Aum Amriteswaryai Namah

Perspectives on Post Quantum Cryptography Migration and Cryptographic Agility

Presented by

Dr. Prabhakar Krishnan
Research Scientist

kprabhakar@am.amrita.edu

AMRITA CENTER FOR CYBER SECURITY SYSTEMS & NETWORKS

Research in Quantum Technologies

Quantum Information: Theory and Applications

Quantum Computing

Quantum Communication

Quantum Security: PQC, QKD, Crypto-Agility

Outline

Post Quantum Security

Post Quantum Cryptography Migration

A New Science of Cryptographic Agility

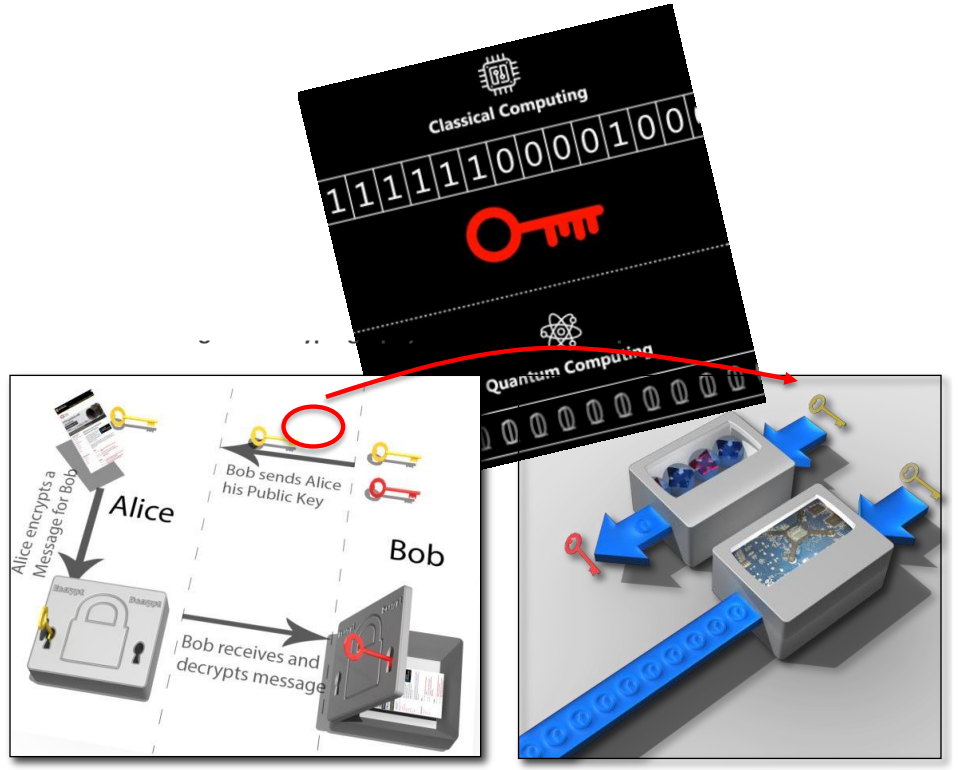
New Frontiers of Cryptography

Concluding Remarks

Future Quantum Computers are a Threat Today

Even if a cryptographically-relevant quantum computer is a decade away...

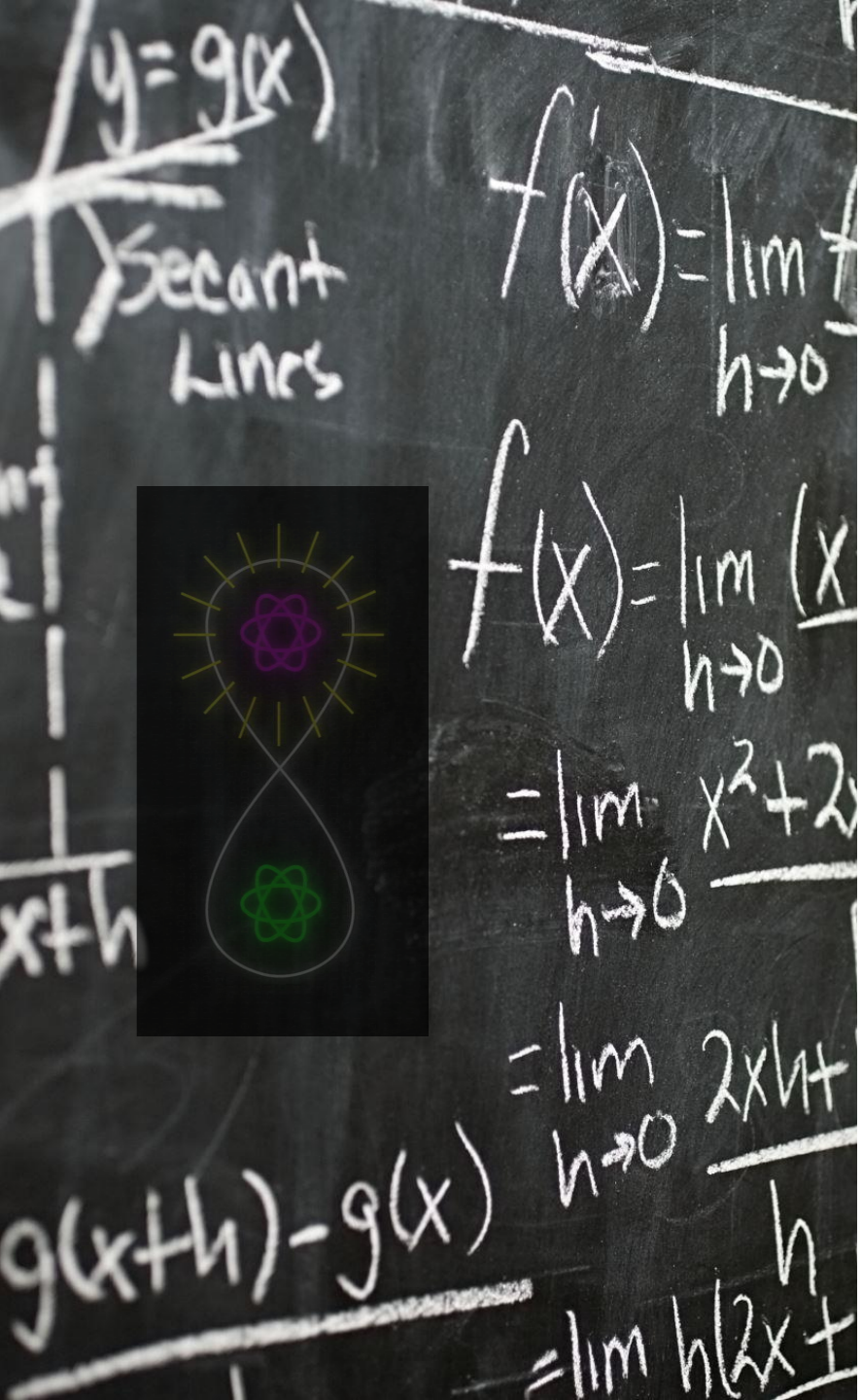
- "Record now, Exploit later" attack
- Today's non-PQ encryption will break in the future
- What is the security life of the data you and your customers transmit and store?
- Authentication, code-signing, and digital signatures
- If I can break the algorithm and determine the private key, I can impersonate, for e.g, the *Windows Update* channel
- What happens if an adversary can "update" the firmware on your processor?



