I seek to understand how quantum computing can be harnessed to provide guarantees that are otherwise impossible to achieve. By exploiting the laws of physics, quantum computing introduces a new model of computation that enables capabilities beyond the reach of classical computers. The impact of quantum computation has been explored across various domains, including machine learning, distributed computing, and chemistry, primarily with the goal of achieving exponential speedups over classical algorithms. The field of cryptography is also affected by such speedups, as adversaries equipped with quantum computers have the potential to break existing cryptosystems. This has motivated the development of schemes that remain secure even in the presence of quantum computers, which is the focus of the field of *post-quantum cryptography*.

At the same time, quantum computing can also be harnessed to construct new kinds of cryptosystems. Moreover, speedups alone are not the extent of what it can offer; quantum capabilities can enable qualitatively new forms of advantage beyond computational efficiency. This direction is explored by the field of **quantum cryptography**, which studies cryptographic tasks enabled by quantum information and computation. In this context, quantum information has been shown to provide several distinct forms of advantage, such as:

1. **Improved efficiency** in terms of computation time, communication cost, latency etc. For example, efficient proof systems (succinct arguments for NP) can be realized by a *three*-round protocol [1] using quantum communication and standard assumptions, whereas comparable classical protocols require at least *four* rounds.
2. **Stronger security guarantees** achievable under weaker computational assumptions than in the classical setting. For instance, quantum protocols for secure multi-party computation (MPC) can be based on the hardness of inverting one-way functions (OWFs) [2, 3], whereas classical protocols necessarily require stronger assumptions.
3. **Fundamentally new forms of security** that cannot be obtained classically under any computational assumption. A canonical example is **quantum money**, which enables the generation of quantum states that serve as banknotes which provably resist counterfeiting. In contrast, any banknote encoded using classical information can, in principle, be copied perfectly.

1 Prior Work

Recently, my research has focused on the third kind of advantage, specifically within the field of **unclonable cryptography**. This area studies how quantum information can be used to protect sensitive data from being copied. For instance, it studies how software can be encoded using quantum information in order to combat the widespread issue of software piracy. The key underlying principle is the *no-cloning theorem* of quantum mechanics, which has no classical analogue: it guarantees that arbitrary unknown quantum states cannot be duplicated. This fundamental distinction has enabled the construction of cryptographic primitives unique to the quantum setting, such as quantum money [4, 5], copy protection [6], encryption with certified deletion [7], and one-time programs [8, 9] to name a few. Despite this rapid progress, there is scope to revisit many of the security definitions of these primitives. This can help to uncover potential vulnerabilities that arise due to modelling choices that may not capture real world requirements. Moreover, as in a lot of cryptography, it is a fruitful pursuit to improve constructions by basing them on weaker and well-understood cryptographic assumptions. Not only would this improve our understanding of different cryptographic primitives, but makes it more practical to deploy them in terms of both security and efficiency. In this light, my prior work has focused on developing new **collusion-resistant** definitions for such primitives, followed by constructing them with a focus on well-understood assumptions. In these definitions, certain meaningful security guarantees are preserved even when multiple adversarial users collude, making it more realistic than the standalone setting with a single adversary. In the following subsections, I will discuss the different primitives I have worked on in this collusion-resistant context.

1.1 Secure Key Leasing for Encryption.

In one of my joint works [10], I studied the unclonable primitive of **secure key leasing (SKL)** [11, 12]. This notion enables a secret key of a cryptosystem to be encoded into a quantum state, which can then be temporarily leased. Later, the recipient can produce a **deletion certificate**, which, if verified to be valid, ensures that they have effectively lost access to the secret key. For instance, SKL in the context of public-key encryption (PKE) is called **PKE-SKL**, and it allows one to securely lease decryption keys of a PKE scheme. Anyone in possession of the leased quantum state can decrypt arbitrarily many ciphertexts, but once a valid deletion certificate is produced, they can no longer distinguish ciphertexts of different messages. Notice that if the leased key was classical, the recipient could simply

make a copy for later use. PKE-SKL is particularly useful for subscription services like Netflix that might wish to provide trial-period access to their content. The content could be broadcast in encrypted form, and quantum keys could be provided to users for a fee. Later, users could be refunded upon returning their keys. While previous works have constructed PKE-SKL, these constructions are not ideal for such applications because they suffer one of two drawbacks:

