Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ М.В.ЛОМОНОСОВА»
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ

УТВЕРЖДАЮ
Декан факультета ВМК МГУ,
Академик _____ /*И.А. Соколов*/
«14» сентября 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Теоретико-кодовые конструкции в криптографии
Coding theory methods in cryptography

Программа (программы) подготовки научных и научно-педагогических кадров в аспирантуре

Москва 2022

Рабочая программа дисциплины разработана в соответствии с Приказом Ректора МГУ №1216 от 24 ноября 2021 года «Об утверждении Требований к основным программам подготовки научных и научно-педагогических кадров в аспирантуре, самостоятельно устанавливаемых Московским государственным университетом имени М.В.Ломоносова»

1. Краткая аннотация:

Курс позволяет расширить знания в области криптографии. В курсе рассматриваются основные проблемы и задачи, связанные с разработкой и анализом теоретико-кодовых постквантовых криптосистем с открытым ключом. Основное внимание уделено кодовым конструкциям типа Мак—Элиса и Нидеррайтера. Рассматриваются вопросы анализа таких криптосистем.

Одна из задач курса заключается в развитии способности к критическому анализу современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях.

2. Уровень высшего образования – подготовка кадров высшей квалификации.

3. Научная специальность в отрасли физико-математических наук - 1.2.1., 1.2.2., 1.2.3., 1.1.2., 1.1.4., 1.1.5., 1.1.6., 2.3.5., 2.3.6., а также в отрасли технических наук - 1.2.2.

4. Место дисциплины (модуля) в структуре Программы аспирантуры: Обязательные Дисциплины (модули) - Факультетская дисциплина (обязательная дисциплина по выбору).

5. Объем дисциплины (модуля) составляет 2 зачетные единицы, всего 72 часа, из которых 28 часов составляет контактная работа аспиранта с преподавателем, 44 часа составляет самостоятельная работа аспиранта.

6. Входные требования для освоения дисциплины (модуля), предварительные условия.

На предыдущих уровнях высшего образования должны быть освоены общие курсы:

1. Математический анализ

2. Линейная алгебра

3. Теория групп, теория колец, теория конечных полей

4. Дополнительные главы комбинаторики

5. Дискретная математика

7. Содержание дисциплины (модуля), структурированное по темам

-	**Всего (часы)**	В том числе								
		Контактная работа (работа во взаимодействии с преподавателем), часы из них						**Самостоятельная работа обучающегося, часы** из них		
		Занятия лекционного типа	Занятия семинарского типа	Групповые консультации	Индивидуальные консультации	Учебные занятия, направленные на проведение текущего контроля успеваемости, промежуточной аттестации	**Всего**	Выполнение домашних заданий	Подготовка к коллоквиумам	**Всего**
Тема 1. Основные понятия теории линейных кодов, исправляющих ошибки Понятия кода, линейного кода над конечным полем. Основные параметры линейного кода: длина, размерность, кодовое расстояние. Порождающая и проверочная матрица линейного кода. Основные факты из области теории линейных кодов,	6	2	-	-	-	-	2	4	-	4

исправляющих ошибки: связь исправляющей способности кода и кодового расстояния, связь кодового расстояния и параметров проверочной матрицы, порождающие и проверочные матрицы, задача декодирования линейных кодов										
Тема 2. Кодовые криптосистемы типа Мак-Элиса и типаНидеррайтера Общая конструкция криптосистемы типа Мак-Элиса на основе произвольного линейного кода, имеющего достаточно эффективные алгоритмы декодирования. Атаки с использованием связанных шифр-текстов на такого типа криптосистемы. Обоснование и оценка сложности такого типа атак. Общая конструкция криптосистемы типа Нидеррайтера. Проблема нумерации двоичных	26	6	-	-	-	-	6	20	-	20

