

Physics-Guided Security-Aware Co-Design of SAC-OCDMA Links with Design-Held-Out SSFM Validation

Mohamed M. Shukra

Moh.M.Shukra@Fezzanu.edu.ly

Acharya Nagarjuna University

G. Prathibha

Acharya Nagarjuna University

Research Article

Keywords: SAC-OCDMA, optical physical-layer security, multi-objective co-design, split-step Fourier method, surrogate-assisted Optimisation, OptiSystem

Posted Date: October 22nd, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11201204/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License. [Read Full License](#)

Additional Declarations: No competing interests reported.

Abstract

Secure spectral-amplitude-coded optical code-division multiple access (SAC-OCDMA) requires jointly designing code structure, transmission resources, Bob-side propagation margin, and a declared Eve model. This paper presents a physics-guided multi-objective framework that selecting code length, code weight, user load, per-user launch power, transmission distance, channel spacing, and Fibre dispersion. The workflow audits 48 structural designs, screens 3,450 resource points under eavesdropper (Eve) budgets of up to 10^6 guesses, uses a stratified 108-point split-step Fourier method (SSFM) data set with design-held-out validation, and enumerates 25,092 supported candidates. Of these, 5,198 satisfy the calibrated constraints, and 96 are Pareto-optimal before auditing. A targeted 39-point audit produces 28 direct passes. All three adaptive-rescue evaluations pass and recover the single failed Pareto role. Final synthesis produces 15 unique directly audited Pareto points and 25 objective-role assignments across five feasible distance-dispersion scenarios. The common secure-reliable boundaries, from direct SSFM at the legitimate receiver (Bob) and analytical Eve constraints, are 65 km at $D = 2 \text{ ps}/(\text{nm} \cdot \text{km})$ and 55 km at $D = 17 \text{ ps}/(\text{nm} \cdot \text{km})$. Multi-slot, multi-seed, propagation-step, and bit-window qualification accepts all 27 final Pareto/boundary points. A 512-bit production window is selected against a 1024-bit reference for the identified bit-sensitive point. Eve-side quantities remain analytical under the stated overlap and guess-budget model. A separate four-wavelength, check at 39 km shows receiver response to matched and mismatched delay patterns. This reduced check does not validate the multiuser search space or establish cryptographic secrecy. The results support surrogate models for screening and ranking, while final threshold decisions remain subject to direct SSFM and explicit convergence control.

1. Introduction

Optical code-division multiple access (OCDMA) supports asynchronous user access through code-domain separation. In spectral-amplitude coding (SAC), each authorized user occupies a code-specific set of wavelength chips and the receiver correlates the received spectrum with the intended signature. Code families and subtraction receivers have been developed to suppress multiple-access interference, phase-induced intensity noise, excessive cardinality, and implementation complexity (Kavehrad and Zaccarin 1995; Wei et al. 2001; Wei and Ghafouri-Shiraz 2002; Djordjevic and Vasic 2003; Aljunid et al. 2004; Penon et al. 2007; Salehi 2007; Hasoon et al. 2008; Anuar et al. 2009; Noshad and Jamshidi 2010). These improvements do not, by themselves, establish a quantitative physical-layer security claim; the code structure, the eavesdropper's observation model, and Bob's post-propagation margin must be assessed together.

An unauthorized receiver may observe occupied wavelengths, test candidate codewords, or exploit repeatable spectral or temporal structure. Reconfigurable coding and optical-domain security mechanisms can increase Eve's uncertainty (Jiang et al. 2006; Wu et al. 2006; Chang et al. 2007; Bakarman et al. 2010); however, this protection is only meaningful relative to a specific eavesdropping capability – how much Eve can observe and how many codewords she can test. We therefore combine constant-weight overlap statistics with expected information leakage, positive-leakage probability, secure-reliable probability, and full-code-recovery probability in one declared threat model.

The link variables are strongly coupled. Increasing launch power can initially improve receiver margin and then intensify self-phase modulation, cross-phase modulation, and four-wave mixing. Narrower channel spacing improves nominal spectral efficiency but increases inter-channel interaction. Longer signatures enlarge the occupied spectral span, while larger user loads increase both aggregate throughput and total launch power. Full-

resolution SSFM over the entire joint code-resource domain is therefore computationally prohibitive and requires controlled propagation-step and spectral-resolution settings (Sinkin et al. 2003; Zhang and Hayee 2008; Deiterding et al. 2013; Musetti et al. 2018).

Semi-analytical equations first exclude invalid, insecure, or clearly unreliable candidates; SSFM supplies high-fidelity labels on a stratified multi-design subset; physics-feature-based quadratic-ridge surrogate models operate only within the supported domain; exact non-dominance testing ranks the finite candidate set; and direct SSFM audits the final Pareto and distance-boundary decisions. The multi-objective and surrogate components are informed by foundational Optimisation and calibration work (Kennedy and O'Hagan 2001; Deb et al. 2002; Forrester et al. 2008), SAC-OCDMA performance analysis (Shi and Ghafouri-Shiraz 2016), and transferable WDM/QoT modelling studies (Nallaperuma et al. 2023; Souza et al. 2023; Gan et al. 2024; Souza et al. 2025). Here, physics-guided denotes this bounded allocation of authority across the full decision chain, as summarized in Fig. 1.

This study extends our previous single-reference-design investigation (Shukra and Prathibha 2026). The earlier work fixed $L = 64$, $K = 16$, and $w = 4$ and used targeted SSFM simulations to identify operating ranges for that configuration. The present work compares multiple code structures, jointly optimizes coding and transmission resources, validates surrogates with complete design hold-out, enumerates 25,092 supported configurations, directly reconstructs the final Pareto set, and subjects every reported Pareto/boundary point to multi-Realisation robustness and numerical-convergence qualification. The operating boundaries reported here are therefore produced by the new co-design pipeline rather than transferred from the earlier study.

To provide an independent implementation-level check without conflating it with the SSFM Optimisation, a reduced OptiSystem 23.0 demonstrator is also reported. It transports one NRZ stream over four WDM carriers and tests matched versus deliberately mismatched delay decoding at a fixed link condition. This limited check is complementary evidence for receiver logic and does not reproduce the multiuser SAC-OCDMA candidate space, the analytical Eve model, or the direct SSFM performance frontier.

The principal contributions are:

1. A finite joint design space spanning code length, code weight, user load, launch power, distance, channel spacing, and Fibre dispersion, with explicit structural and numerical-support constraints.
2. A quantitative eavesdropping model based on constant-weight overlaps and a maximum budget of 10^6 guesses, with declared thresholds on information leakage, positive leakage, secure-reliable probability, and full-code recovery.
3. A 108-point multi-design SSFM data set with design-held-out validation, physics-feature-based quadratic-ridge surrogate modelling, and explicit separation between screening predictions and final direct SSFM confirmation.
4. Exact enumeration of 25,092 supported candidates, avoiding stochastic optimizer dependence and producing an auditable Pareto set.
5. Direct targeted audit, adaptive rescue, and scenario/boundary synthesis yielding 15 unique Pareto points, 25 recommendation roles, and common 65/55-km boundaries.
6. A final multi-slot, multi-seed, propagation-step, and bit-window qualification in which all 27 reported Pareto/boundary points satisfy the predefined computational robustness criteria.

A scoped independent OptiSystem implementation-level check that verifies matched-versus-mismatched delay decoding in a 4-wavelength, single-stream WDM Realisation, with an explicit positive-control test for Eve.

2. Research Gap and Related Work

SAC-OCDMA research has established code constructions and subtraction receivers with increased cardinality and reduced MAI/PIIN (Wei et al. 2001; Wei and Ghafouri-Shiraz 2002; Djordjevic and Vasic 2003; Aljunid et al. 2004; Penon et al. 2007; Hasoon et al. 2008; Anuar et al. 2009; Noshad and Jamshidi 2010), while security studies have shown exposure to spectral observation and code estimation and have proposed reconfigurable coder/decoder and hybrid-sequence mechanisms (Jiang et al. 2006; Wu et al. 2006; Chang et al. 2007; Bakarman et al. 2010). Optimized and symmetrized SSFM schemes clarify the need to control propagation step and spectral resolution (Sinkin et al. 2003; Zhang and Hayee 2008; Deiterding et al. 2013; Musetti et al. 2018). Foundational Optimisation and surrogate-modelling methods (Kennedy and O'Hagan 2001; Deb et al. 2002; Forrester et al. 2008) and SAC-OCDMA-specific performance analysis (Shi and Ghafouri-Shiraz 2016) motivate the finite co-design formulation; recent WDM/QoT studies (Nallaperuma et al. 2023; Souza et al. 2023; Gan et al. 2024; Souza et al. 2025) provide transferable methodology rather than direct SAC-OCDMA security evidence. The unresolved problem is their evidence-preserving integration: security screening must be coupled to link physics; data leakage across code designs must be prevented during validation; the finite supported domain must be enumerated rather than sampled opportunistically; and final Pareto and boundary decisions must be re-simulated and numerically qualified. The present work addresses this gap with an end-to-end, claim-traceable decision architecture.

3. System and Threat Model

3.1 SAC-OCDMA Framework

Each authorized transmitter uses a binary spectral signature of length L (chips) and weight w (occupied chips). For an admitted design, K simultaneous users occupy disjoint or controlled-overlap chip positions. Each user transmits at $R_b = 10 \text{ Gb/s}$; the uncoded aggregate rate is therefore $K R_b$. Secure aggregate throughput is weighted by the minimum secrecy-capacity factor under the strongest evaluated Eve budget.

Bob performs code-matched spectral selection, direct photodetection, chip-dependent delay compensation, and electrical decision processing. The link model includes Fibre attenuation, chromatic dispersion, self-phase modulation, cross-phase modulation, four-wave mixing, receiver noise, and bandwidth limitations. Direct SSFM reliability requires $Q \geq 6$ and $\text{BER} \leq 10^{-9}$.

The OptiSystem check introduced later is intentionally narrower: it represents one data stream on four WDM carriers and uses receiver delay patterns as an implementation proxy for code matching. It is therefore used only to test an independently assembled transmitter–link–receiver chain and a selected wrong-decoder condition; it is not used to re-estimate the SSFM-derived multiuser boundaries or the analytical secrecy metrics.

$P_{\text{total,dBm}} = P_{\text{user,dBm}} + 10\log_{10}(K)$	(1)
$T_{\text{secure}} = KR_b C_{s,\min}$	(2)
$\eta_{\text{secure}} = \frac{T_{\text{secure}}}{B_{\text{allocated}}}$	(3)

In (1), $P_{\text{total,dBm}}$ and $P_{\text{user,dBm}}$ are the total and per-user launch powers in dBm, respectively, and K is the number of simultaneous users. In (2), T_{secure} is the secrecy-capacity-weighted aggregate throughput in Gb/s , (R_b) is the per-user bit rate in Gb/s , and $C_{s,\min} = \min_{G \in \mathcal{G}} \overline{C_s}(G)$ is the minimum dimensionless secrecy-capacity factor over the declared Eve budgets. In (3), η_{secure} is the secure spectral-efficiency metric in $bit/s/Hz$. The allocated optical bandwidth is calculated as $B_{\text{allocated}} = (L - 1) \Delta f + 2R_b$ under the adopted NRZ bandwidth approximation. Here, Δf and R_b are expressed consistently in Hz when calculating $B_{\text{allocated}}$. The throughput and bandwidth units are also converted consistently when reporting η_{secure} . The quantity T_{secure} is used as a model-based Optimisation metric under the declared analytical security model.

