

Keep Private Networks Private II: Wideband Secret Key Generation on a Real 5G NR Testbed

Sachinkumar B. Mallikarjun[†], Christoph Lipps^{*},
Marvin Reski[†], Sneha Bhattacharjee[†], Andreas Weinand[†] and Hans D. Schotten^{*†}

[†] Division of Wireless Communications and Radio Navigation, Department of Electrical and Computer Engineering,
RPTU University Kaiserslautern-Landau, Kaiserslautern, Germany

^{*}German Research Center for Artificial Intelligence (DFKI), Kaiserslautern, Germany

E-mail: [†]{mallikar, marvin.reski, bhattacharjee.sneha, andreas.weinand, schotten}@rptu.de

^{*}{christoph.lipps, schotten}@dfki.de

Abstract—Secret Key Generation (SKG) from wireless channel reciprocity has been demonstrated on WiFi, LTE, and LoRaWAN. SKG feasibility on real 5G New Radio (NR) hardware, using wideband channel estimates from uplink Sounding Reference Signals (SRS) and downlink Channel State Information Reference Signals (CSI-RS), is examined in this work. An over-the-air testbed built from OpenAirInterface (OAI) gNB and nrUE instances on USRP software-defined radios operates at 3.75 GHz (n78) with 40 MHz bandwidth, and frequency-domain estimates are captured at both endpoints across thirteen line-of-sight and non-line-of-sight scenarios in SISO and MIMO antenna configurations. An asymmetry in the subcarrier ordering of OAI channel estimates is identified and resolved by an automatic orientation detector, which restores reciprocity without manual intervention. An offline symmetric pipeline of reciprocity enhancement, quantisation, information reconciliation, privacy amplification, and key verification then yields matching 256-bit keys in every scenario, reducing the bit disagreement rate from 9.3–31.6% to 0% from 571 to 6,592 aligned channel observations at an implied key rate of approximately 1,320 bps. Per-bit Shannon entropy is 0.991 to 1.000, 11 of 12 applicable NIST SP 800-22 tests pass, and an inter-session Hamming distance of 48.8% is close to the 50% expected for independent keys.

Index Terms—5G, 6G, secret key generation, sounding reference signal, CSI reference signal, physical layer security.

I. INTRODUCTION

Secret Key Generation (SKG) based on wireless channel reciprocity enables two communicating parties to derive symmetric cryptographic keys from the inherent randomness of their common wireless channel, without relying on pre-shared secrets or public key infrastructure [1], [2]. The achieved security level exhibits information-theoretic characteristics. An eavesdropper positioned more than half a wavelength ($\lambda/2$) from either party observes a statistically independent channel, yielding positive secrecy capacity regardless of the adversary's computational resources [1].

Prior work has systematically demonstrated SKG across multiple wireless technologies with increasing bandwidth. For instance, in WiFi (IEEE 802.11n, 20 MHz at 2.4 GHz), CSI amplitude features could achieve Key Generation Rates (KGR) of 10–20 bps [2]. In LTE (5 MHz at 2.685 GHz), a Discrete Cosine Transform (DCT) and linear regression (DCT+LR)

reciprocity enhancement reduces the Bit Disagreement Rate (BDR) from 8.2% to 0.39% while increasing entropy to 0.97 bits per sample [1]. Related experimental work covers IEEE 802.11 on the WARP platform [3], D2D links in LTE [4], and MIMO and mmWave heterogeneous networks [5]. Resource-constrained IoT deployments have been extensively studied [6], [7], including utilization of SRAM-PUFs for robust, low-overhead authentication and key derivation [8]. In LoRaWAN (125 kHz at 868 MHz), autoencoder-based feature enhancement increases the KGR from 1.2 to 2.44 bits per probe [9]. These results establish a consistent relationship whereby KGR scales proportionally with bandwidth, as each additional coherence bandwidth (B_c) provides an independent channel sample for key extraction.

5G NR in TDD mode represents the natural progression in this line of investigation. Operating in the n78 band at 3.75 GHz with up to 100 MHz bandwidth, the Sounding Reference Signal (SRS) is an uplink reference signal designed for wideband channel sounding, providing dense frequency-domain channel measurements that are well suited for SKG.

But, to our knowledge, no prior work has demonstrated experimental symmetric SKG on 5G NR using SRS and CSI-RS: existing 5G-targeted studies are simulation-based [10] or use narrowband pilots rather than the wideband SRS/CSI-RS estimates available in operational NR deployments [11]. This work addresses that gap using a real over-the-air OAI testbed: SRS estimates at the gNB and CSI-RS estimates at the UE are captured over the air, and an offline SKG pipeline applied to the two traces yields matching 256-bit keys.

