Introduction To KEM-Based Key Exchange

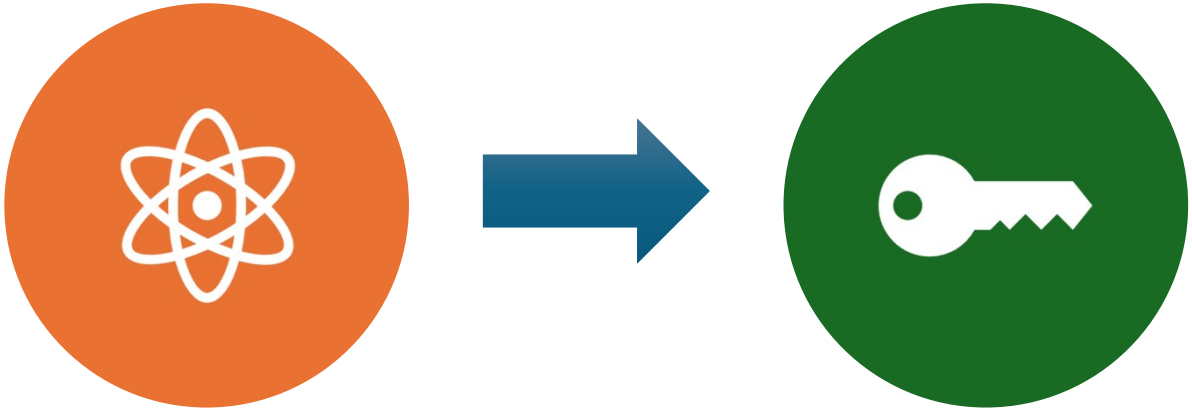
고려대학교 정보보호대학원
Korea University
School of Cybersecurity

Korea University, School of Cybersecurity

Post-Quantum Security and Cryptography Lab.

Prof. Changmin, Lee

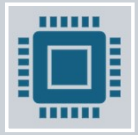
Outlines



POST-QUANTUM THREAT AND
POST-QUANTUM KEY EXCHANGE

PQ KEY EXCHANGE PROTOCOLS:
PQNOISE

1.1 The Post-Quantum Threat



Shor's algorithm breaks X25519 & DH which forms the backbone of current VPN key exchange protocols.

Current cryptography is vulnerable. Quantum algorithms eliminate mathematical hardness assumptions.

Shor's Algorithm: Solves discrete logarithm problem → breaks RSA, ECDH, ECDSA in polynomial time.

Grover's Algorithm: Searches unsorted databases faster → reduces symmetric key security by half.

"Harvest now, decrypt later" attacks already happening.

1.2 Post-Quantum Key Exchange

Lattice-based algorithms (Kyber, etc.) are NIST standardized due to quantum-resistant security guarantees.

- ML-KEM, Kyber, NTRU, etc.

Why Kyber is promising: Module Learning with Errors (MLWE) remains hard even for quantum adversaries.

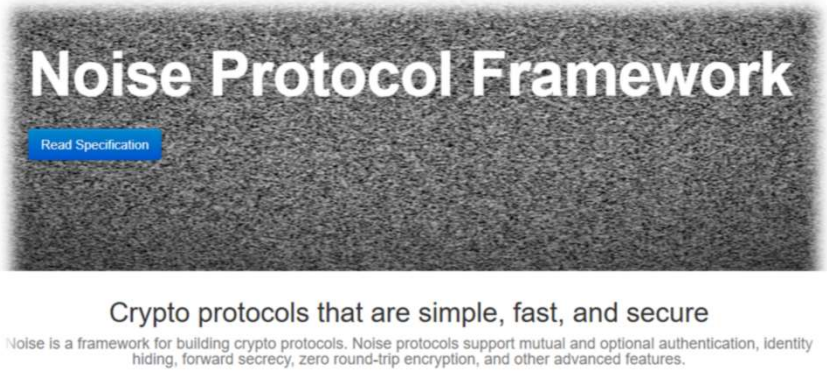
- **Key Sizes**:Kyber-512 (~1,632 bytes), Kyber-768 (~2,400 bytes), Kyber-1024 (~3,168 bytes).
- **Security**: IND-CCA2 secure against quantum attacks.

Alternative: Classic McEliece offers conservative security but impractical sizes.

- Code-based cryptography, public keys ~1MB.

Hybrid approach maximizes security: Classical (X25519, ECC) + Post-Quantum provides protection against both attack vectors.

