МИФИ, 2010.
3. Katz J., Lindell Y. Introduction to Modern Cryptography: Principles and Protocols. Berlin: Chapman & Hall, 2007.
4. Смарт Н. Криптография. М.: Техносфера, 2005.
5. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: ГелиосАРВ, 2002.
6. Desmedt Y., Frankel Y. Threshold cryptosystems // Advances in Cryptology–Crypto '89. 1989. P. 307-315.
7. Aboud S.J., AL-Fayoumi M. Efficient Threshold Signature Scheme // International Journal of Advanced Computer Science and Applications. 2012. Vol. 3, No. 1. P. 1-6.
8. ShoupV. PracticalThresholdSignatures // LNCS: Proc. ofEUROCRYPT 2000. 2000. Vol. 1807. P. 207-220.
9. Borselius N., Mitchell C.J., Wilson A. On the value of threshold signatures // Operating Systems Review. 2002. No. 36(4). P. 30-35 (2002).
10. Bozkurt I.N., Kaya K., Selcuk A. Practical Threshold Signatures with Linear Secret Sharing Schemes // Proceedings of the 2nd International Conference on Cryptology in Africa: Progress in Cryptology. 2009. P. 1-12.
11. Hwang M., Chang T.-Y. Threshold Signatures: Current Status and Key Issues // International Journal of Network Security. 2005. Vol.1, No.3. P. 123-137.
12. ElGamal T. A public key cryptosystem and signature scheme based on discrete logarithms // Trans. Inform. Theory. 1985. P. 469-472.
13. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: ИПК «Стандартинформ», 2013.
14. Desmedt Y., Frankel Y. Shared generation of authenticators and signatures // Advances in Cryptology–Crypto'91. 1991. P. 457-469.
15. Архангельская А.В., Запечников С.В. Схемы цифровой подписи на основе алгоритмов ГОСТ 34.10-2001 с применением аппарата парных отображений // Известия ТРТУ. 2006. С. 194-201.
16. Zhang F., Huang X., Mu Y., Susilo W., Zhang L. Certificateless threshold signature scheme from bilinear maps // Information Science. 2010. P. 194-201.
17. Xiong H., Qin Z., Li F. Identity-based Threshold Signature Secure in the Standard Model // International Journal of Network Security. 2010. Vol.10, No.1. P. 75-80.
18. Yang P., Cao Z., Dong X. Efficient certificateless threshold signatures without random oracles //Journal of Systems Science and Complexity. 2010. Vol. 23, No. 6. P. 1167-1182.
19. Li C.M. Threshold multisignature schemes where suspected forgery implies traceability of adversarial shareholders // New York: Advances in Cryptology. 1995. P. 194-204.
20. Borselius, N. On the value of threshold signatures [Text] / N. Borselius, C. J. Mitchell, A. Wilson. London: Mobile VCE Research Group, Information Security Group, 2002. P. 1-6.
21. ParkC., KurosawaK. NewElGamalTypethresholddigitalsignaturescheme // IEICETransFundamentals. 1996. P. 86-93.
22. Li C.M., Hwang T., Lee N.Y. Remark on the threshold RSA signature scheme // Advances in Cryptology. 1994. P. 413-420.
23. Su P.C., Chang Henry K.S., Lu E.H. ID-based threshold digital signature schemes on the elliptic curve discrete logarithm problem // Applied Mathematics and Computation. 2005. Vol. 164, No. 3. P. 757-772.
24. Chen T.S. A specifiable verifier group-oriented threshold signature scheme based on the elliptic curve cryptosystem // Computer Standard & Interfaces. 2004. Vol. 27, No. 1. P. 33-38.
25. Pederson T.P. Non-interactive and information-theoretic secure verifiable secret sharing // Advances in Cryptology. 1992. P. 129-140.
26. Рябко Б.Я., Фионов А.Н. Основы современной криптографии. М.: «Научный Мир», 2004.
27. Crutchfield C., Molnar D., Turner D., Wagner D. Generic On-line/Off-line Threshold Signatures // Public Key Cryptography, LNCS. 2006. Vol. 3958. P. 58-76.
28. Daza V., Herranz J. Some Protocols Useful on the Internet from Threshold Signature Schemes // Int'l J. Information Security. 2004. Vol. 3, No. 2. P. 61-69.
29. Shamir A. Online/Offline Signature Schemes // CRYPTO'01. 2001. P. 355-367.
30. Goldfeder S., Bonneau J., Felten E.W., Kroll J. Securing Bitcoin wallets via threshold signatures // Princeton: Securing e-wallets. 2014. P. 1-11.
31. Sean R. The OceanStore Write Path. New York: Big Data System, 2002. P. 1-20.