3.2 Eavesdropping Threat Model

Eve observes the optical spectrum and attempts to infer the authorized spectral code. Let (R) denote the overlap between the authorized binary constant-weight codeword of length (L) and weight (w) , and one candidate codeword selected independently and uniformly from the set of all binary words of length (L) and weight (w) . The probability of a single-guess overlap is

$$\Pr(R = r) = \frac{\binom{w}{r} \binom{L-w}{w-r}}{\binom{L}{w}}, \quad r = \max(0, 2w - L), \dots, w$$

4

For a declared budget of G independent guesses sampled with replacement from the same uniform set, let $R_1, \dots, R_G$ denote the corresponding overlap values. Eve retains the guess with the largest overlap, defined as $M_G = \max(R_1, \dots, R_G)$. The cumulative distribution function and probability mass function of M_G are then given by

$$F_{M_G}(m) = \left[\sum_{r=r_{\min}}^m \Pr(R = r) \right]^G, \quad p_m(G) = \Pr(M_G = m) = F_{M_G}(m) - F_{M_G}(m - 1).$$

5

The boundary condition is $F_{M_G}(r_{\min} - 1) = 0$ where $r_{\min} = \max(0, 2w - L)$. For each overlap state m , Bob and Eve probabilities are converted to binary-symmetric-channel capacities. Let $R_s = 0.9$ be the normalized confidential rate. Then

$$\begin{aligned}
p_{B,m} &= \min(BER_{B,m}, 1 - BER_{B,m}), \\
p_{E,m} &= \min(BER_{E,m}, 1 - BER_{E,m}), \\
C_{B,m} &= 1 - h_2(p_{B,m}), \quad C_{E,m} = 1 - h_2(p_{E,m}), \\
C_{s,m} &= \max(C_{B,m} - C_{E,m}, 0), \\
ILR_m &= \min\{\max(R_s - C_{s,m}, 0), R_s\}.
\end{aligned}$$

6

Here, $h_2(\cdot)$ is the binary entropy function. The overlap-averaged secrecy and leakage metrics are

$$\begin{aligned}
\overline{C_s}(G) &= \sum_m p_m(G) C_{s,m}, \\
\overline{ILR}(G) &= \sum_m p_m(G) ILR_m, \\
P_{\text{leak}}(G) &= \sum_m p_m(G) 1\{ILR_m > \epsilon\}, \\
P_{\text{SR}}(G) &= \sum_m p_m(G) 1\{BER_{B,m} \leq 10^{-9} \wedge ILR_m \leq 0.05\}.
\end{aligned}$$

7

Here $\epsilon = 10^{-12}$, and $1\{\bullet\}$ denotes the indicator function. Full-code recovery occurs when the best code guessed by Eve satisfies $M_G = w$. Therefore,

$$P_{\text{full}}(G) = \Pr(M_G = w) = 1 - \left(1 - \frac{1}{\binom{L}{w}}\right)^G$$

8

The declared budget set is $\mathcal{G} = \{1, 10^3, 10^6\}$. A resource point passes the analytical security screen only when

$$\begin{aligned}
\max_{G \in \mathcal{G}} \overline{ILR}(G) &\leq 0.05, \\
\max_{G \in \mathcal{G}} P_{\text{leak}}(G) &\leq 0.05, \\
\min_{G \in \mathcal{G}} P_{\text{SR}}(G) &\geq 0.95, \\
\max_{G \in \mathcal{G}} P_{\text{full}}(G) &\leq 0.05.
\end{aligned}$$

9

These analytical security conditions are combined with the separate Bob-side reliability requirements, $Q_B \geq 6$ and $BER_B \leq 10^{-9}$. The model considers a bounded attacker who makes independent code guesses. It does not enumerate all wrong-code sequences and does not constitute a cryptographic proof.

4. Physics-Guided Co-Design Methodology

4.1 Structural Code Audit

The initial domain used $L \in \{32, 64, 128\}$, $K \in \{8, 16, 24, 32\}$, and $w \in \{2, 4, 6, 8\}$, yielding 48 structural candidates. The zero-cross-correlation feasibility condition $Kw \leq L$ was applied before construction. Remaining designs were checked for weight, uniqueness, pairwise cross-correlation, wavelength mapping, and spectral-bandwidth support; 23 designs advanced to analytical resource screening.

4.2 Security-Conscious Semi-Analytical Screening

For each of the 23 designs, the coarse grid contained five per-user powers (-6 , -2 , 0 , 2 , and 4 dBm), five distances (20 , 40 , 60 , 80 , and 100 km), three channel spacings (25 , 50 , and 100 GHz), and two dispersion values (2 and $17 \frac{\text{ps}}{\text{nm} \cdot \text{km}}$). This produced 3,450 resource points and 10,350 rows across Eve budgets of 1 , 10^3 , and 10^6 guesses. Under the joint worst-budget criteria, 330 resource points passed. Six designs retained at least one admissible point. Their (L, K, w) tuples were $(64, 8, 6)$, $(64, 8, 8)$, $(128, 8, 6)$, $(128, 8, 8)$, $(128, 16, 6)$, and $(128, 16, 8)$.

4.3 Full-Resolution Multi-Design SSFM Data Set

A stratified plan selected 108 operating points: 60 secure points from the current numerical grid, 24 secure points from the expanded grid, 12 physical-boundary failures, and 12 security-boundary failures. Farthest-point sampling preserved diversity across code parameters, launch power, transmission distance, dispersion, and channel spacing. The development simulations used 64-bit sequences, a spectral oversampling factor of three, dynamic FFT lengths from 32,768 to 262,144 samples, and a maximum symmetric-SSFM propagation step of 0.125 km.

$$\frac{\partial A}{\partial z} = -\frac{\alpha}{2} A - j \frac{\beta_2}{2} \frac{\partial^2 A}{\partial t^2} + j \gamma |A|^2 A$$

10

Equation (10) is the scalar lossy nonlinear Schrödinger equation solved by the symmetric SSFM. Here $A(\mathcal{Z}, t)$ is the complex optical-field envelope, $\mathcal{Z}$ is the propagation distance (km) and t is the retarded time (s). The parameter α is the power-attenuation coefficient (km^{-1}). The attenuation value specified in dB/km is converted to the linear power-attenuation coefficient using $\alpha = \ln(10) \alpha_{\text{dB}}/10$ before its use in (10). β_2 is the group-velocity-dispersion coefficient (s^2/km), and γ is the nonlinear coefficient ($\text{W}^{-1} \text{km}^{-1}$). We obtain β_2 from the specified dispersion coefficient D using $\beta_2 = -D \lambda_0^2 / (2\pi c)$, where $\lambda_0 = 1550 \text{ nm}$ and c is the speed of light. Thus, the three terms on the right-hand side represent attenuation, chromatic dispersion, and Kerr nonlinearity, respectively. In the direct SSFM simulations, all active chip carriers are combined into one optical field before propagation. Therefore, SPM, XPM, and FWM arise from the Kerr nonlinear term. The coarse semi-analytical screening includes SPM and XPM estimates, whereas FWM is evaluated only in the direct SSFM simulations.

4.4 Physics-Guided Hybrid Surrogate Construction

Four surrogate formulations were compared for Q and $\log_{10}(BER)$: direct prediction from raw design variables, direct prediction from physics-derived features, residual prediction from raw variables, and residual prediction from physics-derived features. Feature scaling, feature selection, model-family selection,

hyperparameter tuning, one-sided calibration margins, and scoring were nested within leave-one-design-out validation. Therefore, observations from the held-out code design did not influence model selection or calibration.

The final selected model for both targets is a physics-direct quadratic-ridge surrogate. The model predicts the SSFM Q -factor and $\log_{10}(BER)$ directly from the physics-derived feature vector. The workflow remains physics-guided because structural validity, analytical security constraints, numerical-grid support, physics-derived features, SSFM labels, and final direct audits limit the authority of the surrogate. The one-sided calibration margins are used for screening decisions and are not interpreted as formal confidence intervals.

$$\hat{Q}_{\text{SSFM}} = f_Q^{\text{QR}}(\backslash\text{varvec}\phi(L, K, w, P, L_f, \Delta f, D))$$

11

$$\log_{10}(\widehat{BER}_{\text{SSFM}}) = f_{\text{BER}}^{\text{QR}}(\backslash\text{varvec}\phi(L, K, w, P, L_f, \Delta f, D))$$

12

Here, f_Q^{QR} and $f_{\text{BER}}^{\text{QR}}$ denote the selected quadratic-ridge surrogate models for the SSFM Q -factor and $\log_{10}(BER)$, respectively. The vector $\backslash\text{varvec}\phi$ contains the physics-derived features calculated from code length L , user count K , code weight w , per-user launch power P , Fibre length L_f , channel spacing Δf , and chromatic-dispersion coefficient D . Both targets are predicted directly; the selected final models do not use an RBF residual correction.

4.5 Exact Pareto Enumeration

The final Optimisation domain is restricted to the six designs supported by multi-design SSFM. Per-user power spans -6 to 4 dBm in 0.25 – dB steps; distance spans 20 to 100 km in 5 – km steps; channel spacing is 25 , 50 , or 100 GHz; and dispersion is 2 or 17 ps/(nm · km). The resulting finite domain contains $25,092$ candidates $(6 \times 41 \times 17 \times 3 \times 2)$.

Let $x = (L, K, w, P, L_f, \Delta f, D)$ denote one supported candidate. The screening-stage objective vector is

$$f(x) = [T_{\text{secure}}(x), \eta_{\text{secure}}(x), C_{s,\min}(x), -P_{\text{total}}(x)].$$

13

The first three components of $f(x)$ are Maximised. The fourth component, $-P_{\text{total}}$, is also Maximised, which is equivalent to minimizing the total launch power. Within each fixed distance-dispersion scenario, a candidate is Pareto-optimal if no other eligible candidate improves at least one objective without worsening any other objective.

To select a balanced point, the four benefit-form objectives on each Pareto front are normalized using min-max scaling. For candidate i and objective j , the normalized objective and its Euclidean distance from the ideal point $(1, 1, 1, 1)$ are

$$\tilde{f}_{ij} = \frac{f_{ij} - \min_i (f_{ij})}{\max_i (f_{ij}) - \min_i (f_{ij})}, d_i = \sqrt{\sum_{j=1}^4 (1 - \tilde{f}_{ij})^2}.$$

14

Here, f_{ij} is the value of objective j for candidate i . If an objective is constant across the Pareto front, its normalized value is set to one. The candidate with the smallest d_i is selected as the knee point. This rule is used only to select a balanced recommendation and does not replace Pareto dominance.

Every reported Pareto or boundary point is subsequently evaluated by direct SSFM. Candidates must satisfy the calibrated Bob-side reliability requirements, all analytical security constraints, and the numerical-grid support requirement. Exact non-dominance testing is performed within the declared supported domain because this domain is finite and computationally tractable.

