OBFSCURO: A Commodity Obfuscation Engine on Intel SGX

Adil Ahmad1,·, Byunggill Joe2,·,†, Yuan Xiao3, Yinqian Zhang3, Insik Shin2, and Byoungyoung Lee1,4

1Purdue University
2KAIST
3Ohio State University
4Seoul National University

Abstract—Program obfuscation is a popular cryptographic construct with a wide range of uses such as IP theft prevention. Although cryptographic solutions for program obfuscation impose impractically high overheads, a recent breakthrough in systematically leveraging trusted hardware has shown promise. However, the existing solution is based on special-purpose trusted hardware, restricting its use-cases to a limited few.

In this paper, we first study if such obfuscation is feasible based on commodity trusted hardware, Intel SGX, and we observe that certain important security considerations are not afforded by commodity hardware. In particular, we found that existing obfuscation/obliviousness schemes are insecure if directly applied to the SGX environment mainly due to the side-channel limitations. To this end, we present OBFSCURO, the first system providing program obfuscation using commodity trusted hardware, Intel SGX. The key idea is to leverage ORAM-based operations to perform secure code execution and data access. Initially, OBFSCURO transforms the regular program layout into a side-channel-secure and ORAM-compatible layout. Then, OBFSCURO ensures that its ORAM controller always performs data oblivious accesses in order to protect itself from the side-channel attacks. Furthermore, OBFSCURO ensures that the program is secure from timing-based attacks by ensuring that the program always runs for a pre-configured time interval. Along the way, OBFSCURO also introduces a systematic optimization such as register-based ORAM stash. We provide a thorough security analysis of OBFSCURO along with empirical attack evaluations showing that OBFSCURO can protect the SGX program execution from being leaked by access pattern-based and timing-based channels. We also provide a detailed performance benchmark results in order to show the practical aspects of OBFSCURO.

I. INTRODUCTION

Program obfuscation [5, 29] is a popular cryptographic construct which has interesting and wide-ranging applications towards protecting the intellectual property of a software program. As computing trends are rapidly shifting towards cloud-based computing, there is a strong need for systems supporting such a notion of program obfuscation. This need arises from various use-cases where computing is offloaded to remote clouds and the owner of the program desires to shield his/her proprietary algorithm from the cloud providers and/or other tenants. For example, consider a company like 23andMe [2] which could easily outsource its large genomic computations to the cloud without having to worry about the theft of their algorithm.

In program obfuscation, a sender, who owns a program, transforms the program to create an obfuscated version of the program which is functionally identical to the original version, but it always runs for a fixed time before returning an output. The sender then sends this obfuscated program to a receiver. After that, the receiver runs the obfuscated program within a blackbox-like environment—the receiver cannot see (and infer) any intermediate computational results and/or footprints of the obfuscated program. Consequently, although the receiver can keep running the obfuscated program using any input of his/her choice, the receiver learns nothing about the original program. Therefore, as far as the attacker is concerned, he/she is interacting with a virtual blackbox, which only takes an input and returns the resulting output.

In this sphere, there has been significant (mostly cryptographic) research [7, 11, 16, 25] efforts in achieving the program obfuscation, specifically through additional trust on the underlying system. Recently, there has been a systematic breakthrough, HOP [47], in achieving program obfuscation through relaxed assumptions on trust on the underlying hardware. However, HOP relies on special-purpose hardware, severely limiting its practicality. In particular, their system relies on custom RISC-V processors to conveniently transplant the root of trust to implement the core security logic and securely contain the program code. We believe such convenience is not free—it would be challenging and unrealistic to deploy such custom-built hardware to a majority of end-user machines or cloud-computing machines.

In this paper, we propose OBFSCURO, the first system achieving program obfuscation on commodity hardware. Unlike the previous work relying on special-purpose hardware, OBFSCURO is specifically designed to run on Intel SGX, already shipped with millions of machines in the market. The general idea behind OBFSCURO is similar to HOP—it strictly observes the security protocol of Oblivious RAM (ORAM) [23] to support secure code/data accesses between CPU and memory subsystems, because the trusted boundary of Intel SGX only includes CPU itself and excludes memory subsystems. The novelty of OBFSCURO comes from several challenges in supporting such program obfuscation on Intel SGX, ironically
because it has to run on commodity hardware. Intel SGX includes many other features that can be abused to invalidate a key security assumption behind program obfuscation (i.e., the obfuscated program should be running within a blackbox-like environment).

More specifically, researchers have identified that Intel SGX has critical access pattern-based side-channel security flaws. These allow adversaries to infer computational semantics within SGX thereby breaking the blackbox execution environment. Based various side-channels, namely page fault [68, 70], cache [8, 24, 57], and branch-prediction [40] attacks, attackers with high privileges, e.g., OS, can infer substantial information about the execution semantics of the enclave program. For example, previous work [57] has shown how cache attacks can be abused to leak an RSA private key from an enclave program.

As far as access pattern-based side-channels are concerned, the root cause of the problem is that it is challenging to completely hide memory access patterns from privileged adversaries in the current Intel SGX architecture. The reason for this is that the CPU is designed to rely on other subsystems to perform computation on given instructions. In particular, Intel SGX is not designed to secure communication patterns between the CPU and memory-management hardware units (e.g., the MMU/TLB, cache, DRAM, branch-predictors, etc.). For performance reasons, the communication channels and hardware units are designed to be partially shared between trusted and untrusted entities, allowing potentially adversarial entities to observe and collect memory traces exhibited by an SGX enclave.

To address these challenges, OBFSUCRU utilizes three main ideas. First, OBFSUCRU employs a data-oblivious ORAM implementation. Our work improves on the previously proposed secure ORAM implementations [3, 52, 55] by designing an efficient register-based stash. Second, OBFSUCRU designs side-channel resistant scratchpad-based code execution and data access models, in order to neutralize the memory access patterns observed by attackers as well as bridge the gap between traditional ORAM and native program execution. Lastly, OBFSUCRU ensures start-to-end obfuscation of the target programs by providing execution time normalization to all applications thereby protecting the programs against information leakage through timing-based channels.

Our implementation of OBFSUCRU is based on the LLVM compiler suite with an installed runtime library. Through compiler instrumentation, we transform a native SGX program’s code into cache-line-granular and ORAM-compatible basic blocks. OBFSUCRU enforces each basic block to have one data access, and one code access at fixed offsets within the basic blocks thereby neutralizing branch targets. The code and data access instructions are translated into equivalent jump instructions targeting OBFSUCRU’s runtime library functions. Then, OBFSUCRU’s runtime library obliviously serves the program with code and data blocks extracted from ORAM storage onto scratchpad memory regions called C-Pad and D-Pad respectively. The, the code execution and data access (related to the target program) is always performed at these locations, thereby neutralizing the program’s page table and cache footprints. Lastly, the program is instrumented to keep executing till a user-configured time interval has elapsed to mitigate the threat of timing channels.

Furthermore, we highlight that although OBFSUCRU’s performance overhead is quite high, it is still much faster than the state-of-the-art cryptographic obfuscation schemes. In particular, cryptographic obfuscation techniques (which rely on homomorphic encryption and/or circuit construction as security primitives) are still far away to be adopted in practice largely due to severe performances overheads or limited generality to support generic programs (detailed discussion in §IX). However, leveraging the root of trust in the underlying commodity hardware, OBFSUCRU demonstrates comparatively moderate performance overheads on real-world generic programs.

