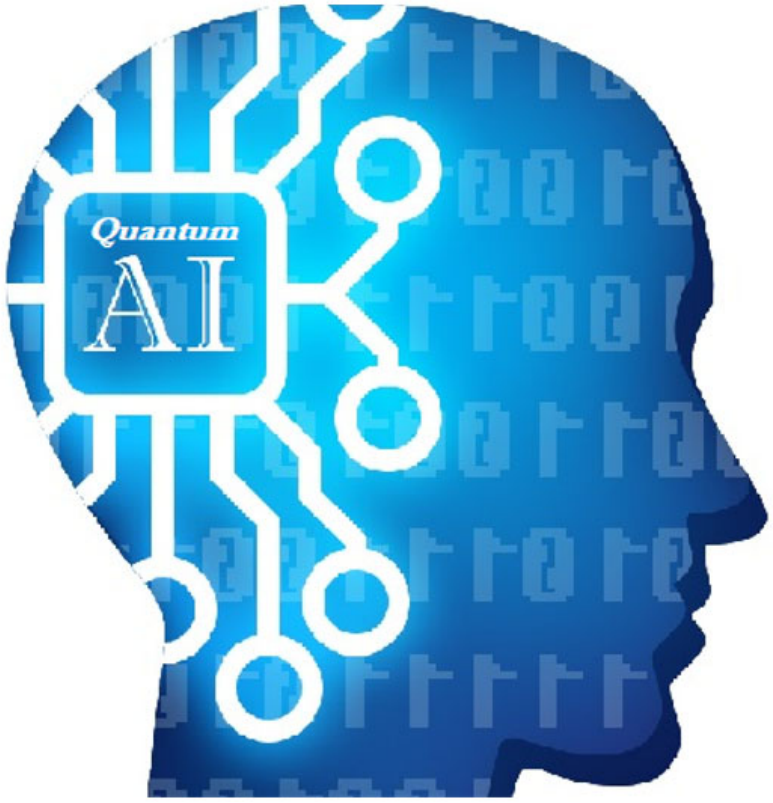


Built on the Cardano Blockchain

QuantumAI Whitepaper Cryptography and Security Protocol

QuantumAI is a tokenized computing security protocol with the ability to learn and create a Quantum resistant network through the Cardano Blockchain with its artificial intelligence computing system.

QuantumAI will use quantum computing for computation of machine learning algorithms. Thanks to computational advantages of quantum computing, QuantumAI can help achieve results that are not possible to achieve with classical computers. Quantum mechanics is a universal model based on different principles than those observed in daily life. A quantum model of data is needed to process data with quantum computing. Hybrid quantum-classical models are also necessary in quantum computing for error correction and correct functioning of the quantum computer.

Overview

Token Information

PolicyID: 354a6c0acd846b195768ead31c92693ad26d82ba013e7df5d9777081

Fingerprint: asset1nylmp38l5uq2szj6kguellahjvpsj6a7uhwxzs

Asset Name: QAI (514149)

Total Supply: 1,000,000,000
Max Supply: 1,000,000,000
Circulating Supply: 150,000,000 (approximately)

Token Economics Distribution

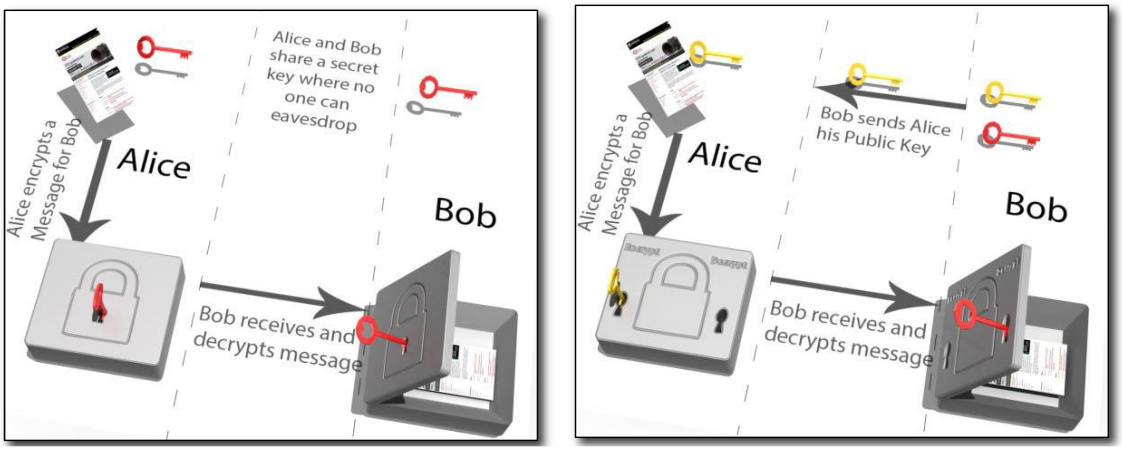
What is cryptography and how is it used?

