I seek to understand the nature of quantum computation and its implications for cryptography and fundamental physics. The idea that certain problems cannot be solved efficiently is the basis of modern cryptography, which leverages this hardness to construct secure protocols. This field is currently undergoing a revolution—arguably, *two* revolutions—due to the advent of quantum computers:

- The threat of quantum attacks demands entirely new paradigms for establishing security.
- On the other hand, **quantum cryptography** (cryptography that runs on quantum devices) has the potential to be more powerful and significantly more secure than classical cryptography.

My research establishes a foundation for cryptography in the quantum era and applies this theory to shed light on the **physical limits of efficient computation**. To give examples:

1. **Pseudorandom unitaries.** The ability to *efficiently* implement a seemingly random function (i.e., a pseudorandom function) is a cornerstone of modern cryptography, underlying the security of nearly every online interaction. Is an analogous statement true in the quantum world? Namely, **can we efficiently implement seemingly random (pseudorandom) unitaries?** This would have broad implications for quantum computing and physics [SHH24, KP23, EFL+24].

   In [**MH24**], we gave the **first proof that pseudorandom unitaries exist** under cryptographic assumptions, analyzing a construction of [MPSY24a]. Our proof introduces a new technique for studying random unitaries that has already found many applications (e.g., [ABGL24, BHHP24]).

2. **Quantum commitments.** Cryptographic protocols rely on commitments, the digital analogue of a locked box. In a commitment, a sender picks a classical bit, which the protocol then "locks in." This appears fundamentally incompatible with quantum information: if the sender wants to commit to a qubit, the protocol needs to "lock in" a state that it cannot fully know or measure.

   Despite this, in [**GJMZ23**], we showed that **commitments to quantum states** are not only possible, but provide a framework for bringing classical functionalities into the quantum world. For example, we showed how to securely "hash" an arbitrarily long *quantum* message. Beyond cryptography, I showed in [**Ma23**] that these commitments give a **precise characterization of computational problems from fundamental physics**. This theory of quantum commitments resulted from a line of work [**CMSZ21, LMS22, GJMZ23**] that broadly **established quantum security of foundational protocols** [FS89, Kil92, GMW91, GK96].

3. **Quantum cryptographic hardness.** If someone were to prove that all problems in NP can be solved efficiently (i.e., $\mathsf{P} = \mathsf{NP}$), all classical cryptography would be broken. But remarkably, [KQST23] showed that quantum cryptography (e.g., quantum commitments) could still be secure even if $\mathsf{P} = \mathsf{NP}$. Then, in [**LMW24**], we showed that this might go far beyond NP: we proved that even if **every function were easy** (including the halting problem) this *still* might not be enough to break quantum cryptography! This suggests that **breaking quantum cryptography might not be captured by existing complexity theory**. Our work also gave the first lower bound for the Unitary Synthesis Problem [AK07], one of central open problems in quantum complexity. This work was recently featured in Quanta Magazine [Bru24].

These results highlight deep connections between cryptography, computation, and the physical world. It is widely believed (i.e., the quantum extended Church-Turing thesis) that any physical process can be efficiently simulated on a quantum computer. Thus, the behavior of the universe itself is constrained by quantum computational hardness. What form does this hardness take? While traditional complexity theory focuses on worst-case, artificially constructed hard problems, these are unlikely to appear in the physical world. Instead, the problems relevant for understanding physical reality, such as "decoding" the radiation of black holes, are average-case problems—arising out of randomness and chaos. Cryptography has been unreasonably effective at studying precisely these kinds of problems, and I aim to leverage this to broaden our understanding of the physical world.

I will now describe my contributions in greater detail and propose directions for future research.

1 Pseudorandom unitaries

1.1 Background

Just as random functions play a fundamental role in classical computing, their quantum analogue—Haar-random unitaries—are fundamental to the study of quantum computing. However, both random functions and Haar-random unitaries are exponentially complex: for inputs of size n, they require $\exp(n)$ random bits to specify and $\exp(n)$ time to implement (on classical and quantum circuits, respectively), which precludes their use in any practical setting.

Classically, we solve this problem with *pseudorandom functions* (PRFs) [GGM86], which are *efficiently implementable* functions that are indistinguishable from truly random functions to any polynomial-time algorithm. In other words, PRFs make it possible to efficiently implement (seemingly) random functions. This is a powerful insight that has had far-reaching implications: for example, PRFs (such as AES) underlie the security of almost every online interaction, forming the backbone of our internet infrastructure.

