On Key Generation Schemes with QKD for applications

PRESENTER: **Andrey** Zhilyaev
Andrey.Zhilyaev@infotecs.ru

Problems:

- QKD protocol consumes keys to generate quantum keys (QK)
- Some systems further use quantum keys to generate working keys (K)
- What is the best way to use one keys to generate another keys and improve the key stream properties?

Our Proposal:

- The hybridization of quantum keys and classical pre-shared keys to construct the optimal key generation and distribution scheme (KGDS)
- Use the best properties of both classic and quantum key generation schemes
- Computation secure MAC can be used for QKD authentication for low speed QKD devices

Approach to analyze KGDS:

- **Cryptographic properties**
  - Impersonation attack on Authentication key
  - Known-text attack on Authentication key
  - Known text attack on Working key
  - An influence of an untrusted courier
  - Consequences of the attacks
- **Operational properties**
  - Initialization problems
  - Key storage problems
  - Key synchronization problems

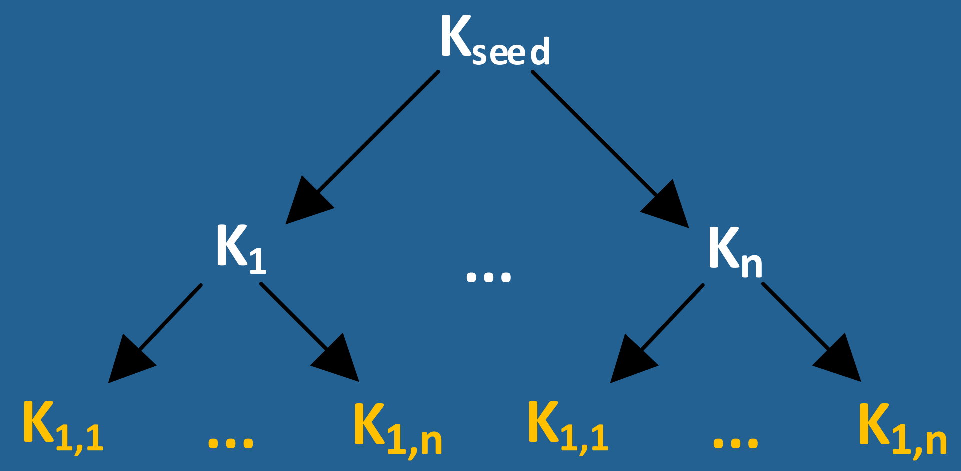
Hybrid KGDS Advantages:

- Perfect forward secrecy can be achieved
- Hybrid Schemes more resistant against considered attacks
- An adversary have limited time to perform an attack
- Partial compromise of generated keys
- An untrusted courier have significantly complicated attack conditions

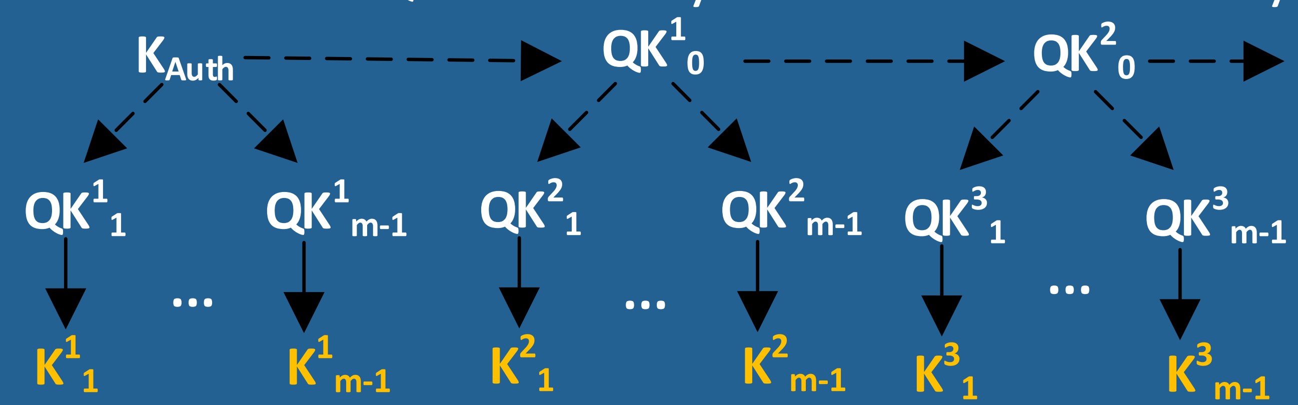
Wherein

- MAC length must be at least equal to the length of the key
- Order of QK usage is important
- Loss of the key synchronization may lead to irreversible problems

