STARRS: Small: GC@Scale: Synthesis, optimization, and implementation of Garbled Circuits for Scalable Privacy-Preserving Computing

Farinaz Koushanfar
University of California San Diego

12:43 Noon Tuesday 14th June, 2016

Contents

PROJECT SUMMARY (STARRS: Small: GC@Scale: Synthesis, optimization, and implementation of Garbled Circuits for Scalable Privacy-Preserving Computing)

Farinaz Koushanfar, University of California San Diego

Overview: Computing on sensitive data is a standing challenge central to several modern-world applications. Secure Function Evaluation (SFE) refers to provably secure techniques that aim at addressing this challenge by enabling two (or more) mistrusting parties to jointly compute an arbitrary function on their private inputs without revealing their information. The first and by far the most efficient two-party SFE method is called the Garbled Circuit (GC) Protocol introduced by the seminal work of Yao. The protocol is built upon transforming the target function to a Boolean circuit and encrypting/communicating the logic gates. Despite a decade of research in GC and several key progresses, scalability of the available methods have been hampered by the circuit representation as a directed acyclic graph, and local logic optimizations at the software level. The proposed GC@Scale project focuses on novel scalable methods for addressing SFE by leveraging hardware design, synthesis, optimization, and implementation techniques.

Intellectual Merit: The GC@Scale STARSS proposal outlines a multi-pronged development plan for building next generation platforms and tools, scalable methodologies, applications, and implementation of the GC protocol and its extensions. Building on PI's recent work which has changed the SFE landscape by viewing GC generation as an atypical sequential logic synthesis task, the project plans to advance the understanding and enable expanded exploration of SFE methodologies adapted from hardware design, synthesis, optimization, and implementation. Since the SFE objective and constraints are drastically different from the classic hardware design, the project simultaneously advance the theory, practice, and tools for logic design, synthesis, mapping and optimization.

The focus of the GC@Scale research is on three modular but inter-linked thrusts: (i) Building a garbled processor, a hardware emulation framework that realizes a general purpose processor for secure computation. The processor allows users to develop applications using high-level languages, utilizing regular compilers, which will be evaluated securely by the GC protocol. The processor receives garbled input data and instructions, evaluates instructions on data non-interactively to avoid costly communication on the one hand, and to achieve leakage-resilience (i.e., eliminating the threat of side-channel attacks) on the other hand. (ii) Creating the challenging application-specific GC matching engines where the underlying algorithms inherently incur a higher than linear complexity. Using secure stable matching as the driver example, the first set of practical methods and tools as well as generalization to a family of standing complex problem will be developed. (iii) Devising new custom garbling engines for outsourcing Machine Learning (ML) applications. Throughout the project, an end-to-end design methodology is adopted to provide abstractions and open source tools for rapid prototyping, as well as proof-of-concept implementation of the methods in hardware with accompanying interfaces (apps).

Broader Impact: The results of GC@Scale will enable effective, scalable, practical and fundamental solutions for design and optimization of SFE protocols that directly translate to stronger cryptography and security for a myriads of modern tasks with sensitive data. The applications are wide reaching and include privacy-preserving processing of medical, genome, and biometric data, as well as personal, government, and industrial cloud computing/data analytics. The research program is interdisciplinary and integrates knowledge not only across the fields of hardware design and security but also from optimization and machine learning. The resulting software tools and hardware modules will contribute to a lively and interactive education in security and will be relevant to a broad set of developers outside academia who design privacy preserving algorithms and applications. The PI plans to embark on an ambitious educational program that targets both undergraduate/ graduate students, and also addresses issues related to outreach. The PI has a track record for mentoring women and continues to play a major role in engaging graduate women in ECE as well as outreaching to younger generations of women and minority students.

1 Introduction

Secure Function Evaluation (SFE) allows two (or more) mistrusting parties to jointly compute an arbitrary function on their private inputs without revealing anything but the result. The seminal work of Yao [1] has introduced the concept of two-party SFE using Garbled Circuits (GC). The two-party case was later generalized to multi-party SFE [2]. While the GC protocol was originally thought to be very expensive and computationally inefficient, algorithmic optimizations and practical implementations have been presented during the last decades. In addition to advances in computing platforms, key enablers for progress include newer cryptographic constructs, logic-level transformations, and compiler/software techniques, see [3–7].

Contemporary literature has cited multiple important privacy preserving and security critical applications that could benefit from a practical realization of SFE, including but not limited to: (privacy-preserving) biometrics matching, face recognition, image/data classification, electronic auctions voting, remote diagnosis, and search [8–13]. A suite of alternative methods for SFE is provides by Fully Homomorphic Encryption (FHE) which allows one party to perform operations one the encrypted input from the other party. While the GC and FHE do not always address the same scenario, for problems that can utilize either of the methods, it was demonstrated that SFE by GC (and GMW) is more efficient for cases where a comparison with FHE was possible [14].

The compilers and programs that enable real-world implementation of SFE have been continually evolving. Two different approaches for GC boolean generation have been developed in prior literature: (i) GC translation based one a custom library for a general purpose programming language such as Java along with functions for emitting the circuit, e.g., [6, 15, 16], or (ii) a new GC compiler for inputs given in a higher-level language that translates the instructions into the Boolean logic, e.g.,[3, 17–19]. Both approaches incur scalability problems and have certain other limitations when it comes to real implementation [20].

