Towards Quantum Sensing for Side-Channel Analysis

Oliver Butowski[1], Paul Haas[2], Jonas Hasenkrug[2], Niklas Mathes[2], Emanuele Strieder[1,4], Michael Kunzer[2], Jan Jeske[2], Nisha Jacob Kabakci[1] and Marc Stöttinger[3]

[1] Fraunhofer Institute for Applied and Integrated Security AISEC, Munich, Germany
firstname.lastname@aisec.fraunhofer.de
[2] Fraunhofer Institute for Applied Solid State Physics IAF, Freiburg, Germany,
firstname.lastname@iaf.fraunhofer.de
[3] RheinMain University of Applied Sciences and Arts, Wiesbaden, Germany,
firstname.lastname@hs-rm.de
[4] Technical University of Munich, Munich, Germany,
firstname.lastname@tum.de

Abstract. Side-Channel Analysis is an established field of research to assess implementation vulnerabilities of cryptographic algorithms. One typically exploited side-channel is the electromagnetic (EM) near-field, which is proportional to the data-dependent currents flowing through an Integrated Circuit (IC). The field of Quantum Sensing (QS) based on Nitrogen-Vacancy (NV) centers has shown promising approaches for different measurement configurations like scanning or spatially resolved wide-field imaging. Already today, QS has been used in the analysis of (quasi-)static magnetic fields on ICs in spatially-resolved wide-field magnetometers. In this work, we study the applicability of QS for the analysis of dynamic EM fields of ICs. For the first time, we demonstrate spectral-temporal analysis of the EM-side-channel using an NV-center-based Radio-Frequency spectrometer. Our sensor has a real-time bandwidth of 1.1 GHz with adjustable center frequency and directly probes the frequency spectrum via NV center interactions in the time domain. The approach circumvents any computations like Fourier transforms or performing frequency sweeps, enabling GHz-real-time bandwidths. We use this spectrometer to analyze the EM emanations of an RSA decryption and perform leakage detection of a software implementation of the Number Theoretic Transform - a building block of all current lattice-based post-quantum algorithms - running on a Cortex M4 commercial off-the-shelf microcontroller.

Keywords: quantum sensing · nitrogen-vacancy · radio-frequency spectrometer · side-channel analysis · electromagnetic

1 Introduction

Side-Channel Analysis (SCA) exploits side-channel leakage which arises during the execution of cryptographic algorithms on Integrated Circuits (ICs). One typically exploited side-channel is the electromagnetic (EM) near-field. The EM near-field can have multiple sources, like data-dependent currents flowing through an IC or high-frequency signals from switching or coupling events. The current state-of-the-art uses coils with diameters of typically around 100 µm to 500 µm to perform localized EM-SCA. This allows the spatial

separation of EM fields, which is not possible when exploiting the power-based side-channel. The spatial and temporal localization and separation of leakage from different cryptographic cores, hardware accelerators or parts of an algorithm are of particular interest for SCA [Str+23; Unt+18; ISU18; SA08; Agr+03].

Advances in the research field of Quantum Sensing (QS) have paved the way for new measurement techniques which seem to be a natural extension for EM-SCA. In this context, a well-established way to measure EM near-fields involves Nitrogen-Vacancy (NV) centers in the diamond lattice. NV centers exhibit unique magneto-optic properties that make them a versatile sensor for a variety of physical quantities, including static magnetic fields [Bar+20; Pha+11; Ste+10; Bal+08], EM radiation [De +11; LHM10; Maz+08], and temperature [Cho+18; Wan+15]. Depending on the experimental configuration, different measurement modalities can be realized. For example, in scanning [Hel+24; Sie24; Sch+14; Bal+08] and wide-field NV magnetometry [Gar+24; Sen+22; Chi+15b; Ste+10], these quantities can be measured in an imaging manner with micrometer spatial resolution. Detection of (quasi-)static magnetic fields of ICs using wide-field magnetometers has found various applications in IC analysis. Due to the large field of view (up to $3.7\,\text{mm} \times 3.7\,\text{mm}$ have been demonstrated in [Tur+20]) and micrometer spatial resolution, wide-field magnetometers have been presented as new sensors for trojan detection, defect localization, or current path visualization [Bis+25; Len+24; Gar+24; Ash+22; Keh+22; Oli+21; Tur+20].

In the context of ICs, wide-field magnetometers were used to measure (quasi)-static magnetic fields but not yet for the detection of the time-varying EM near-fields. Apart from wide-field magnetometers, other measurement modalities exist. Single channel bulk NV magnetometers enable detection of time-dependent magnetic fields with a high temporal resolution due to a high sensitivity to changes in the magnetic field strength [Sch+25; Bar+24; Sek+24; Gra+23], whereas on the other hand NV-based spectrometers [Chi+15a; Mag+22; Haa+25] enable detection of multiple (thousands of) frequency channels simultaneously with GHz-wide spectral coverage.

In this paper, we present the first step towards detecting dynamic EM near-fields on ICs relevant for SCA, with NV centers. We utilize an NV-based spectrometer to analyze the frequency spectrum of a Cortex M4 STM32L4 microcontroller and perform SCA in the frequency domain for the Number Theoretic Transform (NTT) and an RSA decryption. The Radio-Frequency (RF) spectrometer records frequency spectra using Optically Detected Magnetic Resonance (ODMR) measurements on NV centers of EM fields captured by a pickup coil. This allows for rapid one-shot detection of frequency spectra with a sampling-rate independent bandwidth. The RF-spectrometer records the frequency spectrum through direct interaction of the signal with the NV centers, which allows to record time-resolved frequency spectra without the need to compute a Fast Fourier Transform (FFT) or performing a frequency sweep [Chi+15a; Mag+22]. It exhibits several interesting capabilities for SCA: First, the frequency resolution and temporal resolution are largely independent of each other. The spectrometer can therefore achieve a high temporal as well as a high frequency resolution at the same time. Second, it is capable of recording large bandwidths up to multiple GHz with an adjustable center frequency, which is interesting for analysis of higher harmonics, especially for IC's or System on Chips (SoCs) running at clock speeds around and above 1 GHz.

Contributions.

- We present an NV-based RF spectrometer with a real-time bandwidth of 1.1 GHz, an adjustable center frequency, and direct frequency-spectrum acquisition with more than 1000 frequency channels that can be read out in parallel, without requiring FFT computations or frequency sweeps.

- We present time-frequency analysis with the NV-based RF spectrometer on the NTT and for an RSA decryption.
- Although currently limited in practical applicability, we, for the first time, perform leakage detection using the NV-based RF spectrometer, exploiting traces in the frequency domain. Our results show successful detection of unspecific (t-test) as well as specific (correlation-based) leakage of a software implementation of the NTT running on a commercial off-the-shelf IC as the Target of Evaluation (ToE).

2 Related Work

QS with NV centers has found applications in various research fields. To date, research on NV-based sensing for the analysis of ICs has largely focused on the measurement of static magnetic fields using wide-field magnetometers. Wide-field magnetometers work by illuminating an NV-doped diamond with a green laser and capturing the resulting red fluorescence with a camera sensor. The spatial distribution of the fluorescence provides information about the local magnetic field at each point on the diamond. This enables the imaging of both static and dynamic magnetic fields across the entire field of view. The following section provides an overview of the application of wide-field magnetometers to the analysis of ICs. In Section 2.2, we review literature related to the RF-spectrometer used in this work.

2.1 Application of NV Centers for IC Analysis

An extensive introduction to wide-field magnetometry, including measurement modes, sensitivity, and spatial/temporal resolution, is provided by Levine et al. [Lev+19]. Research has mainly focused on hardware trojan detection, current path visualization and defect detection. Hardware trojan detection aims to detect malicious alterations of a circuit, injected during any stage in the development cycle from circuit design to manufacturing, or the identification of counterfeits. Changes in side-channels such as temperature, power consumption, or EM radiation can indicate the presence of hardware trojans. Due to its high spatial resolution, wide-field magnetometry is well suited for localizing additional circuitry present in a trojan chip. Turner et al. [Tur+20] demonstrated the localization of a single ring oscillator (RO) and clusters of ROs on a Xilinx Artix 7 FPGA and identified the number of active ROs from wide-field measurements. Further localization of ROs was presented by Lenz et al. [Len+24], who focused on rare-event detection. Ashok et al. [Ash+22] also presented trojan detection on an Artix 7 FPGA by imaging static EM fields, distinguishing circuits with trojans from ones without trojans based on the amplitude and spatial distribution of the magnetic field.

The next application of wide-field magnetometry is the localization of current paths by measuring the static magnetic fields induced by the currents. Oliver et al. [Oli+21] mapped current paths on an NVIDIA GA106 GPU by measuring static magnetic fields from JTAG pins in all three vector components. Bisgin et al. [Bis+25] applied current path localization for failure analysis, identifying power-ground shorts on an Apple A12 chip by comparing current flow patterns between defective and intact devices.

2.2 RF-Spectroscopy

Experiments utilizing wide-field magnetometers for analyzing ICs have focused on the detection of (quasi-)static or time-averaged magnetic fields. However, in the context of SCA, time-varying fields are of greater relevance for analyzing leakage found in the dynamic power consumption of an IC or in high-frequency signals from switching or coupling events. NV-based spectroscopy, as will be detailed in Section 4.1, is very well suited for the

detection of time- and frequency-varying signals, as first demonstrated in [Chi+15a]. In this technique, microwave signals in the RF regime are transduced into optical signals via the NV spin-dependent fluorescence. Ongoing research activities on NV-based RF spectrometry demonstrate multi-GHz real-time bandwidths up to frequencies of 25 GHz, 1 MHz of frequency resolution and a dynamic range of up to 65 dB [Zho+25; Mag+22]. First demonstrations of real-life RF telecommunication signals have been achieved with compact NV-based sensor systems, reaching spectral refresh rates in the kilohertz regime [Haa+25; Kar20].

Compared to classical spectrum analyzers, which rely on digitization and FFT computation, NV-based RF spectroscopy bypasses any computation entirely. The frequency information is transferred into the optical domain via the NV centers in the diamond, enabling optical readout of the signals without downstream computations. Frequency resolution and obtainable refresh rates are governed by physical properties of the NV center but are largely independent of the bandwidth and center frequency within certain technical boundaries, see [Mag+22].

3 Background

In Section 3.1 we briefly revisit the origin of power and EM side-channels. We introduce the common capture and analysis process to exploit EM side-channels. We then present an in-depth introduction on NV center based QS in Section 3.3. In Section 4.4 we describe the ToE and the used cryptographic algorithms.

