Quantum Computing, Codes, Cryptography, Cryptanalysis - QC^4

04 Sep 2025, PKIA 2025, Bangalore

08 Sep 2025, Amrita Vishwa Vidyapeetham

C.E.Veni Madhavan

Department of CSA, Indian Institute of Science, Bangalore
Center for Cyber Security, Amrita Vishwa Vidyapeetham, Coimbatore

August 31, 2025

14 April, World Quantum Day

World Quantum Day in commemoration Planck's constant

$4.14 * 10^{-15}$ **ev.s**

United Nations'

International Year of Quantum Science and Technology 2025

Previous Talks

25-28, March 2024, IISc, Bangalore
1 - 4 May 2024, Amrita Vishwa Vidyapeetham
13 Dec 2024, Amrita Vishwa Vidyapeetham
02 Jan 2025, Amrita Vishwa Vidyapeetham
19 Mar 2025, CDAC Bangalore
15 Apr 2025 (World Quantum day+1), Home
16 Apr 2025, Amrita Vishwa Vidyapeetham
04 Sep 2025, PKIA 2025
08 Sep 2025, Amrita Vishwa Vidyapeetham

updates
(250324,010524,210524,131224,020125,190325,150425,160425,040925)

Contents I

Contents II

Contents III

Contents IV

Contents II.5 Quantum Codes : Lectures

- II.5.0. Quantum Computing, Codes, Cryptography, Cryptanalysis - resources, capsule, summary
- II.5.1. Quantum Codes - basics, motivation, classical-quantum domains, cat qubits, color codes, magic states, ML decoding
- II.5.2. Quantum Coding, Decoding, CSS codes
- II.5.3. Tutorial on Quantum Codes [Steane 2006]
- II.5.4. Hamming Quasi-Cyclic Code based KEM
- II.5.5. Xanadu breakthrough in QEC reduces qubit overheads:, Linear-optical quantum computation with arbitrary error-correcting codes, Xanadu Quantum Tech., U.Waterloo. 20 pp, arXiv Aug. 2024.
- II.5.6. Qiskit in Practice: a step-by-step guide to programming with popular quantum framework [Quantum Zeitgeist, Oct 2024] Simulating a bosonic error correction code using Bosonic Qiskit
- II.5.7. FPGA-based distributed union-find decoder for surface codes, IEEE Trans. Quant. Engg., Lianage, Wu, Tagare, Zhong, Oct 2024.

Contents II.5 Quantum Codes : Lectures

- II.5.8. Spatially coupled QLDPC codes, Yang, Calderbank, 21 Feb 2025, 36 pp, 66 refs.
- II.5.9. Gottesman-Kitaev-Preskill Codes: A Lattice Perspective, Conrad, Eisert, Arzani, Feb 2022, 30 pp, 53 refs.
- II.5.10. Good Gottesman-Kitaev-Preskill Codes from the NTRU cryptosystem, Conrad, Eisert, Seifert, Jul 2024, 26 pp, 71 refs.
- II.5.11. Quantum error correction below the surface code threshold, Google, 300+ authors, arXiv Dec 2024, Nature, Feb 2025, 8 pp, 53 refs.
- II.5.12. Sparse blossom : correcting million errors per core second with minimum weight matching, Higgott, Gidney, arXiv Jan 2025, 37 pp, 50 refs.
- II.5.13. Concatenate codes, save qubits, Yoshida et al, arXiv Feb 2024, 27 pp, 62 refs.
- II.5.?? References: MUSTREAD related papers (≥ 55 as on 31 Aug 2025)

II.5.0. Quantum Computing, Codes, Cryptography, and Cryptanalysis

Resources

- CalTech lectures by Prof.John Preskill
- U. Rochester lectures by Prof.A.C.Quillen
- My lectures on Cryptography, Cryptanalysis
- Papers : arXiv, PRX Quantum, Nature
- Books: general purpose, special purpose
- Software: general purpose, special purpose
  (my C codes, Python, Sage, Qiskit, MPI, CUDA)
- Standards: NIST, FIPS, ETSI
- Current Announcements: Quanta, Quantum Zeitgeist, Quantum Insider

II.5.0. Quantum Codes

Brief History : Chronology of Developments

- Peres, Bit-flip code 1995
- Shor code 9 qubits for 1 qubit correction 1996
- Laflamme et al 5 qubit perfect code 1996
- Steane code 7 qubits for 1 qubit correction 1997
- Calderbank, Steane, Shor code 1997
- Gottesman Stabilizer code 1997
- Knill, Lflamme, Nec. and Suff. Condn. for QECC recovery 1997
- Kitaev toric codes : topological quantum field theory 1997
- Bravyi, Kitaev: Surface codes 1998
- Grassl et al: Quantum RS codes 1999
- Gottesman surface code : 2D lattice of qubits, 1 qubit correction 2002
- Bacon-Shor subsystem code 2006

II.5.0. Quantum Codes

Brief History : Chronology of Developments

- Brun wt al: E(entanglement)A(assisted) QECC 2006
- 3D color code : almost a generalization of surface code 2006
- Aly: Quantum BCH codes 2008
- Hsieh et al: Quantum LDPC codes 2009
- hypergraph product codes (combination of codes) 2009
- Guardia: Asymmetric Quantum RS codes 2012
- homological product graph codes; transversal gates 2013
- flag-qubit code : combination of codes; transversal gates 2020
- Nadkarni: EA qudit stabilizer codes 2021
- Chandra et al: Universal decoding of QECC using GRAND 2023
- many other codes
  Error Correction Zoo: List of codes in the quantum domain, 47 pp, 547 codes (list 17 pp) 700 refs (30 pp). 2025

II.5.0. Quantum Codes : Basics

- elements: qubits, gates, circuits
- errors; gate, decoherence, measurement, crosstalk
- classical and quantum ECC (error correction codes)
- fundamentals of QEC : 5 steps : state preparation, stabilizer circuit, error detection, error decoder, error correction
- stabilizers : operators that fix quantum states: $A \mid \psi\rangle = \psi$.
- they are tensor products of Pauli matrices I, X, Y, Z; constitute the Pauli group $P = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$.
- a stabilizer (or stabilizer generator) that acts on n qubits is a maximal set of n commuting elements of the Pauli group P with eigenvalue 1.
- structure of the stabilizer generator w.r.t errors

II.5.0. Quantum Codes : Basics

- topological codes such as toric codes, surface codes, color codes exploit global lattice-like structures, making resistant to local errors
- encoding circuits : logical codeword qubits to codeword physical qubits: assembly of repetitive elements : plaquettes, vertices, edges, faces
- practical QECC for different mechanics : superconducting, ion traps, photonics
- decoding algorithms: syndrome measurement, lookup table; MWPM; Union-Find; MLH, belief propagation (BP) networks; other classical decoding
- challenges: scalability; decoding complexity; resource overheads; noise modeling; fault-tolerant gates;

II.0. Quantum Error Correction : A Capsule

based on

PHY265 Introduction to Quantum Error Correction, A.C.Quillen, U. Rochester, Mar 2025, 58 PP.