- They achieve only **bounded collusion-resistance**, meaning the parameters of the scheme (such as public-key and ciphertext sizes) scale polynomially with the number of colluding users. This requires knowing the collusion bound in advance, which is often unrealistic, while choosing a large bound results in highly inefficient schemes.
- They rely on **indistinguishability obfuscation (iO)**, a strong assumption that implies most of cryptography. Constructions based on iO are inefficient and less desirable than those based on simpler assumptions such as the existence of OWFs. Moreover, quantum-secure iO is not yet known from well-understood assumptions.

In our work, we addressed these limitations by constructing a PKE-SKL scheme with **unbounded collusion-resistance** under the standard **learning with errors (LWE)** assumption. Unbounded collusion-resistance means that the scheme parameters grow only polylogarithmically with the number of colluding users, making it well-suited for large-scale applications such as the Netflix scenario above. Our construction introduced several new ideas, including the generation of quantum keys consisting of secret keys of an **attribute-based encryption (ABE)** scheme in superposition. At a high level, our security proof involves switching the ciphertext distribution so that an adversary who deletes its quantum keys cannot detect the change. Using the security of ABE, we then argued that the adversary learns nothing about the plaintext for ciphertexts generated under the new distribution. Apart from the result itself, our techniques have advanced the ways in which quantum states can be entangled with secret classical information, to harness unique phenomena. These ideas could inspire new constructions in other quantum cryptographic contexts.

1.2 SKL for PRFs and Signatures.

After my previous work on SKL, I began wondering whether collusion-resistant SKL based on standard assumptions is possible for other cryptographic primitives. Unfortunately, in the context of SKL, the techniques of my prior work seem specific to the case of encryption. Moreover, nothing was known about collusion-resistant SKL for pseudo-random functions (PRFs) and signatures which are central cryptographic primitives. This became the focus of my next joint work [13], in which we first developed generic definitions for SKL that capture SKL for various primitives as special cases. We then identified an intermediate primitive called multi-level traitor tracing (MLTT), that generalizes the classical notion of traitor tracing and presented a compiler that transforms an MLTT scheme for a primitive X into a collusion-resistant SKL scheme for X. In this way, our result established SKL for a general class of functionalities while also providing collusion-resistance, whereas previous works focused only on individual primitives in the single-key setting. This unified approach makes our construction modular and helps to avoid redundancy. We then leveraged this compiler to obtain a **bounded collusion-resistant SKL scheme for PRFs**. This involved first constructing an MLTT scheme for PRFs and overcoming difficulties related to tracing quantum adversaries [14, 15]. While we achieved only *bounded* collusion-resistance for PRFs, even this task is highly nontrivial—unlike the case of PKE-SKL, where bounded collusion-resistance is straightforward. Additionally, we identified a simpler approach in the case of **digital signatures**. Specifically, we showed how to transform a single-key secure SKL scheme for signatures into one with unbounded collusion-resistance, assuming only OWFs. Our technique is also applicable to copy-protection for signatures, and greatly simplifies the approaches taken by prior works [16, 17]. Finally, assuming OWFs, we presented a compiler that upgrades SKL schemes to satisfy a stronger security notion. Specifically, the notion allows the adversary to have oracle access to the result of certificate verification, which is a desirable property for practical applications.