4.6 Direct Pareto Audit, Rescue, and Synthesis

The targeted audit contains 39 distinct Pareto and operating-boundary points selected to challenge the surrogate near decision thresholds. Direct SSFM outcomes are used to identify false-positive and false-negative decisions. Failed Pareto roles trigger a predeclared local rescue search; three rescue/refinement points were evaluated. Final synthesis removes duplicate operating points, assigns objective roles only to directly passed candidates, explicitly records infeasible scenarios, and constructs the validated boundary table.

4.7 Reproducibility, Leakage Control, and Model Authority

Deterministic seeds, immutable checkpoint rows, design-level data partitions, and staged manifests are used throughout. Screening, development SSFM, nested validation, targeted audit, rescue, and final qualification are logically separate evidence sets. Surrogates may rank candidates only within the six-design supported domain and may not certify final operating limits.

4.8 Multi-Realisation Robustness and Numerical Convergence

The 27 final base points (15 Pareto plus 12 validated-boundary points) are re-evaluated over three code time slots and three deterministic random seeds. Acceptance requires every realisation to satisfy the direct Bob reliability decision. Twelve numerically sensitive points are tested for SSFM propagation-step convergence, and 12 are tested for bit-window sensitivity. Targeted rescue is invoked only when the predeclared tolerance fails. The final production settings are point-specific: one convergence-sensitive point requires a maximum step of 0.03125 km, while the bit-sensitive point uses 512 bits after comparison with a 1024-bit reference. This audit concerns Bob-side SSFM; Eve-side evidence remains analytical.

The reported SSFM BER is not obtained by direct error counting over the finite bit sequences. It is estimated from the receiver Q-factor under the Gaussian decision-statistic approximation as

$BER = 0.5 \operatorname{erfc} \left(Q / \sqrt{2} \right)$. The bit-window test therefore evaluates the stability of the Q-derived receiver metrics rather than the direct observation of error probabilities as small as 10^{-9} . A numerical floor of 10^{-20} is applied only when $\log_{10}(BER)$ is calculated for model fitting, comparisons, and graphical presentation.

5. Simulation and Evaluation Configuration

Table 1 summarizes the design, security, development-SSFM, and final numerical-qualification settings.

Table 1
Principal design, numerical, robustness, and security parameters

Parameter	Value
Per-user bit rate	10Gb/s
Code lengths / user loads / weights	$L = \{32, 64, 128\}; K = \{8, 16, 24, 32\}; w = \{2, 4, 6, 8\}$
Coarse launch-power grid	$-6, -2, 0, 2, 4$ dBm/user
Exact launch-power sweep	-6 to 4 dBm/user in 0.25 – dB steps
Distances / channel spacings	$20 - 100$ km; $25, 50, 100$ GHz
Dispersion	2 and 17 ps/(nm · km)
Centre wavelength	1550 nm
Fibre attenuation	0.2 dB/km
Nonlinear coefficient, γ	$1.3 \text{ W}^{-1} \text{ km}^{-1}$
Photodiode responsivity	0.8 A/W
Dark current	1 nA
Receiver noise bandwidth	$0.7 R_b = 7$ GHz
Receiver temperature	300 K
Load resistance	50Ω
Relative intensity noise	-155 dB/Hz
Development SSFM bit sequence	64 bits
Spectral oversampling	3
Development maximum SSFM step	0.125 km
Development maximum FFT length	262,144
Robustness realisations	$3 \times \text{timeslots} \times 3 \times \text{seeds per final basepoint}$

Parameter	Value
Targeted convergence step	As fine as 0.03125km for the sensitive point
Bit-sensitive production / reference	512/1024bits
Maximum FFT length used in numerical qualification	2,097,152
Bob reliability	$Q \geq 6$ and $BER \leq 10^{-6}$
Maximum Eve budget	10^6 guesses
Security thresholds	$ILR \leq 0.05$; positive leakage ≤ 0.05 ; secure-reliable probability ≥ 0.95 ; full recovery ≤ 0.05
Bit-convergence tolerances	$ \Delta Q \leq 0.25$ and $ \Delta \log_{10}(BER) \leq 0.50$ versus reference

6. Results

6.1 End-to-End Evidence Pipeline

Table 2 and Fig. 2 summarize the end-to-end evidence pipeline. Structural audit retains 23 of 48 designs, analytical screening retains 330 of 3,450 resource points, and 80 of the 108 development points pass direct SSFM. Exact enumeration retains 5,198 calibrated feasible candidates from 25,092 and yields 96 Pareto points before targeted audit. The targeted audit directly passes 28 of 39 points; all three rescue evaluations pass; and final de-duplication produces 15 unique directly audited Pareto points. Retention percentages use different denominators and must not be interpreted as a single cumulative funnel.

Table 2
End-to-end evidence pipeline; percentages use stage-specific denominators

Stage	Unit	Evaluated	Retained	Retention
Structural code audit	Code designs	48	23	47.9%
Security/link screening	Physical resource points	3,450	330	9.6%
Multi-design SSFM evaluation	Selected SSFM points	108	80	74.1%
Exact co-design enumeration	Exact co-design candidates	25,092	5,198	20.7%
Pareto/boundary direct audit	Pareto/boundary audit points	39	28	71.8%
Adaptive rescue/refinement	Rescue/refinement points	3	3	100.0%
Unique audited Pareto synthesis	Unique audited Pareto points	15	15	100.0%

6.2 Multi-Design SSFM Screening Benchmark

On the 108-point development set, the initial semi-analytical screen reproduces the direct pass/fail decision with 96.30\% accuracy (four false positives and no false negatives), but its continuous errors are large: $Q \text{ RMSE} = 11.1104$ and $\log_{10}(\text{BER}) \text{ RMSE} = 2.8665$ decades. It is therefore useful for broad exclusion and not for final operating-point prediction.

6.3 Nested Hybrid Surrogate and Focused Audit Behaviour

Nested leave-one-design-out validation reduces the continuous errors to $Q \text{ RMSE} = 2.6690$ and $\log_{10}(\text{BER}) \text{ RMSE} = 0.7457$ decades. The calibrated classifier is deliberately conservative. It produces 34 true positives, 28 true negatives, no false positives, and 46 false negatives. This corresponds to 57.41\% overall decision agreement and 42.50 \% sensitivity for directly feasible points. Thus, the absence of observed false positives is achieved at the cost of missing 46 feasible cases in the held-out set. This result does not justify autonomous certification by the surrogate; it justifies using the model to rank candidates while protecting against optimistic acceptance.

The targeted 39-point audit is intentionally enriched with near-threshold and Pareto/boundary cases and is not identically distributed with the development set. It yields 92.31\% decision agreement, one false positive, and two false negatives. The three-point adaptive-rescue set yields 100\% agreement. Table 3 and Fig. 3 therefore report each layer separately rather than presenting them as interchangeable test sets.

Table 3
Decision and continuous-error performance on non-identically distributed validation layers

Evaluation layer	n	Q RMSE	$\log_{10}(\text{BER}) \text{ RMSE}$	Agreement	FP	FN
Analytical screening	108	11.1104	2.8665	96.30%	4	0
Nested hybrid	108	2.6690	0.7457	57.41%	0	46
Targeted direct audit	39	3.0347	1.7452	92.31%	1	2
Adaptive rescue	3	4.8272	0.9666	100.00%	0	0

6.4 Exact Co-Design and Pareto Structure

Exact enumeration evaluates 25,092 supported co-design candidates. The calibrated reliability, analytical security, and numerical-support constraints retain 5,198 candidates, from which 96 Pareto-optimal points are identified before direct audit. The final directly audited set reaches 159.88 Gb/s secure aggregate throughput, 0.04997 bit/s/Hz secure spectral efficiency, and 0.9992 minimum secrecy capacity. These maxima need not occur at the same operating point. Reported values retain numerical calculation precision; they are finite-grid simulation outputs and do not imply statistical confidence intervals. Figure 4 shows the recovered knee role and the resulting trade-off structure.

The final 15-point set exhibits the expected trade-off between secure aggregate capacity, spectral occupancy, total launch power, and robustness. $K = 16$ designs dominate the highest-throughput region, while $K = 8$ designs supply lower-power or secrecy-oriented alternatives. Smaller channel spacing improves the nominal

spectral-efficiency objective but can increase nonlinear interaction, so the directly passed solution rather than the nominal analytical optimum is retained (Fig. 4).

6.5 Targeted Direct Audit and Adaptive Rescue

The targeted audit evaluates 39 operating points. Of the 27 points predicted to pass by the calibrated hybrid filter, 26 are confirmed by direct SSFM, giving a positive predictive value of 96.30%. One predicted-pass point is therefore a false positive. Of the 12 points rejected by the filter, two pass direct SSFM and are false negatives, while the remaining ten fail. In total, 28 of the 39 audited points pass direct SSFM, and the filter agrees with the direct decision for 36 points, giving an overall decision agreement of 92.31%. The three disagreements are concentrated near the thresholds of $Q = 6$ and $BER = 10^{-9}$. This finding supports the use of direct SSFM as the final decision rule.

One Pareto role fails the initial direct audit: the 60 – km, $D = 2$ ps/(nm · km) knee point at 0.25 dBm/user. Three nearby rescue candidates are tested and all pass. The selected replacement increases per-user power by 0.25 dB, raises Q from 5.9610 to 6.3057, and changes secure throughput by only -0.0141 Gb/s. Table 4 and Fig. 5 summarize the recovery.

Table 4
Direct rescue audit for the single failed Pareto role

Role	Scenario	Old P	Status	Replacement	New Puser	QSSFM	log10(BER)
Knee	60km, $D = 2$	0.25dBm	Recovered	L128/K16/w8	0.50dBm	6.3057	-9.8432

6.6 Scenario-Wise Final Operating Recommendations

Five objective roles are assigned within each distance-dispersion scenario that contains at least one directly feasible candidate. Five scenarios support all five roles, producing 25 scenario-role assignments represented by 15 unique physical operating points. At 60km and $D = 17$ ps/(nm · km), no candidate within the declared finite domain passes the calibrated screening criteria. This case is therefore reported as having no calibrated candidate, and no value is introduced by extrapolation. This result does not establish that the scenario is physically infeasible outside the evaluated domain. Table 5 lists one balanced, directly audited point for each feasible scenario, and Fig. 6 shows the corresponding Bob-side SSFM margin.

Table 5

Balanced points and infeasible scenario; P user (dBm/user), Δf (GHz), secure T (Gb/s), and η secure (bit/s/Hz)

Scenario	L/K/w	P user	Δf	QSSFM	$\log_{10}(\text{BER})$	Secure T	η secure	Status
20 km, D = 2	128/16/8	-5.00	50	10.8376	-20.0000	159.576	0.025051	Feasible
20 km, D = 17	128/16/8	-6.00	50	8.8624	-18.4073	159.793	0.025085	Feasible
40 km, D = 2	128/16/8	-2.75	50	7.4289	-13.2615	159.813	0.025088	Feasible
40 km, D = 17	128/16/8	-2.00	50	8.2483	-16.0952	159.880	0.025099	Feasible
60 km, D = 2	128/16/8	0.50	50	6.3057	-9.8432	159.870	0.025097	Feasible
60 km, D = 17	—	—	—	—	—	—	—	No calibrated candidate

6.7 Directly Validated Secure–Reliable Boundaries

Across the six supported code designs, the common directly validated boundary is 65 km for $D = 2$ ps/(nm · km) and 55 km for $D = 17$ ps/(nm · km). Individual low-dispersion boundaries range from 65 to 70 km; all standard-dispersion boundaries are 55 km. At $D = 2$, mean boundary Q is 7.3189 and the worst boundary point has $Q = 6.3049$ and $\log_{10}(\text{BER}) = -9.8410$. At $D = 17$, mean boundary Q is 8.0025 and the worst point has $Q = 7.5978$ and $\log_{10}(\text{BER}) = -13.8221$.

