Build Quantum-Safe Security Protocols

Lily Chen, NIST

ETSI 2nd Quantum-Safe Crypto Workshop

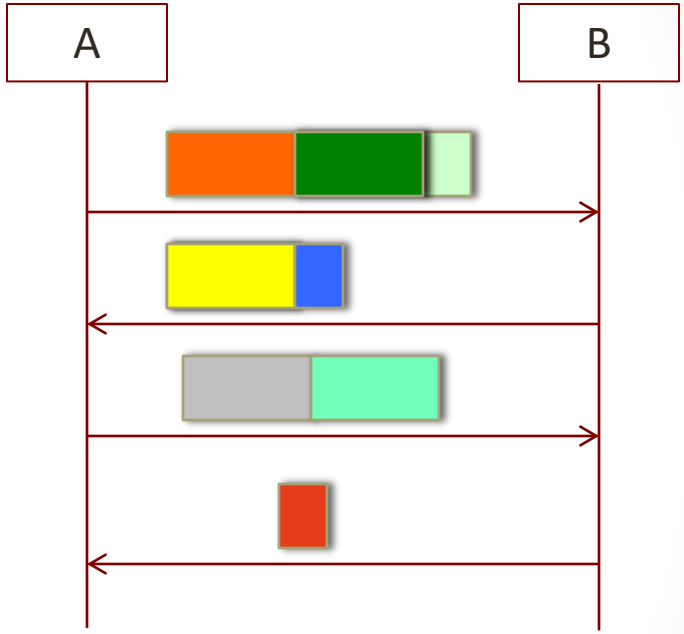
October, 2014

Outline

- The current security protocols
- Possible migration path
- Issues and strategies

Security Protocols

- Security protocols are widely deployed to secure the network and communication systems such as
  - Internet Key Exchange (IKE)
  - Transport Layer Security (TLS)
- When the protocols were designed, it targeted on *accommodating certain cryptographic schemes*
- To build quantum resistant security protocols, can we just replace these schemes with quantum resistant schemes?

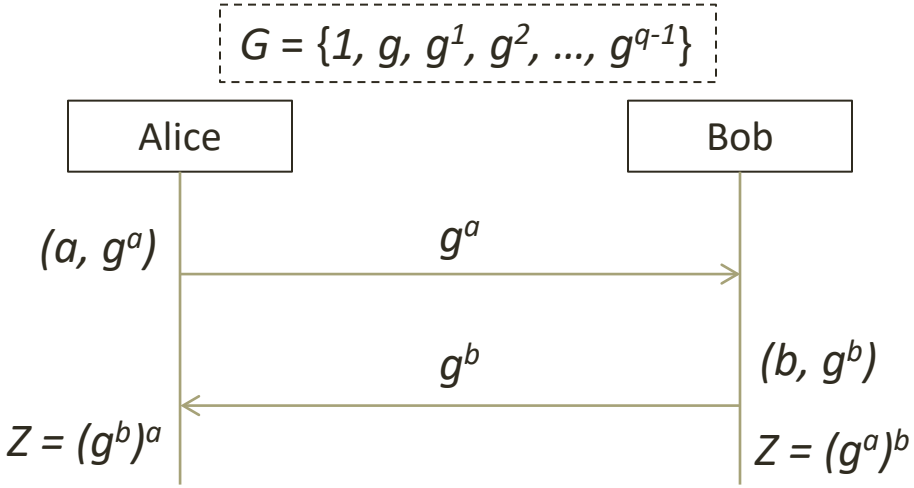


Neither do people pour new wine into old wineskins.

