Designing Maximal Resolution Loop Sensors for Electromagnetic Cryptographic Analysis

Wim Aerts #✿*1, Elke De Mulder ✿2, Bart Preneel ✿*, Guy A.E. Vandenbosch #, Ingrid Verbauwhede ✿*
# dep. ESAT-TELEMIC K.U.Leuven
* dep. ESAT-COSIC K.U.Leuven
Kasteelpark Arenberg 10, B-3001 Leuven, Belgium
✿ Interdisciplinary Institute for BroadBand Technology (IBBT)
1wim.aerts@esat.kuleuven.be 2elke.demulder@esat.kuleuven.be

Abstract—In this paper, the maximal spatial resolution of a circular loop sensor is investigated. This will result in a practical limit determined by the desired signal amplitude and working frequency band.

I. INTRODUCTION

Mid nineties, Kocher [1] published a first paper on timing attacks. It was the foundation of a whole new cryptographic field: side channel analysis. Instead of using mathematical techniques to break cryptographic ciphers, physical properties of the device on which an implementation of the cipher is running are used to recover the secret key. Some examples of physical properties that can contain sensitive information are: power consumption [2], electromagnetic radiation [3], [4] and sound [5], [6].

This paper focuses on sensors for electromagnetic analysis. Such sensors should capture the radiation surrounding the device as accurate as possible with a reasonable amplitude. Most radiation emerging from the device is magnetic in nature as inside the device currents are owing to charge and discharge capacitors. As such, a loop sensor would be a natural choice. Previous work [7] zoomed in on shielded loops. Those loops were quite large in comparison with a micro-controller, ASIC or even FPGA and were consequently not suited for localized measurements. Smaller implementations of the same concept do manage to achieve smaller resolutions. Masuda et al. [8] reports an aperture of 20 μm × 1 mm.

Sect. II of this paper, discusses the maximal spatial resolution of a non-shielded loop sensor, which can inherently be made smaller than the shielded loops, in a theoretical way. Examples in Sect. III give numerical results. A straightforward design methodology can not be derived from the ideas in this work due to the complexity of the equations. Numerical search methods are to be applied. The practical limits on the resolution are however at hand.

II. THEORY

In this section the minimum achievable dimension of a circular inductive sensor for usage in a frequency interval \([f_L, f_H]\) is evaluated and values for the number of turns \(N\) and the loop radius \(r_l\) are derived starting from the value of the magnetic field strength \(B\) and a minimum amplitude \(V_{\text{min}}\) that should be generated over a load \(Z\), the input impedance of the measurement device, in parallel with the loop. This value \(V_{\text{min}}\) is determined by the measurement equipment and relates to the minimum voltage that can be measured by an oscilloscope or the minimum signal amplitude that has to be fed to an amplifier connected to the loop to obtain a reasonable signal-to-noise ratio or the like.

A. General Case: Arbitrary \(Z\)

Faraday-Lenz law states that a varying magnetic flux through a surface induces an extra voltage \(V\) along the line enclosing the surface:

\[
|V| = \left| \frac{d\phi_B}{dt} \right| = \omega N A B, \tag{1}
\]

with \(\phi_B\) the magnetic flux through the sensor, \(\omega = 2\pi f\), \(N\) the number of turns in the loop, \(A\) the area surrounded by one turn and \(B\) the magnetic field strength. The rightmost equality sign implies that the loop is positioned orthogonally to the magnetic field.

If a load \(Z\) is attached to the terminals of the loop sensor, current will flow, resulting in a voltage over \(Z\) equal to:

\[
|V| = \omega N A B \left| \frac{Z}{j\omega L + R + Z} \right|, \tag{2}
\]

with the loop inductance \(L\) [9]:

\[
L = N^2 \mu_0 r_l \left( \ln \left( \frac{2r_l}{r_w} \right) - 2 \right), \tag{3}
\]

with \(r_w\) the wire radius, and the loop resistance \(R\) [10]:

\[
R = \frac{2\pi r_l N}{\sigma \pi (r_w^2 - (r_w - \delta)^2)} \quad \text{with} \quad \delta = \sqrt{\frac{2}{\mu_0 \omega \sigma}}, \tag{4}
\]

with \(\delta\) the skin depth and \(\sigma\) the electrical conductivity of the metal, e.g. 58 MS/m for copper. If \(\delta > r_w\), \(\delta\) should be replaced by \(r_w\) in the formula, for then not the skin depth, but the wire diameter is the limiting factor.