In broad terms, the contributions made by this paper can be described as follows:

- We dissect commodity-off-the-shelf hardware to find out the key hardware features which hinder the adoption of program obfuscation in Intel SGX. We also provide a comparison with existing work mentioning how their approaches are insecure or incomplete if directly applied within Intel SGX.
- We present, OBFSUCRU, the first program obfuscation system built on top of commodity hardware. Motivated by the hardware limitations of Intel SGX, OBFSUCRU provides a complete start-to-end program obfuscation solution which can be readily-adopted without any modifications to legacy code written for SGX programs by the program developer.
- We provide a thorough security analysis of OBFSUCRU showing how it can prevent information leakage through both access pattern-based and timing-based side-channels.
- We provide a performance comparison of OBFSUCRU using a diverse set of benchmarking applications as well as a real-world application, OpenSSL. Our experiments indicate that OBFSUCRU incurs an average overhead of $51 \times$ over native SGX execution for our custom benchmarks and an overhead of $16 - 57 \times$ while executing OpenSSL [20].

II. BACKGROUND

A. Intel SGX

Intel SGX is a new set of x86 instructions which have been commoditized after the Intel Skylake architecture. SGX allows user-level programs to create a protected memory region called an enclave which is inaccessible from other user-level programs as well as privileged components such as BIOS, OS, hypervisor, etc. The Enclave Page Cache (EPC) forms physical memory pages that are dedicated to enclaves. The CPU explicitly revokes access to EPC outside an enclave. Each enclave process is provided its own virtual address space which is divided into trusted and untrusted parts. The trusted part is allocated pages from the EPC to provide memory integrity and confidentiality. The page tables that deal with translation of virtual to physical pages for EPC pages can be updated by untrusted system components.

B. SGX Side-Channel Attacks

The three most prominent categories of side-channel attacks against Intel SGX are summarized as follows.

This is a preprint, and the final paper will appear in NDSS 2019.
Page Table Attacks. As with regular non-enclave processes, the untrusted OS handles page tables for the EPC pages to flexibly provision EPC resources. Previous works [68, 70] have shown that a privileged attacker can exploit page faults and page table walks in order to gain page-level granular insight into the execution of an enclave process. Since the OS handles the page tables, it can invalidate access onto all EPC pages which will result in page faults, thereby capturing trace of all page accesses performed by the enclave. Similarly, the attacker can monitor the access/dirty bit present within the page table to find out which page was last accessed without invoking a page fault.

Cache Attacks. Caches are designed to reduce the access latency of code and data by exploiting temporal and spatial locality of an application’s execution. The caches are divided into a number of cache-sets, which are further divided into fixed-size cache-lines (64 B). Recent reports [8, 24, 57] have shown that the SGX enclave is insecure against the Prime+Probe [50] attack. As part of this attack, the attacker runs an attack application which monitors the cache usage of a victim application, performing some security critical operations. During the Prime phase, the attacker fills one or more cache sets with his/her own data and during the Probe phase, he/she tries to access the data. If the victim has accessed any of these cache sets, it must have evicted some of the cache lines of the attacker, and subsequent access by the attacker will take longer time than if the lines had not been evicted. Therefore, an attacker, with prior knowledge of the victim application, can infer what operation took place (assuming different operations will access different cache sets).

Branch Prediction Attacks. Last Branch Record (LBR) saves the history of the recently taken branches which can be referenced by developers for further optimization. The LBR stores information including source/target address of a branch, and a flag whether the branch is taken or not, etc. SGX disables direct reporting of the LBR information outside the enclave. However, recent reports [40] have shown how it can be indirectly inferred from outside the enclave. To perform this attack, the attacker leverages prior information on the source and destinations of the branches in a target program. Next, the attacker writes a shadow code for a set of branches within the program. The attacker executes both victim and shadow code in parallel. Finally, the attacker monitors the shadow code for mis-predictions (penalized by extra CPU cycles), to figure out which branch was taken by the enclave.

C. ORAM

ORAM [23] is a well-known cryptographic technique which provides secure access to an encrypted memory region located in a remote and untrusted server. ORAM achieves secure memory access by (a) accessing multiple memory locations instead of a single memory location and (b) re-shuffling and re-encrypting the extracted memory regions with a random seed. Path ORAM [63] is an improved variant of ORAM which uses a binary tree-like formation to store the encrypted memory on the server. Each node within the tree is composed of K blocks, where K is a fixed number pre-defined during initialization. An ORAM tree contains both real blocks, i.e., with actual client data, and dummy blocks, i.e., with dummy data, meant to fool an attacker. The number of real blocks within a tree of L leafs can be at most L in order to provide the security guarantees of ORAM. The tree is stored within the untrusted storage in an encrypted format.

Using Path ORAM, the client runs an ORAM controller within a small, completely trusted memory region. There are two key data structures for Path ORAM, i.e., the Position map and the Stash. The position map can be a simple integer array, which links the real block to its corresponding leaf-index within the ORAM tree. Whenever the client needs to access a block from the ORAM tree, the ORAM controller finds the corresponding leaf from the position map and extracts the path from the root to the leaf. The extracted blocks are stored within the stash memory.

Figure 1 illustrates the Path ORAM algorithm. In this figure, the client attempts to access the block D from the untrusted storage containing the ORAM tree (1). First, the client looks-up the leaf index corresponding to block D, which is 11 in our example (2). Then, the client extracts the complete path from the root of the tree to the leaf (i.e., d1, d3, D) and saves it in the stash as shown. The dummy blocks (i.e., d1, d3) are discarded at this point to keep the stash size small. After accessing the block D, the client randomizes its position, i.e., initial leaf was 11 and final leaf is 10, and re-encrypts the block with a random seed (3). The client then tries to write-back to the tree from the old leaf (11) back to the root. To ensure consistency, the client only writes back a real block on a certain node, i.e., not all nodes, and re-encrypts the block with a random nonce and writes it to that node. For example, in the figure, (d4, d5) corresponds to the generated dummy data.

III. Threat Model

We assume a scenario where a user runs an SGX enclave program with some security-sensitive program. The enclave program, OBFSCURO’s runtime and compiler, and the CPU are the only trusted components, and all other software and hardware components (including operating systems, hypervisors, memory hardware units, etc.) are untrusted. The user’s goal is to ensure that the program’s logic is not leaked to any attacker observing the enclave’s execution. Therefore, the program executable is securely provided to the remote SGX enclave through an encrypted channel (e.g., Diffie-Hellman [54] between enclaves). We assume that the enclave is already provisioned with all prerequisite memory and/or files that it would require to correctly execute before it starts executing. Therefore, we can safely assume that the enclave does not perform a synchronous exit (e.g., for system call) after the start of its execution till termination. The attacker’s goal is to obtain the underlying algorithm or program logic. To achieve this,
the attacker can probe the enclave using any input of his/her choice and get the correct output. Furthermore, the attacker can observe the program’s access patterns through a combination of bus snooping attacks and side-channel attacks using page tables, caches, and branch prediction units. The attacker can also measure the program’s execution time and use that to leak some information.

