IBM Security

IBM - Workshop #3 : Securing in the Quantum Frontier

Dr. Walid Rjaibi
CTO & DE for Data Security
IBM Security
wrjaibi@ca.ibm.com

October 26, 2023

Quantum Computing

- Exploits quantum mechanics to process information using quantum bits - **qubits**

- Classical computing bits can only be 1 or 0, at any given time, while qubits can be a combination of 1 and 0 simultaneously (**superposition**)

- Qubits can also be **entangled**, meaning that the state of one qubit can be correlated with another qubit

- Computes much faster than classical computers, leveraging **superposition** and **entanglement**

- Promises to enhance many fields including Medicine, Space Exploration, and AI

Sample Quantum Computing Use Cases for Medicine

Diagnostic Assistance

Quantum Machine Learning has the potential to enhance:

- **Cell Classification** based on their many physical and biochemical characteristics (large feature space)
- **Biomarkers Discovery** may require analysis of complete data sets such as genomics, transcriptomics, proteomics and metabolomics (large feature space)

Precision Medicine

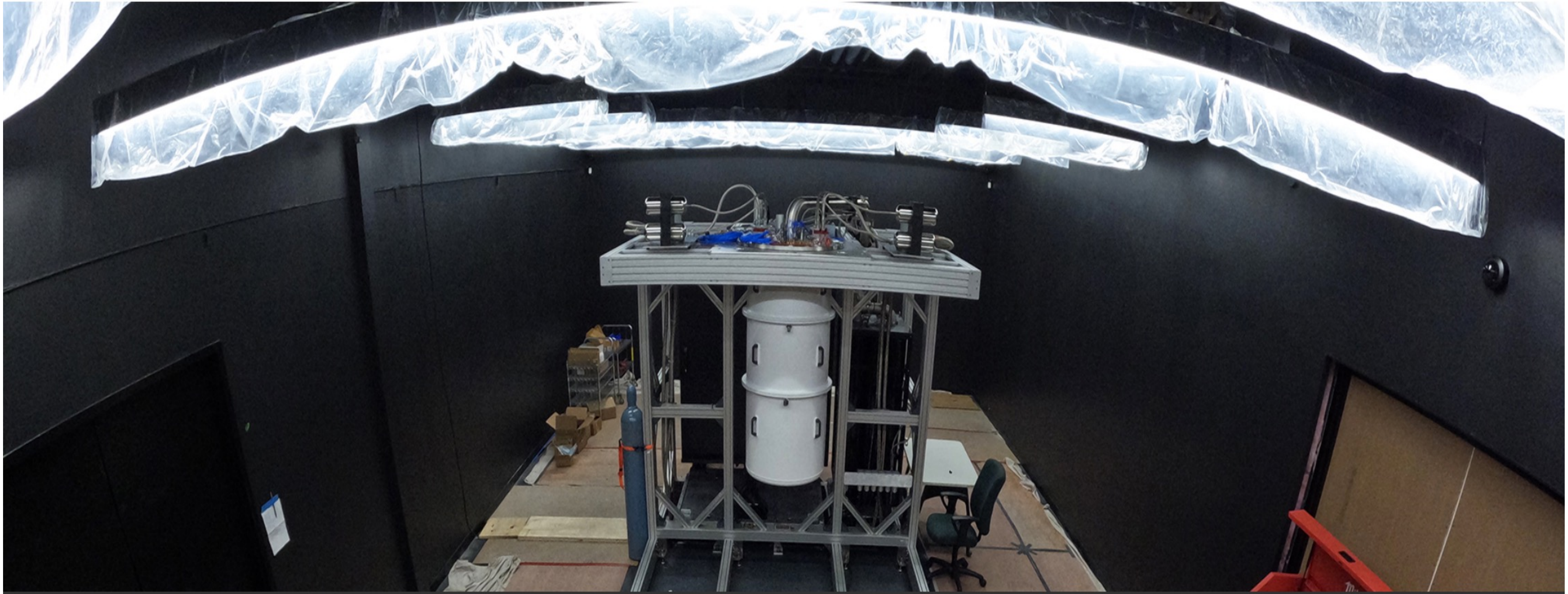
Quantum Computing has the potential to accelerate the transition from umbrella diagnosis and treatment to precision health status intervention:

- Predict the risk of future disease based on EHR
- Predict the effectiveness of cancer drugs at granular level

IBM Quantum System One at Cleveland Clinic at Main Campus O : RYAN LAVINE FOR IBM

IBM and PINQ^2 to Accelerate Quantum Computing in Quebec

PINQ^2 researchers and clients to explore solutions to sustainability challenges in Quebec, Canada, and globally, as well as accelerated computing in financial services



IBM Quantum System One, powered by utility-scale quantum processor, being installed at IBM Bromont for PINQ^2. (Credit: IBM)

Quantum Computing Risk

Ability to quickly solve the math problems which are the basis of key cryptographic algorithms such as integer factorization in RSA

A quantum computer can solve certain problems much **faster**.