A – Eavesdropper obtains public key from public channel

B – Quantum computer can break security by reverse computing private key faster than a conventional computer

We're creating more legacy every day!



Post-Quantum Security

Two Fundamental Techniques to implement Post-Quantum Security:

➢Post-Quantum-Cryptography (PQC)
This is based on hard problems in Mathematics.

➢Quantum-Key-Distribution (QKD)
This is based on the fundamentals of Quantum Physics.

Each of these techniques has its advantages as well as disadvantages.

PQC-based technique of Post-Quantum Security

Advantages

➢Minimal or No Hardware Changes are required.

- All or most changes can usually be implemented in Software only
- Less costly, easy to implement, and easy to deploy
- Time-effective & Suitable for deployment in legacy as well as green-field projects

Disadvantages

➢There are multiple categories of PQC algorithms under standardization and within each category, there are multiple algorithms

➢PQC algorithms are based on hard maths problems and as on date, regress cryptographic security proofs do not exist of most algorithms

QKD-based technique of Post-Quantum Security

Advantages

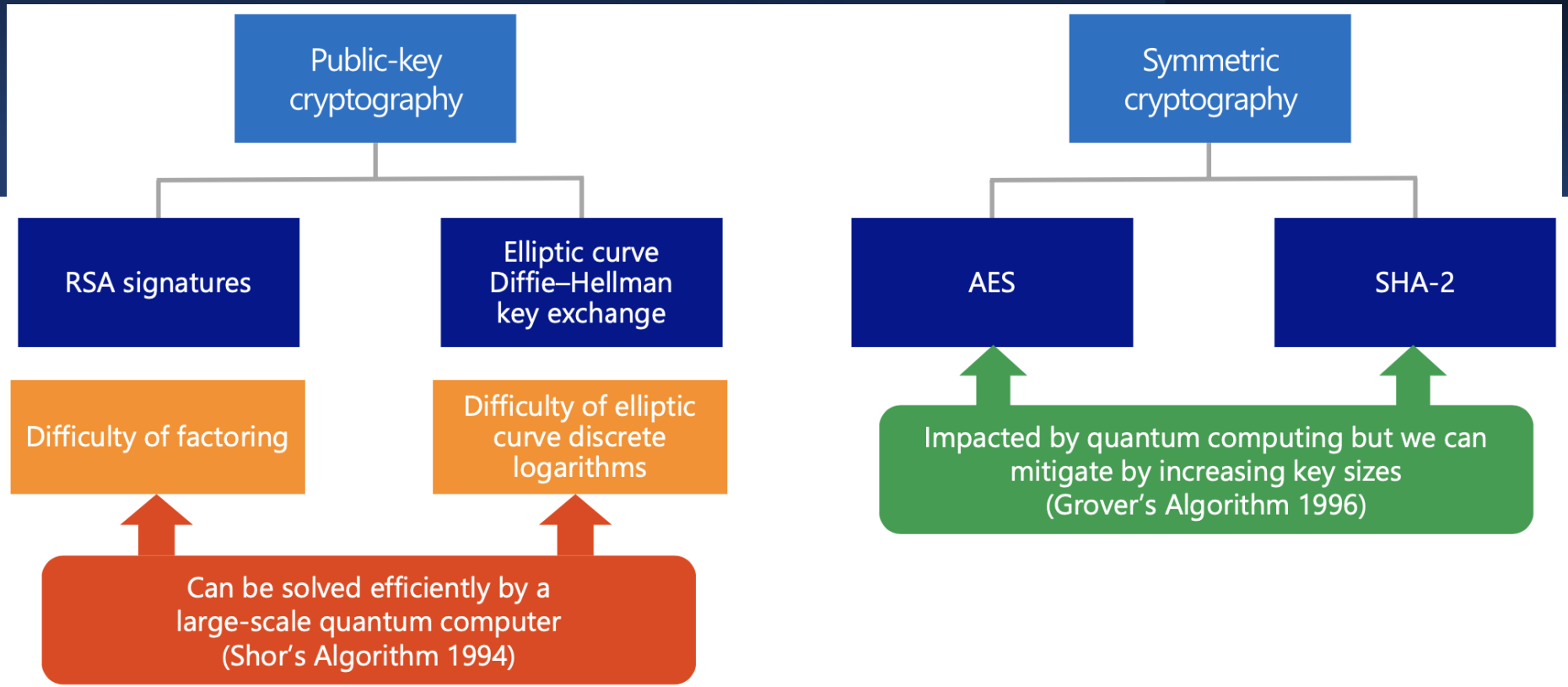
QKD is fundamentally based on a quantum channel, so more secure than the PQC-based technique