- Matthew 9:17

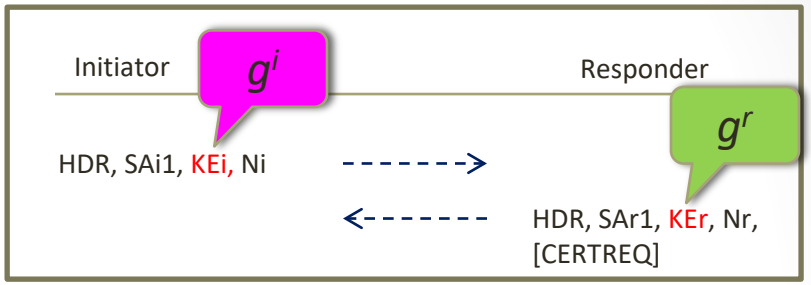
Diffie-Hellman Key Exchange

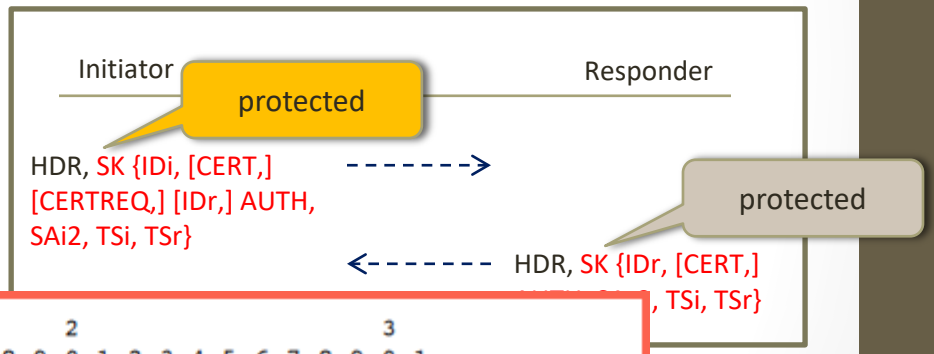
- Symmetric structure
  - Alice and Bob will conduct the same operations
  - Over a set of common parameters
- Perfect forward secrecy
  - When using ephemeral key pairs for each key establishment