векторов фиксированного веса Хэмминга. Основные подходы её решения. Оценка сложности алгоритмов нумерации таких векторов. Вопросы эффективной программной реализации такого рода криптосистем.										
Тема 3. Двоичные коды Гоппы, классическая криптосистема Мак-Элиса Конструкция двоичных кодов Гоппы на основе рациональных функций над конечным полем. Вывод явного вида проверочной матрицы. Связь кодов Гоппы и альтернаных кодов, построенных из кодов Рида—Соломона. Граница на кодовое расстояние двоичных кодов Гоппы. Различные виды кодов Гоппы: неприводимые и сепарабельные. Граница на кодовое расстояние сепарабельных кодов Годов. Алгоритм Паттерсона декодирования двоичных	32	12	-	-	-	-	12	20	-	20

кодов Гоппы. Использование алгоритма Берлекемпа-Месси для декодирования двоичных сепарабельных кодов Гоппы. Примера построения кодов Гоппы. Общая конструкция криптосистемы Мак-Элиса и криптосистемы Нидеррайтера на сепарабельных кодах Гоппы. Оценка сложности алгоритмов генерации ключей, шифрования и расшифрования.										
Тема 4. Основные методы риптоанализа кодовых криптосистем. Два типа атака на кодовые криптосистемы: атаки декодирования, структурные атаки. Связь атак декодирования с задачей поиска слов малого веса. Атаки декодирования Стерна и её сложность. Возможная структурная атака на криптосистемы, построенные на основе двоичных сепарабельных кодов Гоппы.	6	4	2	-	-	-	6	-	-	-

Промежуточная аттестация: экзамен	2	-	-	-	-	-	2	-	-	-
Итого	72	26	2	-	-	-	28	-	-	44

8. Образовательные технологии.

При проведении лекционных занятий предусматривается использование информационных технологий, включающих пакеты математических программ: MATLAB, MATHEMATICA и др. Использование информационных технологий осуществляется, в частности, в процессе реализации активных и интерактивных форм проведения занятий. Информационные и интерактивные технологии используются при обсуждении проблемных и неоднозначных вопросов, требующих выработки решения в ситуации неопределенности.

9. Учебно-методические материалы для самостоятельной работы по дисциплине (модулю):

Самостоятельная работа учащихся состоит в изучении лекционного материала, учебно-методической литературы, подготовки к текущему контролю и промежуточной аттестации.

Литература для самостоятельной работы аспирантов в соответствии с тематическим планом.

Тема 1 «Основные понятия теории линейных кодов, исправляющих ошибки»

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. - М.: Связь, 1979
2. Берлекэмп Э. Алгебраическая теория кодирования. М.:Мир. 1971. 477 с.
3. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. - М.: Мир, 1976
4. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. М.: Мир. 1978. 576 с.

Тема 2 «Кодовые криптосистемы типа Мак-Элиса и типа Нидеррайтера»

1. Ван Тилборг Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. М.: Мир, 2006. — 471 с.
2. Robert J. McEliece. "A public-key cryptosystem based on algebraic coding theory." Jet Propulsion Laboratory DSN Progress Report 42–44, 114–116. http://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF
3. Harald Niederreiter. "Knapsack-type cryptosystems and algebraic coding theory." Problems of Control and Information Theory 15, 19–34. ProblemyUpravlenijaiTeoriiInformacii 15, 159–166.
4. Nicolas Sendrier. "Efficient generation of binary words of given weight." Pages 184–187 in: Colin Boyd (editor). Cryptography and Coding, 5th IMA conference, Cirencester, UK, December 18–20, 1995, proceedings. Lecture Notes in Computer Science 1025. Springer. ISBN 3-540-60693-9. http://www.springerlink.com/content/y43w30176331547m/fulltext.pdf