- It may be more secure than the PQC-based technique in a long-run

Disadvantages

- QKD-based technique requires extensive changes in Hardware
- QKD is more suitable for deployment in greenfield Projects
- Because of the costly components involved, QKD deployment is much more expensive than the PQC solution
- More time is required for QKD implementation as well as deployment

Contemporary → Quantum Cryptography



Quantum Cryptography:

- ✓ Uses quantum physics to achieve higher security
- ✗ Requires quantum infrastructure
- ✗ Restricted to Key Exchange (e.g., [BB84])
- ✗ No standards

Post-Quantum Cryptography:

- ✓ Based on harder math problems
- ✓ Can be implemented in current infrastructure
- ✓ Offers all required features
- ⚠ Standards under development

Achieving Post-Quantum Security - Challenges

- Challenge 1

Which of the two fundamental techniques?

QKD or PQC

- Challenge 2

If PQC is selected, which category? Which algorithm?

- Challenge 3

Legacy IP Networks carry live traffic, so downtime during migration has to be minimal and time-effective. How?

- Challenge 4

Legacy IP Networks have very Limited Budgets available for Support and Enhancements. Hence, Quantum-safe migration must be viable.

- Challenge 5

Many stakeholders managing Legacy IP networks believe that the threat from Quantum computers is not immediate, so they do not want to invest immediately in Quantum-safe migration.

- Challenge 6

What can be an optimal transition strategy for Quantum-safe migration? – investment can gradually increase as the threat perception increases.

PQC transition is an unprecedented move

Standards are being defined at the same time cryptanalysis is being understood

Industry perspective is critical for wide adoption.

Credits: https://www.yahoo.com/news/team-saudis-change-tires-while-vehicle-motion-video-120039718.html

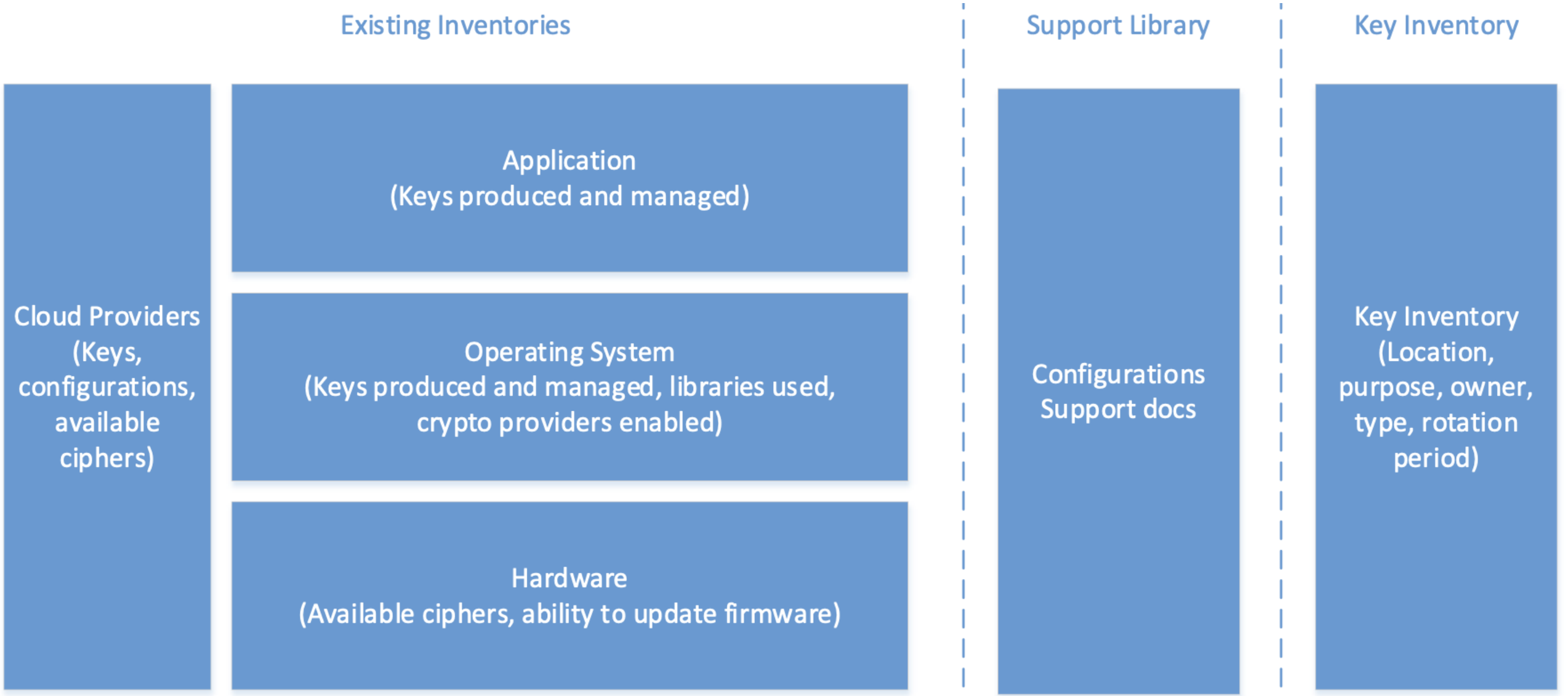
Post-Quantum Crypto literature may not offer drop-in replacements for all features.