The main contributions of this work are as follows: (1) The first symmetric 5G NR SKG demonstration using SRS and CSI-RS using an over-the-air (OTA) testbed (OAI + USRP B210), generating matching 256-bit keys across thirteen independent scenarios spanning both a 1×1 SISO link and a 4×4 MIMO gNB / 1×1 SISO UE link. (2) The discovery and correction of OAI's asymmetric subcarrier storage between gNB and UE, together with an automatic orientation detector that adapts to firmware variants. (3) A back-propagating cascade reconciliation protocol that corrects BDR values up to 31.6% by re-checking earlier pass blocks

after each forward correction pass. (4) An initial key quality evaluation comprising per-key Shannon entropy ($H_1 = 0.991$ – 1.000), min-entropy (218 to 253 effective bits per 256-bit key), and NIST SP 800-22 randomness testing (11 of 12 applicable tests pass). (5) A cross-technology comparison completing the WiFi→LTE→LoRaWAN→5G NR progression.

II. BACKGROUND: SRS FOR SECRET KEY GENERATION

This section describes the relevant SRS configuration and the seven-stage pipeline that derives a symmetric secret key.

A. Sounding Reference Signal in 5G NR

The SRS is an uplink reference signal defined in 3GPP TS 38.211, based on Zadoff-Chu sequences transmitted by the UE for channel sounding [12]. In TDD mode, the gNB utilises the SRS to estimate the uplink channel frequency response $\hat{H}_{UL}(f_k)$ across the full carrier bandwidth. Conversely, the CSI Reference Signal (CSI-RS) is a downlink reference signal that the UE uses to estimate the downlink channel $\hat{H}_{DL}(f_k)$. By TDD reciprocity, $\hat{H}_{UL} \approx \hat{H}_{DL}$ within the coherence time, providing the reciprocal observations required for symmetric SKG.

The SRS supports configurable comb structures ($K_{TC} \in \{2, 4, 8\}$), bandwidths up to 272 resource blocks (RBs), periodicities from 1 to 2,560 slots, and 1/2/4 OFDM symbols. For SKG applications, comb-2 maximises subcarrier density, full bandwidth exploits all available frequency diversity, and the periodicity is configured to satisfy the Nyquist criterion relative to the channel coherence time.

B. SKG Pipeline

The symmetric SKG pipeline realised in this work comprises seven stages, as illustrated in Fig. 1:

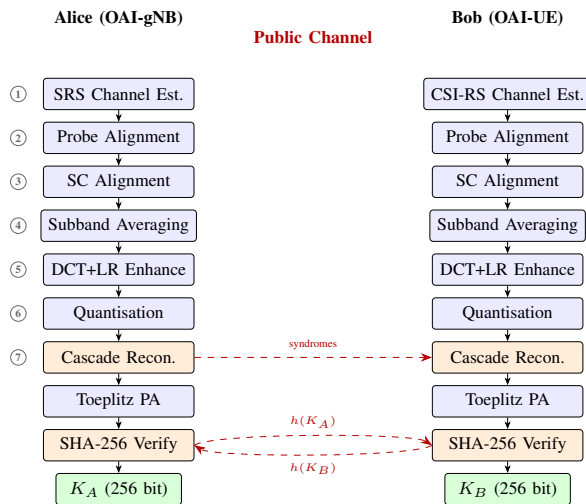


Fig. 1. End-to-end symmetric SKG pipeline. Alice (OAI-gNB) and Bob (OAI-UE) independently extract channel estimates via SRS and CSI-RS, respectively; the recorded estimates are then processed offline by the seven-stage pipeline.

- 1) **Channel probing:** The gNB estimates the uplink channel via SRS, while the UE estimates the downlink channel via CSI-RS. Both frequency-domain estimates

$\hat{H}_{gNB}(f_k)$ and $\hat{H}_{UE}(f_k)$ are recorded via OAI's T tracer tool. Probe pairs are temporally aligned using a greedy nearest-neighbour matcher with a maximum permissible offset of 200 ms.

- 2) **Subcarrier alignment and feature extraction:** Active subcarrier bands are detected, and an automatic orientation detector selects the correct UE negative-frequency mapping. Only the overlapping negative-frequency subcarriers are retained (Section III-C).
- 3) **Subband averaging:** The aligned subcarrier amplitudes $|\hat{H}(f_k)|$ are grouped into N_{sb} subbands and averaged, reducing inter-subcarrier correlation.
- 4) **DCT+LR reciprocity enhancement:** A DCT retains the low-frequency coefficients (top 50%), concentrating channel energy and suppressing noise. Linear regression subsequently aligns the UE's denoised measurements to those of the gNB, compensating for RF chain asymmetries [1].
- 5) **Multi-level quantisation:** Per-subband amplitudes are quantised into $Q = 2$ levels using equi-probable thresholds, producing 1 bit per subband per probe.
- 6) **Back-propagating cascade reconciliation:** A multi-pass cascade protocol with alternating block sizes applies parity-based binary-search error correction. After each forward pass, the protocol back-propagates to re-check all earlier-pass blocks where corrections may have exposed previously hidden even-parity errors [1].
- 7) **Privacy amplification and key verification:** A Toeplitz-matrix universal hash function compresses the reconciled bit string, removing information leaked during reconciliation (security parameter $\epsilon = 32$ bits). Both parties verify key equality via SHA-256 hash exchange.

