Research Directions for Verifiable Crypto-Physically Secure TEEs

`draft`

Sylvain Bellemare*

October 1, 2024

A castle is a very old example of a TEE.

C. Shepherd and K. Markantonakis
Trusted Execution Environments

Information is not a disembodied abstract entity; it is always tied to a physical representation.

Rolf Landauer
The physical nature of information

Abstract

A niche corner of the Web3 world is increasingly making use of hardware-based Trusted Execution Environments (TEEs) to build decentralized infrastructure. One of the motivations to use TEEs is to go beyond the current performance limitations of cryptography-based alternatives such as zero-knowledge proofs (ZKP), fully homomorphic encryption (FHE), and multi-party computation (MPC). Despite their appealing advantages, current TEEs suffer from serious limitations as they are not secure against physical attacks, and their attestation mechanism is rooted in the chip manufacturer's trust. As a result, Web3 applications have to rely on cloud infrastruture to act as trusted guardians of hardware-based TEEs and have to accept to trust chip manufacturers. This work aims at exploring how we could potentially architect and implement chips that would be secure against physical attacks and would not require putting trust in chip manufacturers. One goal of this work is to motivate the Web3 movement to acknowledge and leverage the substantial amount of relevant hardware research that already exists. In brief, a combination of: (1) physical unclonable functions (PUFs) to secure the root-of-trust; (2) masking and redundancy techniques to secure computations; (3) open source hardware and imaging techniques to verify that a chip matches its expected design; can help move towards attesting that a given TEE can be trusted without the need to trust a cloud provider and a chip manufacturer.

*Cornell Tech, New York, `sbellemare@cornell.edu`.

Contents

1 Introduction

This is an initiative to spark research to explore how we could develop a secure chip for TEEs (Trusted Execution Environments) that would ultimately be secure because of cryptophysics (i.e. physics, mathematics & crytpography), rather than economics. This work is aimed at the Web3 (aka "crypto" & blockchain) communities, who are increasingly using TEEs in various protocols to potentially secure substantial amounts of money, and/or to secure the privacy of users. We also hope to motivate more collaboration between the Web3 and the hardware communities, and thus, this work may also be interesting for some hardware communities, especially those interested in hardware-intrinsic security, and open source hardware.

1.1 The Problem TEEs aim to solve

TEEs are an attempt to solve the *secure remote computation* problem. Quoting [33]:

> *"Secure remote computation is the problem of executing software on a remote computer* ***owned and maintained by an untrusted party****, with some integrity and confidentiality guarantees".*

The problem could potentially be solved by combining proving systems (e.g. zkVMs) with FHE schemes, but despite progress being made in this direction, the performance of these systems limits the applications that can be implemented, and as a result, some Web3 projects are turning to TEEs, as they offer better performance. These projects are however facing a serious problem: Current commercial TEEs exclude side-channel and physical protection [33, 93, 100], which implies that attackers with physical access to the TEE could compromise both the integrity and confidentiality guarantees. In order to mitigate this limitation, some projects propose to restrict the TEE to be run in a cloud provider, thus making the cloud provider a trusted party, responsible to protect the TEE from malicious physical attackers [66]. Although reasonable, this approach runs counter with the decentralization goals of Web3. Recently, different teams from the Web3 world, called for the need to seek alternative solutions [65, 114, 115].

1.2 The Misalignment Between TEEs and Web3

Web3 thrives for decentralization meanwhile current Trusted Execution Environments imply a trusted manufacturer, and thus are misaligned with the decentralization direction of Web3. It is arguably more complicated than *just* trusting the manufacturer though, as the physical implementation of the TEE must also be trusted, independently of whether the manufacturer is honest or not. One could also argue that Web3 and current TEEs have radically different adversarial models. At a high-level, Web3 is about trusting nothing and verifying everything, meanwhile current TEEs, require trust in the manufacturer at the very least, but also trust that those who have physical access to the TEEs will not attack it.

1.2.1 Adversarial Model of Current TEEs

In this work we wish to focus on the fact that current TEEs, used by Web3 applications, are not secure against physical attacks, and that they assume an honest manufacturer. For detailed presentations of the threat model of Intel SGX/TDX and the likes, see [8, 33, 100, 104, 109]. For a treatment of TEEs in the context of blockchain applications see [93].

We should point out that some TEEs, used in smartphones, do aim to provide protection against side-channel and fault injection attacks, but have nevertheless been attacked [105, 106]. Moreover, these TEEs (e.g. Apple Secure Enclave) are not used for blockchain applications as far as we know.

1.2.2 Trust Assumptions of Current TEEs

In general, trusting current TEEs, such as Intel SGX, rests on the following assumptions:

Assumption 1 (Secure Design)**.** *Trust that the chip is* ***designed*** *and secured as per the claims of the chip maker.*[1]

Assumption 2 (Manufactured as per the Secure Design)**.** *Trust that the chip is* ***manufactured*** *as per the secure design, as claimed by the chip maker.*[2]

Assumption 3 (Secure Root-of-Trust Generation)**.** *Trust that the* ***root-of-trust*** *is not leaked during the manufacturing process. This means trusting that the manufacturer, or any other entity, have no knowledge of the root-of-trust.*

Assumption 4 (Secure Root-of-Trust Post-Fabrication)**.** *Trust that the* ***root-of-trust*** *cannot be extracted out "cheaply" or "easily" by an attacker who has physical access to the chip.*

Assumption 5 (Secure Computations)**.** *Trust that computations, executed in enclaves, do not leak confidential data, under side-channel attacks such as power analysis.*

Assumption 6 (Unforgeable Attestations)**.** *Trust that* ***attestations*** *cannot be forged, in one way or another. This implies multiple assumptions: (1) trusting that attestation keys are protected against side-channel (e.g. power analysis) or physical attacks (2) trusting that attestation keys are not known to the chip manufacturer.*[3]*, and (3) trusting that the root-of-trust is secure and that deriving the attestation from the root-of-trust would not be feasible,*

These assumptions are a source of troubles for the Web3 communities since they represent a misalignment with the goals of decentralization.

The Malicious Manufacturer Problem The problem of having to trust a manufacturer, is not new, nor unique to Web3 concerns. For instance, quoting [117]:

> *While the economic benefits are clear and many of the manufacturers are honest, outsourcing gives rise to a significant security threat. It takes only one malicious employee to compromise the security of a component that may end up in numerous products.*
>
> *Simply stated the untrusted manufacturer problem occurs in two situations:*
>
> - *an intellectual property (IP)-core designer inserts a secret functionality that deviates from the declared specification of the module*

[1] This trust is necessary because the designs of commercial TEEs are not open source, and despite academic efforts such as [33] to explain the design, we cannot know all the details of the design, and need to trust the chip company.

[2] Note that design and implementation flaws can be fixed and can happen whether the design is open source or not, whether the supply chain is correct, etc. Hence, design and implementation bugs can be treated separately. It could be argued that an open source hardware design may benefit from a broader community and overtime will contain less bugs than a closed source design [21].

[3] See RFC 9334 (section 12) [15] for security considerations when treating the topic of remote attestation.

- *a manufacturer modifies the functionality of the design during fabrication.*

Clearly, besides tampering the goal of the malicious manufacturer is to operate covertly. The ever increasing complexity of hardware and software designs makes it much easier for untrusted manufacturers to achieve this goal.

1.3 Restoring the Alignment Between TEEs and Web3

Rather than working around the above assumptions, we propose to research how we could design and implement novel TEEs that would be aligned with the decentralization goals and adversarial model of Web3.

1.3.1 Adversarial Model of Crypto-Physically Secure TEEs

TEEs should be secure against side-channel and physical attacks, and consequently attackers with physical access are part of the threat model. Moreover, the attacker is considered to be unbounded with respect to resources and skills to perform side-channel and physical attacks. We assume the most sophisticated attacker, with the highest attack potential, as per the industry framework presented in [76]. The manufacturer and its suppliers are considered to be adversaries, that can inject hardware trojans and deviate from the chip design that must be manufactured [117]. For a classificaiton of the types of attacks we are concerned with see [7, 28, 79, 111].

A Note About Economic Security Although the focus of this work is to research directions to develop crypto-physically secure TEEs, if possible it is likely to take considerable time, and in the meantime, it would be important to acknowledge the economical dimension of attacks and to be able to identify the precise costs to perform the attacks, in order to inform protocol designers, who can then introduce game theoretic aspects in their designs [93].

1.3.2 Challenges for Crypto-Physically Secure TEEs

To help orient the research work, we present the following challenges to help us think beyond the current TEEs, and to move towards novel TEEs that do not sacrifice Web3's decentralization efforts. These challenges reflect our view that we need to move towards TEEs which are secure through physics and cryptography.

