BLOCKCHAIN
AT BERKELEY

Post-Quantum Cryptography Deep Dive

October 8, 2017

Welcome! We highly encourage you to spend a few hours focusing on a particular reading / subtopic in your groups. We will allow for short, informal presentations on these readings in **room 310** from 4:00-5:00pm.

Don't worry about making a polished slide deck–try to understand the material and reconstruct this understanding process in a short presentation–with or without slides. We learn best when we teach!

If you don't already have access to our Slack and would like to join to ask questions about the material, use this form. Discussion of this material will be in the #deep-dive channel.

Feel free to leave feedback about our deep dive program. We love hearing from the community and try our best to make these events as enjoyable, informative, and useful as possible.

You're welcome to use rooms 310, 320, 330, and the undergraduate lounge today.

Reading List

This is a comprehensive list of all things post-quantum. Skim the summaries and focus on what interests you most. If unsure, start from the beginning.

Introduction and background

Presentations [intro slides] [intro video] [Rustam's slides]

Bitcoin Is Not Quantum-Safe, And How We Can Fix It When Needed - July 2013 - Vitalik's overview of cryptography used in bitcoin, why breaking it is bad, and proposed solutions. (10 minute read)

A tale of two qubits: how quantum computers work - 2010 - This article explains the basics of quantum computing from a bottom up perspective. It uses the analogy of a polarized pair of sunglasses to describe quantum computing. (35 minute read)

Introduction to post-quantum cryptography - 2009 - This is a technical paper by Daniel J. Bernstein. It is an overview of the state of how quantum computers will impact cryptography, and an introduction to the simpler post-quantum cryptosystems. (30 minute read)

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems - 1978 - This is the original RSA paper by Rivest, Shamir, and Adleman detailing the eponymous public-key cryptosystem. Sixteen years later, Peter Shor showed that a quantum computer could break RSA. (15 pages)

An overview of cryptography - Summarizes cryptography in today's world; a good reference text. (long)

Quantum Computing

Timeline of quantum computing - Self-explanatory.

Quantum Computing and Shor's Algorithm - 1999 - An engaging and easy-to-read reference text for quantum computing and Shor's. Difference between a classical and quantum computer; important primitives, breakthroughs, theses; step-by-step through Shor's.

Grover's description of quantum computing - 1999 - "How the weird logic of the subatomic world could make it possible for machines to calculate millions of times faster than they do today". Pleasant read, written like a story. (25 minute read)

Shor, I'll do it - 2007 **-** Scott Aaronson's overview of Shor's algorithm; praised by Shor. (12 minute read)

Shor's Algorithm – Breaking RSA Encryption - April 2014 - Similar to the above, more comprehensive. (15 minute read)

A fast quantum mechanical algorithm for database search - 1996 - Grover's original paper on the eponymous quantum search algorithm. This paper describes the full algorithm and how it can be used to search a database for a specific entry in an efficient manner. (30 minute read)

From Schrödinger's Equation to the Quantum Search Algorithm - 2001 - Abstract: "The quantum search algorithm is a technique for searching possibilities in only steps. Although the algorithm itself is widely known, not so well known is the series of steps that first led to it, these are quite different from any of the generally known forms of the algorithm. This paper describes these steps, which start by discretizing Schrödinger's equation. This paper also provides a self-contained introduction to quantum computing algorithms from a new perspective" (35 minute read)

Shor's discrete logarithm quantum algorithm for elliptic curves - 2008 - In the preliminary section it explains how Shor's algorithm (Solving the Hidden subgroup problem) applies to DLP / ECDLP. The actual content of the paper goes a step further and shows how to efficiently construct the quantum algorithm for ECDLP. (34 pages)

Applying Grover's algorithm to AES: quantum resource estimates - 2015 - "We present quantum circuits to implement an exhaustive key search for the Advanced Encryption Standard (AES) and analyze the quantum resources required to carry out such an attack. We consider the overall circuit size, the number of qubits, and the circuit depth as measures for the cost of the presented quantum algorithms… " (13 pages)

Quantum Money via the No Cloning Theorem - 2016 - (Just read the Quantum Money section) This article discusses an alternate proposal for electronic money. (4 minute read)

Related projects

RFC Draft to include NTRU in TLS - 2002 - "This document defines a group of new TLS cipher suites that utilize the NTRU encryption algorithm and the NSS signature algorithm. These cipher suites are designed to maximize computational efficiency on both the client and server sides and ease deployment of the TLS protocol on constrained and embedded devices. The document assumes the reader is familiar with the TLS protocol." (medium long)

QRUX - quantum secure blockchain - QRUX website; co-founder and algorithm inventor Prof. Rustam Islamov will give a lightning talk at today's event.

Quantum Resistant Ledger whitepaper - 2016 - A quantum-resistant cryptocurrency; technical description. (15 pages) You can find an updated 7-page description of QRL's proof-of-stake consensus algorithm here.

Quantum Money via Knots - 2010 - A paper co-authored by Peter Shor which describes how money is achievable via quantum cryptography. (This is money that a mint could theoretically produce, and anyone with a quantum computer could verify the authenticity of) (22 pages)

Post Quantum Cryptosystems

Post Quantum RSA - April 2017 - “This paper proposes RSA parameters for which (1) key generation, encryption, decryption, signing, and verification are feasible on today’s computers while (2) all known attacks are infeasible, even assuming highly scalable quantum computers. As part of the performance analysis, this paper introduces a new algorithm to generate a batch of primes. As part of the attack analysis, this paper introduces a new quantum factorization algorithm that is often much faster than Shor’s algorithm and much faster than pre-quantum factorization algorithms... ” (20 pages)

Lattice Signatures and Bimodal Gaussians - 2013 - Paper introducing BLISS (the Bimodal Lattice Signature Scheme). BLISS was suggested for refinement and later standardization by the National Institute of Standards and Technology. (41 pages)

Transcript secure signatures based on modular lattices - 2014 - Post-quantum signature scheme, referred to as NTRU Modular Lattice Signature Scheme (NTRUMLS). (21 pages)

Misc and further reading

Quantum Algorithms via Linear Algebra (Book) - Really useful book which explains how quantum algorithms are constructed, from a purely mathematical perspective. (The physics interpretation of the gates for example are not discussed) The book details Shor's Algorithm and Grover's Algorithm in detail also.

Lattice Based Cryptography for Beginners - A very in-depth introduction to lattice-based cryptography, “which is thought to be a cryptosystem of post-quantum age.” (121 pages)

Ways to get involved with Blockchain at Berkeley

Upcoming events:

- Monday 10/9: Berkeley Bitcoin Meetup with Shin'ichiro Matsuo
- More events next weekend! Stay tuned.

Be updated on our educational and community events by liking our Facebook page, joining our Facebook group, signing up for our newsletter, joining our Meetup, and/or joining our Slack team. We also encourage you to follow us on Twitter and subscribe to our YouTube channel for recordings of our lectures and presentations.

If you are a Berkeley student and are interested in getting involved with B@B consulting or research this fall, we urge you to join the Slack team and reach out to our officers to be included in our summer engagement program. Moreover, our application will open the first week of the fall semester (during which we will have a formal infosession).

Research inquiries: innovation@blockchain.berkeley.edu
Consulting inquiries: consulting@blockchain.berkeley.edu
Education inquiries: education@blockchain.berkeley.edu
Administration: admin@blockchain.berkeley.edu