Cryptography is literally the art of "secret writing". It is used to secure communication by protecting the confidentiality and integrity of messages and sensitive data. Without it, anyone could read a message or forge a private conversation. Messages are made secret by transforming them from "plaintext" into "ciphertext" using a cipher and performing the process of encryption. Decryption turns scrambled and unreadable ciphertext back into plaintext.

When cryptographers talk about a "key", they are referring to a shared secret that controls the ability to hide and un-hide information. There are two types of cryptography that are often referred to as "symmetric key" and "public key" cryptography:

1. In symmetric key cryptography, the same key is used for both encryption and decryption, and that key needs to be kept a secret by everyone who is sending and receiving private messages. The major difficulty of symmetric key cryptography is to provide the secret keys to legitimate parties without divulging the keys to eavesdroppers.
2. Public key cryptography[1] is more involved and complex. There are two keys, one for encrypting and another key for decrypting. The two keys are mathematically related, and only one key is intended to be kept a secret. Public key cryptography allows anyone to send an encrypted message, but only one person, with the private key, can decrypt the message. Public key cryptography can also be used for digital signatures where someone with a private key can sign a message that anyone can verify with the public key.

Figure 1 - Cryptography Basics - Encryption and Decryption



A - Symmetric Key Cryptography **B - Public Key Cryptography**

What is quantum computing?

Today's computers are governed by the laws of classical physics and Moore's law which states that, historically speaking, computers double their speed and capacity every 18 months because chip makers are able to squeeze twice as many transistors onto a computer chip. In order for these computing improvements to continue, placing more transistors on a computer chip means that transistors need to get smaller. But physics presents a natural barrier in that once technology has shrunk a transistor to the size of a single atom there are no more improvements to be made to transistor size. But what if the transistor could be replaced with a better technology, a technology that allows for a new paradigm of computing?

The laws of physics that can be seen, observed, and understood through experiences in everyday life are referred to as classical physics, and these laws govern the workings and computational capabilities of computers as they are known today. However, everything that is described by classical physics at a macroscopic level can be described by quantum physics at a nanoscopic level, and these different physical laws are known as quantum mechanics. In the past few decades, researchers have realized that the ways in which the laws of physics allow different things to happen to very small objects can be harnessed to make computers out of novel materials, with hardware that looks and behaves very differently from the typical classical computers that people use in their homes and offices today.

Quantum computers, obeying the laws of quantum mechanics, can calculate things in ways that are unimaginable from the perspective of people's regular day-to-day experiences.

In classical computing, information is stored in fundamental units called bits, where a bit can hold a binary digit with the value of 0 or 1. In quantum computing, the fundamental unit can hold both a 0 and a 1 value at the same time; this is known as a superposition of two states. These quantum bits are known as qubits and measuring the state of a qubit causes it to select or "collapse into", being a 0 or a 1. Interestingly, if you prepare a string of qubits of the same length in the same way, the resulting bit string will not always be the same. This gives quantum computers an advantage over classical computers in that they can perform very rapid parallel computations.

Quantum mechanics has some novel properties that researchers have realized can be harnessed to make quantum computers that behave very differently than the classical computers commonly used today. Using these novel quantum properties, a quantum computer is able to solve certain problems like searching and factoring much faster than the time it would take a classical computer, with the best known algorithms, to solve the same problem.

