A Low-Power, 65 nm 24.6-to-30.1 GHz Trusted LC Voltage-Controlled Oscillator Achieving 191.7 dBc/Hz FoM at 1 MHz

Abdullah Kurtoglu 1,*, Amir H. M. Shirazi 2, Shahriar Mirabbasi 2 and Hossein Miri Lavasani 1,*

1 Department of Electrical, Computer, and Systems Engineering, Case Western Reserve University, Cleveland, OH 44106, USA
2 Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, BC V6T 1Z4, Canada; amirms@ece.ubc.ca (A.H.M.S.); shahriar@ece.ubc.ca (S.M.)
* Correspondence: axk1214@case.edu (A.K.); sxm1243@case.edu (H.M.L.); Tel.: +1-216-368-4436 (A.K.)

Abstract: This work presents a novel trusted LC voltage-controlled oscillator (VCO) with an embedded compact analog Physically Unclonable Function (PUF) used for authentication. The trusted VCO is implemented in a 1P9M 65 nm standard CMOS process and consumes 1.75 mW. It exhibits a measured phase noise (PN) of $-104.8$ dBc/Hz @ 1 MHz and $-132.2$ dBc/Hz @ 10 MHz offset, resulting in Figures of Merit (FoMs) of 191.7 dBc/Hz and 199.1 dBc/Hz, respectively. With the measured frequency tuning range (TR) of ~5.5 GHz, the FoM with tuning (FoM_T) reaches 197.6 dBc/Hz and 205.0 dBc/Hz at 1 MHz and 10 MHz offset, respectively. The analog PUF consists of CMOS cross-coupled pairs in the main VCO to change analog characteristics. Benefiting from the impedance change and parasitic capacitance of the cross-coupled pairs, the AC and DC responses of the VCO are utilized for multiple responses for each input. The PUF consumes 0.83 pJ/bit when operating at 1.5 Gbps. The proposed PUF exhibits a measured Inter-Hamming Distance (HD) of 0.5058b and 0.4978b, with Intra-HD reaching 0.0055b and 0.0053b for the current consumption and $f_{osc}$, respectively. The autocorrelation function (ACF) of 0.0111 and 0.0110 is obtained for the current consumption and $f_{osc}$, respectively, at a 95% confidence level.

Keywords: analog PUF; LC VCO; trusted VCO; embedded analog PUF

1. Introduction

High-speed wireless communication is becoming a necessity for modern connectivity solutions [1]. With the introduction of the 5G new radio (NR) standard, millimeter wave (mm-Wave) frequency bands are becoming accessible to facilitate such high-speed communications in today’s spectrum-congested network [1]. However, migration to higher frequency bands complicates efforts to reduce the power consumption in wireless data links used for many consumer and medical applications. In addition to low power consumption, maintaining a high level of security and trust is critical in such links to protect sensitive data and preserve user privacy [2,3]. This requirement further complicates the design of low-power high-data throughput wireless transceivers operating at mm-Wave frequency bands.

Depending on the threat type and application, creating an end-to-end secure and trustworthy wireless communication link calls for the inclusion of security features at all levels, including wireless transceivers [4–6]. Unlike data security, which can be accomplished using encryption performed in the digital backend, a trusted wireless transceiver should contain security features in the Radio Frequency Front End (RFFE) for proper authentication. To minimize the energy, area, and delay overhead, it is more efficient to choose an embedded approach in which the trust features are integrated into key sub-blocks within the RFFE.
Designing the proper trust feature for authentication requires knowledge of the main attack vectors in an RFFE. Hardware Trojans (HTs) [5,6] and Side-Channel Attacks (SCAs) [4,7,8] are the main threats to the RFFE. There are a number of authentication solutions that protect devices against HTs [4–9]. Among them, analog PUFs are more suitable for inclusion within RFFEs due to their small size, low complexity, and ease of integration with analog circuits [10–15]. They are particularly useful in authenticating RFFEs built with high-performance wide-bandgap (WBG) technologies, such as GaAs and GaN [16], where the implementation of high-density logic/memory needed for digital PUFs is challenging. Analog PUFs typically rely on the complexity of the Challenge–Response Pair (CRP) instead of only increasing the number of CRPs [10]; they leverage transistors’ intrinsic random process variations to generate a unique fingerprint needed for authentication. Due to their small CRP size, analogs are typically categorized as weak PUFs. However, the complexity of the CRP mechanism beyond a simple binary stream seen from digital PUFs may help with increasing the entropy [9–12]. A few examples are printed differential circuits [11], current-steering digital-to-analog converters (DACs), and VCOs [13].

Presently, nearly all analog PUFs are designed as standalone blocks and are included on the chip as a separate module. While easier to develop, these solutions have a negative impact on the overall power consumption, chip area, and latency in the transceiver. Moreover, analog PUFs typically exhibit low entropy due to their small CRP space [10], further limiting their usefulness for device authentication. To mitigate these concerns, this work proposes to integrate the analog PUF within key transceiver blocks, such as the VCO, to facilitate the authentication process in the wireless transceiver. The resulting low-power 24.6-to-30.1 GHz trusted LC VCO benefits from a custom analog PUF consisting of multiple NMOS and PMOS cross-coupled pairs, which are connected to the main CMOS cross-coupled pair. When properly excited, the impedance across the main cross-coupled CMOS pair varies [14], changing the VCO characteristics. The overall power consumption of the VCO also changes. This change is manifested in variations in the VCO’s DC and AC performance metrics, such as the current consumption, $f_{\text{osc}}$, amplitude, and PN, resulting in increased entropy with the same number of challenges. The remainder of this paper is structured as follows. Section 2 describes the threat model and provides more details on the design of the embedded analog PUF. The proposed low-power trusted LC VCO design is presented in Section 3 and is followed by the characterization results in Section 4. Section 5 provides the concluding remarks.

