Finding the AES Bits in the Haystack: Reverse Engineering and SCA Using Voltage Contrast

Christian Kison[1,2], Jürgen Frinken[2] and Christof Paar[1]

[1] Horst Görtz Institute for IT Security, Ruhr University Bochum, Germany
[2] Bundeskriminalamt, Kriminaltechnisches Institut, Germany

Abstract. In this paper, we demonstrate how the Scanning Electron Microscope (SEM) becomes a powerful tool for Side Channel Analysis (SCA) and Hardware Reverse Engineering. We locate the AES hardware circuit of a XMEGA microprocessor with Capacitive-Coupled Voltage Contrast (CCVC) images and use them in a powerful Voltage Contrast Side Channel Analysis (VCSCA). This enables an attacker to locate AES bit-wires in the top metal-layer and thus, to recover valuable netlist information. An attacker gets a valuable entry-point to look for weaknesses or Intellectual Property (IP) in the AES circuit. Additionally we show the great potential of the VCSCA in a non-invasive Side Channel Analysis for Reverse Engineering (SCARE) approach. Finally, we recover the full key of the AES hardware-engine in a practical template-based VCSCA and a no-plaintext, no-ciphertext and no-key Simple Side Channel Analysis (SSCA). We show that future VCSCA attacks present a big hardware security-risk that IC vendors need to consider.

Keywords: side channel analysis, SCA, hw reverse engineering, voltage contrast, AES, full key recovery, SCARE

1 Introduction

A crucial part in hardware reverse engineering is to know the location of their Region of Interest (ROI) prior to their delayering process. Without this knowledge, the literal search for the needle in the haystack can become a major obstacle for the reverser. ROIs are usually security-sensitive elements, e.g., fuse bytes, cryptographic algorithms or proprietary parts of an Integrated Circuit (IC) [14, 24]. We may have luck if vendors "mark" sensitive areas with a shield or we already know the basic structure from a similar IC within the same vendor family. However, this is an exception especially in today's multi-million gate ICs. Identifying crucial elements is often extremely difficult.

The classical approach is a stepwise delayering down to the silicon substrate while taking images from each layer. After assembling and overlaying the different layers, a hardware reverse engineer can begin to interpret the logical cells to find his ROI. Even with semi-automated tools that help to recognize standard cells of a library and wirings, we need to attend and review the process

of millions of gates to get a flawless netlist from the chip structure: There is not feedback mechanism that alerts of the reverser about mistakes and even the slightest mistake in the image acquisition might lead to faulty connections and a complete different circuit behavior. To make things worse, it is difficult to completely planarize the die with low to medium prized equipment, resulting in bad layer images and therefore worse recognition rates with the current chip-area-to-layer-thickness ratio.

Pinpointing the delayering process to a ROI reduces the costs and processing time when the user can focus on keeping the structure of the ROI still recognizable, neglecting the rest of the chip. Another reason is to achieve better signal-to-noise-ratio with located EM-traces or make other (fault-)attacks possible [18, 19]. Sometimes this might even enable more advanced analysis like inter-gate side channel leakages as discussed in [27].

2 Related Work

In order to find the hot spot or ROI, multiple more practical approaches emerged, often in combination with a Side Channel (SC). The EM near-field cartography, thermal analysis and optical photon emission are the three most noteworthy examples [3, 9, 12, 16, 18, 19, 23]. All techniques are semi-invasive attacks [25]. They depackage the IC to strengthen existing side channels like EM emanation (to make pinpointed small loop measurements possible) and to gain access to additional SCs like photon emission and heat distribution. The mentioned semi-invasive techniques are possible from the top- and backside of the chip, whereby the backside approach usually needs additional equipment for milling and thinning the silicon bulk [12].

To be precise enough for locating the smallest activity areas, spatial located EM emanation cartography takes several hours. It finds multiple high Signal-To-Noise-Ratio (SNR) spots along the power distribution, as the radiation is directly related to the power consumption. Furthermore EM emanation often results in better SNR from the frontside, as the probe can be moved closer to the emanation source [16,18,19]. Nevertheless this approach allows to find a ROI within μm range. Thus, we can can skip most parts of the chip and concentrate on the ROI. The drawback for EM near-field cartography is the long measurement time to scan the whole die surface and may show multiple hot spots.

In the case of the photon emission, the price of the equipment maps directly onto the measuring time and quality: An IR-range sensitive camera with good Quantum Efficiency (QE) and low dark-current costs several 10k€. Transistors have a probability to emit a photon during a state transition which passes through the thinned silicon backside. A first mandatory preparation is the thinning of the silicon bulk on the backside. The basic idea is to capture the emitted photons and visualize them in a highly spatial resolute setup. This becomes a major obstacle for modern CMOS processes, due to the diffraction limit of IR light. Additional preparation steps after the thinning, like a Numerical Aperture

Increasing Lens (NAIL), might become necessary [28]. This extends the preparation time and bears the risk of breaking the chip. After a camera-dependent image integration time, we can find the activity of individual transistors during the loop execution of one code fragment [23]. By increasing the supply voltage during the interesting clock cycles, the authors enhance the IR photon emission probability to highlight corresponding areas. Using this technique the authors of [22] successfully extracted an AES key by observing the memory access pattern of the `subbytes` routine. Meanwhile [12] pinpoints a Picosecond Imaging Circuit Analysis (PICA) attack on single transistors to find `xor` values. Finding the respective hot spots and transistors is done with an optical long time image integration like in [22, 23]. Once a ROI has been determined, PICA can be used to see transistor switches in high-frequency ICs.

Surface Liquid Crystal (LC) is a wide spread analysis method based on the thermal radiation for failure analysis in the industry. It is well established and can be exploited for ROI localisation from the attacker's point of view. LCs allow spatial resolutions of 4 μm and better [3]. For modern CMOS processes this approach has equal spatial limitations, due to the IR light diffraction limit. Therefore new approaches like the Fluorescent Microthermal Imaging (FMI) emerged which try to fluoresce light with shorter wavelength [3]. Furthermore did the authors of [11] try to extend the thermal hot spot detection to the IC backside. Depending on the camera, are thermal and photon emission failure analysis methods qualified to find the ROIs. Both approaches are usually done over multiple program executions to heat-up or gather enough emitted photons in a normal working chip. These failure analysis methods face big challenges and difficulties with the upcoming CMOS sizes and decreasing power supply voltages. The modern CMOS size is below the diffraction limit of IR light and the decreasing power supply voltage drops the probability of photons being emitted and reduce the produced heat due to smaller currents.