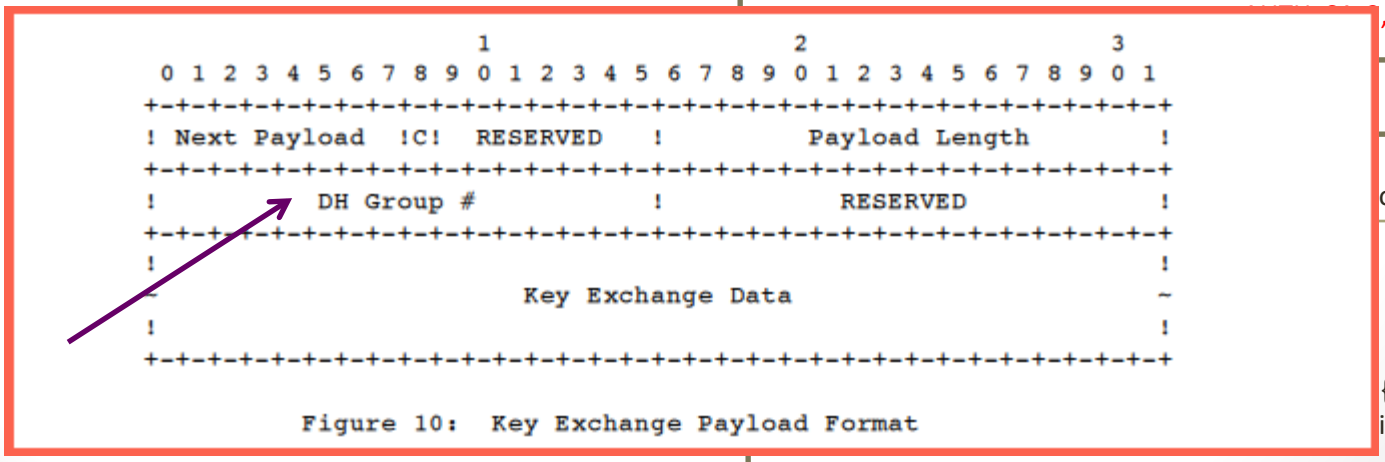


Diffie-Hellman Key Exchange in IKE

- Establish keys between any two IP hosts using Diffie-Hellman key exchange
- An indication for the group (parameters)
- *Internet Key Exchange is indeed Diffie-Hellman Key Exchange for Internet*







```
                    1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
! Next Payload  !C!  RESERVED   !         Payload Length        !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!         DH Group #            !           RESERVED            !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
!                                                               !
~                       Key Exchange Data                       ~
!                                                               !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

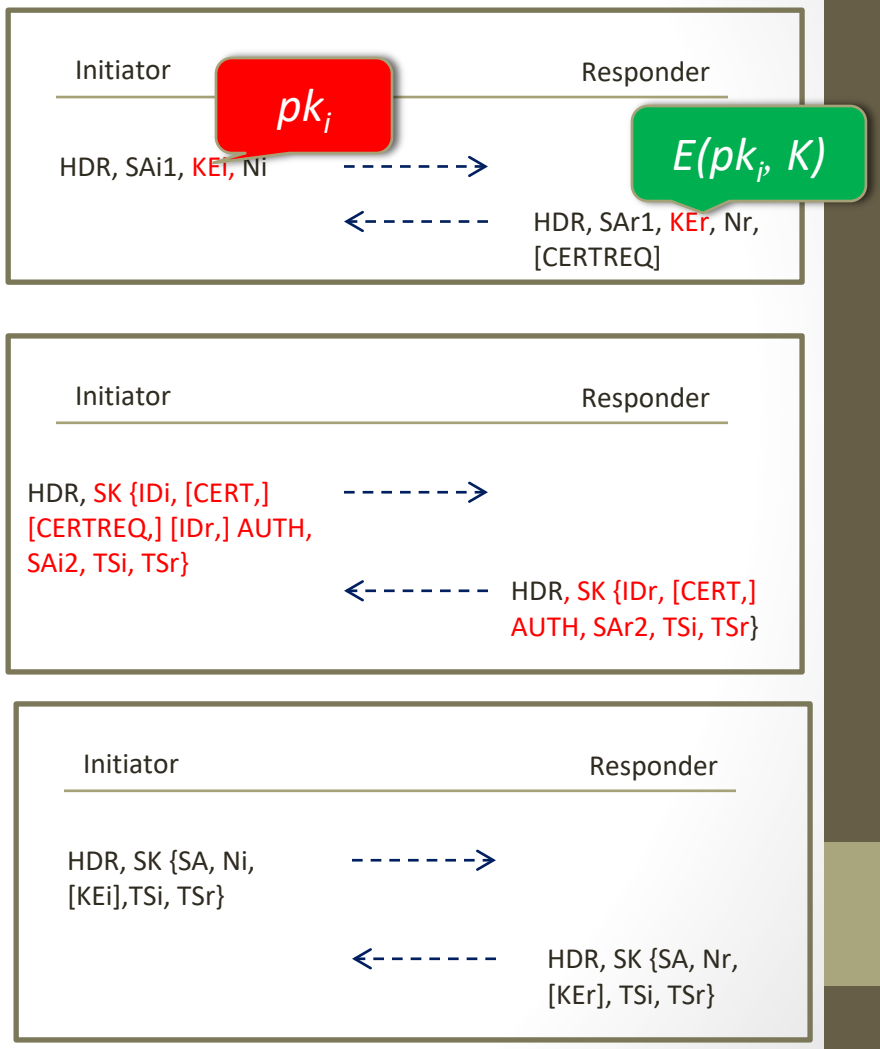
Figure 10: Key Exchange Payload Format

onder

{SA, Nr,
i, TSr}

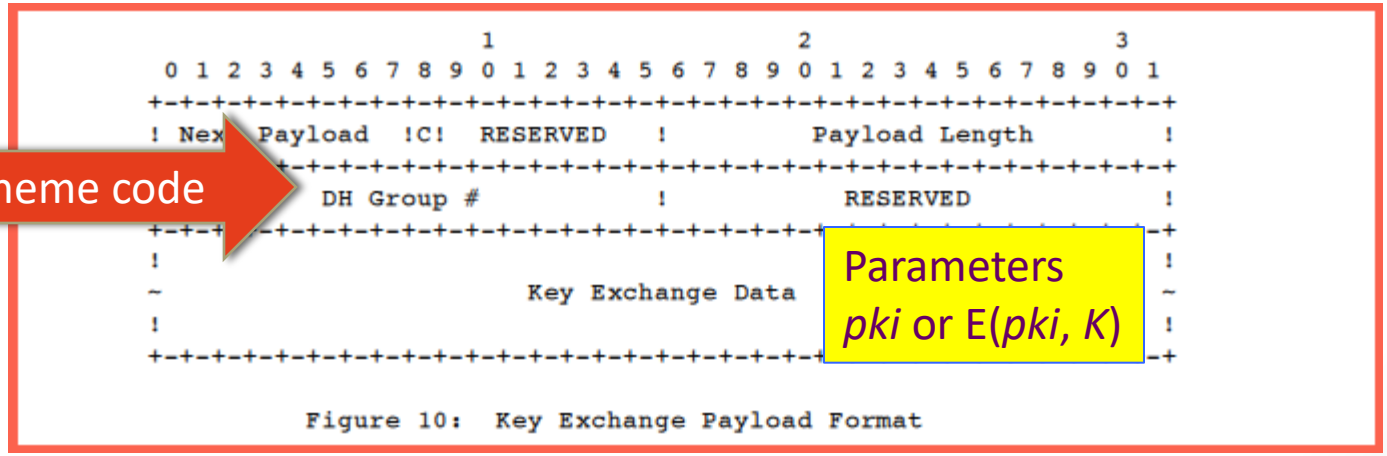
Quantum Resistant IKE

- IKE does not support negotiation of different key establishment schemes
- Currently no exact quantum resistant DH counterpart can be used with symmetry
  - Some key exchange is not as symmetric as DH
- It is very likely that a quantum resistant encryption scheme will be used to establish keys
  - Use one time public key to obtain perfect forward secrecy
  - Require a fast key pair generation



Quantum Resistant IKE Discussion

- Key pair generation with compatible efficiency is possible for quite a few existing quantum resistant schemes
- It lost the symmetric property but security may not be reduced
- The parameters need to be sent, probably together with the public key, which is not accommodated in the current IKE
- It is not straightforward to extend IKE to support multiple schemes
  - Additional extensions are needed

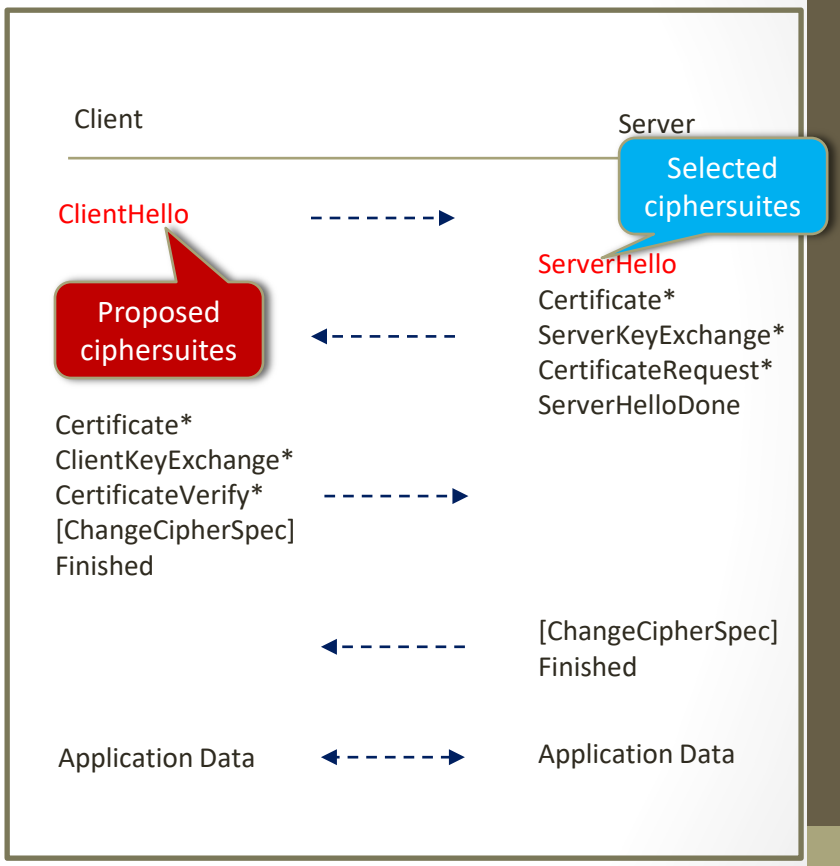