5. Nicolas Sendrier. "Encoding information into constant weight words." Pages 435–438 in: Information theory, 2005. ISIT 2005. Proceedings. IEEE. http://ieeexplore.ieee.org/iel5/10215/32581/01523371.pdf?arnumber=1523371
6. Thomas A. Berson. "Failure of the McEliece public-key cryptosystem under message-resend and related-message attack." Pages 213–220 in: Burton S. Kaliski, Jr. (editor). Advances in Cryptology—CRYPTO '97. 17th annual international cryptology conference, Santa Barbara, California, USA, August 17–21, 1997, proceedings. Lecture Notes in Computer Science 1294. Springer. http://www.springerlink.com/index/g6708p04m618g7r1.pdf
7. Bhaskar Biswas, Nicolas Sendrier. "McEliece cryptosystem implementation: theory and practice." Pages 47–62 in: Johannes Buchmann, Jintai Ding (editors). Post-quantum cryptography, second international workshop, PQCrypto 2008, Cincinnati, OH, USA, October 17–19, 2008, proceedings. Lecture Notes in Computer Science 5299. Springer. http://www.springerlink.com/content/708316211158tt3g/
8. Stefan Heyse. "Code-based cryptography: Implementing the McEliece scheme in reconfigurable hardware." Diploma thesis, Ruhr Universität Bochum. http://www.crypto.rub.de/imperia/md/content/texte/theses/da_heyse.pdf
9. Thomas Eisenbarth, Tim Güneysu, Stefan Heyse, Christof Paar. "MicroEliece: McEliece for embedded devices." Pages 49–64 in: CHES '09: Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems, 2009. Lecture Notes in Computer Science 5747. Springer. http://www.springerlink.com/content/44818244160740r1/
10. Stefan Heyse. "Low-Reiter: Niederreiter encryption scheme for embedded microcontrollers." Pages 165–181 in: Nicolas Sendrier (editor). Post-Quantum Cryptography, Third international workshop, PQCrypto 2010. Lecture Notes in Computer Science 6061. Springer. http://www.springerlink.com/content/uj3418uw97107012/
11. FalkoStrenzke. "A smart card implementation of the McEliece PKC." Pages 47–59 in: Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices. Lecture Notes in Computer Science 6033. Springer. http://www.springerlink.com/content/q241525l8t551182/
12. FalkoStrenzke. "How to implement the public key operations in code-based cryptography on memory-constrained devices." Cryptology ePrint Archive, Report 2010/465, 2010. http://eprint.iacr.org/2010/465/
13. Stefan Heyse. "Implementation of McEliece Based on Quasi-dyadic Goppa Codes for Embedded Devices". Pages 143–162 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedings Lecture Notes in Computer Science 7071. Springer. http://www.springerlink.com/content/1111u8m45r2215n5/

14. Paulo S. L. M. Barreto, Richard Lindner, Rafael Misoczki. "Monoidic Codes in Cryptography." Pages 179–199 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedings Lecture Notes in Computer Science 7071. Springer. http://www.springerlink.com/content/9v23w853vk80n024/
15. Daniel J. Bernstein. "Simplified high-speed high-distance list decoding for alternant codes." Pages 200–216 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedings Lecture Notes in Computer Science 7071. Springer. https://cr.yp.to/papers.html#simplelist

Тема 3 «Двоичные коды Гоппы, классическая криптосистема Мак-Элиса»

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. - М.: Связь, 1979
2. Гоппа В.Д. Коды на алгебраических кривых, ДАН СССР 259 (1981):6, 1289-1290
3. Nicholas J. Patterson. "The algebraic decoding of Goppa codes." IEEE Transactions on Information Theory IT-21, 203–207. MR 51:15175. http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/18/22749/01057049.pdf?arnumber=1057049
4. Elia, Michele &Viterbo, Emanuele &Bertinetti, G. (1999). Decoding of binary separable Goppa codes using Berlekamp-Massey algorithm. Electronics Letters. 35. 1720 - 1721. 10.1049/el:19991190.
5. Daniel J. Bernstein. "List decoding for binary Goppa codes." Pages 62–80 in: Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang Huaxiong Wang, Chaoping Xing (editors). Coding and Cryptology: Third International Workshop, IWCC 2011, Qingdao, China, May 30-June 3, 2011, proceedings. Lecture Notes in Computer Science 6639. Springer. https://cr.yp.to/papers.html#goppalist
6. Paulo S. L. M. Barreto, Richard Lindner, Rafael Misoczki. "Decoding square-free Goppa codes over Fp." Cryptology ePrint Archive, Report 2010/372, 2010. http://eprint.iacr.org/2010/372/

Тема 4 «Основные методы криптоанализа кодовых криптосистем»