As far as memory access patterns are concerned, we assume a worst-case attack scenario: a powerful attacker who learns perfect execution traces at their finest resolution (i.e., 64B from a combination of page table, cache and bus-snooping, and exact branch targets from branch prediction attacks) of both physical and virtual memory addresses that an enclave program accesses. More formally, let Φ be an SGX enclave program, and its runtime memory access trace \( \Phi_k(I) \) (i.e., stripped addresses depending on the attacking method’s granularity) while running an input \( I \). \( \Phi_0 \) denotes a sequence of stripped code and/or data addresses (i.e., stripped addresses depending on the attacking method’s granularity) while running an input \( I \). \( \Phi_0 \) denotes the first address that the program accesses (i.e., an instruction at the program’s entry point) and \( \Phi_n \) denotes the last address that the program accesses (only if the program terminates on the input \( I \)). Furthermore, the attacker can learn some information about the program by monitoring timing channels. The attacker can infer the entire execution time \( T \) of the program on his/her provided inputs to leak some information. Given these memory and timing traces, attacker tries to learn the security sensitive information (e.g., the algorithm or some part of it) of the program.

We do not consider software vulnerabilities in an enclave program (i.e., memory corruption vulnerabilities or semantic/logical vulnerabilities) or physical attacks (power-based, electromagnetic etc.) and security solutions [39, 58] to these issues are orthogonal to Obfscuro. Furthermore, we consider Spectre [38] and Meltdown [43] attacks out of scope as well. Traditional program obfuscation assumes that the program cannot directly disclose the memory contents of the application which is what these attacks do. Also their patch [35] has already been provided by Intel and can be rigorously checked through the CPUSVN number provided during SGX remote attestation.

IV. CHALLENGES

As mentioned before, the goal of Obfscuro is to achieve a strong notion of security—program obfuscation (also called virtual black box (VBB) obfuscation) on market-available commodity trusted hardware, Intel SGX. Unlike supporting program obfuscation on special-purpose hardware, such as HOP [47], there are a number of challenges involved in supporting VBB obfuscation on Intel SGX. These challenges arise partly due to the lower privileged execution supported by SGX enclaves and partly due to side-channel information leakage from SGX enclaves. In particular, these challenges include — (a) how to enforce secure ORAM-based program execution in SGX? and (b) how to secure the ORAM controller in SGX? Unlike with special-purpose hardware, SGX enclaves cannot control the cache and/or the branch-predictors, which can be abused by an attacker to infer significant information from an insecure ORAM-based program execution. Also, while special-purpose hardware provides the program a trusted memory

\[1\] This assumption can be easily relaxed to ensure input/output confidentiality as we describe in §IX.
to protect programs against timing attacks. To do so, firstly, OBFSUCRO utilizes ORAM access to securely randomize each memory access at cache-line granularity. Secondly, OBFSUCRO further provisions the program by introducing a central code execution and data access location—a scratchpad—thereby neutralizing the observed memory traces through all hardware including the branch-predictors. Finally, OBFSUCRO ensures that all programs (irrespective of their intended program logic) terminate after a certain time period $T$ specified by the user at the start.

V. DESIGN

A. Overview

OBFSUCRO is a software framework enabling obfuscated execution for SGX enclave programs. The key idea behind OBFSUCRO is to adopt ORAM operations in conjunction with scratchpad-based code execution and data access, thereby exhibiting memory traces oblivious to program execution (illustrated in Figure 3). The core design features of OBFSUCRO can be summarized as follows.

- **Secure ORAM Scheme.** OBFSUCRO implements its ORAM controller using data oblivious algorithms, thereby protecting it from side-channel attacks (§V-B). OBFSUCRO implements a register-based stash which improves on the prior side-channel resilient ORAM implementations [3, 55].

- **Repurposing Native Programs.** The ORAM scheme is designed to retrieve data, securing the data access patterns rather than program execution. As a result, there exists semantics gap from general program execution. OBFSUCRO bridges the semantic gap between native program execution and ORAM operations by repurposing native programs (§V-C) through memory layout transformation and virtual address translation.

- **Code Execution Model.** OBFSUCRO ensures that all the code execution (for the target program) is only performed within a code scratchpad, a fixed memory location (§V-D). All instructions are loaded onto the scratchpad through ORAM operations and executed from the start to the end of the scratchpad (1-3). Furthermore, OBFSUCRO’s scratchpad is designed with SGX-aware protections unlike previous work [44, 47].

- **Data Access Model.** OBFSUCRO ensures that all data access is performed through a data scratchpad, which is a fixed memory location updated using ORAM operations (§V-E). The target program’s read and write operations are performed at the same memory location regardless of execution context (1-5). OBFSUCRO also ensures that the data access is always performed once per C-Pad, normalizing the number of data accesses patterns.

- **Start-to-End Obfuscation.** OBFSUCRO ensures that the program continues executing till a certain predefined time to mitigate timing-based channels, irrespective of the program logic (§V-F). OBFSUCRO achieves this by instrumenting the target application to introduce dummy memory blocks, after the termination of the intended logic. Furthermore, OBFSUCRO returns a fixed output size at the end of program execution.

![Fig. 3: OBFSUCRO’s system-level overview.](image)

### Table: Scheme Comparison

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Architecture</th>
<th>Protection Scope</th>
<th>Secure Program</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Bus Snooping</td>
<td>Cache Attacks</td>
</tr>
<tr>
<td>Raccoon [52]</td>
<td>commodity hardware</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Phantom [46]</td>
<td>special purpose hardware</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>GhostRider [44]</td>
<td>special purpose hardware</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HOP [47]</td>
<td>special purpose hardware</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>OBFSUCRO (this paper)</td>
<td>commodity hardware</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

![Fig. 2: An overview of the differences in OBFSUCRO and existing oblivious execution schemes.](image)

This is a preprint, and the final paper will appear in NDSS 2019.
This is a preprint, and the final paper will appear in NDSS 2019.

B. Secure ORAM Scheme

In this subsection, we explain how BFSCURO designs a secure ORAM scheme to ensure oblivious program execution. Firstly, BFSCURO places both the ORAM controller and trees within an SGX enclave. Secondly, in response to side-channel threats against SGX enclaves, BFSCURO secures working mechanisms of its ORAM controller, i.e., ensuring that each operation is branch-free (to mitigate the risk of branch-prediction) and data-independent (to mitigate the risk of page table and cache attacks). In this regard, BFSCURO constructs two novel stash designs: CMOV-based and register-based stash for the ORAM controller (§ V-B1). Furthermore, BFSCURO employs a data-oblivious population scheme to securely populate the ORAM trees (§ V-B2).

1) ORAM Controller: In the following, we describe how BFSCURO secures two main data structures of the ORAM controller, i.e., position map and stash, against access-pattern leakage. By securing access onto these data structures, BFSCURO also ensures that its code is devoid of conditional branches (i.e., secure against branch-prediction attacks).

Data Oblivious Position Map. The position map contains sensitive information regarding ORAM blocks, i.e., mapping from block-id to the leaf in ORAM tree. An attacker can leak sensitive information about program execution by observing the access patterns onto the position map. BFSCURO employs data oblivious access mechanism to prevent information leakage from the position map. The key security primitive of this mechanism is in leveraging cmov instruction in x86 to stream through the entire data structures. As shown by Racoon [52], we devise a wrapper function for the cmov instruction to add additional bogus memory access. Depending on the flag value provided to the wrapper function of the cmov instruction, the function performs either the actual memory write (if the flag is true) or a bogus memory access without writing (if the flag is false).

