The McEliece Cryptosystem Resists Quantum Fourier Sampling Attack

Cristopher Moore
University of New Mexico
and the Santa Fe Institute

Joint work with
Hang Dinh, University of Connecticut / Indiana, South Bend
Alex Russell, University of Connecticut

Post-quantum cryptography

- Shor's algorithms for Factoring and Discrete Logarithm break RSA public-key cryptography, Diffie-Hellman, ElGamal, elliptic curve cryptography…
- Are there there cryptosystems we can carry out with classical computers, which will remain secure even if and when quantum computers are built?
- Candidates:
  - lattice-based cryptosystems, and the "Learning With Errors" problem
  - key exchange based on elliptic curve isogenies (see Childs, Jao, Soukharev)
  - the McEliece cryptosystem and its relatives
- We show that some McEliece / Neiderreiter cryptosystems are immune to the natural analog of Shor's algorithm.

Error-correcting codes

- A generator matrix M, giving k linearly independent n-dimensional vectors. E.g. the Hadamard code, with k=3 and n=8:

$$M = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

- We encode a k-bit message as an n-bit codeword, a linear combination of the rows of M:

$$(0,1,1) \cdot M = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

- Minimum distance between codewords is d=4. We can correct $(d$-1$)/2$ errors.

- Finding the closest codeword is NP-hard in general. But there are families of codes where this can be done in polynomial time.

The McEliece cryptosystem

- Alice has the generator matrix *M* of an error-correcting code for which she can correct errors efficiently, e.g. a Goppa code

- She chooses an invertible $k \times k$ matrix *S* and a permutation *P* privately, and publishes a scrambled version of this code:

$$M' = SMP$$

expresses the lattice of codewords in a different basis

permutes the *n* bits of the codeword

- Bob encodes a message according to *M'* and adds some noise

- Alice applies P^{-1}, decodes according to *M,* and applies S^{-1} to the message

- Niederreiter cryptosystem: use *M* and *M'* as dual matrices instead

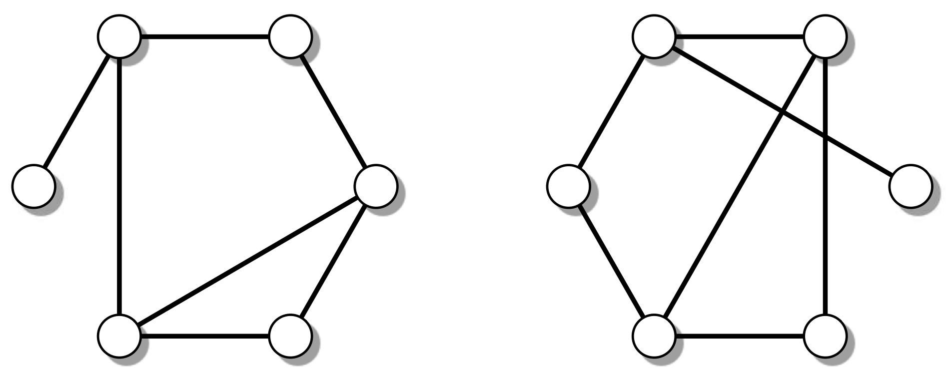
Is this secure?

- Assume that correcting errors in *M'* is just as hard as for linear codes in general
- An attacker can break Alice's cryptosystem once and for all by recovering the private key from the public key
- Assume Alice's original code *M* is publicly known
- Private key (*S*,*P*), public key *M'*
- Given two matrices *M, M',* find a matrix *S* and a permutation *P* such that

$$M' = SMP$$

Hidden symmetries

- We have seen this kind of problem before. Given two graphs G_1, G_2,



  find a permutation π such that $G_2 = \pi(G_1)$.

- A "hidden shift" problem: if $f_1(\mu) = \mu(G_1)$ and $f_2(\mu) = \mu(G_2)$, then $f_2(\mu) = f_1(\mu\,\pi)$

- Suppose we know Aut(G_1), the set of permutations μ such that $\sigma(G_1) = G_1$. Then if we could find π, we would know

$$\mathrm{Aut}(G_2) = \pi\,\mathrm{Aut}(G_1)\,\pi^{-1}$$

- Thus Aut(G_2) is a conjugate of Aut(G_1). Can we tell which one?

