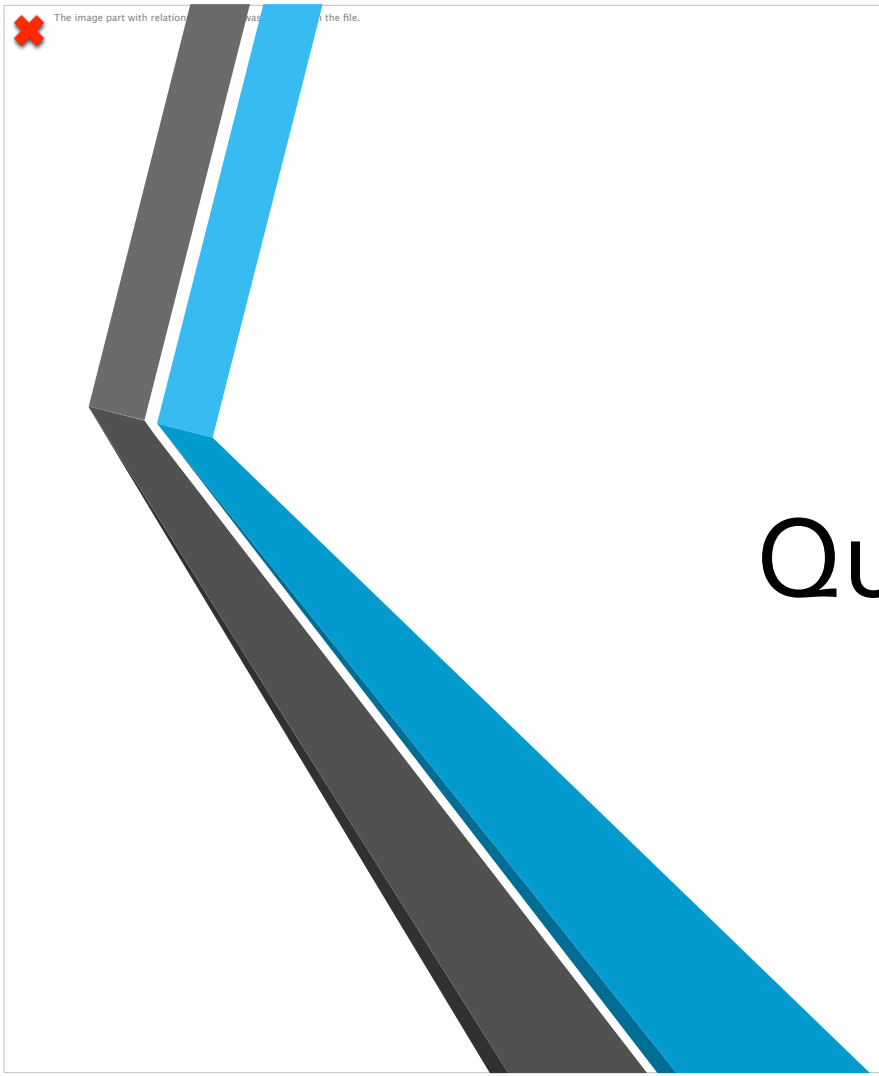
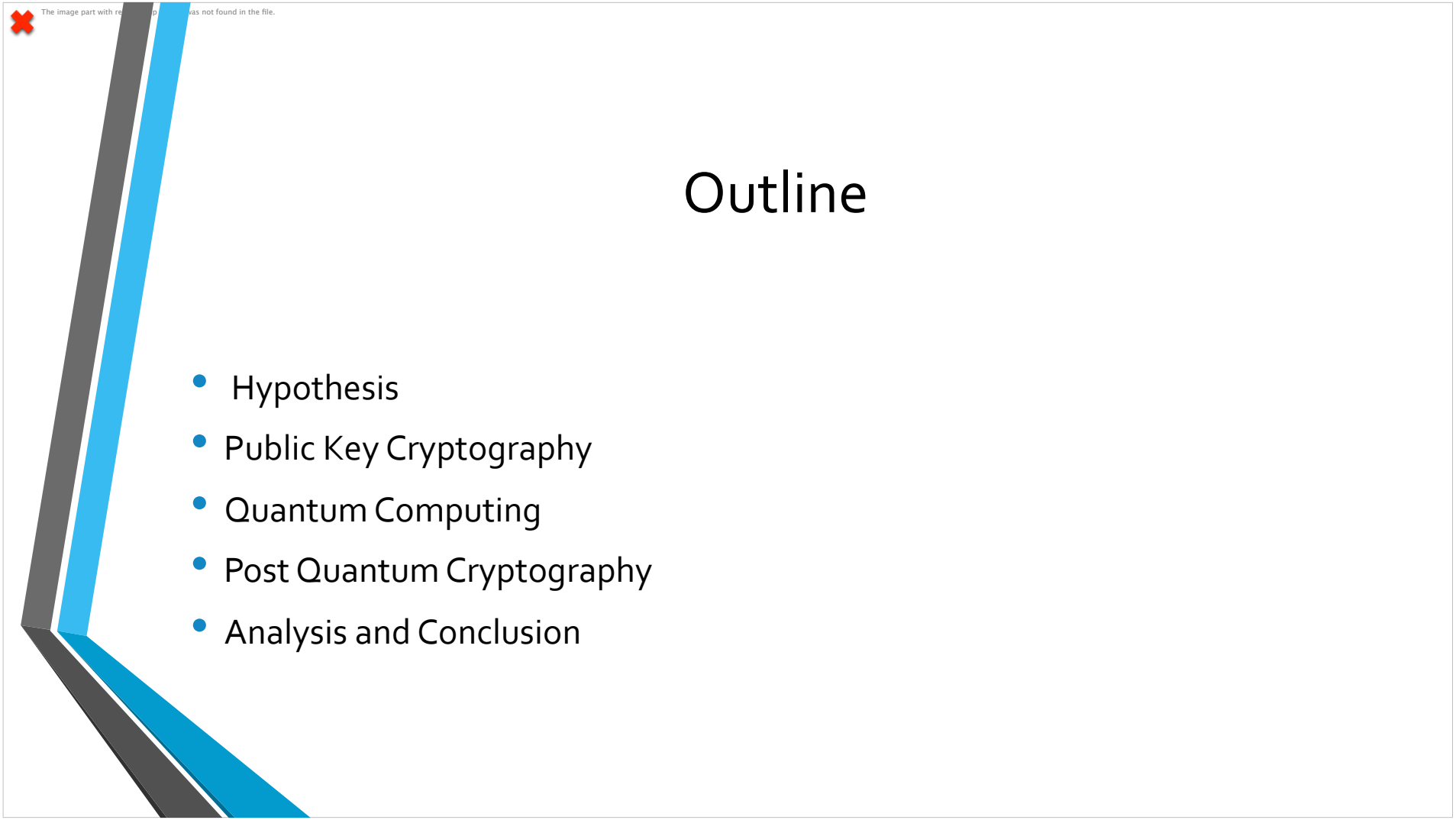