III. SYSTEM DESIGN

This section describes the testbed and the design choices that turn raw OAI channel estimates into quantised key material. It covers the radio configuration, the bilateral capture of SRS and CSI-RS estimates, the subcarrier alignment those estimates require, and the subband, enhancement, and quantisation parameters that set the key generation rate.

A. Testbed Configuration

The testbed comprises two USRP SDRs executing OAI 5G NR gNB and nrUE on the n78 band at 3.75 GHz with 40 MHz bandwidth (106 RBs, 30 kHz SCS). The TDD pattern is configured as DDDSU (3 DL, 1 Special, 1 UL) with a 2.5 ms period. In SISO scenario USRP B210 are used for both gNB and UE, while in MIMO scenario, USRP X410 is used for gNB and USRP B210 for UE. In the MIMO scenario the gNB uses four receive branches and a four-port SRS resource, so the T tracer buffer is laid out as [antenna][port][subcarrier]. The pipeline reads only the first receive antenna and first port, that is, a single spatial channel; no combining or per-stream processing is introduced and the processing is identical to the SISO case. These captures therefore test whether extraction and alignment

survive the change of front end and firmware, not whether spatial multiplexing raises the key rate. Automatic gain control (AGC) is disabled; `rx_gain` is fixed at 60 dB. OAI is used over other projects because it provides built-in SRS channel estimate export via the T tracer tool, recording frequency-domain LS estimates in Q15 format with linear interpolation between comb positions.

The SRS is configured with comb-2, full bandwidth (106 RBs = 636 SRS subcarriers per probe), 1 symbol, and a periodicity of 10 slots (5 ms). Both gNB (via SRS) and UE (via CSI-RS) channel estimates are captured simultaneously using T tracer, thereby enabling symmetric key generation. At 3.75 GHz, the Nyquist criterion requires a probe period satisfying $T_p < T_c/2$; for pedestrian mobility at 3 km/h ($f_d = 10.4$ Hz, $T_c = 48$ ms), the 5 ms period satisfies this criterion with a $9.6\times$ margin.

B. Bilateral CSI Extraction via T tracer

Channel estimates from both sides are recorded simultaneously using OAI's T tracer binary logging tool. On the gNB side, the event `GNB_PHY_UL_FREQ_CHANNEL_ESTIMATE` captures the SRS-based uplink channel estimate. On the UE side, the event `UE_PHY_DL_CHANNEL_ESTIMATE_FREQ` captures the CSI-RS-based downlink channel estimate. Both events store per-subcarrier frequency-domain samples in OAI's `c16_t` format: each 32-bit word encodes an I/Q pair as two signed 16-bit integers (I in the lower 16 bits, Q in the upper 16 bits), normalised by the Q15 scale factor:

$$\hat{H}(f_k) = \frac{I_k + jQ_k}{32768} \quad (1)$$

Each raw event additionally includes a nanosecond-resolution timestamp (`tv_sec`, `tv_nsec`). Probe pairing is greedy over the UE record: each UE probe takes the nearest still-unassigned gNB probe within a 200 ms bound, and the pairs are then re-sorted into gNB temporal order. Since SRS and CSI-RS are driven by the same TDD frame structure, the two streams are quasi-synchronous, so the bound serves only to reject outliers; probes left unmatched are discarded, which is why the aligned pair counts of Table I fall below the recorded probe counts.

C. Subcarrier Layout Discovery and Alignment

A critical implementation finding is that OAI stores the gNB and UE frequency-domain channel estimates with different subcarrier layouts within the 1536-point FFT (corresponding to 40 MHz bandwidth at 30 kHz SCS), as illustrated in Fig. 2. The gNB follows standard FFT ordering, whereas the UE places its [132, 768] 636 positive-frequency bins first, leaves a zero-padded gap, and stores only [900, 1272] 372 negative-frequency bins in reversed order.

Pairing gNB and UE subcarriers without correcting this reversal produces near-zero reciprocity correlation; reversing the UE's negative-frequency bins raises the per-subband amplitude correlation from $\rho \approx 0.05$ to $\rho \approx 0.72$ (6 subbands), restoring the physical frequency alignment required for SKG.