- Maintains current security assumptions
- Adds quantum resistance



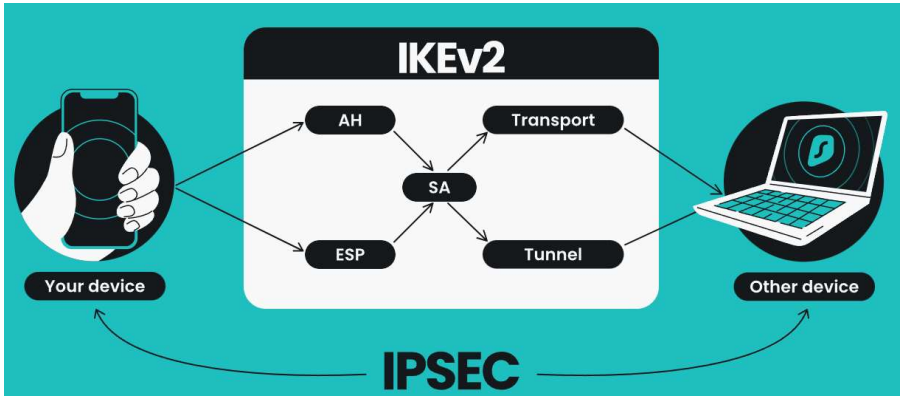
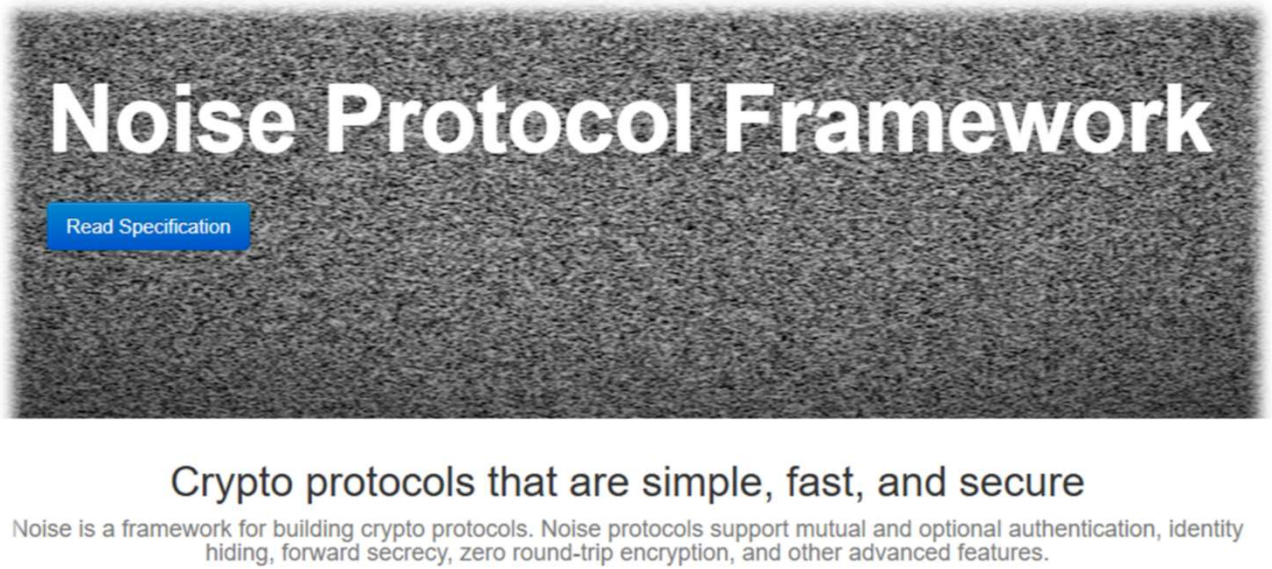


Image source: Surfshark

2.1 Noise Protocol Framework



The Noise Protocol Framework, developed by Trevor Perrin in 2018, is a public domain cryptographic framework for creating secure communication protocols based on **Diffie–Hellman key exchange.**