Challenge 1 (Open Source Hardware Design)**.** *As per Kerckhoffs' principle: "It must not require secrecy, and it must be capable without inconvenience to fall into the enemy's hand". [64]*

Challenge 2 (Proof of Fabrication)**.** *The physical implementation must match its open source design, and it must be verifiable.*

Challenge 3 (Oblivious Root-of-Trust Generation)**.** *The root-of-trust must not be known to any party before, during or after generation time. The process used to generate the root-of-trust must not leak any information that could be used to reconstruct the root-of-trust.*

Challenge 4 (Oblivious Root-of-Trust Usage)**.** *Using the root-of-trust to support computations, such as signatures and key derivations, must not reveal any information that could be used to reconstruct the root-of-trust, or any other confidential data for which the security is rooted in the root-of-trust.*

Challenge 5 (Crypto-Physically Secure Computations)**.** *The trusted execution environments must not leak confidential data, and must be protected against side-channel attacks [7, 28, 79, 111].*

Challenge 6 (Unforgeable Attestations)**.** *Attestations must be authentic and verifiable such that a verifier can link the report to a secure root-of-trust that is tied to the verified implementation, which corresponds to the expected open source hardware design.*

1.4 Related Work

The Secure Cryptographic Implementation Association [21] is actively working on developing open hardware that can withstand physical attacks such as side-channel and fault attacks. Their vision is that an *"open approach to security can lead to a better evaluation of the worst-case security level that is targeted by cryptographic designs"*. OpenTitan [32, 83, 90] is an open source hardware root-of-trust. The importance of verifiable hardware and a novel verification technique, based on infra-red light, are discussed in [53] by Andrew 'bunnie' Huang. The importance of open source hardware and verification techniques is discussed in [120]. The open hardware landscape is surveyed in [49]. For a very detailed and broad survey of TEEs, see [105], which motivates the need for more secure TEEs, including protection against physical attacks.

Sanctum [34,73] addresses software-based side-channel attacks, such as cache timing attacks via minimal hardware extensions in a first work. They also point out the difficulty of securing remote computations even in the presence of strong economic incentives. In a second work, Sanctum leverages PUFs to provide a secure boot and remote attestation. The threat model assumes an honest-but-curious manufacturer, meaning that the manufacturer may attempt to read the root-of-trust, but will implement the chip according to its expected design. In our case the manufacturer is assumed to be malicious, which means that we do not rely on the manufacturer to implement the chip as per the expected design. Keystone enclave [74] is an open source software TEE framework. It needs a hardware layer with a secure root-of-trust.

Motivation to put more research efforts into implementing roots of trust with emerging hardware technologies, such as resistive memories and flexible electronics is discussed in [82]. A brief survey of challenges in hardware security is presented in [62]. In the Web3 context, motivaton for research to address the current limitations of TEEs and their lack of decentralization has been mentioned in [65, 112, 114, 115]. In addition to adressing the lack of decentralization with current TEEs, [93] also points out at the lack of an economic security model to work with when integrating TEEs in a blockchain context. In zach's tech blog [124], the author motivates how the current semiconductor startup ecosystem could benefit from a Silicon Venture Studio.

There's a lot of work that covers the topic of using physics to secure a system, such as [9, 16, 45, 89].

2 Ethics, Morality, and the Cypherpunks

Is it a good idea to attempt to build a secure-through-physics TEE? Are there dangers? Could it be misused? This section is meant to invite the community to reflect on the ethical and moral implications of an eventual secure-through-physics TEE. In order to guide this reflection, we propose a few works to reflect on, as starting points. We don't claim that they're the only ones to reflect on, nor that they're the best ones. We simply wish to encourage discussions on the ethical and moral implications of our work.

- The Moral Character of Cryptographic Work by Phillip Rogaway [97],
- The battle for Ring Zero by Cory Doctorow [39]
- The Crypto Anarchist Manifesto by Timothy C. May [80]
- A Cypherpunk's Manifesto by Eric Hughes [54]
- Trusted Execution Environments (Section 8.5) by Carlton Shepherd and Konstantinos Markantonakis [105]

The battle for Ring Zero Cory Doctorow, in [39] points out:

> *But how can we trust those sealed, low-level controllers? What if manufacturers — like, say, Microsoft, a convicted criminal monopolist — decides to use its low-level controllers to block free and open OSes that compete with it? What if a government secretly (or openly) orders a company to block privacy tools so that it can spy on its population? What if the designers of the secure co-processor make a mistake that allows criminals to hijack our devices and run code on them that, by design, we cannot detect, inspect, or terminate? That is: to make our computers secure, we install a cop-chip that determines what programs we can run and stop. To keep bad guys from bypassing the cop-chip, we design our computer so it can't see what the cop-chip is doing.* ***So what happens if the cop-chip is turned on us?***

3 Oblivious Root-of-Trust Generation

How can we create a signing key (root-of-trust) in an oblivious way, meaning that the key must not be known by any party when it is created?

3.1 Physically Unclonable Functions (PUFs)

Current state-of-the-art chip fabrication, although extremely precise, is not precise enough to prevent unpredictable and uncontrollable physical variations between identical logical components. For instance, two identical transistors will react differently under the same voltage. Hence, millions of chips with the same identical design, will have different physical properties, which can be leveraged as sources of entropy. A physical unclonable function (PUF) is a circuit block in a chip that leverages these physical variations to derive the unique fingerprint of its chip. This fingerprint can be used to uniquely identify and authenticate a chip and also to generate a signing key (root-of-trust) [77]. Quoting [45]:

> "We wish to implement a PUF in silicon so we can **identify and authenticate** a given **integrated circuit** (IC). By exploiting **statistical variations** in the delays of devices and wires within the IC, we create a **manufacturer resistant** PUF".

Physically unclonable functions (PUFs) are said to be manufacturer resistant because the manufacturer cannot predict nor control the physical variations from which entropy is derived. Furthermore, the manufacturer, or anyone, cannot "clone" a PUF such that it will behave the same way as the

original one. Also, for most PUFs, probing the PUF is expected to destroy its entropy, and therefore its associated fingerprint or key. It's important to note that we wish to point to PUFs as a very good potential candidate solution for Challenge 3, (that of intrinsically creating a signing key, such that the key cannot be observed by any entity), but more study and research is required to properly understand their security limits and vulnerabilities. Exploring the security limits of PUFs is outside the scope of this work, but we nevertheless present a brief and partial survey of attacks on PUFs in Section 3.3. As it will be seen in Section 3.1.1 on the core properties of PUFs, the PUF is not really a function since its output is not deterministic as it contains noise from the physical environment of the chip, such as heat, and voltage. For cases like generating a signing key, a deterministic response is required and PUF designs must include some post-processing on the response to clean out the noise. Section 3.1.3 provides a small introduction to the topic of stabilizing a PUF response. We now briefly discuss the two main types of PUFs: strong and weak PUFs, also named authentication and key generation PUFs, respectively.

A Note about Strong PUFs versus Weak PUFs The lierature distinguishes between two main types of PUFs, based on the size of their challenge-response pairs (CRPs) set. PUFs that have a very large set of CRPs are referred to as "strong" or authentication PUFs, whereas PUFs that have very few CRPs, are referred to as "weak" or key (generation) PUFs. Strong PUFs although theoretically promising [38] have been subject to multiple attacks, most notably machine learning attacks, and have yet to be shown to be secure [70]. On the other hand, weak PUFs, used for key generation, are more secure as their small set of CRPs cannot be exploited by machine learning attacks, and are already in use commercially extensively, especially in IoT devices.

3.1.1 PUF Properties

Our goal here in reviewing the properties of PUFs is to show how they are a good fit to address the challenge of obliviously generating the root-of-trust (Challenge 3). We'll use the definitions presented in [78] almost verbatim as a basis. The authors first define a PUF as a physical challenge–response procedure, which implies that it is embedded in a physical device, has an input/output mechanism and is more general than a function, since a PUF can have multiple outputs for the same input [77]. A PUF is denoted as

$$\Pi : \mathcal{X} \to \mathcal{Y} : \Pi(x) = y. \tag{1}$$

Using the above defintion, the authors in [78] outline the following semi-formal properties (see [78] for more details).

Property 3.1 (Evaluatable)**.** *Given a* PUF Π *and a challenge* x*, it is* `easy` *to evaluate the response* $y = \Pi(x)$*.*

Property 3.2 (Unique)**.** PUF $\Pi(x)$ *contains* `some` *information about the identity of the physical entity embedding the* PUF Π*.*

Property 3.3 (Reproducible)**.** *The response* $y = \Pi(x)$ *is reproducible up to a* `small` *error.*

Property 3.4 (Unclonable)**.** *Given a* PUF Π*, it is* `hard` *to construct a procedure* $\Gamma \neq \Pi$ *such that* $\forall x \in \mathcal{X} : \Gamma(x) \approx \Pi(x)$ *up to a* `small error`*.*

Property 3.5 (Tamper evident)**.** *Altering the physical entity embedding* Π *transforms* $\Pi \to \Pi'$ *such that with high probability* $\exists x \in \mathcal{X} : \Pi(x) \neq \Pi'(x)$*, not even up to a* `small error`*.*

Evaluatable The root-of-trust can be efficiently generated.

Uniqueness The root-of-trust will be unique to each chip, which will allow identification of the chip, via the public key associated with the signing key (root-of-trust).