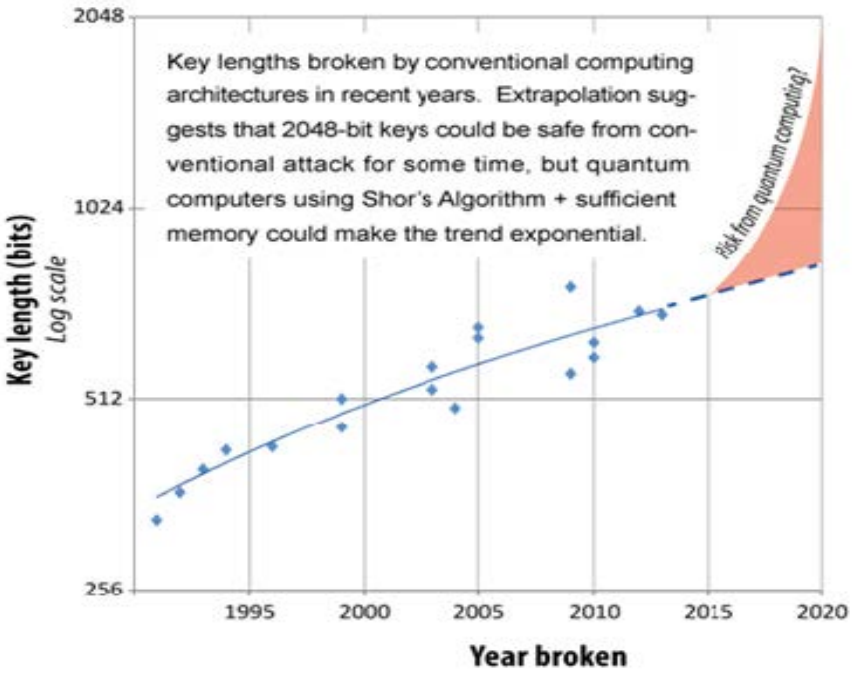


Figure 2 - Breaks of the RSA cryptosystem in recent years using conventional computation.

[2] Moore's law is not an actual law of physics, but instead a general observation and prediction made by a co-founder of Intel that describes the speed in which computing has matured. (source and citation based off previous whitepaper. Link can be found on the last page)

Coding

What is Qis|krypt?

Qis|krypt is a software suite of protocols of quantum cryptography and quantum communications, as well, other protocols and algorithms, built using IBM's open-source Software Development Kit for quantum computing Qiskit.

What is Plutus?

Plutus is the smart contract platform of the Cardano blockchain. It allows you to write applications that interact with the Cardano blockchain.

How we will implement Qis|krypt with Plutus?

Since Plutus allows you to write applications that interact with the Cardano blockchain, we will use this feature to create the QuantumAI Protocol and bring together the world of QuantumAI and Blockchain technology. Plutus allows our team to create customized smart contracts and through the Plutus Playground and together with EVM and KEVM virtual machine environments, the Marlowe and Marlowe Playground. These will all be necessary to implement the Qis|krypt coding into our smart contract. We will also take a look at future plans for greater programming language support on Cardano, and what efforts can be made in scope of this area.

A Plutus contract is a Haskell program that will be partly compiled to on-chain Plutus Core code and partly to off-chain code. Plutus contracts contain pieces of code that run on the blockchain, as well as off-chain code that runs on the user's machine. While the on-chain component of Plutus smart contracts compiles in the Plutus compiler, the off-chain elements are compiled by the Glasgow Haskell Compiler (GHC).

Our team will be using Plutus to write a smart contract for your DApp or DeFi solution, Cardano engineers at IOHK have built the Plutus Playground for us to work with. This is a lightweight browser-based development environment that allows engineers to write and simulate their smart contracts before they are compiled to a mainnet environment.

Our Goal

Our goal is to protect and secure the worlds data at the tip of its fingers. We hope the QuantumAI Security Protocol will change the way you use the Internet & IoT.

QuantumAI is a Community based Token project and is open any and all ideas to make the future of cryptocurrency easier to understand and more secure. QuantumAI is developing a secure and decentralized governance model. A model to give everybody a voice, and control over the future development of the platform and the applications and services that emerge from it in the most secure way possible.

The Mission

The mission is to revolutionize the world of finance as we know it. Bringing together Human and QuantumAI capabilities to help protect assets, predict market trends, secure data and finances from Quantum hacks with our QuantumAI Secuirty Protocol.

The Vision

Our vision of QuantumAI Token is to play a big role in the future of our financial society. We will work to collaborate Humans and AI technologies to make our human lives easier in all aspects of life. This will include Agriculture, Business & Finance, AI Ads and much more.