This paper uses the Scanning Electron Microscope (SEM) as advanced inspection tool. Access to a suitable SEM should not be problematic as bigger institutes and universities with mid-class laboratories usually own one, due to their distribution in many academic fields. Companies and private persons can find second hand SEMs for under 10k€ or rent it on a hourly basis. A well-funded hardware reverse engineer usually has access to a SEM for taking layer images. Once the setup is built and the Device Under Test (DUT) is vulnerable to our approach, we are able identify the ROI faster as the EM cartography and have less sample preparation compared to the photon emission analysis. Furthermore do we not need to run the chip multiple times and have better spatial resolution than thermal analysis methods.
Our contribution in this paper is the following:

1. We demonstrate an approach to pinpoint the AES location of the XMEGA microprocessor with Voltage Contrast (VC) analysis comparable to related work.
2. We exploit the VC as a SC and perform a full key-recovery in a template-attack and a Simple Side Channel Analysis (SSCA).
3. Using the VC images reveals additional information of the AES circuit useful for a reverse engineer. Furthermore are we showing the potential of VC SC in a Side Channel Analysis for Reverse Engineering (SCARE) approach to find additional circuit netlist information.
4. The results show a possibility to counter hardware-obfuscation and hardware protection and to verify parts of an extracted netlist.

The rest of this paper is structured as follows: Section 3 describes the different Voltage Contrast (VC) analysis methods and their physical understanding. Section 4 locates the AES circuit with the common Dynamic Voltage Contrast (DVC) analysis. Section 5 is the main contribution that gives a Proof-of-Concept (PoC) for the Voltage Contrast Side Channel Attack (VCSCA). The DUT is a widespread Atmel XMEGA microcontroller. We show a template-attack and a Simple Side Channel Analysis (SSCA) approach to recover the full AES key. Section 6 concludes this work.

3 Voltage Contrast

The SEM has become a powerful diagnostic tool during the last 60 years, used in many applications for IC inspection and failure analysis. When an electron beam-gun fires (primary) electrons on a scanning surface, secondary electrons are hit out of a solid specimen. These emitted secondary electrons have usually low energy (0 - 50 eV), which makes them easily detectable by using a positive electrical-field metal-plate as a detector. Out of the SEM images are the secondary electron images the most widely used, due to their ease of production and similarity to light microscope with improved depth of field [6].

During VC failure analysis, the natural negative charge of the electrons is used to view different voltage potentials, with the help of their electrical field and their direct influence to secondary electrons. Note that VC also works with positive ions in a Focused Ion Beam (FIB), since only the difference in charge is important. Using VC with positive ions from a FIB achieves better results[3] and the voltage interpretation of brightness and darkness is reversed compared to the SEM VC [5–7]. VC analysis needs the chip to be depackaged to gain access to the die surface.

VC analysis can be classified into two categories, which are on the one hand the static VC methods, including Passive Voltage Contrast (PVC) and Active Voltage Contrast (AVC) and on the other hand the Dynamic Voltage Contrast (DVC).

[3] With individually optimized parameters

3.1 Static Voltage Contrast

The static VC is performed on chips with removed passivation layer or even partly delayered chips. Static VC is split in the two sub-techniques PVC and AVC. The PVC does not connect the DUT to any signals or voltages and thereby shows the charging up of floating gates and capacitances. It is often used to find shorts and imperfectly connected wires and structures during chip manufacturing. The DUT does not have to be functional anymore, allowing to take VC images of intermediate layers. Note that is possible to create floating structures by removing metal layers or by wire cutting with a FIB [17]. To pinpoint shorts and badly connected wires, the structures are split and analyzed separately by applying a voltage in the AVC.

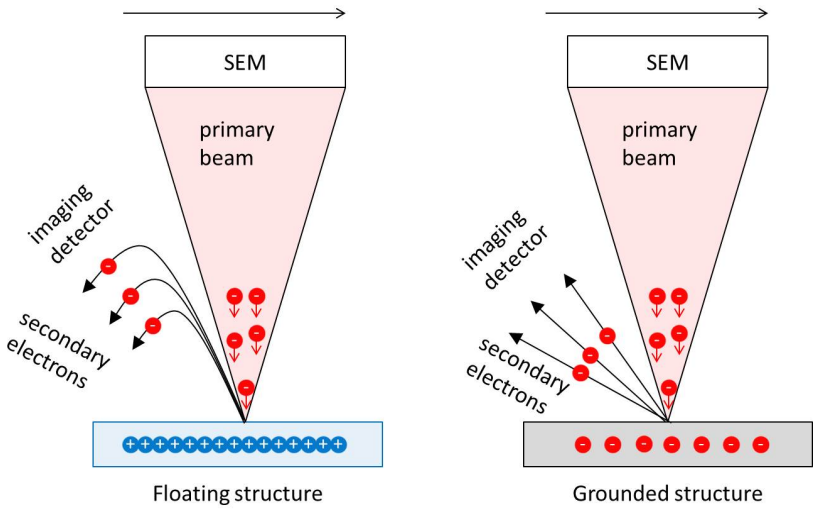


Fig. 1. Passive Voltage Contrast

Figure 1 shows the PVC. Isolated structures are charging up, due to second electrons being hit out of the structure. In the immediate consequence the majority of produced secondary electrons are prevented to reach the detector by the inverted electrical field. These structures appear dark in the image. Grounded structures do not appear bright, because of the high yield [17].

AVC differs from PVC as it applies voltages in some structures to force them look dark or bright in flawless structures. Is the outcome not as expected, a short or open connection can be assumed. Knowing the detailed place-and-route of the netlist and structures is very helpful, but not mandatory. The authors of [26] use the PVC to detect stealthy dopant-level circuits (trojans).

3.2 Dynamic Voltage Contrast

DVC is performed during dynamic rather than static operation of the DUT. In the scope of an IC or microcontroller (uC), the device is running normally, while performing the voltage contrast. If the device is still under a the passivation layer, Capacitive Coupled Voltage Contrast (CCVC) can be applied. CCVC exploits the property that the voltage potentials of the top metal-wires are electrically coupled with the covering dielectric passivation of the die, forming a capacitor. Therefore, CCVC is performed while the passivation layer is still covering the die and the chip is still operational, or at least voltages can be applied to top wires and structures.