Quantum computing

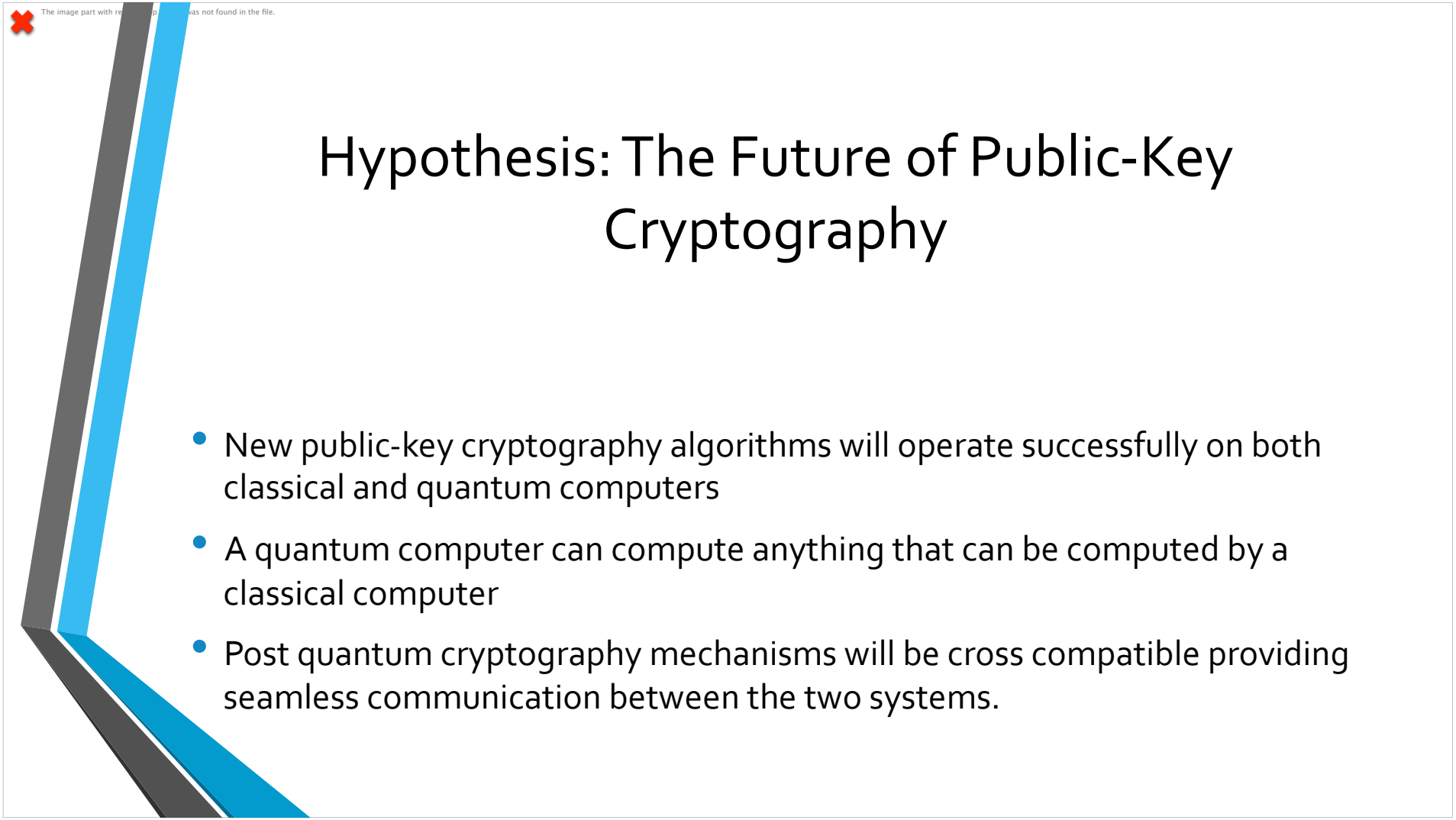
The Future of Public-Key Cryptography

Stacie R Reynolds
Ravinderreddy Bandi
ECE 646 Fall 2013



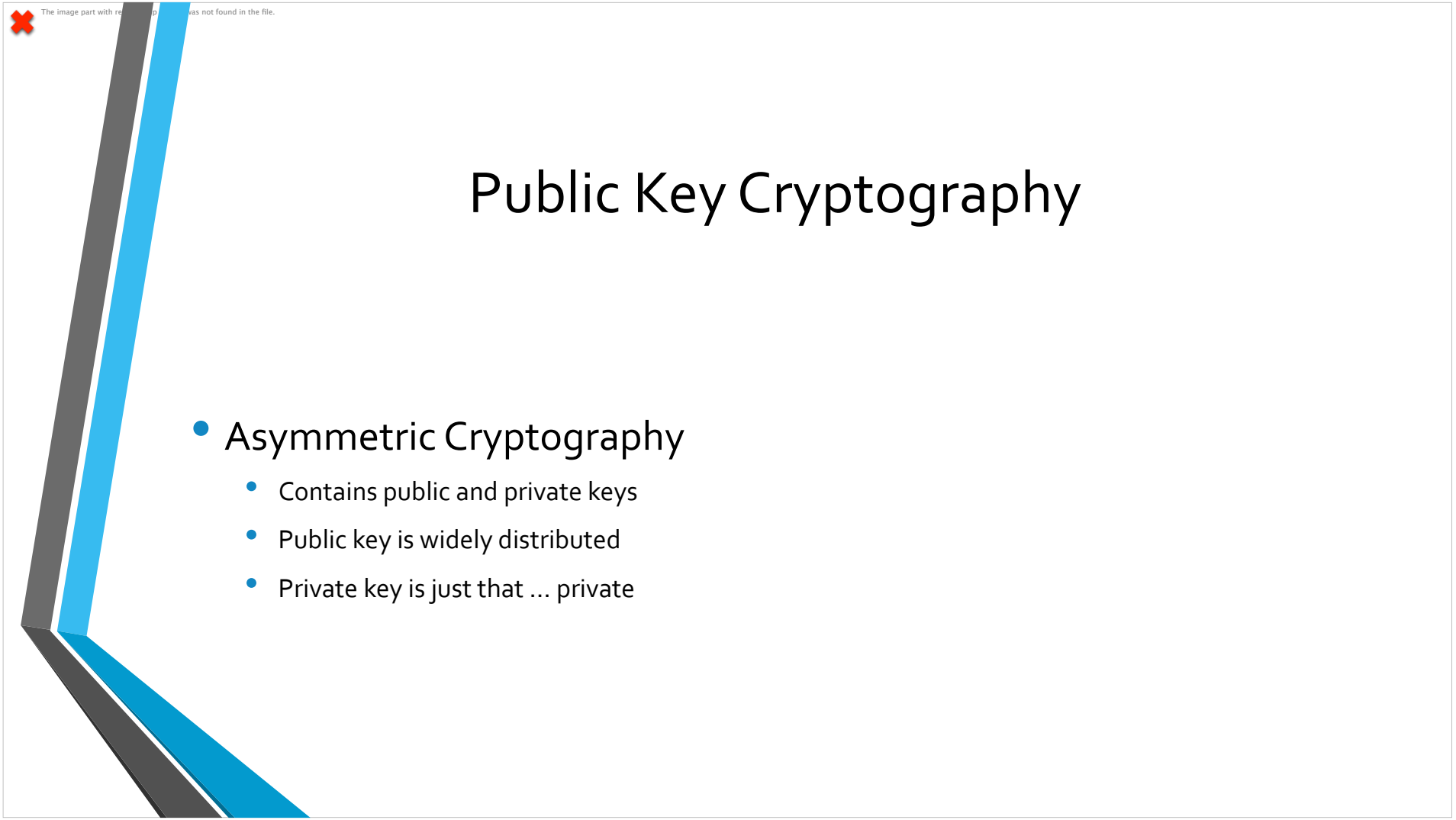
Outline

- Hypothesis
- Public Key Cryptography
- Quantum Computing
- Post Quantum Cryptography
- Analysis and Conclusion



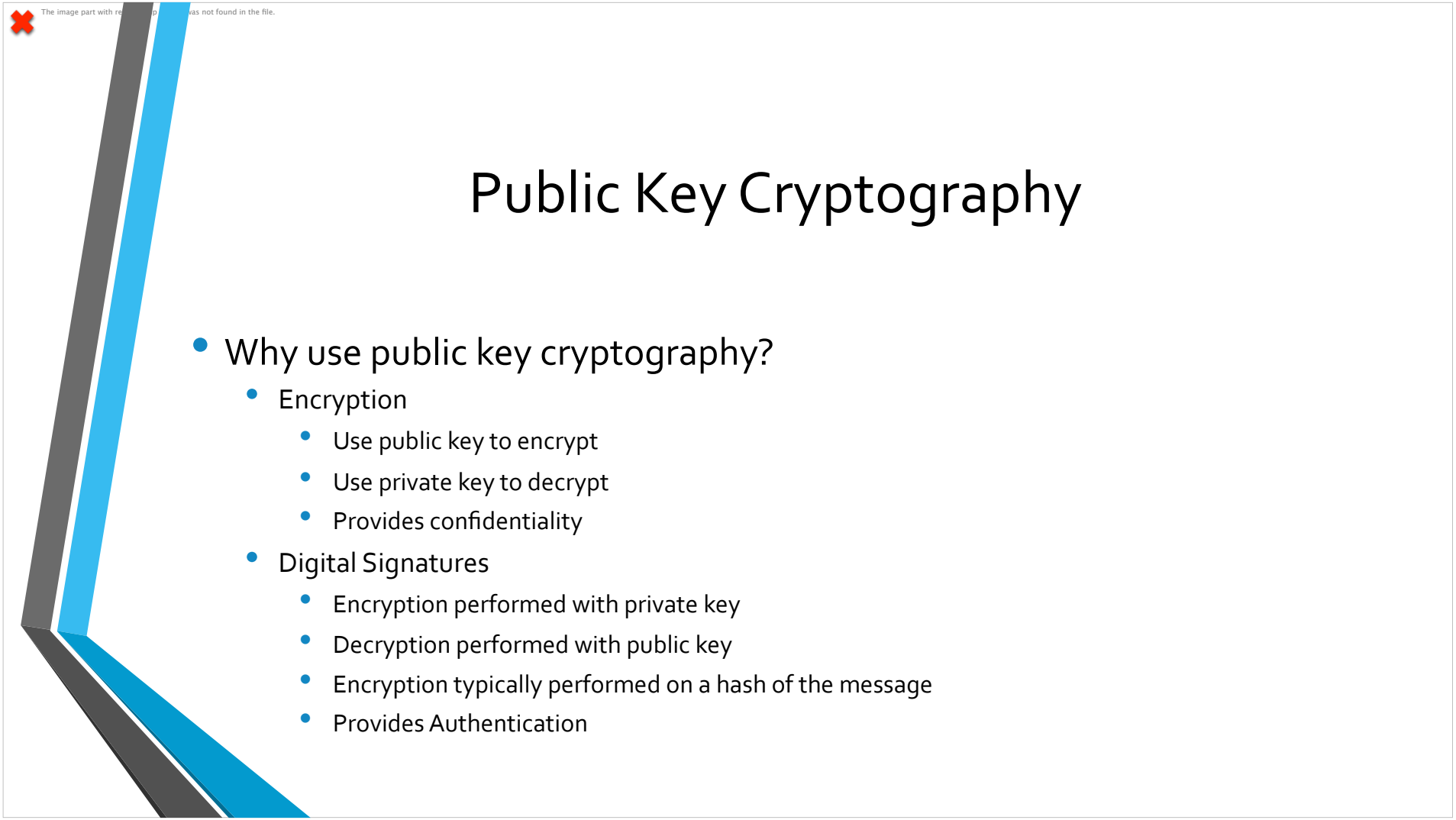
Hypothesis: The Future of Public-Key Cryptography

- New public-key cryptography algorithms will operate successfully on both classical and quantum computers
- A quantum computer can compute anything that can be computed by a classical computer
- Post quantum cryptography mechanisms will be cross compatible providing seamless communication between the two systems.