We hope this will be one of the most comprehensive overviews of Cardano's smart contract environment by a non-Cardano entity, and we hope it brings deep value to our community. It will all start with Plutus then IBM's open source coding will be added to the smart contract as we develop further.

This whitepaper is an updated one to our previous whitepaper and briefly explains how we will use our token and build on top of the previous whitepaper using the Cardano Blockchain and its Native Token QuantumAI to implement the QuantumAI protocol.

We are in no way or form affiliated, associated or in partnership with any other Quantum AI projects or company. All references, sources and citations are listed below.

References & Citations

(Source of previous whitepaper is on our GitHub, references & citations: https://github.com/C-QuantumAi/QuantumAI/blob/main/QuantumAI-Whitepaper.pdf)

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies.
NOTE: While any hyperlinks included in this clause were valid at the time of publication, QuantumAI cannot guarantee their long term validity.
[A+13] Alaoui, S. M. E. Y., Cayrel, P. L., El Bansarkhani, R., & Hoffmann, G. (2013). Code-based identification and signature schemes in software. In Security Engineering and Intelligence Informatics (pp. 122-136). Springer Berlin Heidelberg.
[BB84] C. H. Bennett, G. Brassard. *Quantum cryptography: Public key distribution and coin tossing*. In Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, pages 175-179 (1984).
[BCNS14] J.W. Bos, C. Costello, M. Naehrig, and D. Stebila. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. Cryptology ePrint Archive, report 2014/599. http://eprint.iacr.org/2014/599
[BDH11] Buchmann, Dahmen, and Hülsing, "XMSS - A Practical Forward Secure Signature Scheme based on Minimal Security Assumptions" https://eprint.iacr.org/2011/484.pdf
[BEN97] C. Bennett, E. Bernstein, G. Brassard, U. Vazirani. *Strengths and weaknesses of quantum computation*. SIAM Journal on Computing **26** (5), 1510 (1997).
[BHL05] M. Ben-Or, M. Horodecki, D. Leung, D. Mayers, J. Oppenheim. *The universal composable security of quantum key distribution*. In Theory of Cryptography, Proceedings of TCC 2005, **3378,** 386-406, (2005).
[BHM96] Eli Biham, Bruno Huttner, and Tal Mor. Quantum cryptographic network based on quantum memories. Physical Review A, 54(4):2651–2658, 1996.
[CHA09] T. E. Chapuran et al. Optical networking for quantum key distribution and quantum communications. New Journal of Physics **11,** 105001 (2009).
[CHE10] T.-Y. Chen et al. Metropolitan all-pass and intercity quantum communication network. Optics Express **18**(26), :27217 (2010).
[CVE10] Cayrel, P.-L., Véron, P., El Yousfi Alaoui, S.M.: A Zero-Knowledge Identification Scheme Based on the q-ary Syndrome Decoding Problem. In: Biryukov, A., Gong, G., Stinson, D.R. (eds.) SAC 2010. LNCS, vol. 6544, pp. 171–186. Springer, Heidelberg (2011)
[CW79] J. L. Carter, M. N. Wegman. Universal classes of hash functions. Journal of Computer and System Sciences, **18** (2), pp. 143-154 (1979).
[DDLL13] Lucas et al. , "Lattice Signatures and Bimodal Gaussians". https://eprint.iacr.org/2013/383.pdf
[Ding04] J. Ding: A new Variant of the Matsumoto-Imai Cryptosystem through Perturbation. PKC 04, LNCS vol. 2947, p.305-318. Springer (2004)
[DS05] J.Ding, D. Schmidt: Cryptanalysis of HFEv and Internal Perturbation of HFE. PKC 05, LNCS vol. 3386, p. 288-301. Springer (2005)
[DPW14] J.Ding, A. Petzoldt, L.-C. Wang: The cubic Simple Matrix Encryption Scheme. PQCrypto 2014, LNCS vol. 8772, pp. 76-87. Springer (2014)