2048-bit composite integer

```
25195908475657893494027183240048398571429282126204
03202777713783604366202070759555626401852588078440
69182906412495150821892985591491761845028084891
20072844992687392807287776735971418347270261896375
01497182469116507761337985909570009733045974880842
84017974291006424586918171951187461215151726546
32282216869987549182422433637259085141865462043576
79842338718477444792073993423658482382428119816381
50106748104516603773060562016196762561338441436
03833904414952634432190114657544454178424020924616
51572335077870774981712577246796292638635637328991
21548314381678998850404453640235273819513786365
643921201039712282212072035
```

Problem: find prime factors

= p x q

Expected computation time:

Most powerful computer today: millions of years

Shor’s Quantum Algorithm: Some hours

A Quick Peek into Shor’s Algorithm

How to factor N, a product of 2 primes, p and q?

1. Make a guess g, g < N that shares no factors with N

2. Find r such that $g^r = mN + 1$

3. if r is even, calculate $(g^{r/2} + 1)$ and $(g^{r/2} - 1)$. If r is odd go back to step 1

4. Use Euclid’s algorithm to find the greatest common divisor between $(g^{r/2} + 1)$ and N as well as $(g^{r/2} - 1)$, which gives p and q

Step #1

- Split the qubits into 2 equal sets
- Set 1 is prepared in a superposition of 0, 1, 2, 3, ..., 10^{1234}
  $|x> = |0> + |1> + |2> + |3> + \ldots + |10^{1234}>$
- In Set 2, the qubits are left in the zero state
  |w> = |0>|0>|0>|0> ... |0>

Step #2

- Choose a value for g
- Raise g to the power of the first set of qubits and divide by N
- Store the remainders in the second set of qubits
  $|0>|rem_0> + |1>|rem_1> + |2>|rem_2> + |3>|rem_3> + \ldots$

Step #3

- Measure the remainders portion of the superposition, leaves
  |**i,** rem> + |**i + r,** rem> + |**i + 2r,** rem> + |**i + 3r,** rem> + ...
- Put the remainder to the side since it is the same for all states, leaves a superposition that is periodic
  |**i**> + |**i + r**> + |**i + 2r**> + |**i + 3r**> + ...
- Apply quantum Fourier transform, leaves us with states containing 1/r
  |c1 **1/r**> + |c2 **1/r**> + |c3 **1/r**> + ...
- Perform a measurement and find r by inverting 1/r

Quantum Computing Risk

What is at stake?

- Asymmetric cryptography based on integer factorization and discrete logarithms will be broken
- Symmetric cryptography key strength will be reduced by half

Encryption Algorithm	Key Size	Security Level on Classical Computer	Security Level on Quantum Computer
RSA-1024	1024 bits	80 bits	0
RSA 2048	2048 bits	120 bits	0
ECC 256	256 bits	128 bits	0
ECC 384	384 bits	192 bits	0
AES 128	128 bits	128 bits	**64 bits**
AES 256	256 bits	256 bits	**128 bits**

Shor's algorithm

Exponential improvement in brute-force attacks on asymmetric encryption schemes like RSA, ECC, ElGamal, DH

Grover's algorithm

Quadratic improvement in brute-force attacks on symmetric encryption schemes like AES

Quantum Computing Risk

Example implication #1

- Secure communication protocols: SSL, TLS, HTTPS, SSH

- **Shor's algorithm** running on a large-scale quantum computer may allow an attacker to:
  - Derive the RSA private key
  - Use that information to decrypt the data exchanged

