Post-Quantum Adversarial Modelling:
A User's Perspective

Teik Guan Tan, Jianying Zhou
Singapore University of Technology and Design

Vishal Sharma
Queen's University Belfast

Saraju P. Mohanty
University of North Texas

Abstract—The impending arrival of quantum computers will bring both benefits and risks to the computing industry. The potential threat comes in the form of cryptanalysis attacks by adversaries who can make use of quantum computers in the future to break vulnerable algorithms such as RSA and ECC, resulting in the compromise of confidentiality and integrity of applications and data. But are adversaries doing anything more to exploit this opportunity? We use an adversarial modelling approach by first identifying the various adversarial personas and then fleshing out both passive and active actions that such adversaries can take to gain an advantage. With these actions identified, we then arrive at suitable short and longer-term recommendations on mitigating actions that can be taken.

I. INTRODUCTION

Quantum computers are coming, and they make computer security systems vulnerable to cryptanalysis. Shor's algorithm [1] running on a quantum computer can break asymmetric key cryptosystems such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC). Additionally, Grover's algorithm [2] will weaken symmetric key encryption, hashing and password systems to half their designed security strength. This means that many existing security deployments such as Transport Layer Security (TLS) used to secure Internet browsing, PDF signing used to protect electronic documents, code signing used for automatic system updates, end-to-end encryption used to provide data privacy, etc., will no longer be deemed secure and instead be rendered untrustworthy with the advent of quantum

computers. The good news, though, is that the current noisy intermediate-state quantum computers are not ready to break industrial-strength cryptography. For quantum computers to be cryptanalysis-capable, the number of qubits, depth of circuits, duration of coherence, accuracy of error correction all need to improve several hundred or thousand-fold, and this is not likely to happen for at least another ten years [3].
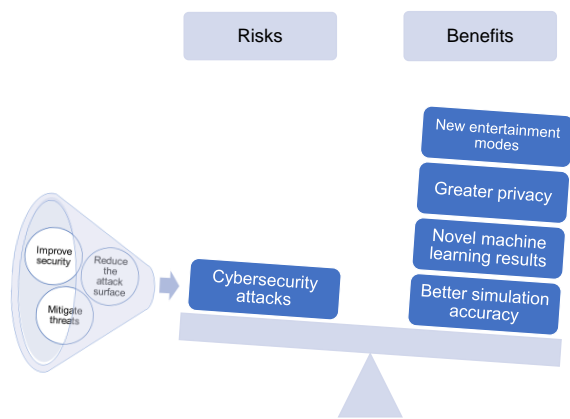

Figure 1: Can quantum benefits outweigh the risks?

Much like how Hurlburt [4] has succinctly described the cybersecurity perils of technology due to untimely prevention and intervention, we view the quantum roadmap as a race between how fast quantum technology is invented versus how soon existing applications can be adapted to shield against its side effects. On the one hand, researchers

are working on building larger, more fault-tolerant quantum technologies which can be used for new applications in simulations [5], machine learning [6], and even entertainment [7]. On the other hand, system owners need to embark on a migration or renewal plan for their applications to defend against possible quantum attacks. As depicted in Figure 1, instead of holding back on quantum technology advancements, we should strive to reduce the impact and likelihood of quantum attacks so that quantum benefits significantly outweigh the risks.

From an adversarial standpoint, quantum computers present a golden opportunity to exploit the vulnerabilities promised. But since fault-tolerant quantum technology is not yet ready, are the adversaries simply waiting or are they already carrying out activities to maximize their impact when cryptanalysis-capable quantum computers become available? In this article, we explore the question:

> What are adversaries doing today to prepare for the impending availability of cryptanalysis-capable quantum computers?

To answer this question comprehensively, we model the adversary in a three-step approach :

Step 1: Profile the different adversarial personas, their resources and motivations. Assuming that each adversary has access to a cryptanalysis-capable quantum computer today, flesh out the attacks with which the adversary can use the quantum computer to compromise their targets. This is covered in Section II.

Step 2: Abstract relevant pre-processing activities that each adversary performs prior to using the quantum computer. We expect these are likely passive work being carried out by adversaries today since they are not bottlenecked by the availability of quantum computers and yet maximize the adversaries' advantage against their peers and targets. We describe these passive actions in Section III.