REFERENCES:

1. Federal'nyj zakon Rossijskoj Federacii ot 06 aprelia 2011 goda № 63-FZ «Ob jelektronnoj podpisi» (redakcia ot 28.06.2014).
2. FomichevV.M. Diskretnaya matematika i cryptologia. M.: Dialog-MIFI, 2010.
3. Smart N. Cryptographia. M.: Tehnosfera, 2005.
4. A.P., Zubov A.U., Kuz'min A.S., Cheremushkin A.V. Osnovi cryptographii. M.: Gelios ARV, 2002.
5. Katz J., Lindell Y. Introduction to Modern Cryptography: Principles and Protocols. Berlin: Chapman & Hall, 2007.
6. Desmedt Y., Frankel Y. Threshold cryptosystems // Advances in Cryptology–Crypto '89. 1989. P. 307-315.

7. Aboud S.J., AL-Fayoumi M. Efficient Threshold Signature Scheme // International Journal of Advanced Computer Science and Applications. 2012. Vol. 3, No. 1. P. 1-6.
8. Shoup V. Practical Threshold Signatures // LNCS: Proc. Of EUROCRYPT 2000, 2000. Vol. 1807. P. 207-220.
9. Borselius N., Mitchell C.J., Wilson A. On the value of threshold signatures // Operating Systems Review. 2002. No. 36(4). P. 30-35 (2002).
10. Bozkurt I.N., Kaya K., Selcuk A. Practical Threshold Signatures with Linear Secret Sharing Schemes // Proceedings of the 2nd International Conference on Cryptology in Africa: Progress in Cryptology. 2009. P. 1-12.
11. Hwang M., Chang T.-Y. Threshold Signatures: Current Status and Key Issues // International Journal of Network Security. 2005. Vol.1, No.3. P. 123-137.
12. ElGamal T. A public key cryptosystem and signature scheme based on discrete logarithms // Trans. Inform. Theory. – 1985. P. 469-472.
13. GOSTR 34.10-2012. Informacionnaja tehnologija. Kriptograficheskaja zashhita informacii. Processy formirovanija i proverkij elektronnoj cifrovoj podpisi. –M.: IPK «Standartinform», 2013.
14. Desmedt Y., Frankel Y. Shared generation of authenticators and signatures // Advances in Cryptology–Crypto'91. 1991. P. 457-469.
15. Arkhangelskaya A.V., Zapechnikov S.V. Shemi cifrovoi podpisi na osnove algoritmov GOST R 34.10-2001 s primeneniem apparata parnih otobrajenii // Izvestia TRTU. 2006. P. 194-201.
16. Zhang F., Huang X., Mu Y., Susilo W., Zhang L. Certificateless threshold signature scheme from bilinear maps // Information Science. 2010. P. 194-201.
17. Xiong H., Qin Z., Li F. Identity-based Threshold Signature Secure in the Standard Model // International Journal of Network Security. 2010. Vol. 10, No.1. P. 75-80.
18. Yang P., Cao Z., Dong X. Efficient certificateless threshold signatures without random oracles //Journal of Systems Science and Complexity. 2010. Vol. 23, No. 6. P. 1167-1182.
19. Li C.M. Threshold multisignature schemes where suspected forgery implies traceability of adversarial shareholders // New York: Advances in Cryptology. 1995. P. 194-204.
20. Borselius, N. On the value of threshold signatures [Text] / N. Borselius, C. J. Mitchell, A. Wilson. – London: Mobile VCE Research Group, Information Security Group, 2002. P. 1-6.
21. Park C., Kurosawa K. New ElGamal Type threshold digital signature scheme // IEICETransFundamentals. 1996. P. 86-93.
22. LiC. M., Hwang T., Lee N.Y. Remark on the threshold RSA signature scheme // Advances in Cryptology. 1994. P. 413-420.
23. Su P.C., Chang Henry K.S., Lu E.H. ID-based threshold digital signature schemes on the elliptic curve discrete logarithm problem // Applied Mathematics and Computation. 2005. Vol. 164, No. 3. P. 757-772.
24. Chen T.S. A specifiable verifier group-oriented threshold signature scheme based on the elliptic curve cryptosystem // Computer Standard & Interfaces. 2004. Vol. 27, No. 1. P. 33-38.
25. Pederson T.P. Non-interactive and information-theoretic secure verifiable secret sharing // Advances in Cryptology. – 1992. P. 129-140.
26. Ryabko B.Ya., FionovA.N. Osnovi sovremennoy cryptografii. – M.: Nauchniu mir, 2004.
27. Crutchfield C., Molnar D., Turner D., Wagner D. Generic On-line/Off-line Threshold Signatures // Public Key Cryptography, LNCS. 2006. Vol. 3958. P. 58-76.
28. Daza V., Herranz J. Some Protocols Useful on the Internet from Threshold Signature Schemes // Int'l J. Information Security. 2004. Vol. 3, No. 2. P. 61-69,
29. Shamir A. Online/Offline Signature Schemes // CRYPTO'01. 2001. P. 355-367.
30. Goldfeder S., Bonneau J., Felten E.W., Kroll J. Securing Bitcoin wallets via threshold signatures // Princeton: Securing e-wallets.2014. P. 1-11.
31. Sean R. The OceanStore Write Path. New York: Big Data System, 2002. P. 1-20.