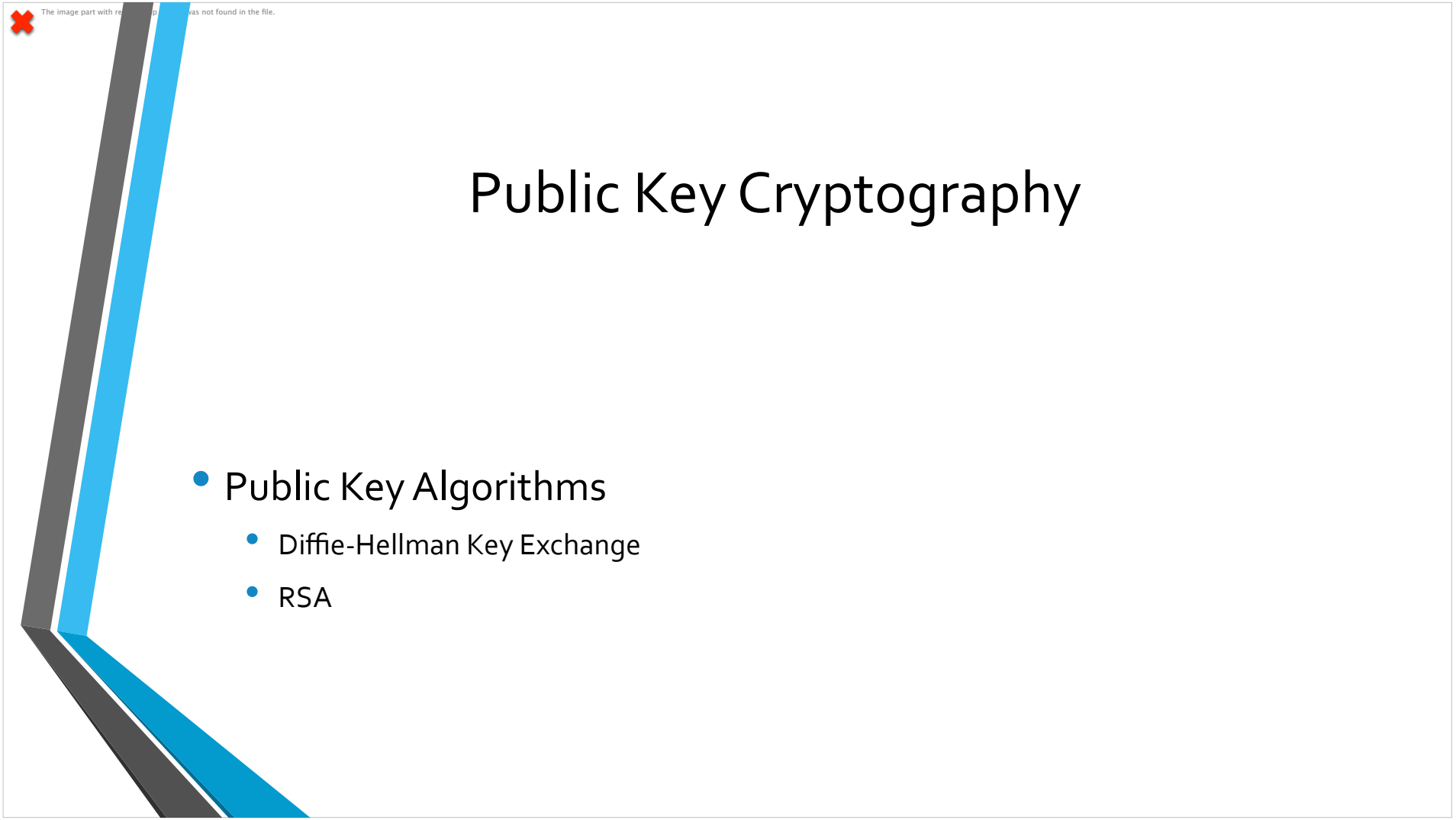
Public Key Cryptography

- Asymmetric Cryptography
  - Contains public and private keys
  - Public key is widely distributed
  - Private key is just that … private



Public Key Cryptography

- Why use public key cryptography?
  - Encryption
    - Use public key to encrypt
    - Use private key to decrypt
    - Provides confidentiality
  - Digital Signatures
    - Encryption performed with private key
    - Decryption performed with public key
    - Encryption typically performed on a hash of the message
    - Provides Authentication

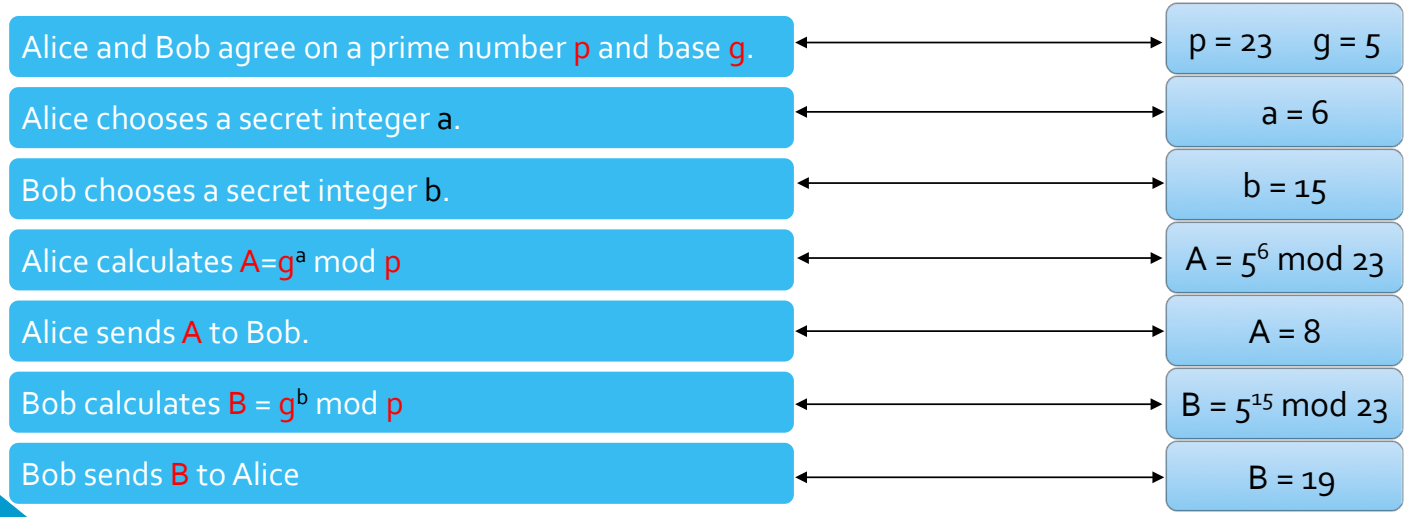


Public Key Cryptography

- Public Key Algorithms
  - Diffie-Hellman Key Exchange
  - RSA

Diffie-Hellman Key Exchange

Allows 2 or more individuals to jointly establish a shared secret key over an insecure communication channel.



The image part with re… p … was not found in the file.

Diffie-Hellman Key Exchange

Calculate Secret Key s

A = 8

$s = A^b \bmod p$

$s = 8^{15} \bmod 23$

$s = 2$

B = 19

$s = B^a \bmod p$

$s = 19^6 \bmod 23$

$s = 2$

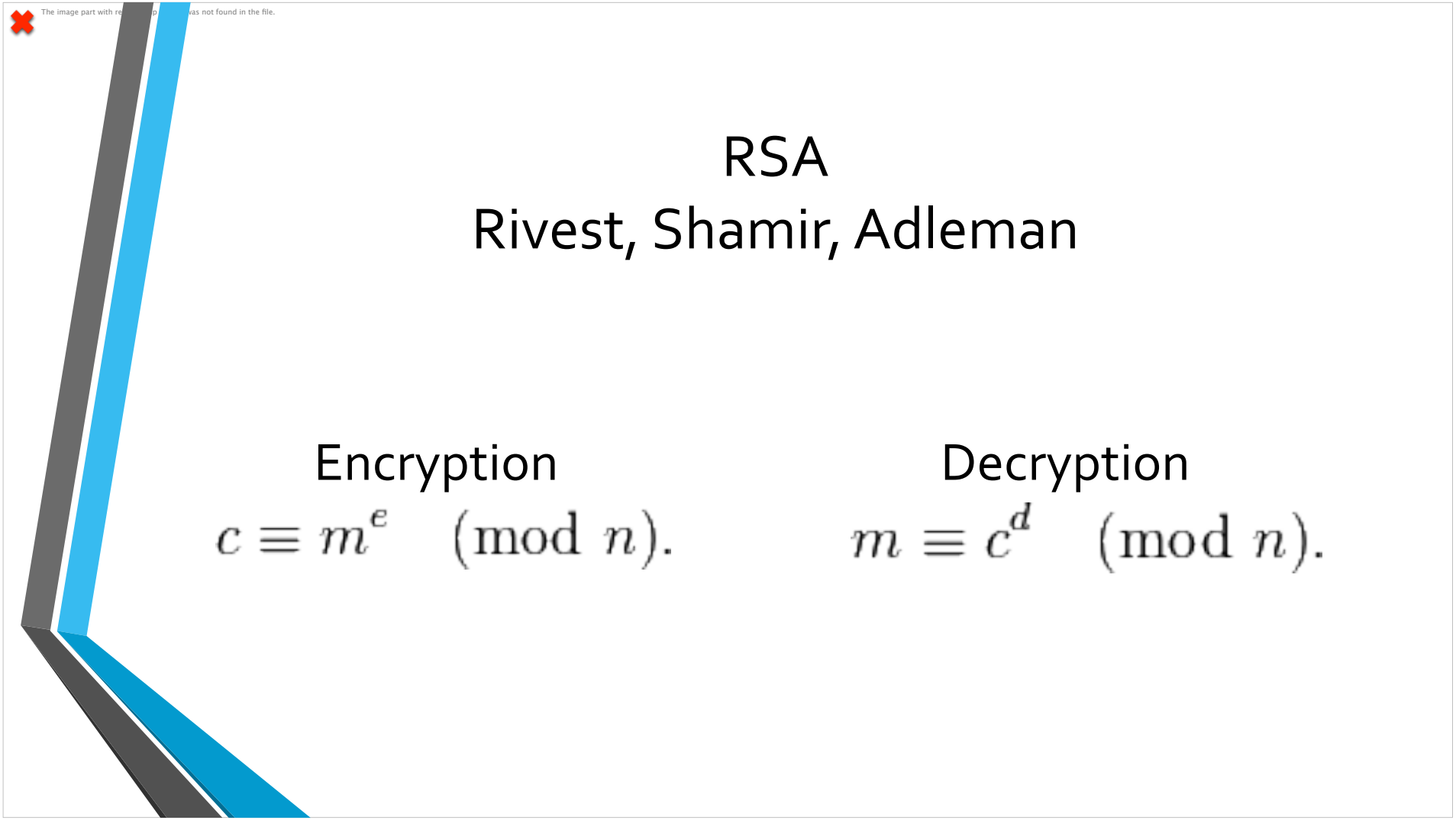
RSA
Rivest, Shamir, Adleman

- Based on the difficulty of factoring the product of two large prime numbers
- Algorithm consists of 3 steps:
  - Key Generation
  - Encryption
  - Decryption