Step 3: Identify various points in the targets' quantum roadmap and their dependencies that can be affected by an adversary. Besides passive steps, we expect some adversaries to take active steps in increasing their targets' exposure to quantum computers. This would be in the form of disrupting the quantum-readiness of the vulnerable targets, with the aim of leaving them still vulnerable when cryptanalysis-capable quantum computers become available. This is analyzed in Section IV.

From this adversary model, we can then derive recommendations on concrete actions that can be taken today to prevent exposure to or mitigate such adversarial activities.

II. PROFILING ADVERSARIAL PERSONAS

We take reference from Rocchetto, and Tippenhauer [9] who perform a comprehensive study on various adversary profiles. We bucket them into five personas below in increasing level of resources:

- *Basic User*. The *Basic User* is a technology-literate individual with limited resources who carries out attacks out of curiosity, personal glory, fun and are typically non-malicious. A "Script Kiddy" is an example of a *Basic User* who uses readily-available hacking tools to attack known vulnerabilities. More sophisticated users include white-hat hackers who participate in bug-bounty challenges to uncover new vulnerabilities.
- *Insider (or Disgruntled Employee)*. The *Insider* is also an individual but festers malicious intent in sabotaging an entity for revenge purposes. The *Insider* would typically have access to protected information and privileged access rights which allow for such adversarial activities to easily take place.
- *Hacktivist*. The *Hacktivist* may operate solo but more commonly in small, decentralized groups where they use cyber-hacking activities to drive specific agendas such as environmental awareness, data emancipation, etc. The "Anonymous" group is a famous *Hacktivist* example fighting against governmental oppression. In its extreme form, *Hacktivists* engage in terrorist activities that spread fear and cause widespread disruption.
- *Cybercriminal (or Hacker for hire)* The *Cybercriminal* is usually part of organized crime syndicates that turn their knowledge and skills
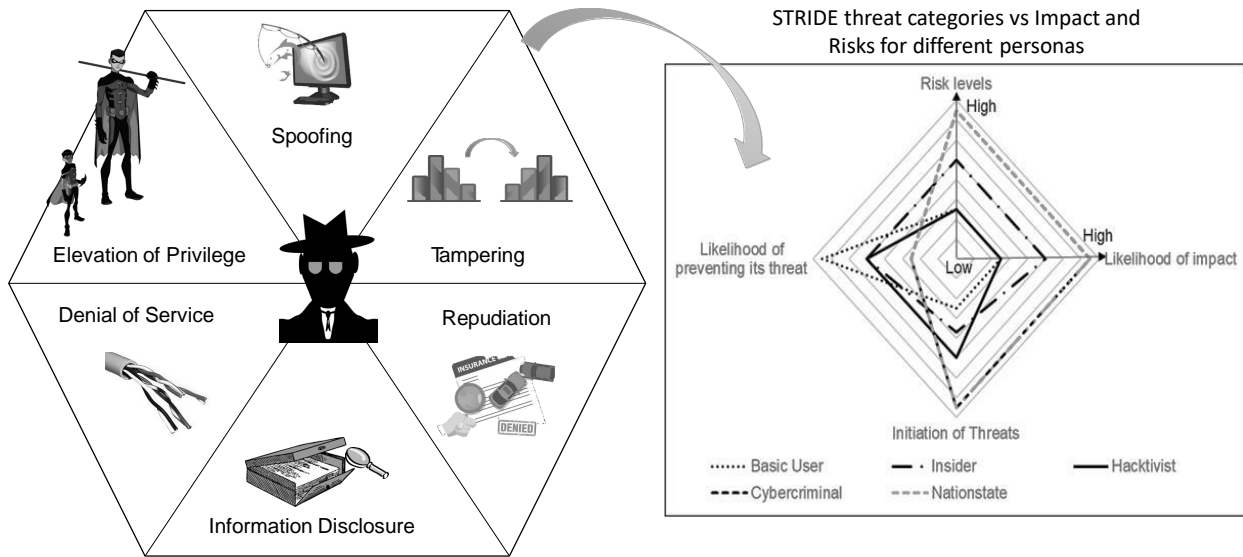
Figure 2: The STRIDE threat categories [8] along with impact and risk range for different users.

of compromising systems into financial gain. Beyond making a statement, the *Cybercriminal* would engage in corporate espionage, black-mail, ransom and other lucrative activities.