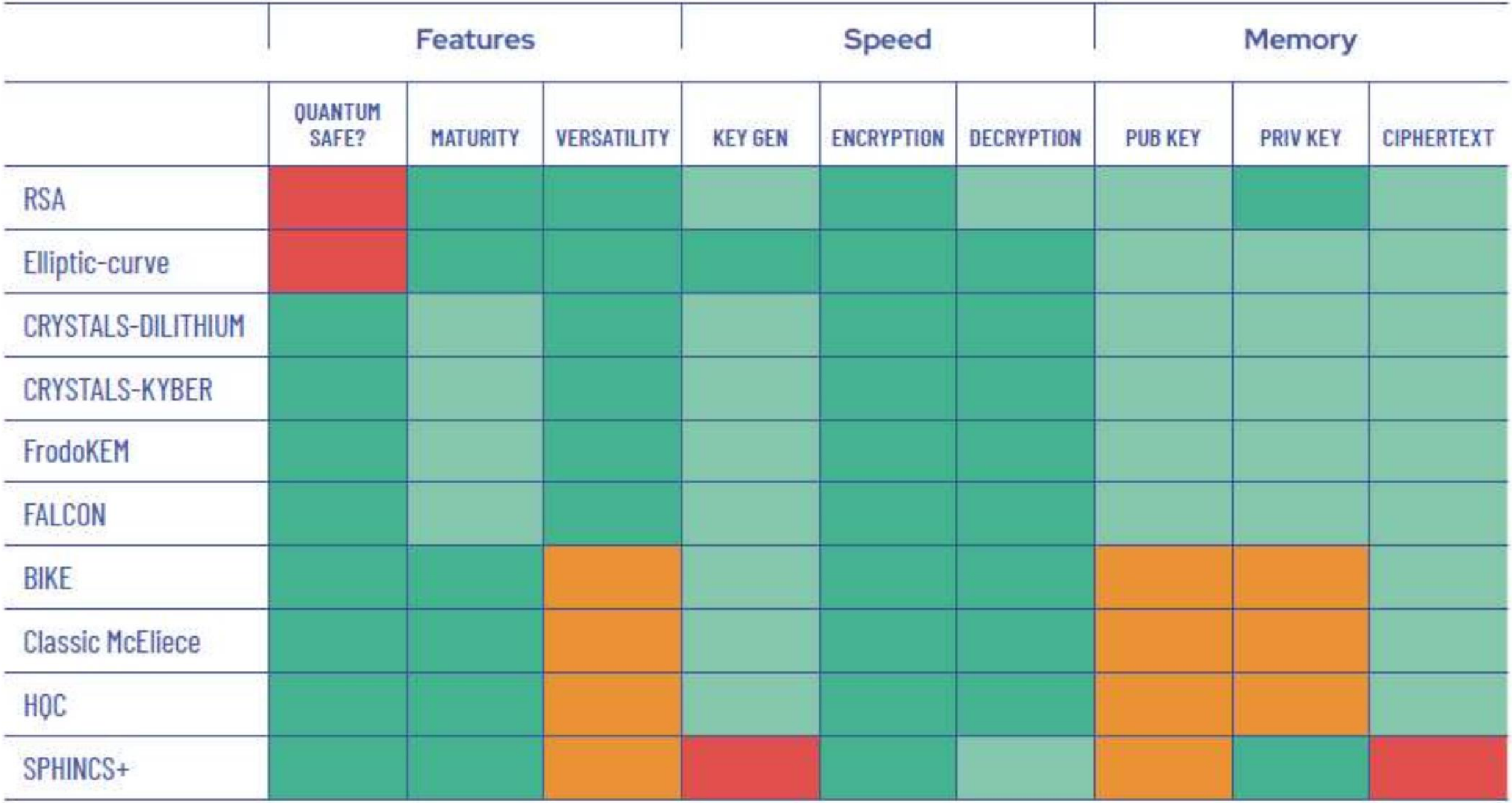
Simple & well-understood

is better than

complex & less-understood

Holistic inventory of Cryptographic assets





From the "THE PQC MIGRATION HANDBOOK " (ETSI)

Transitioning to PQC Algorithms
Performance Considerations

Multiple research efforts deal with the performance of PQC algorithms, focusing on algorithmic complexity, hardware implementations, and network performance.

Algorithm Performance: Regarding execution times, memory usage, power consumption, and speed. PQC algorithms generally have greater computation, memory, storage, and communication requirements (e.g., larger key sizes, more complex algorithms, or both)

Hardware Performance: Implementing PQC algorithms on special hardware and IoT devices,

Network Performance: With larger signatures and keys, more data must be transferred within networks. Packetization and latency patterns within secure communication protocols like TLS. Impacts a spectrum of network-related devices optimized for our current protocols – from network routers and switches to gateway devices, network appliances (e.g., firewalls, intrusion detection systems, WAN accelerators), and content distribution schemes.

How will packetization considerations impact network function virtualization in 5G cellular networks?

What are the implications of new PQC communication patterns for end-user devices like smartphones or applications like web browsers?

Transitioning to PQC Algorithms
Security Considerations

In contrast to well-understood RSA and ECC algorithms, less-understood PQC candidates have different trade-offs in configurable parameters.