When a line or wire buried under the passivation is assumed to have the voltage U_p, an voltage U_S is generated through capacitive effects. This effect can be described as a transfer function U_S/U_p, which depends on the electrical (U_E) and geometrical (d_e, d_p, W) parameters. U_E and d_E are the extraction grid potential and distance, while d_p and W represent the buried line depth and width, repectively [2]:

$$\frac{U_S}{U_p} = f(U_E, d_E, d_p, W) \tag{1}$$

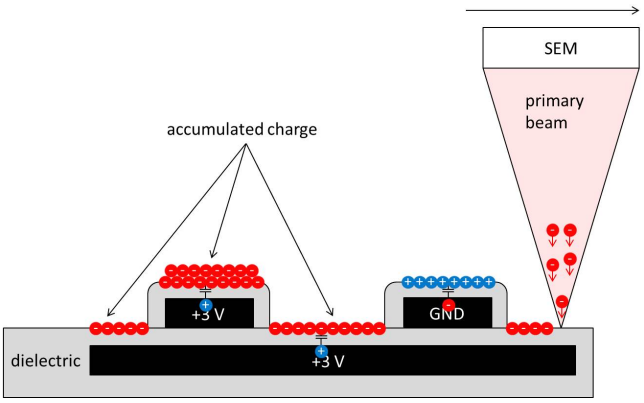
The CCVC phenomena is made visible with a SEM through dynamic changes. Therefore the CCVC is separated in two phases shown in Figure 2.

The first phase charges up the ICs surface with the electron-beam with location-depending accumulated charges (due to U_S), coupled to the underlaying electrical potentials (U_p). In the second phase, the accumulated electrons are hit out as secondary electrons. Compared to the normal structures, are these more detected electrons, brightening the structure. The electrical potential of the top layers can be data-dependent. Please not that this is not always the case as modern CMOS processes route the VCC or GND signal through the top metal layer. The data dependency leaks further information in a SC that are meant to be kept secret. This has already been seen as a theoretical threat in [8]. We show a practical attack and utilise the CCVC as a SC, not considered in the SC community so far[4].

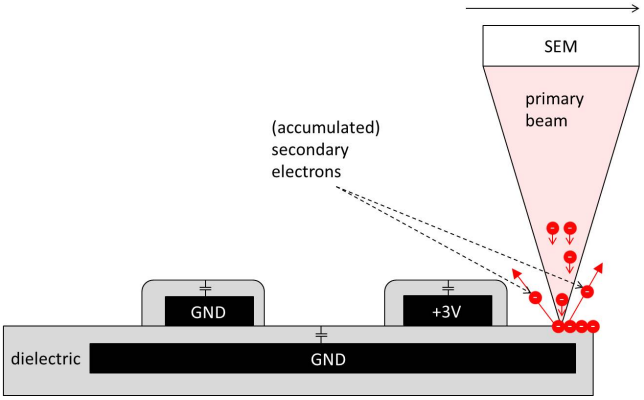
Furthermore we emphasize that the authors of [20, 21] show a possibility for backside CCVC or E-beam probing (EBP). This imposes a big threat for IC vendors and designs, if backside CCVC is scalable to big areas like the shown frontside approach. Backside CCVC has the potential to become one of the most threatening SCs, as there is almost no IC backside protections in todays IC structures. In this work we show a PoC for the frontside CCVC that can be extended to the backside in future work. Therefore we refer to frontside CCVC throughout the rest of this paper, if not stated otherwise.

Note that the DUT needs to be depackaged and we require the passivation layer, which classifies the CCVC as a common semi-invasive approach. If the

[4] To the best of our knowledge



(a) Charging phase



(b) Read-out phase

Fig. 2. Capacitive Coupled Voltage Contrast

attacker is able to remove the passivation with the DUT still operational, other DVCs are possible as well. Therefore we will stick to the term of DVC throughout this paper, rather than CCVC. Figure 2 shows the electrical properties of the CCVC, separated in charging phase in Figure (a) and read-out phase in Figure (b).

We described in Section 3.1 the possibility to distinguish between high and low voltages on the surface from the brightness in the SEM image. With carefully selected SEM parameters, we can see dynamic changes during the clock transition for a short time. By optimizing the parameters, we were even able to observe changes in the second metal layer[5], easily distinguishable as 90° rotated wires.

[5] layers from top to bottom

As the CCVC is built from two phases and especially the first phase needs some time to charge the surface, the clock speed of the DUT has to be very slow. With an external clock, this can be done in a trivial manner. In more complex scenarios, clock stretching [7], invasive mechanical probing or even EM based attacks on ring oscillators [4] could be feasible. By reducing the size of the ROI in the SEM a clock speed of some Hz to some kHz might be possible, as only this small region is charged and read-out. Other DVC techniques solve this problem by introducing a pulse gate in stroboscopic SEMs [29]. Academic publications show scans within GHz clock speed range [30], while commercial EBP products can be found with similar capabilities [20].

4 Voltage Contrast Analysis

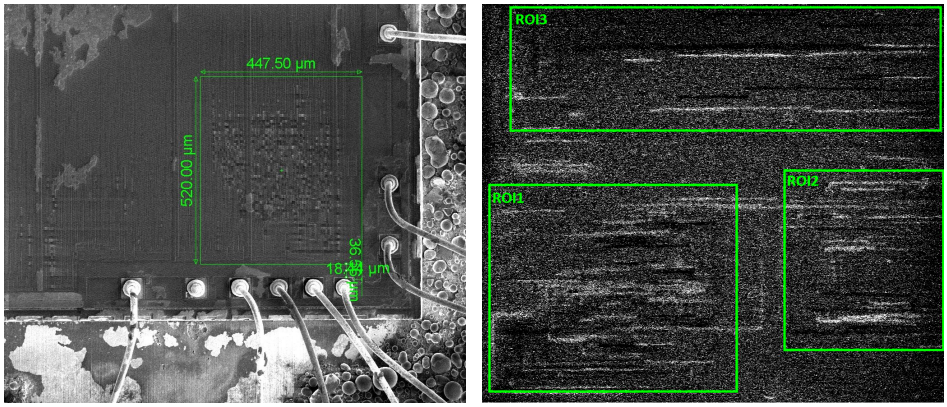
In this section we describe a DVC analysis for successfully locating the AES circuit of our DUT. The DUT is a decapsulated XMEGA32A4U, an 8-bit uC with a dedicated AES hardware unit. The AES-128 core needs 376 clock cycles to en- or decrypt blocks of 16 bytes, with the option to `xor` the result once more for different AES modes [1].