The contour lines of Eq. (2) for \(r_l/r_w = 16\), \(f = 250\ kHz\) and \(Z = 50 \Omega\) are drawn in Fig. 1. Designing a loop sensor with maximal resolution for signal amplitude \(V_{\text{min}}\) boils down to finding the pair \((N, r_l)\) on the \(|V| = V_{\text{min}}\) contour where \(r_l\) is minimum. These loci are connected by the solid black line on Fig. 1.
The optimum value for \( N \) is a trade off between increasing \( N \) to increase the induced voltage of Eq. (1), and decreasing \( N \) to lower \( L \propto N^2 \) and \( R \propto N \), avoiding that \(|j\omega L + R| \gg |Z|\) in the denominator of Eq. (2).

Still, not all \((N,r_l)\) pairs found as the minimum on the appropriate contour are valid. Eq. (2) implies that the total wire length of the loop is small to avoid signal cancellation due to phase differences over the loop:

\[
N2\pi r_l < \frac{\lambda_H}{10} \quad \text{or} \quad N r_l < \frac{\lambda_H}{20\pi} = \frac{c}{10\omega_H}
\] (5)

with \( c \) the speed of light. Due to the inverse proportionality with \( \omega \), this inequality condition only has to be validated for \( f_H \), the upper bound of the intended frequency band.

Moreover, for similar reasons, the resonance frequency of the system \( f_{res} \), consisting of loop sensor and measuring device, should be higher than ten times the highest frequency in the working frequency band:

\[
f_{res} = \frac{1}{2\pi\sqrt{L_{tot}C_{tot}}} = \frac{1}{2\pi\sqrt{N^2L_{1,N=1}\left(\frac{C_u}{NZ} + CZ\right)}} > 10f_H
\] (6)

with \( C_Z \) the capacitive part of \( Z \). The capacitance between two turns \( C_u \) can be calculated with Magnusson [11]:

\[
C_u = 2\pi r_l \epsilon_0 \pi \ln \left(\frac{d}{2r_w} + \sqrt{\left(\frac{d}{2r_w}\right)^2 - 1}\right),
\] (7)

with \( \epsilon_0 \) the dielectric constant and \( d = 2(r_w + t) \) the distance between the centers of two turns, with \( t \) the insulation thickness. The inductance of one turn (in the absence of the other turns) is:

\[
L_{1,N=1} = \mu_0 r_l \left(\ln \left(\frac{8r_l}{r_w}\right) - 2\right),
\] (8)

with \( \mu_0 \) the magnetic permeability of vacuum.

Filling in Eq. (7) and (8) into Eq. (6) results in:

\[
\frac{\lambda}{10} > 2\pi \sqrt{N r_l} \left[\frac{\ln \left(\frac{8r_l}{r_w}\right) - 2}{\left(2\pi r_l + \frac{NC_u}{\epsilon_0} \ln (\alpha)\right)} \frac{\left(2\pi^2 r_l + \frac{NC_u}{\epsilon_0} \ln (\alpha)\right)}{\ln (\alpha)} - \frac{2}{2r_w} - 1\right]
\] with \( \alpha = \frac{d}{2r_w} + \sqrt{\left(\frac{d}{2r_w}\right)^2 - 1}\).

In conclusion, in the general case, for arbitrary values of \( Z \), the minima for \( r_l \) on the contour lines of Eq. (2) must be sought for: e.g. by a minimum search, in the \((N,r_l)\) domain bound by the conditions Eq. (5) and (9), for all frequencies in the \([f_L, f_H]\) interval.

B. Ideal Case: \( Z = \infty \)

In the ideal\(^1\) case that no load is attached to the loop sensor, the voltage between its terminals simply equals the voltage induced by the varying magnetic field, see Eq. (1).

Combining Eq. (5) with (1), only to be checked for \( f_L \), the lower bound of the intended frequency band, due to the proportionality of \(|V| \propto \omega \), results in the maximum amplitude that can be obtained with the best sensor, still obeying the condition imposed on the total wire length:

\[
|V| \leq \frac{\pi c^2 \omega_L B}{100\omega_H N} = V_{max}.
\] (10)

This leads to the obvious conclusion that, in case \( Z = \infty \), for maximum amplitude, \( N = 1 \). \( r_l \), related to the choice for \( N \) via Eq. (5), will then be as large as possible and \( A \) maximal.

