Темы БДЗ для выполнения на сайте cryptowiki.net, группа М17-507, 2017/18 уч.г.:

№	Тема на русск.яз.	Тема на англ.яз.	Ссылки на статьи по теме (указан минимум, можно использовать любую другую литературу)	ФИО студента
1	Модель транзакций и протоколов Биткоина	Bitcoin transaction and protocol model	https://eprint.iacr.org/2017/1124.pdf https://eprint.iacr.org/2018/138.pdf	Глинская Татьяна
2	Краткие неинтерактивные доказательства с нулевым разглашением	Succinct non-interactive zero-knowledge proofs (zk-SNARKs)	https://eprint.iacr.org/2014/349.pdf https://eprint.iacr.org/2013/879.pdf https://chriseth.github.io/notes/articles/zksnarks/zksnarks.pdf	
3	Постквантовые цифровые подписи	Post-quantum digital signature	https://eprint.iacr.org/2017/279.pdf https://eprint.iacr.org/2017/186.pdf https://eprint.iacr.org/2016/1110.pdf	Петров Иван
4	Постквантовые доказательства с нулевым разглашением	Post-quantum zero-knowledge proofs	https://eprint.iacr.org/2017/1154.pdf https://eprint.iacr.org/2017/279.pdf https://eprint.iacr.org/2016/1110.pdf	Андрианова Вера
5	«Храповичное» шифрование	Ratcheted encryption	https://eprint.iacr.org/2016/1028.pdf https://eprint.iacr.org/2016/1013.pdf	
6	Протоколы защищенных групповых коммуникаций в мессенджерах	Secure group messaging	https://eprint.iacr.org/2017/666.pdf https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf https://fbnewsroomus.files.wordpress.com/2016/07/messenger-secret-conversations-technical-whitepaper.pdf	Шингалова Дарина
7	Стойкость криптосхем после	Post-compromise security	https://eprint.iacr.org/2016/221.pdf https://eprint.iacr.org/2015/486.pdf	

	компрометации ключей			
8	Атрибутные удостоверения, позволяющие сохранять анонимность	Privacy-preserving attribute-based credentials	https://yadi.sk/i/ZCr1k9Fa3SmDRq https://yadi.sk/d/d1OH5l1v3SmDcT	
9	Неинтерактивные системы доказательства Грота-Сахаи	Groth-Sahai non-interactive proof systems	https://eprint.iacr.org/2013/662.pdf https://eprint.iacr.org/2007/155.pdf	
10	Луковичное шифрование и его применение в протоколах анонимной сети Tor	Onion encryption and its application for Tor anonymous communication	https://eprint.iacr.org/2018/162.pdf https://eprint.iacr.org/2018/126.pdf http://cs.brown.edu/~anna/papers/cl05.pdf	
11	Криптографически стойкая биометрическая аутентификация	Secure biometric authentication systems	https://eprint.iacr.org/2017/450.pdf https://eprint.iacr.org/2016/484.pdf https://www.researchgate.net/publication/266261762_THRIVE_Threshold_Homomorphic_encryption_based_secure_and_privacy_preserving_bIometric_VErification_system	Биндиман Александр
12	Подписи, сохраняющие алгебраическую структуру	Structure-preserving signatures	https://eprint.iacr.org/2017/524.pdf https://eprint.iacr.org/2015/824.pdf	
13	Прямая анонимная аттестация	Direct anonymous attestation	https://eprint.iacr.org/2015/1246.pdf https://eprint.iacr.org/2004/205.pdf	
14	Аутентичный обмен ключами,	Password authenticated key	https://www.iacr.org/archive/eurocrypt2000/1807/18070140-new.pdf	

	основанный на паролях	exchange (PAKE)	https://www.iacr.org/archive/eurocrypt2005/34940406/34940406.pdf	
15	Семейство масштабируемых протоколов консенсуса Algorand	Algorand: Scaling Byzantine agreements	https://eprint.iacr.org/2017/454.pdf https://arxiv.org/pdf/1607.01341.pdf	
16	Семейство протоколов доказательства обладания долей Ouroboros	Ouroboros: Proof-of-stake protocols	https://eprint.iacr.org/2017/573.pdf https://eprint.iacr.org/2016/889.pdf	
17	Конфиденциальное обучение нейронных сетей	Privacy-preserving neural networks learning	https://eprint.iacr.org/2018/073.pdf http://proceedings.mlr.press/v48/gilad-bachrach16.pdf https://eprint.iacr.org/2017/396.pdf	

Для закрепления темы за Вами необходимо прислать письмо на адрес svzapechnikov@yandex.ru. Приоритет выбора темы определяется по времени получения письма. В случае коллизии необходимо выбрать другую тему из числа свободных.