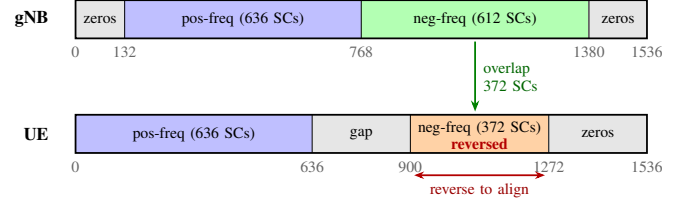


Fig. 2. Asymmetric FFT storage conventions employed by OAI for gNB (SRS) and UE (CSI-RS) channel estimates within the 1536-point FFT. The overlapping negative-frequency subcarriers (372 SCs) are utilised for symmetric SKG following reversal of the UE's bin ordering.

The ordering is not fixed, however: some OAI builds store the negative-frequency bins reversed and others in standard order. The pipeline therefore computes absolute per-probe correlations under both orderings over 200 randomly sampled probe pairs and, when the margin falls below 0.05, processes both orientations through the full quantisation pipeline and selects the one yielding the lower BDR.

D. Subband Quantisation Strategy

Per-subcarrier quantisation yields redundant bits from correlated samples within the coherence bandwidth B_c . The overlapping negative-frequency subcarriers span approximately 22.3 MHz (372×60 kHz effective spacing for comb-2). These subcarriers are grouped into N_{sb} subbands, each averaged and quantised into two equi-probable levels, yielding 1 bit per subband per probe. Starting from $N_{sb} = 12$ (31 SCs, ≈ 1.86 MHz per subband), the pipeline attempts 18, 24 and 31 when reconciliation leakage leaves an insufficient bit budget for a 256-bit key, which is what the high-BDR traces require. The choice $Q = 2$ is empirical: $Q = 4$ produced BDR beyond the correction capability of the reconciliation protocol.

E. DCT+LR Enhancement

The DCT+LR technique, previously validated on LTE (FDD) [1], is applied to the bilateral 5G NR (TDD) subband amplitude sequences. For each aligned probe pair, the subband amplitude vectors from gNB and UE are independently transformed via the DCT; the top 50% of coefficients are retained, thereby suppressing high-frequency noise components. Linear regression is then applied per aligned probe pair. With $\hat{\mathbf{h}}_A$ and $\hat{\mathbf{h}}_B$ the denoised N_{sb} -element subband amplitude vectors at gNB and UE, an ordinary least-squares fit determines the scalar gain a and offset b minimising $\|\hat{\mathbf{h}}_A - (a\hat{\mathbf{h}}_B + b)\|^2$, and the UE vector is replaced by $a\hat{\mathbf{h}}_B + b$ before quantisation. The two-parameter affine model absorbs the systematic RF chain asymmetry between the radios, principally gain imbalance and a constant amplitude offset, while retaining the per-subband variation that carries the key material. DCT+LR raises the mean per-probe subband correlation from 0.30 to 0.69 (Fig. 3), with the residual BDR corrected by cascade reconciliation. A negative fitted slope additionally absorbs the polarity inversion caused by an incorrect bin ordering, which is why two traces recover from negative pre-enhancement correlation in Fig. 3.

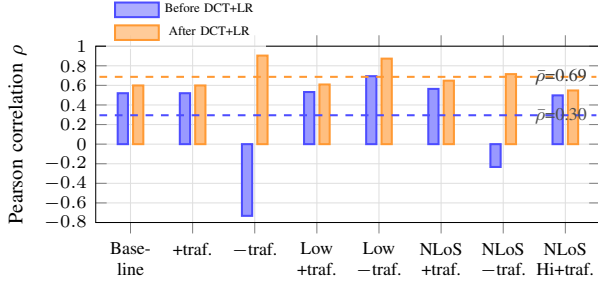


Fig. 3. Per-subband amplitude correlation before and after DCT+LR reciprocity enhancement across the eight SISO baseline traces. DCT denoising and linear regression alignment improve the mean correlation from 0.30 to 0.69. Traces 3 and 7 exhibit negative pre-enhancement correlation due to polarity inversion from the UE's reversed FFT bin ordering (corrected by LR).

F. Key Generation Rate

The raw key generation rate is defined as:

$$\text{KGR}_{\text{raw}} = N_{\text{sb}} \times \log_2 Q \times f_{\text{probe}} \quad (2)$$

With $N_{\text{sb}} = 12$ subbands (baseline configuration), $Q = 2$ quantisation levels, and $f_{\text{probe}} = 200$ Hz (5 ms SRS period), the raw rate is $\text{KGR}_{\text{raw}} = 12 \times 1 \times 200 = 2,400$ bits/s. After accounting for reconciliation leakage and privacy amplification ($\eta \approx 0.55$), corresponding to one 256-bit key per ≈ 194 ms of captured channel material, which would support sub-second key refresh in an in-stack implementation.