Reproducibility (Stability) The root-of-trust can be re-generated repeatedly, across the lifetime of the chip. Recall that the root-of-trust is only present when the chip is powered up. Hence, each time the chip is powered up, the exact same signing key must be re-generated. This is not so simple since the response of a PUF is subject to environmental noise, and aging, and thus will vary. Post-processing steps are necessary to clean out the noise, via error correcting codes or other means. The literature also refers to this property as stability.

Unclonability It is practically infeasible to build chips, for which the PUF will yield identical signing keys. Moreover a mathematical clone should also be hard (infeasible) to build, thus preventing simulating the PUF, and its associated signing key. Quoting [78]:

> [...] the hardness of cloning can be considered from a theoretical and a practical point of view. Practically, cloning can be very hard or infeasible. Demonstrating theoretical unclonability on the other hand is very difficult. The only known systems which can be proven to be theoretically unclonable are based on quantum physics.

Tamper evidence Physically probing the PUF in a chip should change its entropy, effectively destroying the root-of-trust (signing key). Note that this is the ideal goal, but that there has been attacks in which the PUF is probed and yet not altered such that extracting its response (root-of-trust in our case) was possible [36]. As mentioned earlier, PUFs are an active area of research, and more secure PUFs are constructed, but also attacks, thus moving the technology forward. See Section 3.3 for a partial survey of physical attacks on PUFs.

3.1.2 Good and Bad Chaos for PUFs

As mentioned, a PUF leverages the physical variations introduced during manufacturing. When a chip is powered up it is also subject to variations like heat, which will affect the behavior of the PUF, such that its response will not be deterministic. A chip is also subject to aging, and overtime the response of a PUF will also change because of degradation of its physical components. Hence, there's good and bad chaos for reliable PUFs. In order to help us better understand PUFs, we'll review the three types of physical variations in (CMOS) chips, based on the work in [67].

Process Manufacturing Variations Two main types of variations are introduced during the making of chips: (1) *variations in process parameters* for the deposition and/or diffusion of dopants (2) *variations in the dimensions of the transistors*, due to the limited resolution of the photo-lithographic process. [67].

Environmental Variations A PUF is embedded in a chip, and its surrounding environment can have an impact on its response. Factors like heat, voltage and noise coupling can cause the response of a PUF to be different within relatively short amounts of time. For example, the vibration of electrons will cause electronic noise, known as Johnson–Nyquist noise, which will impact a PUF's response. Hence, even in perfectly stable laboratory conditions, a PUF's response is not perfectly reproducible. [36]

Aging Depending on how frequently a chip is used, its components will slowly degrade and these physical changes will impact the PUF response.

3.1.3 PUF Response Stabilization

As mentioned previously, chips are subject to unwanted variations which will destabilize the PUF response, and thus require post-processing steps to re-generate the same signing key (root-of-trust). Error correction schemes [13, 43] are commonly used to recover the original response. Although reliable, error correction schemes require helper data to be stored in non-volatile memory. To circumvent this drawback, other techniques have been developed, such as temporal majority voting, dark-bit masking, and burn-in enhancement. Many PUF designs combine temporal majority voting with dark-bit masking to achieve better stability of the PUF response [29]. Active PUFs were also introduced in [29], by Chuang, as a new method to stabilize the response of a PUF. Such PUFs require an activation step after the fabrication of the circuit. In [29], a metal oxide breakdown PUF is proposed, in which two logically identical transistors are stressed with a high voltage to provoke the formation of oxide breakdown. Depending on which transistor breaks down first, a bit of 0 or 1 is set. Since thee oxide breakdown is permanent the PUF response becomes stable. By building an array of transistor pairs, a stable bit string can be obtained, and used to to generate a key. However, it was shown in [99], to be vulnerable to imaging attacks, by using Voltage Contrast Scanning Electron Microscopy (VC-SEM), to identify which transistor has oxide breakdown, and then reconstruct the key, with very high accuracy.

3.2 Recent PUF Constructions

To give some pointers to recent research work in developing PUFs, readers may consult [30, 31, 119, 121] but also note that the security of these PUFs has been attacked in [99]. Future version of this work intend to add state-of-the-art PUF constructions to this section.

3.3 Physical Attacks on PUFs

Future work should aim at documenting all known physical attacks, but for now we'll summarize the work of Delvaux in [36], and also point to recent work shown in [99] and [70]. One important topic to cover is that of attacks to read volatile memory, and protection against such attacks [18]. Another important category of attacks targets the post-processing step (fuzzy extraction), via side-channel and/or fault injection attacks [61, 72, 91, 113].

3.3.1 A Note on Characterization Techniques for Semiconductors

This is for attacks that aim at characterizing the critical parts of a chip (e.g. PUFs), when it is powered down, in order to derive a mathematical model to perform simulations to predict the

behaviour of the chip when it is powered up. This is super crucial to the current security of PUFs, and more precisely to their mathematical unclonability. It's currently infeasible to characterize a PUF for instance, because the characterization techniques are not advanced enough. That being said, it does not mean that characterization techniques will not improve, and consequently it may be wise to encourage the development of these techniques as it well help us better understand the physical limits of the security of PUFs. Related research can be consulted in [68, 87, 98, 108].

4 Oblivious Root-of-Trust Usage

In this section we wish to focus on the challenge of using the root-of-trust without it being vulnerable to attacks. As discussed in the previous section, a PUF can be used to generate a signing key in a secure way since the generation process of the key depends on physical variations which probing would disturb and cause the key generation step to produce a different key. Moreover, the key is only ever present in volatile memory when the chip is powered up. *It's assumed that reading the volatile memory is infeasible or very hard.* But we need to use the key to perform cryptographic operations such as signing. Does using the key expose the key to attacks? For example, TEEs such as Intel SGX and Sanctum, depend on a privileged enclave that has access to a signing key that is derived from the root-of-trust. Neither Intel SGX nor Sanctum protect the attestation (signing) key from side-channel attacks, such as power analysis attacks [35], and it therefore seems reasonable to assume that the attestation key could be compromised by physical or side-channel attacks when it is under use, such as signing attestation reports.

4.1 Masking and redundancy

In this work, we wish to protect the root-of-trust against side-channel and fault injection attacks. The state-of-the art technique to protect against side-channel attacks is masking [20, 22, 25, 69, 84, 126], meanwhile redundancy is used to protect against fault injection attacks [12]. Masking can be thought of as MPC in silicon, such that a secret key is split into shares and the computation is done on shares. The masking scheme ensures that side-channel attacks such as power analysis or electromagnetic radiation analysis cannot collect enough sufficient information from the shares to reconstruct the secret key [20]. Redundancy techniques run the same computation multiple times through the same circuitry or through duplicate circuitry, and compare the results of the different runs to make sure they are the same. Hence, if some fault was injected in one run it will be detected. Recent work shows that the usage of prime-field masking [19] can help protect against fault injection attacks as well [85]. It should be noted that masking and redundancy provide higher security at a cost with respect to performance.

4.2 Security of Masking Schemes

It is important to note that masking schems depend on a source of randomness [111]. A true random number generator (TRNG) can be used to securely derive the randomness. TRNGs leverage the noise (thermal, jitter, chaos, metastability, etc) [7, 123] in a chip as a source of entropy to derive randomness, and have security properties very simlar to that of PUFs, since the randomness is also derived from unpredictable and uncontrollable physical properties of the chip's circuitry. TRNGs can be attacked though, especially if not designed or implemented properly. For a survey of attacks

on TRNGs see [28]. To mitigate the risks associated with attacks on the TRNG, some additional techniques are suggested in [111].

5 Crypto-Physically Secure Computations

Recall that the goal of a TEE is to perform computations meanwhile providing integrity and confidentiality guarantees. Intel SGX and Sanctum use hardware isolation to secure the computations [35], but the threat model excludes physical side-channel attacks, and fault injection attacks. The state-of-the-art techniques to protect against SCA and FI attacks is masking [20, 22, 25, 69, 84, 126], and redundancy [12], which were both discussed in Section 4, for the purpose of protecting the root-of-trust (signing key) when it is used for signatures. Masking and redundancy offer security at a cost to performance, and it would be useful to better understand the tradeoff and challenges [17] especially if these techniques are to be used for complex computations.

The work in [118] discusses the challenges and tradeoffs associated with implementing masking in both software and hardware. In brief, hardware masking can be designed to be provably secure, both in theory and practice, but cannot be changed post-fabrication unless it is implemented on FPGAs. Software masking can be changed after fabrication, but is not secure in practice, and has a high latency overhead. To get the best of both worlds, a masked instruction set extension has been proposed in [44], but was shown to have flaws in [118]. More recent work presents another instruction set extension [27] that aims at elminating leakage stemming from architectural and microarchitectural overwriting. This approach is still experimental and is a matter of debate as to whether it can meet its security goals [118]. Verifying that the masking used does not leak information is important and is studied in [48] in the context of large masked computations.

Secure computations are likely to require memory to be encrypted [11].