Key Generation:

1. Choose two distinct prime numbers p and q
2. Compute $n=pq$
3. Compute using Euler's totient function, ϕ
   $$\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$$
4. Choose an integer e where
   $$1 < e < \phi(n) \text{ and } \gcd(e, \phi(n)) = 1$$
5. Determine d as $d^{-1} \equiv e \pmod{\phi(n)}$

Public Key consists of modulus n and encryption exponent e
Private Key consists of modulus n and decryption exponent d



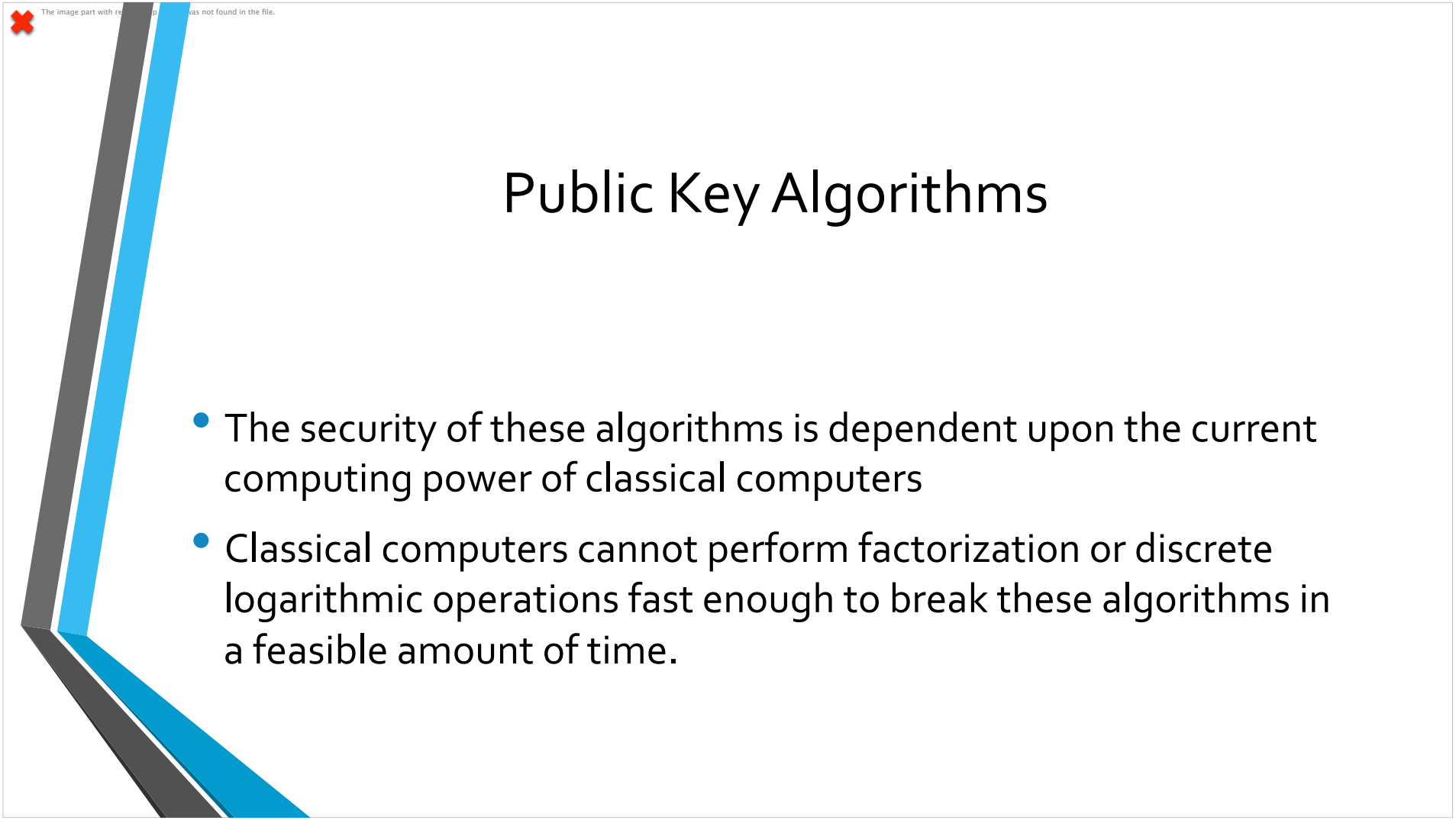
RSA
Rivest, Shamir, Adleman

Encryption

$$c \equiv m^e \pmod{n}.$$

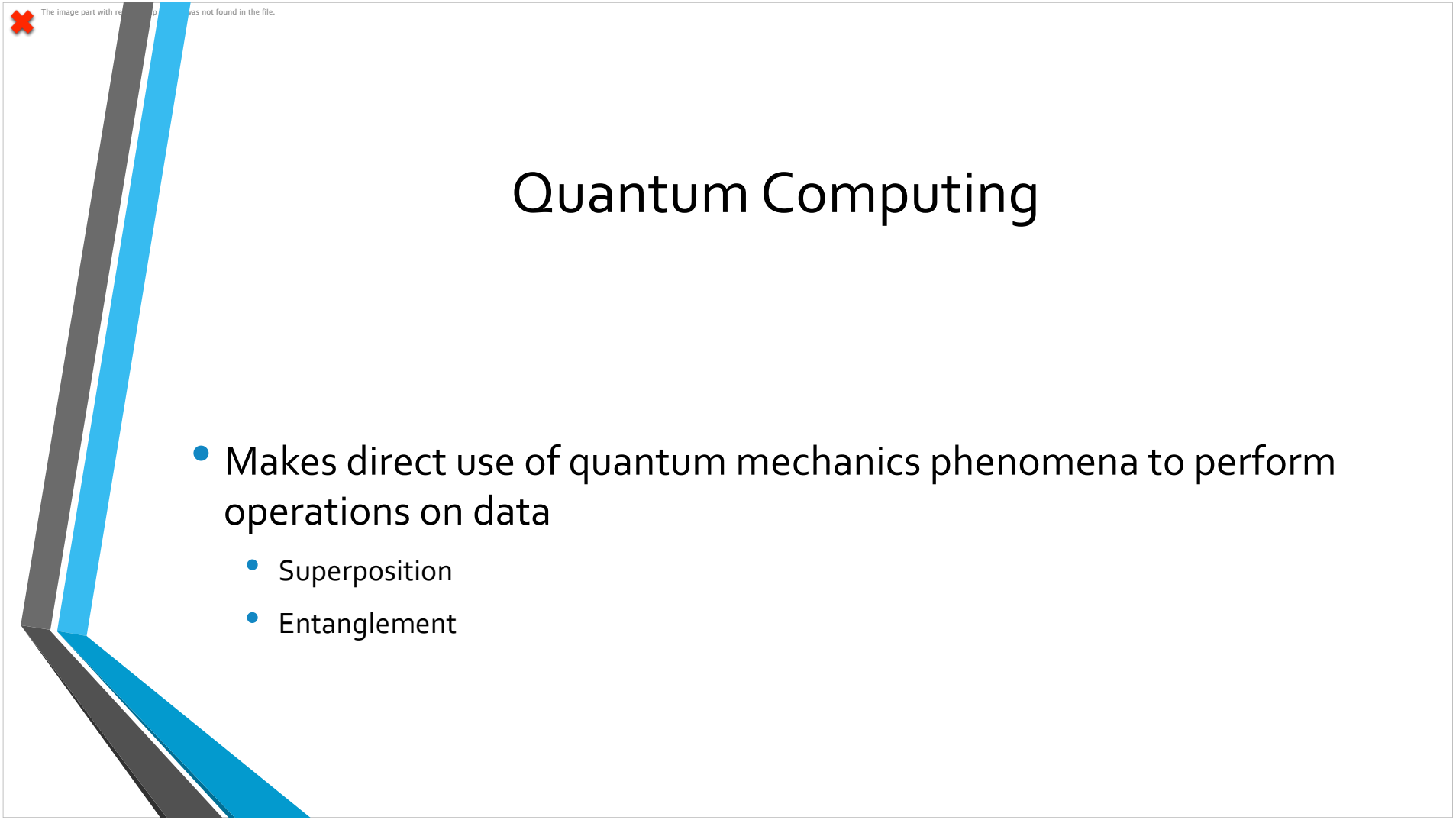
Decryption

$$m \equiv c^d \pmod{n}.$$



Public Key Algorithms

- The security of these algorithms is dependent upon the current computing power of classical computers
- Classical computers cannot perform factorization or discrete logarithmic operations fast enough to break these algorithms in a feasible amount of time.