The user can read the last round key from the key register. After each block encryption, the key has to be set again. The AES hardware is driven by the peripheral clock, which can be fully controlled externally or can be set to a multiple of the internal generated CPU clock.

Locating the AES Circuit
As a first test, we tried to identify the AES circuit by looping the AES encryption with unknown data at 2 MHz, while performing a DVC in the SEM. The CPU is in sleep mode during the encryption. The electron beam accelerating voltage is set to 1 keV and the beam scanning time is set to repeat as fast as possible. We achieved best results with a Through the Lens Detector (TLD). Figure 3 shows the result of the DVC.

A high activity in the bottom right corner indicates a repetitive computation, assumed to be the AES circuit. To verify our assumption we run a normal CPU program without using the AES core and observed the ROI. As it did not show any activity during the verification run, we concluded that the ROI is indeed the AES.

As shown in Figure 3 we were already able to identify the AES circuit by simply running the algorithm and observing the top metal layer using the SEM. We note that this step is considerably simpler and faster compared to other approaches such as EM cartography, thermal imaging or photon emission discussed in Section 2. Also the EM trace acquisition is often non-trivial. Subsequently, a reverser can focus his attacks to the ROI.



(a) AES area

(b) Zoomed-in AES area with labeled regions. Image is saturated for improved visualisation.

Fig. 3. AES located with DVC

5 Voltage Contrast Side Channel Analysis (VCSCA)

This section is the main contribution of this paper. We describe a Side Channel Analysis (SCA) with the DVC explained in Section 3.2. We use the VC as a side channel and perform a SCA to retrieve additional information of the AES circuit positions. Additionally, we recover the full AES key in 2 SCAs explained in Section 5.4 and Section 5.5. However, the attack has a significant potential as a general-purpose tool for extracting data and performing hardware reverse engineering against unknown circuits. This tool has a big potential, even for modern CMOS processes, if we include backside CCVC shown in [21] and [20].

Before explaining the VCSCA in more detail, we want to point out, that we performed an optional EM-based collision-attack in advance. This additional SCA was done to synchronize the retrieved byte-order and timing information with ROI1-3 in Figure 3b. This allowed us to identify ROI1 as the `addroundkey` subroutine. During this section this information became obsolete, as the DUT is vulnerable to the more powerful introduced VCSCA. Nevertheless the combination with another SCA is a general-purpose approach to further reduce the ROI, even if the VCSCA is not applicable. We describe the setup and attack of the VCSCA in more detail during this section.

5.1 Obtaining Voltage Contrast Traces

A simple AES encryption program for the XMEGA has been written. It receives a 16 byte key and plaintext over USART and encrypts a AES-128 data block. Just before the AES is starting, the clock is set to react to an external pin and

the main CPU is configured to enter sleep-mode.

In Section 3.2 we explained that the accumulated charges from the charging-phase disappear quickly after the clock transition. Therefore we have to time a single picture very accurately. To circumvent this problem, we decided to start recording a movie using the SEM software and cover multiple clock cycles in one recording. During the VCSCA the clock has been set to 3 Hz. The SEM parameter are the same as described in Section 4. The final setup can be seen in Figure 4.

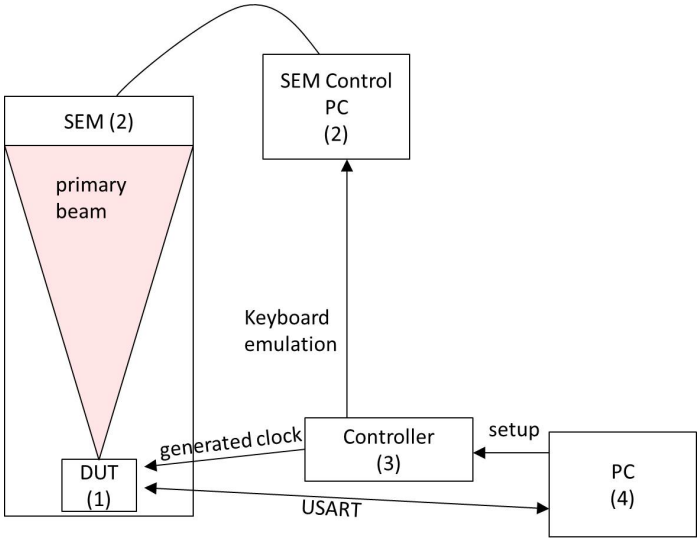
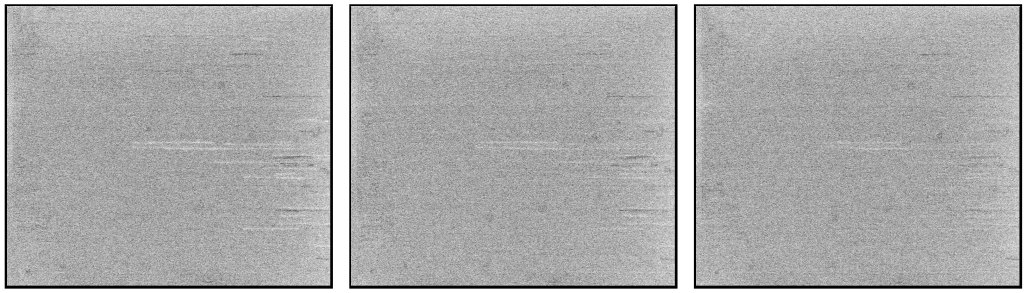
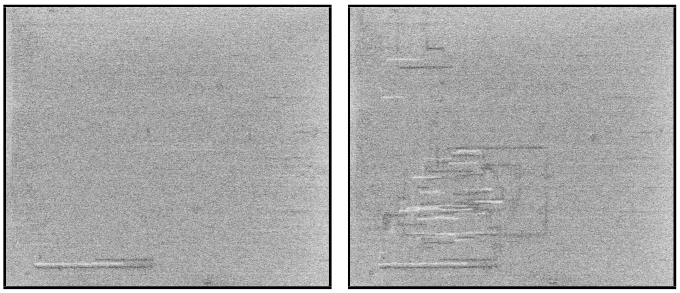