2.1 Noise Protocol Framework

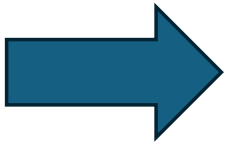
- A framework for crypto protocols based on DHKE
  - Defines 12 patterns: NN, NK, NX, KN, KK, KX, XN, XK, XX, IN, IK and IX.
- Digital signature is not used ➔ easy to achieve deniability
- Combine simple elements to make different protocols
  - Use “sponge-like” symmetric crypto
- Currently used by WhatsApp, WireGuard, Lightning Network, and I2P
- E.g., Noise_IK
  - 1-Round-Trip Time (RTT) protocol
  - **Mutual authentication, forward secrecy**, deniability, identity-hiding, key-compromise impersonation (KCI) resistant

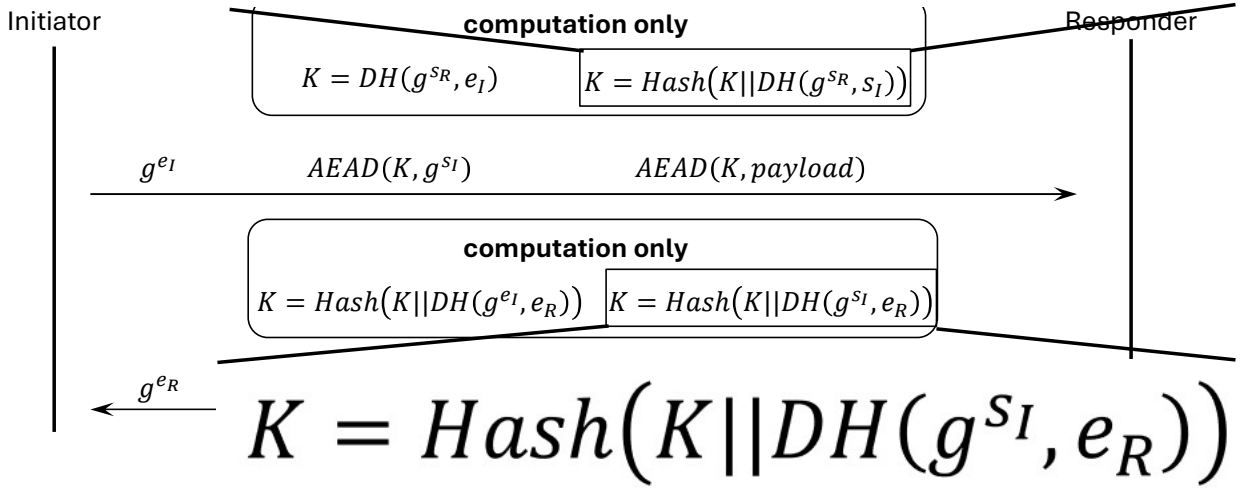
2.1 Noise Protocol Framework

- E.g., Noise_IK
  - I : Static key for initiator Immediately transmitted to responder
  - K : Static key for responder Known to initiator
  - This option satisfies both **mutual authentication**

$$K = Hash\left(K||DH(g^{s_R}, s_I)\right)$$

```
IK
    <- s
    ...
    -> e, es, s, ss
    <- e, ee, se
```





2.2 Migrating to KEM

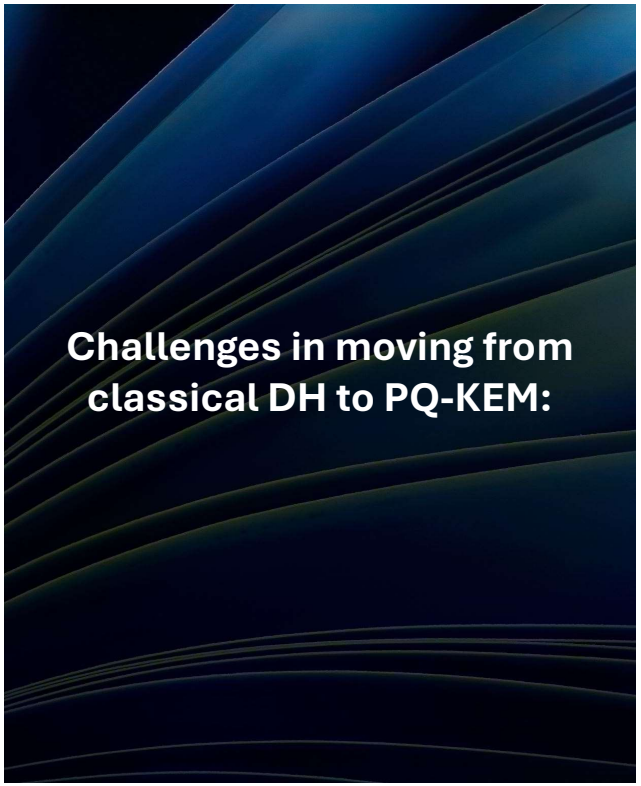
Naïve Replacement is Insufficient:

- Classical protocols like Noise depend on DH properties not directly provided by KEMs.
- PQ-KEMs have fundamentally different operational characteristics (encapsulation/decapsulation).