3.1 Side-Channel Sources

There exist multiple side-channels that can be exploited on ICs. The most common ones are power consumption, EM radiation, or data-dependent timing differences of the targeted implementation. Although the majority of publications exploit the power-based side-channel, the EM near-field is advantageous. If accessible, the local EM field allows the spatial separation of leakage sources of a ToE. To measure these local near-fields, coils with radii of around 70 µm to 500 µm are used. The power consumption P_{total} of an IC can be described as,

$$P_{\text{total}} = P_{\text{dyn}} + P_{\text{static}} + el_{\text{noise}}, \tag{1}$$

where P_{dyn} is the power consumption resulting from switching and data-dependent operations, P_{static} describes power consumption which is the result of the static state of the device, and el_{noise} describes the natural existence of noise [MOP07] in a Complementary Metal-Oxide-Semiconductor (CMOS) circuit. Side-channel leakage predominantly occurs through the dynamic power consumption of a CMOS circuit. The dynamic power consumption arises during the switching of logic cells, which is dependent on the processed data. On ICs, the current periodically passes through the metal layers, which act as antennas and emit EM radiation. The current and thus also the EM radiation is modulated by the clock frequency and influenced by the transistors of the circuit. To utilize a sensor for EM-SCA, it must be capable of measuring the EM near-field around the clock frequency and its higher harmonics. To conduct analysis in the time or frequency domain, this necessitates sampling rates exceeding the clock frequency (Nyquist frequency). The detection of leakage and attacks on the leakage can be done in the time domain as well as in the frequency domain [Bel+14; MG10; GHT05; Agr+03]. Analysis in the frequency domain can be beneficial when traces are misaligned, e.g. due to an unstable clock signal or the absence of a trigger signal. It is typically assumed that leakage is found around the clock frequency and its harmonics, since the electrical current in the metal layers is modulated by the clock frequency. The conversion to the frequency domain requires calculation of a Fourier

transformation, either in hardware or in software. In this work, we performed SCA in the frequency domain.

3.2 Side-Channel Evaluation

In SCA, there are non-specific and specific leakage tests. Specific leakage tests assume the possibility of an attacker to calculate an intermediate value of the target algorithm and the ability to characterize a leakage model that translates the mathematical representation of the intermediate value into the measured signal level. Calculating the intermediate value and finding a fitting leakage model might be a time-consuming process or not even possible when implementation details are missing. Therefore, specific leakage tests are often preceded by non-specific leakage tests. Non-specific leakage tests depend only on the knowledge about the input values to the target algorithm. The captured traces are grouped by their input values and compared by a chosen test statistic. In the following, the non-specific and specific leakage tests are introduced which are used during evaluation of the traces.

Non-Specific Leakage Test. A very popular non-specific leakage test is Test Vector Leakage Assessment (TVLA), which is based on Welch's t-test [Goo+11]. Welch's t-test is a statistical hypothesis test that verifies the null hypothesis whether two groups have equal means. The t-value can efficiently be calculated by using the empirical moments and is defined as

$$t = \frac{\mu_0 - \mu_1}{\sqrt{\frac{s_0^2}{n_0} + \frac{s_1^2}{n_1}}},$$

where μ_0 and μ_1 are the group means, s_0 and s_1 are the standard deviation and n_0 and n_1 the group sample sizes. Welch's t-test can be used if the sample sizes of the two groups are unequal and the variances of the two groups are not the same. This makes it a robust test tool in the SCA field. In TVLA a set of side-channel traces are recorded while executing the target implementation with a fixed input and another set of traces is captured with random inputs. If the t-value between these groups is above 4.5, the null hypothesis can be rejected with high confidence, indicating a significant leaking sample point.

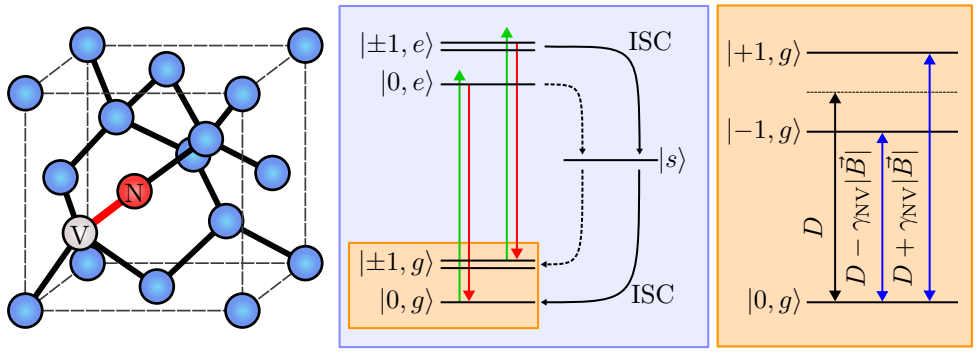
Specific Leakage Test. We use Correlating Points of Interest (CPOI) as a specific leakage test [DS15], which is as Correlation Power Analysis (CPA) based on Pearson's correlation coefficient [MOP07]. It additionally uses cross-validation to improve the reliability of the results. CPOI does not calculate the correlation between the pre-calculated intermediate values and the leakage samples of the traces, as done in CPA. Instead, it calculates the correlation between the leakage samples and a model derived from the grouped traces. As proposed in [DS15], we use the sample means. The grouping is done by using pre-calculated intermediate values. In the following, the algorithm is sketched. For a thorough description, we refer to the original paper [DS15]. The traces X are split into k distinct subsets of approximately equal size. For each cross-validation step j with $1 \leq j \leq k$, a profiling set $X_p^j = \bigcup_{i \neq j} X^i$ and a test set $X_t^j = X \backslash X_p^j$ are generated from the traces. A model m^j is estimated from the profiling set X_p^j. The correlation between the test set X_t^j and the estimated model m^j is calculated. Finally, the individual correlation results from each cross-validation step are averaged to obtain the final correlation values for each sample point. Throughout our evaluations, we used $k = 5$.

Time-Frequency Analysis. Time-resolved frequency spectra allow us to identify which frequencies are active at a certain time, allowing to identify patterns in the frequency domain. They are used in SCA, e.g., to identify starting points of operations of the

cryptographic algorithm under evaluation. In the absence of a trigger signal, patterns can help to define the time range of interest or to align traces [Yan+19; Lon+15; Deb+12]. Time-resolved frequency spectra are often calculated with the Short Time Fourier Transform (STFT). While the Fourier Transform transforms a complete time trace to the frequency domain - losing all time information - the STFT uses a sliding window to calculate a time-resolved frequency spectrum. For the STFT, the uncertainty principle states that the resulting time-resolved spectrum can either have a high frequency resolution or a high time resolution, but not both [Hof05]. The length of the window function determines the resolution. Short window lengths allow for a high time resolution, which is desirable for locating patterns, but results in a low frequency resolution. Contrary, long windows result in high frequency resolution, beneficial for separation of frequencies, but result in low time resolution.

3.3 QS with NV Centers in Diamond

In contrast to classical sensing, quantum sensing is based on the readout of single quantum states. Degen et al. [DRC17] list four conditions that a quantum system must fulfill to be used as a sensor: (1) It must have discrete and resolvable energy levels, (2) it must be possible to initialize a well-defined quantum state and read it out, (3) the quantum state can be manipulated coherently, and (4) the quantum state interacts with the quantity that is to be measured.



Structure of a NV center

Energy level diagram of the NV center

Energy levels in the ground state

Figure 1: Structure of an NV center and the energy level diagram.

Figure 1 depicts the structure of the NV center, consisting of a nitrogen atom (N), an adjacent vacancy site (V), and the surrounding carbon atoms of the diamond lattice. The axis connecting the nitrogen atom and the vacancy is called the NV axis. Due to the tetrahedral structure of the diamond lattice, this axis can take four possible crystallographic orientations. NV centers can exist in different energy states. An overview of these states is also shown in Figure 1 as an energy level diagram. Here, the ground state $|g\rangle$, the excited state $|e\rangle$, and a metastable state $|s\rangle$ can be distinguished, where the $|\cdot\rangle$ notation simply labels the intrinsic quantum states of the system. The ground state $|g\rangle$ and the excited state $|e\rangle$ are further split into three energetic sublevels. These sublevels depend on the spin state of the NV center. The spin can take the values $m_s = 0, \pm 1$. The energy difference between these spin states is determined by two main effects: the zero-field splitting and the Zeeman effect. Since the focus of this paper is on the application of NV-based QS for SCA rather than the detailed physical background, the following explanation is simplified. A more detailed introduction is provided by Abe and Sasaki [AS18].

The zero-field splitting leads to a separation of the energy levels of the states $|0, g\rangle$

and $|\pm 1, g\rangle$, even in the absence of external magnetic fields. The energy difference is given by the zero-field splitting parameter $D = 2.87\,\text{GHz}$. This frequency corresponds to the microwave frequency required to drive the transition between the states. When an additional external magnetic field is applied to the NV centers, the Zeeman effect further alters the energy levels. It results in the states $|-1, g\rangle$ and $|+1, g\rangle$ being shifted symmetrically away from the frequency 2.87 GHz, when the magnetic field is oriented parallel to the NV axis. The resulting energy difference between the state $|0, g\rangle$ and $|\pm 1, g\rangle$ can in this case be calculated with

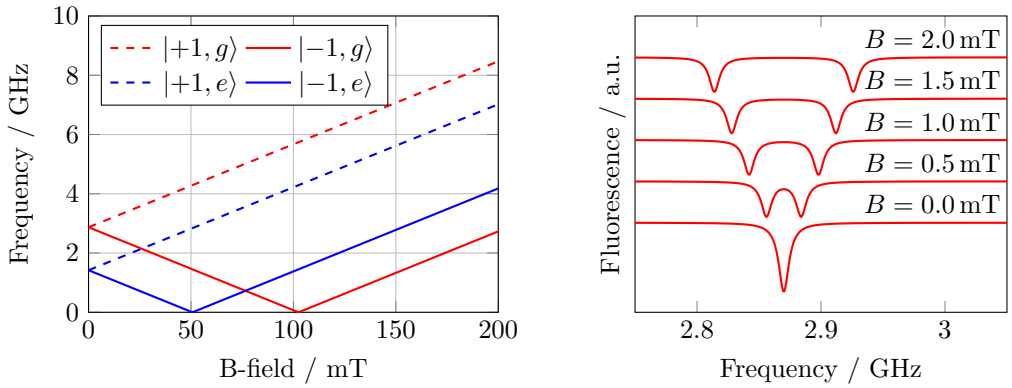
$$f_{\text{res}}^{(\pm)} = D \pm \gamma_{\text{NV}} |\vec{B}| = 2.87\,\text{GHz} \pm 28\,\text{MHz/mT} \cdot |\vec{B}| \quad \text{for } \vec{B} \parallel \vec{n}_{\text{NV}} \tag{2}$$

where D is the zero-field splitting parameter, $\gamma_{\text{NV}} = 28\,\text{MHz/mT}$ is the gyromagnetic ratio, $\vec{B}$ is the magnetic field vector, and $\vec{n}_{\text{NV}}$ is the direction of the NV axis, which is given by the crystallographic orientation of the nitrogen atom to the adjacent vacancy. The described symmetry can only be achieved when the magnetic field is parallel to the NV axis. For the excited state, a similar behavior occurs, with a zero-field splitting parameter of $D_{es} = 1.42\,\text{GHz}$ and the same gyromagnetic ratio of $\gamma_{\text{NV}} = 28\,\text{MHz/mT}$. The resonance frequencies between the $m_s = 0$ and $m_s = \pm 1$ states as a function of magnetic field strength, for both the ground and excited states, are shown in Figure 2a.