Fig. 4. The setup for the VCSCA

Figure 4 shows the setup of the VCSCA. This rather complex setup is needed as the DVC needs to be synchronized with the external clock. The dynamic changes appear only for a brief moment, which led us to start recording a movie. For synchronizing the DUT clock with the recording, an uC(3) is set up to simulate a keyboard to start the recording of videotraces within the SEM-control Software (2). The clock is set to 3 Hz as this is the optimized speed to see each DVC change on the surface, without overlapping charging effects from the clock cycle before. This can be seen in Figure 5. About every 4-5th frame in the recorded video is a "clockframe". They have visible DVC changes and minimal charges from the previous clock cycle. The PC (4) is used to generate, send and validate the plaintext, key and received ciphertext. 300 videotraces with 200 frames each were acquired for the VCSCA. Each frame has the image resolution of 1024 x 885 pixels. Plaintext and keys are chosen randomly, but are known.



(a) frame x (b) frame x+1 (c) frame x+2



(d) frame x+3 (e) frame x+4

Fig. 5. Consecutive frames within one trace. A clock transition takes place, while the SEM scans the last third of frame x+3. The previous clock effect fades out (a)-(d). The colors are inverted for improved visualisation.

5.2 Locating AES bit wires in a VCSCA

In this section we determine the Pearson correlation coefficient between all pixels and the emulated internal AES bit values. The AES is emulated in software with known key and plaintext. Therefore we know every intermediate value, but concentrate on the first AES round. The correlation is done on every pixel in every frame extracted from the (video-)traces. Overall this makes $1024 \times 885 \times 300$ values for each frame and hypothesis to calculate the Pearson correlation from.

Note that we are using the absolute bitvalue (Hamming weight) of single bits and know the key, plaintext and respective processing order from an optional SCA collision Attack. This reduces the computation time significantly, as we know in which frames (clock cycles) the bytes are processed. The CPU overhead for calculating the hypothesis can be neglected. This step can further be optimized to work on some smaller regions and selective pixels if necessary. Please note that we do not try to optimize our trace number or calculation time. Other possible correlation-based approaches could lead to better results, but are not the focus of this paper. The result of the differential VCSCA can be seen in the correlation image in Figure 6.

(a) normal (b) inverted

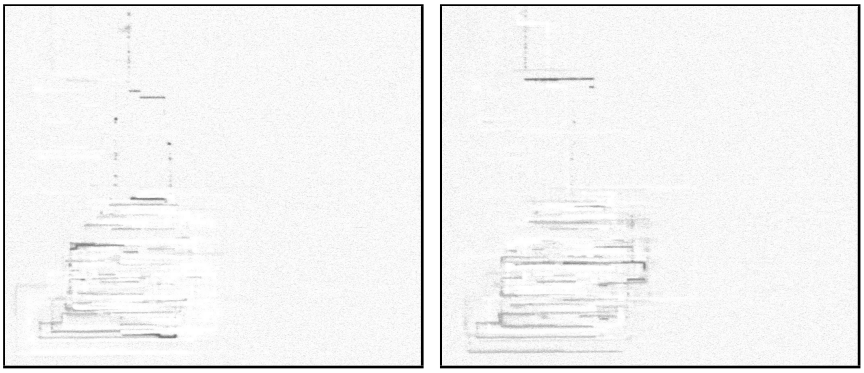
Fig. 6. Results of the correlation based VCSCA of the 8th addroundkey-bit in clock cycle 42. The colors are inverted for improved visualisation.

Figure 7 shows the correlation images of further bits after different AES subroutines (`addroundkey` and `subbytes`). Each have different peak-locations, showing the position of the processed bits. Images labeled with "inverted" invert the sign of the pearson correlation. Each image cuts negative correlations to 0. With this we get two different images for each bit processed that show logical inverted signals and their locations as well. The corresponding hypothesis and respective clock cycles are listed in the subcaption. A high correlation for `addroundkey`, `subbytes` and the plaintext was found in resp. 16 consecutive clock cycles. Interestingly did we find the plaintext bits on the very same spots as the `addroundkey`, indicating a common load/store unit or bus structure within the AES.

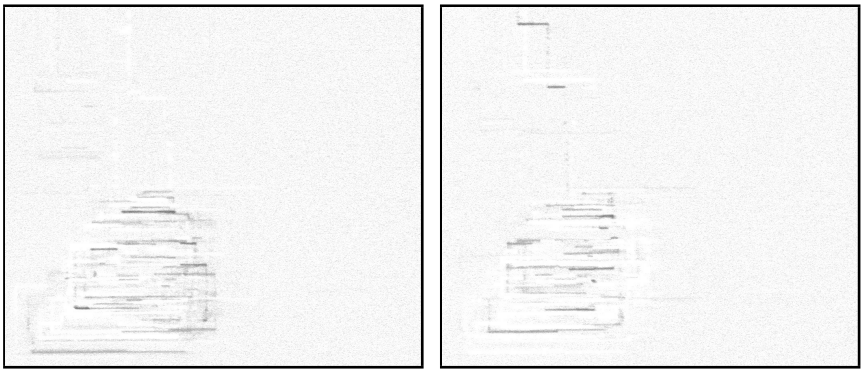
These information immediately allow an attacker to retrieve unknown keys in a template based VCSCA approach. This attack is done in Section 5.4 to recover the full AES key.

Before we introduce a template based key extraction we would like to emphasize the fact that the correlation images provides valuable information for a reverse engineer or sophisticated attacker. We know the location and meaning of selected wires in the highest metal layers. This reveals the location of AES calculations on gate-level when the wires are tracked into the polysilicon layer. The attacker is able to interpret neighboring and connected signals immediately. This might reveal further weaknesses or even whole Intellectual Property (IP) cores.