- *Nation-state* The *Nation-state* adversary is often pictured as an elusive underground organization with vast resources (sponsored by the state) to carry out nefarious activities on behalf of the government. The targets are typically public infrastructure projects, including public utilities, transport and the financial system, which, if compromised, can significantly disrupt the lives of the citizens residing in the target country.

Based on these personas and their motivation, we identify the threats by asking how these adversaries will use quantum computers if they are available today. The threat model we have chosen here is STRIDE [8] as it is an appropriate framework for examining software and data threats that quantum computers present. The six categories of threats are enumerated using the acronym that STRIDE represents, namely i) **S**poofing (when authentication is violated); ii) **T**ampering (when integrity is violated); iii) **R**epudiation (when proof of confirma-

tion is violated); iv) **I**nformation disclosure (when confidentiality is violated); v) **D**enial of service (when availability is violated); and vi) **E**levation of privilege (when access rights is violated). Figure 2 illustrates each of the threat categories pictorially.

Table I shows the range of attacks that can be carried out using a quantum computer by different adversaries. They mainly involve the compromise of authentication credentials (passwords, wifi, access credentials, wallets), protected data (phone data, emails, documents, trade secrets, classified messages), or the protocol (hijacking Internet sessions, modifying transactions, disrupting mobile & satellite communications). Based on this information, we then abstract the actions that can already be performed prior to the availability of cryptanalysis-capable quantum computers and cover this in the next two sections.

III. ABSTRACTING PASSIVE ACTIONS

We define passive actions as non-disruptive actions (akin to eavesdropping) that the adversary can take without affecting the quantum roadmap, both from the invention of cryptanalysis-capable quan-

Table I: Adversarial Personas [9] and how they can use quantum computers to achieve their goals

Persona	Motivation	STRIDE threats
Basic user	Curiosity, personal glory	**S**: Cracking passwords **T**: Defacing websites **R**: Faking crypto-currency payments. **I**: Recovering private data on phones. **D**: Hijacking wifi connections **E**: Sending commands to appliances
Insider	Revenge	**S**: Phishing for supervisor accounts. **T**: Changing employee records. **R**: Erasing audit evidence. **I**: Reading company email. **D**: Deleting databases. **E**: Creating backdoors.
Hacktivist	Publicity, agenda, emotions	**S**: Impersonating others on Internet **T**: Spreading false text messages **R**: Forging documents and contracts **I**: Revealing private documents **D**: Shutting down mobile networks **E**: Getting root access to firewalls
Cyber-criminal	Financial return	**S**: Forging fake passports **T**: Manipulating financial records. **R**: Creating fake payment cards **I**: Stealing trade secrets **D**: Taking over payment wallets **E**: Sending illegal trade instructions
Nation-state	Disruption, erosion of trust	**S**: Faking as official news media **T**: Planting backdoor applications **R**: Issuing fake certificates **I**: Tapping on classified messages. **D**: Disrupting satellite communications. **E**: Taking control of public utilities

tum computers and from the migration to quantum-secure cryptography by system owners.

A. Data Harvesting

An obvious passive action that adversaries can do is to identify and collect authentication credentials and protected data for subsequent cryptanalysis in a "harvest-then-decrypt" attack [10]. From Table I, these include:

- *Password hashes*. Passwords are stored as one-way hashes in the backend database so that they can only be used to verify the users presenting the passwords but not expose the values. However, using Grover's algorithm [2], these protection mechanisms are weakened, and the actual passwords may be revealed.
- *Certification authority (CA) certificates*. Certificates issued by a CA are used to assert the identities of the users associated with the certificates. However, using Shor's algorithm, the CA's private key can be computed from the certificates, thereby allowing forged certificates (possibly with different identities that can be backdated) to be generated.
- *Biometric minutiae*. Similar to password hashes, biometric minutiae are used to verify the identity of the users with the right biometric features. Grover's algorithm could be used to perform a brute-force search to reverse the minutiae to reveal the features, violating privacy and impersonation concerns. The alarming problem here is that while passwords can be updated to mitigate the threat, biometric features on a person cannot be changed.
- *Electronic Contracts*. Electronic contracts are digitally signed using an asymmetric key cryptosystem to ensure the integrity, non-repudiation and time-stamp of the contents. Using Shor's algorithm, the private signing key can be computed from the public verification key, which renders the contract contents untrustworthy since the relying party can no longer prove the difference between a real or fake contract.
- *Trade secrets*. Companies use trade secrets as a means of maintaining a business advantage over their competitors and store such secrets encrypted using hardware vaults. Since many of these vault implementations employ asymmetric key cryptography to protect the encryption keys and their own backups, Shor's algorithm can quickly allow an adversary to decrypt the trade secrets without needing to break the vault.
- *Confidential data exchange*. Secure emails, peer-to-peer messaging, mobile, Internet and satellite communications rely on asymmetric key encryption to exchange session keys used to protect the communication. Using Shor's algorithm, the key exchange protocol can be cryptanalysed to reveal the session keys, which then allows the adversary to see the communication in the clear.

From our analysis, what becomes apparent besides the sheer amount of data mentioned above that can be harvested is that there would be an emergence of a data marketplace or broker of sorts to facilitate the demand-generation, collection,

storage, sale and delivery of such data.

B. Target Prioritization

Even when cryptanalysis-capable quantum computers do become available, we expect the supply of such quantum computing resources to be scarcer compared to the demand. Hence, adversaries will need to figure out which targets they will go after first, and this can be done now.

The prioritization can be done based on the following criteria:

- *By value of target.* Depending on the motivations and available resources behind the adversary, each target may be valued differently. Naturally, we expect a rational adversary to use a cost-benefit ratio to choose targets where *benefit derived from the compromise $\gg$ cost to carry out the compromise.*
- *By ease of break.* Since Shor's algorithm [1] compromises asymmetric key algorithms while Grover's algorithm [2] merely weakens symmetric key and hash algorithms, it is clear that applications using asymmetric key algorithms will be first targeted. The key sizes of the asymmetric key algorithms do matter in sizing the capacity of the quantum computer to carry out the compromise. The estimated number of fault-tolerant qubits needed on a quantum computer to break the RSA and ECC cryptosystems are $2n + 2$ [11] and $6n$ [12] respectively, where n is the key size. This roughly translates to a 4,000+ qubit quantum computer to break an RSA-2048 application and a 1,500+ qubit quantum computer to break the ECC-256 application.
- *By the scope of break.* There is a difference when it comes to compromising RSA and ECC used in key exchange protocols. When RSA is used in TLS for key exchange, the same private RSA key is used repeatedly to decrypt different session keys for the lifetime of the RSA key. This means that an adversary can get access to all session keys once the common private RSA key is compromised by a quantum computer. On the other hand, ECC can be used with perfect-forward secrecy in TLS v1.3 where a different ECC key is used each time a session is established. This means that each

quantum computer cryptanalysis only reveals one session key, which is "annoying" to adversaries and limits the scope of the compromise. Such a difference does not exist for digital signature applications using RSA or ECC.

A result that we can derive from the above criteria is that adversaries will likely prioritize i) ECC-based digital signature applications, followed by ii) RSA-based digital signature & key exchange applications, followed by iii) ECC-based key exchange applications, and lastly iv) symmetric key and hash-based applications assuming the value of the targets are similar and the data prerequisites discussed in Section III-A can be met.

IV. IDENTIFYING ACTIVE INTERVENTIONS

In order to further increase their advantage, we expect some adversaries may choose to carry out active interventions to affect their targets' quantum roadmap. From a modelling perspective, Mosca [3] has prepared a quantum readiness metric which defines three parameters $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ as follows:

- $\mathcal{X}$ refers to the duration of time that the cryptographic secrets need to be kept secret.
- $\mathcal{Y}$ refers to the time needed to deploy tools that are quantum-secure.
- $\mathcal{Z}$ refers to the time duration before a quantum computer breaks the algorithm or reveals the secrets.

Mosca's theorem states that if $\mathcal{X} + \mathcal{Y} > \mathcal{Z}$, then the target should be worried about the vulnerability exposure. Mosca then attempts to assign absolute values to $\mathcal{Z}$, where he estimates a $\frac{1}{7}$ chance of RSA-2048 being broken in 2026, with the chance increasing to $\frac{1}{2}$ by 2031.