To transfer the NV centers from the ground state $|g\rangle$ to the excited state $|e\rangle$, they are illuminated with light in a wavelength range of 400 nm to 637 nm, indicated by the green arrows in Figure 1. In practice, lasers with a wavelength of 520 nm or 532 nm are commonly used, as they are common laser wavelengths and provide efficient excitation. This optical excitation is spin-conserving, meaning that the spin state remains unchanged during the transition. For example, an NV center in the state $|0, g\rangle$ is excited to $|0, e\rangle$ and not to $|-1, e\rangle$ or $|+1, e\rangle$. From the excited state, the NV center can relax back to the ground state via two ways. The first path is a radiative decay, in which a photon is emitted with a wavelength in the range of 637 nm to roughly 850 nm, indicated by the red arrows in Figure 1. Similar to the excitation, this transition is spin-conserving. The second pathway involves a non-radiative intersystem crossing (ISC) to the metastable state $|s\rangle$. From this state, the NV center relaxes to one of the spin states in the ground state via another non-radiative ISC. This relaxation process is not spin-conserving. Predominantly, the NV centers in the state $|\pm 1, e\rangle$ relax via this path and thereby emit less red photons during the relaxation.

These effects enable the NV center to be used as a quantum sensor: (1) The energy levels, as described, are well defined. (2) The spin state of NV centers can be initialized optically by illuminating them with green light. The NV centers in the state $|0, g\rangle$ are excited to $|0, e\rangle$ and relax back to $|0, g\rangle$, thereby remaining in the spin state $m_s = 0$. The NV centers in the state $|\pm 1, g\rangle$ are excited to $|\pm 1, e\rangle$ and can relax via the metastable state back to the ground state and thereby end up in the ground state without remaining in the same spin state. These two processes lead to an accumulation of the NV centers in the spin state $m_s = 0$. The spin state can be read out optically by monitoring the resulting red fluorescence, since the NV centers in the state $m_s = \pm 1$ lead to a lower red fluorescence than the ones in the state $m_s = 0$. (3) By applying a microwave, the frequency of which matches the energy difference between the states $|0, g\rangle$ and $|-1, g\rangle$ or $|+1, g\rangle$, the spin state can be manipulated coherently. (4) Finally, due to the Zeeman effect and the applied microwaves, the quantity that is to be measured, e.g., magnetic fields and EM radiation, interacts with the quantum state of the NV centers.

Measurement of Static Magnetic Fields. To measure the field strength of static magnetic fields, the optically detected magnetic resonance is utilized. A green laser is used to initialize the spin state of the NV centers to $m_s = 0$, while simultaneously monitoring the resulting red fluorescence. Next, a microwave is applied, and its frequency is swept.



(a) Dependence of the ground and excited state resonance frequencies on the magnetic field strength

(b) ODMR spectra at different magnetic field strengths, showing splitting of the resonance frequencies

Figure 2: (a) Static magnetic fields cause shifts in the resonance frequencies of the NV center ground and excited states due to the Zeeman effect. (b) When EM fields with frequencies near the resonance frequencies are applied, the fluorescence of the NV centers decreases, enabling measurement of the magnetic field strength.

When the frequency of the microwave matches the energy difference between the energy levels of the spin states $|0,g\rangle$ and $|-1,g\rangle$ or $|+1,g\rangle$, the fluorescence decreases. When plotting the resulting fluorescence over the applied frequency, as shown in Figure 2b, two resonance dips at the frequencies given by Equation (2) can be observed. If the fluorescence decreases for the frequency $f^{(-)}$ and $f^{(+)}$, then the magnetic field can be calculated with $B = (f^{(+)} - f^{(-)})/(2\gamma_{\mathrm{NV}})$. Up to 8 resonance dips, originating from the four possible orientations of the NV axis in the diamond lattice and the two ground state transitions, can be observed.

Measurement of EM Spectra. As described above, magnetic field measurements rely on probing the resonances of NV centers by applying known microwave frequencies in order to infer the unknown magnetic field strength. NV-based spectroscopy inverts this principle: A well-defined magnetic field with a gradient splits the energy levels of the NV centers due to the Zeeman effect, leading to position-dependent resonance frequencies (see Figure 3). When an unknown signal is applied to the NV-doped diamond, its spectral components can be spatially resolved. This is achieved by monitoring the fluorescence along the magnetic field gradient, where different frequency components become resonant at different positions and thus produce localized decreases in fluorescence. In this way, the NV-doped diamond effectively bridges the RF and optical domains, enabling a direct, time-resolved readout of RF spectra.

4 Experimental Setup

In the following, we present a case study of an NV-based spectrometer for the analysis of the EM fields emitted by ICs. In Section 4.1, we introduce the employed NV-based spectrometer. The measurement setup for SCA measurements is described in Section 4.2 and Section 4.3. We present the ToE and used cryptographic algorithms in Section 4.4.

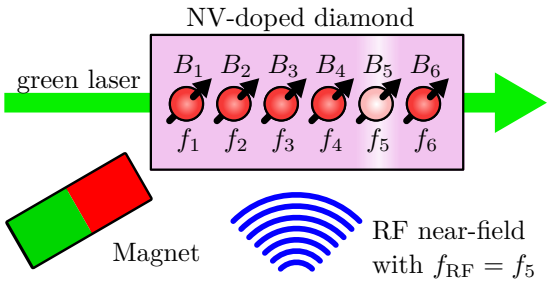


Figure 3: Principle of NV-based spectroscopy: The magnetic field gradient causes each NV center to experience a distinct magnetic field strength $(B_1, \ldots, B_6)$ and thereby having a different resonance frequency $(f_1, \ldots, f_6)$. The signal under analysis is only resonant at certain positions and results in a local decrease in fluorescence. In practice, measurements are performed on an ensemble of NV centers, yielding a continuous spectrum instead of the discrete response of individual NV centers as depicted here.

4.1 NV-Based Spectrum Analyzer

A schematic of the NV-based spectrometer used in this work is depicted in Figure 4. The NV centers in the diamond crystal are excited and initialized using a 532 nm green Diode Pumped Solid State (DPSS) laser. The beam is coupled into a mm-sized diamond through a polished side facet, where it forms an approximately 2 mm-long linear focus with a diameter of about 20 µm along the magnetic-field gradient. This creates a linear region of interest (ROI) in which the NV centers emit a narrow strip of red fluorescence through the main diamond facet. The red fluorescence is collected with a 5× microscope lens, passed through a 630 nm long-pass filter, and imaged onto the sensor of a line scan camera. Because of the high lateral optical resolution of the imaging system, different positions along the ROI map to distinct pixel columns on the camera, effectively forming individual frequency channels.

The center frequency of the RF sensor is defined by the applied bias field, while the simultaneously covered frequency range is determined by the magnetic-field gradient and lateral dimension of the ROI (see Figure 4). The 2 mm-long ROI, combined with a gradient of 20 mT/mm and the NV center's gyromagnetic ratio of 28 MHz/mT results in a coverable bandwidth of more than 1.1 GHz. The fluorescent signal strength of the NV ensemble is strong enough to operate the line scan camera with several thousand frames per second. This in turn results in a 1.1 GHz wide spectrum, which is refreshed every hundreds of µs. A microwave coupling structure is used to feed the RF signals under test into the diamond. In the used setup, a copper coplanar waveguide serves as the base onto which the NV-doped diamond is bonded, similar to the design found in [Jia+18]. To calibrate the spectrometer, a range of known RF frequencies is swept through from a conventional signal source. The swept range must match or include the operating band determined by the magnetic bias field. For each frequency, the spatially encoded Electron Spin Resonance (ESR) with the NV ensemble is revealed. From this calibration step being performed once prior to sensing, the frequency-pixel relation is obtained, which is then applied to the raw data of the camera frames. Additionally, one background image is captured in which no RF signal is fed into the diamond. This background is then subtracted from frames acquired in sensing experiments to create a differential image. Dividing this subtraction by the background yields the ODMR contrast in percent, which is a central metric and is typically given in this form in NV-based QS [Kar20; Mag+24]. Upon alteration of the magnetic bias field or other parameters, a recalibration is required.

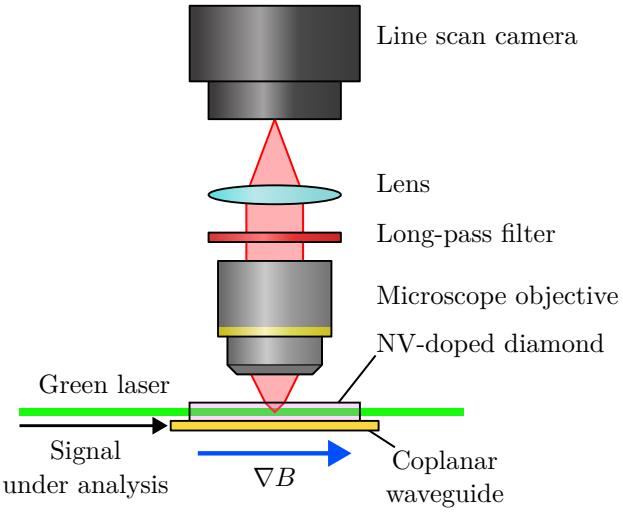


Figure 4: Experimental realization of the NV-based spectroscopy. A diamond crystal containing NV centers is placed in a magnetic gradient field. A laser beam is coupled into the diamond, illuminating a line profile of the NV ensemble. The fluorescence light is imaged on a line camera. A coplanar waveguide is used to couple the signal under analysis to the NV centers.