The PI's recent introduction of TinyGarble [20] has dramatically changed the landscape of implementation of GCs and other SFE methods that are based on mapping to binary description such as GMW [21, 22]. TinyGarble views circuit generation for Yao's as an atypical logic synthesis task that can still take advantage of the existing hardware design and synthesis methods and tools. TinyGarble creates custom libraries and transformations, which along with new (garbled circuit) design objectives and constraints, allow using traditional capable techniques and tools to address this significant challenge. The non-scalability of traditional GC compilers is being eliminated by TinyGarble. Compared with the best known earlier automated tools for this task, our results show considerable savings in terms of memory footprint (up to 10^7) and bandwidth (4 times) on benchmark functions. A side-benefit of the approach is that many functions in usage in custom hardware design along with their IP/design libraries are already available and can be adapted for SFE.

Our GC@Scale proposal outlines an ambitious systematic and modular plan for building novel methodologies, tools, optimization and platforms that enable realizing next generation applications of SFE. While TinyGarble provides a general methodology and tools for addressing SFE in software, more specialized or customized processors and/or hardware implementations are yet to be devised for pending applications. To understand the novel aspects of this proposal, we make an analogy of TinyGarble to a HDL language, e.g., Verilog. TinyGarble provides generic basic libraries for performing common operations in SFE (e.g., addition or multiplication), same as Verilog hardcore IPs (for addition or multiplication). However, while Verilog (or TinyGarble in analogy) is an enabler for designing, optimizing, or implementing new applications, much more work than just simple compilation is needed to design a complex architecture or applications with certain constraints. By leveraging the TinyGarble's unique perspective which has bridged the knowledge gap between hardware design/logic synthesis and the security community, we embark on exciting scalable design, optimization, synthesis, and implementation for myriads of key SFE applications and domains.

1.1 Research Goals

The overarching objective of this GC@Scale STARSS proposal is to enable real-world application of provably secure privacy-preserving protocol. To reach this objective, we plan to create next generation libraries and tools, scalable algorithms and methodologies, applications, and proof-of-concept realization of the GC protocol for various key classes of problems. While our initial focus will be on the standard honest-but-curious adversary model [23], we will work on generalizations to malicious and covert adversaries, as well as extension to multi-party computing scenarios.

Our approach consists of three modular but inter-linked thrusts that enable development of new concepts, designs, optimization, and tools for scalable realization of next generation privacy-preserving applications.

Thrust 1: General-Purpose Garbled Processors for Secure Computation: Project 3.1 aims to create a garbled processor that provides a general solution for SFE by GC. The pertinent function can be described in the native processor instruction set, e.g., MIPS or ARM. The input will be a function and a string (of input data) and the output will also be in the string format. We will devise the details of the architecture and provide proof-of-concept hardware FPGA emulation which will be the first-of-its-kind as the size of the hardware processor would be independent from the program size ensuring scalability. We also plan to utilize reconfigurability for providing efficiency, as only the needed instructions for each class of functions shall be configured. Both regular SFE and private function SFE will be designed and demonstrated.

Thrust 2: Application-Specific Garbling Engines for Complex Matching Algorithms: In Project 3.2, we will develop a systematic and modular approach for addressing complex matching algorithms with an inherently higher than linear complexity. Our driver example will be the well-known challenge of secure stable matching for which no practical solution is available in the literature. We shall work on methodologies that help addressing this standing problem, while we will focus on finding general methodologies that help scaling up secure computation using GC protocol beyond the sizes that can be handled by the hardware synthesis tools at once. This will ensure applicability of the techniques to other challenging problems.

Thrust 3: Application-Specific Garbling Engines for Outsourcing Sophisticated Machine Learning (ML) applications: Project 3.3 investigates building practical and customized privacy-preserving linear algebraic ML computing frameworks enabled by GC primitives. This framework shall account for the resource constraints users who need to outsource the computationally expensive ML tasks to more powerful servers while not revealing anything about the users' data. This framework shall perform most accurate computation given constraints such as runtime, power consumption, memory footprint, and outsourcing dollar costs (e.g., cloud server expenses). Also the process would be heavily optimized by understanding and modeling the performance trade-offs offered by approximate computing approaches and structured/sparse data formats.

1.2 Educational Goals

In the current engineering curriculum, students are exposed to a variety of seemingly disparate components and models in different courses. For example, they learn computer architecture, ASIC design, and security in different settings while they do not gain a system view of how these different components could be related in the design and optimization of secure hardware and/or secure function evaluation. To address this, the key components of my education approach are to adopt paradigm-based teaching methods and to acquire hands-on experience.

To accomplish my educational goals, I will (i) develop new content for both my undergraduate and graduate level courses. The added material will be designed to improve their understanding, implementation, and hands-on skills. To integrate my teaching and research efforts, I will (ii) organize a seminar-based course on secure function evaluation that includes papers from hardware design and architecture in addition to security,

with the goal of exposing students including senior undergraduates and early graduate students to interdisciplinary research. I will also continue to (iii) address the diversity and retention problems among women and minority students; this will be done by studying the roots of the problems, taking personal initiatives, organizing motivational seminars, and by offering for-credit research opportunities for undergraduates. All my class notes, slides, seminar videos, readings, resulting software tools and hardware design source codes, data and other educational materials will be openly accessible via NSF-funded Trust-HUB web portal [24] where I'm a PI and my lab webpage at UCSD.