These are composite secure–reliable limits: Bob’s boundary point is directly propagated by SSFM, whereas the corresponding security constraints are evaluated by the analytical overlap/threat model. Points beyond the common distance can be physically reliable for some designs but are not promoted to a universal secure–reliable claim. Table 6 and Fig. 7 retain both the common and design-specific information.

Table 6
Final directly validated boundary synthesis

D	Designs	Boundary range	Common boundary	Mean Q	Worst Q	Worst $\log_{10}(\text{BER})$
2	6	65–70 km	65 km	7.3189	6.3049	-9.8410
17	6	55–55 km	55 km	8.0025	7.5978	-13.8221

6.8 Multi-Realisation Robustness and Numerical Convergence

All 27 final base points pass the multi-slot/multi-seed worst-case requirement. The global worst Realisation has $Q = 6.2265$ and $\log_{10}(\text{BER}) = -9.6225$, retaining positive margins to both acceptance thresholds. After targeted rescue, all 12 propagation-step convergence points and all 12 bit-length points are accepted; therefore all 27 final points are computationally qualified under the predeclared protocol. The full qualification summary is reported in Table 7.

The critical bit-sensitive point is evaluated across three time slots and three seeds at 256, 512, and 1024 bits. The 256-bit candidate is accepted in only 6/9 realisations and reaches maximum deviations $|\Delta Q| = 0.2069$ and $|\Delta \log_{10}(\text{BER})| = 0.8167$. The 512-bit candidate is accepted in 9/9 realisations with maxima 0.1119 and 0.4397, respectively, and is selected as the production window against the 1024 – bit reference (Fig. 8).

Table 7
Final Stage robustness and numerical-convergence qualification

Qualification layer	Points	Realisation/evaluation structure	Final outcome	Production implication
Worst-case robustness	27	3 time slots × 3 seeds per base point	27/27 pass	Worst Q = 6.2265; worst $\log_{10}(\text{BER}) = -9.6225$
Propagation-step convergence	12	Point-specific step refinement	12/12 accepted	Sensitive point uses maximum step 0.03125 km
Bit-window convergence	12	Critical point: 256/512/1024 bits over 9 Realisations	12/12 accepted	512 bits selected against 1024-bit reference
Final qualification	27	Cumulative robustness + convergence	27/27 qualified	Overall qualification: Qualified

6.9 Independent OptiSystem Implementation-Level Check

The SSFM/analytical framework and the following component-level simulation serve different evidential roles. To check that a representative transmitter-decoder implementation is operational in an independent simulator, a deliberately reduced OptiSystem 23.0 (Optiwave Systems Inc. 2025) demonstrator was assembled. The demonstrator carries one PRBS-NRZ stream on four WDM carriers rather than the full multiuser SAC-OCDMA design space. Its purpose is limited to testing the physical chain and matched-versus-mismatched decoder behaviour; it neither validates all 25,092 numerical candidates nor converts the analytical Eve model into a security proof. The scoped architecture is shown in Fig. 9.

Table 8 gives the complete parameters that were intentionally varied or fixed in this reduced check. Each carrier is independently modulated by an MZ modulator driven by the common 10 – Gb/s NRZ pattern. The optical link is 39 km, each carrier launches at +2 dBm, and both decoder branches include a 4 – dB lumped decoder/connector penalty before PIN detection. Bob uses the ordered delay vector $[0, 0.53187263415, 1.06319542680, 1.59396923205] \text{ ns}$; Eve uses the cyclically shifted vector $[0.53187263415, 1.06319542680, 1.59396923205, 0] \text{ ns}$.

Table 8
Configuration of the reduced independent OptiSystem implementation-level check

Item	Scoped OptiSystem configuration
Software and role	OptiSystem 23.0; independent component-level verification only
Traffic and carriers	One 10-Gb/s PRBS-NRZ stream on four carriers: 193.264, 193.364, 193.464, and 193.564 THz (100-GHz spacing)
Transmitter	Four CW lasers, each at + 2 dBm, followed by an analytical MZ modulator; 4×1 WDM multiplexing
Optical path	39-km Fibre followed by an X coupler; 99% nominal Bob branch and 1% nominal Eve baseline tap
Decoder and loss	1×4 WDM demultiplexer followed by four delay branches and a 4×1 WDM multiplexer; 25-GHz WDM passband; 4-dB lumped decoder/connector attenuation in each receiver branch
Bob decoder	[0, 0.53187263415, 1.06319542680, 1.59396923205] ns
Eve mismatch	Cyclic shift: [0.53187263415, 1.06319542680, 1.59396923205, 0] ns
Electrical receiver	PIN photodiode followed by a second-order Bessel low-pass filter at $0.75 \times$ symbol rate and BER analysis
Threat-scope stresses	Eve tap increased to 20% and 50%; a 50%-tap matched-decoder positive control was run

At the 1% baseline tap with the cyclically mismatched Eve delay sequence, Bob achieved $Q = 6.45988$ and $BER = 4.34412 \times 10^{-11}$. The Eve Analyser reported $Q = 0$ and $BER = 1$. This result shows that Eve does not meet the declared $Q \geq 6$ reception criterion in this selected mismatch case. However, $BER = 1$ is not interpreted by itself as evidence of secrecy because systematic bit inversion or a reversed decision mapping can also produce a BER close to one. The 20% and 50% cyclic-mismatch cases are included to examine the same selected mismatch under stronger taps. At the same 50% tap, a positive-control run with Eve's delays matched to Bob's delays restores Eve's decoding performance. The matched and mismatched 50% results therefore isolate the effect of the selected delay pattern within this reduced model. They do not establish an exhaustive wrong-code result or a cryptographic security guarantee. The numerical outcomes are summarized in Table 9.

Table 9
Independent OptiSystem results at 39 km and + 2 dBm/carrier. Ranges report repeated 50%-tap runs

Tap / decoder condition	Bob: Q; BER	Eve: Q; BER	Interpretation
1% / cyclic mismatch (baseline)	6.45988; 4.34412×10^{-11}	0; 1	Bob meets the declared $Q \geq 6$ computational threshold; raw Eve reception fails in this selected mismatch case.
20% / cyclic mismatch	6.52964; 2.73768×10^{-11}	2.48869; 6.31562×10^{-3}	Eve remains below the declared $Q \geq 6$ reception criterion in this selected mismatch case, although its Q-factor increases relative to the 1% case.
50% / cyclic mismatch (n = 4)	6.08881–6.32619; 1.04×10^{-10} to 4.77×10^{-10}	2.61141–2.67334; 3.70649×10^{-3} to 4.45157×10^{-3}	Across four repeated runs, Eve remains below the declared $Q \geq 6$ reception criterion under the selected cyclic mismatch. This result is not an FEC assessment or a universal security claim.
50% / matched Eve positive control	6.09745; 4.57946×10^{-10}	6.18369; 2.67290×10^{-10}	Eve meets the reception criterion when its delay sequence is matched, confirming that the Eve receiver chain is functional in this reduced model.

These component-level results are scoped to the specific delay pattern tested. The cyclic shift represents only one sampled wrong delay sequence. In the 50% cyclic-mismatch case, Eve BER ranges from 3.70649×10^{-3} to 4.45157×10^{-3} across four runs. These results show that Eve remains below the declared $Q \geq 6$ reception criterion for this selected mismatch, but they do not constitute an FEC assessment or an exhaustive evaluation of wrong delay sequences. Under the 1% tap and cyclically mismatched Eve delay sequence, three additional reruns at 39km produced Bob Q-factors from 6.05945 to 6.20175. Under the same 1% tap and wrong-delay condition at 40km, one run produced $Q = 5.92363$. Therefore, 39 km is the largest repeatedly evaluated distance at which all reported Bob runs satisfy $Q \geq 6$ for this reduced configuration. This result does not replace the 65/55 – km SSFM boundaries, which were obtained using a different multiuser model and acceptance protocol.

7. Discussion

7.1 Meaning of Physics-Guided in This Framework

Physics-guided does not mean that the nonlinear Schrödinger equation is embedded directly in the surrogate objective function. It describes how decision authority is distributed across the workflow. Physics and combinatorial constraints govern code construction and analytical security screening. Numerical-grid rules define the supported prediction domain. Physics-derived features are used as inputs to the selected quadratic-ridge

surrogate models, while SSFM provides the numerical training and validation labels. Exact enumeration identifies the candidate trade-offs, and direct SSFM with numerical-convergence checks determines the final operating limits. Therefore, the surrogate is used only for screening and ranking, whereas final feasibility is determined by direct SSFM.

7.2 Security as the First Design Bottleneck

Only 330 of 3,450 resource points pass the joint analytical criteria. Within the evaluated code families and the 10^6 -guess budget, larger weights (particularly $w = 6$ and $w = 8$) reduce full-code-recovery probability sufficiently to admit secure candidates. This is a domain-specific result, not a universal claim that a particular weight is secure independently of L , K , mapping, attack budget, and observation model.

7.3 Why Exact Enumeration Is Preferable Here

The 25,092-point supported domain is tractable for complete enumeration. Exact non-dominance testing avoids variability due to population size, mutation settings, optimizer convergence, and random seed, and it establishes that no supported candidate is omitted. This advantage applies only to the declared finite domain; amplifier placement, modulation format, code-hopping period, larger code families, and other continuous variables would require a different search strategy.

7.4 Surrogates as Screening Tools

The nested hybrid improves continuous RMSE but is strongly conservative at the decision threshold, with zero false positives and 46 false negatives. On the boundary-enriched targeted audit it produces one false positive and two false negatives. These results make the model useful for prioritizing expensive evaluations but unsuitable for certifying final feasibility. Direct propagation is therefore not an optional confirmatory illustration; it is a required layer of the decision rule.

7.5 Trade-Offs in Power, Spacing, and Dispersion

The single failed Pareto role is recovered by a 0.25 dB/user power increase with negligible throughput loss, showing that the surrogate identifies a useful local neighbourhood even when its threshold decision is optimistic. Channel spacing and power cannot be optimized independently: wider spacing can reduce inter-channel nonlinear interaction but lowers nominal spectral efficiency, while extra power improves Bob's margin until nonlinear penalties dominate.

Low dispersion supports a longer common distance (65 km rather than 55 km), but its worst boundary point is closer to the acceptance threshold. Standard-dispersion boundary points have larger Q margins at their shorter limit. Network planning should therefore distinguish maximum supported distance from margin quality and should retain design-specific boundaries in addition to the common conservative limit.