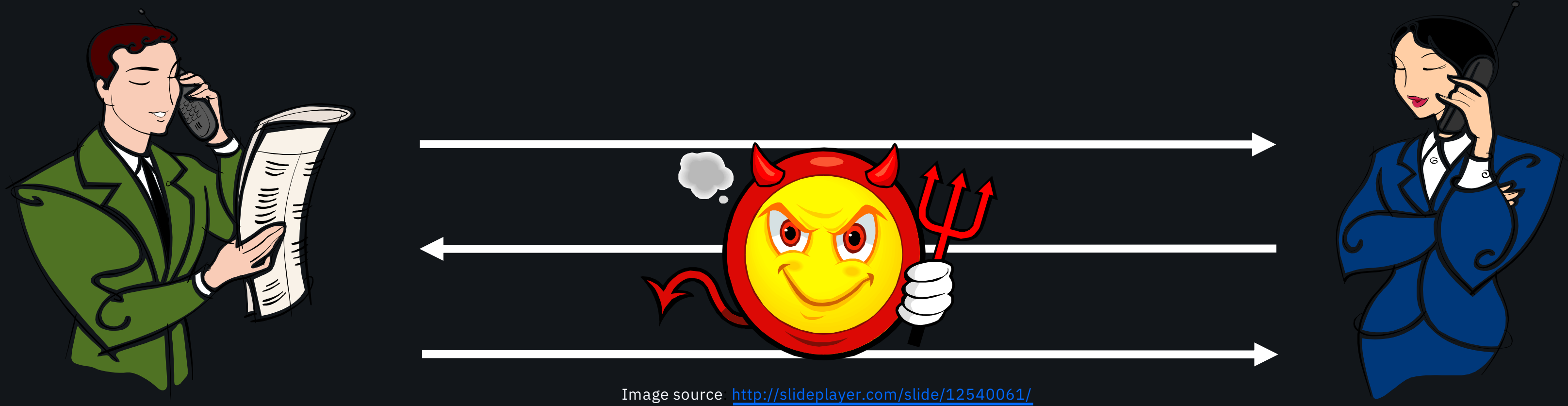


Image source http://slideplayer.com/slide/12540061/

Quantum Computing Risk

Example implication #2

- Secure communication protocols: SSL, TLS, HTTPS, SSH

- **Store copies of today's communications** and **decrypt them later** when large-scale quantum computers become available ("Harvest now, decrypt later")

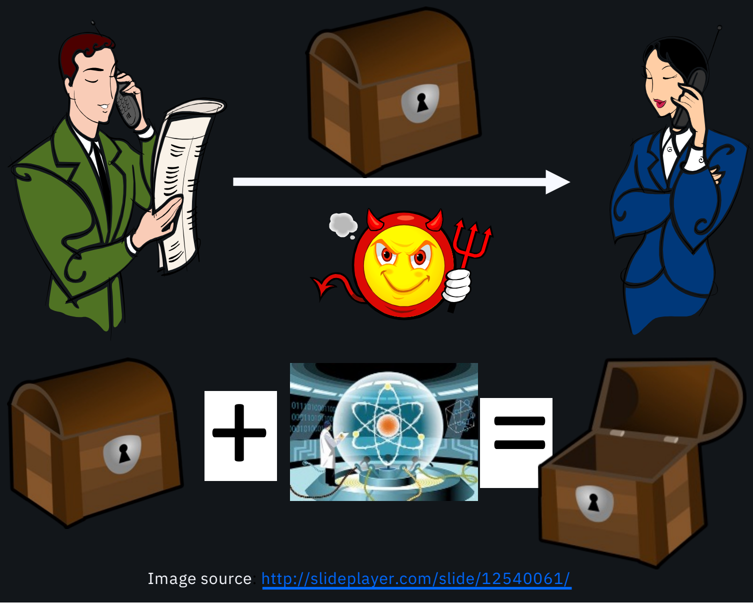


Image source http://slideplayer.com/slide/12540061/

Quantum Computing Risk

Example implication #3

- Signature-based authentications mechanisms
- **Shor's algorithm** running on a **quantum computer** may allow an attacker to **derive a private signing key** from its public key
  - Sign forged documents and no one will be able to tell they are not from a legitimate source
  - Create malicious code and distribute it as a trusted code update
  - Sign certificates as if they are a legitimate Certificate Authority (CA)

Post Quantum Cryptography (PQC)

Algorithms that are safe against attacks by both classical and quantum computers

- US NIST selected 4 algorithms for standardization in July 2022
  - CRYSTALS – KYBER (key exchange)
  - CRYSTALS – DILITHIUM (signature)
  - FALCON (signature)
  - SPHINCS (signature)

- PQC standard itself will not be available before 2024
  - The selected algorithms will undergo significant changes before the standard is published
- TLS PQC standard will follow the PQC standard at a subsequent time

Lattice-Based Cryptography

From the field of mathematics called ‘the geometry of numbers’