2 Motivation and Background

In this section, I use two examples to motivate the need for more scalable and practical privacy-preserving solutions that can serve as a key enabler of several privacy-sensitive applications.

2.1 Motivational Example

Example 1: One of the most serious threat to the security of the crypto-systems is side-channel attacks in which secret information is gained through physical measurements of the system through other than the legitimate *channel*. Examples of this type of attack include: power consumption, acoustic, computation time, and electromagnetic signal analysis [25–27]. A typical victim of side-channel attack is a hardware or software that stores secret information like cryptographic keys used for security-related computation, e.g., for user authentication. It has been shown that the secret information can be easily revealed not only by the owner of the device but also by anyone with an access to the side-channels. For example, it was demonstrated that an adversary within 4 meter proximity of a computer that runs a public key encryption, can learn about the key by recording the computer's sound emitted during computation [26]. Unfortunately, the proposed countermeasures against the physical side-channel attacks are typically ad-hoc and do not guarantee thwarting future information leakage through other channels. However, recent theoretical works [28, 29] show that the side-channel attacks can be eliminated through cryptographic leakage-resilient computations. These computation will stay secure even in face of certain information leakage. Thus, it is possible to evaluate the sensitive parts of computation under leakage-resilient setting in order to ensure a mathematical safety margin against secret leakage. The proposed architecture in Section 3.1 enables leakage-resilience and eliminates the possibility of a side-channel attack.

Example 2: This example considers privacy-preserving fingerprint authentication. Biometric based methods have been widely deployed in various application domains, ranging from government programs to personal devices. Examples of such applications include international visa system, national ID card, and personal information access control on mobile phones. Biometric traits have the properties of universality (the characteristic is owned by each person), distinctiveness (two individuals are sufficiently different regarding to the characteristic), permanence (invariant of time with respect to matching requirements), and collectability (quantitatively measurable), which ensure the usefulness and high reliability of biometric based applications [30]. The popularity of biometric data raises significant privacy concerns, especially when the matching process is performed in partially untrusted environments. However, none of the suggested techniques for applying SFE on biometrics is able to simultaneously provide robustness, scalability, and practicality. This proposed methodologies in Section 3.2 can enable novel scalable and efficient implementation of secure biometric matching, e.g., privacy-preserving fingerprint authentication.

2.2 Yao's Garbled Circuit Protocol

Yao's GC protocol [1] is one of the key SFE methods which allows two parties, *Alice* and *Bob*, to jointly compute a function on their private data inputs $f(x_{Alice}, x_{Bob})$. More precisely, Alice *garbles* the function f, where f is represented as a Boolean circuit. To do this, Alice maps the plain binary values of inputs and

intermediate gates' outputs to random symmetric *keys* (labels). For each gate in the circuit, an encrypted truth table is generated that allows computation of the gate's output label based on its input labels. Alice sends the garbled circuit, consisting of the encrypted truth tables for all gates, along with her corresponding encrypted input labels to Bob. To compute f, Bob needs to know the labels corresponding to his inputs without revealing its inputs to Alice. For this, Bob obtains his labels obliviously through an 1-out-of-2 Oblivious Transfer (OT) protocol [31] and uses them to *evaluate* the garbled circuit gate by gate. Finally, Alice provides a mapping from the encrypted output to plain output. Note that the GC protocol has been generalized to multi-party SFE [32, 33].

An extension to two-party SFE is Private Function SFE (PF-SFE) which allows secure computation of a function $f_{Alice}(\cdot)$ held by one party (Alice) operating on another party's data x_{Bob} (Bob) while both the data and the function are kept private. This is in contrast to the usual setting of SFE where the function is known by both parties.

As a first step we consider standard honest-but-curious [23] (also known as semi-honest or passive) adversaries which means that all parties should follow the protocol but they may be curious to extract additional data from the data which they are receiving. Although this model does not characterize the strongest attack scenario, it is the most commonly used adversary model in the SFE literature. In each of our research thrusts in Sections 3.1-3.3, we utilize this model in our near-term objective. We will consider the stronger malicious adversary model in the mid-term objectives of each thrust.

2.3 GC Implementation and TinyGarble

The first suggested SFE protocol given was Yao's garbled circuits protocol [1] and the protocol of Goldreich-Micali-Wigderson (GMW) [21]. Both protocols securely evaluate a Boolean circuit that represents the desired functionality. Since then, several researchers have been actively investigating the design and implementation of practical circuit-based secure computation in different adversarial settings. While designing efficient and correct circuits for smaller building blocks for simple applications has been performed manually by experts, this task becomes highly complex and time consuming for large applications such as floating-point arithmetic and signal processing, and is thus error-prone. Faulty circuits could potentially break the security of the underlying applications, e.g., by leaking additional information about a party's private inputs. Hence, an *automated* way of generating *correct* large-scale circuits which can be used by regular developers is highly desirable. A large number of compilers for secure computation such as [34–44] implemented circuit building blocks manually. Although tested to some extent, showing the correctness of these compilers and their generated circuits is still an open problem.

