МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

На правах рукописи

Бабуева Александра Алексеевна

Свойства безопасности схем подписи вслепую на основе уравнений Шнорра и Эль-Гамаля

2.3.6. Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2025

Диссертация подготовлена на кафедре информационной безопасности факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова.

Научный руководитель — *Смышляев Станислав Витальевич*, доктор физико-математических наук

Официальные оппоненты — *Нестеренко Алексей Юрьевич*, доктор физико-математических наук, ФГАОУ ВО «Национальный исследовательский университет «Высшая школа экономики», профессор кафедры компьютерной безопасности Московского института электроники и математики им. А.Н. Тихонова

— *Запечников Сергей Владимирович*, доктор технических наук, доцент, ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ», профессор кафедры криптологии и кибербезопасности Института интеллектуальных кибернетических систем

— *Коренева Алиса Михайловна*, кандидат физико-математических наук, ООО «Код безопасности», заместитель руководителя службы сертификации по научно-техническому сотрудничеству

Защита диссертации состоится 12 ноября 2025 г. в 16 часов 45 минут на заседании диссертационного совета МГУ.012.3 Московского государственного университета имени М.В. Ломоносова по адресу: 119234, Москва, ГСП-1, Ленинские горы, д. 1, механико-математический факультет, аудитория 1408.

E-mail: vasenin@msu.ru

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ имени М.В. Ломоносова (Ломоносовский просп., д. 27) и на портале: `https://dissovet.msu.ru/dissertation/3533`.

Автореферат разослан «__» _____ 2025 г.

Ученый секретарь
диссертационного совета,
кандидат физико-математических наук А.В. Галатенко

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Диссертационная работа посвящена решению задачи получения обоснованных оценок стойкости для схем подписи вслепую. Схема подписи вслепую представляет собой криптографический механизм, определяемый алгоритмом генерации ключей, протоколом формирования подписи и алгоритмом проверки подписи. Протокол формирования подписи является интерактивным протоколом, выполняемым между подписывающей стороной (сервером) и запрашивающей стороной (пользователем, клиентом). В результате выполнения этого протокола клиент получает подпись для некоторого сообщения, при этом подписывающий не получает информации ни о сообщении, ни о сформированном значении подписи, а клиент не может сформировать корректное значение подписи без взаимодействия с подписывающим.

Актуальность темы. Схемы подписи вслепую применяются в прикладных информационных системах, в которых возникает необходимость одновременного обеспечения целостности данных и невозможности установления связи между конкретными данными и их владельцем. К таким информационным системам относятся, в том числе, системы дистанционного электронного голосования и системы электронных платежей.

Задача получения обоснованных оценок стойкости для схем подписи вслепую является важной для обеспечения защиты информации как с практической, так и с теоретической точки зрения. Так, при использовании таких схем в прикладных системах наличие обоснованных оценок позволяет определять безопасные условия эксплуатации схем, например, возможность параллельного подписания данных различными пользователями или максимальное количество подписей, сформированное с использованием схемы. Задача получения оценок стойкости предполагает исследование комбинаторных и/или алгебраических свойств схем подписи вслепую и получение строгих доказательств в математических моделях безопасности. Под моделью безопасности понимается совокупность угроз (свойств) безопасности и возможностей нарушителя, потенциально доступных ему при использовании криптографического механизма.

Модели безопасности для схем подписи вслепую. Для схем подписи вслепую традиционно рассматривают[1] два целевых свойства безопасности: свойство неотслеживаемости и свойство неподделываемости. Определим каждое из них, задав соответствующие модели безопасности.

При рассмотрении свойства неотслеживаемости предполагается, что нарушитель может выступать в роли подписывающего и (в зависимости от определения конкретной модели безопасности) обладать или не обладать следующими возможностями: генерировать ключ подписи произвольным образом, навязывать клиенту сообщения для подписи, узнавать о факте завершения протокола с ошибкой в качестве выходного результата на стороне клиента. В качестве угрозы рас-

[1] Juels A., Luby M., Ostrovsky R. Security of blind digital signatures //Annual International Cryptology Conference. – Springer, Berlin, Heidelberg, 1997. – С. 150-164.

сматривается факт получения нарушителем в результате выполнения протокола формирования подписи нетривиальной информации о паре (сообщение, подпись), сформированной на стороне клиента.

При рассмотрении свойства неподделываемости предполагается, что нарушитель может выступать в роли клиента и (в зависимости от определения конкретной модели безопасности) обладать или не обладать возможностью начинать выполнение новых сеансов протокола формирования подписи вслепую до завершения предыдущих (т.е. проводить так называемую атаку с параллельными сеансами). В качестве угрозы рассматривается факт формирования нарушителем подделки. Так же как и для классических схем подписи, для схем подписи вслепую различают свойство сильной неподделываемости (задача нарушителя — сформировать новую пару (сообщение, подпись)) и слабой неподделываемости (задача нарушителя — сформировать подпись для нового сообщения).

Модели безопасности, описывающие свойства неотслеживаемости и неподделываемости для схем подписи вслепую и предоставляющие нарушителю все указанные выше возможности, далее будем называть *расширенными моделями безопасности.*

Выбор модели безопасности для анализа стойкости конкретной схемы подписи вслепую определяется условиями ее эксплуатации, т.е. особенностями той прикладной системы, в рамках которой будет использоваться соответствующая схема. Большой интерес представляют схемы подписи вслепую, стойкие (при некоторых предположениях) в расширенных моделях безопасности, поскольку они предъявляют наименьшее число требований к высокоуровневой прикладной системе.

Вместе с тем некоторые прикладные системы предъявляют к используемым криптографическим механизмам (в том числе схемам подписи вслепую) специфичные требования. При этом соотношение данных требований с обеспечением стойкости в расширенных моделях безопасности зачастую является открытым вопросом. Одним из важных классов таких систем являются системы формирования подписи в условиях, когда ключ подписи хранится на функциональном ключевом носителе (смарт-карте). Для такого типа прикладных систем были введены и математически строго описаны[2] два типа нарушителей: внешний нарушитель и нарушитель с агентом. Задача обеспечения защиты от подделки подписи такими нарушителями может быть решена, в частности, за счет использования классических схем подписи с дополнительными свойствами или схем подписи вслепую. Модели безопасности, описывающие соответствующие свойства схем подписи и схем подписи вслепую, далее будем называть *специализированными моделями безопасности.*

Формализация целевой модели безопасности заключается в формировании строгих определений безопасности путем моделирования возможностей нарушителя по взаимодействию с механизмом, целей нарушителя и его ресурсов. В рамках диссертации применяется алгоритмический подход на основе экспери-

[2]Алексеев Е. К. , Ахметзянова Л. Р., Божко А. А., Смышляев С. В. «Безопасная реализация электронной подписи с использованием слабодоверенного вычислителя», Матем. вопр. криптогр., 12:4 (2021), 5–23.