Required Modifications:

- Changes to key derivation logic to securely integrate KEM outputs.
- Adjustments in handshake patterns to properly authenticate messages.

2.2 Migrating to KEM



Integration Challenges:

- KEM operations are unidirectional (encapsulation vs DH symmetric computation).
- New security models required to handle CPA-secure and CCA-secure KEM differences.

Performance & Size Constraints:

- Larger ciphertext and public key sizes must fit within network MTU limits.
- Computational overhead and latency concerns.

2.3 Post-Quantum Noise Protocol

Post-quantum safe:

- PQNoise replaces Curve25519 with IND-CCA2-secure KEMs.

Handshake Efficiency:

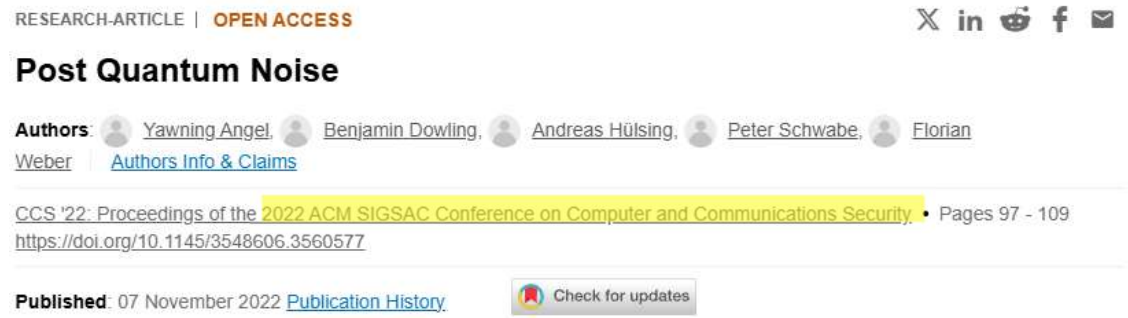
- Maintains 1 RTT where possible, with additional roundtrips as needed.

Security Guarantee:

- Attacker must break KEM assumptions.
- Ensures quantum-resistant confidentiality and authenticity via SEEC and hash-object abstractions.

Packet Size:

- ~3.0KB total, within IPv6 MTU limits (1280 bytes per message).