TinyGarble [45], which was recently developed in PI's lab, took a completely different route by introducing sequential function synthesis and suggesting the usage of already established powerful hardware logic synthesis tools for GC protocol. The advantage of this approach lies in the fact that synthesis tools have been successfully used in designing scalable circuits, and they are verified thoroughly, overcoming the limitations of the earlier compilers in terms of scalability and correctness problems. However, since the conventional synthesis tools are designed primarily to map circuits to a target hardware platforms such as ASICs or FPGA, the design objectives and constraints are drastically different than the GC scenarios.

Using hardware logic synthesis tools for a special purpose such as generating circuits for secure computation, requires customizations and new libraries, objectives and constraints. Exploiting these tools promises accelerated and automated circuit generation, significant speedup, and ease in designing and generating circuits for much more complicated functions, while also maintaining the size (and depth) efficiency of hand-optimized smaller circuit building blocks. TinyGarble's unprecedented compactness is also due to leveraging of sequential circuit description, which is in contrast with the earlier methods that only consider a combinational Boolean logic format and as a result, incur scalability issues.

3 Research Program

Each of the subsections is organized as follows. After describing the motivation, problem statement, and state-of-the-art, I outline preliminary results and near-term objectives that are attainable in relatively early terms, and then more ambitious middle-term objectives. I conclude by summarizing an outlook and impact.

3.1 General-Purpose Garbled Processors for Secure Computation

Research Questions: (i) The current methods for developing applications for multi-party secure computation involves cumbersome Boolean Circuit synthesis, can we design a framework that makes high-level languages directly available for these type of application? (ii) Is it possible to efficiently implement a leakage-resilient device which guarantees no information leakage against the side-channel attacks? (iii) Can we realize a leakage-resilient processor that also obfuscates its instructions?

Motivation and Problem Statement. A standing challenge that we plan to address, is to develop general-purpose garbled processor where the input to the secure computation framework is a set of instructions (i.e., a software program) instead of a Boolean circuit. Using this general purpose processor, the pertinent application can be developed by a non-expert user in a high-level language and then compiled to the native processor instruction set via the available cross-compilers like gcc. This processor receives the compiled program and input data in its memory and writes the output back to the memory. Since a customized hardware implementation can bring orders of magnitude performance gain compared to its software counterpart, we also plan to implement this garbled processor on a hardware platform e.g., FPGA.

Another contemporary challenge is to realize a leakage-resilient platform [28, 46] that stays secure even in face of leakage of certain information, i.e., side-channel attacks. Theoretical work on leakage-resilient cryptography has demonstrated that for GC protocol, where one party is able to (non-interactively) evaluate the function for fixed inputs, the security guarantees of SFE can provide provable leakage-resilience against any side-channel attack [28]. In particular, by leveraging PF-SFE, the execution flow can be fully resilient which means not only it does not leak any information about the private inputs but also hides the underlying application. This is especially useful when the application is proprietary or classified.

State-of-the-Art. Following the recent theoretical research to build provably leakage-resilient cryptography [47], Järvinen et al., introduced the first prototype of a system implemented on an FPGA that uses Yao's GC and a tamper-proof device for OTP [46]. They implemented the AES cipher as their only benchmark function for leakage-resilient computation. However, their proposed framework, like most frameworks in GC, requires the user to describe the underlining function as a combinational Boolean circuit. This results in limited applicability for non-expert users as well as reduction in overall performance due to non-optimized hand-constructed Boolean circuits. Note that the implementation in [46] was constructed before many crucial GC optimizations have been proposed, i.e., fixed-key AES garbling [7], half-gates [48], and our GC sequential circuit descriptions [20]. Therefore, we expect our suggested methods not only to have a superior scalability, but also orders of magnitude better performance.

In TinyGarble [20], we also introduced a garbled processor based on the MIPS instruction set for PF-SFE. We showed that sequential descriptions makes GC scale to a wide range of conventional hardware circuits as well as a general-purpose processor. However, our garbled processor in TinyGarble was demonstrated only under the very limiting assumption of PF-SFE where the function is completely hidden at the expense of large area overhead. Unlike our proposal, TinyGarble's MIPS processor for PF-SFE does not offer a trade-off between privacy and performance which makes it impractical for applications with weaker privacy requirements or larger instruction sets and benchmark functions.

Most recently, Wang et al., introduced a secure computation framework using MIPS code by employing both GC and ORAM [49]. They proposed an off-line code analysis to reduce the number of gates to garble in the MIPS circuit and eventually minimize the overhead of computation. Although their use of ORAM helps

to reduce the overall complexity, it prohibits non-interactive computation as, to the best of our knowledge, there is no protocol to adapt ORAM for non-interactive scenarios. Thus, their framework works only in the presence of two parties and therefore cannot benefit from the leakage-resilience feature. Moreover, their implementation is in software whereas ours will be in hardware.