4.2 Measurement Configuration for SCA

In this work, we chose to analyze the EM side-channel, but the spectrometer could also be used to analyze power side-channels. To employ the spectrometer for the analysis of the near-field emanations of a ToE, the emitted signal needs to be captured and amplified before being fed into the spectrometer. We achieved the highest contrast without saturating the NV centers due to excessive amplification, when using an EM loop coil (Langer EMV LF-B-3 probe) in combination with a series of two amplifiers, consisting of a Langer EMV PA 303 30 dB amplifier and an Ophir 5064 48 dB (50 W) amplifier. The frequency range of the used amplifiers range from 100 kHz to 3 GHz and 1 MHz to 1 GHz, which is sufficient for the experiments conducted here.
As we pick up the near-field emanations with a pick-up coil, the spectrometer captures a field that is proportional to the time derivative of the near-field generated by the ToE. The coil outputs a voltage U_{out} that is proportional to the rate of change of the magnetic flux $\Phi(t)$.

$$U_{\text{out}}(t) = -N\frac{d\Phi(t)}{dt} \quad \text{with} \quad \Phi(t) = \int \mathbf{B}_{\text{EM}}(\mathbf{t}) \cdot d\mathbf{A} \tag{3}$$

Here, N is the number of coil turns, $\mathbf{B}_{\text{EM}}$ is the magnetic field, and $\mathbf{A}$ is the area enclosed by the coil. The output voltage is amplified to $U_{\text{amp}}(t)$ and then applied to the coplanar waveguide. Here, $U_{\text{amp}}(t)$ leads to a time-varying current $I_{\text{amp}}(t)$ in the coplanar waveguide, which results in a time-varying magnetic field $B_{\text{amp}}(t)$ around the coplanar waveguide. This field drives the spin transition of the NV centers and leads to the decrease of their fluorescence. In other words, the NV centers are driven by a field that is proportional to the time derivative of the EM near-field generated by the IC, rather than by the EM near-field itself or a field proportional to it. It should be noted that significant simplifications are assumed in this description, for example, regarding the emission characteristics of the coplanar waveguide, the influence of the amplifier, and other possible effects.

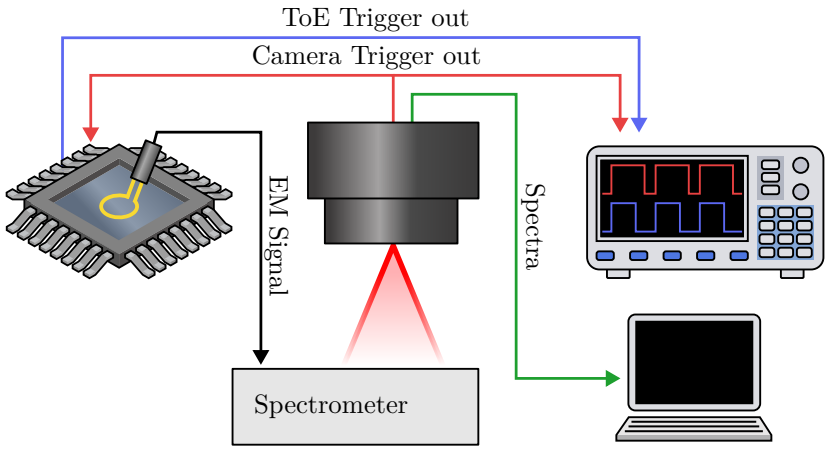


Figure 5: Schematic representation of the synchronization between target and camera.

4.3 Triggered Measurements for TVLA

In this work, we perform TVLA in the frequency domain on the NTT with spectra captured with the QS spectrometer. TVLA requires capturing and labeling individual executions of the cryptographic algorithm with different input values, in this case, fixed and random input values. To achieve this, the spectra recorded by the line-scan camera must be assigned to a corresponding execution of the cryptographic algorithm. As the frame rate of the spectrometer is not high enough to temporally resolve subparts of the NTT (i.e., the butterflies), we set the exposure time of the spectrometer to match the execution time of the NTT, which in our case is around 1 ms. Thus, each recorded spectrum corresponds to a single execution of the NTT. We implemented a synchronization between the camera and the ToE based on a trigger output signal from the camera. Figure 5 illustrates the synchronization used between the camera and the ToE. The camera operates at a fixed frame rate and exposure time. During the exposure interval, the trigger of the camera is set to high, and during the 5 µs sensor readout time, it is set to low. The camera trigger signal is used as an input trigger for the ToE, which is programmed to execute the given algorithm upon the rising edge of the trigger signal. The camera records as many executions as possible until the camera buffer reaches its maximum capacity. An oscilloscope is used to monitor successful triggering. To facilitate fixed versus random TVLA measurements, we implemented a five-step pipeline on the ToE. The pipeline is shown in Figure 6 and consists of the following steps: data initialization, idle state, NTT execution with fixed input, idle state, and NTT execution with random input. During the first stage, the target initializes the fixed and random inputs for the algorithm. We moved this step to a separate block to exclude potential leakage from the random number generation or `memcopy` operations. In the next stage, the target is in an idle state. The idle state serves as a reference for the subsequent measurement blocks. This procedure ensures equal initial conditions prior to the intervals of the NTTs with fixed and random input. The target then executes the NTT with the fixed input, followed again by an idle state and the execution of the NTT with random input. This setup allows for fast acquisition of fixed and random algorithm executions, as the frames are captured in the internal camera buffer. Only when the camera buffer is full is the data downloaded to the PC.

4.4 Target of Evaluation

Hardware Setup. As ToE, we use an STM32L4 microcontroller. To facilitate EM near-field measurements, we decapsulated the LQFP package of the ToE from the backside and

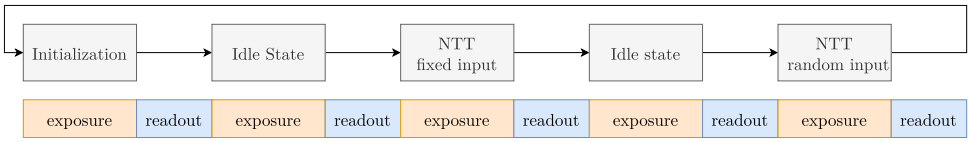


Figure 6: Pipeline implemented on the ToE to capture frames for TVLA measurements.

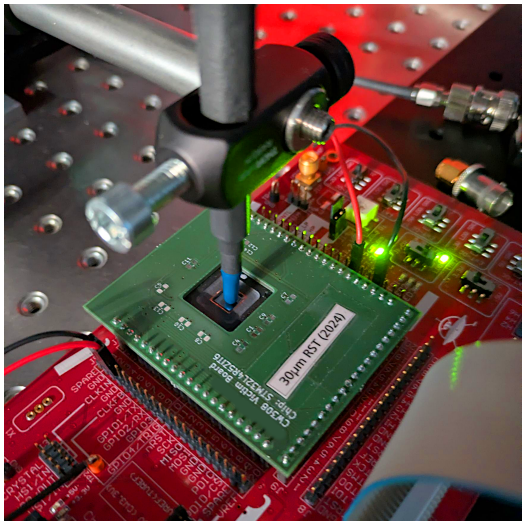


Figure 7: Picture of the measurement setup showing the EM pick-up coil placed on the decapsulated and thinned die of the ToE.

milled the silicon layer to a Remaining Substrate Thickness (RST) of 30 µm. We designed a target Printed Circuit Board (PCB) to operate the ToE on a ChipWhisperer CW308 UFO Board. The ToE is mounted from the backside onto the PCB and EM measurements are possible through a cut-out in the PCB. Figure 7 shows the setup. The microcontroller is operated at a clock frequency of $f = 48\,\text{MHz}$, which is supplied externally to ensure a stable frequency spectrum of the EM emanations.

Software Setup. As cryptographic algorithms in this work, we chose the NTT and the RSA. The Number Theoretic Transform (NTT) is a major building block in lattice-based Post-Quantum Cryptography (PQC) like the recently standardized Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) [Nat24b] or the Module-Lattice-Based Digital Signature Standard (ML-DSA). [Nat24a]. ML-KEM is a key-encapsulation mechanism used to establish a shared secret key between two entities. It operates in the ring $R_q = \mathbb{Z}_q/(X^n+1)$. In ML-KEM, the NTT is used to perform efficient multiplication in R_q. The NTT transforms polynomials f in the ring R_q to the NTT domain, and the Inverse NTT (INTT) transforms the polynomial back to R_q. The NTT is internally constructed with so-called butterflies. Each butterfly consists of a multiplication with a so-called twiddle factor ω_n^0, an addition, and a subtraction. Previous side-channel attacks have attacked the NTT by profiling the inputs x and the outputs $\hat{x}$ of the butterflies and using belief propagation to reconstruct secret intermediate values in ML-KEM [PP19; PPM17]. In this work, we aim to detect leakage of the inputs x and the outputs $\hat{x}$ of an NTT butterfly with QS. Throughout this work, we analyzed a software implementation of the NTT running on the ToE. We used the official reference implementation of Kyber, written in C code [pq-20; Bos+18].

RSA is a public-key cryptographic algorithm, which uses a pair of keys, of which the public key is used for message encryption and the private key is used for decryption. Implementations of the RSA algorithm compute a modular exponentiation, conventionally implemented as a binary exponentiation with the square and multiply algorithm. The modular exponentiation is broken down into sequences of modular square and multiplication steps. For each bit of the private key, a single modular square or a modular square followed by a modular multiplication is executed, based on the value of the key bit. Such naive implementations are subject to timing attacks and Simple Power Analysis (SPA) attacks. Time constant implementations can still be exploited if key-dependent behavior can be distinguished in the power or EM side-channel, e.g., the dummy multiplication in square-and-multiply-always implementations or the extra reduction in the Montgomery ladder implementation. The implementation used in this work implements a sliding window exponentiation with a window length of 2. The RSA implementation is used in this work to demonstrate the time resolution and sensitivity of the spectrometer, rather than to perform an actual attack.

5 Experimental Results

We used the RF-spectrometer to record and analyze the EM emanations of an RSA signature and the NTT running on the Cortex M4 STM32L4 microcontroller (ToE).

