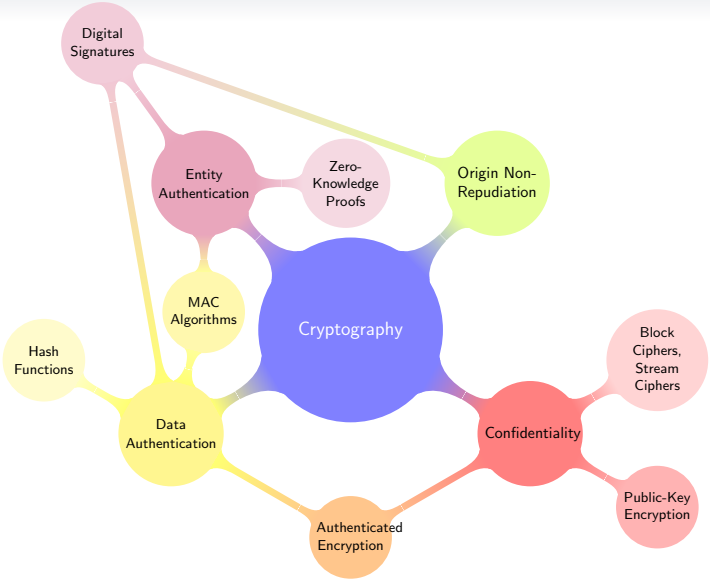
What is cryptography?

SIAM Mini-Conference 2025

Gaurish Korpal

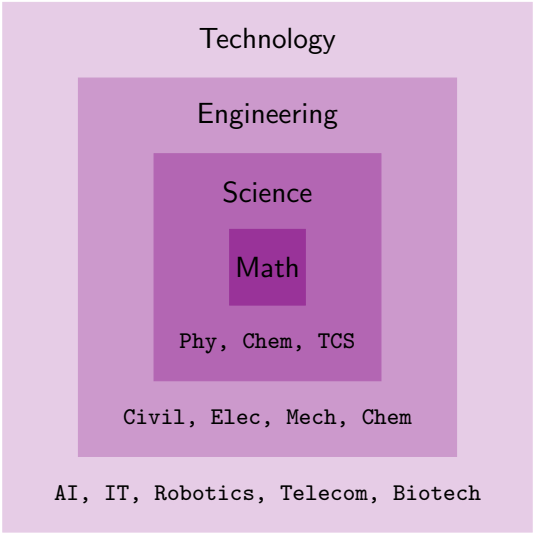
University of Arizona

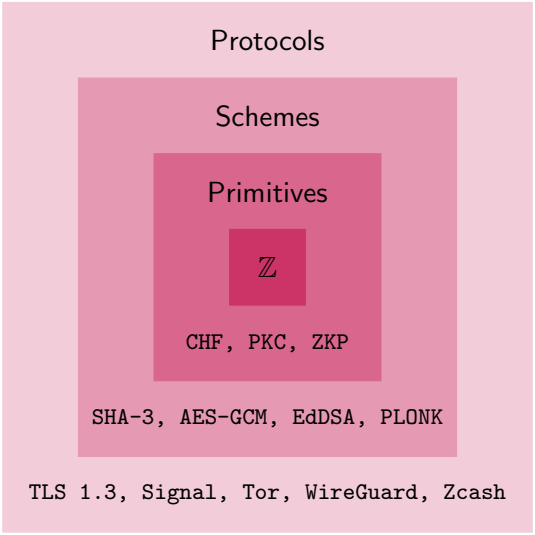
May 02, 2025



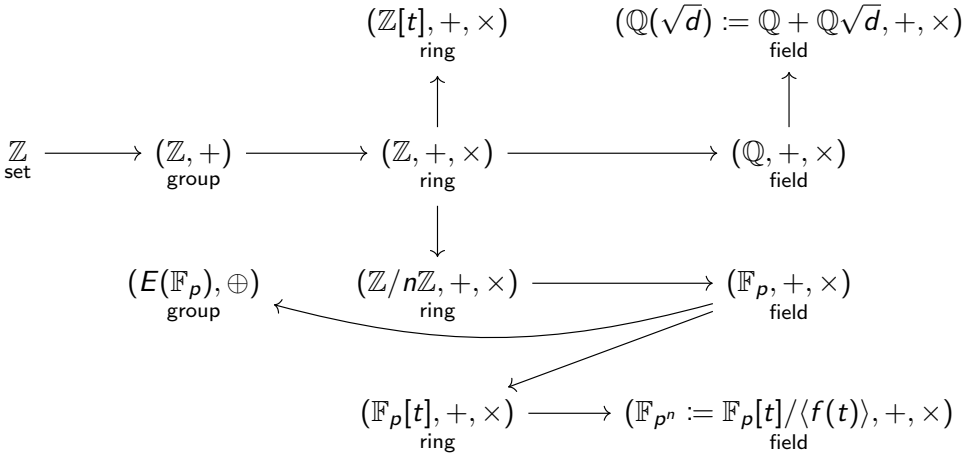
Introduction

Propaganda


Technology
Engineering
Science
Math
Phy, Chem, TCS
Civil, Elec, Mech, Chem
AI, IT, Robotics, Telecom, Biotech