This suggests the following question for the quantum setting:

Do pseudorandom ***unitaries*** *exist?*

This question has been informally considered in the physics literature for decades (e.g., [EWS+03, ELL05]), and formalized by Ji, Liu, and Song [JLS18], who defined pseudorandom unitaries (PRUs) to be *efficiently implementable* unitaries that are indistinguishable from Haar-random unitaries to any quantum polynomial-time algorithm. Since their work, PRUs have found applications spanning quantum cryptography, quantum algorithms, and even fundamental physics. However, despite significant efforts—including many candidate constructions [JLS18, LQS+24, MPSY24a, CBB+24] and impressive progress establishing weaker variants [HBK23, LQS+24, AGKL24, BM24, MPSY24a, MPSY24b, CBB+24]—**the question of whether PRUs actually exist has remained open**.

1.2 My work

With Hsin-Yuan Huang [**MH24**], I settled this question by **proving that PRUs exist** under standard cryptographic assumptions (i.e., the existence of one-way functions). Our proof analyzes a construction of [MPSY24a] by leveraging an elementary principle from quantum information called **purification**.

Purification is the idea that any **randomness** in the (mixed) state of a quantum system S can be seen as arising from a lack of information about a *larger* system SE that is in a **deterministic** (pure) state. The idea to apply purification to quantum pseudorandomness originated at a workshop at the Simons Institute, where I gave a talk on purification in the context of pseudorandom states (a weaker object than PRUs) [**Ma24**]. In my talk, I presented a simple analysis of pseudorandom states that involves applying purification and then "rotating" the purifying system E to reveal a new perspective on the original mixed state.

Incidentally, at the same workshop, Henry Yuen presented a candidate pseudorandom unitary construction [MPSY24a] along with a *partial* security analysis.[1] This led Hsin-Yuan Huang and I to wonder: could purification be the missing piece? Over the following months, we refined the technique, developing new insights into how purification works in the context of random unitaries, eventually culminating in a full proof of PRU security [**MH24**].

[1] Concretely, they showed their construction is a *non-adaptive* PRU, which means it cannot be distinguished from Haar-random by algorithms that only query the unitary on inputs that are **fixed in advance**.

Aside from obtaining PRUs, the [**MH24**] proof also develops **a new framework for analyzing Haar-random unitaries**. Using purification, we showed that any quantum algorithm A^U that makes oracle queries to a Haar-random unitary U (meaning the algorithm is given the ability to apply U as a subroutine) can be *efficiently simulated* by replacing the **random** U with a **deterministic** object that we call the **path-recording oracle**. The path-recording oracle makes it possible to analyze Haar-random unitaries with elementary techniques, and it is key to our PRU proof.

Our stand-alone result and the techniques we develop to prove it have several implications:

- **Applications of PRUs.** Our result enables efficiently instantiating applications of random unitaries in quantum computing and physics, many of which a priori have nothing to do with cryptography. For instance, [SHH24] used (low-depth) PRUs to show that several prominent computational tasks related to learning properties of physical systems are intractable. [GQY+24] used PRUs to prove that traditional signs of a phenomena known as quantum chaos need not be present for a physical system to appear chaotic. In quantum gravity, PRUs have been proposed as a way to model black hole information scrambling [KP23, EFL+24].

- **Applications of the path-recording technique.** Before our work, one of the main bottlenecks in research on Haar-random unitaries was the mathematical complexity of prior techniques, which often required complicated representation theory and combinatorics to bound moments of Haar-random unitaries. Our path-recording oracle circumvents this approach, giving a significantly simpler and oftentimes more powerful framework.

  For example, we showed in [**MH24**] that the path-recording oracle simplifies the proof of the main theorem of [SHH24] (which is used to generically compress the depth of any PRU). Beyond [**MH24**], the broader community has already started to employ our techniques to obtain new results on random unitaries (e.g., [BHHP24, ABGL24]).

  Aside from its utility as a proof technique, the path-recording oracle also makes it possible to efficiently **statistically** simulate any quantum algorithm that queries a Haar-random unitary. Unlike our PRU, this simulation makes no computational assumptions on the adversary and does not use cryptography. This achieves a version of "lazy sampling"—which refers to sampling the outputs of a random function as needed, on the fly—but for random *unitaries*.

The [**MH24**] result was the focus of a one-day workshop at the Simons Institute. I have also presented this work at the Simons Quantum Colloquium and the Institute for Advanced Study.

2 Cryptographic protocols in the quantum age

In this section, I will describe my work on **quantum rewinding** [**CMSZ21**, **LMS22**] and **commitments to quantum states** [GJMZ23].