IV. EXPERIMENTAL SETUP AND RESULTS

This section reports the measurement campaign and the resulting key materials. Performance is assessed by BDR and key agreement, by entropy, and by NIST randomness tests. The results are compared against the other radio technologies.

A. Measurement Campaign

Thirteen independent OTA scenarios were conducted at RPTU Kaiserslautern-Landau with gNB and UE separated by approximately 1–2 m at different positions, all using the radio configuration described above. The baseline campaign comprises eight 1×1 SISO scenarios, five indoor line-of-sight (LoS) and three non-line-of-sight (NLoS) with physical obstructions between transmitter and receiver, varying in background PDSCH traffic (with/without) and PDSCH scheduling rate (standard/reduced). Three longer LoS anchor captures (Anc. 01–03) and two captures with the gNB reconfigured as a 4×4 MIMO receiver complete the set; per-trace pair counts are listed in Table I.

The pipeline is applied offline to the recorded T tracer traces, with automatic configuration: overlapping negative-frequency subcarriers (auto-detected), adaptive subbands (initialised at 12, auto-scaled as required), 2-level quantisation, DCT keep ratio 0.5, back-propagating cascade reconciliation with block size 4 and 4 passes, Toeplitz privacy amplification, and automatic UE bin-ordering detection.

TABLE I
5G NR SYMMETRIC SKG RESULTS (13 SCENARIOS)

Type	Trace	Pairs	BDR _{pre}	BDR _{post}	Match
1×1 SISO gNB / 1×1 SISO UE					
LoS	Baseline	571	16.7%	0.00%	Yes
LoS	+traffic	777	16.7%	0.00%	Yes
LoS	–traffic	788	9.3%	0.00%	Yes
LoS	Low+traf.	771	16.9%	0.00%	Yes
LoS	Low,–traf.	749	10.0%	0.00%	Yes
NLoS	Low+traf.	796	26.0%	0.00%	Yes
NLoS	Low,–traf.	699	11.0%	0.00%	Yes
NLoS	Hi+traf.	792	31.6%	0.00%	Yes
LoS	Anc. 01, –traf.	2,123	14.9%	0.00%	Yes
LoS	Anc. 02, +traf.	5,443	14.3%	0.00%	Yes
LoS	Anc. 03, +traf.	6,397	12.9%	0.00%	Yes
4×4 MIMO gNB / 1×1 SISO UE					
LoS	MIMO	6,592	12.4%	0.00%	Yes
LoS	MIMO Anc. A	6,022	15.8%	0.00%	Yes

B. SKG Performance

Table I summarises end-to-end performance across all thirteen scenarios: every trace produces matching 256-bit keys with zero residual bit errors after reconciliation. The raw BDR ranges from 9.3% (LoS, no traffic) to 31.6% (NLoS, high PDSCH rate with traffic), reflecting hardware asymmetry, imperfect TDD reciprocity, NLoS multipath, co-channel interference, and quantisation noise. The back-propagating cascade protocol corrects all errors across this range. Corrections in pass k can convert even-parity (undetectable) blocks from passes $0, \dots, k-1$ into odd-parity ones, so re-checking earlier passes recovers errors that a forward-only cascade leaves in place. This mechanism is essential for the NLoS traces with BDR above 25%.

The highest-BDR trace (31.6%, NLoS with high PDSCH rate) required auto-scaling from 12 to 18 subbands to supply sufficient raw bits after reconciliation leakage. Traces without background PDSCH traffic consistently exhibit lower BDR (9.3–11.0%) than traces with traffic (16.7–31.6%), indicating that co-channel interference from scheduled PDSCH transmissions adds non-reciprocal distortion to the channel estimates.

The two 4×4 MIMO anchor traces (final rows of Table I), recorded in independent sessions, align 6,592 and 6,022 probe pairs at pre-reconciliation BDR (12.4% and 15.8%) consistent with the SISO LoS anchors and reduce to 0.00% post-reconciliation, yielding matching 256-bit keys $K_A = K_B$ on both pairs. The Hamming distance between the two independent MIMO Alice keys is $d_H = 125/256 = 48.8\%$, close to the 50% expected for independent uniformly random strings, indicating no detectable session-level structural bias after privacy amplification.