Protocols
Schemes
Primitives
$\mathbb{Z}$
CHF, PKC, ZKP
SHA-3, AES-GCM, EdDSA, PLONK
TLS 1.3, Signal, Tor, WireGuard, Zcash

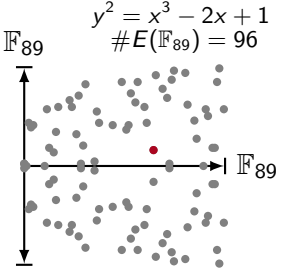
Algebra primer



Pairing-based cryptography

Elliptic curves

- $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \neq 0$.
- Points $E(\mathbb{F}_p)$ form a group with $\mathcal{O}_E$ as identity.
- $P \in E(\mathbb{F}_p)[r]$, that is $\underbrace{P \oplus \cdots \oplus P}_{r\text{-times}} = [r]P = \mathcal{O}_E$.
- ECDLP: Given $Q = [m]P$, find m.



For r prime to p there exists a non-degenerate distorted bilinear map:

$$e_r : E(\mathbb{F}_p)[r] \times E(\mathbb{F}_p)[r] \to \mathbb{F}_{p^u}^{\times}$$

u is called the embedding degree of E w.r.t. r.

- $e_r(aP, bQ) = e_r(P, Q)^{ab}$
- $e_r(Q, Q) \neq 1$
- If $e_r(Q_1, Q_2) = 1$ for all $Q_1 \in E(\mathbb{F}_p)[r]$ then $Q_2 = \mathcal{O}_E$.

Scout's honor!

Short Signature

- Supports non-interactive aggregation property: given a collection of signatures $(\sigma_1, \ldots, \sigma_n)$, anyone can produce a short signature (σ) that authenticates the entire collection.
- BLS short signature (2001) is relies on pairing-friendly curves.
- Ethereum blockchain uses BLS signatures.

Polynomial Commitment Scheme

- Allows one party to prove to another the correct evaluation of a polynomial at some set of points, without revealing any other information about the polynomial.
- KZG polynomial commitment (2010) relies on pairing-friendly curves.
- Irrespective of the degree of the polynomial, KZG commitment size is constant.

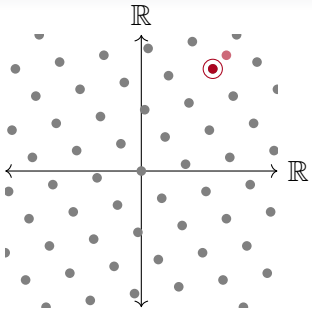
datatracker.ietf.org/doc/draft-boneh-bls-signature/

https://risencrypto.github.io/Kate/

Lattice-based cryptography

Lattices

- A lattice Λ is a discrete subgroup of $\mathbb{R}^n$. Given basis matrix $B \in \mathbb{R}^{m \times n}$, $\Lambda = \{B\mathbf{x} \mid \mathbf{x} \in \mathbb{Z}^n\}$
- CVP: Find a vector closest to given vector $\mathbf{v} \in \Lambda$.
- LWE: Given $A \in \mathbb{F}_p^{m \times n}$ and $\mathbf{b} \in \mathbb{F}_p^m$ such that $A \cdot \mathbf{s} + \mathbf{e} = \mathbf{b}$ find $\mathbf{s} \in \mathbb{F}_p^n$ for unknown error $\mathbf{e} \in \mathbb{F}_p^m$.
- LWE$\leftrightarrow$CVP: The lattice vector $A \cdot \mathbf{s}$ with distance $\mathbf{e}$ is almost always a vector closest to $\mathbf{b}$.



Let $f \in \mathbb{Z}[t]$ be a monic polynomial of degree n and consider the ring $R \coloneqq \mathbb{Z}[t]/f$ and ideal $I \subset R$.

$$(R, +) \longleftrightarrow (\mathbb{Z}^n, +) \quad \text{and} \quad I \longleftrightarrow \Lambda$$

Multiplicative closure property of ideal lattice results in bonus geometric symmetries.