7.6 Physical and Composite Secure–Reliable Boundaries

Bob-side physical reliability and the composite secure–reliable boundary are distinct. Direct SSFM can confirm that a waveform remains decodable beyond a surrogate-predicted limit, while the same resource point can fail an analytical security criterion. The manuscript therefore reports Bob's direct Q/BER evidence together with security quantities derived from the overlap model and avoids describing the combined result as experimental proof of confidentiality.

7.7 Robustness and Numerical Qualification

The final robustness result is stronger than a single deterministic SSFM pass: every reported Pareto and boundary point survives the declared slot/seed grid, and every selected convergence-sensitive point is numerically qualified. Nevertheless, the tolerances are engineering acceptance rules rather than probabilistic confidence intervals. The selected 512 – bit production window is established for the identified bit-sensitive point against a 1024 – bit reference and should not be generalized to arbitrary code families or link settings without repeating the protocol.

7.8 Comparison with Previous Single-Reference Study

The earlier study (Shukra and Prathibha 2026) evaluated one fixed SA-SAC reference configuration with $((L, K, w) = (64, 16, 4))$. Its main objective was to determine directly simulated operating brackets for three selected Fibre scenarios. The present study addresses a different research question: it compares multiple code structures, applies security-aware resource screening, enumerates a finite co-design domain, and directly audits the selected Pareto and boundary points. Table 10 compares the scope, methods, and evidence of the two studies.

Table 10

Comparison between the present multi-design co-design study and the earlier single-reference study (Shukra and Prathibha 2026)

Aspect	Previous study	Present study
Main objective	Direct SSFM operating boundary validation for one reference design	Multi-design security-aware co-design and directly audited Pareto selection
Code-design scope	Fixed design: $(L, K, w) = (64, 16, 4)$	48 initial designs; 23 structurally eligible designs; six SSFM-supported designs
Security model	Keyed time-dependent wavelength allocation with Bob-Eve capacity and ILR evaluation	Constant-weight overlap model evaluated over Eve budgets of 1 , 10^3 , and 10^6 guesses
Development SSFM evidence	27 full-resolution base points, followed by 14 distance and six power validation simulations	108 stratified multi-design SSFM points
Surrogate role	Ridge and quadratic-ridge calibration used to select additional direct SSFM cases	Physics-direct quadratic-ridge models for Q and $\log_{10}(BER)$, selected using nested leave-one-design-out validation and used only for screening and ranking.
Search strategy	Direct distance and power bracketing in three fixed physical scenarios	Exact enumeration of 25,092 supported co-design candidates and multi-objective Pareto analysis
Final direct evidence	Direct distance brackets of 65–70 km, 50–55 km, and 70–75 km for the three selected scenarios	39-point targeted audit, three rescue evaluations, 15 unique directly audited Pareto points, and 27 numerically qualified Pareto/boundary points
Boundary statement	Design-specific operating brackets for one reference code	Common directly validated boundaries of 65 km at $D = 2\text{ps}/(\text{nm} \cdot \text{km})$ and 55 km at $D = 17\text{ps}/(\text{nm} \cdot \text{km})$ across the six supported designs
Independent implementation check	Not included	Scoped OptiSystem matched-versus-mismatched decoder check

The boundary values reported in the two studies should not be interpreted as evidence of a direct improvement in transmission distance. The studies use different code structures, physical scenarios, candidate-selection rules, and validation protocols. The main contribution of the present work is its broader co-design scope and its explicit evidence pipeline, which connects structural code screening, analytical security screening, surrogate-assisted enumeration, direct SSFM auditing, and final numerical qualification.

8. Limitations and Future Work

The study has six principal limitations. First, results are confined to the six SSFM-supported code designs and the declared discrete resource domain. Second, the 108-point development set is modest and targeted enrichment may improve calibration under high-load and near-threshold conditions. Third, Eve's evidence in the co-design framework is analytical under a bounded spectral-code guessing model; side channels, cooperative eavesdroppers, and alternative observation models are outside scope. Fourth, calibrated margins and convergence tolerances are engineering decision rules, not formal confidence intervals. Fifth, the robustness audit covers three time slots and three deterministic seeds and does not replace broader stochastic uncertainty quantification. Sixth, the added OptiSystem check is a restricted four-wavelength, single-stream, component-level simulation. It does not reproduce the full multiuser search, enumerate wrong-code patterns, or validate FEC performance. Accordingly, the study supports bounded computational and implementation-level claims.

9. Conclusion

A physics-guided SAC-OCDMA co-design framework jointly treats code structure, user load, launch power, distance, channel spacing, dispersion, Bob reliability, and a declared analytical security model. The evidence pipeline audits 48 designs, screens 3,450 resource points, directly propagates 108 multi-design development points, and exactly enumerates 25,092 supported candidates. Of these, 5,198 satisfy the calibrated constraints and 96 are Pareto-optimal before direct audit. The targeted audit produces 28 direct passes; all three rescue evaluations pass and recover the single failed Pareto role.

Final synthesis yields 15 unique directly audited Pareto points and 25 objective-role assignments across five feasible scenarios, with common boundaries of 65 km at $D = 2 \text{ ps}/(\text{nm km})$ and 55 km at $D = 17 \text{ ps}/(\text{nm km})$ within the declared domain. All 27 reported Pareto/boundary points pass the stated robustness audit; all 12 propagation-step and 12 bit – length qualification points are accepted, with 512 bits selected against a 1024 – bit reference for the critical point. The OptiSystem check adds a deliberately narrow implementation result: in a 39 – km, four-wavelength, single-stream demonstrator, Bob remains decodable at a 1\% Eve tap under a cyclic delay mismatch, whereas a 50\% – tap matched-decoder control restores Eve decodability. Direct Bob-side SSFM remains the final arbiter for numerical co-design decisions; the OptiSystem check tests one implementation pathway only. The evidence is computational and does not establish cryptographic secrecy.

Declarations

Competing Interests:

The authors have no relevant financial or non-financial interests to disclose.

Funding:

The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Author Contribution

M.M.S.: Conceptualization, methodology, software, formal analysis, investigation, data curation, visualization, and writing original draft. G.P.: Supervision, validation, and writing review and editing. Both authors contributed to the interpretation of the results and approved the final version of the manuscript.

Data Availability

The datasets generated and analysed during the current study (the 108-point stratified SSFM development set, the 25,092-candidate enumerated domain, and the 39-point direct-audit results) are available from the corresponding author on reasonable request.

References

1. Aljunid, S.A., Ismail, M., Ramli, A.R., Ali, B.M., Abdullah, M.K.: A new family of optical code sequences for spectral-amplitude-coding optical CDMA systems. *IEEE Photonics Technol. Lett.* **16**(10), 2383–2385 (2004). <https://doi.org/10.1109/LPT.2004.833859>
2. Anuar, M.S., Aljunid, S.A., Saad, N.M., Hamzah, S.M.: New design of spectral amplitude coding in OCDMA with zero cross-correlation. *Opt. Commun.* **282**(14), 2659–2664 (2009). <https://doi.org/10.1016/j.optcom.2009.03.079>
3. Bakarman, H.A., Hasoon, F.N., Shaari, S., Ismail, M.: Security enhancement for spectral amplitude coding OCDMA based on hybrid EDW/M-sequence code systems. In: *Proceedings of the International Conference on Computer and Communication Engineering* (2010). <https://doi.org/10.1109/ICCCE.2010.5556807>
4. Chang, Y.-T., Sue, C.-C., Huang, J.-F.: Robust design for reconfigurable coder/decoders to protect against eavesdropping in spectral-amplitude-coding optical CDMA networks. *J. Lightwave Technol.* **25**(8), 1931–1948 (2007). <https://doi.org/10.1109/JLT.2007.901333>
5. Deb, K., Pratap, A., Agarwal, S., Meyarivan, T.: A fast and elitist multiobjective genetic algorithm: NSGA-II. *IEEE Trans. Evol. Comput.* **6**(2), 182–197 (2002). <https://doi.org/10.1109/4235.996017>
6. Deiterding, R., Glowinski, R., Oliver, H., Poole, S.: A reliable split-step Fourier method for the propagation equation of ultra-fast pulses in single-mode optical fibers. *J. Lightwave Technol.* **31**(12), 2008–2017 (2013). <https://doi.org/10.1109/JLT.2013.2262654>
7. Djordjevic, I.B., Vasic, B.: Unipolar codes for spectral-amplitude-coding optical CDMA systems based on projective geometries. *IEEE Photonics Technol. Lett.* **15**(9), 1318–1320 (2003). <https://doi.org/10.1109/LPT.2003.816672>
8. Forrester, A., Sobester, A., Keane, A.: *Engineering Design via Surrogate Modelling: A Practical Guide*. Wiley, Chichester (2008)
9. Gan, Z., Shevchenko, M., Nallaperuma Herzberg, S., Savory, S.J.: Fast neural network inverse model to maximize throughput in ultra-wideband WDM systems. *Opt. Express*. **32**(22), 38642–38654 (2024). <https://doi.org/10.1364/OE.536632>
10. Hasoon, F.N., Aljunid, S.A., Samad, M.D.A., Abdullah, M.K., Shaari, S.: Spectral amplitude coding OCDMA using AND subtraction technique. *Appl. Opt.* **47**(9), 1263–1268 (2008). <https://doi.org/10.1364/AO.47.001263>
11. Jiang, Z., Leaird, D.E., Weiner, A.M.: Experimental investigation of security issues in O-CDMA. *J. Lightwave Technol.* **24**(11), 4228–4234 (2006). <https://doi.org/10.1109/JLT.2006.883661>