2. RFFE Threats and Embedded Analog PUF Design

The Integrated Circuit (IC) supply chain (including the fabrication process) is an inherently untrustworthy process that exposes hardware-induced vulnerabilities. For example, an attacker can place malware circuits on the die during the fabrication process to create a backdoor [4] or interrupt the main function of the IC [5]. Or, an attacker may gain information about the design of the RFFE by accessing mask sets during the IC fabrication process and be able to directly hack the RFFE and obtain the raw data [7–9]. Major threats to the RFFE and embedded PUF solutions to protect against such threats are discussed in this section.

2.1. Security Threats in RFFEs

Security threats or attack vectors for hardware are categorized into three classes [4,5]: non-invasive, semi-invasive, and invasive. The difference between classes is defined by the equipment and attackers’ approach [4]. HTs and SCAs are the main security threats for RFFEs; HTs can be easily implanted using all three specified methods and compromise the RFFE [4–6]. An attacker can even minimize scars and marks caused by physical alterations to complicate post-silicon detection efforts performed by the defender. SCAs monitor key IC signatures, such as the power consumption or EM radiation, to gather information about the design, and, hence, do not need access to the digital backend for executing a successful attack [7]. Taking advantage of hardware security primitives employed in PUF blocks, the
aforementioned threats can be detected and neutralized. These blocks leverage random fluctuations in the production process, such as IC process artifacts, to create unclonable and inherent device-specific identifiers of the device. Using PUFs, a challenge applied to the input will produce a unique output, creating a complex CRP that can be used for device authentication. For an RFFE operating at mm-Wave, an analog PUF is easier to implement since it does not require access to the digital backend and additional auxiliary circuits (such as clock generators and memory) needed for the proper operation of digital PUFs [5]. They will also occupy a smaller area and have less delay [10–15].

2.2. Embedded Analog PUFs for RFFEs

Analog PUFs usually suffer from low entropy due to their small CRP space. To solve this problem, an embedded PUF solution is proposed. The proposed PUF uses both DC and AC characteristics of a radio frequency (RF) circuit to enhance the CRP space without increasing the complexity or length of the input challenge. The number of input challenges is defined as \( n \), as shown in Figure 1. In conventional PUF designs, \( n \) input challenges correspond to \( n \) output responses (Figure 1). However, the proposed PUF generates multiple responses for a given challenge (e.g., \( m \) responses). In this way, an \( n \times 1 \) long input generates an \( n \times m \) long output response, increasing the CRP space by a factor of \( m \) compared to a conventional PUF solution (Figure 1). The concept of embedded PUF has been introduced in the early 2000s as a more compact and integration-friendly alternative to conventional PUFs [10]. However, these designs require a more complicated CRP generation and detection system due to inaccuracies caused by the miniaturization of the PUF core, which is needed for integration with the RF/analog block [2–10]. For example, transistor random mismatch is greatly influenced by the area of the device; the larger the area, the more accurate the device geometry can be predicted, leading to the opportunity to design a more accurate PUF with higher entropy. However, utilizing this phenomenon to increase the entropy in the PUF requires a large area for the transistors and a very accurate interface circuit consisting of ultra-low offset comparators and amplifiers. On the other hand, leveraging the high-frequency characteristics of an RF circuit helps break this paradigm with minimal penalty to the size, power consumption, and the size of the RFFE. In this prototype, an innovative embedded analog PUF technique is introduced in the VCO (Figure 2a–c). The CRPs are based on the DC characteristics and the frequency response of the VCO. The current consumption and \( f_{\text{osc}} \) are sensitive to process artifacts and parasitics, and, hence, can be used for authentication. By adding additional cross-coupled pairs whose device sizes are slightly different than the main pair, in parallel to the main CMOS cross-coupled pair, the VCO current consumption changes (Figure 2b). The additional parasitic capacitance from the cross-coupled pair also causes a shift in the \( f_{\text{osc}} \). By adjusting the gate-source voltage \( (V_{\text{GS}}) \) in each pair or adding multiple pairs with different \( W/L \), the variation in the current consumption and \( f_{\text{osc}} \) can be controlled, creating a proper CRP space for authentication. The additional cross-coupled pairs can be turned off so as to not impact the performance of the VCO during the normal operation of the VCO. This is easily performed by pulling up or down the gate voltages for the PMOS and NMOS pairs, respectively. Unlike conventional PUFs, where the input and output vectors have similar dimensions, here, each challenge vector generates multiple response vectors, of which the current consumption and \( f_{\text{osc}} \) are used in this proof-of-concept prototype. The proposed prototype uses 64 challenges (six bits: 3-bit NMOS and 3-bit PMOS), resulting in 128 \( (2^7) \) output responses (Figure 2c). Responses of the 6-bit challenges are analog values but they are digitized for PUF characterization and analysis. In this work, responses are converted into codewords for PUF characterization and analysis. The codeword generation from responses is discussed as part of the PUF characterization efforts discussed in Section 4.
3. Design of the Trusted CMOS LC VCO

The proposed trusted LC VCO uses a complementary (i.e., CMOS) cross-coupled topology without a tail current source to maximize the output swing (Figure 2b). A conventional CMOS LC VCO (CVCO) is also implemented on the same chip for performance comparison. The VCO uses open drain buffers to interface with the measurement equipment. Optimum LC VCO design heavily relies on the bias current (I_D) because it determines the mode of operation, i.e., the voltage-limited or current-limited regime [17,18]. In addition to the g_m of the NMOS and PMOS cross-coupled pairs, the LC tank plays a key role in the power consumption, PN, and TR performance of an LC VCO, requiring a careful design of tank components, particularly the inductance [17–19]. Knowing that the PN is proportional to (L_{tank})^2 [19], a small inductance with the highest quality factor (Q) is chosen for the tank.
Moreover, the TR is inversely proportional to the $L_{\text{tank}}$, further incentivizing the use of a small inductor. To further increase the inductor $Q$ and save chip area, the VCOs use differential inductors with a floating center tap [19]. The 420 pH inductor designed for the CVCO exhibits a $Q\sim 15$ at 28 GHz with 69.2 GHz self-resonance frequency (SRF), while the 315 pH inductor designed for the trusted VCO (Figure 3) shows $Q\sim 17.2$ at 28 GHz with SRF $> 80$ GHz. The trust features are embedded within the VCO as six cross-coupled pairs, three NMOS and three PMOS. These additional cross-coupled pairs are only used for authentication; they are turned off during the normal operation of the VCO and primarily act as parasitic capacitance in this mode.