When using this model from an adversary's point of view, the difference of $(\mathcal{X} + \mathcal{Y}) - \mathcal{Z}$ represents the time advantage the adversary has on the target. The actions of adversaries can thus be classified into extending $\mathcal{X}$, extending $\mathcal{Y}$ and reducing $\mathcal{Z}$ as discussed below.

A. Extending $\mathcal{X}$

We need to first recognize that $\mathcal{X}$ is different depending on the threats posed:

- For **S**poofing, **D**enial-of-Service, and **E**levation of privilege, the value of $\mathcal{X}$ is

close to zero. This is because the duration in which authentication credentials need to be protected is only at the point of usage. If they have been compromised by quantum computers, the credentials just need to be changed to mitigate the threat. The only exception is biometric authentication credentials which cannot be easily changed.

- For **T**ampering and **R**epudiation, the value of $\mathcal{X}$ is the duration in which the information is relied on. If an agreement is tampered with or the origin of the agreement is cast into doubt only after the expiry of the agreement, the risk impact is minimized. We expect long-term contracts (extending for more than five years), financial records and audit logs to have the longest $\mathcal{X}$.
- For **I**nformation disclosure, the value of $\mathcal{X}$ may be exceedingly long since an adversary may still derive benefit from exposing such information long past the validity of the information. An example is wikileaks.org, whose published documents impacted the image and reputation of several persons and their positions, despite them no longer holding public office. In fact, it may be futile to migrate existing quantum-vulnerable encrypted data to quantum-secure encryption since multiple copies of the existing encrypted data may exist and remain vulnerable.

To the adversary, focusing on vulnerabilities related to **T**ampering **R**epudiation and **I**nformation disclosure has an effect of extending $\mathcal{X}$. The actions are similar to the data harvesting actions discussed in Section III-A.

B. Extending $\mathcal{Y}$

In examining $\mathcal{Y}$, we see that $\mathcal{Y}$ can be further broken down into three sub-components that require to run consecutively. We define them here as:

- $\mathcal{Y}_1$: Time needed to design / select a viable quantum-secure solution.
- $\mathcal{Y}_2$: Time needed to upgrade the application code and protocol to support the quantum-secure solution.
- $\mathcal{Y}_3$: Time needed to migrate the users, system, keys, data and processes to use the quantum-secure solution.

The National Institute of Science and Technology (NIST) is working with the industry on a post-quantum cryptography (PQC) standardization process. The process is to select asymmetric key algorithms both for key exchange, where a session key used for confidentiality is mutually established and for digital signing, where the integrity and non-repudiation of signed data are ensured. Now into the fourth round of evaluation [13], a total of one key-exchange and three digital signature algorithms have been selected for standardization. What remains is the selection of non-lattice key-exchange algorithms to complete the portfolio of general-purpose PQC algorithms. NIST expects the draft standards to be finalized by 2024. These coordinated efforts in evaluating each of the candidate algorithms and putting them through various evaluation criteria represent a top-down approach that directly impacts $\mathcal{Y}_1$ with identified preferences (e.g. drop-in replacement) that may help reduce the duration for $\mathcal{Y}_2$ for some applications.

In Table II, we take a bottom-up implementation approach and run through various actions that adversaries can take to affect $\mathcal{Y}$ and their potential impact.

Table II: Actions taken by Adversaries to affect $\mathcal{Y}$

Persona	Actions	Impact
Basic user	Provide inappropriate consulting and advice on how to do quantum migration. Affects $\mathcal{Y}_2$.	Low
Insider	Capture wrong system requirements or omit some systems, resulting in gaps and delays in the migration. Affects $\mathcal{Y}_3$.	Medium
Hacktivist	Drive the importance of other agenda to deflect focus from quantum migration. Affects $\mathcal{Y}_2$	Low
Cyber-criminal	Work with equipment vendors to deliver non-quantum-secure systems. Affects $\mathcal{Y}_2, \mathcal{Y}_3$.	High
Nation-state	Disrupt the post-quantum cryptography standardization process. Affects $\mathcal{Y}_1$	High

When evaluating the impact of the actions, we see that the *Cyber-criminal* and *Nation-state* can cause a systemic failure to quantum migration efforts across the industry while the actions by *Basic User*, *Insider* and *Hacktivist* are generally isolated to individual companies or organizations.