- entanglements are fragile; gate errors accumulate; use extra qubits for detection and correction of errors without disturbing state of computations
- classically repetition codes; qubit is a continuum of probabilities;
- QEC is a mapping of, k qubits (2^k Hilbert space) into n qubits (2^n Hilbert space); the k logical (encoded) qubits into n physical qubits, with the additional $n-k$ redundant qubits for protection
- Peres 3 qubit bit-flip ECC; use ancillae; syndrome computation circuit
- bit-flip errors, described by Pauli X operator, can be corrected; but phase-flip errors, described by Pauli Z operator, can not be corrected.
- a different 3-bit phase-flip code can be constructed
- Shor 9-bit code uses 9 bits to correct for both
- syndrome measurements for detection of errors should not disturb the superposition of the logical states; this is guaranteed by a n.a.s.c

II.0. Quantum Error Correction : A Capsule

based on
PHY265 Introduction to Quantum Error Correction, A.C.Quillen, U. Rochester, Mar 2025, 58 PP.

- a stabilizer group is a subgroup of the Pauli group, that fixes every element of the subspace of vector; there are generating elements for the stabilizer group; the generators commute, they are self-inverses
- measurements, normalizers, centralizers
- Quantum Hamming bound on correctable errors
- CSS code
- topological ECC : stabilizer codes on 2-D lattice (surface code) with stabilizers composed of local (near neighbor qubits) operators
- Q-dit toric codes
- bosonic codes - exploit redundancy within a single physical system - infinite dimensional (energy levels) quantum harmonic oscillator states
- Majorana fermion topological qubit surface codes

II.5.1. Classical and Quantum Codes - Motivation

Error Control Codes have a great role to play in all aspects of *Quantum Computing, Cryptography and Cryptanalysis*. The *three* facets are:

- Fault-tolerant quantum computing: (supremacy, utility, advantage)
- (post) Quantum Cryptography: (encryption, key exchange, signatures)
- (post Quantum) Cryptanalysis: (lattice geometry, algebra, combinatorics)

II.5.1. Quantum Codes - a Motivation

Shor's algorithm for factoring integers works, broadly, as follows:
solve quadratic congruence => determine orders of many elements
=> perform modular exponentions, => large number of $|A\rangle$ states with $|A\rangle = |0\rangle_L + \exp^{i\pi/4} |1\rangle$ (L for logical qb)
=> estimate phase of eigen values corresponding to certain eigen operators
=> compute quantum Fourier transform to required precision
(A.N.Cleland, *An introduction to surface code*, SciPost Phys. Lect.Notes, V49, 2022, pp 75.)

- A powerful QEC mechanism is by *surface codes*
- the precision for $|A\rangle$ states, determines the surface code specs.
- for RSA2048 precision is 1 in 10^{17} to 10^{18}, achieved by a process called *magic state distillation*
- 2^{28} or 256 million physical qb are required for RSA2048 factoring (in about an hour!)

II.5.1. Quantum Codes - a Motivation

How to factor 2048 bit RSA integers with less than a million noisy qubits, Gidney, arXiv May 2025, 40 pp.

- Gidney, Ekera, 2019 : estimate 20 million qubits, 8 hours
- Gidney, May 2025 improves : less than 1 million noisy qubits, 1 week
- qubits - square grid, nearest neighbor connection, uniform gate error rate of 0.1%, surface code cycle time of 1 microsec, control system reaction time of 10 microsec.
- reduction due to approximate residue arithmetic, storing idle logical qb with *yoked surface codes*. allocating less space to magic state distillation by using magic state cultivation.
- longer runtime due to more Toffoli gates, and fewer magic state factories.
- *Yoked surface codes*, Gidney et al, Nature Commun., May 2025, 8 pp.

II.5.1. Quantum Codes - a Motivation

How to factor 2048 bit RSA integers with less than a million noisy qubits, Gidney, arXiv May2025, 40 pp.

- surface codes- leading candidate quantum memory - but requires a thousand physical qubits per logical qubit to reach relevant logical error rates.
- we introduce, a hierarchical memory formed from surface codes concatenated into high density parity check codes.
- these yoked surface codes are organized in a rectangular grid with parity checks (yokes) measured along rows, columns using *lattice surgery*.
- surface code : highly forgiving qubit quality, low (only nearest neighbor) connectivity; but large ratio (1000 to 2000) of pqb to lqb.
- the quantum parity check codes are CSS codes, a generalization of classical parity check codes.

II.5.1. Quantum Codes - Classical-Quantum Domains

The earliest quantum codes were inspired by good classical codes. An early, pioneering, work is by
A.R.Calderbank, E.M.Rains, P.W.Shor, N.J.A.Sloane, *Quantum error correction via codes over GF(4)*, IEEE Info Th., 1998.

- A CSS code (Calderbank-Shor-Steane) uses the classical $[7, 4, 3]$ Hamming code to correct for both qubit flip errors (X errors) and phase flip errors (Z errors).
- The code encodes 1 logical qubit in 7 physical qb, and correct arbitrary single qb errors
- Steane showed an enlargement of such basic quantum codes
- a QECC is an eigen-space of a commutative subgroup of the group E of tensor product of Pauli matrices
- commutativity condition : $H_x.H_x^t + H_z.H_z^t = 0$, where H_x, H_z are $(n - kxn)$ are binary matrices, which together form the *stabilizer* $\mathcal{H} = (H_x|H_z)$.

II.5.1. Quantum Codes

An interesting recent result is:
S.H.Lee et al. *Low-overhead magic state distillation with color codes*, Sep 2024, 42pp.

- *fault-tolerant* implementation of non-Clifford gates is challenging for achieving *universal QC* with QECC
- *magic state distillation*, requiring large, extra resources, need to be optimized for specific codes
- such a class of *color* codes are superior to *surface* codes
- new results on higher encoding rates, transversal implementation of Clifford gates, and efficient *lattice surgery*
- 2D color code lattice : a 3-valent, 3-colorable lattice; one defines Pauli operators X, Y, Z, chains
- define error flips of qubits; detection of errors from check measurements
- logical qubits are encoded in *patches*
- logical operations on qubits in Pauli bases are defined

II.5.1. Quantum Codes

- logical operations generating the Clifford group - Hadamard, phase, CNOT gates are implemented *transversally*
- more technicalities : *domain walls*, *faulty measurements*, *lattice surgery*, *magic state distillation* (MSD) procedure
- *resource estimation - space* : physical qubits = data + syndrome qb
- *resource estimation - time* : number of measurement steps
- *performance estimation - error rates* depend upon MSD, and the specific decoder:
- concatenated *minimum weight perfect matching* (MWPM) algorithm

II.5.1. Quantum Codes

A recent paper presents progress toward fault-tolerant, practicable quantum computing framework. *Learning high-accuracy error decoding for quantum processors*, J.Bausch et al (18 authors of Google), Nature, Nov 2024. 28 pp.