ментатора[3], заключающийся в построении вероятностного интерактивного алгоритма, моделирующего работу схемы в присутствии нарушителя, и определении количественной характеристики успешности нарушителя по реализации угрозы — преимущества нарушителя. Отметим, что алгоритм работы экспериментатора не зависит от конкретного алгоритма работы нарушителя. Задача получения обоснованной оценки стойкости схемы подписи вслепую в конкретной модели безопасности в рамках используемого подхода сводится либо к предъявлению конкретного алгоритма работы нарушителя с заданными ограничениями, реализующего целевую угрозу в данной модели безопасности, и оценке снизу величины его преимущества (верхняя оценка стойкости схемы в данной модели безопасности), либо к получению верхней оценки величины преимущества для любого нарушителя с заданными ограничениями в данной модели безопасности (нижняя оценка стойкости схемы в данной модели безопасности). Верхняя оценка величины преимущества нарушителя в конкретной модели безопасности в общем случае представляет собой функцию от параметров схемы и преимуществ нарушителей в моделях безопасности для некоторых базовых примитивов, на основе которых построена схема.

Существующие схемы подписи вслепую. В основе стойкости существующих схем подписи вслепую могут лежать различные вычислительно трудные задачи. Так, самой первой и широко используемой на практике схемой является схема подписи вслепую Шаума[4], стойкость которой основана на сложности задачи факторизации. Известно также большое количество схем на основе решеток, изогений и других базовых примитивов. С точки зрения практики большой интерес представляет изучение схем подписи вслепую, использующих в качестве базового блока группу точек эллиптической кривой. Это обуславливается тем, что задача дискретного логарифмирования в группе точек эллиптической кривой является одной из наиболее изученных и надежных в мировом криптографическом сообществе. Более того, все отечественные стандартизированные на настоящий момент высокоуровневые асимметричные криптографические механизмы построены именно на основе эллиптических кривых.

Как показывает история анализа схем подписи вслепую, задача синтеза стойкой схемы на основе эллиптических кривых является вовсе не тривиальной. Как и в случае классических схем подписи, большинство схем подписи вслепую на основе эллиптических кривых построены на основе одного из двух уравнений подписи (или их незначительных модификаций):

- уравнение Шнорра[5];
- уравнение Эль-Гамаля[6].

[3]Bellare M., Rogaway P. «The security of triple encryption and a framework for code-based game-playing proofs» // Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 409–426. Springer, Berlin, Heidelberg, 2006.

[4]Chaum D. «Blind signatures for untraceable payments» //Advances in cryptology. – Springer, Boston, MA, 1983. – С. 199–203.

[5]Schnorr C. P. «Efficient identification and signatures for smart cards» //Conference on the Theory and Application of Cryptology. – Springer, New York, NY, 1989. – С. 239-252.

Схемы обоих типов требуют осуществления как минимум трех пересылок между подписывающей и запрашивающей стороной в процессе формирования подписи. Поэтому при рассмотрении свойства неподделываемости для этих схем в общем случае необходимо учитывать в том числе возможность нарушителя проводить атаку с параллельными сеансами. Анализ безопасности относительно этой возможности приводит к интересным результатам[7]: необходимым условием стойкости ряда схем подписи вслепую на основе уравнений Шнорра и Эль-Гамаля, в отличие от классических схем подписи Шнорра и Эль-Гамаля, является сложность новых нестандартных задач в группе точек эллиптической кривой. Диссертационная работа посвящена методам получения обоснованных оценок стойкости для схем подписи вслепую такого типа.

Схемы подписи вслепую на основе уравнения Шнорра. Классической схемой подписи вслепую на основе уравнения Шнорра является схема подписи вслепую Шнорра[8], предложенная в 1996 году. Анализ стойкости этой схемы был проведен Шнорром[7] в 2001 году. Свойство неподделываемости (сильной неподделываемости в модели с параллельными сеансами) было доказано в предположении сложности задачи ROS[7] (Random inhomogeneities in a Overdetermined Solvable system of linear equations) относительно ограниченного множества нарушителей (в генерической модели[9] со случайным оракулом[10]). Позже в 2020 году было построено доказательство[11] свойства неподделываемости относительно более широкого множества нарушителей (в модели с алгебраической группой [12] и случайным оракулом) в предположении сложности задач ROS и OMDL[13] (One-More Discrete Logarithm).

Задача ROS на протяжении 20 лет считалась сложной. В 2002 году она была сведена к обобщенной задаче дней рождения[14], для решения которой может быть использован алгоритм Вагнера[14] с субэкспоненциальной сложностью. В 2020 году был предложен полиномиальный алгоритм[15] решения этой задачи, который

---

[6]Harn L., Xu Y. «Design of generalised ElGamal type digital signature schemes based on discrete logarithm» // Electronics Letters, 30(24), pp. 2025–2026, 1994.

[7]Schnorr C.-P. «Security of blind discrete log signatures against interactive attacks» // In Sihan Qing, Tatsuaki Okamoto, and Jianying Zhou, editors, ICICS 01, volume 2229 of LNCS, pages 1–12. Springer, Heidelberg, November 2001.

[8]Pointcheval D., Stern J. «Provably secure blind signature schemes». Advances in Cryptology — ASIACRYPT'96, volume 1163, pages 252–265. Springer-Verlag, 1996.

[9]Nechaev V. I.«Complexity of a determinate algorithm for the discrete logarithm» //Mathematical Notes, 55(2):165–172, 1994.

[10]Bellare M., Rogaway P. «Random oracles are practical: A paradigm for designing efficient protocols»// In Proceedings of the 1st ACM conference on Computer and communications security, pp. 62–73. 1993.

[11]Fuchsbauer G., Plouviez A., Seurin Y. «Blind Schnorr signatures and signed ElGamal encryption in the algebraic group model» //Annual International Conference on the Theory and Applications of Cryptographic Techniques. – Springer, Cham, 2020. – С. 63-95.

[12]Fuchsbauer G., Kiltz E., Loss J. «The Algebraic Group Model and its Applications». In: Shacham H., Boldyreva A. (eds) Advances in Cryptology – CRYPTO 2018. CRYPTO 2018. Lecture Notes in Computer Science, vol 10992. Springer, Cham. 2018.

[13]Bellare M. et al. «The One-More-RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme» //Journal of Cryptology. – 2003. – Т. 16. – №. 3.

[14]Wagner D. «A generalized birthday problem». In Moti Yung, editor, CRYPTO 2002, volume 2442 of LNCS, pages 288–303. Springer, Heidelberg, August 2002.