C. Reducing $\mathcal{Z}$

For the well-resourced *Nation-state*, they may be able to channel more money and engineers in speeding up research into building a cryptanalysis-capable quantum computer, thus actually reducing $\mathcal{Z}$.

For medium-resourced adversaries such as *Hacktivist* or *Cyber-criminal*, they may adopt a misinformation campaign instead to give the perception of either a shorter or longer $\mathcal{Z}$. If $\mathcal{Z}$ is perceived to arrive quicker, it may force targets to divert resources from the original quantum migration plans and adopt short-term parameter defences instead, thus delaying $\mathcal{Y}$. Separately, an illusion of a longer $\mathcal{Z}$ may loosen the targets' vigilance and inadvertently also lengthen $\mathcal{Y}$.

We do not expect the *Basic User* or *Insider* to impact $\mathcal{Z}$ in any meaningful way.

V. RECOMMENDATIONS AND NEXT STEPS

In this section, we use the analysis done in the earlier section to derive possible actions that can be taken to either mitigate the threats or reduce the adversaries' advantage. Considering that organizations may take several years of planning and execution to migrate cryptographic algorithms [14], we have categorized the recommendations (see Figure 3) into what an organization can start doing now versus what should be done within the next two to three years while awaiting NIST's post-quantum cryptographic standards to become established.

- To start now:
  - *Know your exposure*. Organizations should perform team-based threat modelling exercises [15] to understand their current risk and reduce exposure to insider threats. This will allow planning and allocation of resources and budget for quantum migration.
  - *Use quantum annoyance*. Begin the migration process by upgrading session encryption and other communications to use TLS v1.3 or other protocols which have perfect-forward secrecy to limit the scope of any possible compromise to within each session.
  - *Deter data harvesting*. In order to mitigate against data harvesting, use a minimum of a 256-bit symmetric encryption key, over and above existing security protection, to protect data and files in storage. This can be in the form of encrypted databases or encrypted storage devices that perform blanket encryption of all data.
- To do over the next two to three years:
  - *Update organizational practices*. Increase organizational awareness of potential quantum threats and start to include quantum-secure compliance or requirements into procurement and implementation practices.
  - *Prioritize integrity and non-repudiation*. Based on our adversarial model, the first threats to be mitigated are tampering and repudiation. Long-dated documents, contracts, logs and other data should be time-stamped with a quantum-secure mechanism prior to the availability of cryptanalysis-capable quantum computers to ensure their integrity and non-repudiation status. Such mechanisms include using blockchains, time-stamping digital signatures that are quantum-secure [16] or using stateful hash-based signature scheme [17] by NIST.
  - *Strengthen password authentication*. Despite many issues related to users' passwords being phished, passwords as an authentication mechanism are relatively resistant to quantum cryptanalysis as compared to ECC or RSA-based authentication. Critical systems should have multi-factor authentication implemented where one of the factors is password authentication with password entropy of up to 256-bits to ensure authentication remains secure.

For combating more broad-based threats such as misinformation and the emergence of data marketplaces/brokers, this work is beyond the scope of a single organization.