Our Approach. This project will be the first to use a general-purpose processor for implementing leakage-resilient cryptography by leveraging both SFE and PF-SFE. In fact, our approach takes advantage of non-interactive computation via count-limited execution to ensure leakage-resilience and lower the overhead. Prior work has demonstrated that the input-side of the GC protocol can be made non-interactive by proper hardware, e.g., Trusted Platform Modules (TPM) [50]. The work in [28] suggested the notion of One-Time Programs (OTP) which combine GC with very simple tamper-resistant hardware to achieve full leakage-resiliency for both the input and execution side. Since OTP can be done offline, it also removes the bottleneck of network communications incurred by the interactive solutions. In particular, replacing Oblivious Transfer (OT) in interactive GC with OTP can mitigate the picks in the network traffic and the computation in the pre-evaluation phase. Through OTP, one can also lessen the energy consumption by removing the interactive data transfer steps, which is important for portable and mobile clients. Note that, despite its name, OTP can be extended to count-limited execution and not just one execution. One interesting side-benefit of our approach is that it is possible to use it for licensing count-limited secure execution of products.

We will further deliver a robust and configurable hardware platform for secure computation that works not only in PF-SFE settings but also in a more relax privacy-settings of SFE where parties can evaluate a semi-private, revealing only few information about the function, or public function over their private data while benefiting from simplicity of programming a processor. To do so, both parties decide which instruction set they want to use, instruction and data memories' sizes and data location in data memory. The function, whether public, private or semi-private, can be described in a high-level programming language like C or C++, then compiled into assembly code of the agreed-upon instruction set.

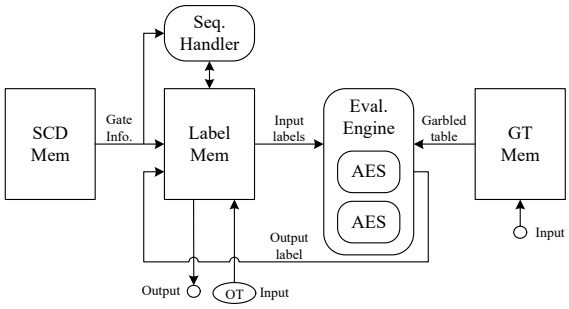

Figure 1: Hardware design for secure evaluator.

In this project, we consider honest-but-curious adversary model as the basis for building a stronger security protocol. Generic ways of modifying GC-based protocols such that they achieve security against stronger malicious adversaries have been proposed, e.g., [51, 52]. We use the most recent reported GC optimizations including free XORs [4], fixed-key block-cipher garbling [7], half-gate [48], and hardware logic synthesis and optimization techniques along with sequential circuit description [20] in order to implement our hardware framework. We demonstrate an implementation of a processor supporting the MIPS (Microprocessor without Interlocked Pipeline Stages) ISA, as an example of a garbled processor for securely evaluating private functions. Figure 2 shows our garbled processor framework which is based on canonical MIPS (Microprocessor without Interlocked Pipeline Stages) instruction set. Figure 1 also illustrates the basic architecture of our secure evaluator on FPGA.

Table 1: Resource allocation and utilization of GC Evaluator on Xilinx Virtex-7 FPGA.

Resource	Estimation	Utilization %
Flip-Flop (FF)	22 035	2,54
Slice LookUp Table (LUT)	21 229	4,90
BRAM	354	24
BUFG	2	6,25

Preliminary Results and Near-Term Objectives.

As preliminary implementation, we realize a GC evaluator that is the essential basic-block for the garbled processor on a Xilinx Virtex-7 FPGA. The resource utilization of this module on our FPGA platform is given

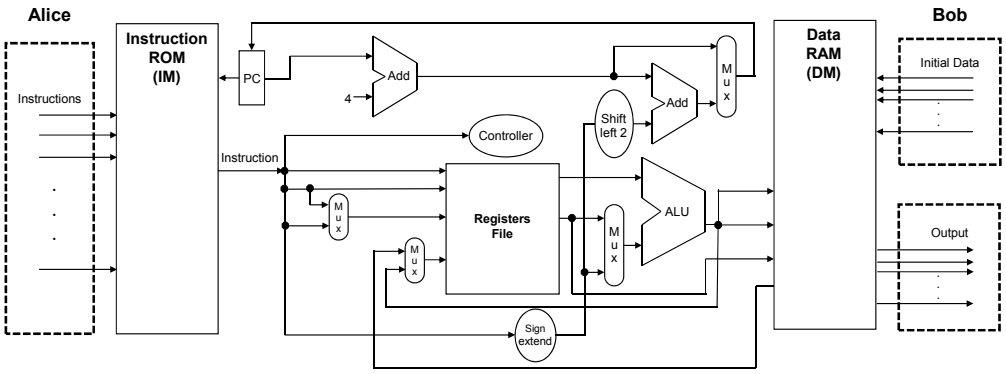

Figure 2: Garbled processor circuit based on MIPS architecture. Alice's and Bob's inputs and the output are shown.

in Table 1. It takes 144 635 clock cycles for this module to execute a single instruction of MIPS processor.

Our near-term objectives include:

- We will design and develop a garbled processor architecture which supports three degrees of freedom for evaluation of an application that would allow trading-off between privacy and performance of the proposed processor: public function, privet function, and semi-private function.
- We plan to implement the first hardware garbled processor on FPGA as proof-of-concept implementation which enables user to develop secure multi-party applications using high-level languages.
- We shall provide an evaluation and performance comparison between our hardware garbled processor and previous GC implementations in software and hardware.
- We will deliver the first practical cryptographically leakage-resilient processor based on our garbled processor using OTP that can hide both function and data from an adversary (PF-SFE).