C. Key Randomness and Entropy Analysis

A generated key is cryptographically useful only if it is statistically indistinguishable from a uniformly random bit

TABLE II
PER-KEY ENTROPY ANALYSIS (256-BIT PA KEYS)

Type	Trace	H_1	H_2	H_4	H_∞	Eff.
1×1 SISO gNB / 1×1 SISO UE						
LoS	Baseline	1.000	0.998	0.950	0.978	250.3
LoS	With traffic	1.000	0.989	0.949	0.967	247.4
LoS	W/o traffic	0.995	0.989	0.949	0.881	225.6
LoS	Low+traffic	1.000	0.990	0.974	0.989	253.1
LoS	Low, no traffic	1.000	0.997	0.971	0.989	253.1
NLoS	Low+traffic	0.991	0.987	0.944	0.850	217.7
NLoS	Low, no traffic	0.999	0.998	0.984	0.945	241.8
NLoS	High+traffic	0.996	0.978	0.930	0.891	228.2
4×4 MIMO gNB / 1×1 SISO UE						
LoS	MIMO Anc. A	1.000	0.996	0.962	0.978	250.3
LoS	MIMO Anc. B	0.999	0.994	0.962	0.945	241.8

Eff. = effective min-entropy bits out of 256.

string. The quality of the generated keys is evaluated using two complementary approaches: per-key entropy analysis and the NIST SP 800-22 statistical test suite. Given the limited quantity of key material available in this campaign, the results below are reported as preliminary evidence of good randomness properties, not as complete statistical validation.

1) *Shannon and Min-Entropy*: Table II presents the per-key entropy analysis for all ten 256-bit privacy-amplified keys (eight SISO and two MIMO). Rényi entropy of orders 1, 2, 4, and 8 (denoted H_1 , H_2 , H_4 , H_8), normalised to bits per bit, is computed along with the min-entropy $H_\infty = -\log_2(\max_i p_i)$, where p_i denotes the probability of the most likely bit value.

The per-bit Shannon entropy H_1 ranges from 0.991 to 1.000 across all keys, indicating near-ideal bit balance. The higher-order Rényi entropies H_2 and H_4 remain above 0.93 in all cases, consistent with statistical independence at the 2-bit and 4-bit block levels.

The min-entropy H_∞ ranges from 0.850 (NLoS, Low PDSCH+traffic, $p(1) = 0.555$) to 0.989 (LoS, Low PDSCH), that is 218 to 253 effective bits per 256-bit key; the worst case exceeds the 128-bit AES-128 level by 1.7 times (Fig. 4).

Two trends recur: LoS keys show higher entropy than NLoS keys, and PDSCH traffic marginally lowers entropy through interference that biases the quantisation statistics.

The H_8 values of 0.60–0.63 reflect under-sampling, not an entropy deficiency: a 256-bit key provides only 32 blocks of 8 bits across 2^8 possible patterns, and the estimate would be expected to increase with a larger key population.

2) *NIST SP 800-22 Randomness Testing*: To evaluate randomness at the aggregate level, the eight SISO 256-bit privacy-amplified keys are concatenated into a single 2,048-bit sequence and subjected to the NIST SP 800-22 statistical test suite [15]. Table III summarises the results.

Of the 15 NIST tests, 12 are applicable to the 2,048-bit sample; Maurer’s Universal and the two Random Excursions tests require substantially longer sequences. Eleven of the 12 pass at the 0.01 significance threshold, with most p -values above 0.3.

The single non-passing result, Approximate Entropy ($p = 0.0002$), is consistent with the limited sample size and need

TABLE III
NIST SP 800-22 RESULTS (2,048 BITS, 8×256 -BIT KEYS)

Test	p -value	Result
Frequency (Monobit)	0.6269	PASS
Block Frequency	0.5546	PASS
Runs	0.1866	PASS
Longest Run of Ones	0.7912	PASS
Binary Matrix Rank	0.7419	PASS
DFT (Spectral)	0.5702	PASS
Non-overlapping Template	0.7295	PASS
Overlapping Template	0.0250	PASS
Maurer’s Universal	—	N/A ^a
Linear Complexity	0.3326	PASS
Serial	0.5978	PASS
Approximate Entropy	0.0002	FAIL ^b
Cumulative Sums	0.7787	PASS
Random Excursions	—	N/A ^a
Random Excursions Variant	—	N/A ^a

^aRequires $\geq 387K$ bits or ≥ 500 cycles.

^bExpected at $n = 2,048$: $m = 10$ requires 2^{10} pattern bins.

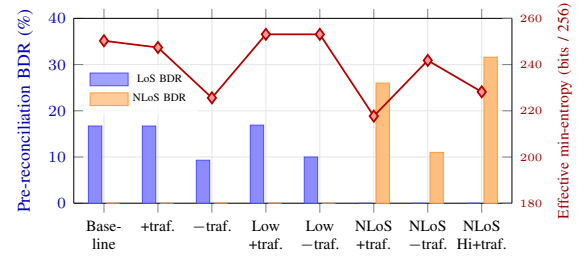


Fig. 4. Pre-reconciliation BDR (bars, left axis) and effective min-entropy bits (diamond markers, right axis) for the eight SISO baseline scenarios. All traces achieve 0% post-reconciliation BDR. The worst-case min-entropy (218 bits, NLoS) exceeds the 128-bit AES security threshold by 1.7 $\times$.

not indicate a deficiency in key randomness. This test employs block length $m = 10$, requiring pattern counts distributed across $2^{10} = 1,024$ bins from only 2,048 bits. With fewer than 2 samples per bin on average, sampling variance dominates the test statistic, making a Type I outcome likely, as corroborated by the passing Block Frequency and Serial tests.