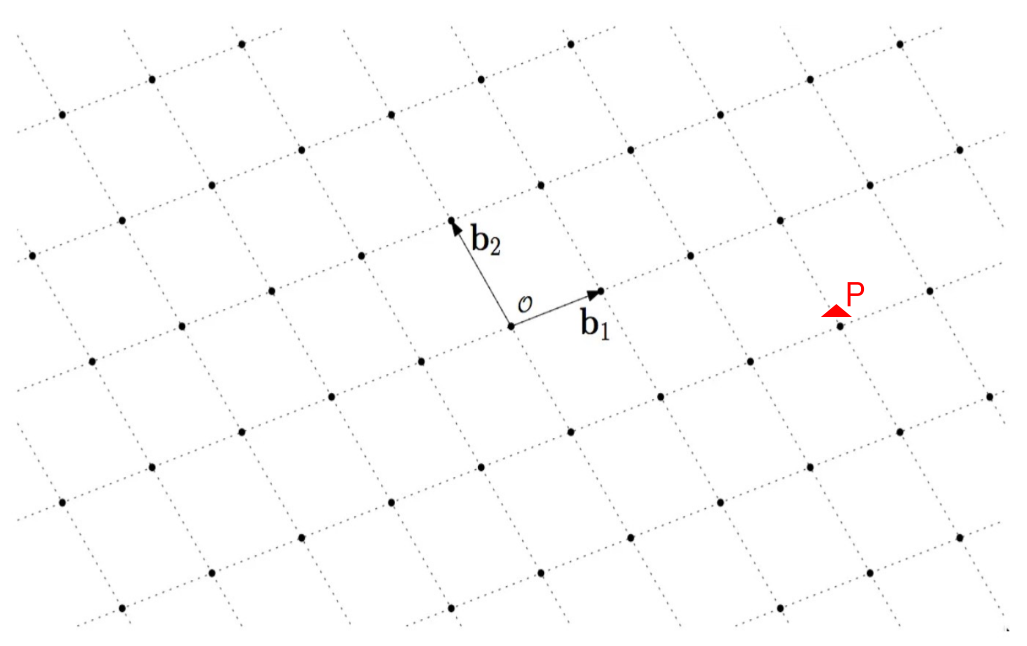


Image source: https://medium.com/nerd-for-tech/the-idea-behind-lattice-based-cryptography-5e623fa2532b

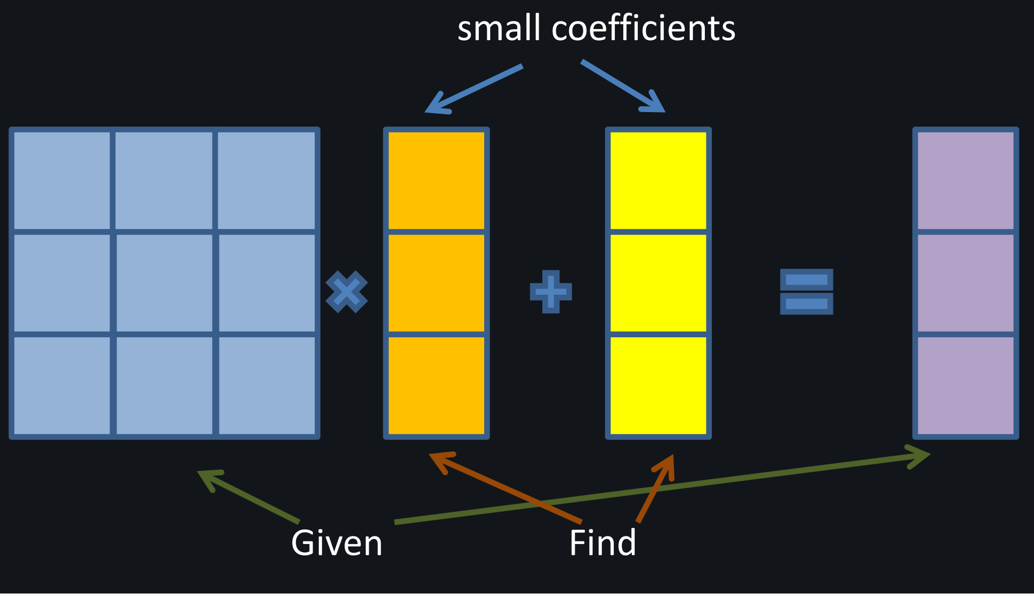
- A lattice is a grid of points described by a set of vectors called the base
- Any linear combination of the base vectors is a point on the lattice
- The lattice problem is: *Given an origin point P, find the closest point to P on the lattice*
- When the number of dimensions is large (i.e., 1000 dimensions), this problem is very hard to solve for both classical and quantum computers (when given a “bad” base)

Lattice-Based Cryptography

From the field of mathematics called ‘the geometry of numbers’

- Most widely studied
- Faster than RSA and ECC
- Multiple primitives (Key Distribution/Signature)
- A versatile building block for more complex crypto schemes (e.g., FHE)

Difficulty of solving linear equation perturbed by small error



A Sample Quantum Safe Transitioning Experience

User Authentication in Db2

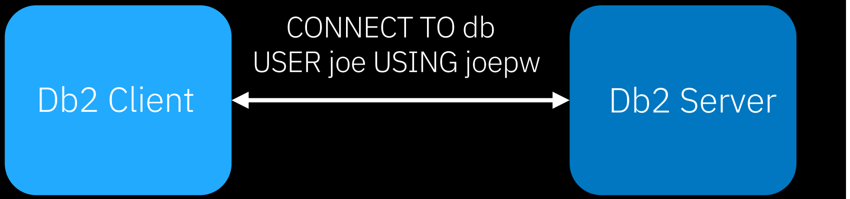
Problem Statement

Db2 User Authentication uses Diffie-Hellman (DH) for key agreement between the Db2 Server and the Db2 Client. DH is not Quantum Safe. The challenges we face are the following:

1. How do we replace DH with a Quantum Safe alternative?
2. How do we mitigate the concern that a Post-Quantum Cryptography (PQC) standard does not exist yet?