2.1 Quantum rewinding

Background. *Rewinding* is the most common technique for proving the security of interactive cryptographic protocols. It is a thought experiment where the adversary's state is saved mid-execution in order to observe the adversary's responses across multiple interactions. However, in 1997, van de Graaf [Van97] made an unsettling observation: **classical rewinding proofs do not rule out quantum attacks**. This is because running a quantum adversary even once and measuring its response can irreversibly disturb its internal quantum state. Consequently, many of cryptography's most celebrated protocols had no justification for security against quantum attacks.

In later years, several prominent works [Wat09, Unr12, Unr16] showed how to rewind quantum adversaries in specific cases, establishing quantum security for a few notable protocols (such as a well-known zero-knowledge protocol for graph isomorphism [GMW91]). However, outside of these special cases, the general problem of quantum rewinding remained open. As a result, many fundamental protocols—such as Kilian's succinct arguments for NP [Kil92] and textbook zero-knowledge proof systems [GMW91, GK96, FS89] (including the zero-knowledge protocol for graph *non*-isomorphism)—were not known to have any security against quantum attacks.

My work. In **[CMSZ21, LMS22]**, my co-authors and I developed a **general method to rewind quantum adversaries**, enabling us to settle the quantum security of all of the protocols mentioned above [FS89, Kil92, GMW91, GK96].

In more detail, the goal of quantum rewinding is to make a stateful quantum algorithm, which succeeds at a given task with some probability (e.g., 1/2), succeed at this task *repeatedly*. As mentioned above, the main challenge lies in the fact that running a quantum algorithm just once and measuring its output causes irreversible disturbance, making it impossible to recover the algorithm's original quantum state. To overcome this, we observed that it is *unnecessary to recover the exact original state*; instead, it suffices to return the algorithm to a different quantum state as long as it is just as good for succeeding at the task. Leveraging this insight, we developed a new quantum procedure to "repair" the state in between each execution, making it possible to run a stateful quantum algorithm as many times as desired.

[CMSZ21] was selected for the SICOMP Special Issue for FOCS 2021, recognizing it as one of the top papers in the conference. It has since become part of the **standard quantum cryptography toolkit**. I have presented these techniques in numerous seminars, workshops, and courses, including the IPAM summer school on post-quantum and quantum cryptography at UCLA, my graduate quantum cryptography course at UC Berkeley, the Simons Quantum Colloquium, and in a one-day quantum rewinding workshop at the Simons Institute. These techniques have since found widespread applications throughout cryptography (e.g., [BBK22, BKL+22, Zha23, MNZ24, CAD+24]).

2.2 Commitments to quantum states

My work on quantum rewinding **[CMSZ21, LMS22]** paved the way for **commitments to quantum states [GJMZ23]**, which I will describe next.

Background. Commitment schemes are foundational to most interactive protocols in cryptography, such as the succinct arguments and zero-knowledge proofs mentioned above [FS89, Kil92, GMW91, GK96]. A commitment scheme acts as a digital locked box: it allows a sender to commit to a message m (placing m in the "locked box") without revealing it until later (opening the "locked box"). A crucial property of any commitment scheme is binding—once the sender commits to a message m, they cannot later open the commitment to a different message.

In the quantum world, it is natural to ask:

Can we commit to quantum information?

Unlike commitments to classical bits, where the protocol can explicitly depend on the chosen bit b, a protocol for committing to a quantum state $|\psi\rangle$ must somehow bind the sender to $|\psi\rangle$ without learning *anything* about it, as learning information about the state inherently requires disturbing it.

My work. In **[GJMZ23]**, we answered this question by giving precise definitions, constructions, and applications of **commitments to quantum states**. The connection between quantum rewinding and commitments was crucial: commitments are used to build interactive protocols, and rewinding arguments are used to reduce the security of the protocol to the security of the underlying commitments. Thus, our work on quantum rewinding **[CMSZ21, LMS22]** directly informed the way commitments

to quantum states are defined. Our definition provides a simple, yet unexpected characterization of commitments to quantum states, framing security in terms of a computational task involving an adversary's ability to efficiently detect entanglement.

As a key application, we showed, *assuming that pseudorandom unitaries (PRUs) exist*, how to commit to an arbitrarily long quantum state (i.e., many qubits) by sending a significantly shorter quantum "hash." This demonstrates that classical succinct hashing, a widely used cryptographic primitive, can be extended to quantum information—a statement that is far from obvious given the inherent differences between classical and quantum information. We also showed how to use these quantum commitments to build quantum zero-knowledge proof systems and quantum succinct arguments, achieving functionality and security guarantees beyond what is possible classically.