1.3 Unclonable Puncturable Obfuscation (Ongoing Work).

After developing a generic way to build collusion-resistant SKL schemes, I began exploring analogous notions for **quantum copy protection**. Intuitively, copy protection encodes software into quantum states in a way that preserves functionality but prevents duplication. While several previous works [16, 17] studied collusion-resistant copy protection, they focused on individual primitives. Other works [18, 19, 20] investigated an intermediate primitive called **unclonable puncturable obfuscation (UPO)** as a means to construct copy-protection schemes, but these are limited to the single-instance setting. As a result, no generic framework for collusion-resistant copy protection was known. In ongoing joint work, we define **collusion-resistant UPO** and present a modular construction for it based on any collusion-resistant copy-protection scheme for the decryption functionality of a PKE scheme. In contrast, prior works on single-instance secure UPO constructed it from scratch, relying on similar techniques as those used for copy protection for PKE. Our construction enables copy protection research to be focused on the PKE case, as it enables

UPO which itself enables many other primitives. This latter implication however, is more involved in the collusion-resistant case, and we are currently exploring it in detail. For some of the results, we require new techniques and workarounds beyond those used in the single-instance setting, due to well-known barriers in unclonable cryptography. Along the way, we are also studying relationships between various definitions of collusion-resistant copy protection. Many questions in this domain remain open, and I will now discuss some that particularly interest me.

2 Future Directions

1. **Identical-Challenge Variants of Copy Protection.** The standard copy-protection security notion involves a tri-partite adversary (Alice, Bob, Charlie), where Alice receives a quantum state and splits it between Bob and Charlie, who then receive an independent challenge each. The setting where Bob and Charlie receive *identical* challenges is known to be significantly more complex, even in the single-instance case. In fact, identical challenge secure copy protection schemes are not yet known in the plain model. Still, intermediate notions with partially identical challenges are known to be achievable in the single-instance setting. However, it is unclear how to generalize these results to the setting of collusions. It is interesting to study whether these generalizations face similar challenges as the identical challenge single-instance setting, or are feasible with different techniques.
2. **Unclonable Primitives vs Quantum Money.** Another open direction concerns the relationship between copy protection and quantum money. Copy protection for publicly verifiable primitives (e.g., PKE, signatures) implies public-key quantum money, which seems to require strong assumptions. On the other hand, copy protection for PRFs is not known to imply quantum money. However, known constructions for it utilize cryptographic machinery that implies quantum money, making the relationship between the primitives unclear. Similarly, SKL with publicly verifiable deletion for publicly verifiable primitives implies quantum money, but not in the PRF case. Another interesting aspect is that known copy protection schemes require iO, while quantum money is also known from other new assumptions [21, 22]. Understanding the relationships between these notions and constructing copy protection without iO would be an important step forward.
3. **NIZK Proofs with Everlasting Zero-Knowledge.** There are several interesting unclonable primitives apart from SKL and copy protection, one of which is a non-interactive zero-knowledge (NIZK) proof with **everlasting zero-knowledge**. Intuitively, it allows a prover to send a quantum proof of an NP statement to a verifier, who can later produce a deletion certificate, after which a statistical zero-knowledge guarantee holds. This is a desirable notion as it is highly unlikely to have NIZK proofs (which have statistical soundness) that also satisfy statistical zero-knowledge. Such everlasting zero-knowledge proofs were previously studied [23, 24] in the interactive setting, but extending them to the non-interactive setting introduces new challenges. Investigating feasibility and barriers in this direction remains an intriguing open problem.
4. **Relationships between Quantum Reductions:** In another joint work [25], I studied reductions in a quantum world as part of a broad framework, apart from showing the impossibility of a special kind of NIZK in the quantum setting. Our work classified quantum reductions between two cryptographic primitives into various categories. Some of the considerations we made include whether the construction of the target primitive is quantum or not, and whether the security reduction accesses the adversary classically or quantumly, and whether this access is black-box or not. There is a lot of room for more fine-grained classifications, such as whether the reduction has access to the inverse or conjugate of an adversarial unitary or not. Surprisingly, recent works have shown constructions which remain secure under certain kind of unitary access but fall apart under other access [26, 27]. However, there are far fewer separations of this kind when it comes to cryptographic primitives instead of specific constructions. It is an exciting direction to understand precisely how different quantum capabilities affect the relation between different cryptographic primitives.
5. **New Uses of Quantum Information:** Beyond unclonable primitives, one can explore whether quantum information enables other fundamentally new cryptographic functionalities. For instance, Coladangelo et al. [28] demonstrated new forms of deniable encryption that are uniquely possible in the quantum setting. It would be interesting to study related notions along this line. The impact of quantum information can also be examined further in the context of achieving stronger security guarantees. For example, can quantum proofs be constructed to resist malleability attacks? Similarly, can quantum secret keys make it harder for adversaries to evade tracing? While classical cryptography offers solutions to such problems, they typically rely on strong computational assumptions. Understanding whether quantum information can reduce these assumptions remains largely unexplored and is an exciting direction for future work.