Furthermore it is also possible to apply other approaches easily, as the locations of the AES bits in top metal-layers are known. Mechanical probing or



(a) ark bit1 (b) ark bit2

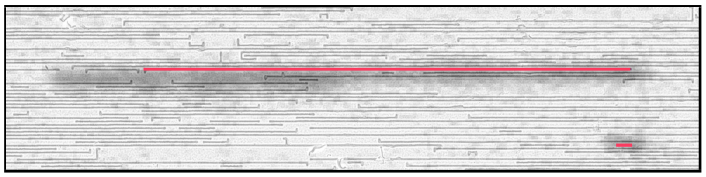


(c) inv ark bit1 (d) inv ark bit2

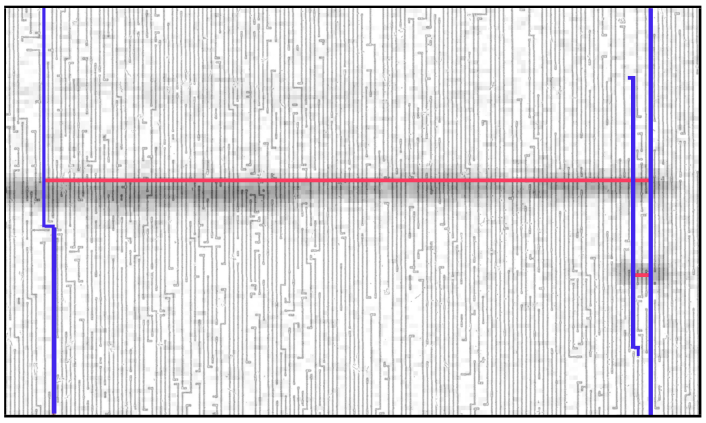
(e) sub bit1 (f) sub bit2

Fig. 7. Different correlation images found in clock cycle 42; addroundkey, inverted addroundkey and subbytes. The colors are inverted for improved visualisation.

fault attacks are two examples to retrieve or alter intermediate AES bits. Figure 8 shows cropped images of the 2 top metal layers from the XMEGA microcontroller scanned with a SEM, overlayed with the extrapolated correlation image of `addroundkey` bit 2. The correlation image is 50% transparent to visualize the manual mapping process.



(a) Top metal layer



(b) Metal layer beneath the top metal layer

Fig. 8. Marked wire of bit 2 of addroundkey in the two top layers. The black "cloud" is the extrapolated correlation image in this ROI. The colors are inverted for improved visualisation.

In Figure 8 we demonstrate that we are capable of identifying the tracked wires of bit 2 in the first two metal-layers. Continuing this, we would be able to pinpoint the location of the origin in the polysilicon and the next "processing steps" after the `addroundkey` subroutine. Nevertheless this is out of the scope for this paper. It is noteworthy that the two marked wires from the top layer are connected in the second layer. This is a good indication that we hit the right wires from our results.

5.3 Extracting additional netlist information

So far we analyzed bits within the AES circuit that are supposed to be part of the AES calculation. We did not look into the possibilities of how the `subbytes`

routine or other subroutines are built. Therefore we provide a Side Channel Analysis for Reverse Engineering (SCARE) like approach in this section.

We applied every $2 \rightarrow 1$ function from the 8 `addroundkey`-bits possible and used the result as a new hypothesis. Each possible $2 \rightarrow 1$ function is given in Table 1 from [13]. The results of the 2bit-function hypotheses revealed additional

Index	**f(B,A)**				**Boolean**	**Name**
of f	$f(1,1)$	$f(1,0)$	$f(0,1)$	$f(0,0)$	**equation**	
0	0	0	0	0	0	Zero
1	0	0	0	1	$\overline{B + A}$	NOR2
2	0	0	1	0	$\overline{B} \cdot A$	AND2B
3	0	0	1	1	$\overline{B}$	NOTB
4	0	1	0	0	$B \cdot \overline{A}$	AND2A
5	0	1	0	1	$\overline{A}$	NOTA
6	0	1	1	0	$B \oplus A$	XOR2
7	0	1	1	1	$\overline{B \cdot A}$	NAND2
8	1	0	0	0	$B \cdot A$	AND2
9	1	0	0	1	$\overline{B \oplus A}$	XNOR2
10	1	0	1	0	A	A
11	1	0	1	1	$\overline{B} + A$	OR2B
12	1	1	0	0	B	B
13	1	1	0	1	$B + \overline{A}$	OR2A
14	1	1	1	0	$B + A$	OR2
15	1	1	1	1	1	One

Table 1. $2 \rightarrow 1$ functions

circuit operations not known so far. For example did we find a correlation of a `xor` between Bit 3 and Bit 4 of the `addroundkey` bits. This allows us to build basic netlist operations and we are able to verify an extracted netlist (by usual means) with these findings or counter hardware obfuscation techniques like the one introduced in [15]. Some hardware protection might even play in our hands by routing sensitive wires through multiple layers, including the top metal [10].

Following this approach we might be able to reverse engineer whole subroutines, without invasive methods. This is not in the scope of this paper and can be done in future work. This small PoC shows the great potential for the VC side channel in SCARE like approaches.
In the following sections we use the VC in more common SCAs, to recover the AES key with our current setup. We execute a template-attack and independently another SSCA on a single trace in a no-plaintext, no-ciphertext and no-key attack. In both cases we retrieve the AES key successfully.

5.4 Template Attack with VCSCA

The setup for the key-recovering template attack is the same as described in Section 5.1, with the difference of choosing a constant (assumed unknown) key for all the traces. 250 Traces are acquired and random plaintexts are AES-128 encrypted by the DUT.
The "templates" are the correlation images generated in Section 5.2. The idea is to correlate the frames that process a specific byte and correlate the resulting `addroundkey` bit with a single key bit hypothesis. The resulting correlation image is either the "normal" or the "inverted" correlation image e.g. of bit 8 shown in Figure 6.

To explain the process, we give a short example with the 8th bit of byte 16 of the i-th trace ($p_{i\_16\_8}$). As we know the that the 16th byte is processed in the 42th frame of each trace, we extract this frame from every trace. Let us assume that our hypothesis of the 8th keybit of byte 16 is "1". We correlate each pixel of these frames with the `addroundkey` hypothesis which is calculated ($p_{i\_16\_8}$ `xor` hypothesis). This results in a correlation image that is either close to Figure 6a or Figure 6b. If the assumption is correct, we will get a correlating image close to Figure 6a. Otherwise the hypothesis is wrong and the 8th bit is "0". Repeating this process, every keybit can be recovered. Taking 250 traces is an estimated value to make sure that the attack succeeds, as we need to extract the right clockframes of the DVC video and to get a good average over noisy images. We verified that the attack is feasible with less traces.