[**GJMZ23**] was invited to the SICOMP Special Issue for STOC 2023, recognizing it as one of the top papers in the conference.

Broader implications Quantum state commitments have surprising connections to other fields. In a talk I gave at the Simons Institute [**Ma23**] (building on [HH13, Aar16, Bra23]), I showed that the key computational task in the [AMPS13] firewall paradox from quantum gravity is syntactically *equivalent* to breaking a quantum state commitment.[2] Previous work [HH13, Aar16, Bra23] had shown that this task is *as hard as* problems in quantum cryptography; my talk demonstrated that it is, in fact, *identical* to breaking a commitment to a maximally entangled quantum state. This is just one example of a broader phenomenon (e.g., [BFV20, ABC+24]): the computational hardness that most commonly arises in physical systems is **cryptographic**.

3 Quantum cryptographic hardness

In this section, I describe how my work [**LMW24**] indicates that breaking quantum cryptography (e.g., the quantum commitments described in Section 2.2) may be harder than evaluating *any* function.

3.1 Background

If it turns out that $\mathsf{P} = \mathsf{NP}$, this would immediately break all classical cryptography. This is because breaking classical cryptography (e.g., one-way functions, classical commitments, etc.), amounts to solving problems in the complexity class NP. But surprisingly, [KQST23] showed that even if all problems in NP turn out to be easy, breaking quantum cryptography might *still* be hard! In fact, we do not know whether breaking quantum cryptography is captured by *any* natural complexity class.

What makes quantum cryptography behave so differently? Part of the answer is that breaking a quantum cryptographic primitive (e.g., quantum commitments) involves performing a computation directly on quantum state inputs. Quantum-input problems do not fit into traditional complexity classes like P, NP, or QMA, as these classes are only defined for problems with classical inputs. But the syntactic mismatch is only a partial explanation. For example, the task of inverting a one-way function (the basic primitive in classical cryptography) is a *search* problem, and syntactically does not match the definition of NP, which contains *decision* problems. However, for all practical purposes, inverting a one-way function is "in" NP, since it can be efficiently reduced to NP decision problems.

Thus, to understand how traditional complexity theory relates to quantum-input problems (henceforth, "quantum problems"), such as those that arise in quantum cryptography, the question is:

Can we efficiently reduce quantum problems to classical problems?

This question is also known as the **Unitary Synthesis Problem** [AK07], and it is arguably the central open problem in quantum complexity. Despite significant attention over nearly two decades,

[2] Video: youtube.com/watch?v=4jcj9WfVQiM. Slides: fermima.com/talks/black-holes.pdf.

this problem has remained wide open [Aar16, Aar21]. Unlike many other longstanding open questions, such as P vs. NP (where it is widely believed that $\mathsf{P} \neq \mathsf{NP}$), the Unitary Synthesis Problem is so poorly understood that *experts cannot even agree on whether the more likely answer is yes or no.*

3.2 My Work

In [**LMW24**], we proved the first one-query lower bound for the Unitary Synthesis Problem. Concretely, we showed that there exist quantum problems that are hard to solve, even given the ability to make a single query to an extraordinarily powerful oracle that **instantaneously evaluates any function** (including the halting problem). This gives the first indication that the answer to the Unitary Synthesis Problem is likely negative.

The key idea behind our result was to leverage the connection between unitary synthesis and quantum cryptography. Specifically, the quantum problem we proved to be hard, even with access to an all-powerful function oracle, corresponds to *breaking a randomly constructed quantum commitment.* Framing the question in terms of breaking commitments allowed us to formulate a natural Boolean optimization problem whose optimal value bounds the algorithm/adversary's advantage (i.e., its ability to break the commitment). We then proved our result by relating this optimization problem to a quantity that we could bound with techniques from random matrix theory.

Our result suggests that **quantum cryptography may be independent of *any* complexity-theoretic statement**. This underscores the need to develop new tools for understanding the complexity of quantum problems, i.e., implementing unitary transformations. This work was recently featured in a Quanta Magazine article and an accompanying podcast episode [Bru24].

4 Additional contributions

Beyond the works highlighted above, I have also made contributions to quantum multi-party computation [**BCKM21b**, **BCKM21a**], efficient verification of quantum computation [**BKL+22**], the Fiat-Shamir transform [**BBH+19**, **CLMQ21**], leakage resilience [**LMQW20**], and program obfuscation [**MZ18**, **BGMZ18**, **BLMZ19**, **BMZ19**, **BCJ+19**, **BIJ+20**].