5.1 Time-Frequency Analysis

First, we assess whether the sensitivity and time resolution of the spectrometer are sufficient to perform time-frequency analysis on the EM side-channel. With the presented spectrometer (see Figure 4) and measurement setup (see Section 4.2), we achieved a maximum frame rate of 4.8 kHz. We recorded the frequency spectrum of an RSA-2048 signature running on the ToE at 48 MHz. The resulting ODMR contrast across the frequency spectrum is shown in a waterfall diagram in Figure 8. The figure shows the ODMR contrast between the fluorescence intensity during the measurement and a background spectrum, which was acquired while the ToE was not powered. We observe the highest contrast at and around the fifth harmonic of the clock frequency $f = 48\,\text{MHz}$. In the frequency spectrum, we can identify several patterns, which we mapped to individual steps of the algorithm by measuring their execution times on the ToE. Thus, we can identify the start of the RSA algorithm and the start of the modular exponentiation module, as the increased contrast stands out. The used RSA implementation uses a sliding window exponentiation with window size 2. With the measured execution times, we can identify the start of the first (1) and second (2) iterations of the sliding window exponentiation. A barely visible gap of lower contrast (3) indicates the start of the second square operation of the second iteration. The results show that the spectrometer is sensitive enough and the time resolution is sufficient to identify individual steps of the modular exponentiation, which motivates further investigation of horizontal SCA attacks with this spectrometer.

Next, we analyzed the NTT, which allows a straightforward analysis with specific leakage tests. As the currently achievable time resolution is not sufficient to analyze individual parts of the NTT, we chose to set the frame rate to match the execution time of the NTT. We determined the execution of the NTT using an oscilloscope and a software trigger. The exposure time was therefore set to 1.1 ms (909 fps). Since the frequency spectrum is directly measured through the interaction of the NV centers with the signal and no sampling or FFT calculation is required, we acquire the complete frequency spectrum of the NTT in a single frame. Before we perform further analysis, we identified the execution of the NTT using visual inspection of two algorithmic configurations with 1 execution and

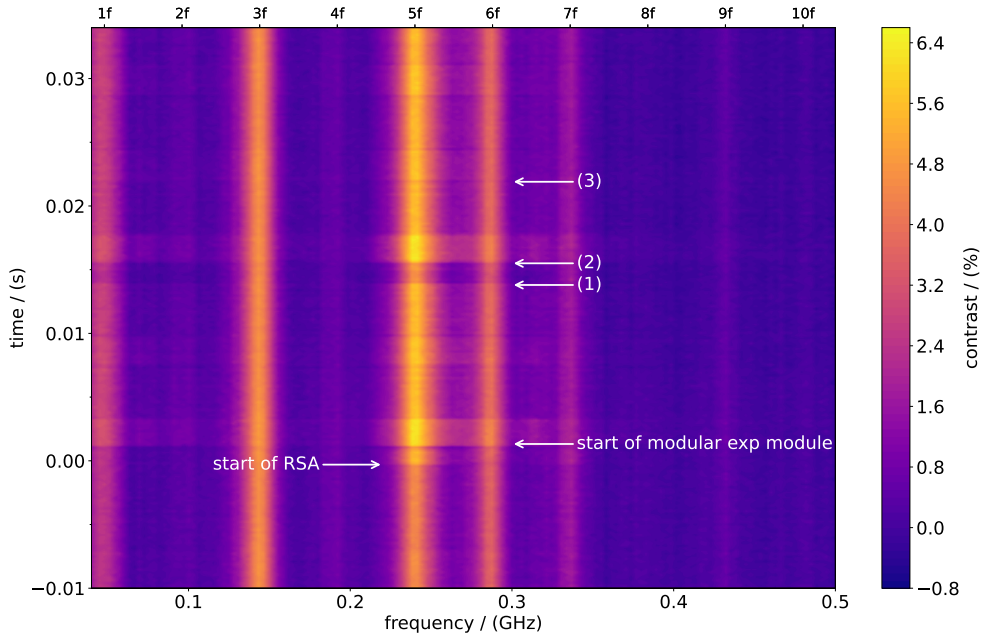


Figure 8: The QS time-frequency analysis of the start of an RSA-2048 signature running at $f = 48\,\text{MHz}$ on the ToE shows the ODMR contrast in percent between the spectrum and a background spectrum recorded while the ToE was not powered.

respectively 10 executions of the NTT. The resulting ODMR contrast of the frequency spectrum for the execution of a block of 10 (top) and a single NTT (bottom) is shown in a waterfall diagram in Figure 9. The waterfall diagram shows the fluorescence contrast (color scale) for frequencies from 14 MHz to 0.5 GHz (x-axis) over a cutout of the measurement time (y-axis).

The clock frequency of $f = 48\,\text{MHz}$ can be identified clearly during the idle state and the execution of the NTTs. We observe an increased ODMR contrast during the execution of the NTT, corresponding to a higher signal strength. From the waterfall diagram, it can be identified that the NTT executions and the idle state can be differentiated across multiple frequency bands. The first difference is observable at the lower end of the RF-spectrometer's bandwidth. Between 14 MHz and around 30 MHz, the NTT execution leads to an increased intensity. Presumably, these resonances are related to higher or subharmonic frequencies of the source resonant with the NV center ground or excited state. While there is no noticeable difference in the frequency spectrum at the clock frequency and the second, third, and forth harmonic, the fifth and sixth harmonics (240 MHz and 288 MHz) show clear differences between the execution of the NTT and the idle state. Also, between the fifth and sixth harmonic, there are slight differences visible. The result shows that the execution of the NTT creates an increased ODMR contrast and can be distinguished from the idle state across multiple frequency bands.

5.2 Unspecific Leakage

In the following, we performed the detection of unspecific leakage by applying TVLA on traces captured with the RF spectrometer. TVLA requires the recording and labeling of individual spectra for the algorithm executions. We implemented the synchronization between camera and ToE (see Section 4.3), allowing us to precisely capture and label the frequency spectra of individual operations. To capture the spectra needed to perform

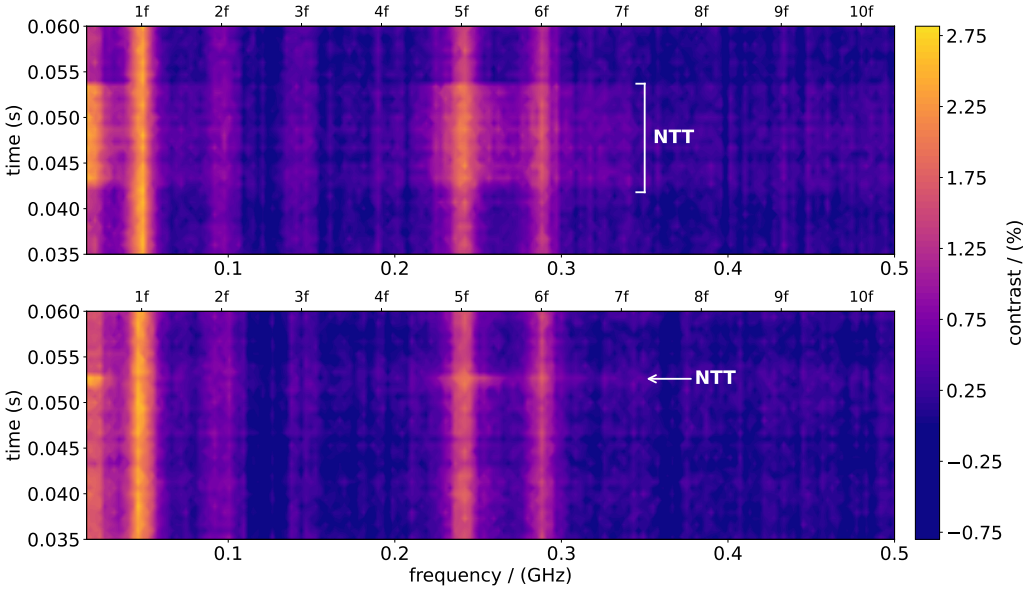


Figure 9: QS time-frequency analysis for the execution of 10 (top) and 1 (bottom) NTT operations surrounded by an idle state executed on the ToE at $f = 48\,\text{MHz}$. Execution of the NTT algorithm leads to an increased ODMR contrast which corresponds to a higher EM signal strength.

TVLA, we implemented the five-stage pipeline shown in Figure 6 on the ToE. The pipeline stages are: initialization, idle state, NTT with fixed input, idle state, and NTT with random input. We fully automated the setup to perform 10 measurements with an automated download of the contents of the camera buffer after each measurement. As in Section 5.1, before each measurement, a separate background spectrum was recorded while the ToE was not powered, to account for possible drifts of the laser power over time. The camera was set to record at 909 Hz to match the execution time of the NTT. In total, we recorded 102 500 traces, which results in 20 500 NTT executions with fixed input, and 20 500 traces with random input due to the pipeline structure, which has 5 steps. The measurement took 2.5 min to record and results in a capture rate of the NTT of 273 traces/s.

The mean fluorescence contrast for the individual pipeline stages can be seen in Figure 10 (top). The vertical dashed lines indicate the higher harmonics of the clock frequency. As expected, we see that the idle states yield the lowest contrast. The initialization phase, which included the random number generation and `memcopy` instructions, shows an increased contrast compared to the idle states. The two algorithm executions yield the highest contrast and, more importantly, yield distinguishable frequency spectra. The largest difference between fix and random execution can be observed between the fourth and seventh harmonic. We performed TVLA on the recorded spectra. The result of the fix-versus-random t-test evaluation (20 500 vs. 20 500 traces) is plotted in Figure 10 (bottom). It shows t-values above the significance threshold mainly between the fourth and seventh harmonic, which could already visually be seen from the means. The maximal t-value can be observed at 268.5 MHz with a t-value of 321. Furthermore, the t-test reveals that fixed and random execution are also differentiable at the third harmonic with a t-value of 113. The results show that fix and random NTT executions can be differentiated in the frequency domain from spectra acquired with the spectrometer, which allows for detection of unspecific leakage.