[DDYCC08] J.Ding, V. Dubois, B.Y. Yang, C.-H. O. Chen, C.-M. Cheng: Could SFlash be repaired? Automata, Languages and Programming (ICALP 2008), LNCS vol. 5126, pp. 691 – 701. Springer (2008)
[DYCCC05] Ding, J., Yang, B.-Y., Chen, C.-H. O., Chen, M.-S, and Cheng, C.M.: New Differential-Algebraic Attacks and Reparameterization of Rainbow. In: LNCS 5037, pp.242-257, Springer, Heidelberg (2005)
[EBACS] EBACS web site http://bench.cr.yp.to/ebasc.html
[EFF14] Electronic Frontier Foundation "Encrypt the Web" Report. https://www.eff.org/encrypt-the-web-report
[EKE91] A. K. Ekert. *Quantum cryptography based on Bell's theorem*. Physical Review Letters, **67**, 661-663, (1991). doi:10.1103/PhysRevLett.67.661.
[ELS12] D. Elser et al. *Network architectures for space-optical quantum cryptography services*. ICSOS 2012 International Conference on Space Optical Systems and Applications, (2012).
[ERE10] P. Eraerds et al. Quantum key distribution and 1 Gbps data encryption over a single fibre. New Journal of Physics **12** 063027 (2010).
[FSXY13] A. Fujioka, K. Suzuki, K. Xagawa, and K. Yoneyama. Practical and post-quantum authenticated key exchange from one-way secure key encapsulation mechanism. In Proc. ASIACCS 13, pages 83–94. ACM, May 2013.
[GIS02] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden. *Quantum cryptography*. Review of Modern Physics **74**, 145–95 (2002).
[GRO02] F. Grosshans, P. Grangier. Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. 88:057902 (2002).
[Gro96] Lou Grover. A fast quantum mechanical algorithm for database search. Proceedings, 28th Annual ACM Symposium on the Theory of Computing, 212, 1996.
[HHHW09] P. Hirschhorn, et al. "Choosing NTRUEncrypt Parameters in Light of Combined Lattice Reduction and MITM Approaches" Applied Cryptography and Network Security, Springer, LNCS 5536, 2009. https://www.securityinnovation.com/uploads/Crypto/params.pdf
[HWA03] W. Y. Hwang. Quantum Key Distribution with High Loss: Toward Global Secure Communication. Phys. Rev. Lett. **91**, 057901 (2003).
[IDQ] ID Quantique SA. www.idquantique.com
[IM11] Lawrence M. Ioannou and Michele Mosca. A new spin on quantum cryptography: Avoiding trapdoors and embracing public keys. In BoYin Yang, editor, Proc. 4th International Workshop on PostQuantum Cryptography (PQCrypto) 2011, LNCS, volume 7071, pp. 255–274. Springer, 2011.
[Ina02] Hitoshi Inamori. Security of practical timereversed EPR quantum key distribution. Algorithmica, 34(4):340–365, 2002.
[LCQ12] H.-K. Lo, M. Curty, B. Qi. Measurement-device-independent quantum key distribution. Phys. Rev. Lett., **108**, 130503 (2012).
[LAN13] Thomas Länger. *Information Security and the Enforcement of Secrecy: The Practical Security of Quantum Key Distribution*. Ph.D. Thesis University of Lausanne (2013)
[LIM13] C. W. Lim et al. Device-Independent Quantum Key Distribution with Local Bell Test. Phys. Rev. X **3**, 031006 (2013).
[LUC13] M. Lucamarini et al. Efficient decoy-state quantum key distribution with quantified security. Optics Express **21**(21), 24550 (2013).
[MAU11] U. Maurer, R. Renner. *Abstract cryptography.* In Proceedings of Innovations in Computer Science, ICS 2010, 1-21, (2011).
[Merkle79] Ralph C. Merkle, Method of providing digital signatures, US Patent 4309569-A, Filed September 5, 1979. proceedings of "1st QuantumAI-Crypto Workshop",
[MSU13] M. Mosca, D. Stebila, B. Ustaoglu, "Quantum Key Distribution in the Classical Authenticated Key Exchange Framework", In Proceedings of the 5th International Conference on PostQuantum Cryptography (PQCrypto 2013), Lecture Notes in Computer Science, Vol. 7932, pp. 136154, Springer (2013).
[MTSB12] R. Misoczki, et al. "MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes" Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on Information Theory. https://eprint.iacr.org/2012/409.pdf
[NMBB12] R. Niebuhr, et al. "Selecting Parameters for Secure McEliece-based Cryptosystems" Informational Journal of Information Security, June 2012, Volume 11, Issue 3, pp 137-147. https://eprint.iacr.org/2010/271.pdf
[PAT14] K. A. Patel et al. Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks. Applied Physics Letters **104** (5), 051123 (2014).
[Patarin96] Patarin, J.: Hidden Field equations (HFE) and Isomorphisms of Polynomials (IP). In: Proceedings of EUROCRYPT'96, pp. 38-48, Springer, Heidelberg (1996)