The design procedure for the proposed trusted LC VCO begins with the choice of topology. Here, a CMOS cross-coupled pair without a tail current source is chosen to maximize the output swing and increase the effective transconductance ($G_m$). Then, the trust features that can be embedded into the VCO core are identified. An important consideration for the design of the embedded PUF is the compatibility of the PUF architecture with the VCO core architecture without a significant hit to the power consumption and size of the VCO. At the same time, the PUF should generate the required entropy for the authentication process [10]. For this design, a cross-coupled PUF topology, which relies on the variation in the impedance, is utilized to generate the change in the current consumption and the oscillation frequency as the unique identifiers for the authentication process. During the normal operation, the trust features are disabled, leaving only the main cross-coupled pair active, which resembles a conventional CMOS LC VCO. In this case, the VCO core design procedure will be straightforward. The cross-coupled pair generates the required $G_m$ to compensate for the loss of the LC tank (modeled by $R_p$). The oscillation frequency, $\omega$, is set by the tank as follows:

$$G_m = \frac{1}{R_p}$$  \hspace{1cm} (1)  

$$\omega = \frac{1}{2\pi\sqrt{L/C_T}}$$  \hspace{1cm} (2)  

$$C_T = C_{in} + C_{pd} + C_V,$$  \hspace{1cm} (3)  

$$C_{in} = C_{VCO} + C_{p_d} = C_{GS} + 4C_{GD} + C_{p_d},$$  \hspace{1cm} (4)

**Figure 3.** $Q$, $L$, and the layout of the inductor used in the proposed design.
where $G_m$ is the total transconductance in the system that is equal to the transconductance of a CMOS device ($g_m$), $R_p$ is equivalent parallel resistance of the LC tank used in the VCO, $C_T$ is the total equivalent capacitance of the tank, $C_{in}$ is the total parasitic capacitance from a cross-coupled pair, $C_V$ is the capacitance from tuning varactors, $C_{pl}$ is the parasitic capacitance from the inactive cross-coupled pairs used for the PUF, $C_{pa}$ is the parasitic capacitance from the active cross-coupled pairs used for the PUF, $C_{VCO}$ is the parasitic capacitance from the CMOS devices that is equal to $C_{GS} + 2C_{GD}$, and $C_{GS}$ and $C_{GD}$ are the gate-source and drain-source MOS capacitance of the CMOS device. In this design, the power consumption is reduced by increasing the Q of the inductor to generate a larger $R_p$, leading to a smaller required $G_m$ for oscillation. Moreover, the stacked combination of NMOS and PMOS pairs used in the VCO core and the PUF allows for reusing the current from the PMOS into the NMOS pair, generating larger overall $G_m$ without increasing the current consumption. When the VCO operates in authentication mode, additional cross-coupled pairs are enabled. Consequently, the current consumption and the frequency are lowered due to larger parasitic capacitance from these pairs.

IC fabrication is an electromechanical process that is prone to process variation and mismatch, of which the device mismatch is the main source of entropy in the proposed analog PUF [5]. However, the effect of the temperature variation on the performance of the analog CMOS circuits cannot be ignored and should also be investigated for the proposed analog PUF. Figure 4 shows changes in the simulated current consumption and $f_{osc}$ when the temperature is varied from $-40^\circ$C to $85^\circ$C for the first challenge, 000000, and the last challenge, 111111. The changes to the current consumption are reasonable and follow the MOS threshold variation with temperature. Since the change in current consumption is almost linear, it can be easily compensated for using adaptive biasing (i.e., changing the supply with temperature) or calibrated out in post-measurement calculations. The changes to the $f_{osc}$ are very small ($<\pm 0.1\%$), as expected, since $f_{osc}$ is mainly determined by the frequency of the LC tank whose variations with temperature are negligible. Expecting a unique response for each input challenge, the accuracy of the analog PUF should be investigated. The amount of mismatch and its impact on the PUF resolution can be found by performing post-layout Monte Carlo (MC) simulations on the trusted VCO when the embedded analog PUF is turned on.