5.5 Simple VCSCA

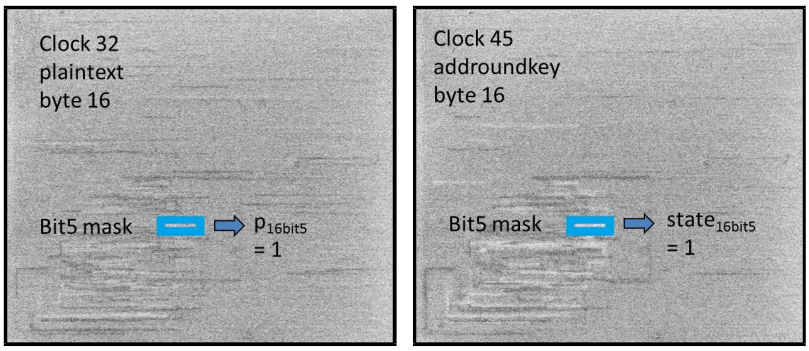
Realizing that the XMEGA reuses the same circuit for every byte sequentially, the bit locations are the same for every round and byte within the AES. Therefore we aim to find plain or key bytes directly being loaded or processed during the AES setup. Interestingly did we find the plaintext being loaded 13 clock cycles before the `addroundkey` function on the same bit locations as the `addroundkey` bit. This indicates a common load/store unit or a bus architecture. During this section we assume not knowing the key once more. Knowing that the plaintext is being processed right before the `addroundkey` allows an attacker a no-plaintext, no-ciphertext **and** no-key SSCA against the XMEGA AES engine. The aim of this section is therefore a PoC of the simple VCSCA with a single trace and 1 byte.

Section 5.2 already revealed the location and timing of individual `addroundkey` bits being processed. These bits have a key dependence through the `xor` with the plaintext, which can be read-out 13 clock cycles before. Therefore, this attack first recovers the plaintext bit and secondly reads-out the processed `addroundkey` bit in a SSCA. The recovered bits are `xored` to get the corresponding keybit as we only target the first round. This is repeated for 8 bits within byte 16 in a single trace. Figure 9 shows the wire positions for 2 bits that we used for recognition. The wire positions are chosen from multiple options, as they are reliable measured by the DVC and are easy recognisable.

(a) Bit 2 (b) Bit 5

Fig. 9. Correlation Image of keybits within clock cycle 48. The colors are inverted for improved visualisation.

In Figure 10 we demonstrate the simple VCSCA based on Bit 5. The other bits can be done in a similar manner.



(a) Clock 32 plaintext (b) Clock 45 addroundkey

Fig. 10. Extracted states of byte 16 bit 5 within one trace. The colors are inverted for improved visualisation.

A direct `xor` of both values, reveals the 5th keybit of byte 16. The keybit correctness was verified for every bit in Byte 16. We discovered that is not easy to find a trace that shows all bits recognizable at once, as the DVC images depend on the previous top-metal layer voltage and the exact beam position during the clock transition. We verified that is is possible to acquire at least one key-byte with one single trace. We did not look for further keybits, since the recognition was done manually. If we would want to automate this process, more traces should be used in order to work on mean images.

6 Conclusion

In this paper we revise an approach to pinpoint the ROI for ICs with VC images. This reduces the complexity of hardware reverse engineers by gaining a-priori knowledge of the location of security-relevant ROIs and allows to perform EM-based SCA with better signal-to-noise ratio. Furthermore this enables more advanced SCAs like inter-gate leakages discussed in [27] and reduces the exhaustive search for fault attacks.
The shown approach is at least as fast and easy to comparable approaches like EM cartography, thermal imaging and photon emission. The only required tool is a SEM, well distributed in universities and institutes due to its application in many academic fields. A SEM can be bought second hand for under 10k€. Specialized commercial EBPs for high speed measurements are also available.

We use the VC as a side channel that exploits the capacitive coupling effect of top metal layers through the covering passivation. We are able to see voltage alterations of the ICs surface in a SEM, revealing secret information through top metal-wire voltage changes. A PoC with a XMEGA microcontroller to locate and identify top metal layers holding intermediate AES bits is given. Any sophisticated attacker can track the wires to the polysilicon layer, revealing data flip-flops and memory structures of the AES. Furthermore we use the VC in multiple SCA approaches to recover the full AES key.

For the VCSCA template-attack, less then 100 traces are enough to reveal the key, while the simple VCSCA is performed in a no-plaintext, no-ciphertext and no-key attack scenario. Additionally we show a SCARE approach to recover further netlist information, that can be used to reverse engineer hardware circuits in a non-invasive way. The gained information can be used to partly verify an extracted netlist or to counter simple hardware obfuscation techniques.

Additionally is the backside CCVC or EBP shown in [21] and [20], a high hardware security threat, if the backside thinning is applicable to big areas and is used in a SCA. IC vendors and designers need to implement front- and backside hardware protection. Especially routing sensitive information into higher metal layers can easily be avoided by the routing software and should be done for multiple reasons: Firstly an attacker can probe the wires easily by mechanical means. Secondly it results in more power and EM emanation leakage, because of the higher capacitances of longer and thicker wires. The device will be vulnerable to a power or EM-based SCA and last but not least is the device vulnerable to the frontside VCSCA approach, shown in this paper.

Acknowledgement The authors would like to thank Michael Gilberg from the Bundeskriminalamt for his valuable experience and technical help with the FIB and SEM. Furthermore we would like to thank the anonymous reviewers at CHES 2015 for their valuable comments and additional references.