- multiple physical qubits to ONE logical qubit
- for factoring RSA2048 we need error rates of 10^{-12} per logical gate op, compared to today's 10^{-3} per physical op.
- currently *surface code* is the most promising - one lqb (logical qubit) to *dxd* pqb called *data qubits*
- errors detected by periodical measuring X, Z stabilizer checks on dqb, using $d^2 - 1$stabilizer qb located between dqb
- qubits and ops are all prone to errors - X (bit flips), Z (phase flips) and Y (combined bit, phase flips)
- a *detection event* occurs - 2 consec measurements of same stabilizer give different parity outcomes
- the pair of observables X, Z$->$ logical state of surface code qb(scqb)

II.5.1. Quantum Codes

- the minimum length is the *code distance* (the number of errors for changing the lqb without flipping a stabilizer check (d in the d^2 dqb grid)
- error correction decoder : from history of stabilizer measurements, error syndromes computes the correction to the noisy measurements
- quantum error correction is *different* from classical-
- need to cope with complex noise effects, leakage of states, cross talk
- these defy some common QECD such as *minimum weight perfect matching* (MWPM)
- challenging to model quantum devices noises
- hence, in principle, it may be better to learn and adapt from realistic noise sources $->$ realistic noisy hw based fault-tolerance
- many ML based decoders in literature

II.5.1. Quantum Codes

- In a recent work the authors present *AlphaQubit* a *recurrent-transformer neural network* that predicts errors in logical observables based on syndrome inputs
- its performance tested on Google Sycamore surface code better than previous ML, non-ML methods
- a major feature of the ML approach is the power of learning from the experimental data
- still to achieve : decoding speed (thruput) 1 μsec per round for super-conducting qb; 1 msec for trapped-ion qb

II.5.1. Quantum Codes

- A.Guillaud, J.Cohen, M,Mairahmi, *Quantum computation with cat qubits*,2023.
- qubits stabilized by a multi-photon driven dissipation process
- self-correcting qubit where bit flip errors are robustly, exponentially suppressed
- toward hardware efficient, fault-tolerant quantum processor
- The company *Alice & Bob* 2030 Road map to useful quantum computers

II.5.1. Quantum Codes: Decoding

The question of speed of decoding in the context of quantum computing is even more vital than in classical computing, in view of the exponential load mismatch situation. The recent paper, addresses this issue:
Caune et al (25 authors from Riverlane, Rigetti, Sheffield), *Real-time, low-latency quantum error correction with super-conducting qubits*, Oct 2024.

- Note that it is sufficient apply correction to only a finite set of errors - than a continuum of analogue values :
- Pauli bases for 2d unitary matrices: I ((1,0),0,1)); X, ((0,1),(1,0)); Y ((0,-i),(i,0)); Z ((1,0)(0,-1))
- design the syndrome table for the 2 qb code which detects an error
- build a 3 qubit code for detection and correction
- info content in 1 qb is entangles with 2 redundancy qb $|0\rangle_2, |0\rangle_3$ to create a logical qb $\psi\rangle_L$
- Shor 9qb code $[[9, 1, 3]]$ by code *concatenation* of bit-flip, and phase-flip code

II.5.1. Quantum Codes: Decoding

- generalize to a *surface* code by patching together repeated elements
- decoding with a syndrome table lookup is infeasible for $n > 40$
- *minimum weight perfect matching* algorithm for identifying error chains between positive syndrome measurements, is quite efficient
- FPGA decoder integrated into the control system of a super-conducting QP
- 8-qb stability experiment with up to 25 decoding rounds, and a mean decoding time per round below 1 μ sec, thus avoiding the *backlog* problem

II.5.2. Quantum Coding,Decoding

1. *Stabilizer codes*, D.Gottesman, Thesis, 122 pp., 1997, arXiv 2024.
2. *QEC Introduction*, J.Roffe, 2019.
3. *Tutorial on QEC*, A.M.Steane, 2006.
4. *QEC*. Book Chapter 7, 90 pp (Preskill Lectures).
5. *Theory of QEC*, E.Knill, R.Laflamme, 34 pp.,LosAlamos TR, 1999.
6. *Knill-Laflamme conditions on correctable errors*, Lecture 4, QEC, UC Berkeley, J.Wright, Sep. 2024.
7. *Near optimal performance of QECC*, Zheng et al., 19 pp., arXiv, Jun 2024.
8. *Weight reduced stabilizer codes with lower overheads*, Sabo et al, PRX Quantum, 43 pp., Oct 2024.
9. *2D local implementation of QLDPC*, Bertheusen,..A.M.Childs,... D.Gottesman, PRX Quantum, 18 pp. 9 Jan 2025.
10. *Bosonic coding - introduction and use cases*, V.V.Albert, 31 pp., arXiv, Nov. 2022.

1. (see paper Section 7.1 on a quantum error correction)
2. (see paper Section 7.2 criteria for quantum error correction)
3. (see paper Section 7.3 general properties of QECC's) distance, located errors, error detection, quantum codes and entanglement
4. (see paper Section 7.4 probability of failure)
5. **Book Ch 7 : 7.5 Classical Codes**
   1. $< n, k, d >$ code $\mathcal{C}$ - k-dim subspace of F_2^n, basis $v_1, \ldots, v_k$
   2. k-bit msg $\alpha - (\alpha_1, \ldots, \alpha_k)$ encoded as $v(\alpha) = \sum(\alpha_i v_i)$
   3. generator matrix $k \times n$, $G = (v_1, \ldots, v_k)^T$; $v(\alpha) = \alpha G$
   4. alternatively, parity check matrix $(n-k) \times n)$, H, s.t. $Hv = 0 \forall v \in \mathcal{C}$. Note $HG^T = 0$
   5. error $\Rightarrow v \rightarrow v + e$, $H(v+e) = Hv + He = He$ and He is called the syndrome of error e
   6. if all syndromes are distint then unambiguous recovery by flipping the bits of e, since $v + e \rightarrow v + e + e = v$
   7. if $He_1 = He_2, e_1 \neq e_2$, then attempted recovery $v + e_1 \rightarrow v + e_1 + e_2$
   8. distance d is the minimum weight of any $v \in \mathcal{C}$; a linear code with $d = 2t + 1$ can correct t errors; the code assigns a distinct syndrome to each $ev \in \mathcal{E}$ containing all vectors of weight $\leq t$

9. *Proof* if $He_1 = He_2$, then $0 = He_1 + He_2 = H(e_1 + e_2)$, hence $e_1 + e_2 \in \mathcal{C}$; if e_1, e_2 with weights $\leq t$, and distinct from 0, their sum is of weight $\leq 2t$; since min distance is $2t + 1$, there is no vector in $\mathcal{C}$; hence He_1 and He_2 can not be equal.
10. *dual code*: We have $HG^T \Rightarrow GH^T = 0$. Thus we have H^T as the generator and G as the parity check matrix of $n - k$ dimensional code $C^\perp$ called the dual of C
11. $C^\perp$ is the orthogonal complement of C in F_2^n. A vector is *self-orthogonal* of it is of even weight. A code C contains its dual if all its code words are of even weight and are mutually orthogonal.
12. if $n = 2k$, it is possible that $C = C^\perp$. THen C is *self-dual*.
13. Important identity:

$$\sum_{v \in C} (-1)^{v.u} = 2^k, u \in C^\perp, 0$$

otherwise.