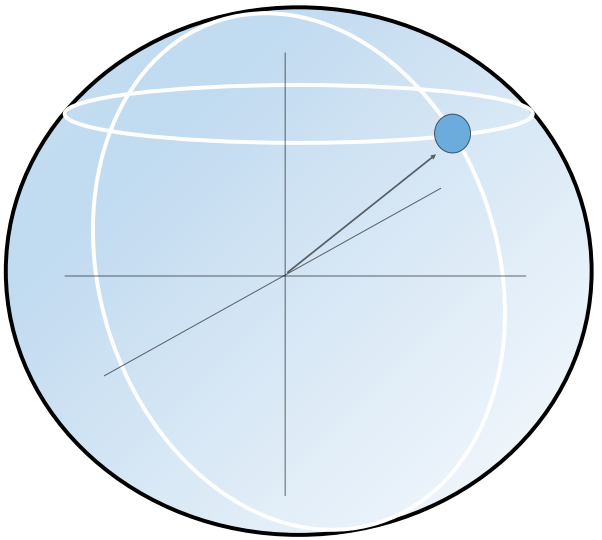


Quantum Computing

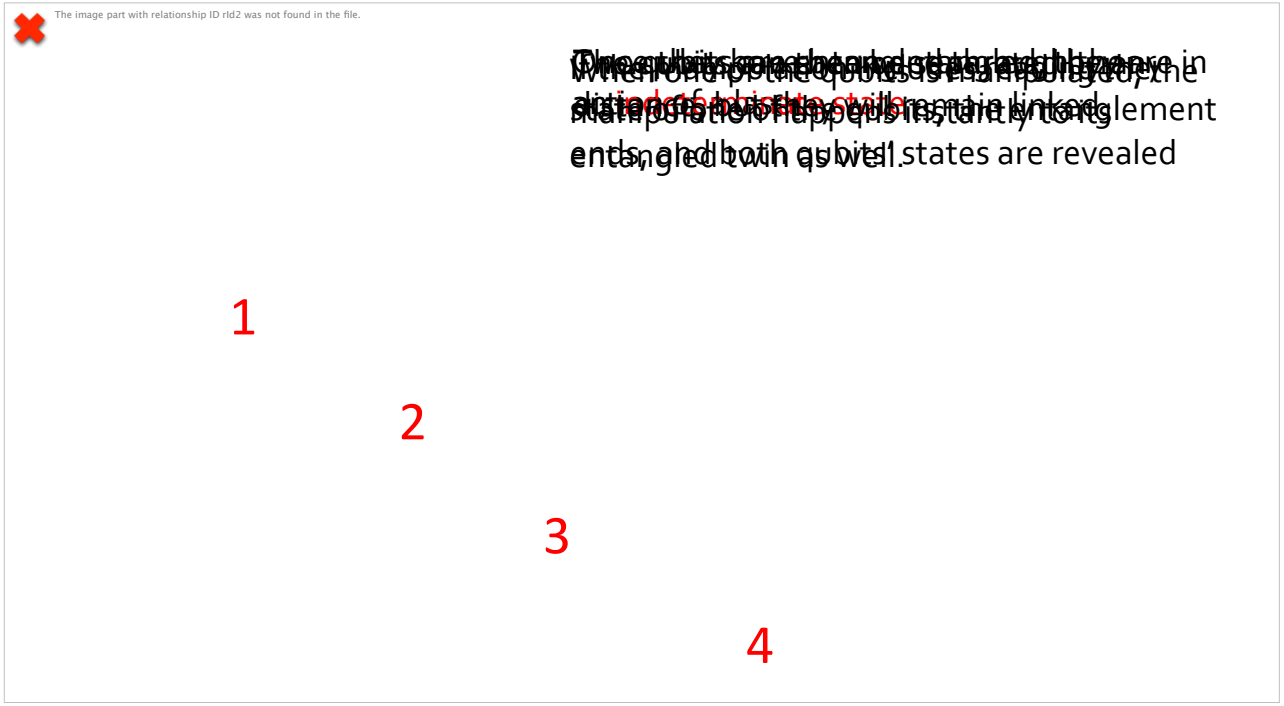
- Makes direct use of quantum mechanics phenomena to perform operations on data
  - Superposition
  - Entanglement

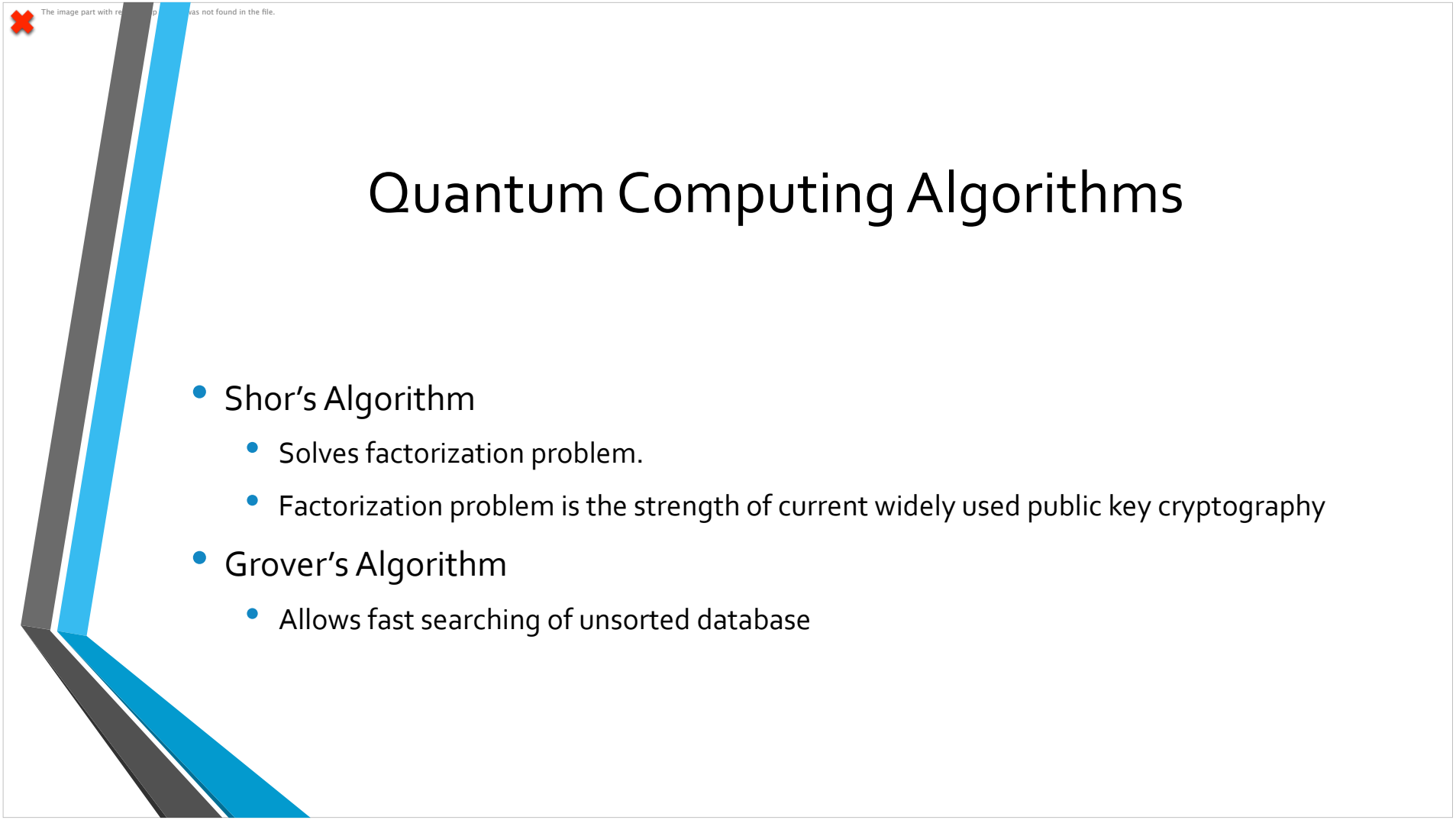
Quantum Computing - Superposition

- Classical computers memory is made up of binary digits (bits) with a value of either 1 or 0.
- Quantum computers are made up of qubits which can represent 1, 0, or both simultaneously.
- When measured or observed only results in one of the possible configurations