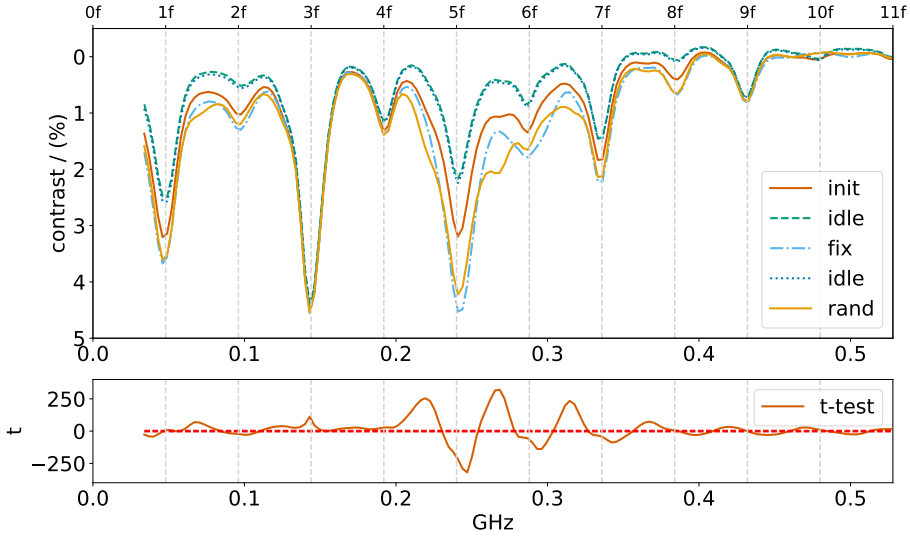


Figure 10: Averaged frequency spectra for the recorded blocks of the five-stage pipeline (top). A t-test evaluation between fixed and random NTT execution (bottom). The dashed vertical lines indicate the multiples of the $f = 48\,\text{MHz}$ clock frequency. The horizontal red line indicates the t-test significance threshold of ± 4.5.

5.3 Specific Leakage

The following results demonstrate a proof-of-concept detection of specific leakage of different intermediates within a single NTT butterfly using the NV-based spectrometer.

The previous experiment demonstrated the possibility of detecting differences in the first statistical moment. However, these differences were computed for the complete NTT because of limitations of the chosen camera frame rate. From a side-channel perspective, leakage of subparts of the NTT is of interest, more precisely of the inputs and outputs of individual butterfly layers. As intermediates, we chose the inputs x and outputs $\tilde{x}$ of a single NTT butterfly, since attacks in the literature have exploited leakage from these intermediates to recover the secret keys processed in, e.g., ML-KEM [Her+23; PP19; PPM17]. A single NTT butterfly of our software implementation takes approximately 2.5 µs to execute at a clock frequency of 48 MHz, which, based on our current sensor architecture, is not resolvable due to an insufficient temporal resolution. To increase the Signal-to-Noise Ratio (SNR) of the leakage within the measurement for this proof-of-concept experiment, we chose to repeat the butterfly multiple times to cover the complete exposure time. After each repetition of the butterfly, we reset the input polynomial. We then calculated the CPOI metric (see Section 3.2) between the intermediates and the spectra for each frequency while using the Hamming weight (HW) leakage model. We performed the experiment with an exposure time of 1.1 ms with 800 butterfly repetitions and with an exposure time of 250 µs and 200 butterfly repetitions. To allow measurements with the lower exposure time, the laser power was increased to increase the number of detected photons. The resulting correlation ρ for the four intermediates $x[0]$, $x[1]$, $\tilde{x}[0]$ and $\tilde{x}[1]$ are shown in Figure 11 for the 1.1 ms (A) and the 250 µs (B) exposure time. The results show that the correlation stands out from the noise floor for all four intermediates and for both exposure times. As already encountered in Section 5.1, leakage is not detected mainly around the clock frequency but between the fourth (192 MHz) and the seventh harmonic (336 MHz). The highest correlation is observed for $\tilde{x}[1]$ with a maximal correlation of $\rho = 0.52$. The

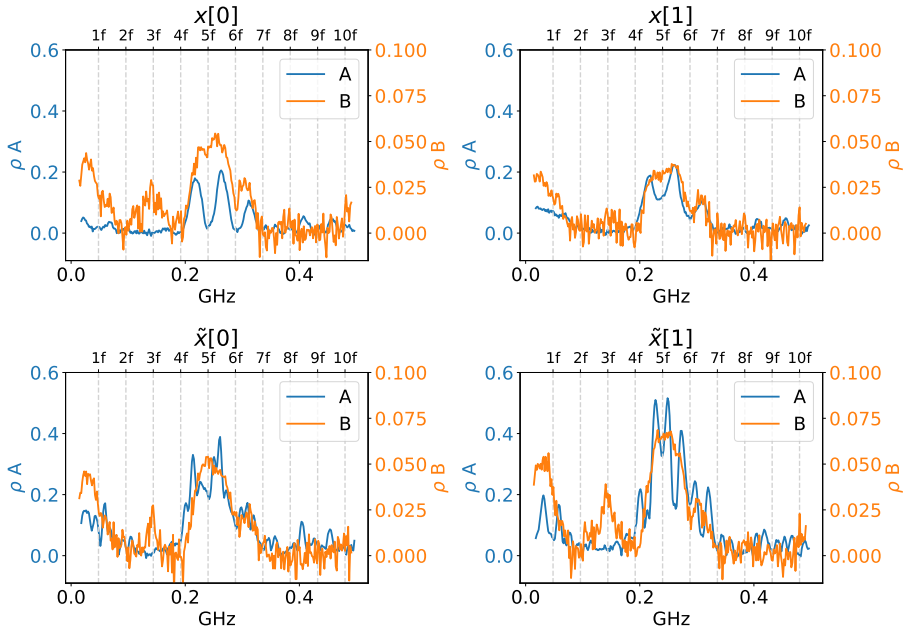


Figure 11: Correlation ρ between the spectra and HW of inputs $x[0], x[1]$ and outputs $\tilde{x}[0], \tilde{x}[1]$ of the first butterfly layer. Measurement conducted with 800 butterfly repetitions (A) and 200 butterfly repetitions (B). The camera exposure time was set to 1.1 ms (A) and 250 µs (B). Multiples of the clock frequency $f = 48$ MHz are indicated by dashed vertical lines.

correlation for the shorter exposure time shows values about a factor of 10 lower than the higher exposure time.

This experiment demonstrates the detectability of signals below the sensor's Nyquist limit. Even though the spectrometer cannot temporally resolve these signals, they are detected spectrally. The results show the general possibility to perform data-dependent leakage detection with the spectrometer, while currently limited in practicability by the achievable frame rate.

6 Discussion

In this section, we discuss the practicability and potential of the presented NV-based spectrometer for EM-SCA. We focus on aspects such as time resolution, leakage detection, and the advantages and future prospects of this technology.

6.1 Practicability for SCA

The time resolution of the used spectrometer is an important factor for the practicability of leakage detection, as it determines how fine leakage can be temporally resolved. We have presented successful measurements with a camera frame rate of up to 4.8 kHz. We found this frame rate to be sufficient for analysis of a software implementation of asymmetric cryptography (see Figure 8) running at 48 MHz. Specifically, we identified individual modular square operations in an RSA-2048 signature, motivating performing horizontal SCA attacks with QS. The analysis of subparts of cryptographic algorithms still requires higher frames rate to temporally resolve leakage. While we presented TVLA of the NTT,

this analysis was performed for the complete NTT with around 1 ms exposure time, instead of individual butterfly operations, which are of interest for SCA. As the RF-spectrometer does not capture phase information, the signal also cannot be transformed to the time domain.

We performed detection of data-dependent leakage of NTT butterflies with 1 ms and 250 µs exposure time and found that in both cases the correlation values clearly stand out from the noise floor, but the shorter execution time showed a factor 10 lower correlation value. This result is to some extent expected due to the shorter presence of the EM emanations from the leakage in the sensor due to fewer butterfly repetitions. Also, the increased laser power necessary for the shorter exposure time increases noise in the measurement, which can decrease the correlation results. However, further adjustment of the laser power could improve the results. In NV-based quantum sensing, for a given microwave power, there is an optimum laser pump intensity or vice versa [Zha+21; Dré+11]. For the lower laser power, i.e., the case with lower exposure time of 1 ms, we are presumably closer to this optimum regarding sensitivity and contrast than in the case with stronger laser power. Therefore, a systematic laser power optimization may result in an even higher SNR of the signal.

We have shown that detection of leakage is possible with the spectrometer, even though the time resolution does not match existing solutions. The time resolution given by the exposure time only determines the granularity at which signals can be temporally resolved, but not which signals can be detected. As the frequency spectrum is recorded through direct interaction with the NV centers, the QS spectrometer records and integrates EM signals shorter than the exposure time. This enables the use of QS for SCA. Our proof-of-concept experiment for detection of data-dependent leakage identified HW leakage of four different NTT intermediate values, which were all processed in the same exposure frame. Due to the detectability of events shorter than the exposure time, leakage from these four intermediates could be measured. Furthermore, we found that leakage from these intermediates could also be differentiated, even though they were captured in the same camera frame. We assume that leakage of these four intermediates in the time domain created a unique EM pattern. This pattern is translated without loss into the frequency domain, which makes the leakage differentiable in the frequency domain. Still, future improvements of the temporal resolution are vital to make leakage detection more practical. A straightforward strategy to improve temporal resolution is to increase the density of NV centers in the diamond. The resulting higher photon count at constant laser power would enable shorter camera exposure times and thus higher frame rates.

6.2 Potential for SCA

Real-Time Bandwidth. The presented QS spectrometer has a real-time bandwidth of 1.1 GHz. The center frequency of the setup can be changed seamlessly up to frequencies of a few GHz. This work does not focus on ultrabroadband, multi-GHz real-time bandwidths or center frequencies beyond 20 GHz. We aim to demonstrate a first proof-of-principle for NV-based SCA. Publications with different NV-based spectrometers show that these metrics are indeed achievable [Mag+22]. As our results demonstrate, leakage occurs not only around the clock frequency but also, and especially, in higher harmonics. For analysis of GHz targets, the higher harmonics can easily span across a double-digit GHz frequency range, posing immense requirements to classic spectrum analyzers. A range-optimized NV-based spectrum analyzer is considered to be a strong and viable solution to this problem. The NV-based spectrum analyzer is also promising for SCA of screaming side-channels, where leakage from digital parts of an IC is modulated and radiated by the carrier frequency of an RF module located on the die [Gui+24].

Improvements of the real-time bandwidth can be achieved through an optimized

magnetic arrangement of permanent magnets aimed for strong bias field gradients. The viability and potential of tailored magnet arrays have been shown in different NV-based applications in [Wic+21; Kar20; Chi+15b]

Independence of Time- and Frequency-Resolution. Time-resolved frequency spectra are often used in SCA in pre-processing or attacks [Yan+19; Lon+15; Deb+12; MG10]. Traditionally, spectra are calculated with the STFT (see Section 3.2). In classical STFT computation, the uncertainty principle states that the product of time and frequency resolution is a constant, which implies that the spectrum can either have a high frequency resolution or a high time resolution, but not both [Hof05]. The NV-based spectrometer records the frequency spectrum through many independent channels by direct interaction of the signal with NV centers resonant at different frequencies and therefore time and frequency resolution are largely independent of each other. As discussed in Section 2.2, the spectrometer can achieve a high temporal resolution as well as a high frequency resolution at the same time.