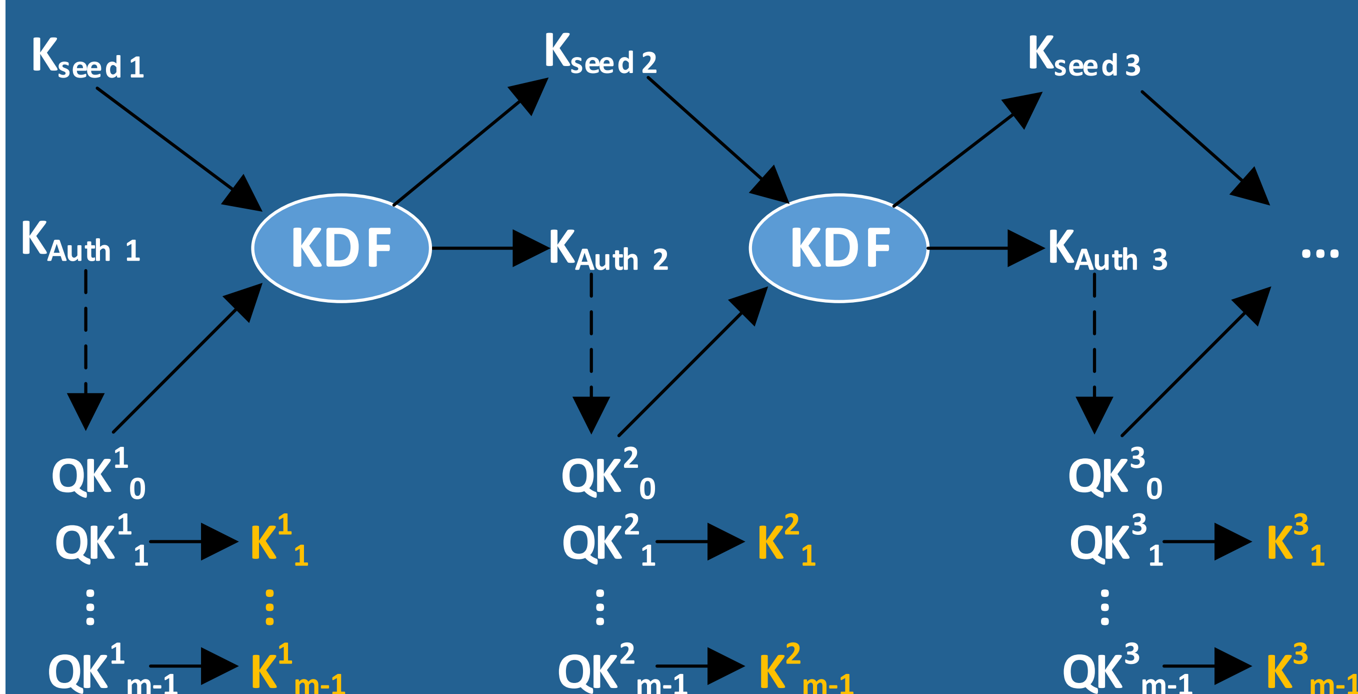
1. KGDS without QK – Key Tree



2. KGDS – First Quantum Key for Authentication Key



3. Hybrid KGDS – Classic + Quantum Key Scheme



Key Generation and Distribution Schemes

Perfect Forward Secrecy Property

KGDS	**Perfect forward secrecy**
Without QK	No
QK for KAuth	Yes
Hybrid KQDS	Yes

Key Compromise Consequences

KGDS	**Key Compromise**
Without QK	Compromise of one derived key compromise all keys
QK for KAuth	• Compromise of QK used for K_{Auth} compromises all QK generated with authentication on this K_{Auth} • Compromise of K_{Auth} before first QKD session on this K_{Auth} compromises all keys • Compromise of K_{Auth} after first QKD session on this K_{Auth} compromises all QK generated with authentication on this K_{Auth}
Hybrid KGDS	• Compromise of K_{Auth} compromises all QK generated with authentication on this K_{Auth} • Compromise of K_{seed} and QK_0 (or K_{Auth}) compromises all keys except previous generated QK

Best Attack Probabilities

KGDS	**MAC length 128 bit**	**MAC length 256 bit**
Without QK	2^{-199}	2^{-199}
QK for K_{Auth}	2^{-125}	2^{-215}
Hybrid Scheme	2^{-125}	2^{-215}

Best Attack Consequences

KGDS	**Best attack consequences**
Without QK	All keys are compromised
QK for K_{Auth}	All further keys are compromised. Already generated keys stay secret
Hybrid Scheme	Only keys generated with authentication on recovered K_{Auth}

Mikhail Borodin,
Alexey Urivskiy and
Andrey Zhilyaev

infotecs