If the voltage that is needed, \( V_{min} < V_{max} \), then \( N \geq 1 \). In this case a trade-off between good resolution, meaning small \( A \), and large frequency band, meaning small \( N \), can be made, still resulting in the same value for \( NA \). As soon as \( N > 1 \), however, Eq. (9) again bounds the solution space. Eq. (9) can be rewritten, in case \( Z = \infty \) and \( C_Z = 0 \), as:

\[
N r_l < \frac{c}{10\omega_H \sqrt{\frac{N}{N_{\text{switch}}}}}
\] (11)

with \( N_{\text{switch}} \) the value where both Eq. (5) and (9) are equivalent:

\[
N_{\text{switch}} = 2\pi^2 \ln \left(\frac{8r_l}{r_w}\right) - 2 \frac{\ln \left(\frac{\pi \omega_L c^2 B}{100\omega_H V_{\text{min}}}\right)}{\ln \left(\frac{d}{2r_w} + \sqrt{\left(\frac{d}{2r_w}\right)^2 - 1}\right)}
\] (12)

If \( N > N_{\text{switch}} \), only Eq. (5) should be checked, and the (integer) number of turns for the loop with minimal dimension or maximal resolution is found with Eq. (10) as:

\[
N_{\text{max}} = \left\lfloor \frac{\pi \omega_L c^2 B}{100\omega_H V_{\text{min}}} \right\rfloor,
\] (13)

else, only Eq. (11) should be checked. Eq. (11) combined with Eq. (1):

\[
N r_l = \sqrt{\frac{\pi N_{\text{min}}}{\pi \omega_L B}} < \frac{c}{10\omega_H \sqrt{\frac{N}{N_{\text{switch}}}}}
\] (14)

\(^1\)This case is ideal in the sense that the voltage measured over the loop terminals is maximal. Any load between the terminals would cause a current through the loop, resulting in a smaller loop voltage.
reveals that this condition is independent of the value for $N$. Stated otherwise, Eq. (11) for any value of $N$ is equivalent with Eq. (5) for $N = N_{\text{switch}}$.

Consequently, the design of an ideal inductive loop sensor with optimal resolution consists of: calculating $N_{\text{max}}$ with Eq. (13) and $N_{\text{switch}}$ with Eq. (12). If $N_{\text{max}} \geq N_{\text{switch}}$, then $N = N_{\text{max}}$, else $N = 1$. Once $N$ is determined, $r_l$ follows from Eq. (1), again only to be evaluated for the lower working frequency, due to $|V| \propto \omega$:

$$r_l = \sqrt{\frac{V_{\text{min}}}{\omega_L B \pi N}}.$$  \hspace{1cm} (15)

III. RESULTS - MAXIMAL RESOLUTION

To give some realistic numeric values, this section evaluates the formulas in Sect. II for a circular inductive sensor to measure a magnetic field of $B = 2 \mu$T that should deliver at least $V_{\text{min}} = 1$ mV.

The values for $r_w$ and $d$ are set to:

$$r_w = r_l/16 \quad \hspace{1cm} (16)$$
$$d = 2.4r_w \quad \hspace{1cm} (17)$$

corresponding to the rules of thumb of bending radii of wires in [12] and breakdown voltage between conductors.

The $r_l$ calculated below are of the order of magnitude of 10 $\mu$m. Loops of such small diameter, with conductors of even smaller dimensions can be produced, as is illustrated in e.g. Seidermann and Büttgenbach [13].

A. Ideal Case: $Z = \infty$

Evaluating Eq. (12) with the values in Eq. (16) and (17) results in $N_{\text{switch}} = 91$. Calculating $N_{\text{max}}$ with Eq. (13) and evaluating Eq. (15) with the appropriate $N$ as explained in Sect. II-B, for zero bandwidth, meaning $f_L = f_H$, results in the radii depicted by the solid line in Fig. 3. This is the practical resolution limit for $V_{\text{min}} = 1$ mV. The sudden discontinuity in the curve as $f = 10$ GHz is due to the jump from $N = 91 \rightarrow 1$, as indicated on Fig. 2. Also note that the curve stops at $f = 900$ GHz, as above this frequency, no sensor can be designed to deliver $V \geq V_{\text{min}}$ due to Eq. (10).