RESEARCH-ARTICLE | OPEN ACCESS

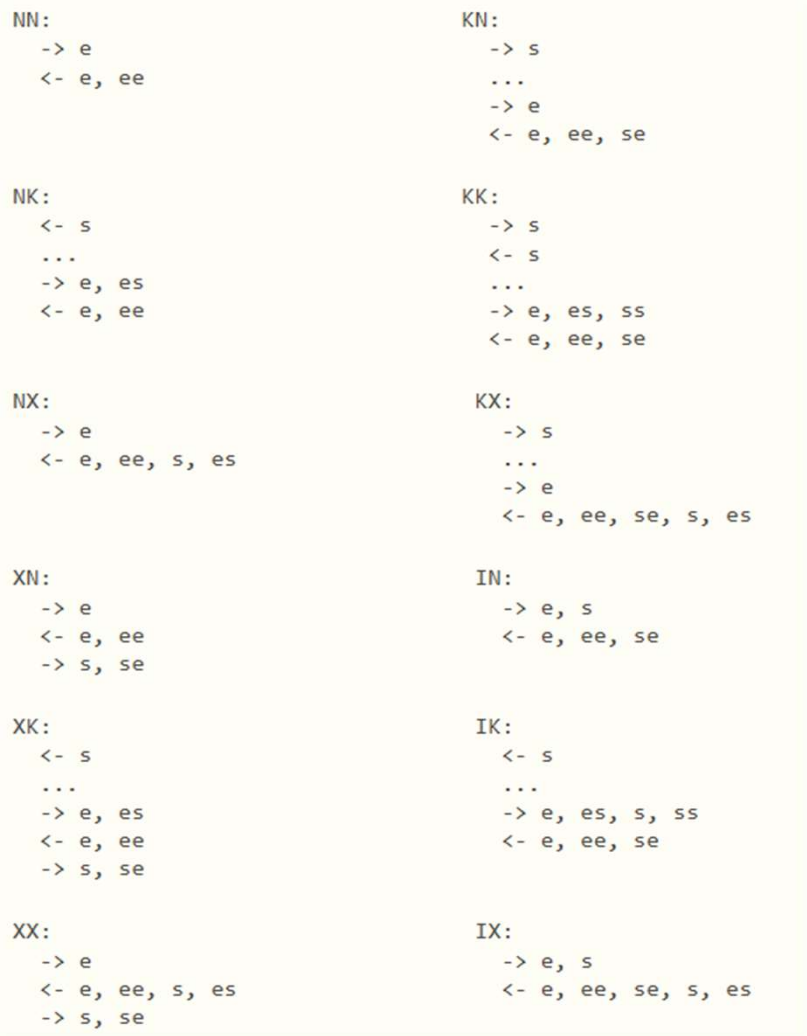
Post Quantum Noise

Authors: Yawning Angel, Benjamin Dowling, Andreas Hülsing, Peter Schwabe, Florian Weber | Authors Info & Claims

CCS '22: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security • Pages 97 - 109
https://doi.org/10.1145/3548606.3560577

Published: 07 November 2022 Publication History | Check for updates

Angel, Yawning, et al. "Post quantum noise." *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM, 2022.



Challenges of PQNoise

- KEMs require interactive challenge-response for authentication due to their unidirectional nature (encapsulation and decapsulation), unlike DH's symmetric key exchange.
- KEMs cannot combine arbitrary keyshares, especially problematic for static-static exchanges, which are common in Noise patterns.
- Noise is extremely flexible and offers a huge amount of possible patterns. Computational security proofs are given for individual patterns which results in a large number of individual security proofs, and many patterns without computational proofs of security.

Solutions of PQNoise

- **Recipe → EKEM / SKEM translation + optional key-confirmation**
  Converts every DH token into a direction-aware encaps/decaps pair; adds ≤1 extra RTT when the sender's *static* key must prove possession, so each PQNoise pattern preserves the same confidentiality + authenticity guarantees as its DH parent.
- **Static–ephemeral entropy combination (SEEC)**
  Generalises the NAXOS trick: fold a party's static secret into the randomness of its encapsulation, so the derived key is hidden if *either* the fresh nonce or the static key remains secret, eliminating the need for a separate static-static exchange.
- **Hash-object abstraction → single generic proof**
  Replaces "hash this list of DH outputs" with a stateful object whose outputs stay pseudorandom once any unknown input is mixed in. This strips pattern-specific DH algebra from the analysis, allowing one computational proof (in a lightly tweaked fACCE model) to cover **all PQNoise protocols**, including hybrids.