Benefits of Direct Spectrum Acquisition. As the spectrometer captures spectra through direct interaction with the NV centers, there is no need to compute a FFT on a digitized signal or perform frequency sweeps. Being a camera-based measurement technique, spectra are acquired in real-time at the camera frame rate. With our automated setup, we achieved to capture NTT spectra at a rate of 237 spectra/s. As the spectra are directly acquired, the data-size is small, with one camera frame per measurement.

6.3 Potential of QS for Localized EM-SCA

While in this work we looked at NV-based spectrum analysis for SCA, we now briefly look at future potential for QS in localized EM-SCA. As ICs become increasingly complex with shrinking feature sizes — pushing towards 3 nm and below — the need for new analysis techniques grows. The field of NV-based QS is rapidly advancing and has shown promising applications. To date, the first applications of NV-based QS in the analysis of ICs have already been demonstrated. Static magnetic field measurements in spatially-resolved wide-field magnetometers have shown promising applications in localization of current paths, trojan detection, or failure analysis [Bis+25; Gar+24; Len+24; Ash+22; Keh+22; Oli+21; Tur+20]. Wide-field magnetometers, with their large field of view and high spatial resolution, could eliminate time-consuming xy-scans in localized EM-SCA, reducing the time-to-result. In the literature, wide-field measurements on ICs have already demonstrated fields of view of up to around 3.7 mm × 3.7 mm [Tur+20]. In the context of ICs, NV-based QS has only been presented for the detection of (quasi-)static magnetic fields or temperature, but not for the dynamic EM near-field. To bridge this gap, future research should focus on testing protocols for the detection of the dynamic EM near-field, such as the Hahn-Echo protocol [LYL20; Miz+20], specifically targeting ICs that are relevant for SCA in wide-field magnetometers.

7 Conclusion

In this work, the first proof-of-principle for the application of quantum sensing for EM-SCA is demonstrated. Using an NV-diamond-based spectrometer, we were able to capture and analyze the frequency-time content of an EM side channel. We presented time-frequency analysis of an RSA decryption and furthermore, showed successful leakage detection of a software implementation of the NTT, which is a relevant building block of PQC algorithms. Advancing and optimizing the real-time bandwidth of our quantum sensor further, we consider a double-digit GHz real-time bandwidth achievable. This opens the way to

analyze the clock and its higher harmonics of GHz targets, which then would fully draw the potential of this quantum technology and potentially overcome bottlenecks of classical detection schemes.

8 Acknowledgement

This research was supported by the Agentur für Innovation in der Cybersicherheit GmbH in the program Side-Channel Attacks with Quantum Sensing (SCA-QS) and the Bavarian Ministry of Economic Affairs, Regional Development and Energy in the context of the project Trusted Electronics Bavaria (TrEB).

References

[Agr+03] Dakshi Agrawal et al. "The EM Side—Channel(s)". In: *Cryptographic Hardware and Embedded Systems - CHES 2002*. Ed. by Gerhard Goos et al. Vol. 2523. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 29–45. DOI: 10.1007/3-540-36400-5_4.

[AS18] Eisuke Abe and Kento Sasaki. "Tutorial: Magnetic Resonance with Nitrogen-Vacancy Centers in Diamond—Microwave Engineering, Materials Science, and Magnetometry". In: *Journal of Applied Physics* 123.16 (Apr. 2018), p. 161101. DOI: 10.1063/1.5011231.

[Ash+22] Maitreyi Ashok et al. "Hardware Trojan Detection Using Unsupervised Deep Learning on Quantum Diamond Microscope Magnetic Field Images". In: *ACM Journal on Emerging Technologies in Computing Systems* 18.4 (Oct. 2022), pp. 1–25. DOI: 10.1145/3531010.

[Bal+08] Gopalakrishnan Balasubramanian et al. "Nanoscale Imaging Magnetometry with Diamond Spins under Ambient Conditions". In: *Nature* 455.7213 (Oct. 2008), pp. 648–651. DOI: 10.1038/nature07278.

[Bar+20] John F. Barry et al. "Sensitivity Optimization for NV-diamond Magnetometry". In: *Reviews of Modern Physics* 92.1, 015004 (Mar. 2020). DOI: 10.1103/RevModPhys.92.015004.

[Bar+24] John F. Barry et al. "Sensitive Ac and Dc Magnetometry with Nitrogen-Vacancy-Center Ensembles in Diamond". In: *Physical Review Applied* 22.4 (Oct. 2024), p. 044069. DOI: 10.1103/PhysRevApplied.22.044069.

[Bel+14] Pierre Belgarric et al. "Time-Frequency Analysis for Second-Order Attacks". In: *Smart Card Research and Advanced Applications*. Ed. by Aurélien Francillon and Pankaj Rohatgi. Vol. 8419. Cham: Springer International Publishing, 2014, pp. 108–122. DOI: 10.1007/978-3-319-08302-5_8.

[Bis+25] Bartu Bisgin et al. *Quantum Diamond Microscopy for Non-Destructive Failure Analysis of an Integrated Fan-Out Package-on-Package iPhone Chip*. 2025. DOI: 10.48550/ARXIV.2512.07619.

[Bos+18] Joppe Bos et al. "CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM". In: *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. London: IEEE, Apr. 2018, pp. 353–367. DOI: 10.1109/EuroSP.2018.00032.

[Chi+15a] M. Chipaux et al. "Wide Bandwidth Instantaneous Radio Frequency Spectrum Analyzer Based on Nitrogen Vacancy Centers in Diamond". In: *Applied Physics Letters* 107.23 (Dec. 2015), p. 233502. DOI: 10.1063/1.4936758.

[Chi+15b] Mayeul Chipaux et al. “Magnetic Imaging with an Ensemble of Nitrogen-Vacancy Centers in Diamond”. In: *The European Physical Journal D* 69.1, 166 (July 2015). DOI: 10.1140/epjd/e2015-60080-1.

[Cho+18] Sunuk Choe et al. “Precise Temperature Sensing with Nanoscale Thermal Sensors Based on Diamond NV Centers”. In: *Current Applied Physics* 18.9 (Sept. 2018), pp. 1066–1070. DOI: 10.1016/j.cap.2018.06.002.

[De +11] G. De Lange et al. “Single-Spin Magnetometry with Multipulse Sensing Sequences”. In: *Physical Review Letters* 106.8 (Feb. 2011), p. 080802. DOI: 10.1103/PhysRevLett.106.080802.

[Deb+12] Nicolas Debande et al. *Wavelet Transform Based Pre-Processing for Side Channel Analysis*. Dec. 2012, p. 38. DOI: 10.1109/MICROW.2012.15.

[DRC17] C. L. Degen, F. Reinhard, and P. Cappellaro. “Quantum Sensing”. In: *Reviews of Modern Physics* 89.3, 035002 (July 2017). DOI: 10.1103/RevModPhys.89.035002.

[Dré+11] A. Dréau et al. “Avoiding Power Broadening in Optically Detected Magnetic Resonance of Single NV Defects for Enhanced Dc Magnetic Field Sensitivity”. In: *Physical Review B* 84.19 (Nov. 2011), p. 195204. DOI: 10.1103/PhysRevB.84.195204.

[DS15] François Durvaux and François-Xavier Standaert. *From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces*. 2015. DOI: 10.1007/978-3-662-49890-3_10.

[Gar+24] Marwa Garsi et al. *Three-Dimensional Imaging of Integrated-Circuit Activity Using Quantum Defects in Diamond*. June 2024. arXiv: 2112.12242.

[GHT05] Catherine H. Gebotys, Simon Ho, and C. C. Tiu. “EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA”. In: *Cryptographic Hardware and Embedded Systems – CHES 2005*. Ed. by Josyula R. Rao and Berk Sunar. Berlin, Heidelberg: Springer, 2005, pp. 250–264. DOI: 10.1007/11545262_19.

[Goo+11] Gilbert Goodwill et al. “A Testing Methodology for Side Channel Resistance Validation”. In: *Nist Non-Invasive Attack Testing Workshop* (2011).

[Gra+23] S.M. Graham et al. “Fiber-Coupled Diamond Magnetometry with an Unshielded Sensitivity of 30 pT / Hz”. In: *Physical Review Applied* 19.4 (Apr. 2023), p. 044042. DOI: 10.1103/PhysRevApplied.19.044042.

[Gui+24] Jeremy Guillaume et al. “Attacking at Non-harmonic Frequencies in Screaming-Channel Attacks”. In: *Smart Card Research and Advanced Applications*. Ed. by Shivam Bhasin and Thomas Roche. Cham: Springer Nature Switzerland, 2024, pp. 87–106. DOI: 10.1007/978-3-031-54409-5_5.

[Haa+25] Paul Haas et al. “Towards Fieldable NVC Quantum Sensors for Defense Applications”. In: *Quantum Technologies for Defence and Security II*. Ed. by Veronica Fernandez, Giacomo Sorelli, and Sylvain Schwartz. Madrid, Spain: SPIE, Oct. 2025, p. 28. DOI: 10.1117/12.3077119.

[Hel+24] G. Puebla Hellmann et al. “Scanning NV Microscopy - Tracing Currents at the Nanometer Scale”. In: *2024 IEEE International Reliability Physics Symposium (IRPS)*. Grapevine, TX, USA: IEEE, Apr. 2024, pp. 1–6. DOI: 10.1109/IRPS48228.2024.10529403.

[Her+23] Julius Hermelink et al. “Adapting Belief Propagation to Counter Shuffling of NTTs”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2023.1 (2023), pp. 60–88. DOI: 10.46586/TCHES.V2023.I1.60-88.

[Hof05] Rüdiger Hoffmann. *Grundlagen der Frequenzanalyse: eine Einführung für Ingenieure und Informatiker ; mit 11 Tabellen*. 2., durchges. Aufl. Kontakt & Studium 620. Renningen-Malmsheim: expert-Verl, 2005.

[ISU18] Vincent Immler, Robert Specht, and Florian Unterstein. "Your rails cannot hide from localized EM: how dual-rail logic fails on FPGAs - extended version". In: *J. Cryptogr. Eng.* 8.2 (2018), pp. 125–139. DOI: 10.1007/S13389-018-0185-X.