Figure 5 shows the Probability Distribution Function (PDF) of the current consumption and $f_{osc}$ at $-40^\circ$C, $27^\circ$C (room temperature), and $85^\circ$C for the first challenge, 000000. As expected, the PDF of the output results resembles those of a Gaussian/normal function for all three temperatures. For a 200-sample MC simulation, the current consumption and $f_{osc}$ show reasonable variations with the standard deviation ($\sigma$) $\approx 67$ $\mu$A and $\sim 15$ MHz at $27^\circ$C (Figure 5). The PDF also remains close to Gaussian when temperature changes with $\sigma$ for the current consumption and $f_{osc} \sim 70$ $\mu$A and $\sim 14$ MHz at $-40^\circ$C, and $\sim 63$ $\mu$A and $\sim 22$ MHz at $85^\circ$C, respectively. The MC simulations are repeated for the last challenge, 111111, showing a similar Gaussian/normal behavior (Figure 6). The MC results are then used to evaluate the randomness of the proposed PUF using the Hamming Distance (HD) function, which is a metric to show the difference between two data strings. There are two HD measurements: Intra-HD and Inter-HD. Intra-HD measures the randomness of a single PUF design (or a single chip) when one bit of the input challenge changes, while the Inter-HD demonstrates the randomness between different PUF designs (or different chips) when the same challenge is applied to the PUFs. For each challenge, a single MC simulation can be used to find Inter-HD since MC simulations based on the device mismatch show the PUF output difference between different samples (i.e., dies). Ideally, the Intra-HD and Inter-HD of a PUF should be 0 and 0.5, respectively. Simulating Intra-HD in an ideal simulation environment where circuit parameters, the supply voltage, biasing, and output load do not experience any variation during the simulation is very challenging since the simulator only uses the mathematical models for the analysis. To emulate a realistic environment for Intra-HD simulations, reasonable uncertainty is added to the test bench by adding randomness to the DC sources and temperature. The DC sources used in the test bench are
randomly varied by considering ±5 mV error. This is consistent with testing conditions in our lab where the DC voltages are set manually. In addition to variations of the DC voltages, the temperature randomly varied from room temperature by ±1 °C (from 26 °C to 28 °C) to emulate fluctuations in the room temperature during the measurement. Figure 7a–f show the Inter-HD and Intra-HD results for the current consumption and $f_{\text{osc}}$ at −40 °C, 27 °C, and 85 °C based on the 200-sample post-layout MC simulations. Since the PDF of the current consumption and $f_{\text{osc}}$ are reasonably close to Gaussian for both challenges, as shown in Figures 5 and 6, the Inter- and Intra-HD results are only presented for the first challenge, 000000. Ideally, Inter-HD for PUFs should be 0.5 and Intra-HD should be 0 [10–15]. The challenge for defining Inter-HD and Intra-HD is to create accurate and reliable bit representations (i.e., codeword) for responses. Codeword generation for this work is based on the Huffman coding algorithm [20] and will be discussed in more detail in Section 4. Using these codewords, the Inter-HD of the simulated responses are 0.4997 at −40 °C, 0.4995 at 27 °C, and 0.5004 at 85 °C for the current consumption, and 0.5010 at −40 °C, 0.4991 at 27 °C, and 0.5090 at 85 °C for $f_{\text{osc}}$, respectively. The Intra-HD of the simulated responses are 0.0107 at −40 °C, 0.0085 at 27 °C, and 0.0092 at 85 °C for the current consumption, and 0.0036 at −40 °C, 0.0029 at 27 °C, and 0.0043 at 85 °C for $f_{\text{osc}}$, respectively. Both simulated Intra- and Inter-HD are very close to the ideal values for a PUF.

![Graphs showing changes to current consumption and $f_{\text{osc}}$](image)

**Figure 4.** Changes to the normalized (a) current consumption (red) and (b) $f_{\text{osc}}$ for the first challenge (blue), 000000, when the temperature is varied; a similar trend is observed for (c) current consumption (red) and (d) $f_{\text{osc}}$ (blue) for the last challenge, 111111.
Figure 5. PDFs of the current consumption and $f_{osc}$ of the proposed trusted VCO for the first challenge, 000000; PDF of the current consumption (red) at (a) $-40 \, ^\circ C$, (b) $27 \, ^\circ C$, (c) $85 \, ^\circ C$, and PDF of $f_{osc}$ (blue) at (d) $-40 \, ^\circ C$, (e) $27 \, ^\circ C$, (f) $85 \, ^\circ C$.

Figure 6. PDFs of the current consumption and $f_{osc}$ of the proposed trusted VCO for the last challenge, 111111; PDF of the current consumption (red) at (a) $-40 \, ^\circ C$, (b) $27 \, ^\circ C$, (c) $85 \, ^\circ C$, and PDF of $f_{osc}$ (blue) at (d) $-40 \, ^\circ C$, (e) $27 \, ^\circ C$, (f) $85 \, ^\circ C$. 
Figure 7. Intra-HD, and Inter-HD of the proposed trusted VCO for the current consumption at (a) −40 °C, (b) 27 °C, and (c) 85 °C, along with those of $f_{osc}$ at (d) −40 °C, (e) 27 °C, and (f) 85 °C for the first challenge.

4. Measurement Results

The proposed trusted VCO is implemented in a 1P9M 65 nm standard CMOS process (Figure 8b) and uses an on-chip open-drain NMOS buffer to interface with the measurement equipment (Figure 8a). A CVCO is also included on the same die for performance comparison (Figure 8c). To enable accurate performance measurement, both mm-Wave VCOs are characterized using RF GSG probes with external bias-Ts facilitating the connection to the power supply (Figure 8a). This way, the loss associated with external components (such as the cables) can be de-embedded from the measurement results. A general view of the test setup is shown in Figure 8a. While the core of both VCOs occupies a similar area (93 $\mu$m × 197 $\mu$m for the trusted VCO and 99 $\mu$m × 182 $\mu$m for CVCO), the trusted VCO needs additional pads to interface with the embedded PUF, resulting in a larger chip area.

A Keysight PXA N9030A signal analyzer and several Keithley 2000 DMM source meters are used for the frequency analysis and DC characterization of the VCOs. The characterization process is split into two parts: VCO performance measurement and comparison and PUF characterization, randomness, and reliability analysis.

4.1. VCO Performance Measurement and Comparison

Both VCOs are interfaced with the signal analyzer to monitor their output spectrum, measure their PN, and determine their TR. In this work, the proposed trusted VCO is designed for low-power applications; as such, the PUF is disabled during normal operation.