12. Kavehrad, M., Zaccarin, D.: Optical code-division-multiplexed systems based on spectral encoding of noncoherent sources. *J. Lightwave Technol.* **13**(3), 534–545 (1995). <https://doi.org/10.1109/50.372451>
13. Kennedy, M.C., O'Hagan, A.: Bayesian calibration of computer models. *J. Roy. Stat. Soc. B.* **63**(3), 425–464 (2001). <https://doi.org/10.1111/1467-9868.00294>
14. Musetti, S., Serena, P., Bononi, A.: On the accuracy of split-step Fourier simulations for wideband nonlinear optical communications. *J. Lightwave Technol.* **36**(23), 5669–5677 (2018). [10.1109/JLT.2018.2877384](https://doi.org/10.1109/JLT.2018.2877384)
15. Nallaperuma, S., Gan, Z., Nevin, J., Shevchenko, M., Savory, S.J.: Interpreting multi-objective reinforcement learning for routing and wavelength assignment in optical networks. *J. Opt. Commun. Netw.* **15**(8), 497–506 (2023). <https://doi.org/10.1364/JOCN.483733>
16. Noshad, M., Jamshidi, K.: Code family for modified spectral-amplitude-coding OCDMA systems and performance analysis. *J. Opt. Commun. Netw.* **2**(6), 344–354 (2010). <https://doi.org/10.1364/JOCN.2.000344>
17. Optiwave Systems Inc: OptiSystem 23.0 [Computer software]. Optiwave Systems Inc., Ottawa (2025)
18. Penon, J., El-Sahn, Z.A., Rusch, L.A., Larochelle, S.: Spectral-amplitude-coded OCDMA optimized for a realistic FBG frequency response. *J. Lightwave Technol.* **25**(5), 1256–1263 (2007)
19. Salehi, J.A.: Emerging OCDMA communication systems and data networks. *J. Opt. Netw.* **6**(9), 1138–1178 (2007)
20. Shi, F., Ghafouri-Shiraz, H.: Performance analysis of two new code families for spectral-amplitude-coding optical CDMA systems. *J. Lightwave Technol.* **34**(17), 4005–4014 (2016). <https://doi.org/10.1109/JLT.2016.2586527>
21. Shukra, M.M., Prathibha, G.: Security-aware spectral amplitude coding for high-speed OCDMA networks: full-resolution SSFM validation and direct operating-boundary optimisation. *Int. J. Comput. Inform. Syst. Industrial Manage. Appl.* **18**(14s), 961–975 (2026). <https://doi.org/10.70917/ijcisim-2026-4305>
22. Sinkin, O.V., Holzlohner, R., Zweck, J., Menyuk, C.R.: Optimization of the split-step Fourier method in modeling optical-fiber communications systems. *J. Lightwave Technol.* **21**(1), 61–68 (2003)
23. Souza, A., Costa, N., Pedro, J., Pires, J.: Comparison of fast quality of transmission estimation methods for C + L + S optical systems. *J. Opt. Commun. Netw.* **15**(11), F1–F12 (2023). <https://doi.org/10.1364/JOCN.486898>
24. Souza, A., Costa, N., Pedro, J., Pires, J.: Raman amplifier design and launch power optimization in multi-band optical systems. *J. Opt. Commun. Netw.* **17**(1), A13–A22 (2025). <https://doi.org/10.1364/JOCN.534006>
25. Wei, Z., Ghafouri-Shiraz, H.: Codes for spectral-amplitude-coding optical CDMA systems. *J. Lightwave Technol.* **20**(8), 1284–1291 (2002). <https://doi.org/10.1109/JLT.2002.800301>
26. Wei, Z., Shalaby, H.M.H., Ghafouri-Shiraz, H.: Modified quadratic congruence codes for fiber Bragg-grating-based spectral-amplitude-coding optical CDMA systems. *J. Lightwave Technol.* **19**(9), 1274–1281 (2001). <https://doi.org/10.1109/50.948274>
27. Wu, B.B., Prucnal, P.R., Narimanov, E.E.: A method for secure communications over a public fiber-optical network. *Opt. Express.* **14**(9), 3738–3751 (2006). <https://doi.org/10.1364/OE.14.003738>
28. Zhang, Q., Hayee, M.I.: Symmetrized split-step Fourier scheme to control global simulation accuracy in fiber-optic communication systems. *J. Lightwave Technol.* **26**(2), 302–316 (2008). <https://doi.org/10.1109/JLT.2007.909861>

Figures

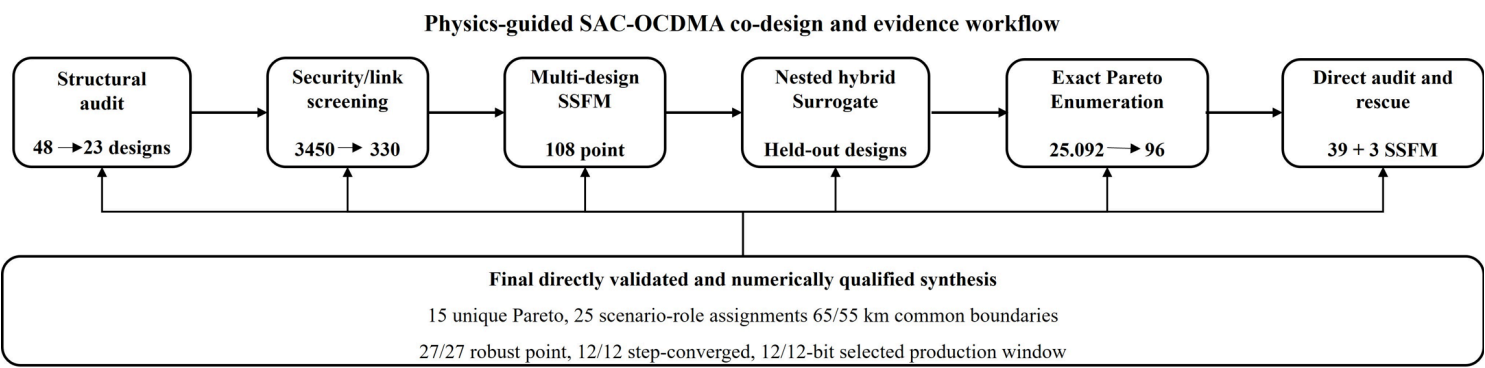


Figure 1

End-to-end physics-guided SAC-OCDMA co-design, direct-validation, and numerical-qualification workflow