Groups and automorphisms for McEliece

- The group $G = \mathrm{GL}_k \times S_n = \{S, P\}$ acts on codes: $(S,P)M=SMP$.
- Alice's code M has an automorphism group $\mathrm{Aut}(M) = \{(S,P) \mid SMP = M\}$.
  To be generous, let's assume it is known.
- Then $\mathrm{Aut}(M') = (S,P)\mathrm{Aut}(M)(S^{-1}, P^{-1})$ is a conjugate of $\mathrm{Aut}(M)$.
- Can we tell which one it is, by querying the function $f(S,P) = SM'P$?
- The level sets of f are the cosets of $\mathrm{Aut}(M')$. That is,

$$f(S_1, P_1) = f(S_2, P_2) \Leftrightarrow (S_1^{-1}S_2, P_1^{-1}P_2) \in \mathrm{Aut}(M')$$

or equivalently, if $f(S_1, P_1), f(S_2, P_2) \in (S', P')\mathrm{Aut}(M')$ for some (S',P')

Hidden conjugates and coset states

- General framework: we have a fixed subgroup $H \subset G$, and a function f hides a conjugate subgroup $H^g = gHg^{-1}$ for some g.

- Here $H = \mathrm{Aut}(M)$, $H^g = \mathrm{Aut}(M')$, $G = \mathrm{GL}_k \times S_n$, and $g = (S, P)$.

- Goal: determine g by querying f.

- Start by creating a uniform superposition over G, $\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle$

- Measuring $f(x)$ collapses the state to a uniform superposition over a random coset of the hidden subgroup H^g,

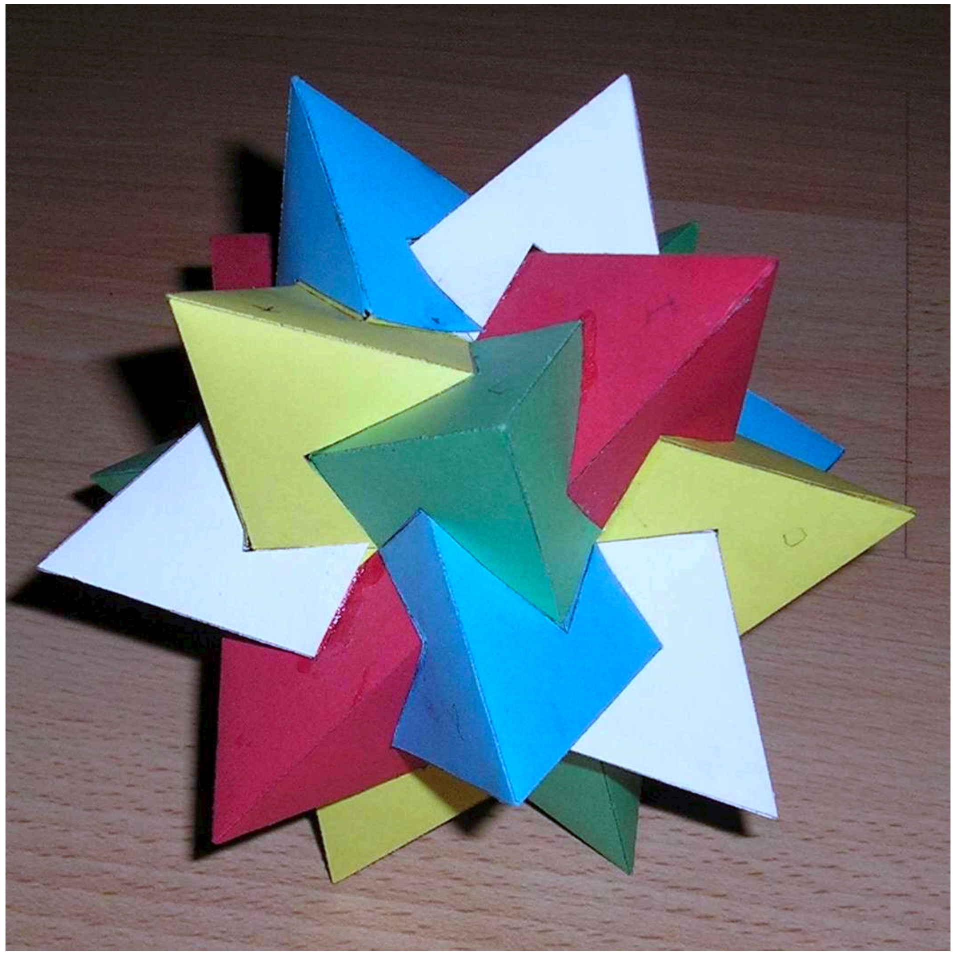
$$|cH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in G} |ch\rangle$$