6. Ch 7.6 CSS codes
   1. classical linear ECC principles can be adapted for QECC
   2. Calderbank-Shor-Steane (CSS) code adapts the concept of a dual code
   3. Let code $C_1, (n-k_1) \times n$, parity check matrix H_1 and let *subcode* $C_2, (n-k_2) \times n$, parity check matrix $H_2, k_2 < k_1$; first $n-k_2$ rows of H_2 coincide with those of H_1
   4. thus words in C_2 are contained in C_1; but satisfy additional constraints; subcode C_2 defines an equivalence relation in C_1; $u, v \in C_1, u \equiv v$ iff $\exists w \in C_2 s.t. v = u + w$; these eq.classes are the *cosets* of C_2 in C_1
   5. A CSS code is a $k = k_1 - k_2$ *quantum code* that associates a codeword with each eq. class.
   6. element of a basis for the code subspace is

$$|\overline{w}\rangle = \frac{1}{\sqrt{(2^{k_2})}} \sum_{v \in C_2} |v + w\rangle$$

   7. an equally weighted superposition of all the words on the coset of w; there are $2^{k_1-k_2}$ cosets or linearly inde[pendent codewords

8. The states $|\overline{w}\rangle$ are normalized and mutually orthogonal: i.e. $\langle\overline{w}|\overline{w'}\rangle = 0$ if w, w' are in different cosets
9. apply bitwise Hadamard transform:

$$\mathbf{H}^{(n)} : |w\rangle_F \equiv \frac{1}{\sqrt{(2^{k_2}}} \sum_{v \in C_2} |v + w\rangle$$

$$\rightarrow |w\rangle_P \equiv \frac{1}{\sqrt{(2^n)}} \sum_u \frac{1}{\sqrt{(2^{k_2}}} \sum_{v \in C_2} (-1)^{u.v} (1)^{u.w} |u\rangle$$

$$= \frac{1}{\sqrt{(2^{n-k_2})}} \sum_{u \in C_2^{\perp}} (-1)^{u.w} |u\rangle$$

10. this is a coherent superposition, weighted by phases,of words in the dual code $C_2^{\perp}$.
11. Let the distances be s.t. $d_1 \geq 2t_F + 1, d_2 \geq 2t_P + 1$, then the corresponding CSS code can correct t_F bit flips and t_P phase flips.

12. Let $\mathbf{E}_e^F$ denote the Pauli operator with an $\mathbf{X}$ acting at each location i with $e_i = 1$; it acts on state $|v\rangle$ as: $\mathbf{E}_e^F|v\rangle \rightarrow |v+e\rangle$. eqn.7.84
13. Let $\mathbf{E}_e^P$ denote the Pauli operator with a $\mathbf{Z}$ acting at each location i with $e_i = 1$; it acts on state $|v\rangle$ as: $\mathbf{E}_e^P : |v\rangle \rightarrow (-1)^{v\cdot e}|v+e\rangle$, which in Hadamard rotated basis is $\mathbf{E}_e^P : |u\rangle \rightarrow |u+e\rangle$. eqn.7.85
14. (see paper for error processing steps)

7. (see paper Section 7.7 on the 7-qubit code corresponding to the $[n,k,d[= [7,4,3]$ classical Hamming code
8. (see paper Section 7.8 on some constraints on code parameters)
9. (see paper Section 7.9 on Stabilizer codes)
10. (see paper Section 7.10 on a non-CSS stabilizer code : the perfect nondegenrate $[[5,1,3]]$ code
11. (see paper Section 7.11 on an application of QECC $[[5,1,3]]$ for secret sharing.
12. (see paper Section 7.12 on other stabilizer codes)
13. (see paper Section 7.13 on Codes over GF_4
14. (see paper Section 7.14 on good quantum codes) : $[[n,k,d]]$ codes s.t. rate $= k/n$, error probability $p = t/n, t = (f-1)/2$ both approach a nonzero limit as $rightarrow\infty$.

15. (see paper Section 7.15 on some codes that correct multiple errors) concatenated codes, toric codes, Reed-Muller codes, Golay code.
16. (see paper Section 7.16 on quantum channel capacity)
17. (see paper Section 7.17 on Summary, and 7.18 exercises)

II.5.3. Tutorial on Quantum Codes [Steane 2006]

1. *Section 1. Introduction*
2. *Section 2. 3-bit code* Pauli operator $\sigma_x(X) : |0\rangle \rightarrow |1\rangle$ randomly with $p < 1/2$
3. *Section 3. Binary fields and discrete vector spaces*: classical codes
4. *Hamming code [7,4,3]*: e.g. $G =< 85, 102, 120, 7 >^T$
5. the $2^k = 16$ elements of the code are $< 0, 85, 102, 51; 120, 45, 30, 75; 7, 82, 97, 52; 127, 42, 25, 76 >$ (Rules for rows of C : 1st row=0, second row of G + first row; third row of G + the first 2 rows; 4th row of G + the first
6. the parity check matrix $H =< 85, 102, 120 >$
7. check $HG^T = 0$.Note that H is made up of rows of G. Hence, the code $C \in C^{\perp}$
8. *Section 4. Classical error correction* : error correcting code; minimum distance coding; bounds on the size of codes; linear codes, error syndromes
9. *Section 5. Quantum error correction*: digitization of noise; error operators, stabilizer and syndrome extractions; quantum Hamming bound

Berthusen, Devulapalli, Schout, Childs, Cullans, Gorshkov, Gottesman, **2D local implementation of quantum low-density parity-check codes** PRX Quantum, Jan 2025.

1. surface codes : large qubit requirement
2. high rate QLDPC codes encode multiple logical qubits : space reduced
3. but long-range connections are required to extract syndromes
4. SupCond qubits designs allow only 2D nearest neighbors, hence implementing long-range entangling gates require large overhead
5. Recent proposals : complex wiring SC circuits, code concatenation, bosonic cat qubits
6. implementing such long-range connections is easier with neutral atoms, ion traps, spin semiconductor qubits, through qubit movement
7. movement incurs penalties: decoherence, heating, loss
8. we propose to use a *stacked model*
9. geometric locality is an important theoretical, practical factor for QLDPC.
10. circuit simulation shows our protocols have error rates comparable to surface codes with fewer qubits

11. bivariate, bicycle QLDPC codes well suited for parallel syndrome measurement

Background, Routing bounds, Architectures, Simulation

1. Quantum error correction : stabilizer codes
2. Architectures
3. Teleportation routing
4. Stacked model
5. Greedy routing
6. Bilayer Architectures
7. Bivariate-bicyclic codes
8. syndrome extraction circuits
9. space-time decoder
10. circuit level simulation