5 Future directions

Quantum cryptography is not just about securing the future—it is a way to understand the nature of efficient computation and physical reality. This is evidenced by each of the research directions highlighted in this statement:

- quantum pseudorandomness can explain information scrambling in physical systems (Section 1).
- quantum commitments capture computational problems from fundamental physics (Section 2).
- quantum cryptographic hardness reveals inherent limits of existing complexity theory (Section 3).

In my view, these connections are no coincidence. The power of quantum cryptography stems from its ability to capture naturally occurring sources of hardness and harness it to constrain the behavior of all efficient quantum adversaries. This is a powerful framework for understanding the physical world: any observer bound by the laws of physics can be seen as such an "adversary," attempting to witness phenomena beyond what our efficient universe allows.

I believe we are just beginning to understand the potential of this perspective. Many fundamental questions about physics and the nature of efficient computation remain wide open, and **my research is guided by the conviction that cryptography will be instrumental in answering them**. Looking ahead, here are some concrete directions I plan to explore:

- **The complexity of unitary transformations.** One of the main goals of complexity theory is to prove that certain functions are hard to compute, e.g., that polynomial-size circuits cannot compute every function in NP (i.e., $\mathsf{P} \neq \mathsf{NP}$). In the quantum setting, we similarly want to prove that certain unitaries are hard to compute (such as those that would break quantum cryptography or perform computational tasks from physics). Unfortunately, in both settings, existing techniques have been woefully inadequate.

  A partial explanation for this is the "natural proofs" barrier of Razborov and Rudich [RR94], which uses pseudorandom functions (PRFs) to explain why complexity-theoretic lower bounds (such as $\mathsf{P} \neq \mathsf{NP}$) have been so elusive. But this only explains the difficulty of obtaining lower bounds for *functions*. As [**LMW24**] suggests, proving lower bounds on unitary complexity might not require proving *any* lower bounds on function complexity. Consequently, we have no known barriers to proving unconditional lower bounds for unitary complexity!

  I want to understand whether we can prove such lower bounds, and if not, why not. Towards this, I plan to study whether the existence of pseudorandom unitaries [**MH24**] represents a barrier for unitary complexity akin to the PRF-based natural proofs barrier [RR94].

- **How to use quantum pseudorandomness.** More broadly, what are the implications of quantum pseudorandomness? We have already found a number of applications of PRUs (in cryptographic contexts [**GJMZ23**] and beyond [SHH24, GQY+24, KP23, EFL+24]), but still many questions remain. Can PRUs shed light on other major questions in cryptography, e.g., how to obfuscate an arbitrary quantum circuit? Will PRUs have implications for modern quantum supremacy experiments (particularly those that rely on random circuit sampling)? What else can PRUs tell us about information scrambling in chaotic physical systems?

- **New sources of quantum hardness.** Cryptography provides an excellent framework for identifying concrete examples of extremely hard quantum problems. For instance, consider the following problem, which naturally arises from viewing random quantum circuits as cryptographic commitments: given a classical description of a random $\mathrm{poly}(n)$-size quantum circuit C on n qubits, along with the first $2n/3$ qubits of either $C|0^n\rangle$ or $C|1^n\rangle$, determine which state you received. Despite its simplicity, essentially nothing is known about this problem; as far as we know, it could be *harder than every classical problem*. What can studying problems such as this tell us about the nature of hardness?

Highlighted Works

(author ordering is alphabetical except in [MH24])

[CMSZ21] Alessandro Chiesa, Fermi Ma, Nicholas Spooner, and Mark Zhandry. "Post-Quantum Succinct Arguments: Breaking the Quantum Rewinding Barrier". In: *62nd IEEE Annual Symposium on Foundations of Computer Science (FOCS)*. 2021 (cit. on pp. 1, 3, 4).

[GJMZ23] Sam Gunn, Nathan Ju, Fermi Ma, and Mark Zhandry. "Commitments to Quantum States". In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC)*. 2023 (cit. on pp. 1, 3–5, 7).

[LMS22] Alex Lombardi, Fermi Ma, and Nicholas Spooner. "Post-Quantum Zero Knowledge, Revisited or: How to Do Quantum Rewinding Undetectably". In: *63rd IEEE Annual Symposium on Foundations of Computer Science (FOCS)*. 2022 (cit. on pp. 1, 3, 4).

[LMW24] Alex Lombardi, Fermi Ma, and John Wright. "A One-Query Lower Bound for Unitary Synthesis and Breaking Quantum Cryptography". In: *Proceedings of the 56th Annual ACM Symposium on Theory of Computing (STOC)*. 2024 (cit. on pp. 1, 5–7).