The NIST results, with the per-key entropy analysis, suggest that the Toeplitz-matrix privacy amplification suppresses both reconciliation leakage and residual structure in the channel-derived bit sequences, operating with effective security parameters from 260 bits (NLoS, high PDSCH+traffic) to 1,316 bits (LoS, without traffic). In the worst case this bounds the statistical distance to a uniform distribution by 2^{-130} under the leftover hash lemma [16], conditional on the min-entropy estimates of Table II.

D. Cross-Technology Comparison

Table IV positions the 5G NR result within the cross-technology progression. At 40 MHz the effective rate of $\sim 1,320$ bps is approximately 66 $\times$ the 20 MHz WiFi baseline, in line with wider bandwidth yielding proportionally more independent frequency-domain taps. The 5G NR system also achieves the lowest post-enhancement BDR (0.00%) among all evaluated technologies and is the first entry in this series to include NLoS scenarios, while the pipeline structure remains consistent across all four technologies [14].

TABLE IV
CROSS-TECHNOLOGY SKG COMPARISON

	WiFi	LTE	LoRa	5G NR
Freq (GHz)	2.4	2.685	0.868	3.75
BW (MHz)	20	5	0.125	40
BDR (enh.)	<1%	0.39%	7.15%	0.00%
KGR (bps)	10–20	5–10	1.2–2.4	~1,320
Enh.	DCT+LR	DCT+LR	AE	DCT+LR
Scenarios	LoS	LoS	LoS	LoS+NLoS
NIST	15/15	15/15	15/15	11/12 [†]

[†]12 applicable; 11 pass (Sec. IV-C).

E. Limitations and Scalability

The present results are bounded in several respects. The links are short-range indoor (1–2 m); at greater separation the lower SNR is expected to raise the pre-reconciliation BDR, and the additional reconciliation leakage must be offset by further subband scaling, which lowers the effective KGR. Both terminals are static: the 5 ms SRS period satisfies $T_p < T_c/2$ only up to approximately 14 km/h ($f_d = 50$ Hz, $T_c \approx 10$ ms), above which probe pairs decorrelate and the BDR rises. The SRS periodicity is configurable down to one slot, 0.5 ms at 30 kHz SCS, which extends the criterion to roughly 140 km/h at a proportional increase in reference signal overhead, so mobility imposes an overhead cost, not a fundamental limit. Finally, the 40 MHz bandwidth is a USRP B210 limitation and not an NR one; the X410 already used for the MIMO gNB supports the full 100 MHz n78 carrier, giving approximately $2.5\times$ the subcarriers and, on the bandwidth-KGR trend of Table IV, a proportionally higher rate. Environments with larger delay spread have a smaller coherence bandwidth and therefore admit more independent subbands, so the usable N_{sb} is deployment dependent. Multi-user operation, in which several UEs are sounded within the same SRS resource, is not evaluated.

V. CONCLUSION

This work presents the first and preliminary experimental symmetric Secret Key Generation system exploiting 5G NR SRS (gNB) and CSI-RS (UE) on a real over-the-air testbed using OpenAirInterface. The principal contributions encompass: (i) discovery and automatic correction of OAI’s asymmetric subcarrier storage via an orientation detector with BDR-probe fallback; (ii) a back-propagating cascade reconciliation protocol accommodating BDR values up to 31.6%; (iii) adaptive subband scaling when reconciliation leakage exhausts the bit budget; and (iv) validation that the pipeline operates unchanged when the gNB front end is upgraded from 1×1 SISO to 4×4 MIMO (UE remaining 1×1 SISO). The seven-stage pipeline generates matching 256-bit keys on all thirteen scenarios (eleven SISO: eight LoS and three NLoS; two MIMO LoS) with 0% post-reconciliation BDR, per-bit Shannon entropy of 0.991–1.000, and 11 of 12 applicable NIST tests passing; the inter-session Hamming distance between the two MIMO keys is 48.8%. Given the limited key material these randomness results should be read as preliminary. The effective KGR of ~1,320 bps implies sub-second key generation, a two-orders-of-magnitude improvement over WiFi. Future work includes

complete NIST testing ($\geq 10^6$ bits), validation on USRP X410 with 100 MHz bandwidth, more mobility scenarios and hybrid post-quantum key establishment via ML-KEM-768.

ACKNOWLEDGMENT

This work was supported by the German Federal Ministry of Research, Technology, and Space (BMFTR) under the projects “Open6GHub+” (16KIS2406) and “SUSTAINET_guardDian” (16KIS2239K). The authors alone are responsible for the content.