- Specific algorithms add new “knobs”; for instance, dimensions in lattice schemes or code length and dimensions in code-based schemes (e.g., Classic McEliece).
- Understanding the trade-offs between security and algorithm requirements for various usage domains is a key challenge. These trade-offs are unlikely to be addressed fully by NIST, which cannot consider all contexts of PQC algorithm usage.
- While NIST will standardize schemes with specific parameter settings, guidelines on selecting algorithms among multiple options and security levels for specific usage contexts will be needed.

Transitioning to PQC Algorithms
Implementation Considerations

Implementing cryptography, whether in software or hardware, is more difficult than it appears.

- The complexity of mathematical algorithms, a common source of errors, reflects the difficulty in translating mathematical algorithms to platform-specific architectures and device contexts.

  For example, the details of data representation and layout, and its interactions with a system's memory hierarchy and operating system buffering mechanisms, can introduce vulnerabilities not apparent within cryptographic algorithm design across a broad range of devices, computer architectures, system software stacks, and programming languages.

- Devices in the embedded domain are constrained in memory size, compute resources, and power availability since battery lifetimes are finite. PQC implementations are needed to understand how specific algorithms can navigate such constraints and how hardware-software boundaries should be defined.

  How can implementations help to guard against adversarial tampering and side-channel attacks? Which PQC approaches and parameter choices are well- or poorly matched with devices in this domain?

Transitioning to PQC Algorithms
Implications Across Domains

The space of cryptography usage domains can also be looked at in a deployment platform- and/or application-centric way,

- ❑ The most obvious increase in key, ciphertext, and signature sizes which many of our current usage domains are not prepared to accommodate.
- ❑ Additional resource requirements impact implementation strategies, performance, system buffering dynamics, communication patterns, and side-channel vulnerabilities.
- ❑ PQC's new requirements: state management (hash-based signatures), auxiliary functions (e.g., Gaussian sampling in lattices), entropy (e.g., lattice-based schemes), and nonzero decryption failure probabilities (e.g., code-based encryptions schemes).

How these considerations play out for various cryptography implementation, and application domains represents a large open space of much-needed research.

USAGE DOMAINS

secure communication protocols
(e.g., TLS, SSH, IPSec),
digital signature schemes,
public key infrastructure (PKI),
authentication protocols,
identity and access management
key management systems.

DEPLOYMENT PLATFORMS

web-based computing
mobile computing
Internet of things (IoT)
Edge computing,
Public, Private, hybrid clouds
Virtual Private Networks
Trusted computing architectures

Migration Frameworks: How will we get there?

- ***Hybrid Schemes:*** *T*wo cryptographic algorithms are applied, one from our current canon of standards (e.g., RSA or ECC) and one from the newer array of PQC alternatives (e.g., lattices). Hash combiners construct a new hash function from two component hash functions and exhibit robust security if at least one is secure. Encryption combiners, used with identity-based encryption schemes, take public keys from component encryption schemes and create a combined public key—cipher suite negotiation as seen in IETF protocols like TLS.
- ***Formal Modelling:*** *formal modeling of cryptographic migration* schemes, whether hybrid or combiner-based, negotiation-based, or examining the security of inserting migration frameworks into common cryptographic protocols. What attack surfaces are associated with specific hybrid instantiations for key encapsulation mechanisms, encryption schemes, and digital signatures? What do formal models tell us about the level of security for common misuses or flawed implementations? How are adversaries to be modeled under a variety of assumptions?
- ***Automated Tools:*** *D*evelop active and passive approaches to scanning infrastructure and provide an analysis of legacy cryptography usage based on network traffic, open ports, end-user devices, system binaries, source code repositories, and more. Trace dependencies, identify runtime control flow, probe for common vulnerabilities, and verify the security of new PQC libraries and migration mechanisms.
- ***Complex Infrastructures:*** understanding PQC migration challenges in complex computing infrastructures like private data centers, public cloud, hybrid and federated architectures, edge computing, smart home or building environments, and more. Such infrastructures exhibit architectural complexity, deepen the layering of our system software stacks, and add heterogeneity.

Workstreams in PQC Transition

Three Parallel Workstreams are active in the PQC Transition.

- Algorithms: Selections (“winners”) of the NIST PQC Standardization process
- Protocols: “PQC-enable” protocols by adding NIST-selected algorithms
- Systems: PQC support to PKI/Cas, HSMs, and other engineering processes.

Crypto-agile PQC Libraries Exist Today- Open Quantum Safe (OQS) group

- PQC and hybrid cipher suites
- Hybrid: keep your FIPS or otherwise approved crypto, add PQ protection
- OpenSSL, with TLS 1.2 and 1.3 support, OpenSSH
- OpenVPN: For securing links against “record now/exploit later” attacks.
- X.509v3 Hybrid Certs (RSA/ECDSA)-PQ certificates with new signature OID

Key findings for PQC migration

- No candidate has everything we want. Nothing works as well as RLWE Key Exchange. All involve trade-offs (*Confidence in Security* Vs. *Ease of Deployment* Vs *Performance*)
- Parameter selection and final tweaks to the algorithms are still being considered.
- Need more security analysis, especially for parameter selection. Longer keys and signatures are relatively acceptable.
- Custom modifications to protocols to integrate PQC could introduce flaws and may result in interoperability challenges with future deployments.
- If the PQC algorithm has a flaw, then a hybrid scheme does not guarantee post-quantum security.
- Hybrid PQC may allow communications to satisfy both policies. Hybrid Key Exchange (protects against "store now and harvest later" and FIPS compliant). Hybrid Signatures have different pros and cons.
- Size constraints: Unexpected bugs due to larger public keys/ciphertexts/signatures
- Memory constraints: Large stack usage problematic in multi-threaded software
- PQC overhead can be amortized over long tunnel lifetimes.