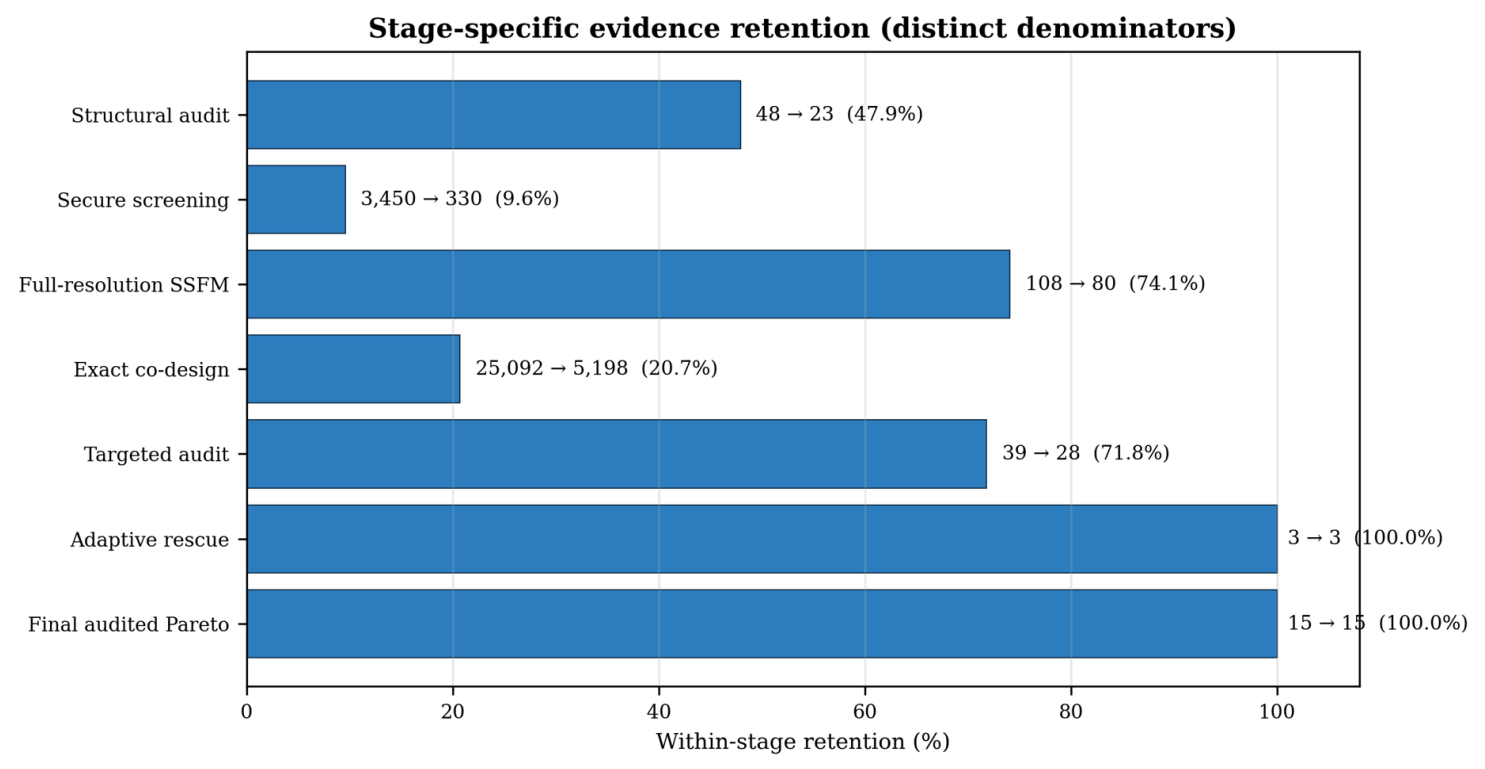


Figure 2

Stage-specific retention across the evidence pipeline

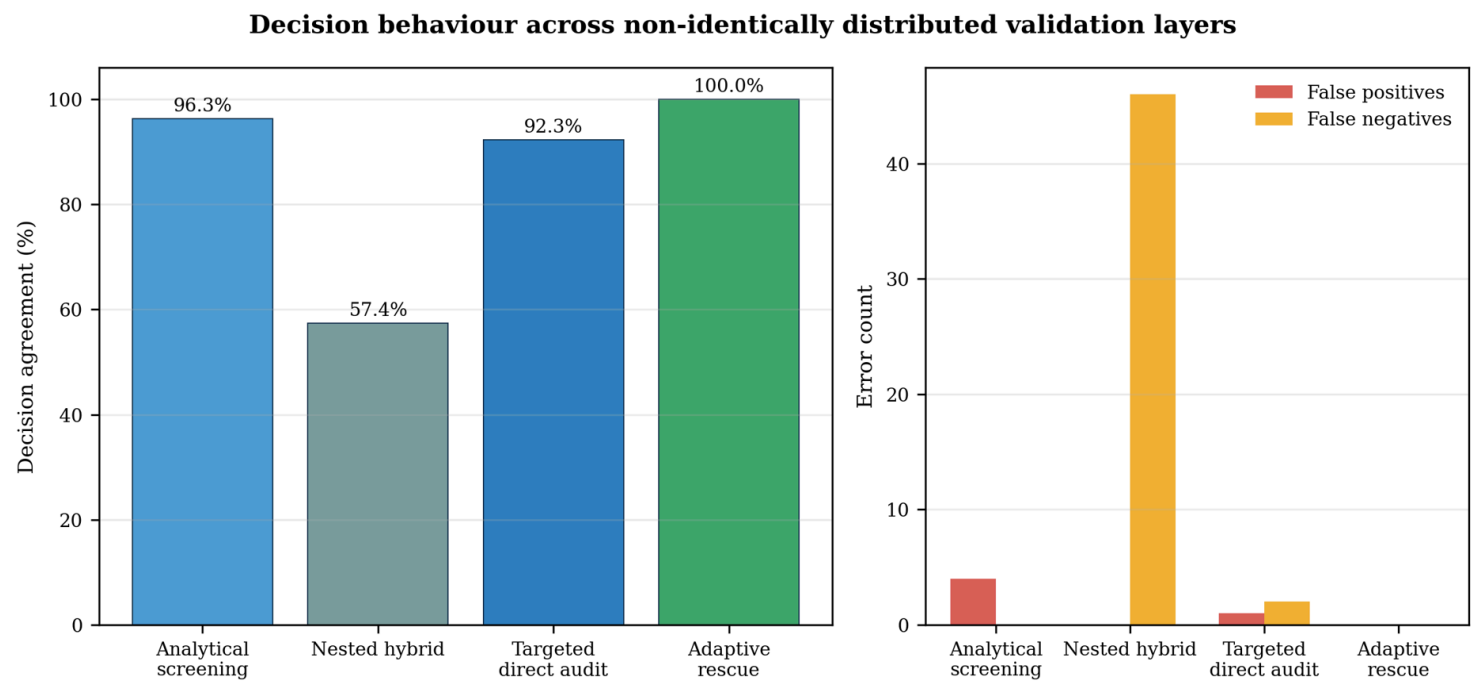


Figure 3

Decision agreement and error counts across the four validation layers

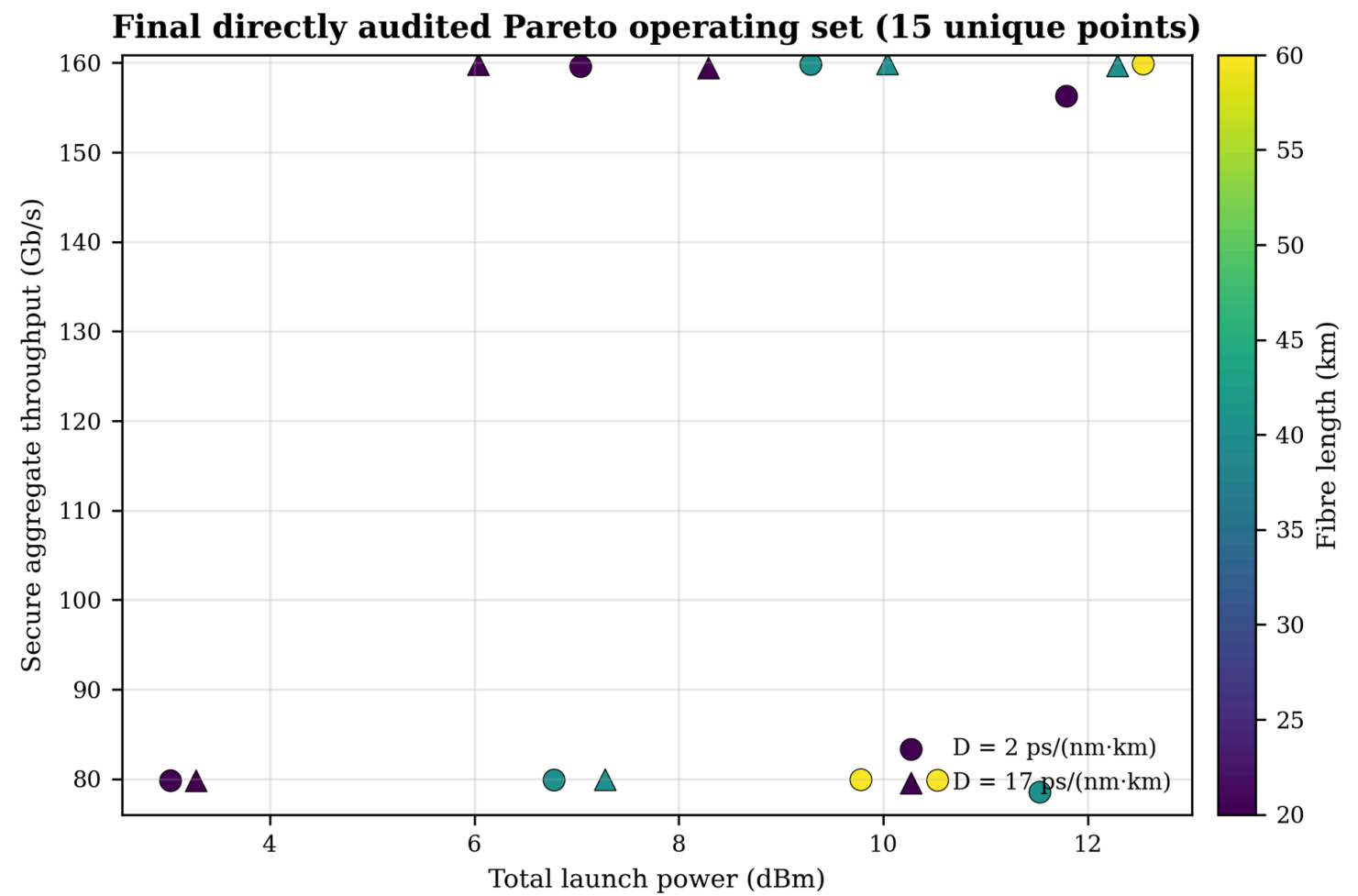


Figure 4

Final directly audited Pareto operating set; marker shape denotes dispersion and colour denotes fibre length

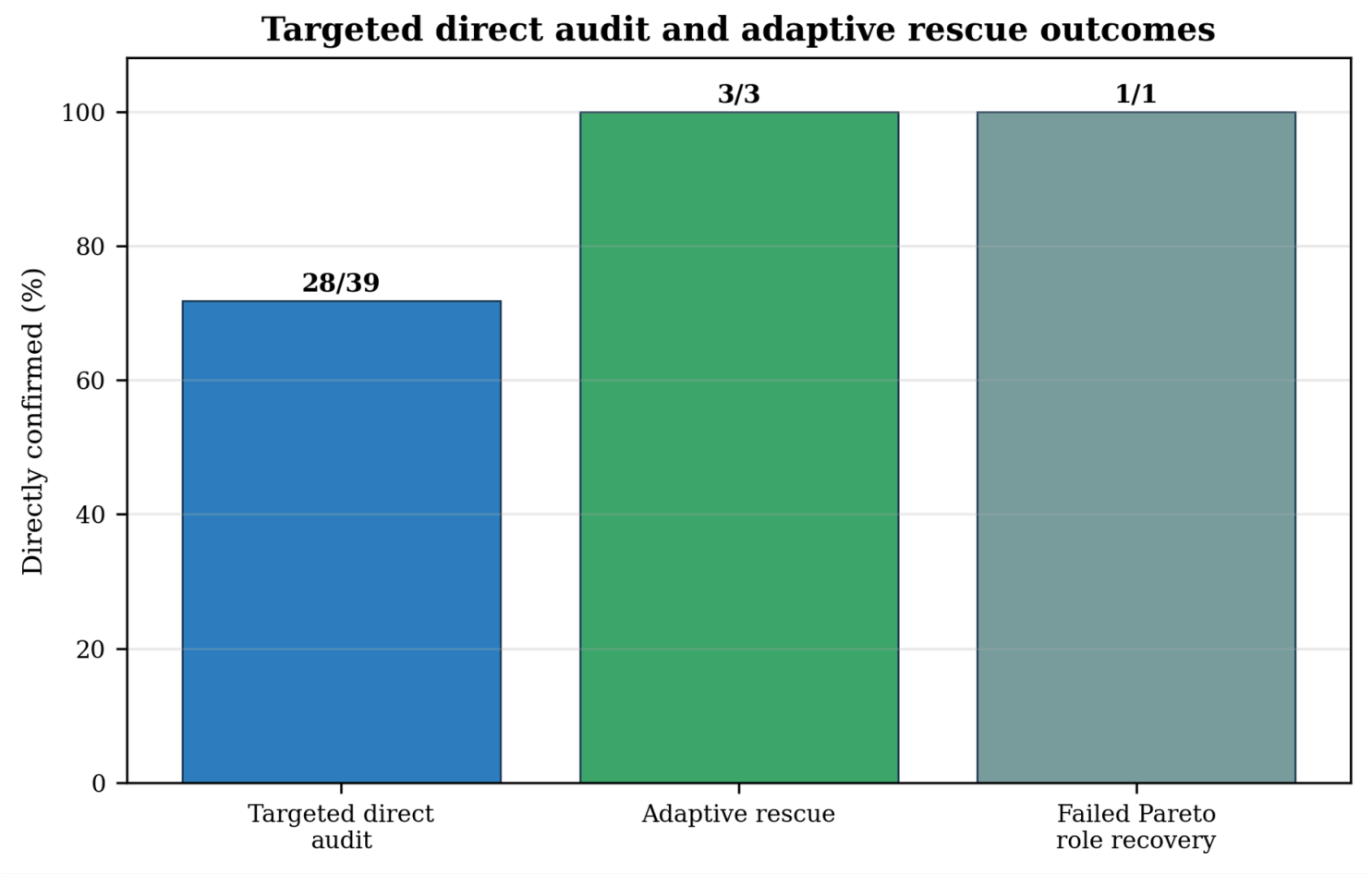


Figure 5

Direct audit, rescue, and failed-role recovery outcomes

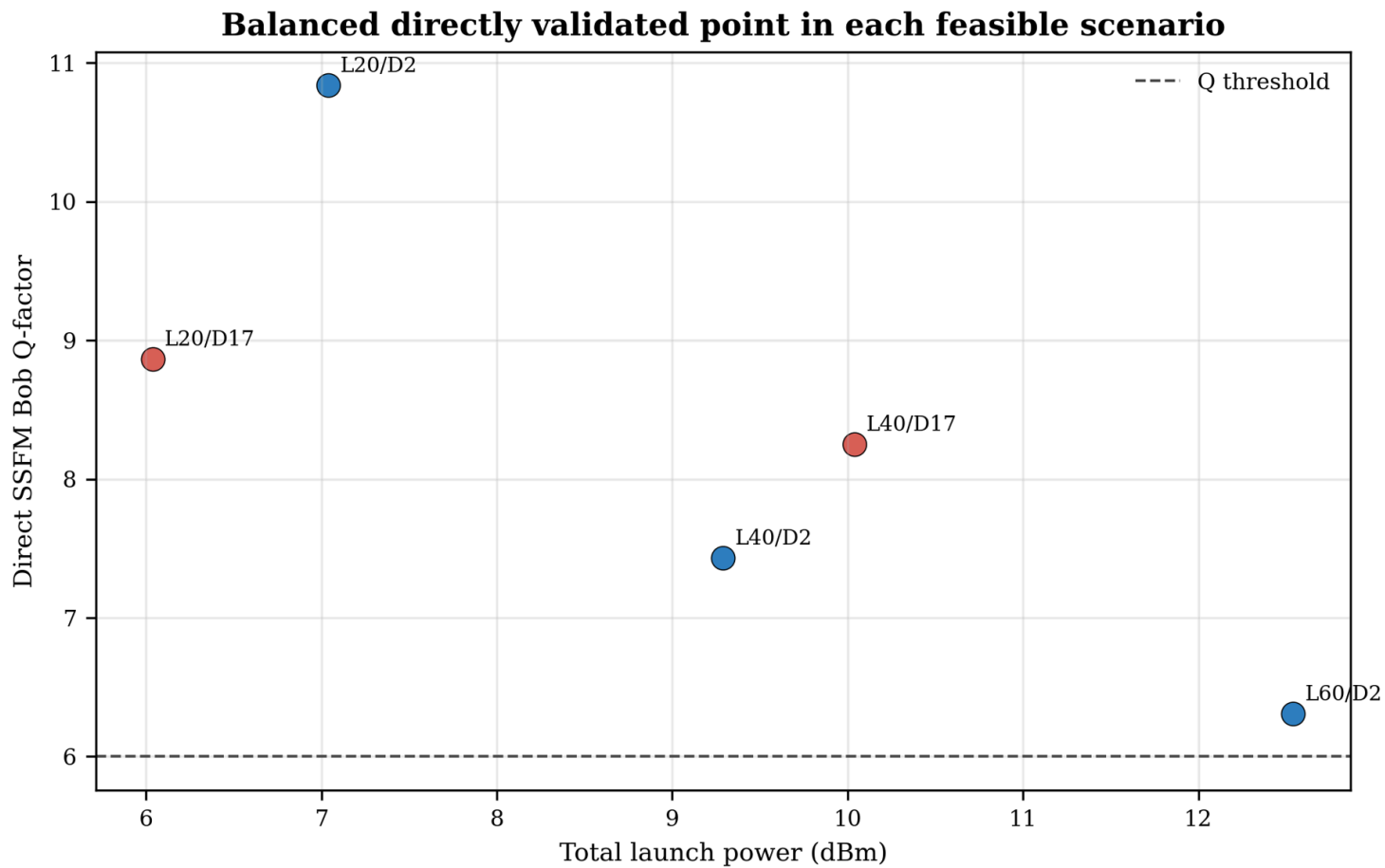


Figure 6

Direct SSFM Q-factor of the balanced point in each feasible distance–dispersion scenario