6 Open Source Hardware

The core reasoning behind moving from close source to open source hardware is that it would encourage collaboration, which would eventually lead to better hardware and at a faster pace. Consider the story behind the CERN Open Hardware License [23] [24]:

> "For us, the drive towards open hardware was largely motivated by well-intentioned envy of our colleagues who develop Linux device-drivers", said Javier Serrano, an engineer at CERN's Beams Department and the founder of the OHR."They are part of a very large community of designers who share their knowledge and time in order to come up with the best possible operating system. We felt that there was no intrinsic reason why hardware development should be any different". [...] "By sharing designs openly" said Serrano, CERN expects to improve the quality of designs through peer review and to guarantee their users — including commercial companies — the freedom to study, modify and manufacture them, leading to better hardware and less duplication of efforts.

For some reason, the hardware world does not embrace open source like the software world. Moreover, it is common practice to use hardware obfuscation [42, 103] as a core design principle to secure hardware. Simply said, for whatever reason, the current hardware industry appears to be dominated by the belief that it's best to hide the design and inner workings of a chip by adding

unnecessary elements to the design, just to confuse a potential attacker, in the hope that the attacker will not be able to understand the design, and thus reverse engineer it. Not everyone agrees with this vision. The Secure Cryptographic Implementation Association (SIMPLE-Crypto) [21] has already established a very good foundation to research and develop open source hardware. They have implemented AES in hardware with strong side-channel security countermeasures, which is currently under public evaluation. Auguste Kerckhoffs, back in 1883, in his paper entitled "La Cryptographie Militaire" (Military Cryptography), argued that security through obscurity wasn't a desirable defense technique.

> ***Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi***

roughly translated to:

> ***It must not require secrecy, and it must be capable without inconvenience to fall into the enemy's hand***

(Perhaps, one may point out that Kerckhoffs was assuming that the private key would be held secretly and not be part of an open design.) The need to secure a private key in an open design begs for physics to enter the arena (e.g. PUFs). The Secure Cryptographic Implementation Association (SIMPLE-Crypto Association) aims to apply Kerckhoffs's Principle to hardware and lays out their vision[4]:

> ... **our vision is that as research advances, the security by obscurity paradigm becomes less justified and its benefits are outweighted by its drawbacks.** That is, while a closed source approach can limit the adversary's understanding of the target implementations as long as their specifications remain opaque, it also limits the public understanding of the mechanims on which security relies, and therefore the possibility to optimize them. By contrast, an open approach to security can lead to a better evaluation of the worst-case security level that is targeted by cryptographic designs.

Open source hardware development depends on three key things [101]:

- Open Electronic Design Automation (EDA) sofware tools
- Open Process Design Kit (PDK) software
- Foundries to build the chip, that will allow the design to be open source

6.1 Open Source EDA Tools

Open source electronic design automation (EDA) sofware such as OpenRoad [26, 59, 60, 88] can be used to design chips and be sent for tapeout at foundries, such as Google Skywater and IHP, that support open sourcing the design. An EDA workflow to optmize the design of masking schemes is presented in [69] and may be useful to consult.

[4] www.simple-crypto.org/about/vision

6.2 Foundries and Open Source PDKs

The Leibniz Institute for High Performance Microelectronics (IHP) maintains an open source PDK that targets a 130 nm process node (SG13G2) of their pilot line, which manufactures circuits using high-performance SiGe BiCMOS technologies [51]. Google currently maintains three open source PDKs [2], in partnership with two foundries: SkyWater Technologies (90nm and 130nm) and GlobalFoundries (180nm) [10, 41, 50, 58, 81].

6.3 Research and Community Initiatives

- SIMPLE-Crypto — "develops open-source implementations of cryptographic algorithms, specialized for embedded systems (hardware and software), with strong physical security guarantees (e.g., against side-channel and fault attacks), featuring state-of-the art security and performance, maintained in the long-term" [21]
- The HEP Alliance [4,6] is dedicated to "Hardening the value chain through open source, trustworthy EDA tools and processors", and is working on a project (VE-HEP) to demonstrate the feasibility of using open source tools to develop secure chips.

  > "The use case to implement all these ambitious goals is the design and fabrication of an open-source hardware security module (HSM) that will be integrated into an automotive application".

- Free Silicon Foundation (F-Si) [1]
- The FOSSi Foundation — the custodian of the Free and Open Source Silicon movement[5]
- Workshop on Open-Source EDA Technology — The WOSET workshop aims to galvanize the open-source EDA movement[6]
- The Silicon Salon — Semiconductor Solutions for Cryptography [5]

6.4 Economic Challenges for Open Source Hardware

What is the economic model for open source hardware?

6.5 Technical Challenges for Open Source Hardware

Open source hardware is currently far behind the cutting-edge closed source hardware. What can be done to work towards closing that gap?

7 Proof of Fabrication (Verifiable Chip Implementation)

How do we know whether a given chip corresponds to a given design? Some possible approaches, which can perhaps be combined together:

- (**Pre-fab**) Logic Encryption encrypts the design [95]

[5] https://fossi-foundation.org
[6] https://woset-workshop.github.io/

- (**Peri-fab**) A public blockchain to track the stages of fabrication of a chip, which can be uniquely identified by its PUF or TRNG-based key [57]
- (**Post-fab**) Microscope imaging of the chip to compare it against its design [92]

7.1 Pre-Fabrication: Logic Encryption

Logic Encryption [95, 110, 116] locks the netlist of a chip design to protect against a malicious foundry. The key to unlock the netlist is written to non-volatile memory after fabrication, by the IP owner [94]. The company HENSOLDT Cyber [3] has numerous research works [127–130], on the topic, in addition to actually making chips, and hence, is probably worth studying.

Logic encryption schemes can be attacked though. One type of attack targets the key used to unlock the netlist [94], as the key is being transferred from memory to the key-gates to unlock. The author in [94] propose some countermeasures. Protecting the locking key from physical attacks is a field of research. For instance, recent work [40] propose to use nanomagnet logic to secure the locking key.

7.2 Blockchain and PUF-based Trusted Supply Chain

Various works propose to leverage the use of a blockchain to trace the various steps of the supply chain. These works make use of a PUF or TRNG to uniquely identify a chip. See for instance [55–57, 71, 75, 96, 122].

7.3 Post-Fabrication: Microscope Imaging

See [92] in which SEM imaging was used to detect hardware trojan insertions in chips.

Some imaging techniques (invasive) destroy the chip in the process meanwhile others (non-invasive) do not. Invasive analysis would need to be combined with a Cut-and-Choose protocol as proposed by Miller in [14][7].

It's important to point out that there seems to be newer techniques that are non-invasive, based on X-ray ptychography, X-ray nanotomography [63] or Photonic Emission Analysis/Microscopy (PEM).

Quoting [92]:

> New non-invasive scanning methods based on X-Rays [52] seem more promising for the future than the lengthy process of delayering and imaging the chip. These non-invasive techniques are potentially able to scan all metal layers and provide a 3D-image of the entire routing without destroying the device, but the research on this subject is still at an early stage.

Also see [86] and [52, 63], and [53].

8 Unforgeable Attestation

In the context of TEEs, attestation can be thought of as a proof provided by the hardware that proves that a specific software binary is loaded into a specific execution environment that will

[7] See comment at https://github.com/sbellem/qtee/issues/2#issuecomment-1464600086

guarantee the integrity and confidentiality of the computations, programmed in the software binary. Hence, they are two parts to the attestation:

- Proof of legit hardware
- Proof of loaded software binary

TEEs like Intel SGX and Sanctum, implement the proof of legit hardware by using a signing key that is tied to a public key associated with the manufacturer. The signing key is secured by the hardware implementation and can only be accessed via a dedicated enclave; (quoting enclave for Intel SGX, and signing enclave for Sanctum). Neither Intel SGX nor Sanctum protect against physical side-channel attacks, such as differential power analysis (DPA) attacks, and it is therefore reasonable to assume that an attacker with physical access could extract the signing key and forge attestations (proofs). Needless to say that this is problematic.

A design that would be capable to withstand physical attacks could make use of PUFs to generate the signing key, as discussed in Section 3. In order to protect the key against attacks when it is used to sign attestations, masking and redundancy techniques could be used as discussed in Sections 4 and 5.

How can the hardware prove that it is legit, without relying on a trusted manufacturer? Using PUFs helps to secure the key, but it does not help with proving that the hardware is implemented as expected. If we could derive a PUF key from the entire circuitry of the chip, such that any modification to any part of the chip would cause the PUF to yield a different key, that would help towards making sure that the hardware wasn't modified maliciously. Techniques discussed in Section 7 must be used to provide a proof that the hardware was fabricated as expected.

Novel remote attestation schemes are presented in [37, 38, 46, 47, 107] and be worth reviewing in the context of this research. For a thorough and formal treatment of remote attestation in the more general context of control flow attestation, we recommend consulting [102], which also stresses the importance of considering physical attacks.