1. Robert J. McEliece. "A public-key cryptosystem based on algebraic coding theory." Jet Propulsion Laboratory DSN Progress Report 42–44, 114–116. http://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF
2. Dilip V. Sarwate. "On the complexity of decoding Goppa codes." IEEE Transactions on Information Theory 23, 515–516. http://www.ifp.illinois.edu/~sarwate/pubs/Sarwate77Complexity.pdf
3. Jacques Stern. "A method for finding codewords of small weight." MR 1023683. Pages 106–113 in: Gerard D. Cohen, Jacques Wolfmann (editors). Coding theory and applications. Proceedings of the Third International Colloquium on Coding Theory held in Toulon, November 2–4, 1988. Lecture Notes

in Computer Science 388, Springer. ISBN 0-387-51643-3. MR 90i:94001. http://www.springerlink.com/index/7g665155m26n9g72.pdf

4. Anne Canteaut, Nicolas Sendrier. "Cryptanalysis of the original McEliece cryptosystem." MR 2000i:94042. Pages 187–199 in: Kazuo Ohta, Dingyi Pei (editors). Advances in cryptology—ASIACRYPT'98. Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security held in Beijing, October 18–22, 1998. Lecture Notes in Computer Science 1514, Springer. ISBN 3-540-65109-8. http://www.springerlink.com/index/64RNX94MG0Y32KNG.pdf
5. Anne Canteaut, Florent Chabaud. "A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511." IEEE Transactions on Information Theory 44, 367–378. MR 98m:94043. ftp://ftp.inria.fr/INRIA/tech-reports/RR/RR-2685.ps.gz
6. Anne Canteaut, Herve Chabanne. "A further improvement of the work factor in an attempt at breaking McEliece's cryptosystem." In: Pascale Charpin (editor). EUROCODE 94. http://www.inria.fr/rrrt/rr-2227.html
7. Alexei E. Ashikhmin, Alexander Barg. "Minimal vectors in linear codes." IEEE Transactions on Information Theory 44, 2010–2017. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=705584

10. Ресурсное обеспечение:

Основная литература:

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. - М.: Связь, 1979
2. Берлекэмп Э. Алгебраическая теория кодирования. М.:Мир. 1971. 477 с.
3. Ван Тилборг Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. М.: Мир, 2006. — 471 с.
4. Robert J. McEliece. "A public-key cryptosystem based on algebraic coding theory." Jet Propulsion Laboratory DSN Progress Report 42–44, 114–116. http://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF
5. Harald Niederreiter. "Knapsack-type cryptosystems and algebraic coding theory." Problems of Control and Information Theory 15, 19–34. ProblemyUpravlenijaiTeoriiInformacii 15, 159–166.
6. Nicolas Sendrier. "Efficient generation of binary words of given weight." Pages 184–187 in: Colin Boyd (editor). Cryptography and Coding, 5th IMA conference, Cirencester, UK, December 18–20,

1995, proceedings. Lecture Notes in Computer Science 1025. Springer. ISBN 3-540-60693-9. http://www.springerlink.com/content/y43w30176331547m/fulltext.pdf