Next, we describe how BFSCURO secures access onto the stash. Naively accessing the stash would leave memory traces that can be used to distinguish between real and dummy blocks in the extracted ORAM tree path. BFSCURO can utilize two different stash designs, CMOV-based stash and a novel register-based stash. While both completely secure stash accesses, it imposes different performance characteristics depending on the underlying hardware architecture.

CMOV-based Stash. BFSCURO can use data-oblivious access (using CMOV) to stream through the complete stash memory region (Figure 4-a), similar to previous schemes [3, 55]. As a result, the CMOV-supported access guarantees that the attacker learns nothing from the leaked access patterns as the attacker observes accesses onto all stash indices. One caveat of this approach is that the stash is a large memory region, i.e., >= Blog2N bytes; where B is the block-size in bytes and log2N is the size of the ORAM tree containing N nodes. Therefore, using CMOV within the stash can result in performance overhead as noted by previous works and reported in § VIII-1. Figure 5a shows a code snippet illustrating how the CMOV-based stash functions.

Register-based Stash. BFSCURO also designs a novel register-based stash, which leverages Advanced Vector Extensions (AVX) instruction set along with the XMM and YMM registers. We collectively refer to these registers as AVX registers. The key idea is to reserve these registers for ORAM stash only and restrict the program and associated libraries from using them. An operation performed on any CPU register does not imprint traces on memory-related units (cache, TLB/MMU, DRAM etc.) and is therefore oblivious to even privileged attackers such as the OS (Figure 4-b). Therefore, BFSCURO copies each tree block onto a set of AVX registers and performs all required operations on these registers. This limits the involvement of CMOV and therefore provides a performance improvement of 30–40% as compared to the CMOV-based stash as shown in § VIII-1. Figure 5b shows an example of where the memory located at rsi is moved in chunks of 32-bytes into ymm5 and ymm6.

However, there are two things to consider while opting for the register-based stash over the CMOV-based stash. Firstly, the register-based stash limits the involvement of AVX registers for other important operations such as AES-NI instruction set and if the enclave program requires these operations, it would be better suited to use the CMOV-based stash. Secondly, current desktop
Workflow. Based on the above building blocks, we now illustrate how OBFSUCRO performs a secure ORAM access. First, OBFSUCRO uses CMOV to scan through the whole position map to find the required ORAM block. Then, OBFSUCRO sequentially copies the tree blocks to either memory (if CMOV-based stash is used) or the registers (if the register-based stash is used). Afterwards, OBFSUCRO performs an oblivious retrieval of the required block from the stash. In the case of CMOV-based stash, it performs a sequential CMOV access on each individual stash index and in the case of register-based stash, it performs an inline assembly move operation to move it from the register to the memory. After performing the relevant tasks on the ORAM block, we rewrite the block back using similar approach as mentioned above.

2) ORAM Bank: OBFSUCRO places the ORAM bank, comprising of the ORAM trees, within the enclave memory. OBFSUCRO performs secure ORAM tree population to mitigate side-channel leakage.

Allocation. The ORAM trees are allocated as global arrays within the enclave program’s memory space (i.e., within the EPC). OBFSUCRO can avoid encrypting ORAM trees, which is an important step in the ORAM protocol, because the Memory Encryption Engine (MEE) in SGX [28] implicitly performs the encryption. There are two things to note here: (a) the allocation step does not leak any important information to the attacker apart from the location of the ORAM tree (which is public information in the ORAM attack model) and (b) the size of the code and data trees should be carefully considered prior to allocation since as per Path ORAM’s design, the size of the trees cannot be dynamically adjusted.

Population. As per Path ORAM’s requirement, the population of each block into the ORAM tree should be performed as a regular ORAM access. To further illustrate, the population of code and data blocks in C-Tree and D-Tree respectively, is carried out as follows: (a) OBFSUCRO picks a block which is to be added to the ORAM tree. (b) OBFSUCRO determines a random position to store the block within the ORAM tree. The random position is determined using the RDRAND hardware instruction, which only involves the trusted CPU. (c) OBFSUCRO performs an ORAM access onto the path that corresponds to the selected position. At first glance, this might leak some information to the attacker. However, since this is an ORAM access, the final destination of the block will be randomized within the path once more which ensures strong secrecy. (d) OBFSUCRO repeats the above steps until all real blocks are populated to the ORAM tree.

C. Repurposing Native Programs

In order to bridge semantic gaps between native execution and oblivious execution, OBFSUCRO transforms the native program’s memory layout into an ORAM-compatible memory layout, provides virtual address translation to support dynamic memory relocation, and introduces a scratchpad region for code execution and data access.

Memory Layout Transformation. OBFSUCRO separates the target program into two sections, i.e., code and data, and allocates a dedicated ORAM tree for each section, namely C-Tree for code and D-Tree for data. OBFSUCRO can estimate the size of the C-Tree since the program’s code size remains static. Since the size of dynamically allocated data (e.g., heap and stack) cannot be precisely estimated, OBFSUCRO sets a maximum limit on the size of the D-Tree. This is not a limitation since SGX programs themselves are initialized with a user-provided stack and heap size. Code blocks are prepared during the compilation phase, where the code is divided into blocks of the same size and filled with instrumented instructions by OBFSUCRO (more details in §V-D). During program initialization, OBFSUCRO populates both the code and data blocks into the C-Tree and D-Tree respectively. The initialized data objects (i.e., global variables) are filled in their corresponding blocks whereas the blocks corresponding to uninitialized data blocks are zero-initialized.

Virtual Address Translation. All the code and data accesses in a traditional program are realized through the virtual address, while ORAM operations deal in blocks of the ORAM tree. To bridge this semantic gap, OBFSUCRO performs on-the-fly translation of virtual addresses into ORAM block indices. To ensure secure translation, OBFSUCRO linearly maps the virtual address space of a program into ORAM blocks and performs bitwise right-shift. In order to achieve linear mapping, OBFSUCRO modifies a linker configuration, specifying code and data to be located contiguously within enclave’s virtual address space. Hence, OBFSUCRO can perform a constant bitwise right-shift operation to securely translate the virtual address to block index.

Heap Management. Since SGX enclaves do not have support for dynamic memory allocation, the maximum heap size required for the application has to be decided at compilation time. To handle runtime requests, OBFSUCRO provides a wrapper for the malloc and free function calls, i.e., malloc_ob and free_ob, which are responsible for managing the heap memory (alongside the metadata) requested by the enclave program. In particular, malloc_ob obliviously picks a block from the D-Tree which is already provisioned with blocks to handle heap memory requests during program initialization. The wrapper function returns the virtual address corresponding to the selected block. Later, when free_ob is called, it deallocates the heap memory region, figures out which blocks from the D-Tree are now free and simply tags them as such.

Scratchpad. In traditional ORAM, the program can simply access the extracted block from the stash. However, doing so within the SGX environment will leak the position of the required block within the stash through observed memory traces. To deal with this problem, OBFSUCRO prepares two fixed locations (determined during program initialization) of fixed...
size (one cache line, i.e., 64 B) to access code and data blocks, called C-Pad and D-Pad respectively. These memory regions are provisioned with SGX-specific defenses (refer to §V-D and §V-E). After OBSCURO performs oblivious operation and locates a target block in stash, OBSCURO copies the target block in stash to scratchpad. Note that this copy from stash is oblivious as described in §V-B1. Therefore, by normalizing access location and size through scratchpads, OBSCURO can successfully hide actual memory location and the attacker can not infer that information. We provide more details as to how this is accomplished in the next two sections.