[PBB10] Petzoldt , Bulygin, and Buchmann “Selecting Parameters for the Rainbow Signature Scheme” https://eprint.iacr.org/2010/437.pdf
[PBB11] A. Petzoldt, S. Bulygin, J. Buchmann: Linear Recurring Sequences for the UOV Key Generation. PKC 2011, LNCS vol. 6571, p. 335-350, Springer, 2011.
[PDG14] Pöppelmann, Thomas, Léo Ducas, and Tim Güneysu. "Enhanced Lattice-Based Signatures on Reconfigurable Hardware." to appear inCHES 2014.
[Pei14] C. Peikert. Lattice cryptography for the Internet. In Proc. 6th International Conference on Post-Quantum Cryptography (PQCrypto) 2014, LNCS. Springer, 2014. To appear. Full version available at http://eprint.iacr.org/2014/070.
[PER09] R. Perlner, D. Cooper. *Quantum Resistant Public Key Cryptography: A Survey*. Proc. of IDtrust 2009, pp. 85 (2009).
[PET09] N. A. Peters et al. Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments. New J. Phys. **11**, 045012 (2009).
[PPS07] Kenneth G. Paterson, Fred Piper, and R¨udiger Schack. Quantum cryptography: A practical information security perspective. In Marek Zukowski, Sergei Kilin, and Janusz Kowalik, editors, Proc. NATO Advanced Research Workshop on Quantum Communication and Security, NATO Science for Peace and Security Series, Sub-Series D: Information and Communication Security, volume 11. IOS Press, 2007.
[QBC13] T. Lunghi et al. Experimental Bit Commitment Based on Quantum Communication and Special Relativity, Phys. Rev. Lett. **111**, 180504 (2013).
[QLI] QuintessenceLabs Inc. www.quintessencelabs.com
[QPQ11] Markus Jakobi et al. Practical private database queries based on a quantum-key-distribution protocol. Phys. Rev. A **83**, 022301 (2011).
[SARG04] V. Scarani, A. Acin, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys. Rev. Lett. **92**(5), 057901 (2004).
[SAS11] M. Sasaki et al. Field test of quantum key distribution in the Tokyo QKD Network. Optics Express, **19**, (11), 10387-10409 (2011). doi: 10.1364/OE.19.010387.
[SEC09] M. Peev et al. The SECOQC quantum key distribution network in Vienna. New Journal of Physics **11** 075001 (2009).
[SecInn13] Security Innovation, Inc. ntru-crypto: Open Source NTRU Public Key Cryptography Algorithm and Reference Code. Github. https://github.com/NTRUOpenSourceProject/ntru-crypto
[SHA49] C. Shannon. *Communication Theory of Secrecy Systems*. Bell System Technical Journal **28** (4), 656 (1949).
[SMA07] T. Schmitt-Manderbach et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. Phys. Rev. Lett. **98**, 010504 (2007).
[SSH11] K. Sakumoto, T. Shirai and H. Hiwatari: Public-Key Identification Schemes based on Multivariate Quadratic Polynomials. CRYPTO 2011, LNCS vol. 6841, pp. 706 – 723, Springer 2011.
[Stern94] Stern, J.: A New Identification Scheme Based on Syndrome Decoding. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 13–21. Springer, Heidelberg (1994)
[STU09] D. Stucki et al. High rate, long-distance quantum key distribution over 250 km of ultra-low loss fibres. New Journal of Physics **11**, 075003 (2009).
[STU11] D. Stucki et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. New Journal of Physics **13**, 123001 (2011).
[VBF04] V. Verykios et al. State-of-the-art in privacy-preserving data mining. ACM SIGMOD Record, 33 (1), 2004
[WAL14] N. Walenta et al. A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. New Journal of Physics **16**, 013047 (2014).
[WAN12] Shuang Wang et al. 2 GHz clock quantum key distribution over 260 km of standard telecom fiber. Optics Letters, **37** (6), 1008 (2012).
[ZZDS14] Jiang Zhang and Zhenfeng Zhang and Jintai Ding and Michael Snook, Authenticated Key Exchange from Ideal Lattices, http://eprint.iacr.org/2014/589 (2014)