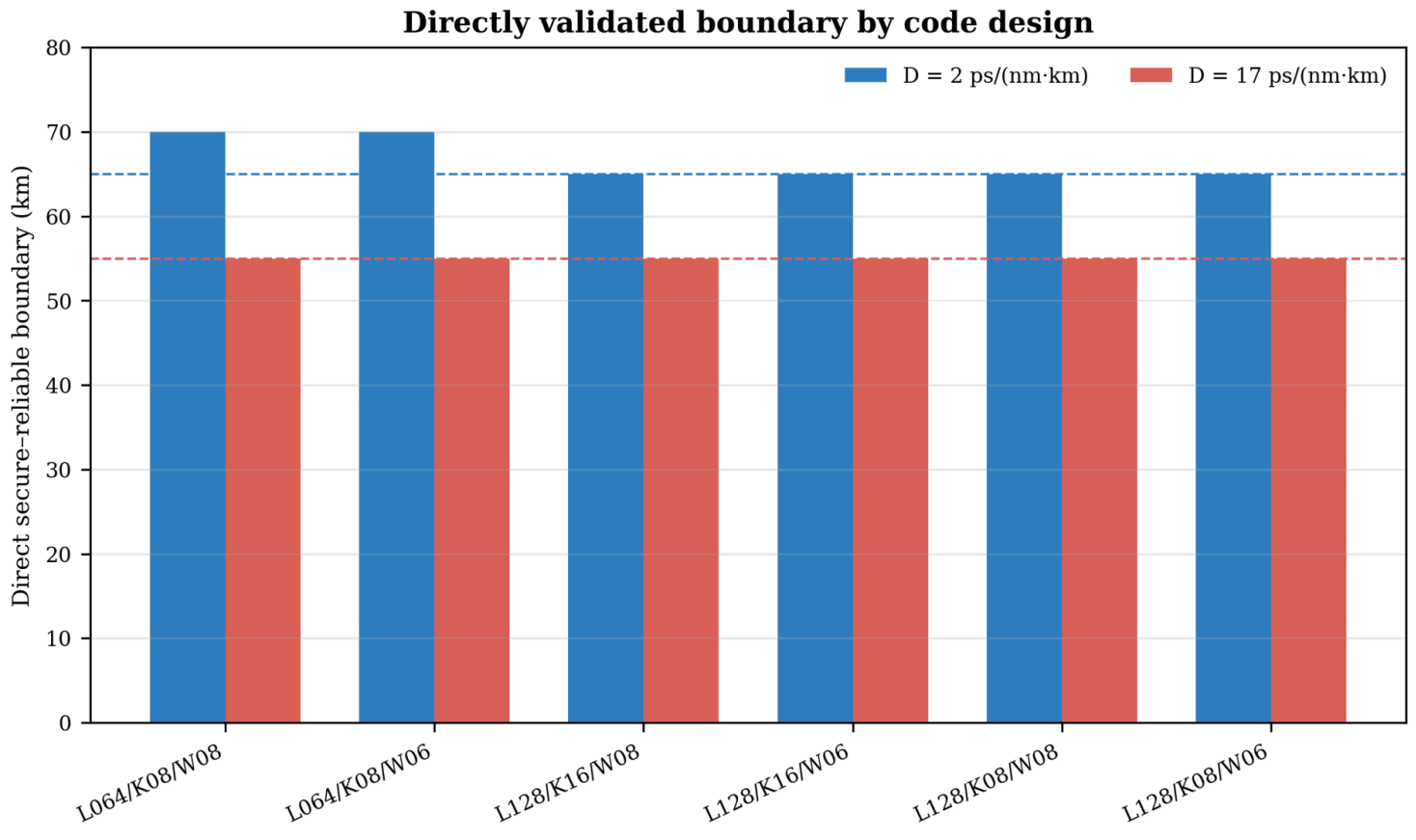


Figure 7

Directly validated boundary for each supported code design; dashed lines mark the common boundaries

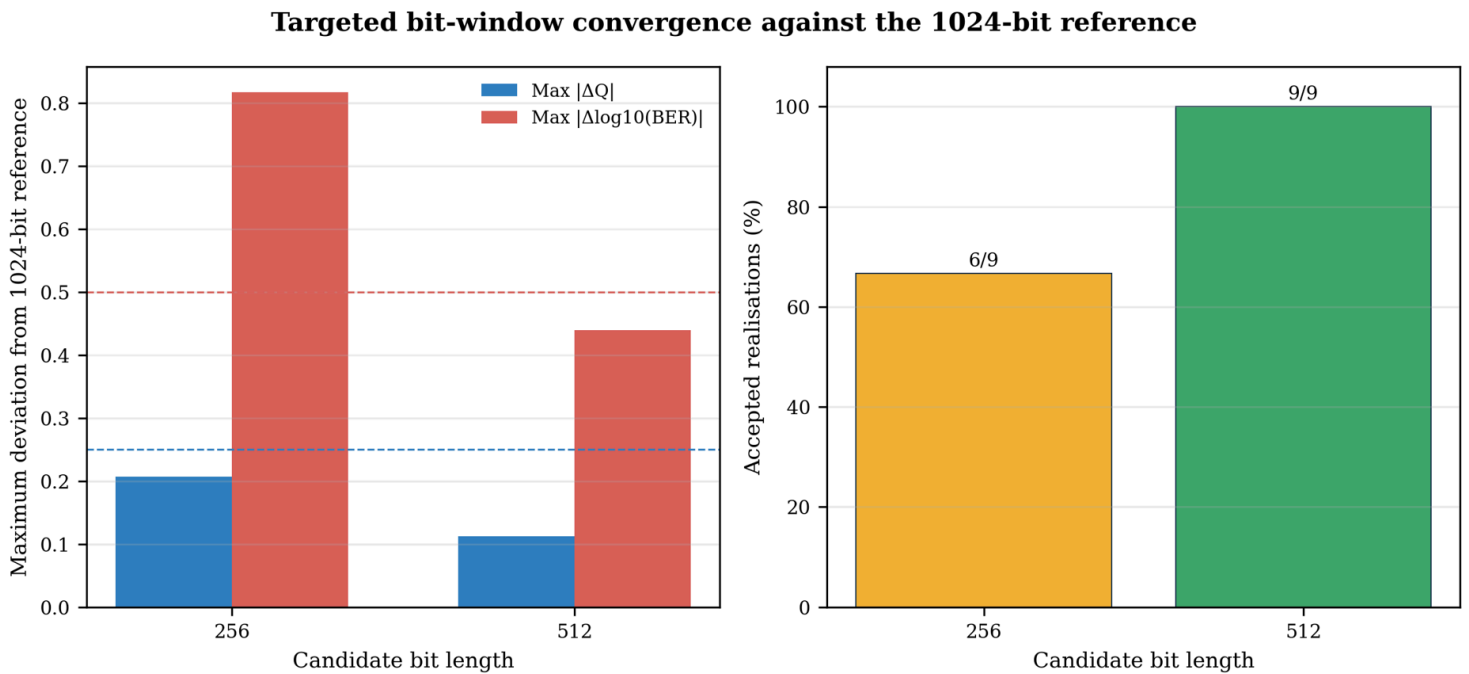


Figure 8

Targeted bit-window convergence for the critical point against the 1024-bit reference; dashed lines denote the predeclared tolerances

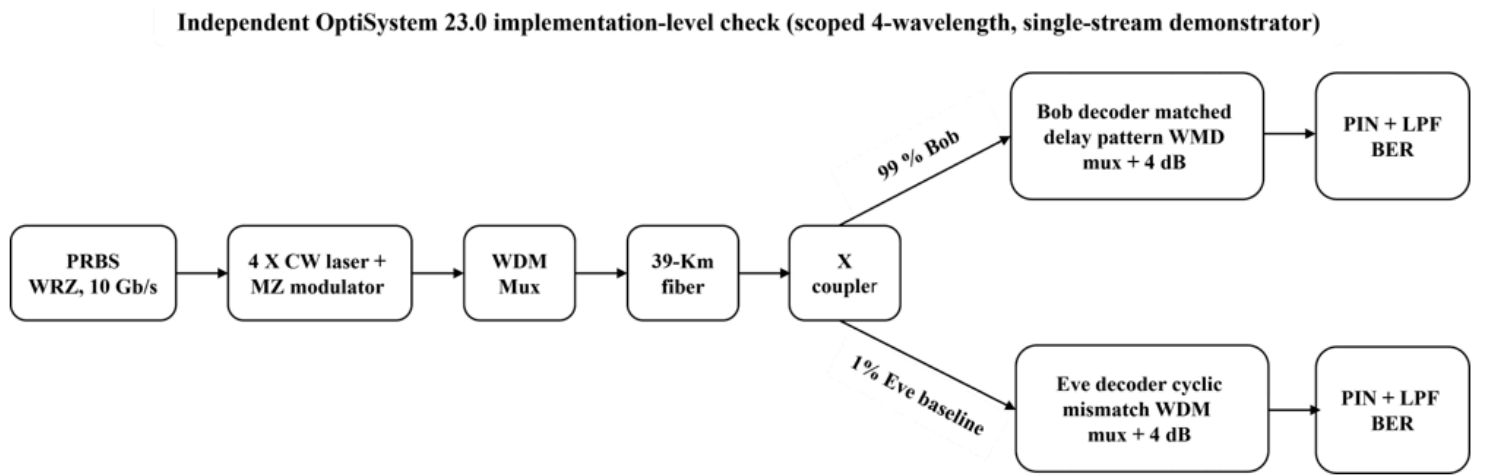


Figure 9

Scoped independent OptiSystem 23.0 implementation-level check. A 1% baseline tap is used for Eve; the 20% and 50% cases are stress tests. The delay sequences are a receiver-matching proxy, not a cryptographic key-space enumeration