Mid-Term Objectives.

- We investigate building a leakage-resilient processor using other circuit-based secure computations, e.g., GMW [2], in order to provide trade-off between computation and communication.
- We also plan to study the feasibility of offline ORAM protocol in which communication can be done at once. If possible, one can benefit form the ORAM's lower amortized computation complexity in the garbled processor for leakage-resilient applications.
- We will extent our adversary model from honest-but-curious to a stronger and more realistic malicious model in which the adversary is not required to follow the protocol anymore.

Outlook and Broader Impact. The garbled processor will enable non-expert user to efficiently program in a high-level languages e.g., C/C++ for developing secure multi-party applications. On the other hand, the computation with the garbled processor will ensure a leakage-free computation and guarantee the privacy of both inputs and application against any side-channel attacks. The user-friendly interface and implementation flexibility provided by this thrust pave the way for several new and exciting privacy-preserving tasks.

3.2 Application-Specific Garbling Engines for Complex Matching Algorithms

Research Questions: (i) Can one design the circuit required by an application with a higher than linear complexity such that the task can be performed with a linear circuit size? For example in stable matching (SM) application, is it possible to design a linear size circuit that perform SM? (ii) Can we build a secure stable matching platform that can scale up to large set sizes required by the real applications, beyond the capabilities of the conventional hardware synthesis tools?

Motivation and Problem Statement. The common drawback of modern SFE protocols is their high overhead, mainly due to the inter-party communications, which prohibits the wide usage for real world applications. Therefore, for SFE protocols to be widely adopted, it is crucial to devise methodologies that lower their overhead and make them scalable.

The overhead problem becomes even more pronounced when one considers algorithms with inherently high complexity, i.e., higher than linear. A well-known example of a challenging SFE task is the Stable Matching (SM) problem which has a complexity of $\mathcal{O}(n^2)$. Because of its importance and the challenging nature we use this problem as our driver example. In SM there are two groups of individuals, e.g., men and women, students and universities, or resident students and hospitals. Each individual ranks the members of the other group as a list in the order of preferences, meaning that the first individual in the list is the one that s/he prefers the most. The goal is to assign the members of these two groups to each-other while satisfying the following post-match condition: There shall be no pairs from two groups such that they prefer each-other more than their already assigned partners.

The informal description of this kind of matching is as it sounds: stable; that is, upon termination of the algorithm, if an individual in Group A tries to get assigned to a more preferred member of Group B, it will not be successful as the member of Group B would not accept this assignment. This is because the member of Group B prefers his currently assigned partner to the proposing individual. Thereby, no change will happen and the matching is said to be stable.

Stable Matching has substantial real-world applications: the National Residency Matching Program (NRMP) [53] yearly matches around 34,000 graduating medical students to residency programs in the US [54]. The New York City Department of Education (NYCDOE) matches over 90,000 entering students to public high schools every year [55]. Also many financial applications require SM such as vertical networks and their application in supply chains [56].

A contemporary well known challenging development of SM involves processing of sensitive data which has to be kept private. The current practice to ensure data privacy is by exposing the personal preferences to a third party server and relying on its trustworthiness to perform a secure matching. However, relying on the trusted third party might be unacceptable because there is still a high risk of information leakage and data abuse by the third party. Even if a third party server is indeed trustworthy, it can accidentally expose the user's private data in the event of a compromise. In addition to information leakage, multiple studies [57–59] show that if certain individuals in a SM problem know the input of others, they could leverage this information to manipulate the results. Therefore, a scalable secure SM system is of great value.

State-of-the-Art. A number of researchers have focused on addressing the SM problem since early days of computing, but Gale and Shapley [60] were the first to formalize the SM algorithm. They centered their work on the special case of the marriage problem. In this case there is a set of men of cardinality $|M|$ and a set of women of cardinality $|W|$. They introduce an algorithm which results in stable marriage. Gale and Shapley also proved that the stable match always exists. However, they show that there can be more than one stable assignment and so the stable matching is not a unique assignment. Roth [61] demonstrates that there is always a stable match preferred by men (male-optimal) and there is always a stable match preferred by women (female-optimal). The algorithm which Gale and Shapley propose consists of a number of rounds in which the men propose and the women review these proposals. This algorithm always produces a match which is preferred by men and thus is male-optimal. Gusfield and Irving [58] performed a complete review of stable-matching algorithms.

Fairness is a good motivation that shows how much privacy is crucial in the stable marriage problem: Several researchers showed that when the preferences are known by all individuals, the matching process could be manipulated in different ways [61, 62]. It is even possible for a strategic woman player to misrepresent her preferences list to change the matching process form male-optimal to female-optimal. Golle [63] proposed a privacy-preserving SM system based on re-encryption mixnets and homomorphic encryption.

Franklin et al., then improved this system [64] and made it more efficient by using an efficient multi-party indirect indexing [65]. However, all protocols for secure SM proposed so far use a large number of expensive public-key operations and have not been implemented yet.