References

[1] S. Gunn, N. Ju, F. Ma, and M. Zhandry, "Commitments to quantum states," in *55th ACM STOC* (B. Saha and R. A. Servedio, eds.), pp. 1579–1588, ACM Press, June 2023.

[2] A. B. Grilo, H. Lin, F. Song, and V. Vaikuntanathan, "Oblivious transfer is in MiniQCrypt," in *EUROCRYPT 2021, Part II* (A. Canteaut and F.-X. Standaert, eds.), vol. 12697 of *LNCS*, pp. 531–561, Springer, Cham, Oct. 2021.

[3] J. Bartusek, A. Coladangelo, D. Khurana, and F. Ma, "One-way functions imply secure computation in a quantum world," in *CRYPTO 2021, Part I* (T. Malkin and C. Peikert, eds.), vol. 12825 of *LNCS*, (Virtual Event), pp. 467–496, Springer, Cham, Aug. 2021.

[4] S. Wiesner, "Conjugate coding," *ACM Sigact News*, vol. 15, no. 1, pp. 78–88, 1983.

[5] S. Aaronson and P. Christiano, "Quantum money from hidden subspaces," in *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pp. 41–60, 2012.

[6] S. Aaronson, "Quantum copy-protection and quantum money," in *2009 24th Annual IEEE Conference on Computational Complexity*, pp. 229–242, IEEE, 2009.

[7] A. Broadbent and R. Islam, "Quantum encryption with certified deletion," in *TCC 2020, Part III* (R. Pass and K. Pietrzak, eds.), vol. 12552 of *LNCS*, pp. 92–122, Springer, Cham, Nov. 2020.

[8] A. Broadbent, G. Gutoski, and D. Stebila, "Quantum one-time programs," in *Annual Cryptology Conference*, pp. 344–360, Springer, 2013.

[9] A. Gupte, J. Liu, J. Raizes, B. Roberts, and V. Vaikuntanathan, "Quantum one-time programs, revisited," in *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, pp. 213–221, 2025.

[10] F. Kitagawa, R. Nishimaki, and N. Pappu, "PKE and ABE with collusion-resistant secure key leasing," in *CRYPTO 2025, Part III*, LNCS, pp. 35–68, Springer, Cham, Aug. 2025.

[11] P. Ananth, A. Poremba, and V. Vaikuntanathan, "Revocable cryptography from learning with errors," in *TCC 2023, Part IV* (G. N. Rothblum and H. Wee, eds.), vol. 14372 of *LNCS*, pp. 93–122, Springer, Cham, Nov. / Dec. 2023.

[12] S. Agrawal, F. Kitagawa, R. Nishimaki, S. Yamada, and T. Yamakawa, "Public key encryption with secure key leasing," in *EUROCRYPT 2023, Part I* (C. Hazay and M. Stam, eds.), vol. 14004 of *LNCS*, pp. 581–610, Springer, Cham, Apr. 2023.