9 Roadmap: The Path Towards Crypto-Physically Secure TEEs

In this section we wish to explore the possible small steps that can be taken towards implementing a TEE that meets the challenges presented in Section 1.3.2. Some of these steps may also be worked in parallel. For instance, it's reasonable to envision making progress on the open source hardware front (Challenge 1), meanwhile making progress on verifying that a chip was fabricated as expected (proof-of-fabrication Challenge 2). Perhaps each challenge can be worked on separately, thus allowing the formation of specialized teams to research and develop towards improved TEEs. In the meantime, what does that mean for Web3 projects who wish to implement applications relying on TEEs? Must they wait for a new chip? Must they accept the flaws of current TEEs, and work arround them? We think there may be a middle way, where it's possible to complement current TEEs with emerging technologies like PUFs, thus resulting in a wide array of novel hybrid models. As a support to this argument, there are works that have already proposed this such as [125].

10 Conclusion

We have a lot of work to do!

Acknowledgements

We thank Thorben Moos, François-Xavier Standaert and Alex Obadia for valuable feedback.

References

[1] Free silicon foundation (f-si), https://wiki.f-si.org, accessed: 2024-09-25

[2] Google maintained open source pdks, https://open-source-pdks.readthedocs.io, accessed: 2024-09-25

[3] Hensoldt cyber, https://hensoldt-cyber.com/, accessed: 2024-09-30

[4] Hep alliance, https://hep-alliance.org, accessed: 2024-09-25

[5] The silicon salon - semiconductor solutions for cryptography, https://www.siliconsalon.info/, accessed: 2024-09-25

[6] Secure and sovereign: Open-source processor designs boosted by new hep project delivering free verification tools (4 2021), https://www.ihp-microelectronics.com/fileadmin/user_upload/PM_2021-14-04_Project_HEP_EN.pdf, accessed: 2024-09-25

[7] Acosta, A.J., Addabbo, T., Tena-Sánchez, E.: Embedded electronic circuits for cryptography, hardware security and true random number generation: an overview. International Journal of Circuit Theory and Applications **45**(2), 145–169 (2017)

[8] Aktas, E., Cohen, C., Eads, J., Forshaw, J., Wilhelm, F.: Intel trust domain extensions (tdx) security review. Tech. rep., Google technical report (2023)

[9] Alikhani, P., Brunner, N., Crépeau, C., Designolle, S., Houlmann, R., Shi, W., Yang, N., Zbinden, H.: Experimental relativistic zero-knowledge proofs. Nature **599**(7883), 47–50 (2021)

[10] Ansell, T., Saligane, M.: The missing pieces of open design enablement: A recent history of google efforts. In: Proceedings of the 39th International Conference on Computer-Aided Design. pp. 1–8 (2020)

[11] Armknecht, F., Maes, R., Sadeghi, A.R., Sunar, B., Tuyls, P.: Memory leakage-resilient encryption based on physically unclonable functions. Towards Hardware-Intrinsic Security: Foundations and Practice pp. 135–164 (2010)

[12] Bar-El, H., Choukri, H., Naccache, D., Tunstall, M., Whelan, C.: The sorcerer's apprentice guide to fault attacks. Proceedings of the IEEE **94**(2), 370–382 (2006). https://doi.org/10.1109/JPROC.2005.862424

[13] Batina, L., Chmielewski, L., Haase, B., Samwel, N., Schwabe, P.: Sok: Sca-secure ECC in software - mission impossible? IACR Trans. Cryptogr. Hardw. Embed. Syst. **2023**(1), 557–589 (2023). https://doi.org/10.46586/TCHES.V2023.I1.557-589, https://doi.org/10.46586/tches.v2023.i1.557-589

[14] Bellemare, S., Miller, A.: Thoughts on current trusted hardware core problems (2023), https://github.com/sbellem/qtee/issues/2, accessed: 2024-09-12

[15] Birkholz, H., Thaler, D., Richardson, M., Smith, N., Pan, W.: Remote ATtestation procedureS (RATS) Architecture. RFC 9334 (Jan 2023). https://doi.org/10.17487/RFC9334, https://www.rfc-editor.org/info/rfc9334

[16] Brassard, G.: Relativity could ensure security for cash machines (2021)

[17] Buschkowski, F., Sasdrich, P., Güneysu, T.: Easimask-towards efficient, automated, and secure implementation of masking in hardware. In: 2023 Design, Automation & Test in Europe Conference & Exhibition (DATE). pp. 1–6 (2023). https://doi.org/10.23919/DATE56975.2023.10137330

[18] Cannon, A., Farheen, T., Roy, S., Tajik, S., Forte, D.: Protection against physical attacks through self-destructive polymorphic latch. In: 2023 IEEE/ACM International Conference on Computer Aided Design (ICCAD). pp. 1–9 (2023). https://doi.org/10.1109/ICCAD57390.2023.10323716

[19] Cassiers, G., Masure, L., Momin, C., Moos, T., Standaert, F.X.: Prime-field masking in hardware and its soundness against low-noise sca. IACR Transactions on Cryptographic Hardware and Embedded Systems **2023**(2), 482–518 (Mar 2023). https://doi.org/10.46586/tches.v2023.i2.482-518, https://tches.iacr.org/index.php/TCHES/article/view/10291

[20] Cassiers, G., Grégoire, B., Levi, I., Standaert, F.X.: Hardware private circuits: From trivial composition to full verification. IEEE Transactions on Computers **70**(10), 1677–1690 (2021). https://doi.org/10.1109/TC.2020.3022979

[21] Cassiers, G., Momin, C., Standaert, F.X., Udvarhelyi, B., Bronchain, O., Mangard, S., Oswald, E., Schwabe, P.: The secure cryptographic implementation association. https://www.simple-crypto.org/about/vision/, accessed: 2024-07-21

[22] Cassiers, G., Standaert, F.X.: Provably secure hardware masking in the transition- and glitch-robust probing model: Better safe than sorry. IACR Transactions on Cryptographic Hardware and Embedded Systems **2021, Issue 2**, 136–158 (2021). https://doi.org/10.46586/tches.v2021.i2.136-158, https://tches.iacr.org/index.php/TCHES/article/view/8790

[23] CERN: Cern open hardware licence. https://ohwr.org/project/cernohl, accessed: 2024-07-23

[24] CERN: Cern launches open hardware initiative. https://web.archive.org/web/20120701165927/http://public.web.cern.ch/Press/PressReleases/Releases2011/PR08.11E.html (2011), accessed: 2024-07-23

[25] Chari, S., Jutla, C.S., Rao, J.R., Rohatgi, P.: Towards sound approaches to counteract power-analysis attacks. In: Wiener, M. (ed.) Advances in Cryptology — CRYPTO' 99. pp. 398–412. Springer Berlin Heidelberg, Berlin, Heidelberg (1999)

[26] Chen, J., Jiang, I.H.R., Jung, J., Kahng, A.B., Kim, S., Kravets, V.N., Li, Y.L., Varadarajan, R., Woo, M.: Datc rdf-2021: Design flow and beyond iccad special session paper. In: 2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD). pp. 1–6 (2021). https://doi.org/10.1109/ICCAD51958.2021.9643553

[27] Cheng, H., Page, D., Wang, W.: eliminate: a leakage-focused ise for masked implementation. IACR Transactions on Cryptographic Hardware and Embedded Systems **2024**(2), 329–358 (Mar 2024). https://doi.org/10.46586/tches.v2024.i2.329-358, https://tches.iacr.org/index.php/TCHES/article/view/11431

[28] Chowdhury, S., Covic, A., Acharya, R.Y., Dupee, S., Ganji, F., Forte, D.: Physical security in the post-quantum era: A survey on side-channel analysis, random number generators, and physically unclonable functions. Journal of Cryptographic Engineering pp. 1–37 (2021)

[29] Chuang, K.: Highly reliable physically unclonable functions: Design, characterization and security analysis. Ph.D. thesis, Ph. D. thesis, KU Leuven, Leuven, Belgium (2020)

[30] Chuang, K.H., Bury, E., Degraeve, R., Kaczer, B., Linten, D., Verbauwhede, I.: A physically unclonable function using soft oxide breakdown featuring 0native ber and 51.8 fj/bit in 40-nm cmos. IEEE Journal of Solid-State Circuits **54**(10), 2765–2776 (2019). https://doi.org/10.1109/JSSC.2019.2920714

[31] Chuang, K.K.H., Chen, H.M., Wu, M.Y., Yang, E.C.S., Hsu, C.C.H.: Quantum tunneling puf: A chip fingerprint for hardware security. In: 2021 International Symposium on VLSI Technology, Systems and Applications (VLSI-TSA). pp. 1–2 (2021). https://doi.org/10.1109/VLSI-TSA51926.2021.9440114

[32] Ciani, M., Parisi, E., Musa, A., Barchi, F., Bartolini, A., Kulmala, A., Psiakis, R., Garofalo, A., Acquaviva, A., Davide, R.: Unleashing opentitan's potential: a silicon-ready embedded secure element for root of trust and cryptographic offloading. ACM Trans. Embed. Comput. Syst. (sep 2024). https://doi.org/10.1145/3690823, https://doi.org/10.1145/3690823, just Accepted