Fourier sampling

- Decompose the Hilbert space over G into *irreducible representations*: these are homomorphisms $\rho : G \to \mathsf{U}(d)$

$$\rho(xy) = \rho(x)\rho(y) \quad \text{and} \quad \rho(x^{-1}) = \rho(x)^\dagger$$

- e.g. 3-dimensional representation of A_5, even permutations of five objects:

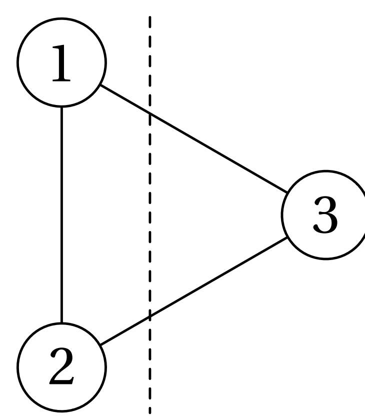


Basis vectors

- In standard Fourier analysis, we change basis to vectors $|k\rangle$ corresponding to a given frequency
- For nonabelian groups, each basis vector $|\rho, i, j\rangle$ corresponds to a matrix element of some irreducible representation
- There are just enough of these, since for any finite group G,

$$\sum_{\rho \in \widehat{G}} d_\rho^2 = |G|$$

- For instance, if $G = S_3$ we have the trivial representation (1), parity (±1), and one two-dimensional irrep:



$$\rho(1) = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$$

$$\rho(1 \longleftrightarrow 2) = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$$

$$\rho(1 \to 2 \to 3 \to 1) = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}$$

Measuring coset states doesn't work

- "Weak sampling": we measure the representation ρ. This probability distribution is the same for all conjugates.
- "Strong sampling": we measure the column *j*, in a basis of our choice. This distribution depends on the conjugate. (The distribution on rows is uniform.)
- Any measurement on a coset state can be described this way—the coset state is block diagonal, so measuring ρ doesn't destroy any coherence.
- But we will show that for almost all conjugates, these measurements yield exponentially little information. In fact...
- The distribution is exponentially close to that for the completely mixed state, where $H=\{1\}$.

A projection operator and a distribution on irreps

- In each irrep ρ and any subgroup *H*, we can define an operator

$$\Pi_H = \mathop{\mathbb{E}}_{h \in H} \rho(h)$$

- This is a projection operator of rank

$$\mathrm{rk}\ \Pi_H = \mathop{\mathbb{E}}_{h \in H} \chi_\rho(h)$$

- The probability we observe ρ under weak sampling is

normalized character

$$\frac{d_\rho |H|}{|G|} \mathrm{rk} \Pi_H = \frac{d_\rho^2}{|G|} \left(1 + \sum_{h \neq 1} \frac{\chi_\rho(h)}{d_\rho} \right)$$

- If normalized characters are small for $h \neq 1$, close to $d_\rho^2 / |G|$, the *Plancherel distribution*, same as for the completely mixed state

How much does strong sampling tell us?