[Jia+18] Wenfei Jia et al. "Ultra-Broadband Coplanar Waveguide for Optically Detected Magnetic Resonance of Nitrogen-Vacancy Centers in Diamond". In: *Review of Scientific Instruments* 89.6 (June 2018), p. 064705. DOI: 10.1063/1.5028335.

[Kar20] David Karcher. "Quantal-Sensory Frequency-Time-Analysis of HF-Signals by Means of NV-Centers in Diamonds". MA thesis. Karlsruhe: Karlsruhe Institute of Technology (KIT), 2020.

[Keh+22] P. Kehayias et al. "Measurement and Simulation of the Magnetic Fields from a 555 Timer Integrated Circuit Using a Quantum Diamond Microscope and Finite-Element Analysis". In: *Physical Review Applied* 17.1 (Jan. 2022), p. 014021. DOI: 10.1103/PhysRevApplied.17.014021.

[Len+24] Jacob N. Lenz et al. *Hardware Trojan Detection Potential and Limits with the Quantum Diamond Microscope*. Feb. 2024. arXiv: 2402.08004.

[Lev+19] Edlyn V. Levine et al. "Principles and Techniques of the Quantum Diamond Microscope". In: *Nanophotonics* 8.11 (Nov. 2019), pp. 1945–1973. DOI: 10.1515/nanoph-2019-0209.

[LHM10] Abdelghani Laraoui, Jonathan S. Hodges, and Carlos A. Meriles. "Magnetometry of Random Ac Magnetic Fields Using a Single Nitrogen-Vacancy Center". In: *Applied Physics Letters* 97.14 (Oct. 2010), p. 143104. DOI: 10.1063/1.3497004.

[Lon+15] J. Longo et al. "SoC It to EM: ElectroMagnetic Side-Channel Attacks on a Complex System-on-Chip". In: *Cryptographic Hardware and Embedded Systems – CHES 2015*. Ed. by Tim Güneysu and Helena Handschuh. Berlin, Heidelberg: Springer, 2015, pp. 620–640. DOI: 10.1007/978-3-662-48324-4_31.

[LYL20] Myeongwon Lee, Jungbae Yoon, and Donghun Lee. "Atomic Scale Magnetic Sensing and Imaging Based on Diamond NV Centers". In: *Magnetometers - Fundamentals and Applications of Magnetism*. Ed. by Sergio Curilef. London: IntechOpen, Oct. 2020. DOI: 10.5772/intechopen.84204.

[Mag+22] Simone Magaletti et al. "A Quantum Radio Frequency Signal Analyzer Based on Nitrogen Vacancy Centers in Diamond". In: *Communications Engineering* 1.1 (July 2022), p. 19. DOI: 10.1038/s44172-022-00017-4.

[Mag+24] Simone Magaletti et al. "Magnetic Sensitivity Enhancement via Polarimetric Excitation and Detection of an Ensemble of NV Centers". In: *Scientific Reports* 14.1 (May 2024), p. 11793. DOI: 10.1038/s41598-024-60199-z.

[Maz+08] J. R. Maze et al. "Nanoscale Magnetic Sensing with an Individual Electronic Spin in Diamond". In: *Nature* 455.7213 (Oct. 2008), pp. 644–647. DOI: 10.1038/nature07279.

[MG10] Edgar Mateos and Catherine H. Gebotys. "A New Correlation Frequency Analysis of the Side Channel". In: *Proceedings of the 5th Workshop on Embedded Systems Security*. Scottsdale Arizona: ACM, Oct. 2010, pp. 1–8. DOI: 10.1145/1873548.1873552.

[Miz+20] Kosuke Mizuno et al. “Simultaneous Wide-Field Imaging of Phase and Magnitude of AC Magnetic Signal Using Diamond Quantum Magnetometry”. In: *Scientific Reports* 10.1 (July 2020), p. 11611. DOI: 10.1038/s41598-020-68404-5.

[MOP07] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Advances in Information Security 31. New York: Springer, 2007.

[Nat24a] National Institute of Standards and Technology (US). *Module-Lattice-Based Digital Signature Standard*. Tech. rep. NIST FIPS 204. Washington, D.C.: National Institute of Standards and Technology (U.S.), Aug. 2024, NIST FIPS 204. DOI: 10.6028/NIST.FIPS.204.

[Nat24b] National Institute of Standards and Technology (US). *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. Tech. rep. NIST FIPS 203. Washington, D.C.: National Institute of Standards and Technology (U.S.), Aug. 2024, NIST FIPS 203. DOI: 10.6028/NIST.FIPS.203.

[Oli+21] Sean M. Oliver et al. “Vector Magnetic Current Imaging of an 8 Nm Process Node Chip and 3D Current Distributions Using the Quantum Diamond Microscope”. In: *ISTFA 2021*. Phoenix, Arizona, USA, Oct. 2021, pp. 96–107. DOI: 10.31399/asm.cp.istfa2021p0096.

[Pha+11] L M Pham et al. “Magnetic Field Imaging with Nitrogen-Vacancy Ensembles”. In: *New Journal of Physics* 13.4 (Apr. 2011), p. 045021. DOI: 10.1088/1367-2630/13/4/045021.

[PP19] Peter Pessl and Robert Primas. *More Practical Single-Trace Attacks on the Number Theoretic Transform*. 2019.

[PPM17] Robert Primas, Peter Pessl, and Stefan Mangard. *Single-Trace Side-Channel Attacks on Masked Lattice-Based Encryption*. 2017.

[pq-20] pq-crystal. *Pq-Crystals/Kyber*. https://github.com/pq-crystals/kyber/blob/main/ref/ntt.c. GitHub Repository. Nov. 2020.

[SA08] François-Xavier Standaert and Cédric Archambeau. “Using Subspace-Based Template Attacks to Compare and Combine Power and Electromagnetic Information Leakages”. In: *Cryptographic Hardware and Embedded Systems - CHES 2008, 10th International Workshop, Washington, D.C., USA, August 10-13, 2008. Proceedings*. Ed. by Elisabeth Oswald and Pankaj Rohatgi. Lecture Notes in Computer Science. Springer, 2008, pp. 411–425. DOI: 10.1007/978-3-540-85053-3_26.

[Sch+14] Romana Schirhagl et al. “Nitrogen-Vacancy Centers in Diamond: Nanoscale Sensors for Physics and Biology”. In: *Annual Review of Physical Chemistry* 65.1 (Apr. 2014), pp. 83–105. DOI: 10.1146/annurev-physchem-040513-103659.

[Sch+25] Florian Schall et al. *Laser-Enhanced Quantum Sensing Boosts Sensitivity and Dynamic Range*. 2025. DOI: 10.48550/ARXIV.2509.05204.

[Sek+24] N. Sekiguchi et al. “Diamond Quantum Magnetometer with Dc Sensitivity of Sub-10 pT Hz - 1 / 2 toward Measurement of Biomagnetic Field”. In: *Physical Review Applied* 21.6 (June 2024), p. 064010. DOI: 10.1103/PhysRevApplied.21.064010.

[Sen+22] S. Sengottuvel et al. “Wide-Field Magnetometry Using Nitrogen-Vacancy Color Centers with Randomly Oriented Micro-Diamonds”. In: *Scientific Reports* 12.1, 17997 (Oct. 2022). DOI: 10.1038/s41598-022-22610-5.

[Sie24] Patrick Siegwolf. “Exploring Two-Dimensional Magnetism by Scanning Nitrogen-Vacancy Magnetometry”. In: (2024). DOI: 10.5451/UNIBAS-EP96548.

[Ste+10] S. Steinert et al. “High Sensitivity Magnetic Imaging Using an Array of Spins in Diamond”. In: *Review of Scientific Instruments* 81.4, 043705 (Apr. 2010). DOI: 10.1063/1.3385689.

[Str+23] Emanuele Strieder et al. “ASCA vs. SASCA - A Closer Look at the AES Key Schedule”. In: *Constructive Side-Channel Analysis and Secure Design - 14th International Workshop, COSADE 2023, Munich, Germany, April 3-4, 2023, Proceedings*. Ed. by Elif Bilge Kavun and Michael Pehl. Vol. 13979. Lecture Notes in Computer Science. Springer, 2023, pp. 65–85. DOI: 10.1007/978-3-031-29497-6_4.

[Tur+20] Matthew J. Turner et al. “Magnetic Field Fingerprinting of Integrated Circuit Activity with a Quantum Diamond Microscope”. In: *Physical Review Applied* 14.1 (July 2020), p. 014097. DOI: 10.1103/PhysRevApplied.14.014097. arXiv: 2004.03707.

[Unt+18] Florian Unterstein et al. “High-Resolution EM Attacks Against Leakage-Resilient PRFs Explained - And an Improved Construction”. In: *Topics in Cryptology - CT-RSA 2018 - The Cryptographers’ Track at the RSA Conference 2018, San Francisco, CA, USA, April 16-20, 2018, Proceedings*. Ed. by Nigel P. Smart. Lecture Notes in Computer Science. Springer, 2018, pp. 413–434. DOI: 10.1007/978-3-319-76953-0_22.

[Wan+15] Junfeng Wang et al. “High-Sensitivity Temperature Sensing Using an Implanted Single Nitrogen-Vacancy Center Array in Diamond”. In: *Physical Review B* 91.15 (Apr. 2015), p. 155404. DOI: 10.1103/PhysRevB.91.155404.

[Wic+21] Arne Wickenbrock et al. “High Homogeneity Permanent Magnet for Diamond Magnetometry”. In: *Journal of Magnetic Resonance* 322 (Jan. 2021), p. 106867. DOI: 10.1016/j.jmr.2020.106867.

[Yan+19] Guang Yang et al. “Convolutional Neural Network Based Side-Channel Attacks in Time-Frequency Representations”. In: *Smart Card Research and Advanced Applications*. Ed. by Begül Bilgin and Jean-Bernard Fischer. Cham: Springer International Publishing, 2019, pp. 1–17. DOI: 10.1007/978-3-030-15462-2_1.

[Zha+21] Chen Zhang et al. “Diamond Magnetometry and Gradiometry Towards Subpicotesla Dc Field Measurement”. In: *Physical Review Applied* 15.6 (June 2021), p. 064075. DOI: 10.1103/PhysRevApplied.15.064075.

[Zho+25] Feifei Zhou et al. “Imaging Frequency-Modulated Microwaves Using a Robust Quantum Spectrum Analyzer”. In: *ACS Photonics* 12.12 (Dec. 2025), pp. 7030–7037. DOI: 10.1021/acsphotonics.5c02451.