Capabilities Available

IBM Security Global Security Toolkit (GSkit) includes implementation of the Kyber & Dilithium PQC algorithms



A Sample Quantum Safe Transitioning Experience

User Authentication in Db2

Application issues:

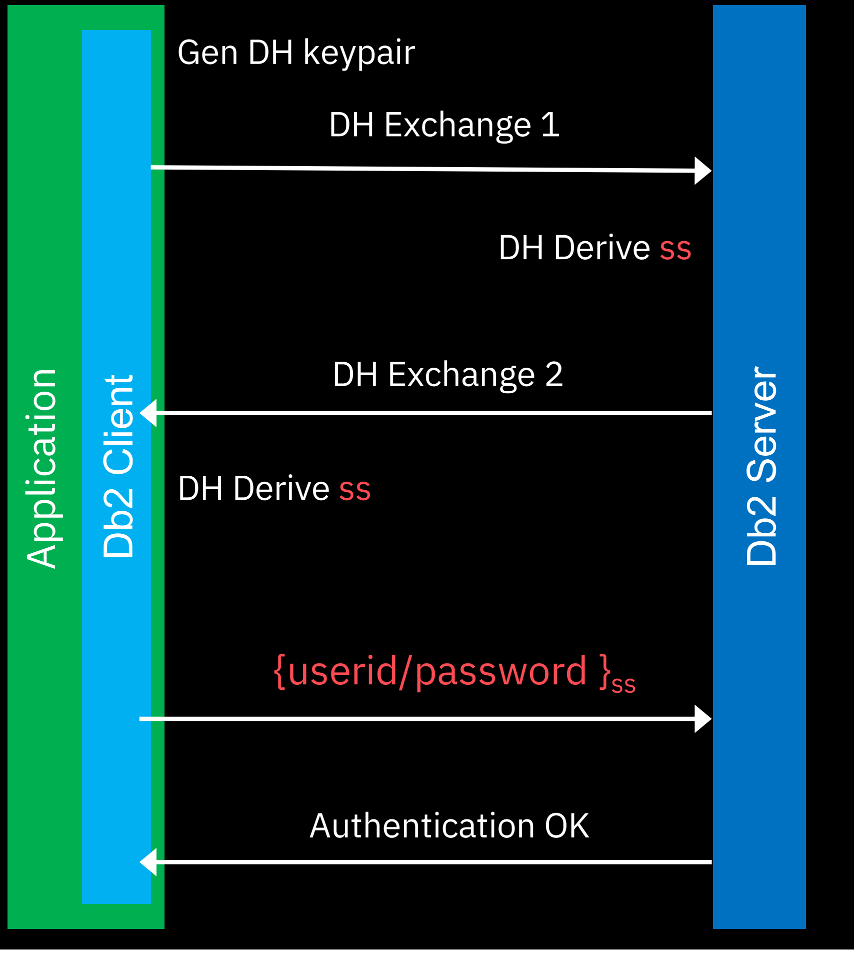
```
CONNECT TO <db-name>
   USER <user-name>
   USING <password>
```