Key findings for PQC migration

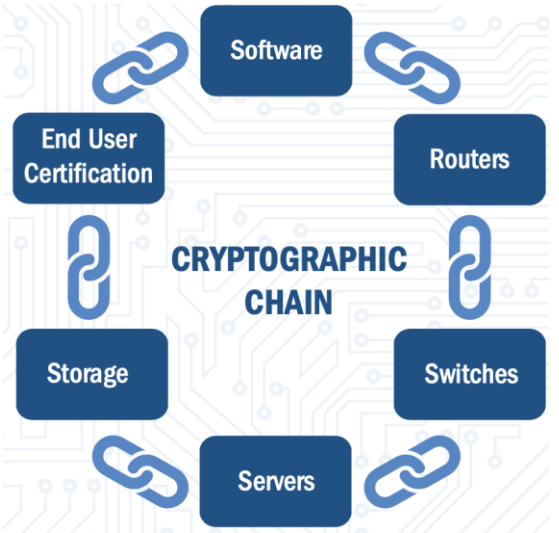
- API Problems: NIST competition focuses on Key Encapsulation Mechanisms, but some cryptographic APIs lack abstractions for KEMs (e.g., OpenSSL EVP API)
- Versioning difficulties: While NIST competition is still in progress, algorithm specifications continue to change. Interoperability and algorithm versioning is hard.
- Bigger PQ public key, ciphertext, and signature sizes can lead to extra round-trips due to the TCP Initial Congestion Window and a slowdown in lossy environments.
- Web: PKI, OCSP, and SCT signatures increase the transferred handshake data even more.
- "*Keygen, encaps, decaps, sign, verify*" performance is important for "fast and short," high-volume connection applications.
- The migration of long-lived Hardware Roots of Trust is more urgent.
- (D)TLS, SSH, IKEv2: Some lattice schemes perform acceptably compared to classical algorithms.
- Software Signing, Secure Boot: HBS signatures (Stateful & Stateless (SPHINCS+)) perform OK.
- Use small signature size schemes (e.g., Rainbow) where public keys are not transferred (e.g., Root CA cert, SCTs in TLS)

A New Science of Cryptographic Agility

- ❑ Cryptographic agility is the ability of a system to adopt alternatives to the cryptographic primitives easily.
- ❑ Many information systems cannot adopt new cryptographic algorithms without costly and time-consuming changes to hardware and infrastructure.
- ❑ A design feature and principle enables future cryptographic algorithms and standards updates without modifying or replacing the surrounding infrastructure.
- ✓ The entire software stack is easy to swap cryptographic primitives.
- ✓ Increase diversity of cryptosystems (reduce the probability of related breaks.)
- ✓ Maintain an inventory of the devices accessing your network + Automate cryptographic inventories and updates.

Crypto Agility (CA) Scope

Algorithm (e.g., key encapsulation mechanisms),
Program code (e.g., an authentication function)
Protocol module (e.g., TLS),
Application (e.g., an email or web server),
Service (e.g., an online banking portal),
System (e.g., an operating system or IoT device),
Computing infrastructure (e.g., an enterprise),
Cloud hosting (e.g., public and/or private cloud),
Complex vertical domain (e.g., a smart building)?