[33] Costan, V., Devadas, S.: Intel SGX explained. Cryptology ePrint Archive, Paper 2016/086 (2016), https://eprint.iacr.org/2016/086, https://eprint.iacr.org/2016/086

[34] Costan, V., Lebedev, I., Devadas, S.: Sanctum: Minimal hardware extensions for strong software isolation. In: 25th USENIX Security Symposium (USENIX Security 16). pp. 857–874. USENIX Association, Austin, TX (Aug 2016), https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/costan

[35] Costan, V., Lebedev, I., Devadas, S.: Secure processors part ii: Intel sgx security analysis and mit sanctum architecture. Foundations and Trends® in Electronic Design Automation **11**(3), 249–361 (2017). https://doi.org/10.1561/1000000052, http://dx.doi.org/10.1561/1000000052

[36] Delvaux, J.: Security analysis of puf-based key generation and entity authentication. Ph. D. dissertation (2017)

[37] van Dijk, M., Gurevin, D., Jin, C., Khan, O., Nguyen, P.H.: Autonomous secure remote attestation even when all used and to be used digital keys leak. Cryptology ePrint Archive, Paper 2021/602 (2021), https://eprint.iacr.org/2021/602, https://eprint.iacr.org/2021/602

[38] van Dijk, M., Jin, C.: A theoretical framework for the analysis of physical unclonable function interfaces and its relation to the random oracle model. Journal of Cryptology **36**(4), 35 (2023)

[39] Doctorow, C.: The battle for ring zero. https://pluralistic.net/2022/01/30/ring-minus-one/#drm-political-economy, accessed: 2024-07-20

[40] Edwards, A.J., Hassan, N., Arzate, J.D., Chin, A.N., Bhattacharya, D., Shihab, M.M., Zhou, P., Hu, X., Atulasimha, J., Makris, Y., Friedman, J.S.: Physically secure logic locking with nanomagnet logic. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems pp. 1–1 (2024). https://doi.org/10.1109/TCAD.2024.3434362

[41] Edwards, R.T.: Google/skywater and the promise of the open pdk. In: Workshop on Open-Source EDA Technology (2020)

[42] Fyrbiak, M., Wallat, S., Déchelotte, J., Albartus, N., Böcker, S., Tessier, R., Paar, C.: On the difficulty of fsm-based hardware obfuscation. IACR Transactions on Cryptographic Hardware and Embedded Systems **2018**(3), 293–330 (Aug 2018). https://doi.org/10.13154/tches.v2018.i3.293-330, https://tches.iacr.org/index.php/TCHES/article/view/7277

[43] Ganorkar, A.M., Sahula, V.: Error correction using pufs for reliable key generation. In: 2022 IEEE International Symposium on Smart Electronic Systems (iSES). pp. 643–646 (2022). https://doi.org/10.1109/iSES54909.2022.00142

[44] Gao, S., Großschädl, J., Marshall, B., Page, D., Pham, T.H., Regazzoni, F.: An instruction set extension to support software-based masking. IACR Transactions on Cryptographic Hardware and Embedded Systems **2021**(4), 283–325 (Aug 2021). https://doi.org/10.46586/tches.v2021.i4.283-325, https://tches.iacr.org/index.php/TCHES/article/view/9067

[45] Gassend, B., Clarke, D., van Dijk, M., Devadas, S.: Silicon physical random functions. In: Proceedings of the 9th ACM Conference on Computer and Communications Security. p. 148–160. CCS '02, Association for Computing Machinery, New York, NY, USA (2002). https://doi.org/10.1145/586110.586132, https://doi.org/10.1145/586110.586132

[46] Ghaeini, H.R., Chan, M., Bahmani, R., Brasser, F., Garcia, L., Zhou, J., Sadeghi, A.R., Tippenhauer, N.O., Zonouz, S.: PAtt: Physics-based attestation of control systems. In: 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019). pp. 165–180. USENIX Association, Chaoyang District, Beijing (Sep 2019), https://www.usenix.org/conference/raid2019/presentation/ghaeini

[47] Gurevin, D., Jin, C., Nguyen, P.H., Khan, O., van Dijk, M.: Secure remote attestation with strong key insulation guarantees. IEEE Transactions on Computers pp. 1–12 (2023). https://doi.org/10.1109/TC.2023.3290870

[48] Hadžić, V., Cassiers, G., Primas, R., Mangard, S., Bloem, R.: Quantile: Quantifying information leakage. IACR Transactions on Cryptographic Hardware and Embedded Systems **2024**(1), 433–456 (Dec 2023). https://doi.org/10.46586/tches.v2024.i1.433-456, https://tches.iacr.org/index.php/TCHES/article/view/11258

[49] Hannig, F., Teich, J.: Open source hardware. Computer **54**(10), 111–115 (2021). https://doi.org/10.1109/MC.2021.3099046

[50] Herman, K., Montanares, M., Marin, J.: Design and implementation of integrated circuits using open source tools and sky130 free pdk. In: 2023 30th International Conference on Mixed Design of Integrated Circuits and System (MIXDES). pp. 105–110 (2023). https://doi.org/10.23919/MIXDES58562.2023.10203216

[51] Herman, K., Scholz, R., Andreev, S.: Reflections on the first european open source pdk by ihp - experiences after one year and future activities. In: 2024 31st International Conference on Mixed Design of Integrated Circuits and System (MIXDES). pp. 19–22 (2024). https://doi.org/10.23919/MIXDES62605.2024.10614043

[52] Holler, M., Odstrcil, M., Guizar-Sicairos, M., Lebugle, M., Müller, E., Finizio, S., Tinti, G., David, C., Zusman, J., Unglaub, W., et al.: Three-dimensional imaging of integrated circuits with macro-to nanoscale zoom. Nature Electronics **2**(10), 464–470 (2019)

[53] 'bunnie' Huang, A.: Infra-red, in-situ (iris) inspection of silicon (2023), https://arxiv.org/abs/2303.07406

[54] Hughes, E.: A cypherpunk's manifesto. https://www.activism.net/cypherpunk/manifesto.html, accessed: 2024-07-20

[55] Islam, M.N., Kundu, S.: Enabling ic traceability via blockchain pegged to embedded puf. ACM Trans. Des. Autom. Electron. Syst. **24**(3) (Apr 2019). https://doi.org/10.1145/3315669, https://doi.org/10.1145/3315669

[56] Islam, M.N., Patii, V.C., Kundu, S.: On ic traceability via blockchain. In: 2018 International Symposium on VLSI Design, Automation and Test (VLSI-DAT). pp. 1–4 (2018). https://doi.org/10.1109/VLSI-DAT.2018.8373269

[57] Jadon, S., Rao, A., Jagadish, N., Nadakatti, S., R., T., Honnavalli, P.B.: Blockchain in the electronics industry for supply chain management: A survey. IEEE Access **12**, 7089–7120 (2024). https://doi.org/10.1109/ACCESS.2024.3351370

[58] Jaramillo-Toral, U., Garcia-Lopez, J.C., Ortega-Cisneros, S., Baungarten-Leon, E.I., Torres-González, C., Sandoval-Ibarra, F.: Automated ic design flow using open-source tools and 180 nm pdk. In: 2024 IEEE 67th International Midwest Symposium on Circuits and Systems (MWSCAS). pp. 1393–1397. IEEE (2024)

[59] Kahng, A.B.: Leveling up: A trajectory of openroad, tilos and beyond. In: Proceedings of the 2022 International Symposium on Physical Design. p. 73–79. ISPD '22, Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3505170.3511479, https://doi.org/10.1145/3505170.3511479

[60] Kahng, A.B., Spyrou, T.: The openroad project: Unleashing hardware innovation. In: Proc. GOMAC (2021)

[61] Karakoyunlu, D., Sunar, B.: Differential template attacks on puf enabled cryptographic devices. In: 2010 IEEE International Workshop on Information Forensics and Security. pp. 1–6. IEEE (2010)

[62] Karimi, N., Basu, K., Chang, C.H., Fung, J.M.: Hardware security in emerging technologies: Vulnerabilities, attacks, and solutions. IEEE Journal on Emerging and Selected Topics in Circuits and Systems **11**(2), 223–227 (2021). https://doi.org/10.1109/JETCAS.2021.3084498

[63] Karpov, D., Djeghdi, K., Holler, M., Abdollahi, S.N., Godlewska, K., Donnelly, C., Yuasa, T., Sai, H., Wiesner, U., Wilts, B., et al.: High-resolution three-dimensional imaging of topological textures in nanoscale single-diamond networks. Nature Nanotechnology pp. 1–8 (2024)

[64] Kerckhoffs, A.: La cryptographie militaire. https://www.petitcolas.net/kerckhoffs/la_cryptographie_militaire_i.htm (1883), accessed: 2024-07-22

[65] Kilbourn, Q.: Project t-tee: From trusted to trustless execution environments. https://collective.flashbots.net/t/project-t-tee-from-trusted-to-trustless-execution-environments/3541/1 (2024), accessed: 2024-07-24