II.5.4 Hamming Quasi-Cyclic Code based KEM

1. NIST 4th round selection : HQC KEM : IND-CCA2 KEM, small public key; precise decoding failure rate (DFR) analysis; efficient implementation based on classical decoding techniques
2. Aguilar, Aragon, Bettaieb,Bioux, Blazy,Bos, Deneuville, Dion, Gaborit, Lacan, Persichetty, Robert, Veron, Zemor
3. U.Limoge, ISAE Suaero, Wordline, ENAC, U.Toulon, U.Bordeaux, U.Florida
4. Preliminaries and Definitions
5. $S_w^n(F_2) = \{\mathbf{v} \in F_2^n : \omega(\mathbf{v}) = w\}$
6. R poly ring over F_2, irreducible poly, prime integer n is primitive if $(X^n - a)/(X - 1)$ is irreducible in $\mathcal{R}$.
7. ν vector space of dim n over F_2, similar to poly product in R, define vector product $\mathbf{uv} = \mathbf{w}$ with elements $w_k = \sum_{i+j \equiv k \pmod n} u_i v_j, k \in \{0, \ldots n-1\}$

8. **rot**(h) for vectors h denotes the circulant matrix induced by h.
9. Hence the product of any two vector $u, v \in R$ can be expressed as the vector-matrix product :
   $u.v = u \times \mathbf{rot}(v)^T = (\mathbf{rot}(u) \times v^T)^T = v \times \mathbf{rot}(u)^T = b.u$
10. linear code $\mathcal{C}$, of length n, dimension k, denoted $([n, k])$ is a subspace of R of dimension k. Elements are called codewords.
11. $G \in F_2^{k \times n}$ is a generator matrix : $\mathcal{C} = mG, m \in F_2^k$
12. $H \in F_2^{(n-k) \times n}$ is a parity check matrix for $\mathcal{C}$ if H is the generator matrix of the dual code $\mathcal{C}^\perp$, or $\mathcal{C} = \{v \in F_2^n s.t. Hv^T = 0\}$, or $\mathcal{C}^\perp = \{uH, u \in F_2^{n-k}\}$
13. Syndrome of a word $v \in F_2^n$ is Hv^T and we have $v \in \mathcal{C}$ iff $Hv^T = 0$.
14. The minimum distance of $\mathcal{C}$ is $d = \min_{u \neq v \in \mathcal{C}} \omega(u - v)$

15. quasi-cyclic codes shorten the keys by a strategy of Gaborit.
16. quasi-cyclic codes $[sn, k, d]$, consist of code words of size $s \times n$, by viewing the vectors as s blocks of n elements, and each block circularly rotated n times.
17. systematic quasi-cyclic codes $[sn, n]$ code of index s and rate $1/s$ is a quasi-cyclic code with an $(s-1) \times sn$ parity check matrix $H = (I_n, 0, \ldots, A_0)(I_n, 0, \ldots, A_1) \ldots (I_n, 0, \ldots, A_{s-2})$ and $A_0, \ldots, A_{s-2}$ are circulant $n \times n$ matrices.

II.5.5. Xanadu breakthrough in QEC reduces qubit overheads for fault-tolerant computing

Linear-optical quantum computation with arbitrary error-correcting codes, 14 authors, Xanadu Quantum Tech., U.Waterloo. 20 pp, arXiv Aug. 2024, Phys. Rev. Mar 2025., 61 refs.

- Salient points of the paper
  1. high-rate QEC mitigates errors for the imposing scale of fault-tolerant QC
  2. requires efficient generation of non-local many-body entanglements
  3. paper provides a linear-optical architecture with these properties
  4. use Gottesman-Kitaev-Preskill (GKP) qubits on generic lattices
  5. Simulations of hyperbolic surface codes. QLDPC codes reveal threshold comparable to the 2D surface code at about 10 fold improvement in encoding rate
- Organization of the paper
  1. Introduction
  2. Arbitrary graph state from passive transformations of GKP states item Incorporating GKP states on arbitrary lattices
  3. Fault-tolerance analysis
  4. Major references

- Supplemental material for the paper:
  1. Notations, conventions and Gaussian operations
  2. Gate identities via LDU-type decompositions
  3. Stitching and reduction : (a)measuring the splitter (b) obtaining the target GKP graph state (c) projective Gaussian measurements as rescaled homodyne measurements (d) GKP qubit measurements on the central modes
  4. Splitter designs : (a) star splitter (b) cascade splitter (c) tree splitter (d) 2^j splitter
  5. Accommodating arbitrary GKP lattices and anisotropic noise
  6. Leveraging quadrature bias and poof of noise decoupling
  7. Uniform isotropic noise propagation from square-lattice GKP states
  8. Error correction simulation details
  9. References

II.5.6. Qiskit in Practice: a step-by-step guide to programming with popular quantum framework [Quantum Zeitgeist, Oct 2024]

Simulating a bosonic error correction code using Bosonic Qiskit

- logical information is nonlocally "smeared" across many qubits such that it cannot be corrupted by local errors
- this leads to a vicious cycle of increase in number of noisy physical qb
- an alternative is to encode a logical qb into a single bosonic mode using its infinite dimensional Hilbert space to provide redundancy for error control
- quantum circuits that contain bosonic modes (also called as oscillators or qumodes) alongside qubits
- logical qubits are encoded into the infinite dimensional Hilbert space of quantum systems known as the quantum harmonic oscillator (QHO)
- like qubits QHO has discrete or quantized energy levels
- qubits have only two levels; oscillators have infinite levels (useful for error correction)
- another advantage is the simplicity of the dominant error channel, photon loss

- physical realizations of QHO : electromagnetic modes of a microwave cavity, vibrational modes of a chain of ions ...
- advantages demonstrated recently, experimentally in 3 types of codes, (a) cat code, (b) GKP code, (c) binomial code
- simplest example : binomial kitten code
- code words of Bosonic ECC are superpositions of Fock states which are quantum states defined by photon number n, labeled by $|n\rangle$. In the kitten code the two logical code words are:
  $|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |4\rangle)$ $\qquad\qquad$ $|1\rangle = |2\rangle$
- NOTE: the photon loss rate will be same in both code words (this means it is impossible to infer logical information from photon loss detection
- NOTE: since both code words have even photon parity, single photon loss errors will map logical states onto odd parity Fock states: ($|1_L\rangle \rightarrow |1\rangle$, $\qquad$ $|0_L\rangle \rightarrow |3\rangle$ enabling detection of single photon loss errors by only measuring the photon number parity, without learning the photon number.

- kitten code implementation has 3 components : (a) photon loss error channel (b) measurement of the photon number parity, (c) detection and error recovery
- Refer to Qiskit : Jupyter Notebook for details (link provided in the document)

II.5.7. FPGA-based distributed union-find decoder for surface codes, IEEE Trans. Quant. Engg., Lianage, Wu, Tagare, Zhong, Oct 2024, 17pp.