D. Code Execution Model

OBSCURO ensures the following three security properties in its code execution model: C1) Code execution is always performed within the C-Pad\(^2\); C2) Code access instructions (i.e., branch instructions which impact the control-flow of a program, including call, return, unconditional branch, and conditional branch instructions) are only executed at a fixed location (i.e., the end of the C-Pad); C3) All code access instructions are replaced with an instruction jumping to a runtime function (i.e., code_oram_controller), which performs an ORAM operation to fetch the code block required.

The above mentioned security properties of OBSCURO protect code execution from access-based side-channel attacks. Since the size of the C-Pad is the same as the minimum granularity of page table and cache-based attacks (i.e., 64 B), C1 prevents these attacks from gaining any meaningful information. C2 and C3 prevent a branch prediction attack, because all the control-flow changes are made from the same location (i.e., the end of C-Pad as specified by C2) to the same destination (i.e., code_oram_controller as specified by C3), irrespective of the semantics of the original branch instruction.

To meet the property C1, OBSCURO restricts all basic blocks to be at the size of C-Pad (i.e., 64 B) during the compilation phase. Specifically, OBSCURO breaks up larger basic blocks into smaller ones equaling the size of the C-Pad. If the size of the basic block is smaller than the C-Pad, OBSCURO inserts nop instructions to fill the space. To meet the properties C2 and C3, OBSCURO replaces all branch instructions with a sequence of equivalent instructions invoking code_oram_controller. This invocation is always performed using jmp instruction to code_oram_controller, which is aligned at the end of the basic block.

For example, Figure 6a shows how OBSCURO replaces a unconditional branch instruction. Given the original jmp instruction, OBSCURO first instruments an instruction storing the virtual address of the jump target in R15. Then, OBSCURO inserts a jmp instruction to the code_oram_controller. The code ORAM controller computes the ORAM block index using the virtual address stored in R15 (as mentioned in §V-C), and retrieves the required code block from the C-Tree through an ORAM access. Afterwards, OBSCURO overwrites C-Pad using the obtained code block and resumes execution from the beginning of C-Pad. In this manner, OBSCURO translates all types of control flow instructions, including conditional jump, function call, return.

\[\text{Before}\]
\begin{verbatim}
    jmp jump_target
\end{verbatim}
\[\text{After}\]
\begin{verbatim}
    mov R15, jump_target
    jmp code_oram_controller ; Pass_jump_target through R15
    code_oram_controller loads the code block to C-Pad and then jumps to the beginning of C-Pad.
\end{verbatim}

(a) Unconditional branch (code access)

E. Data Access Model

OBSCURO ensures the following security properties in the data access model: D1) Data access is always performed within the D-Pad of size 64 B; D2) Data access instructions are only executed once per C-Pad at a fixed location (i.e., the beginning of the C-Pad); and D3) All data access instructions are replaced with an instruction jumping to a runtime function, data_oram_controller, which performs an ORAM operation to load the the corresponding data block onto the D-Pad. Similar to the code execution model (§V-D), these properties prevent cache and page table attacks. This is because attackers will always observe the same data access patterns onto D-Pad.

One thing to note here is that D2 enforces each code block to perform a single jump to the data_oram_controller. This restriction is partly due to the constraint of the 64-byte code block. In particular, OBSCURO’s data access instructions take 28-bytes and the code access instructions (mentioned in §V-D) take 20-bytes. Since a code block requires at least one code access instruction, i.e., to access the next code block, it leaves room for only a single data access. However, as a result of this, OBSCURO ensures that there is a normalized number of data access per code block, which cannot be exploited by an attacker. OBSCURO also prevents branch-prediction attacks by placing the data access instruction at a fixed location. If a certain code block does not require a data access, OBSCURO performs a dummy data access in order to portray the same memory footprints for each block.

Unlike the code execution model, the data access model allows offset-based access within the D-Pad such that a memory access can be directly performed at any location within D-Pad. This offset-based access is secure against memory-based side-channel attacks since the D-Pad is the size of the minimum granularity of attack resolution, i.e., 64 B. In order to reflect changes made by the enclave code on the D-Pad back to the ORAM tree, OBSCURO flushes the extracted data block after performing required memory access.

For example, Figure 6b illustrates how OBSCURO instruments the store instruction. Similar to the code execution model, OBSCURO uses the reserved R15 register to pass the virtual address (i.e., the memory operand of a store instruction) to the data_oram_controller. Then the

\[\text{Before}\]
\begin{verbatim}
    mov (RAX), RBX
    lea R15, 4(RAX)
    jmp data_oram_controller ; data_oram_controller fetches data block
    and returns address of (D-Pad + offset)
\end{verbatim}
\[\text{After}\]
\begin{verbatim}
    mov (R15), RBX
    ; Store RBX at where (RAX + 4) points to
    lea R15, 4(RAX)
    mov R14, after_fetch
    jmp data_oram_controller
    ; data_oram_controller fetches data block
\end{verbatim}

(b) Store (data access)

\[\text{D-Pad}\]
\[\text{C-Pad}\]

---

\(^2\)The C-Pad is a writable and executable region but it can be secured against memory corruption by employing SFI similar to SGX-Shield [58] and/or dynamic page protection to be available in SGXv2.
This is a preprint, and the final paper will appear in NDSS 2019.

Now, we explain the workflow of the instrumented target program. The application code is defined as `target_main` whereas the enclave officially starts execution from the entry function (1). At the start of the entry, `OBSCURO` ensures that the return address `R` is passed to the runtime library by writing `RT_return_addr` (2). Afterwards, `OBSCURO` starts running the `target_main` function and writes its output to a global memory within the program (3). It is worth noting that this write will also be achieved through an ORAM access (as per all data access mentioned in §V-E) and is therefore oblivious to the attacker. Then, `OBSCURO` invokes `continuous_dummy` (4), ensuring that the program continues executing.

As the program executes, it will jump to the `code_oram_controller` on each code access. At this time, `OBSCURO` checks that the predefined limit on the number of code blocks has been reached or not. If the limit has been reached, the program jumps back to `RT_return_addr` instead of jumping to the C-Pad (5). At this point, we completed the execution of original program logic but have not obtained the output. To get the output, `OBSCURO` calls the `data_oram_controller` to extract the output from the D-Tree (6). Through the above mentioned steps, `OBSCURO` ensures that there is a start-to-end obfuscation of the target program, which always executes the same number of code blocks and thus terminates after a fixed amount of time.