The trusted VCO sustains oscillation when the supply voltage ($V_{DD}$) is raised to 0.8 V with the power consumption ($P_{DC}$)~0.72 mW. For $P_{DC}$~1.75 mW, the output power is increased to −9.7 dBm and the VCO exhibits a TR ≈ 5.5 GHz (Figure 9a), from ≈24.6 GHz to 30.1 GHz. Under such conditions, the PN measures better than −104.8 dBc/Hz and −132.2 dBc/Hz at 1 MHz and 10 MHz offset, respectively (Figure 9b), when the frequency is tuned to the upper end of the range (≈29.3 GHz). These results correspond to FoM~191.7 dBc/Hz and ~199.1 dBc/Hz @1MHz and @10MHz, respectively. When TR is considered, the FoM_T of ~197.6 dBc/Hz and ~205 dBc/Hz are obtained at 1 MHz and 10 MHz, respectively. On the other hand, the CVCO sustains oscillation when the
supply voltage ($V_{DD}$) is raised to 0.8 V with the power consumption ($P_{DC}$)~0.6 mW. For $P_{DC}$~1.5 mW; the output power is increased to −10.1 dBm, and it exhibits a frequency tuning range (TR) of ≈6.1 GHz, from ≈25 GHz to 31.1 GHz (Figure 9a). Under such conditions, the PN measures better than −101.1 dBC/Hz and −130.4 dBC/Hz at 1 MHz and 10 MHz offset, respectively (Figure 9b), when the frequency is tuned to the upper end of the range (≈29.6 GHz). The CVCO PN results correspond to FoM−188.7 dBC/Hz and −198 dBC/Hz @ 1 MHz and −204 dBC/Hz @ 1 MHz and @ 10 MHz, respectively. When TR is considered, the FoM_T of −194.7 dBC/Hz and −204 dBC/Hz are obtained at 1 MHz and 10 MHz, respectively. These results clearly show that the proposed trusted VCO exhibits similar performance (esp. PN), if not better, when compared against the CVCO under a similar power consumption.

![Intra-HD micrographs](image)

Figure 8. Intra-HD micrographs of the (a) proposed trusted VCO and (b) CVCO dies alongside (c) the measurement bench.

![Comparison Graphs](image)

Figure 9. (a) TR and (b) PN comparison of the trusted VCO with the CVCO. The spectrum of the trusted VCO is also shown.

The deterioration in the TR of the proposed trusted VCO is due to the extra capacitance resulting from parasitics of additional cross-coupled pairs and additional metal wiring in the layout. However, the slight closed-in PN improvement (esp. $f_{\text{offset}} <$ 1 MHz) in the proposed trusted VCO compared to the CVCO requires a more detailed analysis.

A number of PN models have been developed for LC VCOs [21–25]. Among them, the time variant PN model developed by Hajimiri et al. [21] is more accurate in predicting the PN of LC oscillators, particularly in the $1/f^2$ and $1/f^2$ regions. Considering this time variant PN model [21], calculating the change in the Impulse Sensitivity Function (ISF),
which is a periodic and dimensionless function, is necessary \cite{21}. Since the ISF is periodic, it can be represented by Fourier coefficients as follows:

\[
\Gamma(\omega \tau) = \frac{\Gamma_0}{2} + \sum_{n=1}^{\infty} \left( \Gamma_n \cos(n\omega_0 \tau + \theta_n) \right),
\]

where the coefficients \((\Gamma_n)\) are real values and \(\theta_n\) is the phase of the nth harmonic. \(\theta_n\) is small and can be ignored at random input noise \cite{21}, and the coefficients can be estimated analytically or calculated from the simulation. Given its similarities with the ISF, the Perturbation Projection Vector (PPV), which represents the sensitivity of the per cycle jitter variance to current perturbations at the nodes of the oscillator \cite{23}, can be used to estimate the ISF changes \cite{21–23}. PPV results can be obtained via periodic simulations.

Figure 10 gives the PPV results obtained from Cadence Harmonic Balance (HB) and HB noise simulations for both VCOs. HB PPV results are shown in V and HB noise PPV results are shown in 1/V. Then, the PN of the LC VCO can be expressed as follows \cite{24,25}:

\[
L(\Delta \omega) = 10 \log \left( \frac{1}{4q_{\text{max}}^2 \Delta \omega^2} \left( \frac{\Gamma_{\text{id, rms}}^2 \pi \omega_{\text{DC}}}{\Gamma_{\text{rms}}^2} / \Delta f + \Gamma_{\text{Rrms}}^2 / \Delta f \right) \right)
\]

where \(q_{\text{max}}\) is the maximum charge displacement across the equivalent output capacitance where the impulse was injected, i.e., \(q_{\text{max}} = V_{\text{max}} C (V_{\text{max}}\) is the maximum voltage swing at the output). \(\Gamma_{\text{id, rms}}^2\) is the ISF from active devices and can be expressed in several forms, e.g., \(\Gamma_{\text{id, rms}}^2 = 2V_{\text{TH}}^2 / \pi V_{\text{max}}^2\) \cite{24} or \(\Gamma_{\text{id, rms}}^2 = 2I_{\text{DS}} / \pi \beta V_{\text{max}}^2\) \cite{25}, where \(\beta = \mu e C_{\text{ox}} W / L\), \(\mu\) is the electron mobility, \(C_{\text{ox}}\) the gate oxide capacitance per unit area, and \(W\) and \(L\) are the transistor width and length, respectively. \(\Gamma_{\text{Rrms}}^2\) is the ISF from the thermal noise source of the oscillator (R), which is mostly produced by the tank. It is assumed to be \(1/2\) for single-ended output and \(1/8\) for differential outputs \cite{25}. \(\Gamma_{\text{R}} / \Delta f\) is the power spectral density of active devices’ noise current. The portion associated with the thermal noise can be expressed as \(\Gamma_{\text{R,thermal}} / \Delta f = 4kT \gamma \beta V_{\text{max}}\), where \(k\) is the Boltzmann constant, \(\gamma\) is the fitting parameter, and \(T\) is the temperature as Kelvin. In most cases, \(\beta V_{\text{max}} \approx g_m\) of the device. The portion associated with the flicker noise can be expressed as \(\Gamma_{\text{R, flicker}} / \Delta f = K_f g_m^2 / (C_{\text{OX}} W L \Delta f)\), where \(K_f\) is the flicker noise fitting parameter. \(\Gamma_{\text{R}} / \Delta f\) is the power spectral density of the thermal noise current due to R and can be expressed as \(\Gamma_{\text{R}} / \Delta f = 4kT / R\). Equation (6) includes the thermal and flicker noise sources \cite{19,21–30} for both active and passive devices in the VCO. Since the flicker and thermal noises of MOS devices are considered uncorrelated, their impact on the PN can be studied separately, and the results can be superimposed \cite{22}. Knowing that flicker noise is dominant at low offset frequencies, the impact of the flicker noise on the PN should be studied in more detail. Hajimiri et al. \cite{21} expresses the flicker noise-dominant region of the PN (i.e., \(1/f^3\) region) in terms of the \(1/f\) noise corner, \(\omega_{1/f}\). In this case, the \(1/f^3\) corner frequency, \(\omega_{1/f^3}\), can be expressed as follows:

\[
\omega_{1/f^3} = \omega_{1/f} (\Gamma_{\text{DC}} / \Gamma_{\text{rms}})^2,
\]

where \(\omega_{1/f}\) is \(1/f^3\) corner frequency, \(\omega_{1/f}\) is \(1/f\) corner frequency, and \(\Gamma_{\text{DC}}\) and \(\Gamma_{\text{rms}}\) are DC and root mean square (RMS) values of the ISF coefficients, respectively. Using (7), the flicker noise-dominant portion of the PN can be expressed as follows:

\[
L(\Delta \omega)_{1/f^3} = 10 \log \left( \frac{\Gamma_0^2}{q_{\text{max}}^2} \times \frac{\Gamma_{\text{R}} / \Delta f}{8 \Delta \omega^2} \times \frac{\omega_{1/f}}{\Delta \omega} \right),
\]

where \(\Gamma_0\) is the first coefficient of the ISF, and is equal to \(2\Gamma_{\text{DC}}\), and \(\Gamma_{\text{R}} / \Delta f\) is the total noise current, \(\Gamma_{\text{R}} / \Delta f + \Gamma_{\text{id, rms}}^2 / \Delta f\). At low offset frequencies, the flicker noise will be dominant; hence, \(\Gamma_{\text{R}} / \Delta f\) can be expressed as \(K_f g_m^2 / (C_{\text{OX}} W L \Delta f)\). Knowing the flicker and thermal noise of
the MOS devices and the tank, the flicker noise- and thermal noise-dominant portions of the PN can be derived separately as follows [31–33]:

\[
L(\Delta \omega)_{\text{flicker}} = 10 \log \left( \frac{\Gamma_0^2 \pi K_F S_m^2}{8 q_{\text{max}} C_{\text{ox}} W L \Delta \omega^3} \right),
\]

(9)

\[
L(\Delta \omega)_{\text{thermal}} = 10 \log \left( \frac{k T \pi^2}{I_{DD}^2} \left( \frac{1}{R} + \gamma S_m \right) \left( \frac{\omega_0}{2 Q \Delta \omega} \right)^2 \right),
\]

(10)

where \(I_{DD}\) is the RMS current consumption of the VCO. Superimposing (9) to (10) leads to a simplified PN expression that covers both the flicker noise- and thermal noise-dominant regions of the PN as follows:

\[
L(\Delta \omega) \approx 10 \log \left( \frac{k T \pi^2}{I_{DD}^2} \left( \frac{1}{R} + \gamma S_m \right) \left( \frac{\omega_0}{2 Q \Delta \omega} \right)^2 + \frac{\Gamma_0^2 \pi K_F S_m^2}{8 q_{\text{max}} W L \Delta \omega^3} \right),
\]

(11)

**Figure 10.** PPV results: HB noise results for (a) the CVCO and (b) trusted VCO; HB results for (c) the CVCO and (d) trusted VCO.

The PN for two LC VCOs can then be compared using this simplified PN expression. PPV results for both designs are gathered and compared. \(\Gamma_0\) obtained from the HB noise simulation is 1.085 1/V and 1.44 1/V for the differential outputs of the CVCO and 0.36 1/V and 0.19 1/V for the differential outputs of the trusted VCO, respectively (Figure 10). Utilizing HB simulations reveals \(\Gamma_0 \approx -0.16\) V and 0.14 V for the differential outputs of the CVCO and \(-0.0049\) V and \(-0.058\) V for the differential outputs of the trusted VCO, respectively (Figure 10). The minimum ratio between \(\Gamma_0\) for two VCOs is \(-2.4 \times\), which amounts to a ~7 dB improvement in the close-in PN for the trusted VCO. Additionally, the trusted VCO exhibits larger \(q_{\text{max}}\) compared to the CVCO due to larger parasitic capacitors from the additional cross-coupled pairs and the resulting on-chip metal wiring. This larger \(q_{\text{max}}\) further improves the close-in PN performance of the proposed trusted VCO. The measured PN results presented in Figure 9 reveal up to a 9 dB improvement in the PN at 100 kHz offset for the trusted VCO compared to the CVCO. As the frequency increases, the
effect of flicker noise diminishes, and the thermal noise of active devices and the Q of the LC tank become the dominant factor affecting the PN [18]. In this region, the PN can be better modeled with (11). Considering (11), it is evident that the difference between the PN of two VCOs gradually narrows until it becomes negligible at high offset frequencies near the PN floor. To conclude this study, the performance of the trusted VCO is summarized and presented in Table 1. Compared with the state-of-the-art VCOs [26–29] operating in a similar frequency range and built with the 65 nm CMOS process, the proposed trusted VCO exhibits competitive FoMs while consuming lower power.