[Ma23] Fermi Ma. *Quantum Commitments and Black Hole Radiation Decoding*. Talk at the Simons Institute Workshop on Quantum Gravity. 2023. URL: https://www.youtube.com/watch?v=4jcj9WfVQiM (cit. on pp. 1, 5).

[Ma24] Fermi Ma. *Pseudorandom states and the purification trick*. Talk at the Simons Institute Workshop on Pseudorandom States and Unitaries. 2024. URL: https://fermima.com/talks/prs-simons.pdf (cit. on p. 2).

[MH24] Fermi Ma and Hsin-Yuan Huang. *How to Construct Random Unitaries*. 2024. arXiv: 2410.10116 [quant-ph]. URL: https://arxiv.org/abs/2410.10116 (cit. on pp. 1–3, 7).

Additional References

[Aar16] Scott Aaronson. *The Complexity of Quantum States and Transformations: From Quantum Money to Black Holes*. 2016. arXiv: 1607.05256 [quant-ph]. URL: https://arxiv.org/abs/1607.05256 (cit. on pp. 5, 6).

[Aar21] Scott Aaronson. *Open Problems Related to Quantum Query Complexity*. 2021. arXiv: 2109.06917 [quant-ph]. URL: https://arxiv.org/abs/2109.06917 (cit. on p. 6).

[ABC+24] Chris Akers, Adam Bouland, Lijie Chen, Tamara Kohler, Tony Metger, and Umesh Vazirani. *Holographic pseudoentanglement and the complexity of the AdS/CFT dictionary*. 2024. arXiv: 2411.04978 [hep-th]. URL: https://arxiv.org/abs/2411.04978 (cit. on p. 5).

[ABGL24] Prabhanjan Ananth, John Bostanci, Aditya Gulati, and Yao-Ting Lin. *Pseudorandomness in the (Inverseless) Haar Random Oracle Model*. 2024. arXiv: 2410.19320 [quant-ph]. URL: https://arxiv.org/abs/2410.19320 (cit. on pp. 1, 3).

[AGKL24] Prabhanjan Ananth, Aditya Gulati, Fatih Kaleoglu, and Yao-Ting Lin. "Pseudorandom Isometries". In: *43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. 2024 (cit. on p. 2).

[AK07] Scott Aaronson and Greg Kuperberg. "Quantum versus Classical Proofs and Advice". In: *22nd Annual IEEE Conference on Computational Complexity (CCC)*. 2007 (cit. on pp. 1, 5).

[AMPS13] Ahmed Almheiri, Donald Marolf, Joseph Polchinski, and James Sully. "Black holes: complementarity or firewalls?" In: *Journal of High Energy Physics* (2013) (cit. on p. 5).

[BBH+19] James Bartusek, Liron Bronfman, Justin Holmgren, Fermi Ma, and Ron D. Rothblum. "On the (In)security of Kilian-Based SNARGs". In: *Theory of Cryptography - 17th International Conference (TCC)*. 2019 (cit. on p. 6).

[BBK22] Nir Bitansky, Zvika Brakerski, and Yael Tauman Kalai. "Constructive Post-Quantum Reductions". In: *42nd Annual International Cryptology Conference, (CRYPTO)*. 2022 (cit. on p. 4).

[BCJ+19] James Bartusek, Brent Carmer, Abhishek Jain, Zhengzhong Jin, Tancrède Lepoint, Fermi Ma, Tal Malkin, Alex J. Malozemoff, and Mariana Raykova. "Public-Key Function-Private Hidden Vector Encryption (and More)". In: *25th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*. 2019 (cit. on p. 6).

[BCKM21a] James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. "On the Round Complexity of Secure Quantum Computation". In: *41st Annual International Cryptology Conference, (CRYPTO)*. 2021 (cit. on p. 6).

[BCKM21b] James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. "One-Way Functions Imply Secure Computation in a Quantum World". In: *41st Annual International Cryptology Conference, (CRYPTO)*. 2021 (cit. on p. 6).

[BFV20] Adam Bouland, Bill Fefferman, and Umesh V. Vazirani. "Computational Pseudorandomness, the Wormhole Growth Paradox, and Constraints on the AdS/CFT Duality (Abstract)". In: *11th Innovations in Theoretical Computer Science Conference (ITCS)*. 2020 (cit. on p. 5).

[BGMZ18] James Bartusek, Jiaxin Guan, Fermi Ma, and Mark Zhandry. "Return of GGH15: Provable Security Against Zeroizing Attacks". In: *Theory of Cryptography - 16th International Conference (TCC)*. 2018 (cit. on p. 6).