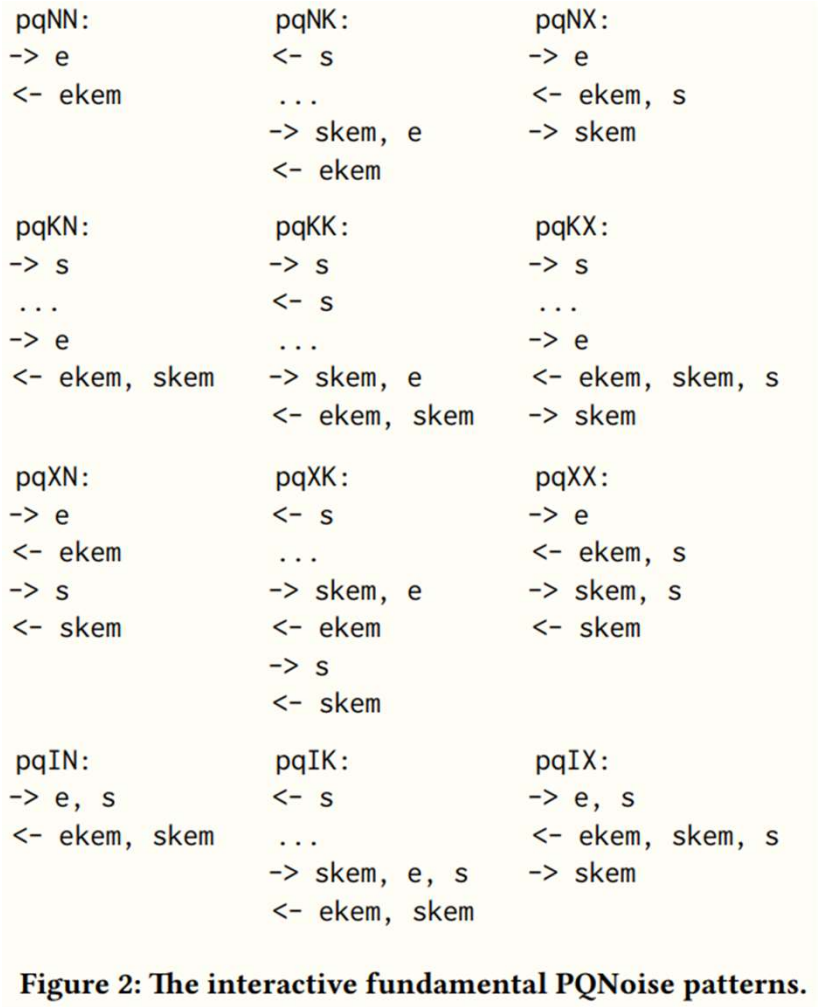


Figure 2: The interactive fundamental PQNoise patterns.

Solutions of PQNoise

- PQNoise handshakes stay safely below common IPv4/IPv6 path-MTU limits
  - **“One-ciphertext-per-flight” rule**
    The generic EKEM / SKEM translation emits *at most one* PQ ciphertext in any single Noise message.
  - **Responder static key is not transmitted**
    PQNoise patterns assume the server’s post-quantum static public key is pinned out-of-band (exactly like a WireGuard public key).
  - **Size-tuned reference suite**
    PQNoise standardises on Kyber-512 (or hybrid X25519 + Kyber-512) for all “fundamental” patterns; larger KEMs are left to future profiles so that today’s baseline fits even constrained IoT uplinks.