### VI. Implementation

We have implemented a prototype of `OBSCURO` based on the LLVM Compiler project 4.0 as well as Intel SGX SDK’s enclave loader. `OBSCURO` modified following two components in LLVM: a) LLVM backend to emit 64B of code blocks as well as to instrument code and data access instruction; and b) Compiler runtime library for ORAM controllers. In the LLVM backend, especially the assembly emitter, we arranged a new code emitter to measure the size of instructions in parallel with default emitter. We also utilized built-in machine code builder to redirect the codes and data accesses to the runtime ORAM controllers. The compiler runtime library includes the implementation of data-oblivious ORAM, and interfaces for LLVM backend and applications to employ it. The oblivious stash access is implemented with `vinsertti128`, and `vextractti128` AVX register manipulating instructions in the assembly language level. The oblivious position map access is based on the `CMOV` instruction, and we generalized its operation to variable lengths. We also changed the enclave loader of the Intel SGX SDK to make C-Pad using SGX’s `EADD` instruction. In total, `OBSCURO` introduces 3,117 LoC in LLVM backend, 2,179 LoC in compiler runtime library, and 25 LoC in Intel SGX SDK.

### VII. Security Analysis

This subsection provides a security analysis of `OBSCURO`. In general, there are two ways an attacker can steal information from SGX enclaves using side-channels. Firstly, an attacker can abuse observed access-patterns to infer some information about the program and/or its input. Secondly, an attacker can perform timing-based attacks to leak some information. We provide a systematic security analysis of `OBSCURO` against both these attack avenues.
A. Access Pattern Attacks.

As OBFSCURO is composed of multiple components to realize obfuscated program execution, we start by showing the security properties of the individual components of OBFSCURO. Then we show how these components interact with each other and show that these interactions are completely oblivious as well. Finally, we present the results of an empirical study showing that OBFSCURO achieves access pattern obliviousness.

Obliviousness of Individual Components. OBFSCURO introduces newer components to legacy programs in order to achieve obfuscated execution, as shown in Figure 8. In the figure, we show the four components of OBFSCURO (labeled as 1 ~ 4). We comment on each component individually in the following.

1. Code ORAM controller: The code ORAM controller takes the virtual address of next required code block as input, and it places the corresponding code block on the C-Pad. An attacker cannot decipher the virtual address because OBFSCURO performs secure computation based on this address. In particular, the address is first translated to a specific ORAM block using data oblivious right-shift operation (§V-C), which returns the corresponding block number in the ORAM tree. Then, OBFSCURO finds the corresponding leaf for this block through sequential CMOV-based scanning of the position map.

For the stash, OBFSCURO uses two variants, a CMOV-based and a register-based. The CMOV-based stash performs CMOV-based memory access similar to how OBFSCURO shields the position map. This includes both (a) while copying the required block from the stash to the C-Pad or D-Pad and (b) while writing back the blocks from the C-Pad or D-Pad to the stash. For the register-based stash, the AVX registers are retrofitted as stash space. Since all operations on the AVX registers are oblivious to the underlying system, we can perform a direct memory access to/from a specific register while ensuring that no information is leaked. Please refer to Figure 9 for detailed operations performed by the code controller.

2. C-Pad: OBFSCURO ensures that the C-Pad has a fixed location (determined at the program loading) and a fixed size (i.e., 64B), and ensures that all oblivious code execution occurs from this location. Since 64B is the cache-line size (i.e., the finest visible granularity through access pattern-based side-channel attacks), the attacker learns no useful information to infer semantics during the C-Pad execution. In other words, as OBFSCURO runs the target program, the attacker will keep observing the same memory activity over C-Pad, which is completely independent of the code block being executed.

3. Data ORAM controller: The data ORAM controller takes the virtual address of data objects as input, and places the corresponding data block to D-Pad. The data controller follows the exact same workflow of the code controller except that it operates on the D-Tree instead of the C-Tree. As previously shown for the code controller, the data controller also does not leak any sensitive information.

4. D-Pad: The D-Pad is functionally and structurally similar to the C-Pad, except that data access is performed on it and not code execution. Similar to the C-Pad, it has a fixed location and the same size, thereby showing the same memory activity for each data access.

Oblivious Interactions b/w Components. The aforementioned components perform five interactions between them (labeled as 1 ~ 4). We illustrate below how each of these interactions is secure against access pattern-based attacks.

- Jump from Code ORAM controller to C-Pad after fetching code block: After obliviously extracting a block from the C-Tree and copying it to C-Pad, the code controller performs a single jump to the start of the C-Pad. This step only reveals that some code block of a target program will now be executed, which entails no semantics behind the code block being executed.

- Jump from C-Pad to Data ORAM controller for fetching data block: Each code block (executing within the C-Pad) is strictly enforced to perform a single jump to the data controller, because OBFSCURO normalizes the number of data access within each code block to be exactly one (refer §V-E). Moreover, this jump is performed at a fixed offset within C-Pad to mitigate the risk of branch prediction attacks. The target address of this jump is also fixed, i.e., the start of the data controller’s logic.

- Return from Data ORAM controller to C-Pad: There is only a single jump from the data controller to the C-Pad at a fixed offset within the C-Pad, after fetching/updating the required data block on the D-Pad.

- Single D-Pad access: There is only a single access to the D-Pad per code block. Since the size of the D-Pad is 64B, this access does not reveal offset information either.

- Jump from C-Pad to Code ORAM controller: Finally, OBFSCURO enforces that there is only one jump from C-Pad to the code controller at a fixed address located towards the end of the C-Pad. The target address of this jump is also fixed at the start of the code controller logic.

Empirical Study. Lastly, we present the results of our empirical study on obfuscated memory traces exhibited by various applications. The results are depicted in Figure 10. We choose six target applications for the study, including anagram, pi, mattranspose, sum, fibonacci, and palindrome. These applications were chosen due to the diversity of their computational complexity.

In Figure 10, we attempt to show that there is no correlation between obfuscated and obfuscated memory traces of the same program. We measure multiple runs for each aforementioned application, and for each run we accumulate data corresponding a timing sequence to the address accessed by the program. Using the accumulated data, we can perform a Pearson correlation value between the test applications and populate the corresponding cell in the confusion matrix. For example, consider the (anagram, anagram) cell in Figure 10-(a), the Pearson correlation value is very close to 1 because this
This is a preprint, and the final paper will appear in NDSS 2019.

<table>
<thead>
<tr>
<th>ORAM operations</th>
<th>Sensitive information</th>
<th>OBSFUCRO defense</th>
<th>Observed traces by adversaries</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Locating corresponding pos.map element</td>
<td>Offset in pos.map</td>
<td>CMOV-scanning read</td>
<td>Sequential read traces on pos.map</td>
</tr>
<tr>
<td>2. Extracting requested ORAM path to stash</td>
<td>No sensitive info.</td>
<td>-</td>
<td>Sequential copy traces from requested ORAM path to stash</td>
</tr>
<tr>
<td>3-a. Copying ORAM block in stash to scratchpad (CMOV-based)</td>
<td>Offset in stash</td>
<td>CMOV-scanning copy</td>
<td>Sequential copy traces from stash to scratchpad</td>
</tr>
<tr>
<td>3-b. Copying ORAM block in stash to scratchpad (Register-based)</td>
<td>Offset in stash</td>
<td>Register operations</td>
<td>No traces since registers are oblivious to memory</td>
</tr>
<tr>
<td>4. Updating pos.map with new leaf number</td>
<td>Offset in pos.map</td>
<td>CMOV-scanning write</td>
<td>Sequential write traces on pos.map</td>
</tr>
<tr>
<td>5-a. Writing back scratchpad to stash (CMOV-based)</td>
<td>Offset in stash</td>
<td>CMOV-scanning write</td>
<td>Sequential write traces from scratchpad to stash</td>
</tr>
<tr>
<td>5-b. Writing back scratchpad to stash (Register-based)</td>
<td>Offset in stash</td>
<td>Register operations</td>
<td>No traces since registers are oblivious to memory</td>
</tr>
<tr>
<td>6. Writing back stash to requested ORAM path</td>
<td>No sensitive info.</td>
<td>-</td>
<td>Sequential write traces from stash to requested ORAM path</td>
</tr>
</tbody>
</table>

Fig. 9: Security analysis of secure ORAM implementation used by the code and data controller.