<table>
<thead>
<tr>
<th>Table 1. Trusted VCO performance summary and comparison with state-of-the-art VCOs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>This Work (CVCO/Trusted VCO)</td>
</tr>
<tr>
<td>P DC (mW)</td>
</tr>
<tr>
<td>f osc (GHz)</td>
</tr>
<tr>
<td>PN@1MHz (dBc/Hz)</td>
</tr>
<tr>
<td>PN@10MHz (dBc/Hz)</td>
</tr>
<tr>
<td>FoM@1MHz (dBc/Hz)</td>
</tr>
<tr>
<td>FoM f T@1MHz (dBc/Hz)</td>
</tr>
<tr>
<td>FoM@10MHz (dBc/Hz)</td>
</tr>
<tr>
<td>FoM f T@10MHz (dBc/Hz)</td>
</tr>
<tr>
<td>Core Area (mm²)</td>
</tr>
<tr>
<td>Technology</td>
</tr>
</tbody>
</table>

FoM = |PN| + 20log(fo/Δf) − 10.log(Pdc/1 mW); FoM f T = FoM + 20log(TR/10). *: Up-converted to account for dividing by two used for testing by the authors. #: It can be found via Figure 5 of [28], it is not given in [28].

4.2. PUF Characterization and Randomness Analysis

To characterize a PUF, the randomness, uniqueness, and correlation criteria should be evaluated. For conventional PUFs, the direct analysis of the response is sufficient. However, the proposed embedded PUF requires customized digitization since each challenge will generate multiple responses. As the first step, the expected PDF of the responses is presented to quantify the reliability of the PUF [5]. Figure 11 shows the distribution of the measured current consumption and f osc for a trusted VCO chip operating under V DD = 1.2 V at room temperature (27 °C). Since the current consumption and f osc are directly affected by the device size, which follows the near-Gaussian mismatch profile of CMOS devices, a normal distribution is expected. To perform HD analysis, the measured current consumption and f osc should be converted to binary strings. The conversion is customized considering the accuracy of the measurement equipment and biasing (which sets the minimum resolution) and the variation range of the measured parameters (current consumption and f osc). In this work, measurement devices have 1 MHz and 1 µA accuracy. However, the accuracy of biasing voltage sources used for the challenge pairs is ~10 mV and, hence, sets the minimum resolution for the responses. During the authentication, each challenge input based on the “C N3 CN2 CN1 CP3 CP2 CP1” codeword produces its own unique response as current consumption and f osc. Knowing that the length of the output bit string should be equal to or greater than that of the challenge codeword [20], a lower bound (six bits) on the length of the bit string is found. However, accurate conversion of the output analog response to bit strings is a challenge for this work since multiple outputs are generated for each challenge input. Unlike most analog PUFs [10–15], setting a fixed decision threshold is difficult for all chips given normal PVT variations affecting the high-frequency path. As such, the soft decision technique [12] is used for output bit string generation before the HD analysis.
First, the responses are analyzed to find the variation range. When the input challenge moves from 000000 to 111111, the current consumption (i.e., the DC response) changes from ~2.6 mA to ~3.8 mA, and $f_{\text{osc}}$ (i.e., the AC response) varies from ~29 GHz to ~29.4 GHz, respectively. Then, the weight of each digit in the decimal number is considered. Knowing the accuracy of the measurement equipment, both current (in mA) and $f_{\text{osc}}$ (in GHz) readings can be expressed with three decimal digit accuracy, i.e., A.XYZ for current and BC.TVU for frequency. A level change for the current response can be 2 or 3, other level changes can be from 0 to 9, indicating that the changes have an unequal impact on the response. In such conditions, coding theory approaches, such as Huffman coding [20], where higher probability represents fewer bits and vice versa, are desired. Due to the limited accuracy of the biasing network (~10 mV), the least significant digits, i.e., Z and U, require soft decision thresholds. Finally, the proposed customized coding can be expressed as 1-bit for A, 4-bit for X, 4-bit for Y, 1-bit for Z, 1-bit for B, 1-bit for C, 3-bit for T, 4-bit for V, and 1-bit for U. The result will be two 10-bit codewords, one for the current consumption response and the other for $f_{\text{osc}}$. Using this customized code, a sample set consisting of eight dies operating under similar conditions ($V_{\text{DD}} = 1.2$ V and $T \approx 27$ °C) is evaluated for Inter-HD and Intra-HD analyses (Figure 12). The measured average Inter-HD of the current consumption and $f_{\text{osc}}$ are ~0.5058b and 0.4978b, respectively, which are very close to the ideal value of 0.5b. Similarly, the measured average Intra-HD of the current consumption and $f_{\text{osc}}$ are ~0.0055b and 0.0053b, respectively, which are very close to the ideal value of 0, demonstrating acceptable randomness for the proposed analog embedded PUF.

To quantify the degree of correlation between the PUF outputs for different challenges, the ACF of the proposed analog PUF is evaluated [34]. ACF measures the correlation of a signal with a delayed copy of itself as a function of delay. The smaller the value of the correlation is, the lower the correlation of the responses and the higher the resemblance to the Gaussian distribution. For conventional PUFs, bit streams of responses are used for ACF measurements. In this work, the ACF is applied to current consumption and $f_{\text{osc}}$, which make up the output responses to each challenge. To compute ACF, a stochastic time series of measured responses is created since the ACF aims to detect the correlation between two random responses in a sample set. To this end, 40K responses are gathered for each output to create the required stochastic time series for the eight chips. Then, the ACF of both 40K sample sets, one for current consumption and the other for $f_{\text{osc}}$, is calculated when considering 10K lags (Figure 13). The ACF of the responses for the current consumption and $f_{\text{osc}}$ at a 95% confidence level are 0.0111 and 0.0110, respectively, which are very close to the ideal value of zero, demonstrating a desired level of randomness for the proposed PUF (Table 2).