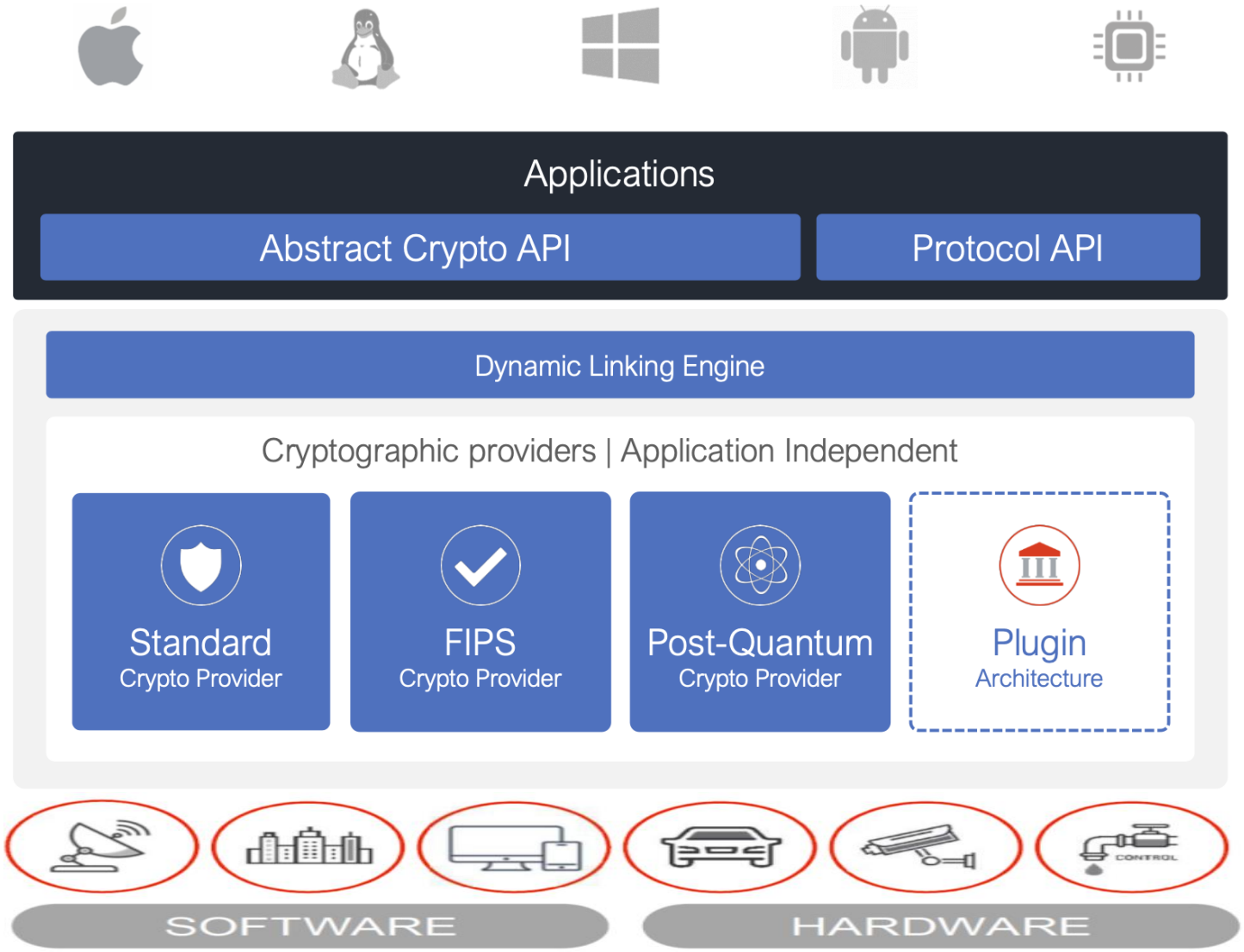


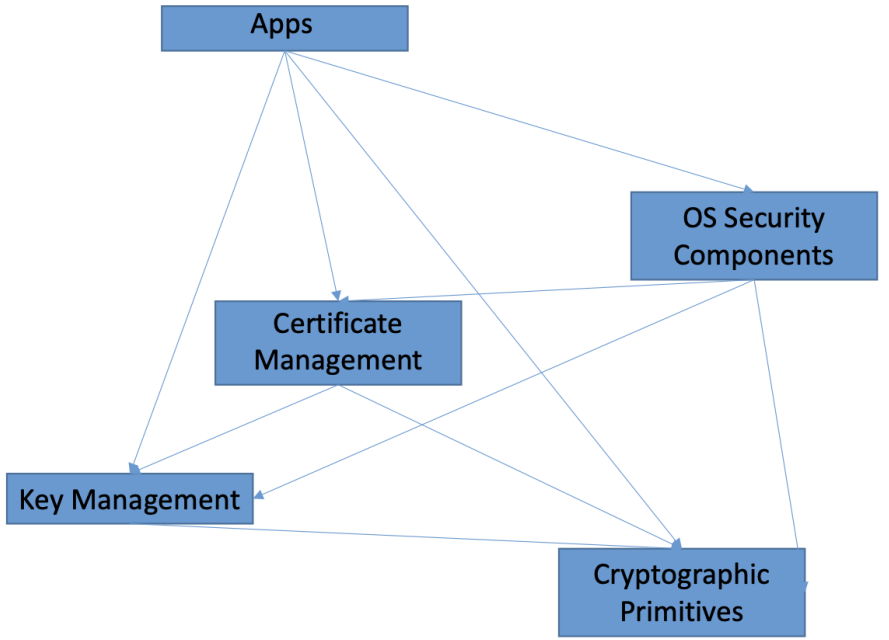
Need for Cryptographic Agility

Modern Cryptography	Platform Optimized Cryptography	FIPS Certified Crypto	Custom Crypto Integration
Use modern, resilient and clean crypto implementation	Implement dedicated algorithms, counter measures or optimizations	Certify specific platform for use in government	Allow end-user to select crypto to use in their systems

Post-Quantum Readiness	In Field Crypto Update	Sovereign Crypto Program	Future Cryptography
Swap to post-quantum crypto standards as soon as available	Update crypto foundation of systems running in the field	Deploy National Crypto Program	Prepare systems for future standards

Crypto Agile Architecture





Every level of this software stack:

- Can call into every layer below it.
- abstracts the underlying algorithms, including parameters such as key, signature, or ciphertext length.

Key findings for cryptographic agility

- There is a need to broaden and recast traditional notions of cryptographic agility in light of the size and complexity of global PQC migration.
- cryptographic agility should include an expanded set of goals, a set of compute domains, a broader range of modalities and time scales, and the full canon of security research methodologies.
- Research should include frameworks and architectures enabling agility across various compute contexts, usable interfaces addressing various user roles, and understanding security and complexity trade-offs.
- Context agility, or cryptographic frameworks that automatically select among algorithms and configurations based on the user context.
- It enables change in response to evolving security policy within an organization.
- In the context of PQC, it enables agility across multiple standards likely approved by NIST.
- Cryptographic agility, independent of PQC migration, makes security systems more robust against algorithmic breakthroughs, implementation flaws, emerging hardware accelerators, and other threats.

New Frontiers of Cryptography

- ***Secure Multi-Party Computation (MPC):*** *P*rivacy-preserving computation enables multiple parties to jointly compute the output of a function over private data sets in a way that maintains the secrecy of input data.
- ***Identity-based Encryption / Attribute-based Encryption (IBE/ABE)****: A* message is encrypted using a set of attributes and can be decrypted only by a user who holds the private key matching the attribute formula.
- ***Fully Homomorphic Encryption (FHE)****:* protects the privacy of data by enabling computation directly on ciphertexts allowing, for example, private data to be outsourced for processing.
- ***Blockchain***: offers an approach to implementing an immutable and distributed digital ledger, characteristically with no central repository and no central authority. Uses cryptographic hashing and public key cryptography.
- ***Password-authenticated Key Agreement (PAKE)****.* enables interacting parties to authenticate each other and derive a shared cryptographic key using one or more party's knowledge of a password.
- ***Threshold Cryptography:*** a private key is split and shared across multiple parties who can reconstruct the key from a threshold number of participants who must cooperate to decrypt a message.

One key question is how PQC migration and cryptographic agility apply to each approach.