позволил построить полиномиальную атаку, приводящую к нарушению свойства неподделываемости для схемы подписи вслепую Шнорра в случае, если нарушитель имеет возможность открыть $\ell \geqslant \lceil \log q \rceil$ параллельных сеансов протокола формирования подписи с подписывающим, где q — простой порядок подгруппы группы точек эллиптической кривой.

Оказалось[15], что аналогичная атака применима не только к схеме подписи вслепую Шнорра, но и к ряду других схем на основе эллиптических кривых: схеме Окамото-Шнорра[16], схеме Абе[17], обеспечивающей частичную неотслеживаемость, а также схеме Брандса[18], используемой в системе подтверждения персональных данных без их разглашения (anonymous credentials) U-Prove[19]. При этом для схемы Брандса атака позволяет строить подделки только при некоторых ограничениях на подписываемые в рамках атаки сообщения (для их формирования должен использоваться один и тот же «номер аккаунта» пользователя). Схема Брандса, в свою очередь, построена на основе схемы подписи вслепую Шаума-Педерсена[20]. Для схемы Шаума-Педерсена в литературе не представлено ни атак, ни строгого математического обоснования свойства неподделываемости, поэтому вопрос ее стойкости в расширенных моделях безопасности оставался открытым. Таким образом, актуальной задачей является получение верхних и/или нижних оценок стойкости этой схемы.

С момента публикации ROS атаки в литературе было предложено несколько схем подписи вслепую на основе уравнения Шнорра, для которых данная атака неприменима. Первым примером такой схемы является схема Clause Blind Schnorr[21], предложенная в 2020 году. Свойство неподделываемости для этой схемы обосновано в модели с алгебраической группой и случайным оракулом в предположении сложности задач OMDL и MROS (Modified ROS problem). Однако задача MROS введена только в 2020 году и почти не изучена, для нее отсутствуют нижние оценки трудоемкости ее решения. Позже в 2022 году была предложена схема подписи вслепую Tessaro-Zhu[22]. Авторы этой схемы предложили мо-

[15]Benhamouda F, Lepoint T., Loss J., Orru M., Raykova M. «On the (in)security of ROS»// Annual International Conference on the Theory and Applications of Cryptographic Techniques. – Cham : Springer International Publishing, 2021. – С. 33-53.

[16]Pointcheval D., Stern J. «Security arguments for digital signatures and blind signatures». Journal of Cryptology, 13(3):361–396, June 2000.

[17]Abe M., Okamoto T. Provably secure partially blind signatures // Advances in Cryptology — CRYPTO 2000, Springer, Berlin, Heidelberg, pp. 271–286, 2000.

[18]Brands S. Untraceable off-line cash in wallet with observers //Advances in Cryptology—CRYPTO'93: 13th Annual International Cryptology Conference Santa Barbara, California, USA August 22–26, 1993 Proceedings 13. – Springer Berlin Heidelberg, 1994. – С. 302-318.

[19]Paquin C., Zaverucha G. U-Prove Cryptographic Specification. V. 1.1. Microsoft Corporation. 2013. `https://www.microsoft.com/en-us/research/publication/u-prove-cryptographic-specification-v1-1-revision-3/`

[20]Chaum D., Pedersen T. P. «Wallet databases with observers». //Annual international cryptology conference. – Springer, Berlin, Heidelberg, 1992. – С. 89–105.

[21]Fuchsbauer G., Plouviez A., Seurin Y. «Blind Schnorr signatures and signed ElGamal encryption in the algebraic group model» //Annual International Conference on the Theory and Applications of Cryptographic Techniques. – Springer, Cham, 2020. – С. 63-95.

[22]Tessaro S., Zhu C. «Short pairing-free blind signatures with exponential security». Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cham, Springer International Publishing,

дифицировать уравнение подписи Шнорра путем добавления в него еще одного случайного элемента для защиты от атак типа ROS. Свойство неподделываемости этой схемы математически строго обосновано в модели с алгебраической группой и случайным оракулом в предположении сложности задачи дискретного логарифмирования. Более того, в 2023 году была предложена пороговая схема подписи вслепую Snowblind[23], которая построена на основе схемы Tessaro-Zhu и позволяет уменьшить размер подписи (даже в случае одного подписывающего), свойство неподделываемости этой схемы было обосновано в тех же предположениях, что и для схемы Tessaro-Zhu. Наконец, в том же году была предложена схема подписи вслепую[24], которая построена на основе схемы Tessaro-Zhu и для которой удалось обосновать свойство неподделываемости в предположении сложности задачи CDH (Computational Diffie-Hellman) в модели со случайным оракулом, т.е. без использования модели с алгебраической группой. Также можно отметить схему подписи вслепую Абе[25] на основе уравнения Шнорра, предложенную в 2001 году. Для этой схемы ROS атака также оказалась неприменимой, однако обоснование стойкости этой схемы, представленное в оригинальной работе, содержало ошибки. Более того, исправленное обоснование[26], предложенное в 2020 году, также содержит ошибки, что подтверждают сами авторы доказательства.

Схемы на основе уравнения Эль-Гамаля. В литературе известно большое количество схем подписи вслепую[27,28,29,30,31,32,33,34,35,36,37], в основе которых лежит уравнение Эль-Гамаля. Однако ни для одной из этих схем авторами не было

pp. 782–811, 2022.

[23]Crites, E., Komlo, C., Maller, M., Tessaro, S., Zhu, C. «Snowblind: A Threshold Blind Signature in Pairing-Free Groups»// In Annual International Cryptology Conference (pp. 710-742). Cham: Springer Nature Switzerland. 2023.

[24]Chairattana-Apirom R., Tessaro S., Zhu C. «Pairing-Free Blind Signatures from CDH Assumptions» //Cryptology ePrint Archive, Paper 2023/1780, 2023.

[25]Abe M. «A secure three-move blind signature scheme for polynomially many signatures» //International Conference on the Theory and Applications of Cryptographic Techniques. – Springer, Berlin, Heidelberg, 2001. – С. 136-151.

[26]Kastner J., Loss J., Xu J. «On Pairing-Free Blind Signature Schemes in the Algebraic Group Model» //Cryptology ePrint Archive. – 2020. – Т. 2020. – №. 1071.

[27]Camenisch J. L., Piveteau J. M., Stadler M. A. «Blind signatures based on the discrete logarithm problem» //Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1994. pp. 428–432.

[28]Gorbenko I., Yesina M., Ponomar V. «Anonymous electronic signature method» //2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T). – IEEE, 2016. – С. 47-50.

[29]Jena D., Panigrahy S. K., Acharya B., Jena S. K. A Novel ECDLP-Based Blind Signature Scheme //National Conference on Information Security – Issues & Challenges, NCISIC 08, pp. 37–40, 2008.