When comparing with other relevant works [13], [18], we adopt a broader perspective to dispel the notion that quantum computers simply pose a cryptographic threat and that a replacement of algorithms would address the problem. This is similarly echoed by Mashatan and Turetken [19]. We also note that our recommendations are more comprehensive as compared to the infographic guide [20] prepared by the Department of Homeland Security. More work still needs to be done to
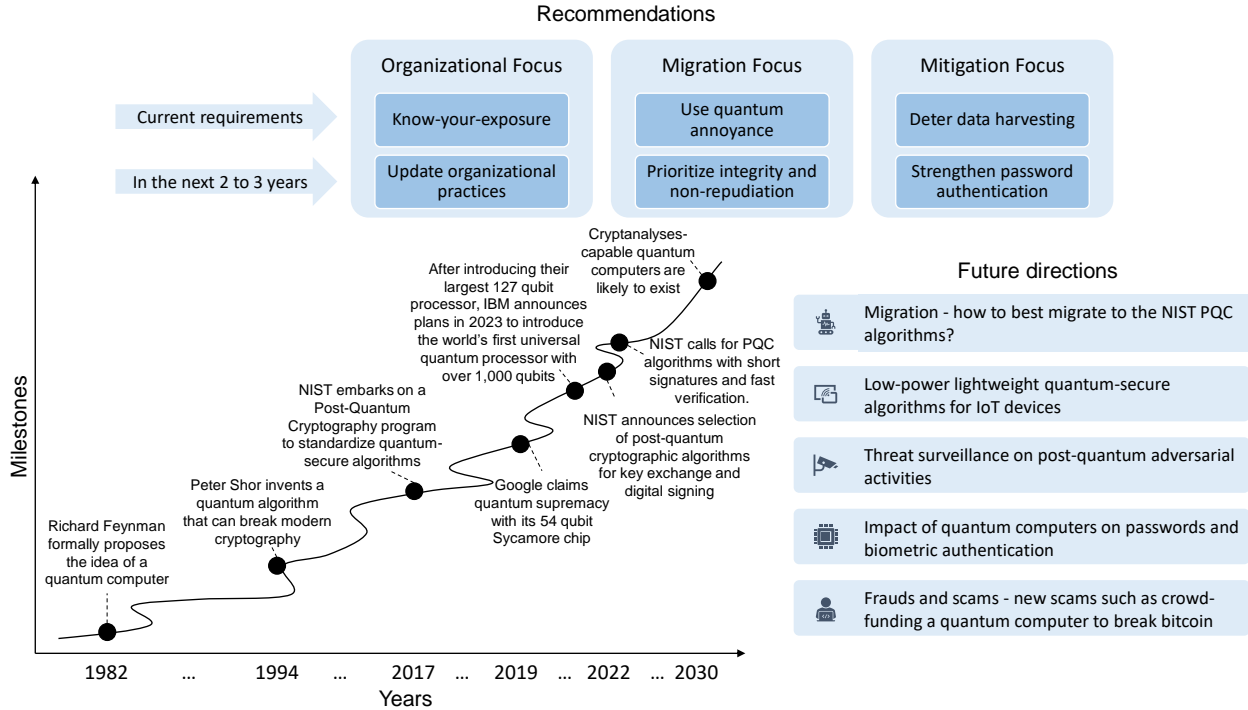
Figure 3: An illustration of the milestones for Quantum-research, recommendations, and future directions.

prepare for quantum readiness. We have highlighted the timeline and future directions in Figure 3. Besides looking for an appropriate replacement cryptographic algorithm to RSA and ECC, work must now focus on how these algorithms can be properly migrated to, and how other applications such as IoT devices and biometric authentication may need different algorithms. This direction is clearly demonstrated by NIST who has started a new call for a specific PQC algorithm with short signatures and fast verification, soon after announcing the general-purpose PQC algorithms for standardization. Developing possible frameworks on how the industry can establish additional norms in transparent surveillance and coordinated responses to deny adversaries any advantage is the crucial future direction of this study.

VI. CONCLUSION

Tracing the quantum timeline, it has been almost 40 years since the idea of a quantum computer was floated. The industry's developments in the past few years in achieving quantum supremacy are nothing short of awe. While we look forward to breakthroughs facilitated by the power of quantum computing, we are mindful of the security and privacy threats that quantum computers pose. Adversaries are not sitting on their hands, and we highlight various approaches and scenarios where they can already gain an advantage. We have provided recommendations and included additional areas where research work is needed to close the gap.

REFERENCES

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[2] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Physical review letters*, vol. 79, no. 2, p. 325, 1997.

[3] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.

[4] G. F. Hurlburt, "The tyranny of urgency," *Computer*, vol. 52, no. 6, pp. 68–72, 2019.

[5] C. C. McGeoch, R. Harris, S. P. Reinhardt, and P. I. Bunyk, "Practical annealing-based quantum computing," *Computer*, vol. 52, no. 6, pp. 38–46, 2019.

[6] M. Roetteler and K. M. Svore, "Quantum computing: Codebreaking and beyond," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 22–36, 2018.

[7] T. Humble, "Consumer applications of quantum computing: A promising approach for secure computation, trusted data storage, and efficient applications," *IEEE Consumer Electronics Magazine*, vol. 7, no. 6, pp. 8–14, 2018.