Fig. 10: Confusion matrix for naive access patterns vs. obfuscated pattern by OBSFUCRO

Figure 10-(b) shows the confusion matrix formed while comparing obfuscated programs (using OBSFUCRO) to their native access patterns. Since OBSFUCRO ensures that all applications proceed in a fixed pattern of execution, the access patterns of these programs are completely different from their counterparts in native execution. Furthermore, all cells in Figure 10-(b) are almost 0 because none of obfuscated programs have any correlation with any of the native programs.

B. Timing-based Attacks.

Apart from access pattern attacks, a privileged attacker can also break program obfuscation within Intel SGX by abusing timing channels. In particular, we can think of two ways in which an attacker can abuse timing channels to leak information from OBSFUCRO— (a) observing the time it takes for individual code blocks (in C-Pad) to execute, and (b) observing the total time it takes for an obfuscated program to execute. We individually show the infeasibility of each of these timing channels.

C-Pad Execution Time. Timing differences in executing each code block (i.e., C-Pad) can leak information about the execution semantic of the program. We statistically prove that this side channel is infeasible within OBSFUCRO’s execution. The reason for this is that the execution time for the data ORAM access (which is performed exactly once per C-Pad) dominates the entire execution time of the C-Pad. We conducted a statistical experiment measuring CPU cycles in executing different classes of code blocks. We constructed five different code blocks, including NOP, ADD, SUB, IMUL, IDIV code blocks. Each code block initially jumps to the data controller to fetch a data block and the remaining space is filled using one of the instruction type. Furthermore, we impose data dependencies within the instructions to prevent out-of-order execution. We accumulated the execution times for each class over 10,000 repetitions, and the distribution is shown in Figure 11. As illustrated, the 10%–90% percentile intervals for each type (marked as two broken lines) largely overlap, which is hardly possible for an attacker to distinguish.

Program Execution Time. As mentioned in §V-F, OBSFUCRO enforces a property that a program continues executing until its number of executed code blocks reaches fixed user-configured limit. In particular, OBSFUCRO allows the user to define the total number of C-Pad executions a program should perform. If the program’s logic terminates before configured C-Pad execution number, OBSFUCRO continues executing dummy code blocks to complete the number of
C-Pad executions.

In order to prove that this results in a uniform execution time irrespective of the target program being executed, we performed an experiment on a diverse set of applications as shown in Figure 12. In the experiment, we fixed the total number of C-Pad executions for each of these applications to 30,000 and measured the total execution time. We accumulate 50 executions for each program, and plot the distributions of them. As shown in the figure, the ranges of total execution times for the chosen evaluation set largely overlaps, despite computational diversity of these applications. The reason for this is that each C-Pad execution, as shown above, is bounded at very similar execution times irrespective of the underlying CPU instructions. Therefore, it is expected that the program execution time (with same number of C-Pad executions) will also be very similar.

VIII. PERFORMANCE EVALUATION

In this section, we report a detailed performance benchmark through both micro-benchmarking custom applications and macro-benchmarking by running OpenSSL [20].

Experimental Setup. All our evaluations were performed on Intel(R) Core(TM) i7-6700K CPU @ 3.40GHz (Skylake with 8 MB cache, 8 cache-slices and 16-way set-associativity) with 64 GB RAM (128 MB for EPC). Our system ran Ubuntu 16.04 with Linux 4.4.0.59 64-bit. We performed our experiments using Intel SGX SDK [1] and the Intel SGX drivers [34]. Due to the current unavailability of AVX-512 for SGX-enabled computers, most of our experiments (having large code and data sizes) used CMOV-based stash. However, we experimented with AVX2 registers to find the expected benefit of using the register-based stash and have accordingly simulated the performance improvement achieved by register-based stash on our target applications.

1) Micro-Evaluation. Firstly, we start by providing a detailed performance evaluation result by running several programs with Obfuscuro. Next, we show the performance improvement achieved by the novel register-based stash designed by Obfuscuro.

Benchmarks. We ported simple benchmarking applications on Obfuscuro in order to show the feasibility of obfuscated execution using commodity hardware such as Intel SGX. In particular, we ported a diverse set of applications from simple applications like finding the maximum within a given array to complex binary searching.

Figure 13-(a) shows the performance shown by Obfuscuro while running the test set of applications described above. We also simulate the performance of Obfuscuro-AVX (the version of Obfuscuro which uses register-based stash). These simulated results are based on the experiments we performed on AVX2. In general, the performance overhead of Obfuscuro-CMOV is on average 83\times and Obfuscuro-AVX is 51\times. The performance overhead of Obfuscuro is expected since it has to cater to the plethora of side-channels plaguing Intel SGX. In no particular order, the overhead is attributed to: (a) code access control especially dealing with branch-alignment, (b) data access normalization and (c) side-channel-resistant ORAM-based access inside Intel SGX.

Comparison: CMOV-based vs Register-based Stash. In the coming paragraphs, we provide a comparison of the CMOV-based stash versus the register-based stash. We attempt to answer the question — what is the performance benefit attained by using register-based stash over the CMOV-based stash? One caveat is that all our experiments are based on the AVX2 registers and although we expect the performance benefits to be similar while using the AVX-512 registers. Figure 14 attempts to illustrate the performance benefit achieved by AVX extensions over CMOV while accessing data of variable size through ORAM. Compared to the CMOV-based stash, since the register-based stash performs just a single oblivious access onto the AVX registers, it outperforms the CMOV-based stash. The average improvement is around 30-40%.

2) Macro-Evaluation. In order to show how real-world applications perform with Obfuscuro, we provide a case-study with a real-world application, OpenSSL [20]. Figure 13 shows the result of our evaluations using OpenSSL with Obfuscuro and without Obfuscuro. In this experiment, we perform a variable number of consecutive encryptions and compare the results. As the number of encryptions increase, the difference between the performance of Obfuscuro and native also increases. The reason for this is that Obfuscuro has to perform a fixed number of ORAM operations which adds significant overhead per-encryption whereas the per-encryption overhead of native execution is very small.

IX. DISCUSSION

Comparison with Cryptographic Schemes. There has been extensive research thrusts in cryptographic circles to achieve secure remote computation. On par with what Obfuscuro provides, we discuss following two security properties: 1) computational confidentiality (i.e., whether a computational
artifact of a target program can be known to the untrusted party) and 2) integrity (i.e., whether the integrity of program execution can be disrupted by the untrusted party). Towards these security properties, we focus our discussion on theoretical program obfuscation techniques, which construct virtual blackbox (VBB) using various techniques. We note that, unlike OBFSUCRO which performs hardware-assisted secure remote computation, theoretical program obfuscation techniques [12, 17, 26] do not rely on specific architectural characteristics and thus are designed to be generally resistant to memory-based side-channel attacks.