[30]Khater M. M., Al-Ahwal A., Selim M. M., Zayed H. H. New Blind Signature Scheme Based on Modified ElGamal Signature for Secure Electronic Voting // International Journal of Scientific & Engineering Research, 9(3), pp. 917–921, 2018.

[31]Moldovyan N.A. «Blind Signature Protocols from Digital Signature Standards». International Journal of Network Security, Vol.13, No.1, PP.22–30, July 2011.

[32]Ростовцев А. Г. «Подпись «вслепую» на эллиптической кривой для электронных денег» //Проблемы информационной безопасности. Компьютерные системы. – 2000. – №. 1. – С. 40-45.

[33]Shen, V. R., Chung, Y. F., Chen, T. S., Lin, Y. A. A blind signature based on discrete logarithm problem // International Journal of Innovative Computing, Information and Control, 7(9), pp. 5403–5416, 2011.

представлено математически строгое обоснование свойства неподделываемости. Единственным исключением является схема YL19[34]. Для этой схемы было математически строго обосновано свойство неподделываемости в модели с параллельными сеансами относительно ограниченного множества нарушителей. Однако настоящая схема представляет меньший интерес с точки зрения задачи синтеза схемы подписи на основе группы точек эллиптической кривой, поскольку для обеспечения неотслеживаемости она использует механизм неинтерактивного доказательства с нулевым разглашением, стойкость которого основана на сложности решения задачи факторизации.

Вместе с тем для схем, построенных на основе только группы точек эллиптической кривой, неизвестно каких-либо атак, позволяющих нарушить свойство неподделываемости. Таким образом, актуальной задачей является получение верхних и/или нижних оценок стойкости данных схем.

Цель диссертационной работы — построение новых математических методов получения обоснованных оценок стойкости схем подписи вслепую на основе уравнений Шнорра и Эль-Гамаля.

Для достижения поставленной цели были решены следующие задачи.

1) Разработка методов получения оценок стойкости схемы подписи вслепую Шаума-Педерсена в расширенных моделях безопасности.

2) Разработка методов получения оценок стойкости схем подписи вслепую на основе уравнения Эль-Гамаля в расширенных моделях безопасности.

3) Разработка методов получения оценок стойкости схем подписи и схем подписи вслепую на основе уравнения Эль-Гамаля в специализированных моделях безопасности, актуальных для систем формирования подписи в условиях использования функциональных ключевых носителей.

Научная новизна. В диссертации получены следующие новые результаты.

1) Для схемы подписи вслепую Шаума-Педерсена разработан метод нарушения свойства сильной неподделываемости в модели с параллельными сеансами и доказана содержательная верхняя оценка преимущества нарушителя, реализующего угрозу нарушения свойства слабой неподделываемости в модели с параллельными сеансами. Полученные результаты демонстрируют,

[34]Yi X., Lam K. Y. «A new blind ECDSA scheme for bitcoin transaction anonymity» //Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security. – 2019. – С. 613-620.

[35]Tan D. N., Nam H. N., Van H. N., Thi, L. T., Hieu M. N. New blind mutisignature schemes based on signature standards // 2017 International Conference on Advanced Computing and Applications (ACOMP), IEEE, pp. 23–27, 2017.

[36]Tan D. N., Nam H. N., Hieu M. N., Van H. N «New blind muti-signature schemes based on ECDLP» //International Journal of Electrical and Computer Engineering. – 2018. – Т. 8. – №. 2. – С. 1074.

[37]Zhang Y., He D., Zhang F., Huang X., Li D. An efficient blind signature scheme based on SM2 signature algorithm //LNCS, 12612. International Conference on Information Security and Cryptology, Springer, Cham, pp. 368–384, 2020.

что схема Шаума-Педерсена не обеспечивает стойкость в наиболее сильной расширенной модели безопасности, при этом в основе стойкости схемы в более слабой расширенной модели безопасности лежит новая нестандартная задача в группе точек эллиптической кривой.

2) Синтезирован класс схем подписи вслепую на основе уравнения Эль-Гамаля, не использующих дополнительные криптографические механизмы, покрывающий все существующие схемы такого типа. Для существенной части схем из этого класса разработан метод нарушения свойства неподделываемости в модели с параллельными сеансами. Среди оставшихся схем выявлен подкласс схем, для которых разработан метод нарушения одного из свойств: свойства неподделываемости в модели с последовательными сеансами или свойства неотслеживаемости. Построенные методы демонстрируют, что все существующие схемы подписи вслепую на основе уравнения Эль-Гамаля не обеспечивают стойкость в расширенных моделях безопасности.

3) Разработан метод модификации схемы подписи Эль-Гамаля, позволяющий уменьшить размер подписи на четверть и обеспечить безопасность в условиях использования недоверенного датчика случайных чисел при формировании подписи. Для модифицированной схемы доказана содержательная верхняя оценка величины преимущества нарушителя в специализированной модели безопасности, предоставляющей нарушителю возможность выбирать случайные значения, используемые в процессе формирования подписи.

4) Для схем подписи вслепую на основе уравнения Эль-Гамаля доказаны содержательные верхние оценки преимущества нарушителя в специализированных моделях безопасности, актуальных в системах формирования подписи в условиях использования функциональных ключевых носителей.

Положения, выносимые на защиту.

1) Метод нарушения свойства сильной неподделываемости схемы Шаума-Педерсена в модели с параллельными сеансами.

2) Нижняя оценка стойкости схемы Шаума-Педерсена в модели, учитывающей свойство слабой неподделываемости и атаку с параллельными сеансами.

3) Методы нарушения свойств неподделываемости и неотслеживаемости схем подписи вслепую на основе уравнения Эль-Гамаля.

4) Нижняя оценка стойкости модифицированной схемы подписи Эль-Гамаля в специализированной модели безопасности, актуальной в системах формирования подписи в условиях использования функциональных ключевых носителей.

5) Нижние оценки стойкости схем подписи вслепую на основе уравнения Эль-Гамаля в специализированных моделях безопасности, актуальных в системах формирования подписи в условиях использования функциональных ключевых носителей.

Методология и методы исследования. В рамках исследования применяется математический аппарат и подходы различных разделов математики, таких как теория вероятностей, линейная алгебра, теория сложности вычислений.

Степень достоверности. Достоверность полученных результатов обеспечивается строгими математическими доказательствами утверждений. Результаты опубликованы в открытой печати и прошли апробацию на международных и всероссийских конференциях и научно-исследовательских семинарах.

Результаты других авторов, упомянутые в тексте диссертации, отмечены соответствующими ссылками.

Соответствие диссертации паспорту научной специальности. Тема, объект и предмет исследований диссертации соответствуют паспорту специальности 2.3.6 (физико-математические науки) по следующим областям исследования:

1. теория и методология обеспечения информационной безопасности и защиты информации;

9. модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности;

10. модели и методы оценки защищенности информации и информационной безопасности объекта;

15. принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности;

19. исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.