- Suppose we observe an irrep ρ. Then in a given basis $B=\{b\}$,

$$P_g(b) = \frac{\langle b|\Pi_{H^g}|b\rangle}{\mathrm{rk}\ \Pi_H}$$

- Averaged over conjugates H^g, this is uniform, since

$$\mathop{\mathbb{E}}_g \Pi_{H^g} = \mathop{\mathbb{E}}_h \mathop{\mathbb{E}}_g \rho(h^g) = \mathop{\mathbb{E}}_h \frac{\chi_\rho(h)}{d_\rho} \mathbb{1} = \frac{\mathrm{rk}\,\Pi_H}{d_\rho} \mathbb{1}$$

- In expectation over g, how far is P_g from uniform? Total variation distance:

$$\left(\mathop{\mathbb{E}}_g \sum_{b\in B} \left| P_g(b) - \frac{1}{d_\rho} \right| \right)^2 \leq d_\rho^2 \mathop{\mathbb{E}}_b \mathop{\mathbb{E}}_g \left(P_g(b) - \frac{1}{d_\rho} \right)^2$$

$$= d_\rho^2 \mathop{\mathbb{E}}_b \mathop{\mathrm{Var}}_g P_g(b) = \left(\frac{d_\rho}{\mathrm{rk}\,\Pi_H} \right)^2 \mathop{\mathbb{E}}_b \mathop{\mathrm{Var}}_g \langle b|\Pi_{H^g}|b\rangle$$

Bounding the variance

- We have
$$\operatorname*{Var}_g \langle b|\Pi_{H^g}|b\rangle \le \operatorname*{Var}_g \mathop{\mathbb{E}}_{h\neq 1} \langle b|\rho(h^g)|b\rangle$$
$$\le \mathop{\mathbb{E}}_g \left(\mathop{\mathbb{E}}_{h\neq 1} \langle b|\rho(h^g)|b\rangle \right)^2$$
$$\le \mathop{\mathbb{E}}_g \mathop{\mathbb{E}}_{h\neq 1} \left| \langle b|\rho(h^g)|b\rangle \right|^2$$
$$\le \mathop{\mathbb{E}}_{h\neq 1} \langle b\otimes b^*| \mathop{\mathbb{E}}_g (\rho\otimes\rho^*)(h^g)|b\otimes b^*\rangle$$
- Decompose $\rho\otimes\rho^*$ into irreducibles:
$$\mathop{\mathbb{E}}_g (\rho\otimes\rho^*)(h^g) = \mathop{\mathbb{E}}_g \bigoplus_{\tau\prec\rho\otimes\rho^*} \tau(h^g) = \bigoplus_{\tau\prec\rho\otimes\rho^*} \frac{\chi_\tau(h)}{d_\tau}\mathbb{1}$$
- Then
$$\operatorname*{Var}_g \langle b|\Pi_{H^g}|b\rangle \le \sum_{\tau\prec\rho\otimes\rho^*} \left(\mathop{\mathbb{E}}_{h\neq 1} \frac{\chi_\tau(h)}{d_\tau} \right) \left| \Pi_\tau (b\otimes b^*) \right|^2$$

Large and small representations

- We have

$$\mathop{\mathbb{E}}_{b} \mathop{\mathrm{Var}}_{g} \langle b | \Pi_{H^g} | b \rangle \le \sum_{\tau \prec \rho \otimes \rho^*} \left(\mathop{\mathbb{E}}_{h \ne 1} \frac{\chi_\tau(h)}{d_\tau} \right) \mathop{\mathbb{E}}_{b} \left| \Pi_\tau(b \otimes b^*) \right|^2$$

$$\le \sum_{\tau \prec \rho \otimes \rho^*} \left(\mathop{\mathbb{E}}_{h \ne 1} \frac{\chi_\tau(h)}{d_\tau} \right) \frac{d_\tau^2}{d_\rho}$$

exponentially small if τ is large (we hope)

exponentially small if τ is small

- So, is this true when $H=\mathrm{Aut}(M)$, and when $G=\mathrm{GL}_k \times S_n$?

