

HB-TS-QKD-01, Quantum Key Distribution for Interplanetary Cryptographic Security

Heidenbillg: Technology division

February 2026

Abstract

This technical report details the implementation of the **HB-TS-QKD-01** protocol, a quantum-secure communication framework designed for high-latency, high-loss interplanetary optical links. We analyze the convergence of the *BB84* protocol with decoy-state modulation and the mitigation of decoherence in deep-space environments. The document establishes the cryptographic baseline for the *HEIDENBILLG_OS* network across the *HB_01-07* sectors, ensuring absolute secrecy against post-quantum computational threats.

1 Introduction

Interplanetary communication is inherently vulnerable to "Eavesdrop-and-Forward" (EF) attacks. Conventional RSA or Elliptic Curve Cryptography (ECC) relies on the computational difficulty of prime factorization or discrete logarithms—problems that are solvable via Shor's algorithm on a sufficiently large quantum computer.

The **HB-TS-QKD-01** protocol bypasses these vulnerabilities by utilizing the fundamental laws of physics. Any measurement by an unauthorized observer (Eve) inevitably collapses the wave function of the signal, introducing a detectable error rate. This allows the *Tech_Sys* division to guarantee that the cryptographic keys have not been compromised during transit between planetary nodes.

2 Quantum Channel Dynamics and State Preparation

The secure key is encoded in the polarization states of single photons. In the HB-TS configuration, a Spontaneous Parametric Down-Conversion (SPDC) crystal generates en-

tangled photon pairs at 1550 nm.

2.1 Basis Selection and Sifting

Two non-orthogonal bases are used: the rectilinear basis \oplus (horizontal $|H\rangle$ and vertical $|V\rangle$) and the diagonal basis \otimes ($|+45^\circ\rangle$ and $|-45^\circ\rangle$). The transmitter (Alice) sends a sequence of qubits:

$-\psi\rangle_{Alice} = \sum_i \alpha_i |0\rangle_B + \beta_i |1\rangle_B$ where $B \in \{\oplus, \otimes\}$. Upon reception, the receiver (Bob) selects a basis at random. The "sifting" process then occurs over a classical authenticated channel, where only the events with matching bases are retained.

3 Deep Space Decoherence and Signal Loss

Communication over distances > 0.5 AU (Astronomical Units) introduces severe signal attenuation due to beam divergence and interstellar dust scattering.

3.1 The Channel Loss Model

The total transmission efficiency η_{total} is modeled as:

$$\eta_{total} = \eta_{atm} \cdot \eta_{diff} \cdot \eta_{det} \quad (2)$$

where η_{diff} (diffraction loss) follows the Rayleigh-Sommerfeld integral. For a transmitter aperture D_{tx} and receiver D_{rx} , the loss scales with λL . In the *HB-04* sector (vacuum), $\eta_{atm} = 1$, but the "pointing-and-tracking" jitter becomes the dominant error source.

3.2 Quantum Bit Error Rate (QBER)

The QBER is defined as the ratio of erroneous bits to the total bits received:

$$QBER = \frac{R_{false}}{R_{true} + R_{false}} \approx \frac{1}{2} \frac{p_{dark} + \eta_{sys} p_{noise}}{\eta_{channel}} \quad (3)$$

where p_{dark} is the dark-count rate of the Superconducting Nanowire Single-Photon Detectors (SNSPDs). The **HB-TS-QKD-01** protocol requires $QBER < 11\%$ to proceed with Information Reconciliation.

4 Information Reconciliation and Privacy Amplification

Once a raw key is established, it must be "cleaned" of errors introduced by the channel.

4.1 The Cascade Protocol

We implement a modified Cascade algorithm that performs multiple passes of parity checks over blocks of increasing size. The efficiency $f(QBER)$ determines the amount of classical information leaked during this process:

$$leak_{IR} = f(QBER) \cdot H(QBER) \quad (4)$$

where H is the binary entropy function.

4.2 Privacy Amplification (PA)

To eliminate any partial knowledge Eve might have gained, the key is compressed via Universal Hashing. The final secret key length S is given by:

$$S \approx n[1 - H(QBER)] - leak_{IR} - \log_2 \left(\frac{2}{\epsilon_{sec}} \right) \quad (5)$$

with $\epsilon_{sec} = 10^{-15}$ representing the security parameter for Level 7 clearance.

5 Relativistic Timing and Gravitational Compensation

In interplanetary scenarios, the relative motion between stations (e.g., Earth and a Mars-orbiting HB-OS node) causes significant Doppler shifts and time dilation.

5.1 Synchronous Time-Binning

The time-stamping of photons must be corrected using the Schwarzschild metric to account for gravitational time dilation near planetary bodies:

$$\tau = \int \sqrt{1 - \frac{2GM}{rc^2} - \frac{v^2}{c^2}} dt \quad (6)$$

This ensures that Alice and Bob remain within the 100-picosecond coincidence window required for valid qubit correlation.

6 Experimental Simulations and Results

Simulations for a 1.5 AU link (Earth to Mars at aphelion) utilizing a 10W laser source and a 1.2m receiver array yield the following performance metrics:

Parameter	Metric	Value
Raw Key Rate	R_{raw}	15.4 kbps
Sifted Key Rate	R_{sift}	7.2 kbps
Final Secret Key Rate	R_{sec}	1.1 kbps
System QBER	Q_s	2.45 %
Decoherence Factor	Γ	0.012

Table 1: HB-TS-QKD-01 Performance under Interplanetary Conditions.

7 Conclusion

The **HB-TS-QKD-01** protocol provides a robust, physics-based security layer for the *HEIDENBILLG_OS*. By integrating relativistic corrections with decoy-state QKD, we achieve stable cryptographic links even across the vast distances of the *HB_01-07* sectors. This ensures that all classified technical data remains impenetrable to any current or future decryption technology.

Technical Appendix: Hardware Stack

The implementation requires the following hardware configuration:

- **Source:** 1550nm CW Laser with EOM-based decoy-state modulation.
- **Detection:** SNSPD arrays cooled to 2.1 K.
- **Timing:** Hydrogen Maser Clock with $< 10^{-16}$ stability.
- **Buffer:** Cryogenic Quantum RAM for delay-tolerant sifting.