7. Nicolas Sendrier. "Encoding information into constant weight words." Pages 435–438 in: Information theory, 2005. ISIT 2005. Proceedings. IEEE. http://ieeexplore.ieee.org/iel5/10215/32581/01523371.pdf?arnumber=1523371
8. Thomas A. Berson. "FailureoftheMcEliecepublic-keycryptosystemundermessage-resendandrelated-messageattack." Pages 213–220 in: Burton S. Kaliski, Jr. (editor). AdvancesinCryptology—CRYPTO '97. 17th annualinternationalcryptologyconference, Santa Barbara, California, USA, August 17–21, 1997, proceedings. Lecture Notes in Computer Science 1294. Springer. http://www.springerlink.com/index/g6708p04m618g7r1.pdf
9. BhaskarBiswas, NicolasSendrier. "McEliececryptosystemimplementation: theoryandpractice." Pages 47–62 in: JohannesBuchmann, JintaiDing (editors). Post-quantumcryptography, secondinternationalworkshop, PQCrypto 2008, Cincinnati, OH, USA, October 17–19, 2008, proceedings. Lecture Notes in Computer Science 5299. Springer. http://www.springerlink.com/content/708316211158tt3g/
10. StefanHeyse. "Code-basedcryptography: ImplementingtheMcElieceschemeinreconfigurablehardware." Diplomathesis, RuhrUniversitätBochum. http://www.crypto.rub.de/imperia/md/content/texte/theses/da_heyse.pdf
11. Thomas Eisenbarth, TimGüneysu, StefanHeyse, ChristofPaar. "MicroEliece: McElieceforembeddeddevices." Pages 49–64 in: CHES '09: Proceedingsofthe 11th International WorkshoponCryptographicHardwareandEmbedded Systems, 2009. Lecture Notes in Computer Science 5747. Springer. http://www.springerlink.com/content/44818244160740r1/
12. StefanHeyse. "Low-Reiter: Niederreiterencryptionschemeforembeddedmicrocontrollers." Pages 165–181 in: NicolasSendrier (editor). Post-Quantum Cryptography, Thirdinternationalworkshop, PQCrypto 2010. Lecture Notes in Computer Science 6061. Springer. http://www.springerlink.com/content/uj3418uw97107012/
13. FalkoStrenzke. "A smartcardimplementationoftheMcEliece PKC." Pages 47–59 in: Information Security TheoryandPractices. Security andPrivacyofPervasive Systems and Smart Devices. Lecture Notes in Computer Science 6033. Springer. http://www.springerlink.com/content/q241525l8t551182/
14. FalkoStrenzke. "Howtoimplementthepublickeyoperationsincode-basedcryptographyonmemory-constraineddevices." CryptologyePrintArchive, Report 2010/465, 2010. http://eprint.iacr.org/2010/465/

15. StefanHeyse. "ImplementationofMcEliece Based onQuasi-dyadicGoppaCodesforEmbedded Devices". Pages 143–162 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedingsLecture Notes in Computer Science 7071. Springer. http://www.springerlink.com/content/1111u8m45r2215n5/
16. Paulo S. L. M. Barreto, Richard Lindner, Rafael Misoczki. "Monoidic Codes in Cryptography." Pages 179–199 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedingsLecture Notes in Computer Science 7071. Springer. http://www.springerlink.com/content/9v23w853vk80n024/
17. Daniel J. Bernstein. "Simplified high-speed high-distance list decoding for alternant codes." Pages 200–216 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedingsLecture Notes in Computer Science 7071. Springer. https://cr.yp.to/papers.html#simplelist
18. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. - М.: Связь, 1979
19. Гоппа В.Д. Коды на алгебраических кривых, ДАН СССР 259 (1981):6, 1289-1290
20. Nicholas J. Patterson. "The algebraicdecodingofGoppacodes." IEEE Transactionson Information Theory IT-21, 203–207. MR 51:15175. http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/18/22749/01057049.pdf?arnumber=1057049
21. Elia, Michele &Viterbo, Emanuele &Bertinetti, G. (1999). Decoding of binary separable Goppa codes using Berlekamp-Massey algorithm. Electronics Letters. 35. 1720 - 1721. 10.1049/el:19991190.
22. Robert J. McEliece. "A public-key cryptosystem based on algebraic coding theory." Jet Propulsion Laboratory DSN Progress Report 42–44, 114–116. http://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF
23. Dilip V. Sarwate. "On the complexity of decoding Goppa codes." IEEE Transactions on Information Theory 23, 515–516. http://www.ifp.illinois.edu/~sarwate/pubs/Sarwate77Complexity.pdf
24. Jacques Stern. "A method for finding codewords of small weight." MR 1023683. Pages 106–113 in: Gerard D. Cohen, Jacques Wolfmann (editors). Coding theory and applications. Proceedings of the Third International ColloquiumonCodingTheoryheldinToulon, November 2–4, 1988. Lecture Notes in Computer Science 388, Springer. ISBN 0-387-51643-3. MR 90i:94001. http://www.springerlink.com/index/7g665155m26n9g72.pdf

Дополнительная литература:

1. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. - М.: Мир, 1976

2. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. М.: Мир. 1978. 576 с.
3. Bhaskar Biswas, Nicolas Sendrier. "McEliece cryptosystem implementation: theory and practice." Pages 47–62 in: Johannes Buchmann, Jintai Ding (editors). Post-quantum cryptography, second international workshop, PQCrypto 2008, Cincinnati, OH, USA, October 17–19, 2008, proceedings. Lecture Notes in Computer Science 5299. Springer.http://www.springerlink.com/content/708316211158tt3g/
4. Stefan Heyse. "Code-based cryptography: Implementing the McEliece scheme in reconfigurable hardware." Diploma thesis, Ruhr Universität Bochum. http://www.crypto.rub.de/imperia/md/content/texte/theses/da_heyse.pdf
5. Thomas Eisenbarth, Tim Güneysu, Stefan Heyse, Christof Paar. "MicroEliece: McEliece for embedded devices." Pages 49–64 in: CHES '09: Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems, 2009. Lecture Notes in Computer Science 5747. Springer. http://www.springerlink.com/content/44818244160740r1/
6. Stefan Heyse. "Low-Reiter: Niederreiter encryption scheme for embedded microcontrollers." Pages 165–181 in: Nicolas Sendrier (editor). Post-Quantum Cryptography, Third international workshop, PQCrypto 2010. Lecture Notes in Computer Science 6061. Springer. http://www.springerlink.com/content/uj3418uw97107012/
7. FalkoStrenzke. "A smart card implementation of the McEliece PKC." Pages 47–59 in: Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices. Lecture Notes in Computer Science 6033. Springer. http://www.springerlink.com/content/q241525l8t551182/
8. FalkoStrenzke. "How to implement the public key operations in code-based cryptography on memory-constrained devices." CryptologyePrintArchive, Report 2010/465, 2010. http://eprint.iacr.org/2010/465/
9. Stefan Heyse. "Implementation of McEliece Based on Quasi-dyadic Goppa Codes for Embedded Devices". Pages 143–162 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedings Lecture Notes in Computer Science 7071. Springer. http://www.springerlink.com/content/1111u8m45r2215n5/
10. Paulo S. L. M. Barreto, Richard Lindner, Rafael Misoczki. "Monoidic Codes in Cryptography." Pages 179–199 in: Post-Quantum Cryptog-raphy 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedings Lecture Notes in Computer Science 7071. Springer. http://www.springerlink.com/content/9v23w853vk80n024/
11. Daniel J. Bernstein. "Simplified high-speed high-distance list decoding for alternant codes." Pages 200–216 in: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011, proceedings Lecture Notes in Computer Sci-ence 7071. Springer. https://cr.yp.to/papers.html#simplelist

12. Daniel J. Bernstein. "List decoding for binary Goppa codes." Pages 62–80 in: Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yu-ansheng Tang Huaxiong Wang, Chaoping Xing (editors). Coding and Cryptology: Third International Workshop, IWCC 2011, Qingdao, China, May 30-June 3, 2011, proceedings. Lecture Notes in Computer Science 6639. Springer. https://cr.yp.to/papers.html#goppalist
13. Paulo S. L. M. Barreto, Richard Lindner, Rafael Misoczki. "Decoding square-free Goppa codes over Fp." Cryptology ePrint Archive, Report 2010/372, 2010. http://eprint.iacr.org/2010/372/
Anne Canteaut, Nicolas Sendrier. "Cryptanalysis of the original McEliece cryptosystem." MR 2000i:94042. Pages 187–199 in: Kazuo Ohta, Dingyi Pei (editors).
14. Advances in cryptology—ASIACRYPT'98. Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security held in Beijing, October 18–22, 1998. Lecture Notes in Computer Science 1514, Springer. ISBN 3-540- 65109-8. http://www.springerlink.com/index/64RNX94MG0Y32KNG.pdf
15. Anne Canteaut, Florent Chabaud. "A new algorithm for finding minimum-weight words in a linear code: application to McEliece'scryptosys- tem and to narrow-sense BCH codes of length 511." IEEE Transactions on Information Theory 44, 367–378. MR 98m:94043. ftp://ftp.inria.fr/INRIA/tech-reports/RR/RR-2685.ps.gz
16. Anne Canteaut, Herve Chabanne. "A further improvement of the work factor in an attempt at breaking McEliece's cryptosystem." In: Pascale Charpin (editor). EUROCODE 94. http://www.inria.fr/rrrt/rr-2227.html
17. Alexei E. Ashikhmin, Alexander Barg. "Minimal vectors in linear codes." IEEE Transactions on Information Theory 44, 2010–2017. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=705584