For example, how might cryptographic agility be added to blockchains not designed for it? How will blockchain implementations navigate migration from RSA- based signatures, DSA, and ECDSA to PQC alternatives?

Concluding Remarks

Even if you don't believe Quantum Computation will ever become a reality, there are benefits to implementing and deploying post-quantum algorithms now.

- Obvious benefits of migrating to post-quantum crypto: Potentially small probability but very high payoff.
- Cryptographic Agility – across the software stack, seamless, less disruptive crypto upgrades/updates Increase the diversity of cryptosystems.
- Past Algorithm Transitions Have Taken Years PQC Will Be No Different
  - ECC: proposed by mid-1980's + 2 decades to gain some adoption
  - AES: 4 years of competition + more than a decade to gain wide adoption
  - SHA-3: 5 years of competition + 6 years since publication. No wide adoption (yet?)
- Implementing only a PQC-based technique currently and keeping a provision for using a QKD-based approach will be a future-proof solution for the Quantum-safe migration of Legacy IP Networks.
- Implementing multiple under-standardization PQC algorithms and Selecting a suitable post-quantum hybrid scheme (algorithms, hybrid schemes, KEM combiners, etc.) will provide the way forward.

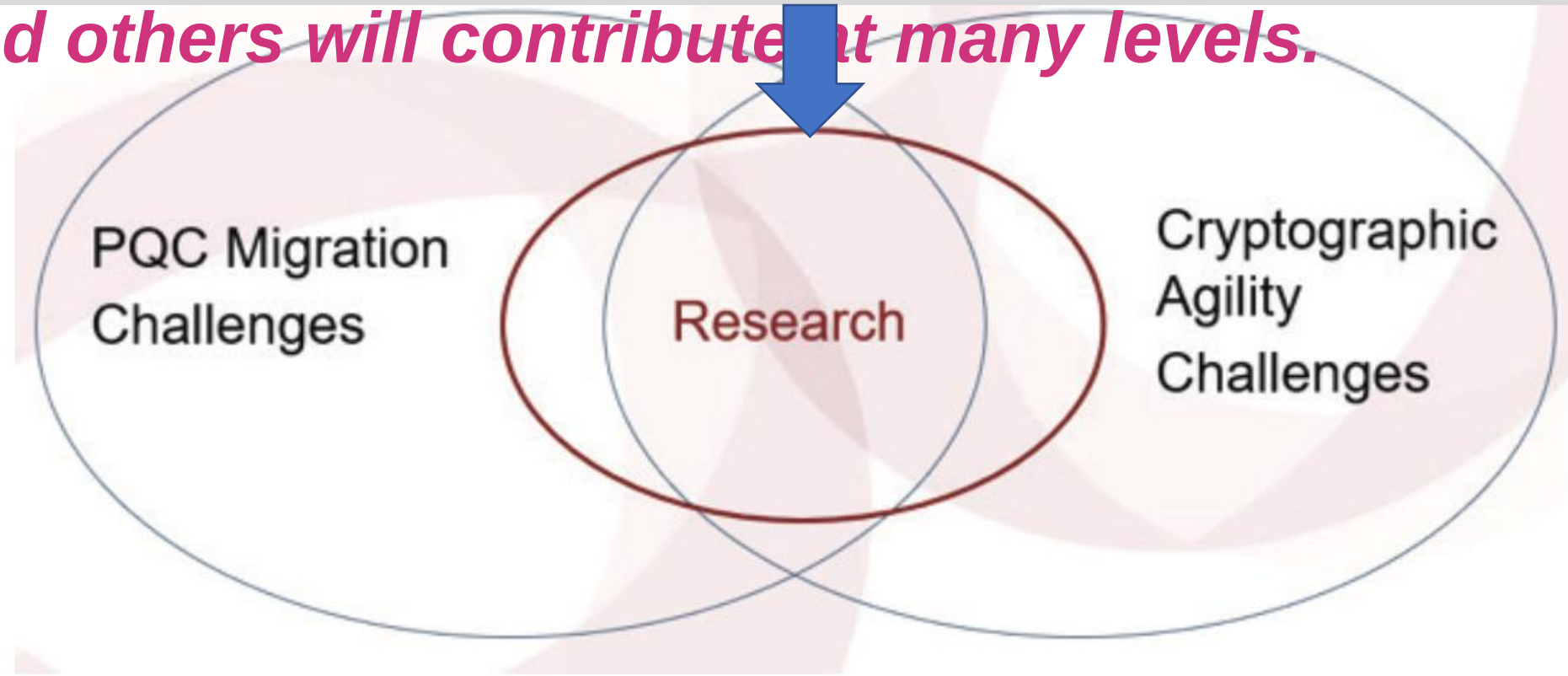
Concluding Remarks

- NIST standardization needs to finish. Other standards (IETF, IEEE) must work in parallel. Experimentation and public discussions have to reach a consensus soon.
- Research on policy, process, and people is needed since these determine whether and when PQC adoption occurs.
- Research is needed on the new frontiers of cryptography with respect to extending the PQ techniques.
- Steps to take now
  - ✓ Start building an inventory of your uses of cryptography and deployed implementations.
  - ✓ Identify top candidates to move to PQC first and begin planning/prototyping.
  - ✓ Ensure cryptographic agility (and support for new PQC algorithms) is part of everything you build
  - ✓ Temporary options for some use cases (e.g., RFC8784, RFC8696)

As quantum computing continues to make advancements in qubit technologies -->

scaling architectures, algorithms, applications, software tools, and more simultaneously fuels the urgency for a major transition in cryptography across the Internet as we know it today.

Software solution providers, hardware vendors, government standards bodies, international consortiums, the open-source developer community, and others will contribute at many levels.



Thank You