Code automorphisms

- Recall that $\mathrm{Aut}(M) = \{(S, P) \mid SMP = M\} \subseteq \mathrm{GL}_k \times S_n$
- Exercise: what are the automorphisms of the Hadamard code,

$$M = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \quad ?$$

- If M has full rank, then for each $P \in S_n$ there is at most one S such that $SMP=M$
- We can focus on the subgroup $K \subseteq S_n$ of permutations for which such an S exists

Product representations

- The irreps of a direct product $G_1 \times G_2$ are tensor products $\mu \otimes \lambda$ where μ and λ are irreps of G_1 and G_2 respectively. Their normalized characters are

$$\left| \frac{\chi_{\mu\otimes\lambda}(a,b)}{d_{\mu\otimes\lambda}} \right| = \left| \frac{\chi_\mu(a)}{d_\mu} \right| \left| \frac{\chi_\lambda(b)}{d_\lambda} \right| \leq \left| \frac{\chi_\lambda(b)}{d_\lambda} \right|$$

- We can bound normalized characters of $(S,P) \in \mathrm{Aut}(M) \subseteq \mathrm{GL}_k \times S_n$ in terms of those of $P \in K \subseteq S_n$

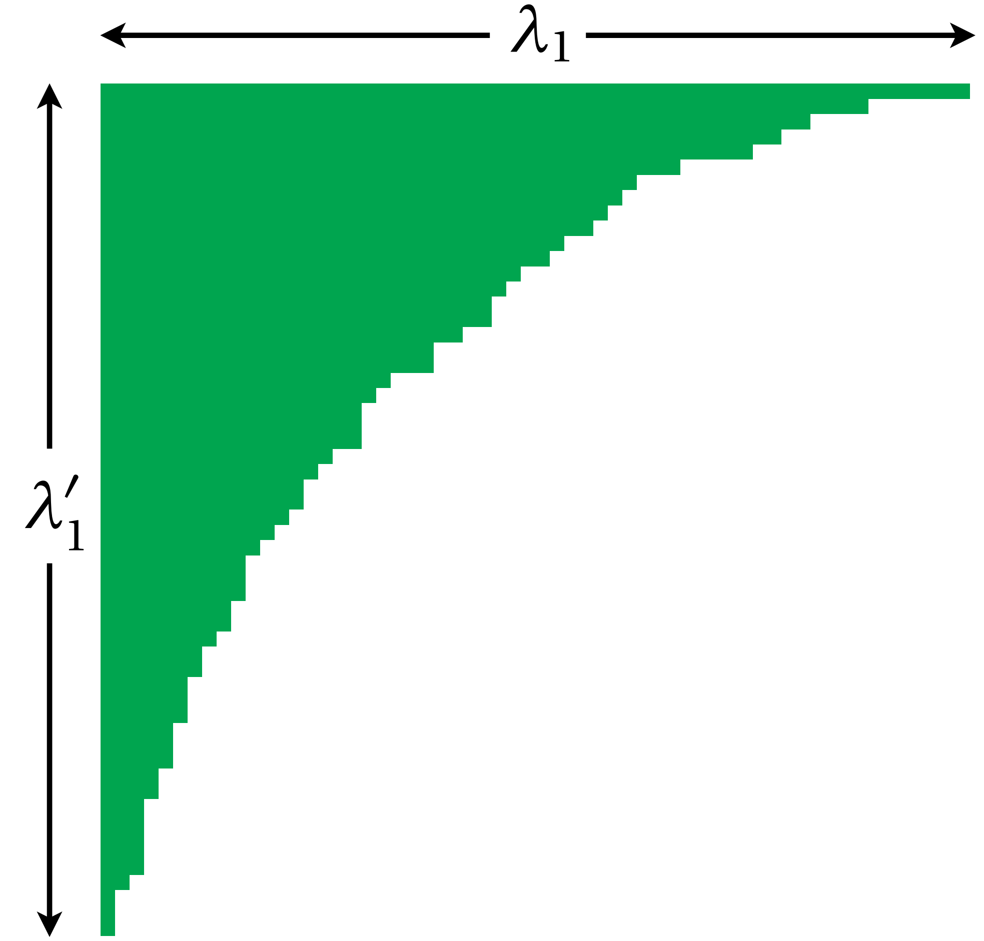
- Happily, the representation theory of S_n is very well understood, and we have good bounds on characters