Our Approach. In this project we will work on the first scalable secure SM system based on the GC protocol. We plan to build this application by bootstrapping sequential synthesis and TinyGarble framework. However, as the size of groups involved in the SM process increases, no available logic synthesis tool (such as the ones suggested in TinyGarble) has the ability to generate the massive circuit. To overcome this limitation, this proposal suggests designing an alternative Linear Size Circuit (LSC) where the size of the sequential circuit grows linearly instead of quadratic with the group size n. We also propose a general method to scale up the circuit generation which eliminates the constraint on previous circuit generation tools for GC. This method is not limited to SM and can be applied to other GC-based applications. The introduction of LSC along with this new method facilitates an implementation for very large secure SM set sizes, e.g., for matching 65,536 pairs. Furthermore, we devise a new general approach, called early termination technique, to significantly decrease the computation time by reducing the total number of times that the sequential circuit needs to be evaluated.

Preliminary Results and Near-Term Objectives. Our preliminary results show that the early termination technique can bring a tremendous improvement. For example, for set size 1,024, using early termination results in $218\times$ improvement in computation time and communication. Also, our newly proposed sequential circuit has substantially less number of gates. For instance, for set size 1,024, the circuit has only about 22M gates; an infeasible task for the previous art in this domain since the circuit size for any combinational circuit has the complexity of $\mathcal{O}(n^4 \log n)$ and this prohibits them for scaling up to large set sizes.

Our near-term objectives include:

- We plan to implement the first sequential circuit architecture in Figure 3. Prior to this circuit, any GC-based privacy preserving protocol should have used only combinational circuit. Any combinational circuit has the size of $\mathcal{O}(n^4 \log n)$ where the n is the number of participants in each group whereas our sequential circuit size is $\mathcal{O}(n^2 \log n)$. Having this circuit will enable us to scale the secure SM for much higher set sizes since considering a fixed capability of circuit synthesis tool, we can now synthesize the circuit for considerably larger groups.
- We shall design a linear size circuit for SM. We need a synthesis tool to synthesize the circuit required by GC protocol and in fact any synthesis tool has certain limits on the size of the circuit that it can synthesis. In our experiment, Synopsys Design Compiler can at most generate the circuit for set size of 1,000 which may not be enough for many applications. However if we can devise a linear size circuit, using the same synthesis tool, we can produce the circuit for set sizes as big as 50,000.
- We will investigate new techniques to terminate the secure computation as soon as it reaches the final output. In many algorithms, such as SM, it is very difficult to know the execution time of algorithm for reaching the final results. Prediction of runtime of these algorithms is said to be difficult because finding the runtime is as difficult as the actual answer itself. Since every variable in GC protocol is encrypted, we need to design a new mechanism to know when the protocol should be terminated.

Mid-Term Objectives.

- We plan to implement our proposed circuits on various platforms including FPGAs and GPUs to achieve a better performance and faster execution time.
- We shall research and investigate new methods for implementing and efficient secure memory access such as ORAM. Having a secure memory with constant time complexity access will reduce the overhead of one memory access from $\mathcal{O}(n^2)$ to $\mathcal{O}(ploylog(n))$. Reducing the overhead of one secure memory access will cause the total complexity of our methodology to drop down from $\mathcal{O}(n^4 \log n)$ to $\mathcal{O}(n^2 polylog(n))$ which then we can scale our method to much higher set sizes.

- Currently, the power of synthesis tool is the bottleneck of our system. We shall develop a tool to aid our commercial synthesis tool to scale better and generate the circuit with higher number of gates.
- We will investigate usage of other cryptography tools such as homomorphic encryption and GMW to divide the secure SM task into some sub-problems in which each method works more efficiently and hence achieving a better overall performance for this problem.
- We aim to implement our methodology for practical robust efficient fingerprint-based authentication system which can authenticate a user very fast by taking advantage of the scalable GC-based methods discussed in this project by directly translating a robust algorithm such as Bozorth to GC.
- We plan to elevate our security model from standard honest-but-curious to malicious adversary which means we can achieve security even when one of the parties deviates from the protocol but still no information is leaked.

Outlook and Broader Impact. Scalable secure SM algorithm and implementation will yield a framework where different individuals can securely find the stable match list without trusting and relying on any third party. This framework can be used by National Residency Matching Program (NRMP) and other organizations where there is a need to match the members of two different groups with stability condition while not revealing any information related to the preference lists. Secure biometric authentication and matching can help protecting of personal private data.

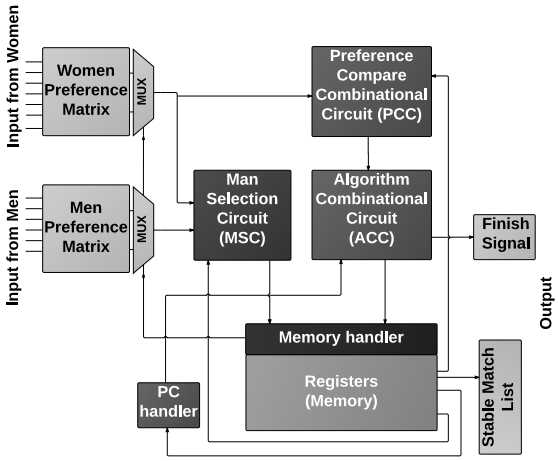

Figure 3: Block diagram architecture of the sequential circuit for implementing secure SM.