- minimum weight perfect matching (MWPM) algorithm based decoders and speed-up steps
- this paper : distributed union-find decoder
- distance d rotated surface code is a topological code made of $2d^2 - 1$ physical qubits arranged as shown (Fig. 1)
- advantage of surface code : larger d can exponentially reduce the rate of logical errors

II.5.8. Spatially coupled QLDPC codes, Yang, Calderbank, 21 Feb 2025, 36pp, 66refs.

- a class of convolutional codes; important classical code due to high performance, compatibility with low latency decoders
- we describe toric codes as quantum counterparts of classical 2 D spatially coupled (2D-SC) codes and introduce spatially coupled quantum LDPC (SC-QLDPC) codes as generalization.
- we use convolutional structure to represent the parity check matrix of 2D-SC code as a polynomial in 2 indeterminates, and derive a n.a.s.c algebraic condition for a 2D-SC code to be a stabilizer code.
- this algebraic framework facilitates construction of new families.
- we use the algebraic framework to optimize short cycles in the Tanner graph of 2D-SC hypergraph product (HGP) that arise from short cycles in either component code.
- prior work focuses on QLDPC codes with rate less than 1/10.
- we construct 2D-SC HGP codes with small memories, higher rates (about 1/3) and superior thresholds.

II.5.9. Gottesman-Kitaev-Preskill Codes: A Lattice Perspective, Conrad, Eisert, Arzani, Feb 2022, 30 pp, 53 refs.

- general GKP codes for continuous variable QEC including concatenated GKP codes through lens of lattice theory for a better understanding of the structure of this class of stabilizer codes.
- derive formal bounds on code parameters,
- show relationships between decoding strategies
- propose new constructions using glued lattices, tensor product of lattices
- illustrate through examples from different lasses of codes including scaled self-dual codes and the concatenated surface-GKP code
- Gottesman PhD thesis : Stabilizer codes and QEC, 1997.

II.5.10. Good Gottesman-Kitaev-Preskill Codes from the NTRU cryptosystem, Conrad, Eisert, Seifert, Jul 2024, 26 pp, 71 refs.

- new class of random GKP codes derived from the cryptanalysis of NTRU PKCS
- they are *good* : constant rate, average distance scaling $\Delta \propto \sqrt{n}$, where n is the number of bosonic modes
- leads to a qubit QEC with linear distance
- *decoding* for a stochastic displacement noise model is equivalent to *decrypting* the NTRU cryptosystem, such that every random instance of the code comes with an efficient decoder.
- this construction highlights how GKP code bridges the aspects of classical error correction, quantum error correction and post-quantum cryptography.
- hence we propose a simple public key communication protocol with security inherited from the NTRU PKCS.

II.5.11. Quantum error correction below the surface code threshold, Google Team, 300+ authors, arXiv Dec 2024, Nature, 27 Feb 2025, 8 pp, 53 refs.

- multiple physical qubits to a logical qubit requires exponential logical error rate suppression
- this is possible only if the physical error rate is below a critical threshold
- we present 2 below-threshold surface code memories on our newest gen SC-QPU Willow.
- distance 7, distance 5 code integrated with a real-time decoder
- logical error rate is suppressed by a factor $\Lambda = 2.14 \pm 0.02$ when increasing the code distance by 2, culminating in a 101 qubit distance-7 code with $0.143\% \pm 0.003\%$ error per cycle of error correction.
- average decoding latency is 63 microsecs at distance 5 up to million cycles with a cycle time of 1.1 microsecs
- we also run a repetition code up to distance 29 and find that logical performance is limited by a rare correlated error, approximately once an hour or 3×10^9 cycles.

- Hence, when scaled we can reach large-scale fault-tolerant quantum algos.

II.5.12. Sparse blossom: correcting a million errors per core second with minimum weight matching Higgott and Gidney,arXiv Jan 2025, 37 pp, 50+ refs.

- we introduce a fast implementation of the minimum weight perfect matching (MWPM) decoder.
- MWPM decoder is the most commonly use for many QEC (including surface codes)
- sparse blossom avoid all-to-all Dijkstra search
- for 0.1 % circuit=level depolarizing noise, sparse blossom processes syndrome data in both X and Z bases of distance-17 surface code circuits in less than 1 microsec per round of syndrome extraction on a single core matching the rate of generation of syndrome data by superconducting qubit quantum processor.
- open source - version 2 of PyMatching library

II.5.13. Concatenate codes, save qubits, Yoshida et al, arXiv Feb 2024, 27 pp, 62 refs.

- critical requirement of fault-tolerant quantum computing (FTQC) is a balance of space overhead, threshold, modularity.
- obstacle with surface code, concatenated Steane code is space overhead (ratio of physical to logical qubits)
- existing QLDPC codes reduce space overhead at the expense of other overheads
- We reduce overheads simultaneously using concatenated codes rather than QLDPC codes
- under physical error rate of 0.1.% , we reduce the space overhead to achieve logical CNOT error rate of $10^{-10}, 10^{-24}$ by more than 90 % and 97 % respectively, compared to the protocol for surface code.
- our protocol achieves the threshold of 2.4 % under the conventional circuit-level error model, outperforming the surface code.
- Also concatenated codes, naturally, introduce abstraction layers essential for the modularity of FTQC architectures.

II.5. Quantum Codes: Decoding

Improved belief-propagation is sufficient for real-time decoding of quantum memory, IBM Quantum, arXiv, Jun 2025, pp.8, refs. 50..

- new *Relay-BP* decoding - outperforms BP+OSD+CS-10 for bivariate bicycle codes, and comparable to min-weight-matching (MWPM) for surface codes
- lightweight, message-passing decoder, parallel, low footprint FPGA/ASIC
- decoding with a syndrome table lookup is infeasible for $n > 40$
- *minimum weight perfect matching* algorithm for identifying error chains between positive syndrome measurements, is quite efficient
- FPGA decoder integrated into the control system of a super-conducting QP

II.5. Quantum Codes: Decoding

Hardware-w=efficient quantum error correction via concatenated bosonic qubits, Nature, Feb 2025, 150 authors (AWS, multiple institutions). 9 pp, 65 refs.