Апробация работы. Результаты, полученные в диссертационной работе, докладывались на международных и всероссийских конференциях и научно-исследовательских семинарах:

- XVI международной научно-практической конференции «Современные информационные технологии и ИТ-образование», Москва, 25–27 ноября 2021 года;

- семинаре «Математические методы криптографического анализа» кафедры информационной безопасности факультета вычислительной математики и

кибернетики Московского государственного университета им. М.В. Ломоносова под руководством Логачева О.А., Смышляева С.В., Алексеева Е.К., 2022 год;

- XI международной научной конференции «Современные тенденции в криптографии» (CTCrypt 2022), Новосибирск, 6–9 июня 2022 года;
- XII международной научной конференции «Современные тенденции в криптографии» (CTCrypt 2023), Волгоград, 6–9 июня 2023 года;
- XIII международной научной конференции «Современные тенденции в криптографии» (CTCrypt 2024), Петрозаводск, 3–6 июня 2024 года.

Публикации по теме исследования. Результаты работы изложены в 5 публикациях общим объемом 4,6 п.л. в рецензируемых журналах. Из них 4, общим объемом 4,2 п.л., — в журналах, индексируемых в базе ядра Российского индекса научного цитирования «eLibrary Science Index», рекомендованных для защиты в диссертационном совете МГУ имени М.В. Ломоносова по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Теоретическая значимость. В ходе исследования получены результаты, существенно развивающие математические методы, применяемые при синтезе и анализе схем подписи вслепую.

При анализе схемы подписи вслепую Шаума-Педерсена были выявлены особенности способа маскирования сообщений для защиты от атак с параллельными сеансами и развиты математические методы обоснования оценок стойкости на основе матричного анализа. Также была выявлена новая задача в группе точек эллиптической кривой, сложность которой является достаточным условием обеспечения схемой свойства слабой неподделываемости, и установлена ее связь с другими существующими задачами.

Для схем подписи вслепую на основе уравнения Эль-Гамаля были изучены свойства базовых уравнений, а также способ выработки первой компоненты подписи и их влияние на обеспечение схемой подписи вслепую целевых свойств безопасности. Были выделены условия, которым должна удовлетворять схема подписи вслепую такого типа (в частности, конкретный вид уравнения подписи), чтобы потенциально обеспечивать стойкость в расширенных моделях безопасности. Данные условия могут быть использованы при синтезе новых схем подписи вслепую. Кроме того, доказана связь между специализированными моделями безопасности, релевантными при анализе систем формирования подписи в условиях использования функциональных ключевых носителей, с известными в литературе моделями безопасности для схем подписи вслепую.

Практическая значимость. Результаты диссертации использовались при выборе стандартизируемой в Российской Федерации схемы подписи вслепую.

Так, схемы подписи вслепую на основе уравнения Эль-Гамаля и схема Шаума-Педерсена были исключены из рассмотрения в силу разработанных в диссертационной работе методов нарушения свойств неподделываемости и/или неотслеживаемости для этих схем.

Внедрение схем подписи вслепую на основе уравнения Эль-Гамаля в прикладные системы формирования подписи, предполагающие хранение ключа подписи на смарт-карте, позволяет повысить защищенность данных систем относительно внешнего нарушителя и нарушителя с агентом. При этом полученная нижняя оценка стойкости в специализированных моделях безопасности позволяет выбрать безопасные значения параметров эксплуатации схемы подписи вслепую без проведения дополнительных исследований.

Структура и объем диссертации. Диссертационная работа состоит из введения, двух вспомогательных разделов, трех глав, заключения и списка литературы из 91 наименования. Работа изложена на 120 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во Введении обоснована актуальность темы диссертации, сформулированы цели и задачи исследований, отражены научная новизна, теоретическая и практическая значимость полученных результатов, представлены основные результаты, которые выносятся на защиту.

В разделе Обозначения, определения и общие сведения вводятся используемые в работе общие обозначения и определения, а также описываются базовые понятия алгоритмического подхода к формализации моделей безопасности. В рамках этого подхода формально вводятся объекты «нарушитель $\mathcal{A}$» и «экспериментатор **Exp**» — пара вероятностных интерактивных алгоритмов, взаимодействующих друг с другом определенным образом и моделирующих функционирование схемы в условиях присутствия нарушителя. Вводится понятие «преимущество нарушителя Adv» как мера успешности нарушителя по реализации угрозы.

Раздел Модели безопасности для схем подписи вслепую посвящен описанию известных в литературе моделей безопасности для схем подписи вслепую и их формализации. Для каждого из целевых свойств безопасности подробно рассматриваются особенности формирования модели нарушителя и модели угроз.

Для свойства неотслеживаемости определяются различные типы атаки (модели нарушителя) в зависимости от возможности нарушителя контролировать процесс генерации ключей, навязывать клиенту сообщения для подписи, а также получать информацию об ошибках в процессе формирования подписи. Математически строго определяется расширенная модель безопасности Blind (Blindness) для свойства неотслеживаемости, которая предоставляет нарушителю возможность генерировать ключи произвольным образом, навязывать клиенту сообщения для подписи и узнавать информацию о номере взаимодействия, завершившегося с ошибкой. Кроме того, формально определяется более слабая модель

HS-Blind (Honest-Signer Blindness), которая отличается от модели Blind следующим образом: нарушитель не имеет возможности влиять на процесс генерации ключей, а также не получает информацию о номере взаимодействия, завершившегося с ошибкой. В качестве угрозы в обеих моделях рассматривается факт получения нарушителем нетривиальной информации о паре (сообщение, подпись), сформированной в результате взаимодействия с честным пользователем. Данная угроза формализуется через задачу различения бита в соответствующем эксперименте[38].

Для свойства неподделываемости модель угрозы определяется с помощью понятия «еще одной подделки». Задача нарушителя состоит в создании $(\ell + 1)$ корректной пары (сообщение, подпись) в результате ℓ успешных взаимодействий с подписывающим. Под успешным взаимодействием понимается конкретный сеанс протокола формирования подписи, завершившийся с выходным результатом 1 на стороне подписывающего. В зависимости от ограничений, накладываемых на сформированные нарушителем пары, вводятся две различные угрозы: сильная неподделываемость (все пары должны быть различными) и слабая неподделываемость (все сообщения должны быть различными). Для данного свойства определяются также различные модели нарушителя в зависимости от возможности нарушителя осуществлять атаку с последовательными или с параллельными сеансами. Поскольку нарушитель выступает в роли клиента, он в том числе имеет возможность не завершать выполнение сеансов протокола формирования подписи. Математически строго определяется расширенная модель безопасности UF (UnForgeability) для свойства неподделываемости, рассматривающая угрозу нарушения сильной неподделываемости при атаке с параллельными сеансами. Экспериментатор в этой модели не контролирует порядок осуществления запросов на подпись нарушителем, т.е. позволяет начинать новый сеанс протокола формирования подписи в произвольный момент времени, в том числе до завершения предыдущих сеансов. Кроме того, формально определяются более слабые модели, модель SEQ-UF (SEQuential UnForgeability) и модель wUF (weak UnForgeability), отличающиеся от модели UF следующим образом. В модели SEQ-UF нарушителю предоставляется возможность осуществлять атаку только с последовательными сеансами, в модели wUF рассматривается угроза нарушения слабой неподделываемости.