![Figure 11. PDF of the (a) current consumption and (b) $f_{\text{osc}}$ for the 6-bit input challenge.](image-url)
The performance of the proposed embedded analog PUF is summarized in Table 2 and compared against those of the published state-of-the-art analog PUFs. The proposed analog-embedded PUF offers a competitive performance in terms of entropy, energy consumption, and bit rate while occupying a smaller chip area in a similar 65 nm CMOS process. An important advantage of the proposed analog PUF is its high sampling rate. The sampling rate is calculated by simulating the settling time of the VCO when switching the input challenge, enabling a bit rate as high as 1.5 Gbps for each response type due to the 6-bit length criterion.) and the number of bits for each symbol, which is the length of challenges in this work [35] as shown below:

\[
\text{Data rate} = f_0 \times \frac{l}{t_{\text{settling}}},
\]

where \(f_0\) is the sampling rate, and \(t_{\text{settling}}\) is the slowest settling time from the first challenge to the last response.

### Table 2. PUF performance summary and comparison with state-of-the-art analog PUFs.

<table>
<thead>
<tr>
<th>Entropy Source</th>
<th>Capacitance and Impedance mismatch</th>
<th>Process variation</th>
<th>Impedance mismatch</th>
<th>Process variation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit rate</td>
<td>1.5 Gbps</td>
<td>100 Mbps</td>
<td>320 Kbps</td>
<td>40 Kbps</td>
</tr>
<tr>
<td>ACF</td>
<td>0.0111/0.0110</td>
<td>0.0108</td>
<td>0.0123</td>
<td>0.0142</td>
</tr>
<tr>
<td>Energy/bit</td>
<td>0.83 pJ</td>
<td>0.36 pJ</td>
<td>6 pJ</td>
<td>0.91 pJ</td>
</tr>
<tr>
<td>Intra-HD</td>
<td>0.0055/0.0054</td>
<td>0.0906</td>
<td>0.0031</td>
<td>N/A</td>
</tr>
<tr>
<td>Inter-HD</td>
<td>0.5113/0.4892</td>
<td>0.4859</td>
<td>0.4986</td>
<td>0.4681</td>
</tr>
</tbody>
</table>

The performance of the proposed embedded analog PUF is summarized in Table 2 and compared against those of the published state-of-the-art analog PUFs. The proposed analog-embedded PUF offers a competitive performance in terms of entropy, energy consumption, and bit rate while occupying a smaller chip area in a similar 65 nm CMOS process. An important advantage of the proposed analog PUF is its high sampling rate. The sampling rate is calculated by simulating the settling time of the VCO when switching the input.
challenge bit (Figure 14). As shown in Figure 14, the VCO frequency changes and settles to the new frequency within ~4 ns when switching from the first to the last challenge, enabling a bit rate as high as 1.5 Gbps for each response type due to the 6-bit length of the challenge. The bit rate is calculated by multiplication of the sampling rate (Nyquist criterion) and the number of bits for each symbol, which is the length of challenges in this work [35] as shown below:

\[
\text{Data rate} = f_s \times l = l/t_{\text{settling}},
\]

where \( l \) is the number of bits for each symbol (i.e., six bits for the proposed PUF), \( f_s \) is the sampling rate, and \( t_{\text{settling}} \) is the slowest settling time from the first challenge to the last challenge (i.e., ~4 ns for the proposed PUF). Such a high data rate allows for reducing the time needed for the authentication process and reducing the unwanted latency when trying to establish a trusted data link. Using (12), the energy per bit can be calculated by subtracting the VCO power during the authentication with the one during the normal operation (i.e., challenge set to 000000), revealing a competitive performance compared to the state-of-the-art (Table 2). The very high data rate achieved for the proposed embedded PUF along with its low power consumption allows for delivering an energy/bit as low as 0.83 pJ, which is comparable to the state-of-the-art PUFs [12,14,15] implemented in a similar CMOS technology. Moreover, the larger CRP size made available by the generation of multiple outputs for a single challenge has created a relatively compact design compared to other analog PUFs implemented in similar CMOS process nodes, making the design well-suited for integration with communication transceivers.

![Figure 14. Transient simulation results of the trusted VCO showing the settling time when input challenge changes criterion and the number of bits for each symbol.](image)

5. Conclusions

An innovative 1.75 mW trusted CMOS LC VCO, which employs an embedded analog PUF and operates at 24.6 GHz to 30.1 GHz, is presented. The VCO benefits from an analog PUF, which is integrated within the cross-coupled CMOS pair, allowing for a larger set of CRPs with the same number of input challenges. Fabricated in a 1P9M 65 nm standard CMOS process, the proposed trusted VCO delivers the measured PN ~−104.8 dBc/Hz @ 1 MHz and −132.2 dBc/Hz @ 10 MHz, revealing FoMs of 191.7 dBc/Hz and 199.1 dBc/Hz, respectively. With TR~5.5 GHz, the FoMF reaches 197.6 dBc/Hz and 205.0 dBc/Hz @ 1 MHz and @ 10 MHz, respectively. The embedded PUF consumes as low as 0.83 pJ/b and is capable of running at 1.5 Gb/s. It exhibits sufficient uniqueness with the measured Inter-HD of 0.5113b and 0.489b and measured Intra-HD of 0.0055b and 0.0053b for the current consumption and \( f_{\text{osc}} \), respectively. Moreover, an ACF of 0.0111 and 0.110 is achieved for the current consumption and \( f_{\text{osc}} \) responses of the proposed PUF, respectively, at a 95% confidence level. Compared with the state-of-the-art LC VCOs operating in the same frequency range, the proposed
trusted VCO shows competitive performance at lower power with added device security and authentication features.


**Funding:** The research received no external funding.

**Data Availability Statement:** All the materials used in the study are mentioned within the article.

**Conflicts of Interest:** The authors declare no conflicts of interest.

**References**


32. Razavi, B. The Design of a Millimeter-Wave VCO [The Analog Mind]. *IEEE Solid-State Circuits Mag.* 2022, 14, 6–12. [CrossRef]


Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.