1. Db2 client and server “agree” on shared secret key (ss) using Diffie-Hellman (DH)

2. Db2 client encrypts user ID and password using agreed upon key (ss)

3. Db2 server decrypts user ID and password using that same key (ss)

4. Usual authentication process follows



Application

Db2 Client

Gen DH keypair

DH Exchange 1

DH Derive ss

DH Exchange 2

DH Derive ss

$\{userid/password\}_{ss}$

Authentication OK

Db2 Server

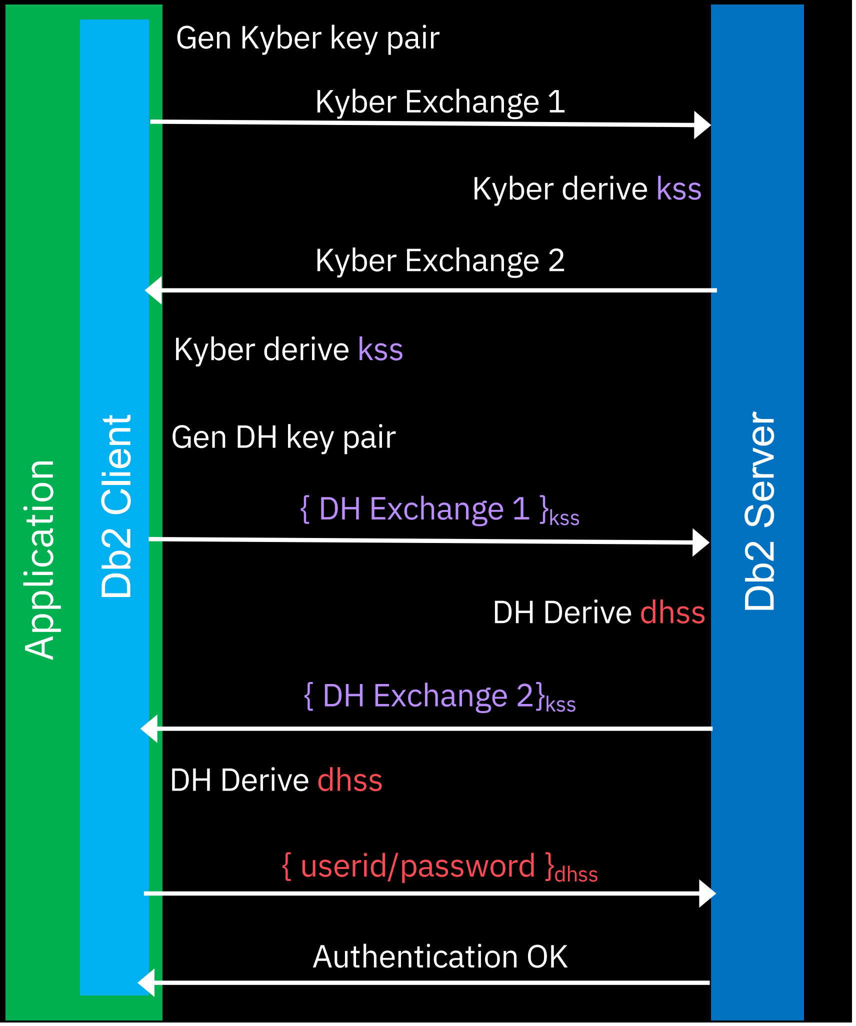
$\{x\}_s$ = x encrypted using key s

A Sample Quantum Safe Transitioning Experience

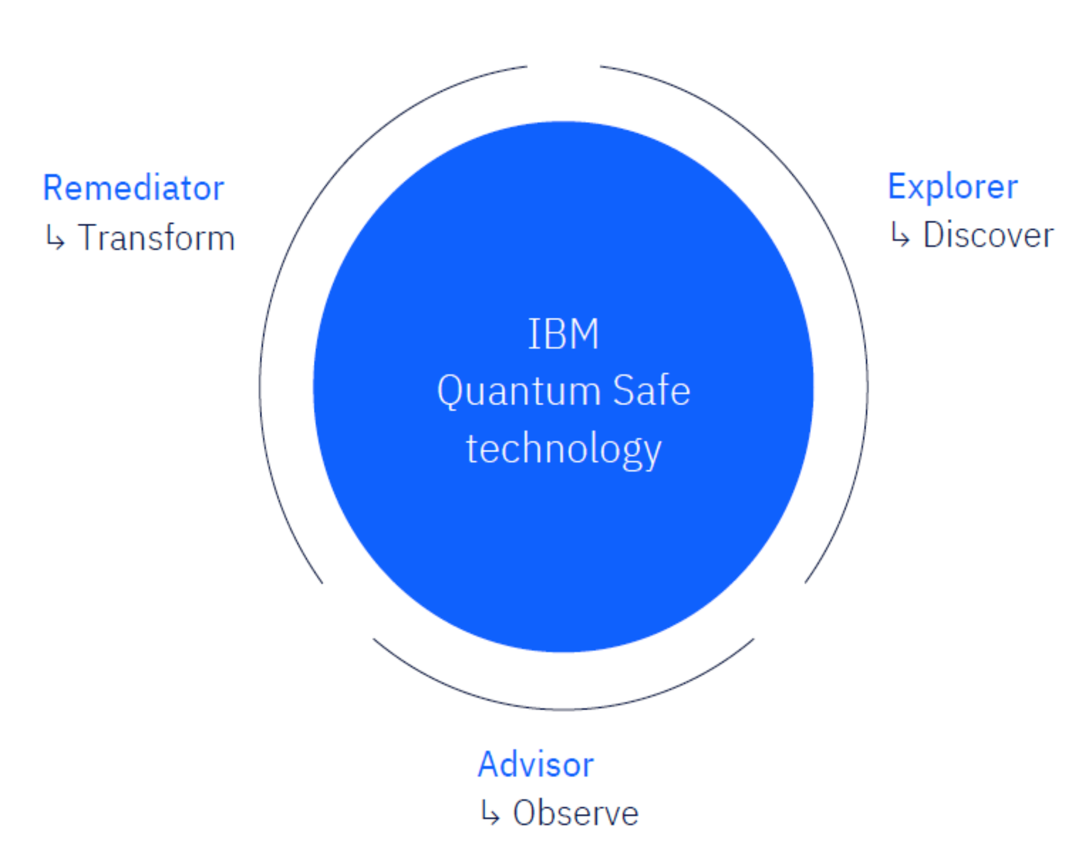
Quantum Safe User Authentication in Db2 – Hybrid Model