[BHHP24] John Bostanci, Jonas Haferkamp, Dominik Hangleiter, and Alexander Poremba. *Efficient Quantum Pseudorandomness from Hamiltonian Phase States*. 2024. arXiv: 2410.08073 [quant-ph]. URL: https://arxiv.org/abs/2410.08073 (cit. on pp. 1, 3).

[BIJ+20] James Bartusek, Yuval Ishai, Aayush Jain, Fermi Ma, Amit Sahai, and Mark Zhandry. "Affine Determinant Programs: A Framework for Obfuscation and Witness Encryption". In: *11th Innovations in Theoretical Computer Science Conference (ITCS)*. 2020 (cit. on p. 6).

[BKL+22] James Bartusek, Yael Tauman Kalai, Alex Lombardi, Fermi Ma, Giulio Malavolta, Vinod Vaikuntanathan, Thomas Vidick, and Lisa Yang. "Succinct Classical Verification of Quantum Computation". In: *42nd Annual International Cryptology Conference, (CRYPTO)*. 2022 (cit. on pp. 4, 6).

[BLMZ19] James Bartusek, Tancrède Lepoint, Fermi Ma, and Mark Zhandry. "New Techniques for Obfuscating Conjunctions". In: *38th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. 2019 (cit. on p. 6).

[BM24] Zvika Brakerski and Nir Magrafta. *Real-Valued Somewhat-Pseudorandom Unitaries*. 2024. arXiv: 2403.16704 [quant-ph]. URL: https://arxiv.org/abs/2403.16704 (cit. on p. 2).

[BMZ19] James Bartusek, Fermi Ma, and Mark Zhandry. "The Distinction Between Fixed and Random Generators in Group-Based Assumptions". In: *39th Annual International Cryptology Conference (CRYPTO)*. 2019 (cit. on p. 6).

[Bra23] Zvika Brakerski. "Black-Hole Radiation Decoding Is Quantum Cryptography". In: *43rd Annual International Cryptology Conference, (CRYPTO)*. 2023 (cit. on p. 5).

[Bru24] Ben Brubaker. "Cryptographers Discover a New Foundation for Quantum Secrecy". In: *Quanta Magazine* (June 3, 2024). URL: https://www.quantamagazine.org/cryptographers-discover-a-new-foundation-for-quantum-secrecy-20240603/ (cit. on pp. 1, 6).

[CAD+24] Alessandro Chiesa, Marcel Dall Agnol, Zijing Di, Ziyi Guan, and Nicholas Spooner. *Quantum Rewinding for IOP-Based Succinct Arguments*. 2024. arXiv: 2411.05360 [cs.CR]. URL: https://arxiv.org/abs/2411.05360 (cit. on p. 4).

[CBB+24] Chi-Fang Chen, Adam Bouland, Fernando G. S. L. Brandão, Jordan Docter, Patrick Hayden, and Michelle Xu. *Efficient unitary designs and pseudorandom unitaries from permutations*. 2024. arXiv: 2404.16751 [quant-ph]. URL: https://arxiv.org/abs/2404.16751 (cit. on p. 2).

[CLMQ21] Yilei Chen, Alex Lombardi, Fermi Ma, and Willy Quach. "Does Fiat-Shamir Require a Cryptographic Hash Function?" In: *41st Annual International Cryptology Conference, (CRYPTO)*. 2021 (cit. on p. 6).

[EFL+24] Netta Engelhardt, Åsmund Folkestad, Adam Levine, Evita Verheijden, and Lisa Yang. *Cryptographic Censorship*. 2024. arXiv: 2402.03425 [hep-th]. URL: https://arxiv.org/abs/2402.03425 (cit. on pp. 1, 3, 7).

[ELL05] Joseph Emerson, Etera Livine, and Seth Lloyd. "Convergence conditions for random quantum circuits". In: *Physical Review A* 72.6 (Dec. 2005) (cit. on p. 2).

[EWS+03] Joseph Emerson, Yaakov S Weinstein, Marcos Saraceno, Seth Lloyd, and David G Cory. "Pseudo-random unitary operators for quantum information processing". In: *science* 302.5653 (2003), pp. 2098–2100 (cit. on p. 2).

[FS89] Uriel Feige and Adi Shamir. "Zero Knowledge Proofs of Knowledge in Two Rounds". In: *9th Annual International Cryptology Conference (CRYPTO)*. 1989 (cit. on pp. 1, 4).

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. "How to construct random functions". In: *J. ACM* (1986) (cit. on p. 2).

[GK96] Oded Goldreich and Ariel Kahan. "How to construct constant-round zero-knowledge proof systems for NP". In: *Journal of Cryptology* (1996) (cit. on pp. 1, 4).