Глава 1 посвящена анализу безопасности схемы подписи вслепую Шаума-Педерсена. В разделе 1.1 приводится описание схемы для группы точек эллиптической кривой.

В разделе 1.2 приведены результаты анализа схемы Шаума-Педерсена с точки зрения обеспечения схемой свойства сильной неподделываемости в модели с параллельными сеансами (модель UF). Разработан конкретный метод нарушения свойства сильной неподделываемости с вероятностью близкой к 1 в результате открытия $\ell \geqslant \lceil \log q \rceil$ параллельных сеансов с подписывающим (раздел 4 [4], теорема 1.2.1 в диссертации). В результате применения этого метода нарушитель

[38]Juels A., Luby M., Ostrovsky R. Security of blind digital signatures //Annual International Cryptology Conference. – Springer, Berlin, Heidelberg, 1997. – С. 150-164.

предъявляет подделку для сообщения, ранее подписываемого в результате легитимного взаимодействия с подписывающим. Вместе с тем конструкция схемы Шаума-Педерсена не позволяет обобщить данный метод на случай построения подделки для нового, ранее не подписываемого сообщения.

В разделе 1.3 приведены результаты анализа схемы Шаума-Педерсена с точки зрения обеспечения схемой свойства слабой неподделываемости в модели с параллельными сеансами (модель wUF). С помощью техники сведений удалось доказать, что достаточным условием стойкости схемы в модели wUF с алгебраической группой и случайным оракулом является сложность решения двух задач: задачи REPR и SOMDL (теорема 1 [4], теорема 1.3.1 в диссертации). Модель с алгебраической группой накладывает следующее требование на алгоритм нарушителя: для любого элемента группы, который появляется на выходе алгоритма нарушителя в процессе его работы, нарушитель должен предоставить коэффициенты разложения этого элемента в линейную комбинацию всех элементов, пришедших ему на вход к текущему моменту. Модель со случайным оракулом предполагает, что вместо хэш-функции в исследуемой схеме используется случайная функция. При инициализации эксперимента экспериментатор выбирает эту функцию равновероятно и независимо из множества всех функций с соответствующими областями определения и значения, после чего предоставляет нарушителю доступ к ней как к «черному ящику». Задача REPR является модификацией задачи «Representation», определенной в работе Брандса[39], ее сложность также является необходимым условием стойкости схемы Шаума-Педерсена. Задача SOMDL является новой задачей, определенной для группы точек элиптической кривой. Доказано, что настоящая задача не сложнее задачи OMDL[40] и задачи SDL[41] (альтернативное название — задача q-dlog). Для задачи SDL доказано также, что ее сложность является необходимым условием стойкости схемы Шаума-Педерсена.

Таким образом, безопасное применение схемы Шаума-Педерсена потенциально возможно только в прикладных информационных системах, в которых обеспечивается уникальность подписываемых сообщений. При этом нижняя оценка стойкости схемы в таких условиях (в модели безопасности wUF) существенно зависит от нижней оценки трудоемкости решения новой нестандартной задачи SOMDL, а потому может быть существенно понижена в будущем. В силу того, что схема Шаума-Педерсена не обеспечивает стойкость в наиболее сильной расширенной модели безопасности, настоящая схема была исключена из рассмотрения в процессе выбора перспективной схемы подписи вслепую для стандартизации в Российской Федерации.

В Главе 2 представлены результаты, обосновывающие невозможность по-

[39]Brands S. Untraceable off-line cash in wallet with observers //Advances in Cryptology—CRYPTO'93: 13th Annual International Cryptology Conference Santa Barbara, California, USA August 22–26, 1993 Proceedings 13. – Springer Berlin Heidelberg, 1994. – С. 302-318.

[40]Bellare M. et al. «The One-More-RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme» //Journal of Cryptology. – 2003. – Т. 16. – №. 3.

[41]Bauer B., Fuchsbauer G., Loss J. «A classification of computational assumptions in the algebraic group model» //Annual International Cryptology Conference. – Cham: Springer International Publishing, 2020. – С. 121-151.

строения стойкой в расширенных моделях безопасности схемы подписи вслепую на основе уравнения Эль-Гамаля. В разделе 2.1 вводится общий вид классической схемы подписи семейства Эль-Гамаля, а также определяются допустимые виды уравнений подписи.

В разделе 2.2 для трех схем подписи вслепую на основе уравнения Эль-Гамаля (GYP16[42], R00[43], TNHV18[44]) разработаны конкретные методы нарушения свойства неотслеживаемости с вероятностью близкой к 1 в результате только одного выполнения протокола формирования подписи (раздел 3 [2]). Данные методы могут быть применены сторонним пассивным нарушителем, не выступающим в роли подписывающего, т.е. даже в самых слабых моделях безопасности для свойства неотслеживаемости.

В разделе 2.3 определяется новый класс схем подписи вслепую — схемы подписи вслепую Эль-Гамаля GenEG-BS. Серверная сторона протокола формирования подписи в таких схемах зафиксирована и представляет собой классический алгоритм подписи Эль-Гамаля для маскированного хэш-значения сообщения e, сформированного пользователем произвольным образом. Введенная конструкция покрывает все существующие схемы на основе уравнения Эль-Гамаля за исключением схемы YL19[45], в которой алгоритм работы сервера включает в том числе проверку доказательства с нулевым разглашением.

Для введенного класса схем GenEG-BS в разделе 2.4 исследуется вопрос их стойкости в расширенных моделях безопасности. Все схемы класса GenEG-BS разделяются на два типа в зависимости от вида уравнения подписи. Для схем первого типа разработан метод нарушения свойства неподделываемости в модели UF с вероятностью близкой к 1 в результате открытия $\ell \geqslant \lceil \log q \rceil$ параллельных сеансов с подписывающим (теорема 1 [1], теорема 2.4.1 в диссертации). Среди схем второго типа выделен подкласс схем, в которых зафиксирован способ выработки пользователем первой компоненты подписи r'. Все известные в литературе схемы GenEG-BS второго типа лежат в этом подклассе. Схемы из этого подкласса также разделены на два вида в зависимости от способа маскирования первой компоненты подписи и хэш-значения. Для первого вида схем разработан метод нарушения свойства неотслеживаемости в модели Blind с вероятностью близкой к 1 в результате выполнения одного протокола формирования подписи с честным пользователем (теорема 2 [1], теорема 2.4.2 в диссертации). Для второго вида схем разработан метод нарушения свойства неподделываемости в модели SEQ-UF с вероятностью близкой к 1 в результате выполнения одного протокола формирования подписи с честным подписывающим (теорема 3 [1], теорема 2.4.3

[42]Gorbenko I., Yesina M., Ponomar V. «Anonymous electronic signature method» //2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T). – IEEE, 2016. – С. 47-50.