[8] L. Kohnfelder and P. Garg, "The threats to our products," 1999. Online: https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx [accessed: August 2022].

[9] M. Rocchetto and N. O. Tippenhauer, "On attacker models and profiles for cyber-physical systems," in *European Symposium on Research in Computer Security*, pp. 427–449, Springer, 2016.

[10] Mashatan, Atefeh and Heintzman, Douglas, "The complex path to quantum resistance," *Communications of the ACM*, vol. 64, no. 9, pp. 46–53, 2021.

[11] Y. Takahashi and N. Kunihiro, "A quantum circuit for shor's factoring algorithm using 2n+2 qubits," *Quantum Information & Computation*, vol. 6, no. 2, pp. 184–192, 2006.

[12] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," *arXiv preprint quant-ph/0301141*, 2003.

[13] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, C. Miller, D. Moody, R. Peralta, *et al.*, "Status report on the third round of the nist post-quantum cryptography standardization process," tech. rep., National Institute of Standards and Technology Gaithersburg, MD, 2022.

[14] Gardiner, Michael and Truskovsky, Alexander and Neville-Neil, George and Mashatan, Atefeh, "Quantum-safe trust for vehicles: The race is already on," *Communications of the ACM*, vol. 64, no. 9, pp. 54–61, 2021.

[15] C. C. Lee, T. G. Tan, V. Sharma, and J. Zhou, "Quantum computing threat modelling on a generic cps setup," in *International Conference on Applied Cryptography and Network Security*, pp. 171–190, Springer, 2021.

[16] T. G. Tan and J. Zhou, "Layering quantum-resistance into classical digital signature algorithms," in *Proceedings of 24th International Security Conference (ISC 2021)*, Springer, 2021.

[17] Cooper, David A and Apon, Daniel C and Dang, Quynh H and Davidson, Michael S and Dworkin, Morris J and Miller, Carl A, "Recommendation for stateful hash-based signature schemes," *NIST Special Publication 800-208*, 2020.

[18] G. Mone, "The quantum threat," *Communications of the ACM*, vol. 63, no. 7, pp. 12–14, 2020.

[19] Mashatan, Atefeh and Turetken, Ozgur, "Preparing for the Information Security Threat from Quantum Computers.," *MIS Quarterly Executive*, vol. 19, no. 2, 2020.

[20] DHS, "Preparing for post-quantum cryptography," *Online: https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf [accessed: August 2022]*, 2021.

ABOUT THE AUTHORS

Teik Guan Tan (Member, IEEE) completed the PhD in Cybersecurity at the Singapore University of Technology and Design (SUTD), Singapore. His research interests are in the intersection of authentication, applied cryptography and Quantum algorithms. He has co-founded a cybersecurity startup focused on post-quantum security. Contact him at: teikguan@pqcee.com

Jianying Zhou (Senior Member, IEEE) is a professor and co-center director for iTrust at Singapore University of Technology and Design (SUTD). He received the PhD in Information Security from Royal Holloway, University of London. His research interests are in applied cryptography and network security, cyber-physical system security, mobile and wireless security. Contact him at: jianying_zhou@sutd.edu.sg

Vishal Sharma (Senior Member, IEEE) is an Assistant Professor in the School of Electronics, Electrical Engineering and Computer Science (EEECS) at the Queen's University Belfast (QUB), NI, United Kingdom. He received the PhD in Computer Science and Engineering from Thapar University (2016). His areas of research and interests are Autonomous Systems, UAV Communications, Network Behavior Modeling, 5G and Beyond, Blockchain, and CPS-IoT. Contact him at: v.sharma@qub.ac.uk

Saraju P. Mohanty (Senior Member, IEEE) is a Professor in the Department of Computer Science and Engineering (CSE), University of North Texas (UNT), Denton, TX, USA. He received the Ph.D. degree in Computer Science and Engineering from the University of South Florida, Tampa, in 2003. His research is in "Smart Electronic Systems" which has been funded by National Science Foundations (NSF), Semiconductor Research Corporation (SRC), U.S. Air Force, IUSSTF, and Mission Innovation. Contact him at Saraju.Mohanty@unt.edu.