[66] Kilbourn, Q., Miller, A.: Debunking tee fud: A brief defense of the use of tees in crypto. https://collective.flashbots.net/t/debunking-tee-fud-a-brief-defense-of-the-use-of-tees-in-crypto/2931 (2024), accessed: 2024-07-24

[67] Kim, I., Maiti, A., Nazhandali, L., Schaumont, P., Vivekraja, V., Zhang, H.: From statistics to circuits: Foundations for future physical unclonable functions. Towards Hardware-Intrinsic Security: Foundations and Practice pp. 55–78 (2010)

[68] Kim, Y., Bielecki, J., Sikorski, M., de Wijn, R., Fortmann-Grote, C., Sztuk-Dambietz, J., Koliyadu, J., Letrun, R., Kirkwood, H., Sato, T., et al.: Expected resolution limits of x-ray free-electron laser single-particle imaging for realistic source and detector properties. Structural Dynamics **9**(6) (2022)

[69] Koblah, D.S., Ganji, F., Mehta, D., Forte, D., Hashemi, M.: Eda workflow for optimization of robust model probing-compliant masked hardware gadgets

[70] Kraleva, L., Mahzoun, M., Posteuca, R., Toprakhisar, D., Ashur, T., Verbauwhede, I.: Cryptanalysis of strong physically unclonable functions. IEEE Open Journal of the Solid-State Circuits Society **3**, 32–40 (2023). https://doi.org/10.1109/OJSSCS.2022.3227009

[71] Kulkarni, A., Hazari, N.A., Niamat, M.Y.: A zero trust-based framework employing blockchain technology and ring oscillator physical unclonable functions for security of field programmable gate array supply chain. IEEE Access **12**, 89322–89338 (2024). https://doi.org/10.1109/ACCESS.2024.3418572

[72] Lai, X., Jenihhin, M., Selimis, G., Goossens, S., Maes, R., Paul, K.: Early rtl analysis for sca vulnerability in fuzzy extractors of memory-based puf enabled devices. In: 2020 IFIP/IEEE 28th International Conference on Very Large Scale Integration (VLSI-SOC). pp. 16–21 (2020). https://doi.org/10.1109/VLSI-SOC46417.2020.9344071

[73] Lebedev, I., Hogan, K., Devadas, S.: Invited paper: Secure boot and remote attestation in the sanctum processor. In: 2018 IEEE 31st Computer Security Foundations Symposium (CSF). pp. 46–60 (2018). https://doi.org/10.1109/CSF.2018.00011

[74] Lee, D., Kohlbrenner, D., Shinde, S., Asanović, K., Song, D.: Keystone: an open framework for architecting trusted execution environments. In: Proceedings of the Fifteenth European Conference on Computer Systems. EuroSys '20, Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3342195.3387532, https://doi.org/10.1145/3342195.3387532

[75] Van der Leest, V., Guilley, S., Baili, I., Le Guyader, M., Kyung Lee, T.: Root of trust (December 2021), https://www.synopsys.com/dw/doc.php/wp/gsa-end-to-end-traceability-of-ip-wp.pdf, accessed: 2024-09-30

[76] Library, J.I.: Application of attack potential to hardware devices with security boxes. https://www.sogis.eu/documents/cc/domains/hardware_devices/JIL-Application-of-Attack-Potential-to-Hardware-Devices-with-Security-Boxes-v3.1.pdf (2023), accessed: 2024-07-24

[77] Maes, R., Maes, R.: Physically unclonable functions: Concept and constructions. Springer (2013)

[78] Maes, R., Verbauwhede, I.: Physically unclonable functions: A study on the state of the art and future research directions. Towards Hardware-Intrinsic Security: Foundations and Practice pp. 3–37 (2010)

[79] Mangard, S., Oswald, E., Popp, T.: Power analysis attacks: Revealing the secrets of smart cards, vol. 31. Springer Science & Business Media (2008)

[80] May, T.C.: The crypto anarchist manifesto. https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html, accessed: 2024-07-20

[81] Medinceanu, P.C., Enachescu, M.: Open skywater130nm pdk-based ip development platform: A pwm peripheral case study. In: 2024 IEEE 22nd Mediterranean Electrotechnical Conference (MELECON). pp. 856–861 (2024). https://doi.org/10.1109/MELECON56669.2024.10608632

[82] Mentens, N.: Hardware security in the era of emerging device and system technologies. IEEE Security & Privacy **22**(3), 4–6 (2024). https://doi.org/10.1109/MSEC.2024.3379768

[83] Meza, A., Restuccia, F., Oberg, J., Rizzo, D., Kastner, R.: Security verification of the opentitan hardware root of trust. IEEE Security & Privacy **21**(3), 27–36 (2023). https://doi.org/10.1109/MSEC.2023.3251954

[84] Momin, C., Cassiers, G., Standaert, F.X.: Handcrafting: Improving automated masking in hardware with manual optimizations. In: International Workshop on Constructive Side-Channel Analysis and Secure Design. pp. 257–275. Springer (2022)

[85] Moos, T., Saha, S., Standaert, F.X.: Prime masking vs. faults - exponential security amplification against selected classes of attacks. IACR Transactions on

Cryptographic Hardware and Embedded Systems **2024**(4), 690–736 (Sep 2024). https://doi.org/10.46586/tches.v2024.i4.690-736, https://tches.iacr.org/index.php/TCHES/article/view/11807

[86] Mosavirik, T., Monfared, S.K., Safa, M.S., Tajik, S.: Silicon echoes: Non-invasive trojan and tamper detection using frequency-selective impedance analysis. IACR Transactions on Cryptographic Hardware and Embedded Systems **2023**(4), 238–261 (Aug 2023). https://doi.org/10.46586/tches.v2023.i4.238-261, https://tches.iacr.org/index.php/TCHES/article/view/11165

[87] Nakano, M., Miyashita, O., Tama, F.: Molecular size dependence on achievable resolution from xfel single-particle 3d reconstruction. Structural Dynamics **10**(2) (2023)

[88] OpenRoad: Supply chain and hardware security using open-source solutions. https://theopenroadproject.org/supply-chain-and-hardware-security-using-open-source-solutions/ (2024), accessed: 2024-09-19

[89] Pappu, R., Recht, B., Taylor, J., Gershenfeld, N.: Physical one-way functions. Science **297**(5589), 2026–2030 (2002). https://doi.org/10.1126/science.1074376, https://www.science.org/doi/abs/10.1126/science.1074376

[90] Parisi, E., Musa, A., Ciani, M., Barchi, F., Rossi, D., Bartolini, A., Acquaviva, A.: Assessing the performance of opentitan as cryptographic accelerator in secure open-hardware system-on-chips. In: Proceedings of the 21st ACM International Conference on Computing Frontiers. p. 172–179. CF '24, Association for Computing Machinery, New York, NY, USA (2024). https://doi.org/10.1145/3649153.3649213, https://doi.org/10.1145/3649153.3649213

[91] Pehl, C.M.: Design, evaluation, and application of security primitives that are based on hardware-intrinsic features (2024)

[92] Puschner, E., Moos, T., Becker, S., Kison, C., Moradi, A., Paar, C.: Red team vs. blue team: A real-world hardware trojan detection case study across four modern cmos technology generations. In: 2023 IEEE Symposium on Security and Privacy (SP). pp. 56–74. IEEE Computer Society, Los Alamitos, CA, USA (may 2023). https://doi.org/10.1109/SP46215.2023.10179341, https://doi.ieeecomputersociety.org/10.1109/SP46215.2023.10179341

[93] Rabimba, K., Xu, L., Chen, L., Zhang, F., Gao, Z., Shi, W.: Lessons learned from blockchain applications of trusted execution environments and implications for future research. In: Workshop on Hardware and Architectural Support for Security and Privacy. HASP '21, ACM (Oct 2021). https://doi.org/10.1145/3505253.3505259, http://dx.doi.org/10.1145/3505253.3505259

[94] Rahman, M.T., Tajik, S., Rahman, M.S., Tehranipoor, M., Asadizanjani, N.: The key is left under the mat: On the inappropriate security assumption of logic locking schemes. In: 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). pp. 262–272 (2020). https://doi.org/10.1109/HOST45689.2020.9300258

[95] Rajendran, J.J., Garg, S.: Logic Encryption, pp. 71–88. Springer International Publishing, Cham (2017), https://doi.org/10.1007/978-3-319-49019-9_3

[96] Rekha, S.S., Suraj, K., Sudeendra Kumar, K.: A holistic blockchain based ic traceability technique. In: 2021 IEEE International Symposium on Smart Electronic Systems (iSES). pp. 307–310 (2021). https://doi.org/10.1109/iSES52644.2021.00078

[97] Rogaway, P.: The moral character of cryptographic work. USENIX Association, Austin, TX (Aug 2016)

[98] Samuel Russell, P.P., Alaeen, S., Pogorelov, T.V.: In-cell dynamics: the next focus of all-atom simulations. The Journal of Physical Chemistry B **127**(46), 9863–9872 (2023)