[43]Ростовцев А. Г. «Подпись «вслепую» на эллиптической кривой для электронных денег» //Проблемы информационной безопасности. Компьютерные системы. – 2000. – №. 1. – С. 40-45.

[44]Tan D. N., Nam H. N., Hieu M. N., Van H. N «New blind muti-signature schemes based on ECDLP» //International Journal of Electrical and Computer Engineering. – 2018. – Т. 8. – №. 2. – С. 1074.

[45]Yi X., Lam K. Y. «A new blind ECDSA scheme for bitcoin transaction anonymity» //Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security. – 2019. – С. 613-620.

в диссертации). Как следствие, удалось доказать, что все известные в литературе схемы GenEG-BS не обеспечивают стойкость в расширенных моделях безопасности. Данные схемы были исключены из рассмотрения в процессе выбора перспективной схемы подписи вслепую для стандартизации в Российской Федерации.

Глава 3 посвящена вопросам безопасности, актуальным в системах формирования классической подписи в условиях использования смарт-карт. В работе Алексеева Е.К. и соавторов[46] введены два типа нарушителей для систем такого типа: внешний нарушитель и нарушитель с агентом. Внешний нарушитель моделирует «честного, но любопытного» нарушителя, действующего на стороне приложения формирования подписи; его цель — сформировать подделку подписи. Нарушитель с агентом моделирует ситуацию использования уязвимой смарт-карты. Этот нарушитель является составным. Первая часть представляет собой активного нарушителя на стороне смарт-карты, который может взаимодействовать только с доверенным приложением, т.е. отсутствуют другие каналы передачи данных от смарт-карты. Вторая часть представляет собой агента, который накапливает пары (сообщение, подпись), вычисленные приложением и недоверенной смарт-картой. Цель агента — сформировать подделку подписи. В диссертации предлагается рассматривать два возможных вида нарушителя с агентом: сильный (нарушитель на стороне смарт-карты может формировать значение подписи произвольным образом) и слабый (нарушитель на стороне смарт-карты формирует значение подписи согласно заданному протоколу, но использует недоверенный датчик случайных чисел, т.е. выбирает произвольным образом случайные значения, используемые в алгоритме формирования подписи).

Раздел 3.1 содержит результаты анализа метода обеспечения защиты от внешнего нарушителя и слабого нарушителя с агентом. Для классической схемы подписи определяется специализированная модель безопасности SUF-CMRA[47], которая рассматривает угрозу построения подделки и предоставляет нарушителю возможность адаптивно выбирать сообщения для подписи, а также случайные значения и метки времени, используемые в процессе формирования подписи. Предлагается метод модификации классической схемы подписи Эль-Гамаля, обеспечивающий защиту от использования низкоэнтропийных случайных значений за счет дополнительного замешивания ключа подписи в процесс генерации одноразового секрета с помощью функции HMAC[48]. Кроме того, данный метод позволяет на четверть сократить длину подписи по сравнению с оригинальной схемой, что позволяет повысить производительность рассматриваемого типа систем. Для модифицированной схемы подписи Эль-Гамаля получена содержательная верхняя оценка преимущества нарушителя в модели SUF-CMRA со случайным оракулом (теорема V.1 [5], теорема 3.1.1 в диссертации). Данная

[46]Алексеев Е. К. , Ахметзянова Л. Р., Божко А. А., Смышляев С. В. «Безопасная реализация электронной подписи с использованием слабодоверенного вычислителя», Матем. вопр. криптогр., 12:4 (2021), 5–23.

[47]Ristenpart T., Yilek S. «When Good Randomness Goes Bad: Virtual Machine Reset Vulnerabilities and Hedging Deployed Cryptography». NDSS, 2010.

[48]Krawczyk, H. and Bellare, M. and R. Canetti. HMAC: Keyed-Hashing for Message Authentication, RFC 2104, RFC Editor, 1997.

оценка демонстрирует, что разработанный метод является безопасным в модели SUF-CMRA в предположении псевдослучайности функции HMAC.

Раздел 3.2 содержит результаты анализа метода обеспечения защиты целевых прикладных систем от внешнего нарушителя и сильного нарушителя с агентом, основанный на использовании схем подписи вслепую. В диссертации вводятся новые специализированные модели безопасности для схем подписи вслепую — SA-UF и HBC-UF, стойкость в которых требуется от схемы подписи вслепую для защиты от сильного нарушителя с агентом и внешнего нарушителя соответственно. Модель SA-UF описывает нарушителя, состоящего из двух алгоритмов. Первый алгоритм обладает всеми возможностями сервера, второй алгоритм (агент) имеет возможность накапливать для адаптивно выбираемых сообщений значения подписей, формируемых честным клиентом в результате взаимодействия с нарушителем-сервером. В качестве угрозы рассматривается построение подделки агентом. Модель HBC-UF описывает так называемого «честного, но любопытного» нарушителя, она предоставляет нарушителю возможность навязывать клиенту сообщения для подписи, получать стенограммы протокола формирования подписи и все случайные значения, выбранные клиентом в процессе выполнения протокола. В качестве угрозы также рассматривается построение поддлелки. Изучается связь между специализированными моделями безопасности и известными в литературе моделями безопасности для схем подписи вслепую. Доказано, что любая схема подписи вслепую обеспечивает стойкость в модели SA-UF, если она обеспечивает свойство неподделываемости относительно внешнего нарушителя и свойство неотслеживаемости в модели HS-Blind (теорема 1 [3], теорема 3.2.1 в диссертации). Для частного случая схем подписи вслепую на основе уравнения Эль-Гамаля доказано, что они обеспечивают стойкость в модели HBC-UF, если базовая схема подписи Эль-Гамаля обеспечивает свойство неподделываемости (теорема 2 [3], теорема 3.2.2 в диссертации). Для использования в прикладных системах, реализующих схему подписи ГОСТ Р 34.10-2012 на основе эллиптических кривых, определенных документом Р 1323565.1.024-2019[49] [50], предложено использовать схему подписи вслепую Камениша[51], в основе которой лежит такое же уравнение подписи. Удалось доказать, что эта схема обеспечивает защиту целевых прикладных систем при единственном предположении, что схема подписи ГОСТ Р 34.10-2012 обеспечивает свойство неподделываемости. Таким образом, схемы подписи вслепую на основе уравнения подписи Эль-Гамаля могут использоваться для защиты целевых прикладных систем несмотря на то, что они не обеспечивают стойкость в расширенных моделях безопасности.