RSA Encryption/Signature

- RSA encryption and signature has a specific asymmetry property when selecting e small, e.g. $e = 2^{16}+1$
  - Light operations using (n, e) for
    - Encryption M^e; and
    - Signature verification S^e, $H(M)$
  - Heavy operations using (d, p, q), where $d \cdot e = 1 \bmod \Phi(n)$ for
    - Decryption C^d; and
    - Signing $H(M)^d$
- Certified RSA public key can be used for authentication
  - Explicitly by signature
  - Implicitly by key confirmation on encrypted key

Transport Layer Security (TLS)

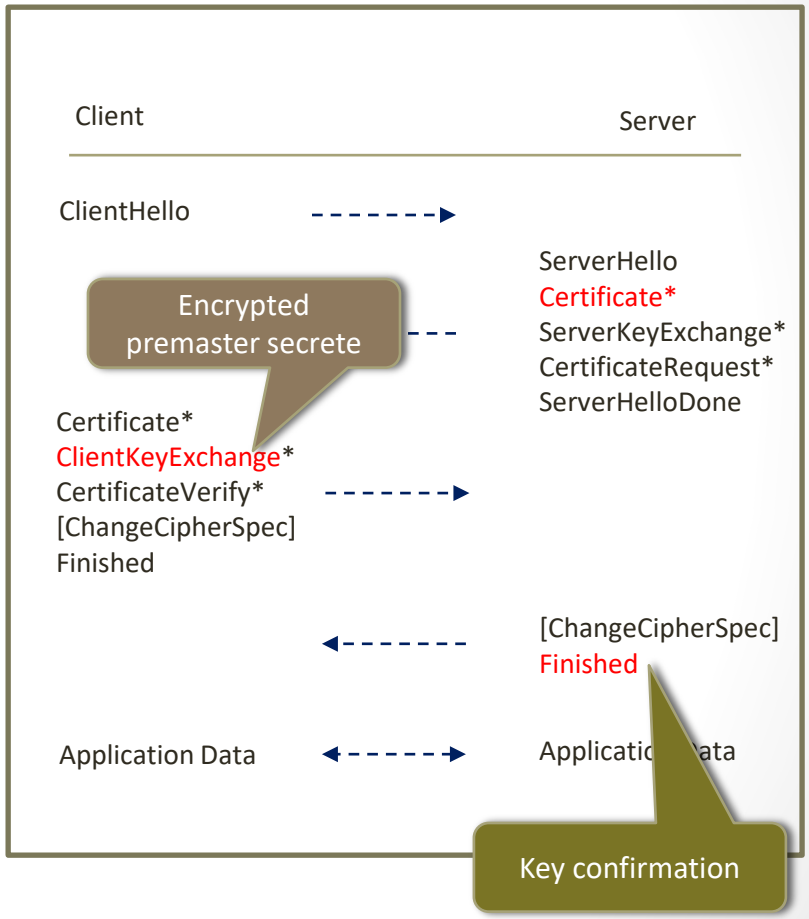
- A protocol between a server and a client
  - In early days, the client can have limited processing capacities
  - The purpose is for a client to securely login an authenticated server
    - Server authentication is required, while client authentication is optional
- Support three major methods for key establishment
  - RSA key transport (most commonly supported)
  - Ephemeral-static DH
  - Ephemeral DH
- TLS support ciphersuite negotiation
  - TLS ciphersuite examples
    - TLS_RSA_WITH_AES_128_CBC_SHA
    - TLS_DH_WITH_AES_128_CBC_SHA
    - TLS_DHE_WITH_RSA_AES_CBC_SHA



TLS 1.2 (or lower version). TLS 1.3 will change the handshake

RSA in TLS

- RSA key transport
  - Client selects a pre-master secret, encrypts with server's certified public key
  - Server conducts implicit authentication by key confirmation
- The server's RSA key is certified
  - The client verifies CA's RSA signature (again, to take advantage of RSA with small "e")



Quantum Resistant TLS

- Introduce quantum resistant ciphersuite, e.g.
  - TLS_NTRU_AES_128_CBC_SHA
- Today's TLS clients may be powerful to handle the processing requirements for PQ crypto schemes
  - Asymmetry for client and server may not be as important as in the early days
- When perfect forward secrecy property is required, TLS needs to adapt to one-time encryption key pair schemes