References

1. Atmel. Atmel AVR XMEGA AU Manual, 04 2013.
2. R. Barille. Analytical formulation of the capacitive coupling voltage contrast of a buried line. *Electronics Letters*, 29(20):1756–1758, Sept 1993.
3. D. L. Barton and P. Tangyunyong. Thermal defect detection techniques. *Microelectronics failure analysis: desk reference*, page 378, 2004.
4. P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson, and P. Maurine. Contactless electromagnetic active attack on ring oscillator based true random number generator. In Schindler, Werner and Huss, SorinA., editor, *Constructive Side-Channel Analysis and Secure Design*, volume 7275 of *Lecture Notes in Computer Science*, pages 151–166. Springer Berlin Heidelberg, 2012.
5. J. D. Benzel. Bugs in Black and White: Imaging IC Logic Levels with Voltage Contrast. *HEWLETT PACKARD JOURNAL*, 46:102–106, 1995. 00000.
6. K. J. Bertsche and J. Charles, H.K. The Practical Implementation of Voltage Contrast as a Diagnostic Tool. In *Reliability Physics Symposium, 1982. 20th Annual*, pages 167–178, March 1982.
7. J. Bindell and J. McGinn. Voltage Contrast SEM Observations with Microprocessor Controlled Device Timing. In *Reliability Physics Symposium, 1980. 18th Annual*, pages 55–58, April 1980.
8. C. Boit, C. Helfmeier, and U. Kerst. Security Risks Posed by Modern IC Debug and Diagnosis Tools. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on*, pages 3–11. IEEE, 2013.
9. O. Breitenstein, C. Schmidt, and D. Karg. Thermal failure analysis by IR lock-in thermography. *Microelectronics failure analysis desk reference, 5th ed., EDFAS*, 2004.
10. S. Briais, S. Caron, J.-M. Cioranesco, J.-L. Danger, S. Guilley, J.-H. Jourdan, A. Milchior, D. Naccache, and T. Porteboeuf. 3D hardware canaries. In *Cryptographic Hardware and Embedded Systems–CHES 2012*, pages 1–22. Springer, 2012.
11. O. Crépel, F. Beaudoin, L. D. de Morais, G. Haller, C. Goupil, P. Perdu, R. Desplats, and D. Lewis. Backside hot spot detection using liquid crystal microscopy. *Microelectronics Reliability*, 42(9-11):1741–1746, 2002.
12. J. Ferrigno and M. Hlavac. When AES blinks: introducing optical side channel. *Information Security, IET*, 2(3):94–98, September 2008.
13. S. Guilley, L. Sauvage, J. Micolod, D. Réal, and F. Valette. Defeating Any Secret Cryptography with SCARE Attacks. In *Progress in Cryptology - LATINCRYPT 2010* , pages 273–293. Springer-Verlag, 2010.
14. M. Kammerstetter, M. Muellner, D. Burian, C. Platzer, and W. Kastner. Breaking Integrated Circuit Device Security Through Test Mode Silicon Reverse Engineering. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 549–557, New York, NY, USA, 2014. ACM.
15. J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri. Security Analysis of Integrated Circuit Camouflaging. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 709–720, New York, NY, USA, 2013. ACM.
16. D. Real, F. Valette, and M. Drissi. Enhancing correlation electromagnetic attack using planar near-field cartography. In *Design, Automation Test in Europe Conference Exhibition, 2009. DATE '09.*, pages 628–633, April 2009.

17. R. Rosenkranz. Failure localization with active and passive voltage contrast in FIB and SEM. *Journal of Materials Science: Materials in Electronics*, 22(10):1523–1535, 2011.
18. L. Sauvage, S. Guilley, J.-L. Danger, N. Homma, and Y. Hayashi. Practical results of EM cartography on a FPGA-based RSA hardware implementation. In *Electromagnetic Compatibility (EMC), 2011 IEEE International Symposium on*, pages 768–772, Aug 2011.
19. L. Sauvage, S. Guilley, and Y. Mathieu. Electromagnetic Radiations of FPGAs: High Spatial Resolution Cartography and Attack on a Cryptographic Module. *ACM Trans. Reconfigurable Technol. Syst.*, 2(1):4:1–4:24, Mar. 2009.
20. R. Schlangen, R. Leihkauf, U. Kerst, C. Boit, R. Jain, T. Malik, K. Wilsher, T. Lundquist, and B. Kruger. Backside e-beam probing on nano scale devices. In *2007 IEEE International Test Conference*, 2007.
21. R. Schlangen, R. Leihkauf, U. Kerst, C. Boit, and B. Kruger. Functional IC analysis through chip backside with nano scale resolution-E-beam probing in FIB trenches to STI level. In *Physical and Failure Analysis of Integrated Circuits, 2007. IPFA 2007. 14th International Symposium on the*. IEEE, 2007.
22. A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, and J.-P. Seifert. Simple Photonic Emission Analysis of AES. In E. Prouff and P. Schaumont, editors, *Cryptographic Hardware and Embedded Systems – CHES 2012*, volume 7428 of *Lecture Notes in Computer Science*, pages 41–57. Springer Berlin Heidelberg, 2012.
23. S. Skorobogatov. Using Optical Emission Analysis for Estimating Contribution to Power Analysis. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2009 Workshop on*, pages 111–119, Sept 2009.
24. S. Skorobogatov and C. Woods. Breakthrough silicon scanning discovers backdoor in military chip. In *Proceedings of the 14th international conference on Cryptographic Hardware and Embedded Systems*, CHES'12, pages 23–40, Berlin, Heidelberg, 2012. Springer-Verlag.
25. S. P. Skorobogatov. Semi-invasive attacks – A new approach to hardware security analysis, 2005.
26. T. Sugawara, D. Suzuki, R. Fujii, S. Tawa, R. Hori, M. Shiozaki, and T. Fujino. Reversing stealthy dopant-level circuits. In *Cryptographic Hardware and Embedded Systems–CHES 2014*, pages 112–126. Springer, 2014.
27. T. Sugawara, D. Suzuki, M. Saeki, M. Shiozaki, and T. Fujino. On Measurable Side-Channel Leaks Inside ASIC Design Primitives. In G. Bertoni and J.-S. Coron, editors, *Cryptographic Hardware and Embedded Systems - CHES 2013*, volume 8086 of *Lecture Notes in Computer Science*, pages 159–178. Springer Berlin Heidelberg, 2013.
28. L. Tian. Simple, novel and low cost numerical aperture increasing lens system for high resolution infrared image in backside failure analysis . In *Physical and Failure Analysis of Integrated Circuits (IPFA), 2014 IEEE 21st International Symposium on the*. 2014.
29. K. Ura, H. Fujioka, and T. Hosokawa. Stroboscopic scanning electron microscope to observe two-dimensional and dynamic potential distribution of semiconductor devices. In *Electron Devices Meeting, 1977 International*, volume 23, pages 502–505, 1977.
30. K. URA, H. FUJIOKA, and T. HOSOKAWA. Picosecond Pulse Stroboscopic Scanning Electron Microscope. *Journal of Electron Microscopy*, 27(4):247–252, 1978.