1. Client generates a private/public Kyber key pair, sends the public key to the server
2. Server takes public key and uses a random seed to derive a shared key (kss) and cipher text
3. Client uses private key and cipher text to derive the same shared key (kss)
4. Use Kyber shared secret as an AES 256 bit key to encrypt the Diffie-Hellman key exchange
5. Use DH normally over this protected channel
6. Change the key used on the protected channel to the one from DH (dhss) to encrypted user ID and password

$\{x\}_s$ = x encrypted using key s



IBM Technology Helping Clients Throughout Their Quantum Safe Journey



- IBM Quantum Safe Explorer
  ↳ discover your cryptography
  Scan source code and object code for cryptography usage and generate cryptography bill of materials (CBOM)

- IBM Quantum Safe Advisor
  ↳ observe your cryptography
  Analyze cryptography posture of compliance and vulnerabilities, prioritize remediation actions

- IBM Quantum Safe Remediator
  ↳ transform your cryptography
  Apply remediation patterns for implementation of crypto-agility

Quantum Cryptography vs Post Quantum Cryptography

Quantum Cryptography*

- Key distribution exploits quantum physics (e.g., use of single photons)
- Provably secure against (quantum) eavesdroppers
- Requires special infrastructure (e.g., optical fibers)
- Range limitations
- Confidentiality

Post Quantum Cryptography

- Classical algorithms based on hard mathematical problems
- Considered secure against (quantum) attackers
- Can be implemented on today's infrastructure (e.g., update TLS)
- No range limitations
- Confidentiality, Authentication, Integrity, Repudiation

*Also known as Quantum Key Distribution (QKD)

Quantum Computing Risk Summary

1. The impact is in the future, but the problem is NOW
2. We need to start preparing for the transition to Quantum Safe Encryption NOW
3. The transition to Quantum Safe Encryption is an opportunity to modernize encryption implementations and establish cryptographic governance

References & Further Reading

[1] Why Quantum Computing Capabilities Are Creating Security Vulnerabilities Today
[2] IBV Report on Security in the quantum computing era
[3] Making Existing Software Quantum Safe: Lessons Learned

Thank you

More on Quantum & Quantum Safe Encryption

https://www.ibm.com/quantum-computing

https://csrc.nist.gov/projects/post-quantum-cryptography

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM **Security**

IBM

Symmetric Cryptographic Algorithms

- Use the same key for both encryption & decryption
  - AES and 3DES are the most used algorithms