REFERENCES

- [1] C. Lipps, S. B. Mallikarjun, M. Strufe, C. Heinz, C. Grimm, and H. D. Schotten, “Keep Private Networks Private: Secure Channel-PUFs, and Physical Layer Security by Linear Regression Enhanced Channel Profiles”, *3rd International Conference on Data Intelligence and Security (ICDIS)*, South Padre Island, TX, USA, 2020, pp. 93–100, DOI: 10.1109/ICDIS50059.2020.0001.
- [2] A. Ambekar and H. D. Schotten, “Enhancing channel reciprocity for effective key management in wireless ad-hoc networks” *IEEE 79th Vehicular Technology Conference (VTC Spring)*, Seoul, Korea (South), 2014, pp. 1–5, doi: 10.1109/VTCSpring.2014.7022913
- [3] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, “Experimental Study on Key Generation for Physical Layer Security in Wireless Communications”, *IEEE Access*, vol. 4, pp. 4464–4477, 2016, DOI: 10.1109/ACCESS.2016.2604618.
- [4] L. Wang, J. Liu, M. Chen, G. Gui, and H. Sari, “Optimization-Based Access Assignment Scheme for Physical-Layer Security in D2D Communications Underlying a Cellular Network”, *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 5766–5777, 2018, DOI: 10.1109/TVT.2017.2789022.
- [5] N. Yang, L. Wang, G. Geraci, M. Elksashan, J. Yuan, and M. D. Renzo, “Safeguarding 5G wireless communication networks using physical layer security”, *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015, DOI: 10.1109/MCOM.2015.7081071.
- [6] R. Guillaume, F. Winzer, A. Czylik, C. T. Zenger, and C. Paar, “Bringing PHY-Based Key Generation into the Field: An Evaluation for Practical Scenarios”, *IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, Boston, MA, USA, 2015, DOI: 10.1109/VTCFall.2015.7390857.
- [7] C. T. Zenger, M.-J. Chur, J.-F. Posielek, C. Paar, and G. Wunder, “A Novel Key Generating Architecture for Wireless Low-Resource Devices”, *International Workshop on Secure Internet of Things (SIoT)*, Wroclaw, Poland, 2014, DOI: 10.1109/SIoT.2014.7.
- [8] C. Lipps, A. Weinand, D. Krummacker, C. Fischer, and H. D. Schotten, “Proof of Concept for IoT Device Authentication Based on SRAM PUFs Using ATMEGA 2560-MCU”, *1st International Conference on Data Intelligence and Security (ICDIS)*, South Padre Island, TX, USA, 2018, DOI: 10.1109/ICDIS.2018.00013.
- [9] A. Weinand, S.B. Mallikarjun, C. Lipps, M. Karrenbauer, and H.D. Schotten, “Multi-bit Secret Key Generation for LoRaWAN based 6G mMTC using Autoencoders,” *35th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Valencia, Spain, 2024, DOI: 10.1109/PIMRC59610.2024.10817249.
- [10] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, “Key Generation From Wireless Channels: A Review” *IEEE Access*, vol. 4, pp. 614–626, 2016, DOI: 10.1109/ACCESS.2016.2521718.
- [11] G. Li, C. Sun, J. Zhang, E. Jorswieck, B. Xiao, and A. Hu, “Physical Layer Key Generation in 5G and Beyond Wireless Communications: Challenges and Opportunities” *Entropy*, vol. 21, no. 5, p. 497, 2019, DOI: 10.3390/e21050497.
- [12] 3GPP, “NR; Physical channels and modulation,” TS 38.211, v17.4.0, 2023.
- [13] Ettus Research, “USRP B210 data sheet,” National Instruments, 2023. [Online]. Available: <https://www.ettus.com/all-products/ub210-kit/>
- [14] A. Weinand, S.B. Mallikarjun, C. Lipps, M. Karrenbauer, and H.D. Schotten, “Secret Key Generation for LoRaWAN using Autoencoders for Reciprocity Enhancement” in *European Wireless*, Rome, Italy, 2023.
- [15] L.E. Bassham III, A.L. Rukhin, J. Soto, J. Nechvatal, M. Smid, S. Leigh, M. Levenson, M. Vangel, N.A. Heckert, and D.L. Banks, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”, NIST Special Publication 800-22 Rev. 1a, National Institute of Standards and Technology, Gaithersburg, MD, USA, Apr. 2010.
- [16] R. Renner and R. König, “Universally Composable Privacy Amplification Against Quantum Adversaries”, *Theory of Cryptography. TCC 2005. Lecture Notes in Computer Science*, vol. 3378, pp. 407–425, 2015, DOI: 10.1007/978-3-540-30576-7_22.