Supports and normalized characters in S_n

- The *support* supp(P) of a permutation P is the number of elements moved
- Each irrep of is described by a *Young diagram*, a partition $n = \lambda_1 + \lambda_2 + \cdots$ with $\lambda_1 \geq \lambda_2 \geq \cdots$
- Roichman: there are constants $b > 0$, $q < 1$ s.t.

$$\left| \frac{\chi_\lambda(\pi)}{d_\lambda} \right| \leq \left(\max\left(q, \frac{\lambda_1}{n}, \frac{\lambda'_1}{n} \right) \right)^{b \cdot \mathrm{supp}(\pi)}$$

- If $\lambda_1, \lambda'_1 < (1-c)n$ and $\mathrm{supp}(\pi) = \Omega(n)$, normalized characters are exponential small



- Conversely, if λ_1 or $\lambda_2 \geq (1-c)n$, the dimension d_λ is vanishingly small compared to d_ρ chosen from the Plancherel distribution.

Automorphisms of Goppa codes

- The generator matrix of a Goppa code over $\mathbb{F}_q$ is of the form

$$M = \begin{pmatrix} g(z_1)/h(z_1) & \dots & g(z_n)/h(z_n) \\ z_1 g(z_1)/h(z_1) & \dots & z_n g(z_n)/h(z_n) \\ \vdots & \ddots & \vdots \\ z_1^r g(z_1)/h(z_1) & \dots & z_n^r g(z_n)/h(z_n) \end{pmatrix}$$

  where $g(z)/h(z)$ is a rational function and $z_1,\dots,z_n$ are distinct

- One type of action on the columns is a Möbius transformation, $z \mapsto \dfrac{az+b}{cz+d}$

- The group of all such transformations is $\mathrm{PGL}_2(\mathbb{F}_q)$; it is three-transitive on the projective plane $\mathbb{F}_q \cup \{\infty\}$. Any one that fixes three distinct z_i is the identity.

- *Stichtenoth's Theorem* states that all automorphisms of M are of this form. Therefore, the support of any $P \neq 1$ is at least n–2.

Putting it all together

- Recall our bound on the variance:

$$\mathop{\mathbb{E}}_{b} \mathop{\mathrm{Var}}_{g} \langle b | \Pi_{H^g} | b \rangle \leq \sum_{\tau \prec \rho \otimes \rho^*} \left(\mathop{\mathbb{E}}_{h \neq 1} \frac{\chi_\tau(h)}{d_\tau} \right) \frac{d_\tau^2}{d_\rho}$$

exponentially small if τ's Young diagram is typical, since *P* has support at least *n*–2

exponentially small if τ's Young diagram is too wide or tall

- Summing over all τ, the expected variance—and therefore the expected information yielded by measuring the coset state—is exponentially small.

- By Markov's inequality, almost all conjugates are indistinguishable.

A cautionary note

- We have *not* shown that other quantum algorithms, or even classical ones, cannot break the McEliece cryptosystem.
- Nor have we shown that such an algorithm would violate a natural hardness assumption (such as lattice-based cryptosystems and Learning With Errors).
- In fact, classical attacks exist on some Goppa codes, such as generalized Reed-Solomon codes [Sidelnikov and Shestakov]
- However, we have shown that any algorithm that treats M as a "black box," and only probes its symmetries, requires new ideas.
- Our next goal: multiregister results à la Hallgren et al. for Graph Isomorphism, and sieve results à la Moore, Russell, and Sniady.