- $I \subseteq R$ is called an ideal if it is a subgroup of $(R, +)$ that absorbs multiplication by elements of R.
- If $I = \alpha R$ then I is principal ideal.
- $\mathbb{Z}[t]/f = \{g \mod f \mid g \in \mathbb{Z}[t]\}$ where $\deg(g \mod f) < \deg(f)$.

Bend, don't break!

Post-Quantum Cryptography

- Symmetric cryptography do not rely on mathematics vulnerable to quantum computers.
- Security of common key exchange and digital signature schemes rely on hardness of factorization and discrete logarithm, vulnerable to Shor's quantum algorithm.
- Cryptographic Suite for Algebraic Lattices (CRYSTALS) is one of the first standardized PQC scheme (2024).

https://pq-crystals.org/index.shtml

Fully Homomorphic Encryption

- Homomorphic refers to homomorphism in algebra: $\varphi(a \oplus b) = \varphi(a) \otimes \varphi(b)$
- Allows computations to be performed on encrypted data without first having to decrypt it.
- Gentry constructed the first ever FHE scheme using ideal lattices (2009).
- All known fully-homomorphic encryption schemes with compact ciphertexts use lattice techniques.

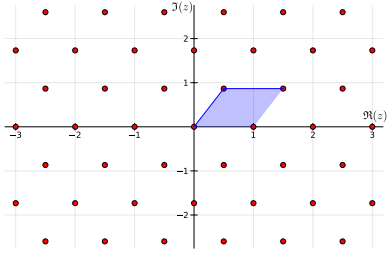
https://fhe.org/history/

Class-group-based cryptography

Imaginary quadratic orders

- Let $D < 0$ be such that $D \equiv 0, 1 \pmod 4$. Then the ring $\mathbb{Z}[\omega] = \mathbb{Z} + \mathbb{Z}\omega$ where $\omega = \frac{D+\sqrt{D}}{2}$ is called an imaginary quadratic order of discriminant D.
- The field of fractions is $\mathbb{Q}(\sqrt{D})$.
- A fractional ideal of $\mathbb{Z}[\omega]$ is a subset $J \subset \mathbb{Q}(\sqrt{D})$ such that aJ is an ideal of $\mathbb{Z}[\omega]$ for some $a \in \mathbb{N}$.
- J is invertible if there is fractional ideal J' such that $JJ' := \{\sum_{i=1}^{n} a_i b_i \mid a_i \in J, b_i \in J'\} = \mathbb{Z}[\omega]$.

$\mathbb{Z}\left[\frac{-3+\sqrt{-3}}{2}\right]$ in $\mathbb{C}$



- The class group $\mathrm{Cl}(D)$ of $\mathbb{Z}[\omega]$ is the quotient group of invertible fractional ideals by principal ideals with ideal multiplication.
- It is a composite order group of unknown order with a subgroup of known order where the DL is easy.

DDH for $\mathrm{Cl}(D)$ can be characterized as a HSM since it is hard to determine if a given element is a member of $\mathrm{Cl}(D)$.

Rest assured!

Multi-Party Computation

- Allows a group of mutually distrustful parties to compute a joint function on their inputs without revealing any information beyond the result of the computation.
- Class groups were first proposed as an alternative to ECC, but CL attack broke it.
- Ideas from the CL attack make class groups well-suited for MPC protocols that require a one-time transparent setup with minimal interaction among parties.

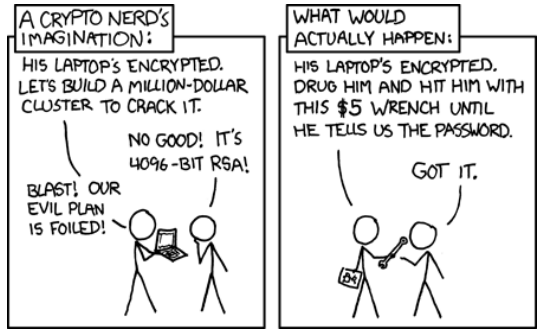
Verifiable Delay Function

- Allows a prover to show a verifier that a certain amount of time running a function was spent, and do it in a way that the verifier can check the result quickly.
- Groups of unknown order are great candidates for VDF construction.
- Class groups are one of the most popular choice because the can be generated without trusted setup (Wesolowski, 2018)

https://eprint.iacr.org/2022/1466.pdf

https://eprint.iacr.org/2018/712.pdf

Thank you!



Randall Munroe, Security. https://xkcd.com/538/.