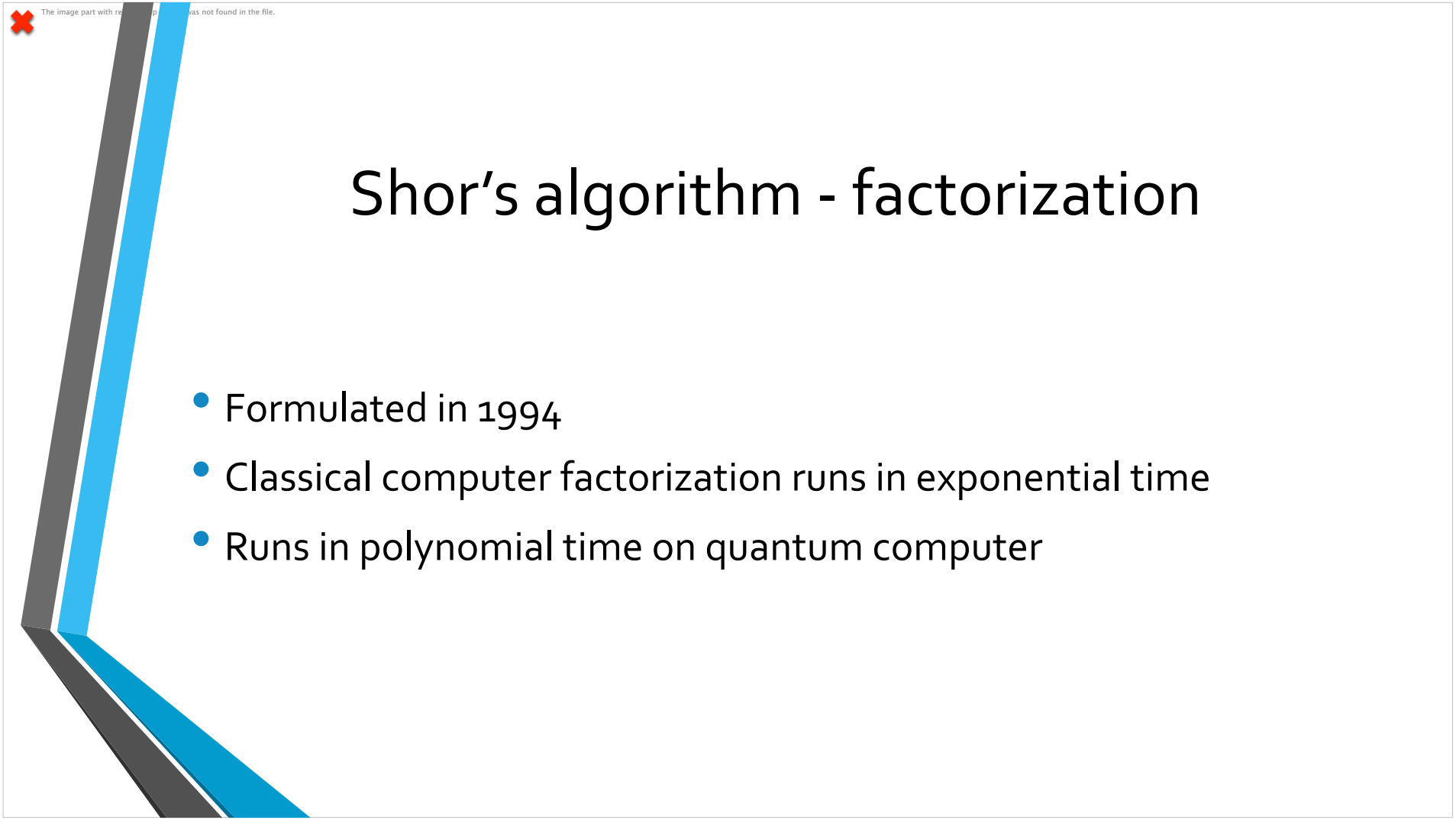
Quantum Computing - Entanglement





Quantum Computing Algorithms

- Shor's Algorithm
  - Solves factorization problem.
  - Factorization problem is the strength of current widely used public key cryptography
- Grover's Algorithm
  - Allows fast searching of unsorted database



Shor's algorithm - factorization

- Formulated in 1994
- Classical computer factorization runs in exponential time
- Runs in polynomial time on quantum computer

Shor's algorithm- Analysis

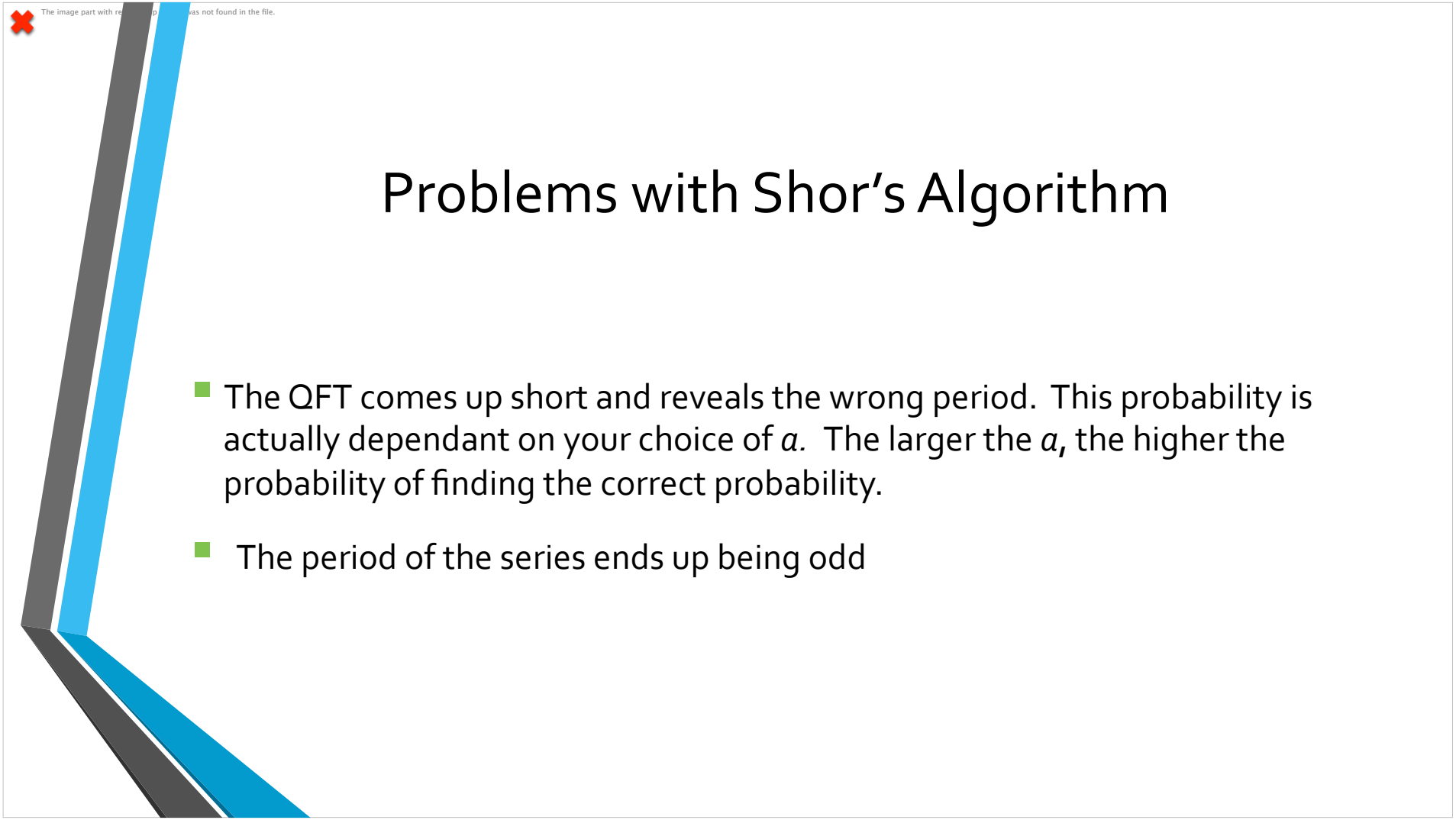
- Pick a random number $a < N$
- Compute gcd(a, N).
- If gcd(a, N) ≠ 1, then there is a nontrivial factor of N, so we are done.
- Otherwise, use the period-finding subroutine f(x)=a^x mod N to find r
- If r is odd, go back to step 1(i.e selecte a random number a<N).
- If $a^{r/2} \equiv -1 \pmod{N}$, go back to step 1.
- gcd($a^{r/2} \pm 1$, N) is a nontrivial factor of N. We are done.

The image part with re… p … was not found in the file.

Quantum Fourier Transformation

- We now apply the Quantum Fourier transform on the partially collapsed input register. The fourier transform has the effect of taking a state |a> and transforming it into a state given by:

$$\frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} |c\rangle * e^{2\pi i ac / q}$$



Problems with Shor's Algorithm

- The QFT comes up short and reveals the wrong period. This probability is actually dependant on your choice of a. The larger the a, the higher the probability of finding the correct probability.
- The period of the series ends up being odd

Breakthroughs In Quantum Computing

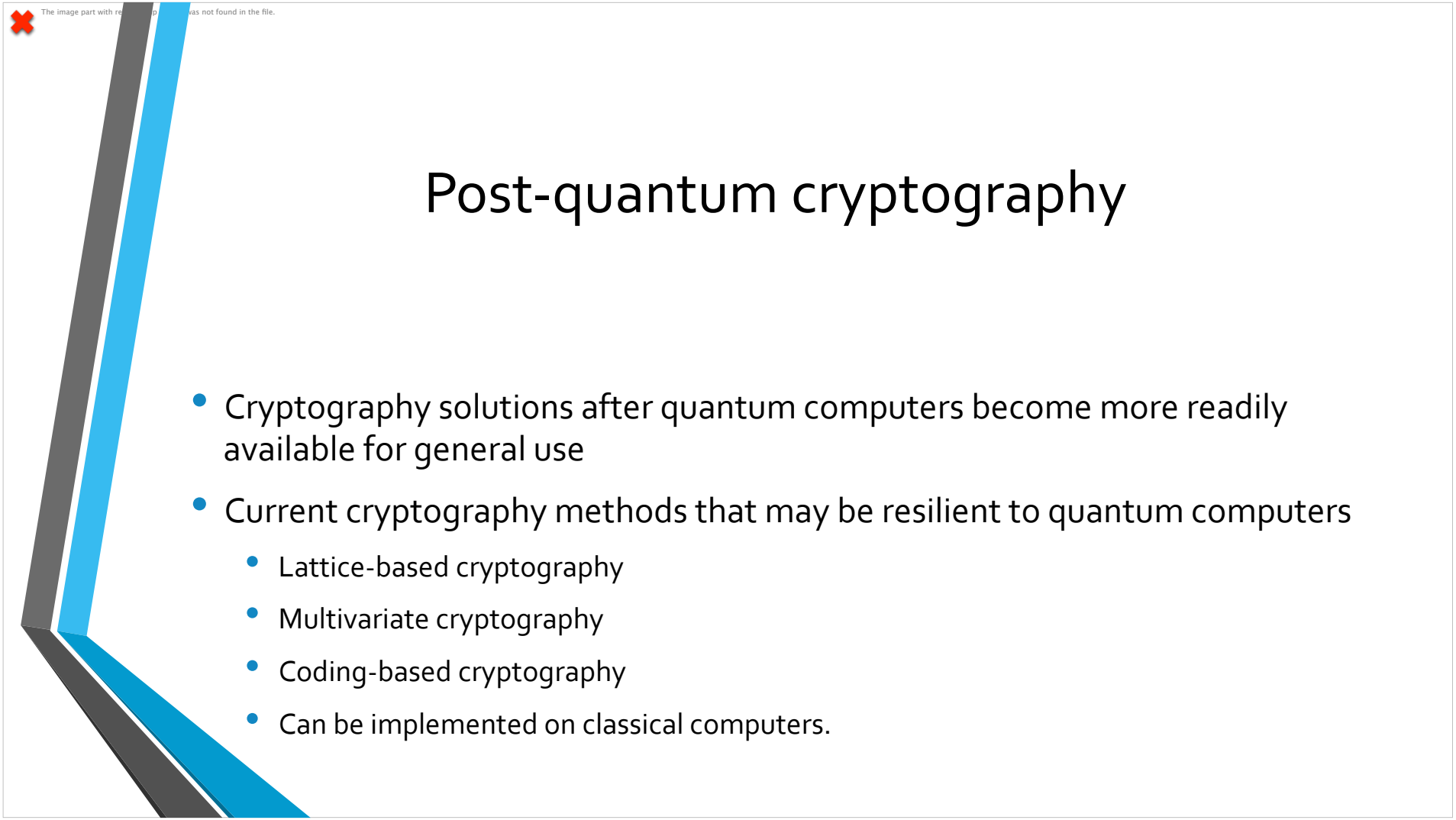
- 1970s
  - "Quantum Information Theory" seminal paper published
- 1980s
  - First universal quantum computer is described
- 1990s
  - Shor and Grover's Algorithm developed
  - First working 3-qubit nuclear magnetic resonance (NMR) computer
  - Grover's Algorithm first execution

Breakthroughs In Quantum Computing

- 2000s
  - First working 7-qubit NMR computer
  - Shor's algorithm first execution
  - Quantum Memory developed
- 2010s
  - Qubits manipulated electronically not magnetically
  - Entanglement of 3 billion qubits for 39 minutes at room temperature.
  - D-Wave Inc. has produced a 512 qubit processor which has been purchased by Google and NASA.