- AWS new chip *Ocelot* using cat qubits - reduces errors exponentially
- 5 data qubits, 5 buffer circuits (superconducting tantalum) to stabilize the cat qubits; and 4 additional qubits to detect errors
- logical qubit memory formed from concatenation of encoded bosonic cat qubits with an outer repetition code of distance d=5.
- a stabilizing circuit passively protects cat qubits against bit flips
- the repetition code, using ancilla transmons for syndrome measurements, corrects cat qubit phase flips.
- improves threshold at which scaling of the erro-correcting code size leads to exponential improvements in the logical qubit error rates.
- qubits are realized by two levels of a physical element OR
- encoded in the infinite-dimensional Hilbert space of a bosonic mode (a quantum harmonic osicllator); using cat codes, binomial codes, GKP codes;

II.5.??. References : MUSTREAD related papers

1. Building fault-tolerant quantum computer using concatenated cat codes, Chamberland et al (18 authors), arXiv Dec 2020, 118 pp, 132 refs.
2. Closest lattice point decoding for multimode GKP codes, Lin,Chamberland ,Noh, PRX Quantum,Jan 2024, 36 pp, 94 refs.
3. LDPC-cat codes for low-overhead quantum computing in 2D, Ruiz, Guillaud, arXiv Feb 2024, 23 pp, 103 refs.
4. Almost-linear time decoding algorithm for topological codes, Delfosse, Nickerson, arXiv Nov 2021, 12 pp, 68 refs. (union-find, data structures)
5. Certified randomness from quantum supremacy, Aaronson, Hung, Mar 2023
6. Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes, Gheorghiu, Mosca, arXiv Feb 2019, 19pp, 25 refs.
7. Blockchain with proof-of-quantum work, Amin et al, D-Wave, arXiv 18 Mar 2025, 23 pp, 50 refs, 18 Mar 2025,

8. Decision-tree decoders for general QLDPC codes, arXiv 23 Feb 2025, 40 pp, 60 refs.
9. Demonstrating dynamic surface codes, Google Quantum AI (300+authors) arXiv 18 Dec 2024, 48 pp, 12 refs.
10. Resource estimation of Grover-kind quantum cryptanalysis against FSR based ciphers, Anand, Maitra et al, arXiv 2019, 33 pp, 30 refs.
11. High-threshold low-overhead fault-tolerant quantum memory, Bravyi et al, IBM, arXiv Aug 2023, 38 pp, 64 refs.
12. Very low overhead fault-tolerant quantum error correction with the surface-GKP code, Noh, Chamberland, Brando, AWS, IQIM, arXiv 2023, 38 pp, 85 refs.
13. Bosonic coding - introduction and use cases, V.V.Albert, arXiv, Nov. 2022, 31 pp, 129 refs.
14. Weight-reduced stabilizer codes with low overhead, Sabo et al, PRX Quantum, Oct 2024, 43 pp, 105 refs.
15. New quantum codes from self-dual codes over F_4, Dastbasteb, Lisonek, arXiv Nov 2022, 16 pp, 22 refs.

16. algebraic quantum codes linking quantum mechanics and discrete mathematics, Grassl, arXiv Nov 2020, 19 pp, 24 refs.
17. Computing efficiently in QLDPC codes, Malcolm et al (13 authors), Photonic Inc, U.Edinburgh,R Feb 2025, 46 pp, 45 refs.
18. Magic states of top quarks, Phys. Rev., Dec 2024, 15 pp, 48 refs.
19. Efficient magic states not as costly as you think,Litinski, arXiv Nov 2019, Quantum, 22 pp, 42 refs.
20. Low-overhead qutrit magic state distillation. S.Prakash, T.Saha, arXiv Aug 2024, 12pp, 25 refs.
21. Universal quantum computation with ideal Clifford gates and noisy ancillae, Bravyi, Kitaev, arXiv Dec 2004, 15pp, 35 refs.
22. Stabilizer codes and QEC, Thesis, Gottesman, 1997, 122 pp, 65 refs.
23. Constructing quantum codes from any classical code and their embedding in ground space of local Hamiltonian, Nov 2024, 21 pp, 34 refs.
24. quantum stabilizer codes, Lattices and (CFTs)Conformal Field Theories, arXiv, JHEP 2020,99pp, 99refs.

25. Concatenate codes, save qubits, Yoshida et al, arXiv Feb 2024, 27 pp, 62 refs.
26. Large-scale simulation of Shor's quantum factoring algorithm, Willsch (+4), arXiv Oct 2023, 32 pp,115 refs.
27. Optimization and performance analysis of Shor's algorithm in Qiskit, Sun (+2), arXiv Oct 2023, 7 pp, 20 refs.
28. A software simulator for noisy quantum circuits, Chaudhary (+5) IISc, arXiv Dec 2024, 10 pp, 20 refs.
29. Construction of binary linear code from boolean functions, C.Ding, Discr.math., 2016, 16 pp, 20 refs.
30. Fault-tolerant hyperbolic Floquet QECC., Fahimniya (+6), arXiv Jun 2024, 23 pp, 53 refs.
31. Forrelation: A problem that optimally separates quantum from classical computing, Aaronson and Ambainis, arXiv Nov 2014, 60 pp.
32. Tensor networks for quantum computing, 27 auth, arXiv Mar 2025, 17 pp, 211 refs.
33. A first successful factorization of RSA 2048 integer by D-wave quantum computer,Wang (+4), Tsinghua Sc. and Tech, V30, June 2025, 13 pp, 28 refs. (*** ONLY A SPECIAL CASE ***)

34. Quantum computation,D.Ahoronov, arXiv Dec 1998 (2024),78 pp, 220 refs.
35. Adiabatic quantum computation is equivalent to standard quantum computation, D.Ahoronov, ... O.Regev, arXiv Mar 2005, 30 pp, 36 refs.
36. Logical operators and fold-transversal gates of bivariate, bicycle codes, Eberhardt, 21pp.
37. Bivariate, bicycle QLDPC codes in gross codes of IBM (April 2025)
38. Quantum LDPC codes, Breuckman, Eberhardt, Oct 2021, 19 pp, 147 refs. (deep, homology, topology, complexity)
39. Architectures for heterogeneous QECC, Stein (+8), Nov 2024, 13 pp, 29 refs. (MUST READ - resource tradeoffs)
40. Post-quantum RSA, Bernstein, Heninger (+8), Apr 2017, 20 pp, 57 refs. (MUST READ - new, large (1 TB) RSA modulii)
41. Error Correction Zoo: List of codes in the quantum domain, 47 pp, 547 codes (list 17 pp) 700 refs (30 pp).
42. Quantum circuits for ECC: a tutorial,Mondal, Parhi, Sep 2023, 15 pp, 38 refs.

43. Automatic implementation, evaluation of QECC, Grurl et al, Jan 2023,6pp.
44. Qiskit QEC Software Framework, IBM 2022, updated Jan 2025, 68 pp.
45. Quantum circuit simulation at scale with NVIDIA cuQuantum Appliance, NVIDIA Sep 2022, updated Mar 2025.
46. Less quantum, more advantage: An end-to-end quantum algorithm for the Jones polynomial, Lakkonen (+8), arXiv Mar2025, 34 pp, 77 refs.
47. Artificial Intelligence for QEC: a comprehensive review, Wang, Tang, Dec 2024, 20pp, 150 refs.
48. Quantum algorithms zoo (a curated collection of brief descriptions of quantum algorithms) 50 pp, 34 pp of 513 refs.
49. How to factor RSA 2048 in million qubits, Gidney, 40 pp, May 2025.
50. Yoked surface codes, Gidney, Nature, 12pp, May 2025.