Перечень используемых информационных технологий при осуществлении образовательного процесса, включая программное обеспечение, информационные справочные системы (при необходимости):

http://elibrary.ru

www.scopus.com

http://pqcrypto.org/

https://link.springer.com/

http://eprint.iacr.org

https://arxiv.org/

Занятия проводятся в аудитории, оснащенной мультимедийным экраном

11. Язык преподавания – русский

12. Преподаватели.

к.ф.-м.н., доцент Чижов Иван Владимирович

Фонды оценочных средств, необходимые для оценки результатов обучения

Образцы домашних заданий:

Каждый учащийся в процессе обучения готовит научный проект, который заключается в построении кодовой криптосистемы на основе какого-либо типа кодов. Для построенной кодовой криптосистемы должны быть указаны:

1. Алгоритм генерации ключей, оценка сложности
2. Открытый ключ
3. Секретный ключ
4. Алгоритм шифрования, оценка сложности
5. Алгоритм расшифрования, оценка сложности
6. Описываются возможные типа атак на криптосистему, известные из открытых источников.

Возможные типы кодов для научной работы:

1. Коды Хэмминга
2. Коды Рида—Маллера первого порядка
3. Коды Рида—Соломона
4. Расширенные коды Хэмминга
5. Эквидистантные коды (коды, дуальные к коду Хэмминга).

Вопросы для промежуточной аттестации –**экзамена**:

1. Криптосистема Мак-Элиса, общая конструкция
2. Криптосистема Нидеррайтера, общая конструкция
3. Атаки с использованием связанных шифр-текстов на такого типа криптосистемы. Обоснование и оценка сложности такого типа атак.
4. Проблема нумерации двоичных векторов фиксированного веса Хэмминга. Основные подходы её решения. Оценка сложности алгоритмов нумерации таких векторов. Вопросы эффективной программной реализации такого рода криптосистем.

5. Конструкция двоичных кодов Гоппы на основе рациональных функций над конечным полем. Вывод явного вида проверочной матрицы. Связь кодов Гоппы и альтернатных кодов, построенных из кодов Рида—Соломона.
6. Граница на кодовое расстояние двоичных кодов Гоппы. Различные виды кодов Гоппы: неприводимые и сепарабельные. Граница на кодовое расстояние сепарабельных кодов Годов.
7. Алгоритм Паттерсона декодирования двоичных кодов Гоппы.
8. Использование алгоритма Берлекемпа-Месси для декодирования двоичных сепарабельных кодов Гоппы. Примера построения кодов Гоппы.
9. Общая конструкция криптосистемы Мак-Элиса и криптосистемы Нидеррайтера на сепарабельных кодах Гоппы. Оценка сложности алгоритмов генерации ключей, шифрования и расшифрования.
10. Два типа атака на кодовые криптосистемы: атаки декодирования, структурные атаки.
11. Связь атак декодирования с задачей поиска слов малого веса. Атаки декодирования Стерна и её сложность.
12. Возможная структурная атака на криптосистемы, построенные на основе двоичных сепарабельных кодов Гоппы.

Методические материалы для проведения процедур оценивания результатов обучения

Экзамен проходит по билетам, включающем 2 вопроса. Уровень знаний аспиранта по каждому вопросу на «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Критерии и показатели оценивания ответа на экзамене			
2	3	4	5
Неудовлетворительно	**Удовлетворительно**	**Хорошо**	**Отлично**
Фрагментарные знания актуальных проблем, алгоритмов, теорем в области криптографии.	Неполные знания актуальных проблем, алгоритмов, теорем в области криптографии.	Сформированные, но содержащие отдельные пробелы знания актуальных проблем, алгоритмов, теорем в области криптографии.	Сформированные и систематические знания актуальных проблем, алгоритмов, теорем в области крипторафии.