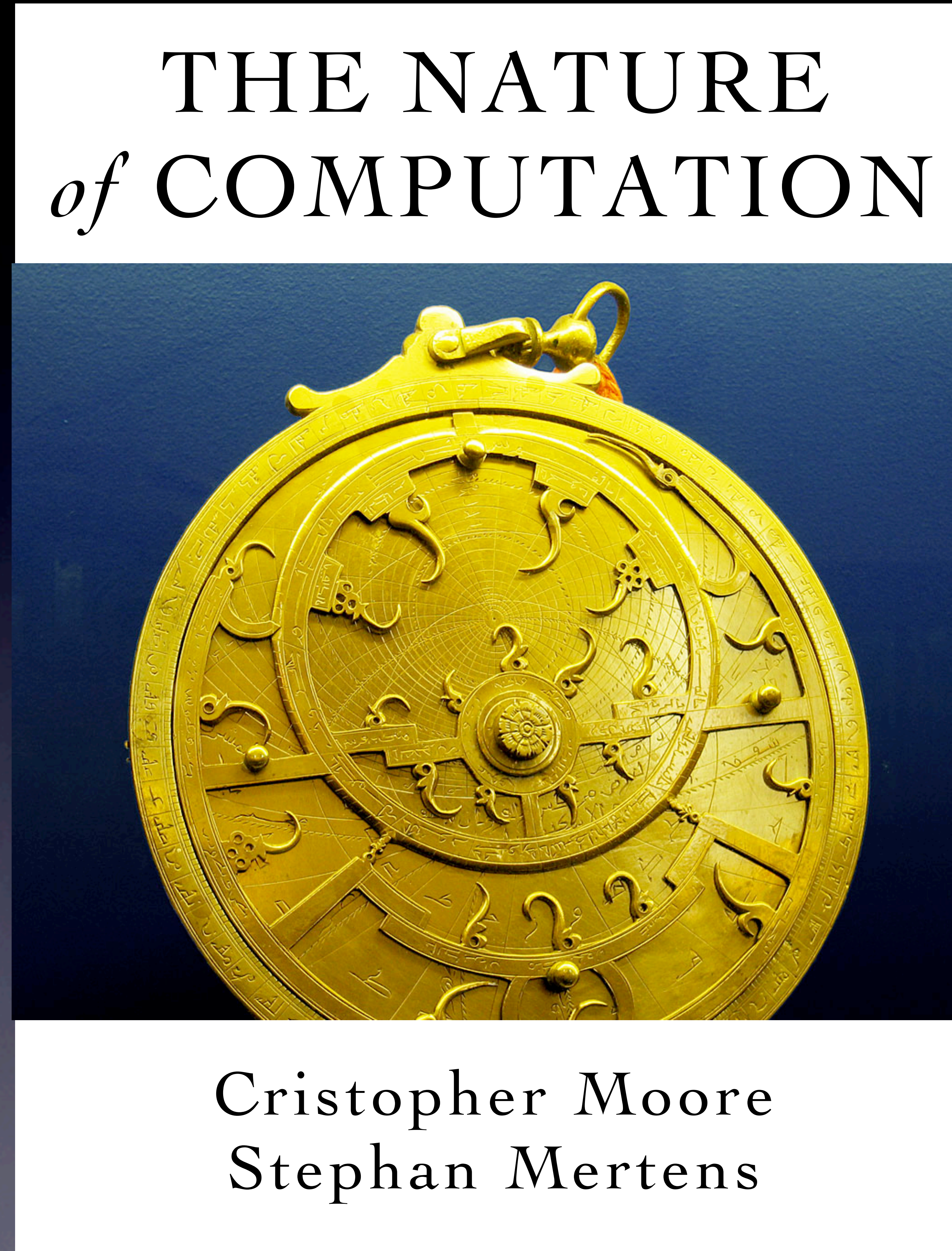
Shameless Plug

This book rocks! You somehow manage to combine the fun of a popular book with the intellectual heft of a textbook.
— Scott Aaronson

A treasure trove of information on algorithms and complexity, presented in the most delightful way.
— Vijay Vazirani

A creative, insightful, and accessible introduction to the theory of computing, written with a keen eye toward the frontiers of the field and a vivid enthusiasm for the subject matter.
— Jon Kleinberg

Oxford University Press, 2011



Acknowledgements