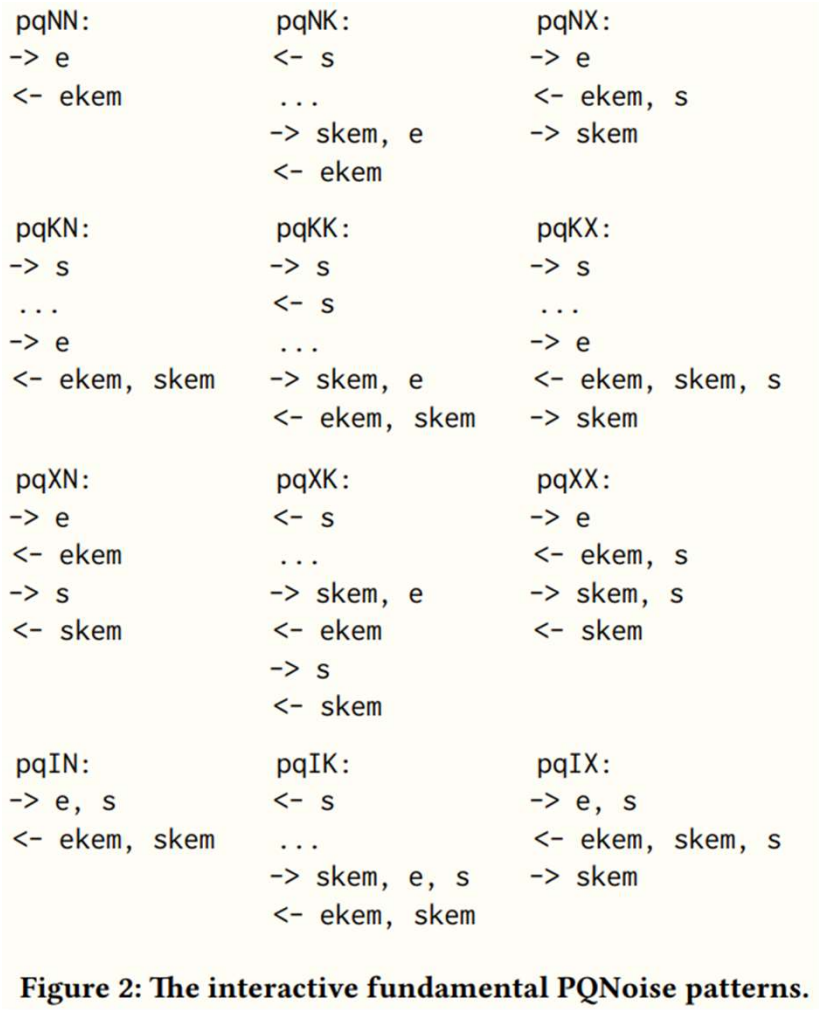
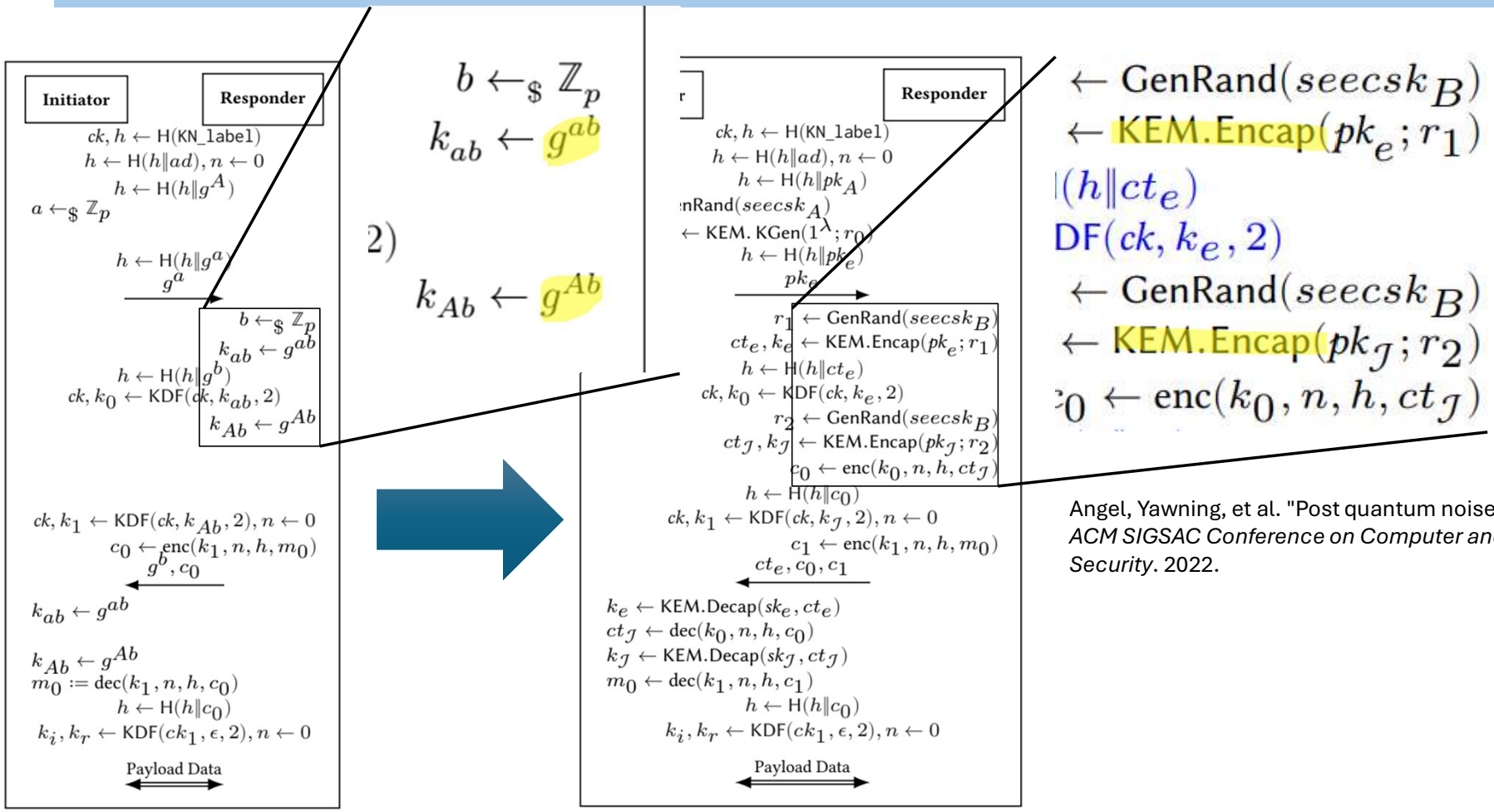


Figure 2: The interactive fundamental PQNoise patterns.

2.3 Post-Quantum Noise Protocol



Angel, Yawning, et al. "Post quantum noise." *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. 2022.

Q&A