[49]Рекомендации по стандартизации Р 1323565.1.024-2019 «Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов». М.: Стандартинформ, 2019.

[50]Эллиптические кривые, определенные в настоящем документе, имеют достаточно большую степень расширения (англ. embedding degree), что делает неприменимыми для них атаки, описанные в работе: Черепнёв М. А., Грачева С. С. Решение задачи Диффи-Хеллмэна на некоторых эллиптических кривых, удовлетворяющих ГОСТ 34.10-2018 //Информационные технологии. – 2020. – Т. 26. – №. 3. – С. 159-168.

[51]Camenisch J. L., Piveteau J. M., Stadler M. A. «Blind signatures based on the discrete logarithm problem» //Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1994. pp. 428–432.

В Заключении перечислены основные результаты диссертации.

Заключение

1) Для схемы подписи вслепую Шаума-Педерсена разработан метод нарушения свойства сильной неподделываемости в модели с параллельными сеансами и доказана содержательная верхняя оценка преимущества нарушителя, реализующего угрозу нарушения свойства слабой неподделываемости в модели с параллельными сеансами. Полученные результаты демонстрируют, что схема Шаума-Педерсена не обеспечивает стойкость в наиболее сильной расширенной модели безопасности, при этом в основе стойкости схемы в более слабой расширенной модели безопасности лежит новая нестандартная задача в группе точек эллиптической кривой.

2) Синтезирован класс схем подписи вслепую на основе уравнения Эль-Гамаля, не использующих дополнительные криптографические механизмы, покрывающий все существующие схемы такого типа. Для существенной части схем из этого класса разработан метод нарушения свойства неподделываемости в модели с параллельными сеансами. Среди оставшихся схем выявлен подкласс схем, для которых разработан метод нарушения одного из свойств: свойства неподделываемости в модели с последовательными сеансами или свойства неотслеживаемости. Построенные методы демонстрируют, что все существующие схемы подписи вслепую на основе уравнения Эль-Гамаля не обеспечивают стойкость в расширенных моделях безопасности.

3) Разработан метод модификации схемы подписи Эль-Гамаля, позволяющий уменьшить размер подписи на четверть и обеспечить безопасность в условиях использования недоверенного датчика случайных чисел при формировании подписи. Для модифицированной схемы доказана содержательная верхняя оценка величины преимущества нарушителя в специализированной модели безопасности, предоставляющей нарушителю возможность выбирать случайные значения, используемые в процессе формирования подписи.

4) Для схем подписи вслепую на основе уравнения Эль-Гамаля доказаны содержательные верхние оценки преимущества нарушителя в специализированных моделях безопасности, актуальных в системах формирования подписи в условиях использования функциональных ключевых носителей.

Разработанные в диссертации методы могут применяться при разработке и исследованиях средств защиты информации, а также использоваться в учебном процессе студентов, проходящих обучение в рамках специализации «Математические и программные методы обеспечения информационной безопасности».

Благодарности. Автор диссертации выражает благодарность своему научному руководителю доктору физико-математических наук Смышляеву Станиславу

Витальевичу за постановку задачи, постоянное внимание к работе и поддержку, а также доктору физико-математических наук Логачеву Олегу Алексеевичу, кандидату физико-математических наук Ахметзяновой Лилии Руслановне, кандидату физико-математических наук Алексееву Евгению Константиновичу, кандидату физико-математических наук Кяжину Сергею Николаевичу за полезные обсуждения и рекомендации. Автор также признателен заведующему кафедры Информационной безопасности ВМК МГУ имени М.В. Ломоносова академику Соколову Игорю Анатольевичу и всем ее сотрудникам за поддержку и внимание к диссертационной работе.

СПИСОК ПУБЛИКАЦИЙ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность и индексируемых в базе ядра Российского индекса научного цитирования «eLibrary Science Index»:

[1] Akhmetzyanova L. R., Alekseev E. K., Babueva A. A., Smyshlyaev S. V. «On the (im)possibility of secure ElGamal blind signatures» //Математические вопросы криптографии. – 2023. – Т. 14. – №. 2. – С. 25–42 (RSCI WoS, импакт-фактор 0,071 (РИНЦ), 1,1 п.л.). EDN: MTAYSS.
Соавторам принадлежит постановка задачи и обзор существующих схем подписи вслепую на основе уравнения Эль-Гамаля. Остальные результаты статьи получены Бабуевой А.А. (1 п.л., 90%)

[2] Akhmetzyanova L. R., Alekseev E. K., Babueva A. A., Taraskin O. G. «On blindness of several ElGamal-type blind signatures» //Прикладная дискретная математика. – 2023. – №. 62. – С. 13–20 (Scopus, RSCI WoS, импакт-фактор 0,135 (SJR), 0,5 п.л.). EDN: IIXNSY.
Бабуевой А.А. принадлежат три метода нарушения свойства неотслеживаемости (0,4 п.л., 80%). Остальные результаты статьи получены соавторами.

[3] Akhmetzyanova L. R., Babueva A. A., Bozhko A. A. «Blind signature as a shield against backdoors in smart-cards» //Прикладная дискретная математика. – 2024. – №. 63. – С. 49–64 (Scopus, RSCI WoS, импакт-фактор 0,135 (SJR), 1 п.л.). EDN: KLXDGE.
Соавторам принадлежит сравнение разработанного метода обеспечения безопасности систем формирования подписи на основе использования схем подписи вслепую с методом на основе использования доказательства с нулевым разглашением Шнорра. Остальные результаты статьи получены Бабуевой А.А. (0,9 п.л., 90%)

[4] Ахметзянова Л. Р., Бабуева А. А. «О свойстве неподделываемости схемы подписи вслепую Шаума-Педерсена» //Прикладная дискретная математика. – 2024. – №. 65. – С. 41–65 (Scopus, RSCI WoS, импакт-фактор 0,135 (SJR), 1,6 п.л.). EDN: VEOFUM.
Соавторам принадлежит постановка задачи и обзор сложных задач в группе точек эллиптической кривой. Остальные результаты статьи получены Бабуевой А.А. (1,4 п.л., 88%)

Иные публикации по теме диссертации:

[5] Бабуева А. А. «О модификации схемы подписи Эль-Гамаля для применения в одном классе систем голосования, использующих механизм подписи вслепую» //International Journal of Open Information Technologies. – 2023. – Т. 11. – №. 5. – С. 15–21 (импакт-фактор 0,458 (РИНЦ), 0,4 п.л.). EDN: GLDDTU.