[13] F. Kitagawa, R. Nishimaki, and N. Pappu, "Collusion-resistant quantum secure key leasing beyond decryption," *arXiv preprint arXiv:2510.04754*, 2025.

[14] M. Zhandry, "Schrödinger's pirate: How to trace a quantum decoder," in *TCC 2020, Part III* (R. Pass and K. Pietrzak, eds.), vol. 12552 of *LNCS*, pp. 61–91, Springer, Cham, Nov. 2020.

[15] M. Zhandry, "Tracing quantum state distinguishers via backtracking," in *CRYPTO 2023, Part V* (H. Handschuh and A. Lysyanskaya, eds.), vol. 14085 of *LNCS*, pp. 3–36, Springer, Cham, Aug. 2023.

[16] J. Liu, Q. Liu, L. Qian, and M. Zhandry, "Collusion resistant copy-protection for watermarkable functionalities," in *TCC 2022, Part I* (E. Kiltz and V. Vaikuntanathan, eds.), vol. 13747 of *LNCS*, pp. 294–323, Springer, Cham, Nov. 2022.

[17] A. Çakan and V. Goyal, "Unclonable cryptography with unbounded collusions and impossibility of hyperefficient shadow tomography," in *TCC 2024, Part III* (E. Boyle and M. Mahmoody, eds.), vol. 15366 of *LNCS*, pp. 225–256, Springer, Cham, Dec. 2024.

[18] P. Ananth and A. Behera, "A modular approach to unclonable cryptography," in *CRYPTO 2024, Part VII* (L. Reyzin and D. Stebila, eds.), vol. 14926 of *LNCS*, pp. 3–37, Springer, Cham, Aug. 2024.

[19] P. Ananth, A. Behera, and Z. Huang, "Copy-protection from upo, revisited," *Cryptology ePrint Archive*, 2025.

[20] F. Kitagawa and T. Yamakawa, "Copy protecting cryptographic functionalities over entropic inputs," *Cryptology ePrint Archive*, 2025.

[21] M. Zhandry, "Quantum money from abelian group actions," in *ITCS 2024* (V. Guruswami, ed.), vol. 287, pp. 101:1–101:23, LIPIcs, Jan. / Feb. 2024.

[22] J. Liu, H. Montgomery, and M. Zhandry, "Another round of breaking and making quantum money: How to not build it from lattices, and more," in *EUROCRYPT 2023, Part I* (C. Hazay and M. Stam, eds.), vol. 14004 of *LNCS*, pp. 611–638, Springer, Cham, Apr. 2023.

[23] T. Hiroka, T. Morimae, R. Nishimaki, and T. Yamakawa, "Certified everlasting zero-knowledge proof for QMA," in *CRYPTO 2022, Part I* (Y. Dodis and T. Shrimpton, eds.), vol. 13507 of *LNCS*, pp. 239–268, Springer, Cham, Aug. 2022.

[24] J. Bartusek and D. Khurana, "Cryptography with certified deletion," in *CRYPTO 2023, Part V* (H. Handschuh and A. Lysyanskaya, eds.), vol. 14085 of *LNCS*, pp. 192–223, Springer, Cham, Aug. 2023.

[25] C. Lu and N. Pappu, "Notions of quantum reductions and impossibility of statistical NIZK." Cryptology ePrint Archive, Report 2024/1847, 2024.

[26] M. Zhandry, "How to model unitary oracles," in *CRYPTO 2025, Part II*, LNCS, pp. 237–268, Springer, Cham, Aug. 2025.

[27] E. Tang, J. Wright, and M. Zhandry, "Conjugate queries can help," 2025.

[28] A. Coladangelo, S. Goldwasser, and U. V. Vazirani, "Deniable encryption in a quantum world," in *54th ACM STOC* (S. Leonardi and A. Gupta, eds.), pp. 1378–1391, ACM Press, June 2022.