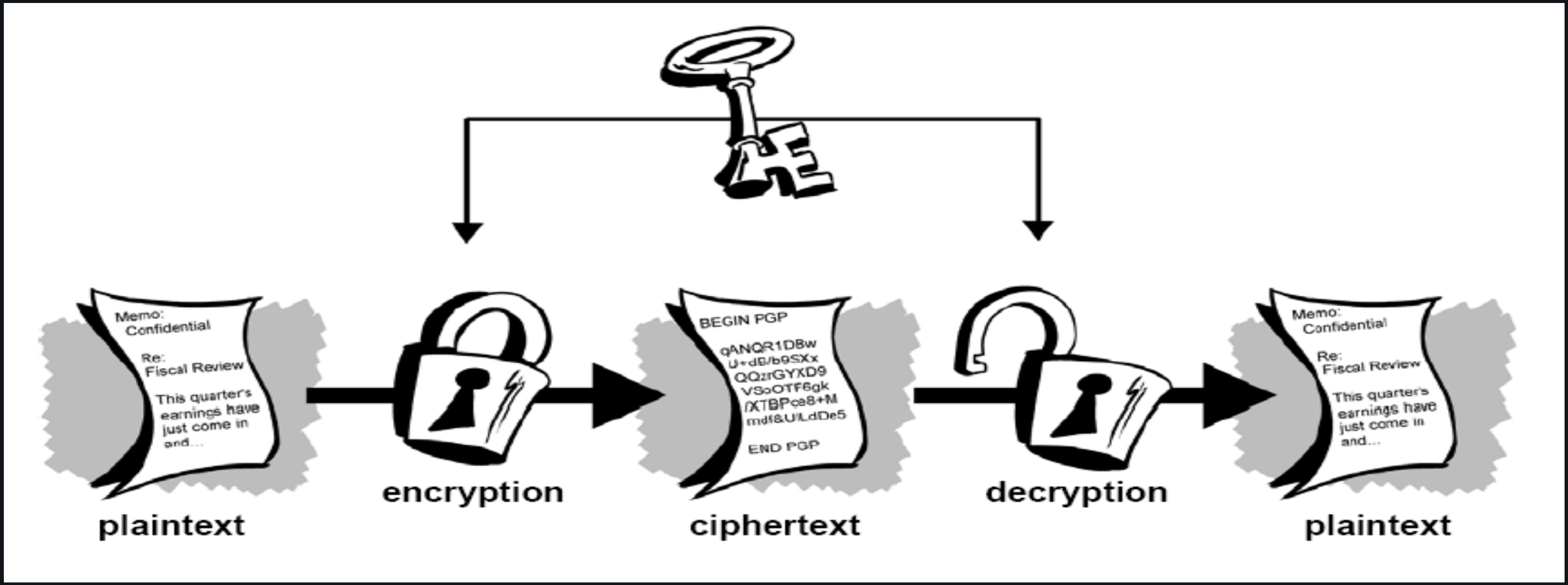


Image source https://chrispacia.wordpress.com/2013/09/07/bitcoin-cryptography-digital-signatures-explained/

Asymmetric Cryptographic Algorithms

- Use different keys for encryption & decryption
  - RSA, ECC, DH are the most commonly used algorithms

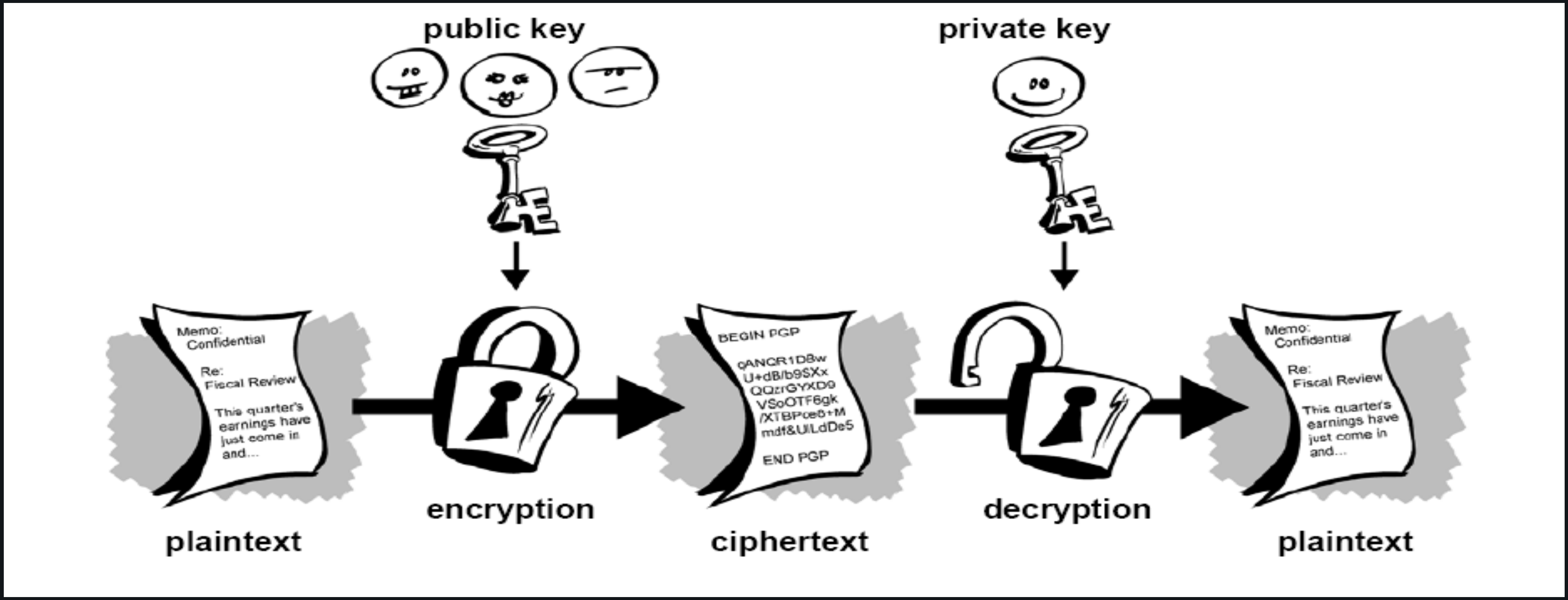


Image source https://chrispacia.wordpress.com/2013/09/07/bitcoin-cryptography-digital-signatures-explained/