Lecture IV.1
Quantum Computing, Coding, Cryptography, Cryptanalysis : Projects Categories

- 3 Years : reports, seminars, conferences, journals, software
- 5 Levels: 1.Post-doc, 2.PhD, 3.MTech, 4.BTech, 5.Interns
- 5 Branches:
  1. Mathematics (algebra, linear algebra, number theory, combinatorics, probability, information theory)
  2. Computer Science (algorithms, data structures, complexity, o/s, programming)
  3. s/w Implementation (C, C++, Java, Python, MPI, CUDA, Qiskit,Cirq, QSim)
  4. h/w implementation (FPGA, VLSI,
  5. Physics (quantum mechanics), Electrical Engineering (circuits)
- 3 Topics:
  1. IF (integer factoring),DL (discrete logarithm),AC (algebraic cryptanalysis) (classical, quantum)
  2. ECC-classical,quantum

3. Qsimulation, HPC clusters: CPU-GPU-FPGA; Hybrid clusters: QPU-CPU-GPU-FPGA

List of Projects

1. Assessment of NFS, QFT algorithms for IFP.
2. Assessment of IC, QFT algorithms for DLP over finite fields.
3. Assessment of IC, QFT algorithms for DLP over elliptic curves.
4. Development of QECC from classical linear codes RM, RS, based on CSS
5. Comparison of CSS, GKP codes and variants. construction.
6. Development and evaluation of of QECC using CSS code concatenation.
7. Development and evaluation of QECC using stabilizer formulation.
8. Comparison of recent code constructions - resource requirements, rates, decoding failure rates (DFR) - suitable for items 1,2,3.
9. Adaptation of list decoding techniques for augmenting QECC performance.
10. Construction of classical ECC and QECC from classes of Boolean functions.
11. Construction of classical ECC and QECC from classes of Boolean lattices, braid groups and sphere packings.

12. Quantum algorithms for SAT and their applications in large-scale symmetric key cryptanalysis.
13. Development of hybrid quantum algorithms using hidden subgroup structures (Shor-type) together with lattice search (Grover-type) for asymmetric and symmetric key systems.
14. Use of Information Set (IS) decoding in QECC.
15. Use of Minimum weight perfect matching MWPM) in weighted graphs based decoding in QECC.
16. Comparison of sieving and combinatorial enumeration heuristics for SVP, CVP, SIS in lattices.
17. Adaptation of the above for classical and quantum ECC.
18. Resource and Performance Analysis of quantum linear algebraic algorithm, of Hasimi, Harrow, Lloyd (HHL) for algebraic cryptanalysis of stream, block ciphers.
19. Comparison of superconducting loops, ion traps, photonic polarizations, neutral atom, nitrogen vacancies based circuit / analog quantum devices for salient applications.

20. Comparative study of algorithms for decoding, cryptanalysis and their HPC and Quantum implementations.
21. Translation of algorithmic specifications to quantum circuits, optimization, resource, performance estimation of width, depth, coherence times,and error rates.
22. Simulation, measurements, and scaling estimation of quantum circuits width, depth, coherence times,and error rates.
23. Optimization, approximations, and error control for tweaking Shor's algorithm.
24. Refinements and trade-offs on Shor's algorithm.
25. Software simulator for noisy quantum circuits.
26. Building quantum circuits - Qiskit implementation.
27. Fault-tolerant ECC using hyperbolic surface codes.
28. Quantum supremacy, advantage, utility, complexity, separation.
29. Quantum supremacy, advantage, utility: metrics and benchmarking.
30. Tensor networks for quantum computing.
31. Factorization of specific integers by quantum annealing, QAOA, QUBO.

32. Equivalence of adiabatic, annealing QC computation and gated circuit QC.

Classification of Projects

Project Sl.No.	Levels	Branches	Topics
1	1,2	1,2	1
2	1,2	1,2	1
3	1,2	1,2	1
4	1,2	1,2	2
5	1,2	1,2	2
6	1,2	1,2	2
7	1,2	1,2	2
8	1,2	1,2	2
9	1,2	1,2	2
10	1,2	1,2	2
11	1,2	1,2	2
12	1,2,3	1,2,3	1
13	1,2,3	1,2,3	1
14	1,2,3	1,2,3	2
15	1,2,3	1,2,3	2
16	1,2,3	1,2,3	1

Project Sl.No.	Levels	Branches	Topics
17	1,2,3	1,2,3	1
18	1,2	1,2	1,2,3
19	1,2	1,2	3
20	1,2,3	1,2,3	1,2,3
21	2,3,4,5	2,3,4	2,3
22	2,3,4,5	3,4,5	2,3
23	1,2,3,4,5	1,3,4,5	1,3
24	1,2,3,4,5	1,3,4,5	1,2,3
25	3,4,5	3,4,5	1,2,3
26	3,4,5	3,4,5	1,2,3
27	1,2	1,2	2
28	1,2	1,2	1,2
29	1,2,3	3,4,5	3
30	1,2,3	1,2,3	1,2
31	1,2,3	1,2,3	1
32	1,2,3,4,5	1,2,3,4,5	1,2,3

Crypto-verses

If computers that you build are quantum,
Then spies everywhere will all want 'em.
Our codes will all fail,
And they will read our email,
Till we get crypto that's quantum, and daunt 'em.

Jennifer and Peter Shor 1994

To read our email, how mean
of the spies and their quantum machine;
be comforted though,
they do not yet know
how to factorize twelve or fifteen.

V.Strassen 1995

Can Committees Cultivate Code Crackers?

The answer is an imponderable **qubit** *at large.*
Sums of powers of moderate members do converge,
although not *all views align in the same area,*
unlike the conjectured conduct code of zeros of zeta.
A standing committee is a sitting duck on an average.

cevm 2016

Power of Quantum

It isn't easy to make practical crypto crackers.
by all the King's mathematical, statistical hackers,
and all the Queen's computational, physicist nerds
until they get together to build SCQ machines in herds,
keeping entanglements, sieves, superpositions, free of errors.

cevm 2022

Crypto-verses

Quo Vadis Quantum Computing?

From qubits to superpositions and entanglements,
via trapped ions to cold atoms and photon alignments-
Key labs of the world race in the quirky quantum forest,
to search faster, predict better and optimize best.
Will crypto cracking be worthy of quantum denouements?

cevm Apr 2024

Quo Vadis Quantum Factoring?

I factored RSA640, in 2008, with NFS and cluster compute of 120 Gflop-years;
my, unfulfilled, wish was RSA1024 crack by 2024 with MNFS in 4 Pflop-years.
While super-conducting loops, quirky spins, trapped ions, photon alignments,
are all in a global race to lead to useful quantum computing grand denouements,
I predict, an RSA2048 crack before 2048 is full of quantum noisy nightmares!

cevm 12 Dec 2024 : 12+12+2024=2048

Crypto-verses

Quo Vadis Q–nt-m E–or Co–e–ion?

Logical to physical qubits ratios, and circuit modularity,
are entangled obstacles to quantum advantage and utility.
Classical to quantum error detection, correction jumps,
are doubly challenging due to magnitude and phase flips.
Yet, squeezing cats, concatenation, may be good checks on
error parity.

cevm 14 Apr 2025 : World Quantum Day