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. "Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems". In: *Journal of the ACM (JACM)* (1991) (cit. on pp. 1, 4).

[GQY+24] Andi Gu, Yihui Quek, Susanne Yelin, Jens Eisert, and Lorenzo Leone. *Simulating quantum chaos without chaos*. 2024. arXiv: 2410.18196 [quant-ph]. URL: https://arxiv.org/abs/2410.18196 (cit. on pp. 3, 7).

[HBK23] Tobias Haug, Kishor Bharti, and Dax Enshan Koh. *Pseudorandom unitaries are neither real nor sparse nor noise-robust*. 2023. arXiv: 2306.11677 [quant-ph]. URL: https://arxiv.org/abs/2306.11677 (cit. on p. 2).

[HH13] Daniel Harlow and Patrick Hayden. "Quantum computation vs. firewalls". In: *Journal of High Energy Physics* (2013) (cit. on p. 5).

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. "Pseudorandom Quantum States". In: *38th Annual International Cryptology Conference (CRYPTO)*. 2018 (cit. on p. 2).

[Kil92] Joe Kilian. "A Note on Efficient Zero-Knowledge Proofs and Arguments (Extended Abstract)". In: *Proceedings of the 24th Annual ACM Symposium on Theory of Computing (STOC)*. 1992 (cit. on pp. 1, 4).

[KP23] Isaac H Kim and John Preskill. "Complementarity and the unitarity of the black hole S-matrix". In: *Journal of High Energy Physics* 2023.2 (2023), pp. 1–46 (cit. on pp. 1, 3, 7).

[KQST23] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. "Quantum Cryptography in Algorithmica". In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC)*. 2023 (cit. on pp. 1, 5).

[LMQW20] Xin Li, Fermi Ma, Willy Quach, and Daniel Wichs. "Leakage-Resilient Key Exchange and Two-Seed Extractors". In: *40th Annual International Cryptology Conference (CRYPTO)*. 2020 (cit. on p. 6).

[LQS+24] Chuhan Lu, Minglong Qin, Fang Song, Penghui Yao, and Mingnan Zhao. *Quantum Pseudorandom Scramblers*. 2024. arXiv: 2309.08941 [quant-ph]. URL: https://arxiv.org/abs/2309.08941 (cit. on p. 2).

[MNZ24] Tony Metger, Anand Natarajan, and Tina Zhang. *Succinct arguments for QMA from standard assumptions via compiled nonlocal games*. 2024. arXiv: 2404.19754 [quant-ph]. URL: https://arxiv.org/abs/2404.19754 (cit. on p. 4).

[MPSY24a] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. *Pseudorandom unitaries with non-adaptive security*. 2024. arXiv: 2402.14803 [quant-ph]. URL: https://arxiv.org/abs/2402.14803 (cit. on pp. 1, 2).

[MPSY24b] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. *Simple constructions of linear-depth t-designs and pseudorandom unitaries*. 2024. arXiv: 2404.12647 [quant-ph]. URL: https://arxiv.org/abs/2404.12647 (cit. on p. 2).

[MZ18] Fermi Ma and Mark Zhandry. "The MMap Strikes Back: Obfuscation and New Multilinear Maps Immune to CLT13 Zeroizing Attacks". In: *Theory of Cryptography - 16th International Conference (TCC)*. 2018 (cit. on p. 6).

[RR94] Alexander A. Razborov and Steven Rudich. "Natural proofs". In: *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing (STOC)*. 1994 (cit. on p. 7).

[SHH24] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. *Random unitaries in extremely low depth*. 2024. arXiv: 2407.07754 [quant-ph]. URL: https://arxiv.org/abs/2407.07754 (cit. on pp. 1, 3, 7).

[Unr12] Dominique Unruh. "Quantum Proofs of Knowledge". In: *31st Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. 2012 (cit. on p. 4).

[Unr16] Dominique Unruh. "Computationally Binding Quantum Commitments". In: *35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. 2016 (cit. on p. 4).

[Van97] Jeroen Van De Graaf. *Towards a formal definition of security for quantum protocols*. Citeseer, 1997 (cit. on p. 3).

[Wat09] John Watrous. "Zero-Knowledge against Quantum Attacks". In: *SIAM J. Comput.* 39.1 (2009), pp. 25–58 (cit. on p. 4).

[Zha23] Mark Zhandry. "Tracing Quantum State Distinguishers via Backtracking". In: *43rd Annual International Cryptology Conference, (CRYPTO)*. 2023 (cit. on p. 4).