More specifically, two well-known cryptographic primitives, fully-homomorphic encryption and garbled circuits are generally used for the program obfuscation, but both of them are limited in terms of either performance and generality. In the case of fully-homomorphic encryption [21], its performance overhead is in twelve orders of magnitude scale in string search [51], severely impeding its adoption in practice today (and near future). Moreover, while fully-homomorphic encryption ensures confidentiality of its inputs, its construction does not ensure integrity. In the case of garbled circuits [22], its performance overhead is about four orders of magnitude for circuit evaluation alone. Moreover, it cannot be used for generic programs (i.e., a loop structure in a program cannot be supported and thus the loop should be completely unrolled), and the integrity cannot be guaranteed similar to fully-homomorphic encryption. For both of these solutions, verifiable computing techniques can be adopted to provide integrity, but verifiable computing itself imposes huge over performance overheads (i.e., about $10^4$ times [65]).

Compared to these theoretical solutions, OBFSUCRO efficiently achieves confidentiality and integrity, leveraging memory protection and remote attestation mechanisms of SGX. From the performance perspectives, OBFSUCRO is a much more practical solution as it imposes two orders of magnitude performance overhead, as opposed to twelve and four orders in the case of fully-homomorphic encryption and circuit representation, respectively. OBFSUCRO also supports generic programs, as it still retains the form of the host-architecture instruction in conjunction with secured ORAM, which is automatically transformed at the compiler level.

**Protecting Input/Output.** Traditional program obfuscation assumes that the attacker has an oracle-like access to the obfuscated program. Therefore, the assumption is that the attacker can provide any input that he/she desires and get the corresponding correct output from the obfuscated program. However, this assumption can be further relaxed to protect the input/output of the program. In that case, the scenario could be of a cloud provider who hosts an enclave on his/her machine but cannot directly access the enclave because the enclave requires prior authentication to access. In this case, OBFSUCRO can be further leveraged to guarantee that an attacker does not figure out the input/output either. For the input, since it is not controlled by OBFSUCRO, we assume that the user of the enclave will provide us a fixed-length encrypted memory buffer to extract the input from. OBFSUCRO will execute for a fixed time $T$ based on the input and extract a fixed-size output from the D-Tree at the end of $T$. Then, OBFSUCRO will encrypt this data and send it back to the user. During all this, the attacker knows that the program is executing but is completely blind to what the execution might be.

**Potential Applications.** There are various potential applications for OBFSUCRO ranging from protection of a developer’s intellectual property from theft to hiding exploitable vulnerabilities in programs. Firstly, OBFSUCRO can ensure that machine learning services requiring huge computing resources and therefore cloud machines, can safely outsource their computational load. For example, companies like 23andMe [2] want to outsource genomic analysis but also want to stay ahead of the competition by preventing the theft of their algorithm. Another potential application is in the prevention of vulnerability exploitation. For example, an attacker can extract information about the open-source libraries used by the program and perform various code-reuse exploits against the program. In both cases, obfuscated memory traces of program execution provided by OBFSUCRO will be meaningless to the attacker.

**General side-channel defense for SGX.** OBFSUCRO can be utilized as a general-purpose side-channel defense, whose main objective is to protect an input of a target program from attackers. The attackers usually exploit unique memory access patterns leaked from side channels consisted of caches, page fault, and branch predictor [8, 24, 40, 57, 70]. Because OBFSUCRO is specially designed to remain obfuscated from the channels, OBFSUCRO can protect the target program, utilizing its obfuscated execution. For that purpose, we can relax the obfuscation problem to a side channel defense problem, and apply the obfuscation mechanism to a subset of program functions which are sensitive, resulting in performance improvement.

**Other Use-cases of OBFSUCRO.** Our current design for an oblivious execution framework is SGX-specific. However, we believe its design characteristics and optimization techniques are general, which can be applied to other trusted platforms such as AEGIS [64], Ascend [19], XOM [41], Bastion [9], and Sanctum [14]. For example, our register-based stash (§V-B1) can be considered as a generic optimization for ORAM, if the underlying trust architecture shares any of memory-related subsystem such as cache, TLB, MMU, and DRAM.

**X. Related Work**

**SGX Based Systems.** Haven [6], Graphene [66, 67] and Panoply [61] provide LibOS for SGX, which enable easier application porting and prevent Iago attacks [10]. OpenSGX [36] provides an open research framework for running SGX applications. VC3 [56] provides oblivious data analytical algorithms such as MapReduce [15]. SGX-Shield [58] performs fine-grained ASLR within SGX environments. Some of OBFSUCRO’s design schemes, particularly how OBFSUCRO breaks a program into smaller ORAM-compatible blocks, have been inspired by SGX-shield. Ryoan [30] provides a secure framework to port Native Client (NaCl) [71] in Intel SGX. SCON [4] provides performance optimizations and ports containers within SGX. Eleos [49] provides a framework to use non-enclave space to improve enclave performance. Glamdring [42] provides automatic partitioning within enclave programs. These systems do not consider side-channel issues within SGX and can be used together with OBFSUCRO.

**Attacks on Intel SGX.** SGX is vulnerable to both page fault [70] and page table [68] attacks. Recent works [8, 24, 57]...
have shown that cache-based attacks are possible with an SGX enclave. SGX has also been found to be vulnerable against the branch-prediction attack [40]. Wang et. al [69] provide an overview of the attack vectors against SGX and the limitations of current defense solutions.

Defenses with Intel SGX There have been various defenses [59, 60] proposed against the page table attacks. T-SGX [59] uses Transactional Memory (TSX) to run a program. However, T-SGX is vulnerable to the improved controlled channel attack [68]. Cloak [27] also utilizes TSX as a defense primitive, but it only considers cache side channel attacks, and it is limited to a cache size of CPU. Another work [60], provides a way to prevent page faults from the OS-level attacker by periodically modifying the program’s memory access patterns. Ohrimenko et. al [48] show how to re-adapt ML-algorithms to exhibit data-oblivious memory access patterns. For cache-based attacks, the previous solutions [13, 37, 72], for non-SGX environments, are not directly applicable since most of them require OS-level support. Compared to these defenses, OBFSDDURO proposes a generic security framework against all memory-based side-channel attacks. Obliviate [3] and ZeroTrace [55] provide access to files and data structures respectively using secure ORAM implementations. Compared to OBFSDDURO, their scope of protection is limited, i.e., files and data arrays respectively.

Hardware and Software-based Oblivious Systems. Previous work has alluded to the concept of creating oblivious systems based on custom hardware [18, 46, 47], software-level defenses [45, 52] or hybrid [44]. All aforementioned systems use variants of ORAM [23] to achieve oblivious execution. Out of all these works, HOP [47] and Phantom [46] are the most similar. However, both Phantom and HOP use RISC-V processors to implement secure ORAM controllers while OBFSDDURO runs on commodity trusted hardware.

XI. CONCLUSION

This paper presents OBFSDDURO, the first system which provides program obfuscation using commodity trusted hardware. OBFSDDURO systematically protects the SGX enclave against information leakage through all side-channels, thereby neutralizing all memory and timing footprints to create a virtual blackbox for obfuscated program execution. Our evaluation shows that OBFSDDURO can provide strong obfuscation guarantees within Intel SGX while performing much faster than existing cryptographic schemes and being more deployment-friendly than existing system-based solutions.

REFERENCES