Possible Migration Path

- High priority: Introduce quantum resistant schemes for key establishment
  - Early migration will provide backward security, i.e. keep confidentiality for the information protected by the old schemes
- For digital signature schemes used for entity authentication, backward security is not required
  - Move to quantum computing resistant signature schemes can identify practical impact
- One step migration is ideal, if we have mature candidates for both encryption (key exchange) and signature

How about Security?

- The security proofs for IKE and TLS were published after they have been deployed
  - with formalized assumptions on the underlying crypto schemes
- The results may not hold with the new schemes
  - That is, new schemes are based on new assumptions
- The security vulnerability may or may not be identified right away
- The extensive research can be motivated by the deployments
  - For possible vulnerabilities, early stage discovery is good and can avoid the disasters
  - The current information system cannot afford disasters

Summary

- The security protocols shall not be considered as old wineskins
- The agility can be introduced, with certain effort
- The practical impact will be more clear when the new schemes are implemented in the protocols
- The trigger for more serious security analysis is the deployment
- We may not know every thing until the new schemes are plugged in
  - We do need to know something to start

NIST Workshop on Cybersecurity in a Post-Quantum World

April 2–3, 2015 in Gaithersburg, Maryland (co-located with PKC, March 30 - April 1, 2015)

- Security of proposed Post-Quantum Crypto schemes
- Impacts to current security protocols
- Challenges in adopting quantum resistant crypto
- Transition strategies to make cyberspace quantum ready

Submission to pqc2015@nist.gov, before Dec.15, 2014