Fig. 4 depicts the loop radius in case $f_L$ is fixed and $f_H$ is varied from 1MHz $\rightarrow$ 10 GHz. This figure nicely illustrates the trade-off between resolution and working frequency band. At a certain value for $f_H$, no sensor can be designed to deliver $V \geq V_{\text{min}}$ due to Eq. (10) and the curve goes to zero. The curve has no meaning for values of $f_H < f_L$ and is hence set to zero. The flat part in the curves corresponds with $N = 1$. For zero bandwidth, Fig. 3, the radius decreased again with increasing frequency after the steep rise, due to the proportionality of $V$ with $\omega$ in Eq. (1). For a non-zero bandwidth, $f_L$ limits the resolution, resulting in the flat part of the curve.

Effects of the parameters on the optimal resolution

Eq. (12) reveals that $N_{\text{switch}}$ depends slightly on $r_w/r_l$ and heavily on $d/2r_w$ (especially for $d/2r_w \approx 1$, which is often the case when winding a conductor). Fig. 5 plots this dependency in the interval of interest for $r_w/r_l$ and $d/2r_w$. If $N_{\text{switch}}$ drops, a higher frequency upper bound can be achieved with the sensor, although this implies that if the same resolution has to be kept, the lower frequency bound has to go up. Fig. 6 shows the effect of varying ratio $d/2r_w$ on the resolution.

B. General Case: Arbitrary $Z$

As soon as a load is attached to the sensor, the resolution is equal to or worse than in the ideal case of no load over the loop. This is due to the division in Eq. (2). For $Z = 1$ M\(\Omega\), the difference in resolution is negligibly small, except for smaller frequencies. The dashed line in Fig. 3 indeed deviates from the solid line below 300 MHz. This is due to the difference in $N$. In case of no load $Z = \infty$, $N$ should be taken as high.
as possible with Eq. (13). In case of a finite load, however, an excessive value for $N$ results in a smaller loop voltage as $|j\omega L + R| \gg |Z|$ in Eq. (2).

The cases of Sect. III-A are reviewed here, for $Z = 50 \, \Omega$ and $Z = 1 \, M\Omega \parallel 13 \, pF$, which are typical oscilloscope input impedances. For the high impedance and zero bandwidth case, in Fig. 7, the curve for $r_l$ shows several spikes. Those abrupt changes in resolution are due to a decrease by one of $N$ (which has to be an integer), similar to the spike in the ideal case for the transition of $N : N_{\text{switch}} \to 1$. The results in the non-zero bandwidth case are depicted in Fig. 8.

As the number of turns in e.g. Fig. 2 is impractically high for some values of $f_L = f_H$, the effect of limiting $N \leq 30$ is illustrated for the case of $Z = 50 \, \Omega$ in Fig. 9. This deteriorates the resolution for lower values of $f_L$.

From a practical point of view, $N = 10^4$ can be regarded as excessive too. This treatment is however purely mathematical as a starting point.

Effects of the parameters on the optimal resolution

$d/2r_w$ now no longer has any effect. The curves for $d/r_w = 1.5$ and $2$ coincide with the curve for $d/r_w = 1.2$ (and $Z = 1 \, M\Omega \parallel 13 \, pF$) on Fig. 7. Fig. 10 shows the effect of varying ratio $r_w/r_l$ on the resolution in case of $Z = 1 \, M\Omega \parallel 13 \, pF$.

IV. CONCLUSION

In this paper, the practical resolution limit for a circular loop sensor, based on the magnetic field strength and the minimum voltage amplitude that should be provided by the loop, was evaluated. This resulted in numerical values for loops with an infinite load as well as for loops connected to a common oscilloscope input impedance. A straightforward design method could not be derived from the theory developed. A numerical search routine was used to achieve the optimal values for loop radius and number of turns.
Fig. 8. Minimum $r_l$ for some common oscilloscope input impedances with varying working frequency band.

Fig. 9. Minimum $r_l$ as function of $f_L = f_H$ for $Z = 50 \, \Omega$ with and without restriction on $N$.

**ACKNOWLEDGMENT**

This research is partially funded by the FWO under project G.0475.05, the “Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen)”, the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy) and K.U.Leuven-BOF (OT/06/40).

The authors would like to thank Frederik Vercauteren for the mathematical support.

**REFERENCES**