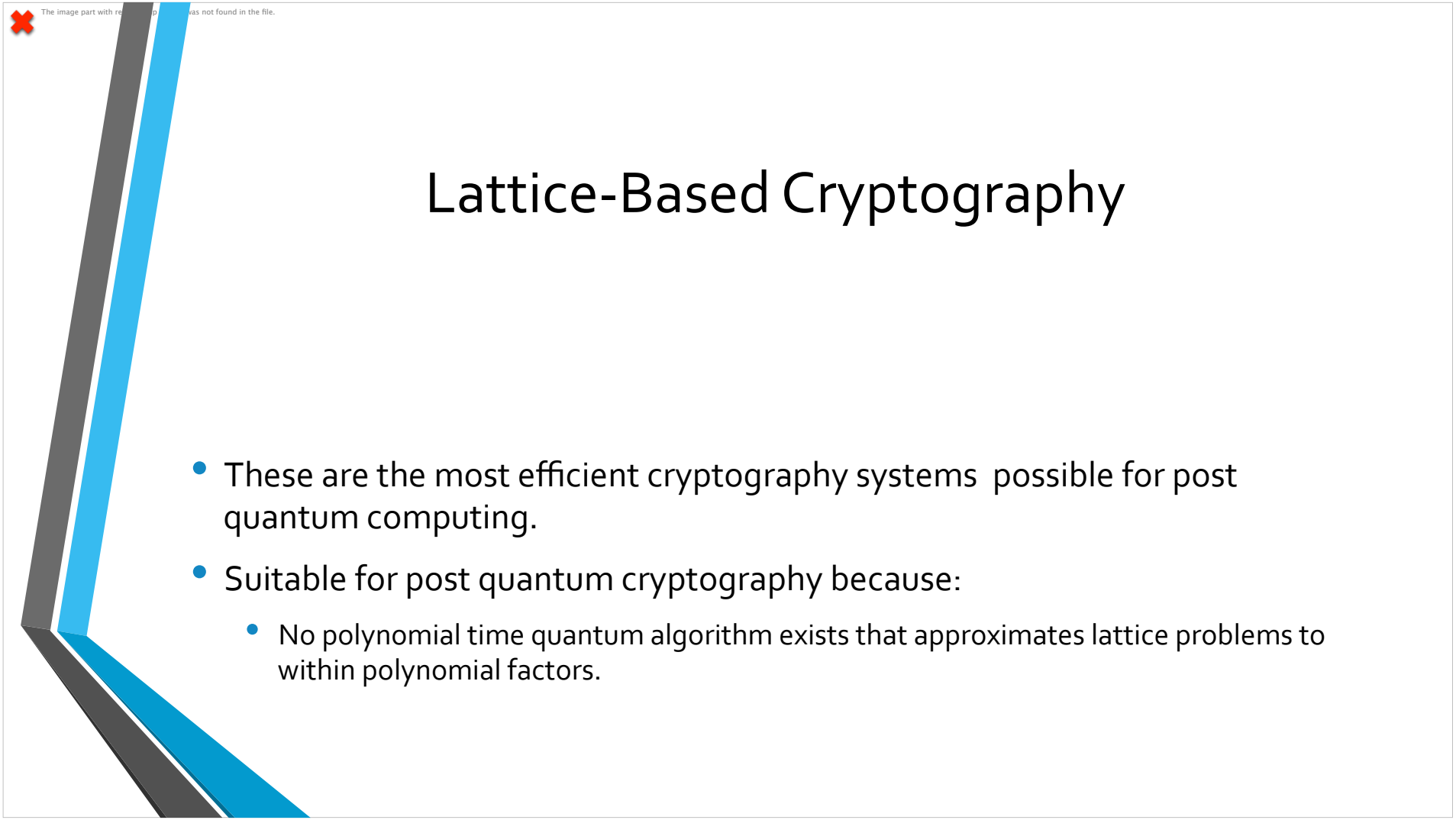
Weaknesses In Quantum Computing

- Must operate at near absolute zero temperature
  - Made up of single atoms that get "knocked around" by stray electrons and photons in the environment.
  - To cut down on the chance of this occurrence, the entire apparatus must be cooled to absolute zero temperature – As cold as outer space.
- Classical and quantum algorithms are not interchangeable
  - Answers are produced in the form of probability
  - Problems are executed thousands of times or more, probability distribution is examined, and values measured accordingly.
- Quantum Decoherence
  - The loss of information into the environment which can occur during entanglement.
  - Coherent states need to be preserved to perform quantum computation.



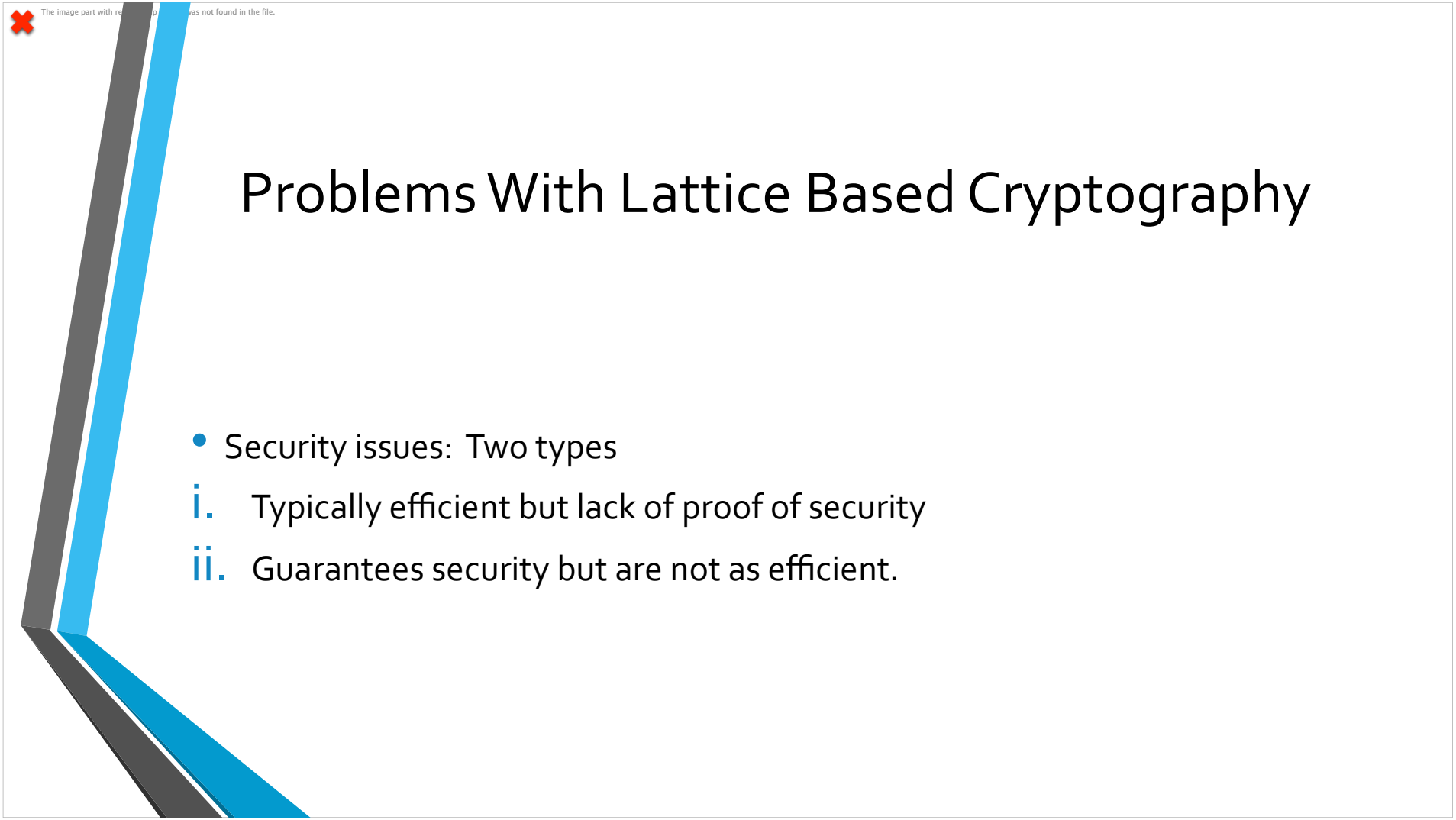
Post-quantum cryptography

- Cryptography solutions after quantum computers become more readily available for general use
- Current cryptography methods that may be resilient to quantum computers
  - Lattice-based cryptography
  - Multivariate cryptography
  - Coding-based cryptography
  - Can be implemented on classical computers.



Lattice-Based Cryptography

- These are the most efficient cryptography systems possible for post quantum computing.
- Suitable for post quantum cryptography because:
  - No polynomial time quantum algorithm exists that approximates lattice problems to within polynomial factors.