[99] Saraza-Canflanca, P., Fodor, F., Diaz-Fortuny, J., Gierlichs, B., Degraeve, R., Kaczer, B., Verbauwhede, I., Bury, E.: Unveiling the vulnerability of oxide-breakdown-based puf. IEEE Electron Device Letters **45**(5), 750–753 (2024). https://doi.org/10.1109/LED.2024.3369860

[100] Schneider, M., Masti, R.J., Shinde, S., Capkun, S., Perez, R.: Sok: Hardware-supported trusted execution environments (2022), https://arxiv.org/abs/2205.12742

[101] Scholz, R., Andreev, S., Herman, K.: Update on ihp open pdk initiative & how to submit free open source designs in ihp technology. https://wiki.f-si.org/images/4/4d/Scholz_Andreev_Herman.pdf, accessed: 2024-07-23

[102] Sha, Z., Shepherd, C., Rafi, A., Markantonakis, K.: Control-flow attestation: Concepts, solutions, and open challenges (2024), https://arxiv.org/abs/2408.06304

[103] Shakya, B., Tehranipoor, M.M., Bhunia, S., Forte, D.: Introduction to hardware obfuscation: Motivation, methods and evaluation pp. 3–32 (2017), https://doi.org/10.1007/978-3-319-49019-9_1

[104] Shepherd, C., Arfaoui, G., Gurulian, I., Lee, R.P., Markantonakis, K., Akram, R.N., Sauveron, D., Conchon, E.: Secure and trusted execution: Past, present, and future - a critical review in the context of the internet of things and cyber-physical systems. In: 2016 IEEE Trustcom/BigDataSE/ISPA. pp. 168–177 (2016). https://doi.org/10.1109/TrustCom.2016.0060

[105] Shepherd, C., Markantonakis, K.: Trusted execution environments (2024)

[106] Shepherd, C., Markantonakis, K., van Heijningen, N., Aboulkassimi, D., Gaine, C., Heckmann, T., Naccache, D.: Physical fault injection and side-channel attacks on mobile devices: A comprehensive analysis. Comput. Secur. **111**(C) (Dec 2021). https://doi.org/10.1016/j.cose.2021.102471, https://doi.org/10.1016/j.cose.2021.102471

[107] Shepherd, C., Markantonakis, K., Jaloyan, G.A.: Lira-v: Lightweight remote attestation for constrained risc-v devices. In: 2021 IEEE Security and Privacy Workshops (SPW). pp. 221–227 (2021). https://doi.org/10.1109/SPW53761.2021.00036

[108] Stransky, M., Shen, Z., Jurek, Z., Fortmann-Grote, C., Bean, R., Santra, R., Ziaja, B., Mancuso, A.P., et al.: Water layer and radiation damage effects on the orientation recovery of proteins in single-particle imaging at an x-ray free-electron laser. Scientific reports **13**(1), 1–11 (2023)

[109] Subramanyan, P., Sinha, R., Lebedev, I., Devadas, S., Seshia, S.A.: A formal foundation for secure remote execution of enclaves. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. p. 2435–2450. CCS '17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3133956.3134098, https://doi.org/10.1145/3133956.3134098

[110] Sweeney, J., Garg, D., Pileggi, L.: Quantifying the efficacy of logic locking methods. In: 2024 37th International Conference on VLSI Design and 2024 23rd International Conference on Embedded Systems (VLSID). pp. 541–546 (2024). https://doi.org/10.1109/VLSID60093.2024.00096

[111] Tajik, S., Schaumont, P.: The technological arms race in hardware security. In: 2022 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI). pp. 303–308 (2022). https://doi.org/10.1109/EMCSI39492.2022.9889394

[112] Team, O., Team, K.: Towards an open-source secure enclave. https://medium.com/oasislabs/towards-an-open-source-secure-enclave-659ac27b871a (2018), accessed: 2024-09-16

[113] Tebelmann, L., Pehl, M., Sigl, G.: Em side-channel analysis of bch-based error correction for puf-based key generation. In: Proceedings of the 2017 Workshop on Attacks and Solutions in Hardware Security. pp. 43–52 (2017)

[114] Technologies, P.: Autonomous tee manifesto. https://poeticte.ch/posts/autonomous-TEEs-manifesto.html (2024), accessed: 2024-07-24

[115] Technologies, P.: Poetic intents: Seeding the next generation of tees (September 2024), https://poeticte.ch/posts/poetic-intents.html, accessed: 2024-09-28

[116] Tehranipoor, M., Zamiri Azar, K., Asadizanjani, N., Rahman, F., Mardani Kamali, H., Farahmandi, F.: Advances in Logic Locking, pp. 53–142. Springer Nature Switzerland, Cham (2024), https://doi.org/10.1007/978-3-031-58687-3_2

[117] Tehranipoor, M., Sunar, B.: Hardware trojan horses. Towards Hardware-Intrinsic Security: Foundations and Practice pp. 167–187 (2010)

[118] Uhle, F., Stolz, F., Moradi, A.: Another evidence to not employ customized masked hardware: Identifying and fixing flaws in scarv. IACR Transactions on Cryptographic Hardware and Embedded Systems **2024**(4), 133–155 (Sep 2024). https://doi.org/10.46586/tches.v2024.i4.133-155, https://tches.iacr.org/index.php/TCHES/article/view/11786

[119] Wang, P.F., Zhang, E.X., Chuang, K.H., Liao, W., Gong, H., Wang, P., Arutt, C.N., Ni, K., Mccurdy, M.W., Verbauwhede, I., Bury, E., Linten, D., Fleetwood, D.M., Schrimpf, R.D., Reed, R.A.: X-ray and proton radiation effects on 40 nm cmos physically unclonable function devices. IEEE Transactions on Nuclear Science **65**(8), 1519–1524 (2018). https://doi.org/10.1109/TNS.2017.2789160

[120] Weber, A., Guilley, S., Rathfelder, R., Stöttinger, M., Lüth, C., Malenko, M., Grawunder, T., Reith, S., Puccetti, A., Seifert, J.P., Herfurth, N., Sankowski, H., Heiser, G.: Verified value chains, innovation and competition. In: 2023 IEEE International Conference on Cyber Security and Resilience (CSR). pp. 470–476 (2023). https://doi.org/10.1109/CSR57506.2023.10224911

[121] Wu, M.Y., Yang, T.H., Chen, L.C., Lin, C.C., Hu, H.C., Su, F.Y., Wang, C.M., Huang, J.P.H., Chen, H.M., Lu, C.C.H., Yang, E.C.S., Shen, R.S.J.: A puf scheme using competing oxide rupture with bit error rate approaching zero. In: 2018 IEEE International Solid-State Circuits Conference - (ISSCC). pp. 130–132 (2018). https://doi.org/10.1109/ISSCC.2018.8310218

[122] Xu, X., Rahman, F., Shakya, B., Vassilev, A., Forte, D., Tehranipoor, M.: Electronics supply chain integrity enabled by blockchain. ACM Trans. Des. Autom. Electron. Syst. **24**(3) (May 2019). https://doi.org/10.1145/3315571, https://doi.org/10.1145/3315571

[123] Yang, B.: True random number generators for fpgas. PhD Thesis (2018)

[124] Zach: The missing silicon venture studio building chip companies could be so much easier. zach's tech blog (2024), https://www.zach.be/p/the-missing-silicon-venture-studio, accessed: 2024-09-26

[125] Zhang, X., Qin, K., Qu, S., Wang, T., Zhang, C., Gu, D.: Teamwork makes tee work: Open and resilient remote attestation on decentralized trust (2024), https://arxiv.org/abs/2402.08908

[126] Zhang, Z., Nikova, S., Nikov, V.: Glitch-stopping circuits: Hardware secure masking without registers. Cryptology ePrint Archive, Paper 2024/891 (2024). https://doi.org/10.1145/3658644.3670335, https://eprint.iacr.org/2024/891

[127] Šišejković, D., Leupers, R., Ascheid, G., Metzner, S.: A unifying logic encryption security metric. In: International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation (SAMOS). ACM (Jul 2018). https://doi.org/10.1145/3229631.3229636

[128] Šišejković, D., Merchant, F., Leupers, R., Ascheid, G., Kegreiß, S.: Inter-lock: Logic encryption for processor cores beyond module boundaries. In: 2019 IEEE European Test Symposium (ETS). pp. 1–6 (May 2019). https://doi.org/10.1109/ETS.2019.8791528

[129] Šišejković, D., Merchant, F., Leupers, R., Ascheid, G., Kiefer, V.: A critical evaluation of the paradigm shift in the design of logic encryption algorithms. 2019 International Symposium on VLSI Design, Automation and Test (VLSI-DAT) p. 4 (Apr 2019). https://doi.org/10.1109/VLSI-DAT.2019.8741531

[130] Šišejković, D., Merchant, F., Reimann, L.M., Leupers, R., Kegreiß, S.: Scaling logic locking schemes to multi-module hardware designs. Architecture of Computing Systems (ARCS 2020) pp. 138–152 (2020), https:/doi.org/10.1007/978-3-030-52794-5_11