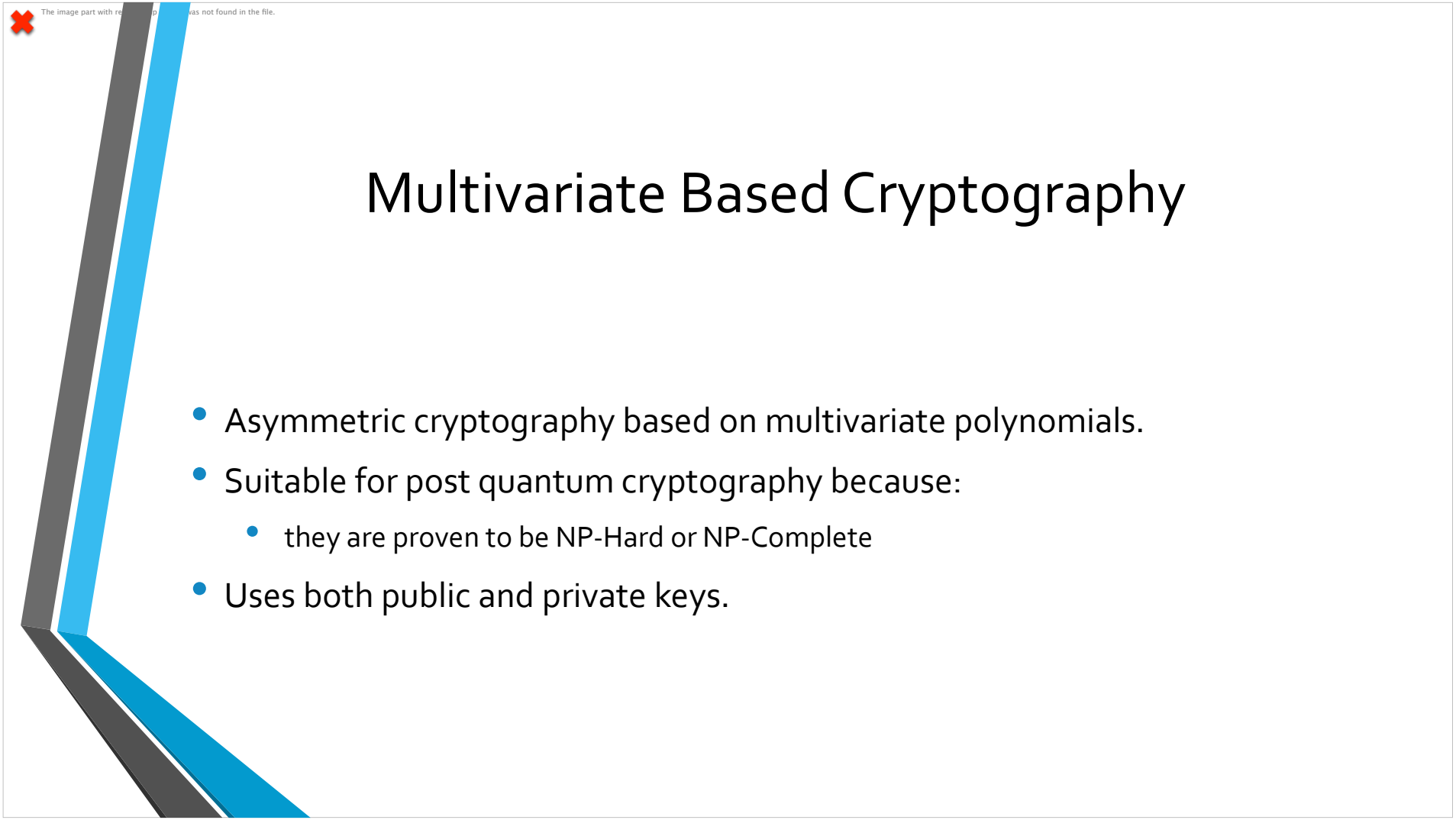


Problems With Lattice Based Cryptography

- Security issues: Two types

i. Typically efficient but lack of proof of security

ii. Guarantees security but are not as efficient.



Multivariate Based Cryptography

- Asymmetric cryptography based on multivariate polynomials.
- Suitable for post quantum cryptography because:
  - they are proven to be NP-Hard or NP-Complete
- Uses both public and private keys.

Problems With Multivariate-Based Cryptography

- Can only be used only for building signatures.
  - Will not protect sensitive data
  - Attempts to implement other encryptions have failed.

Coding-Based Cryptography

- Public-key encryption system

Assumptions	***b* is a power of 2** **$d = \log_2 n$** **$n = 4b \log_2 b$** **$t = 0.5n/d$**
Public Key *K*	***dt* x *n* matrix**
Message *m*	***n*-bit string with exactly *t* bits set to 1**
Encryption	**Multiply *K* by *m***

- Security
  - Though its easy to work backward using linear algebra, it is extremely difficult to find *t*

Problems with Coding-Based Cryptography

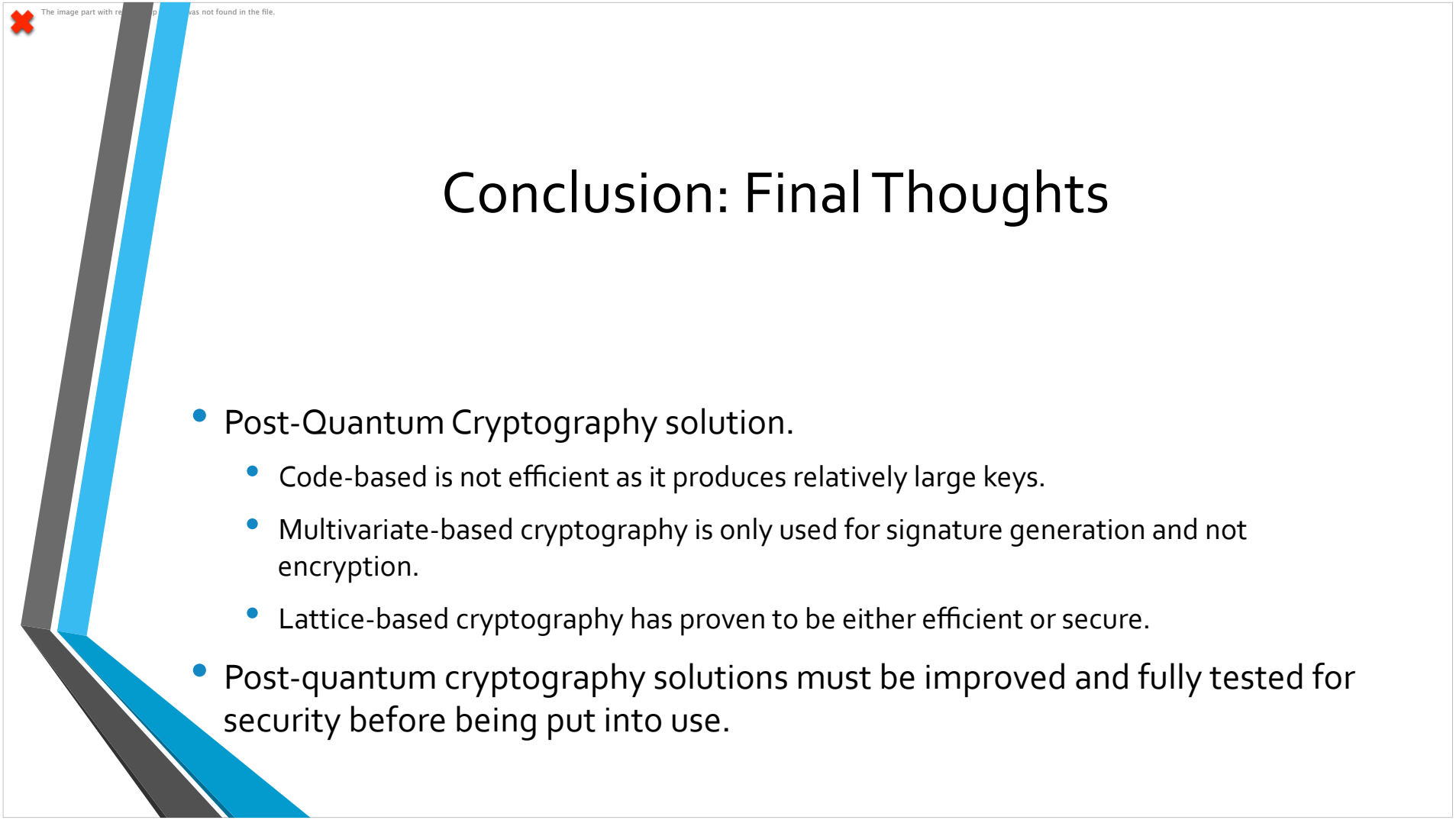
- It is not efficient for post quantum cryptography
  - Requires very large public key
- All the most known hard attacks proved to take more time for attacking a quantum crypto system.

Conclusion: Analyzing the Threat of Quantum Computing

- Hypothesis has not been fully supported by the results of the research
  - Algorithms are not easily interchangeable between classical and quantum computers
  - Algorithms have to be geared toward the environment in which they will execute.
  - Data encrypted using current public-key cryptography must be decrypted and re-encrypted using post-quantum methods.

Conclusion: Analyzing the Threat of Quantum Computing

- Shor's algorithm successfully executed however,
  - High costs of quantum computing prevents malicious actors from obtaining quantum computing resources to use against public key cryptography.
- Hashing algorithms are not threatened by quantum computing.
  - Hash algorithms are used as part of post-quantum cryptography especially in signature generation.



Conclusion: Final Thoughts

- Post-Quantum Cryptography solution.
  - Code-based is not efficient as it produces relatively large keys.
  - Multivariate-based cryptography is only used for signature generation and not encryption.
  - Lattice-based cryptography has proven to be either efficient or secure.
- Post-quantum cryptography solutions must be improved and fully tested for security before being put into use.

Questions?