3.3 Customize Garbling Engines for Outsourcing Sophisticated Machine Learning Applications

Research Questions: (i) Is it possible to have a privacy-preserving delegation of ML tasks to untrusted server ensuring client-side efficiency and practicality? (ii) Is it possible that the process of outsourcing ML applications leverage the underlying data structure to customize the delegation and make it more efficient? (iii) Can one integrate GC with other secure computation methods, e.g., fully homomorphic encryption, in order to achieve a better efficiency and scalability?

Motivation and Problem Statement. ML is an indispensable tool for extracting value and knowledge from contemporary massive datasets. While complex ML algorithms can benefit a significant number of applications, it is well-known that ML for increasingly large datasets incurs expensive matrix-based storing and linear algebraic costs. Examples of such costly ML approaches are decent-based regression algorithms such as Ridge, Elastic Nets, and Lasso [66], power methods [67], and interior point methodologies [68] that are widely used for computer vision, speech recognition, and pattern recognition tasks. For resource-limited users such as mobile or wearable devices, it is common to delegate the required storage and computations of such intensive tasks involving complex ML algorithms to the cloud servers. Meanwhile, since ML applications typically include handling of sensitive personal, medical, and financial records, privacy of user's data is of central concern in an increasing number of scenarios.

The research problem here is to build practical and customized privacy-preserving linear algebraic ML outsourcing framework enabled by GC primitives. Our framework shall account for the resource constraints imposed by the physical entities involved in an outsourcing task. Conventional secure computing by GC incurs a similar complexity on both the client and server sides which is not desirable in our constrained

client scenario. Instead, our scenario consists of a constrained client securely outsourcing its computation to two different servers. This scenario can be built efficiently since the client only sends an encrypted version of its input by XOR-sharing. Therefore, the client only needs to perform two XOR operations on its input. We plan to design and implement algorithms that for the given constraints including runtime, power consumption, memory footprint, and outsourcing dollar costs (e.g. cloud server expenses), provide secure solutions with the highest accuracy of ML results. Our approach would heavily take advantage of the optimization opportunities that are available for processing a typical ML application by understanding and modeling the performance trade-offs offered by approximate computing, data dimensionality reduction, and structured/sparse data formats as we shown in our previous work [69–71].

State-of-the-Art. Performing privacy-preserving ML algorithms on the cloud has been subject of intensive research, e.g., [72–77]. The available methods range from solutions relying on fully homomorphic encryption (FHE) and Garbled Circuits (GC), to secret sharing [72], trusted hardware [74] and to secure compilers [73]. However, most earlier works in privacy-preserving ML assume different computing models than our ML delegation scenario, and thus they are inappropriate for computationally weak users.

Several practical methods for secure delegation of specific applications have also been in development. For example, (privacy-preserving) large-scale mapping of genomes [78], MapReduce framework [73], and linear programs [72]. The available solutions are either based on security in a non-standard (weak) model [72], or they are inapplicable to massive data learning scenarios that are of interest to our work. For instance, general parallel programming frameworks such as MapReduce ([73]) are not suitable for addressing large-scale ML problems that include iterative updates on a dense correlation matrix. The dependencies prohibit task parallelization that is the basic assumption of the MapReduce framework.

In summary, little work has been done to address the generic problem of secure and scalable delegation of complex ML algorithms in practice; prior works either focus on non-proven secure settings [72] or utilize costly cryptographic operations for a different delegation scenario [75, 77, 79] (such as simpler learning algorithms or multi-party computing).

Note that the large body of ongoing work in differential privacy [80] is orthogonal to our approach, as our threat models are not the same. In their model, a database owner has a complete access to all the data and the assumed threat is that a function over the data is released to a third party. In our model, the one with whom the database is shared poses a threat. Another relevant but orthogonal area to ours is the field of verifiable computing [81–83]. Verifiable computing schemes are orthogonal to our delegation scenario as their focus is on finding ways to verify that the algorithm is run correctly by the cloud, rather than hiding the information regrading the data and the solution to the algorithm (from the cloud). Such protocols can be added on the top of our suggested method.

Our Approach and Near-Term Objectives. We make the following two observation for building our customized secure outsourcing framework: (i) ML applications provide the unique opportunity in that the solution results are tolerant to approximations of the input data, as supported by our earlier results [84]. (ii) Many real world ML datasets exhibit properties such as sparsity or low-dimensional modularized structures. We have shown that it is possible to exploit these structures to increase the performance, reduce the communication, and reduce the memory constraint on various ML algorithms in our previous works [69–71]. We believe it is possible to take advantage of this property to design a customizable and efficient implementation of our framework. Our near-term goals include:

- We will complete our circuit implementations of GC-based dense and sparse matrix multiplication as those are the key building blocks of linear algebraic ML applications.
- Investigate and design mechanisms for breaking down the computing task between local resource-limited client vs. remote powerful cloud server based on the physical constraints such as network bandwidth and computational power.

Mid-Term Objectives.

- We shall design GC implementations that are optimized for different data structures. We plan to customize GC for matrix data structures such as sparse and dense formats, as well as graph data structures including bipartite and power-law graphs that widely appear in ML applications.
- We plan to investigate hybrid methodologies that consider other security primitives along with GC such as secret sharing and fully homomorphic encryption. Our objective is to optimize the overall performance (in terms of runtime, memory footprint, power and computational expenses) by leveraging the trade-offs between different cryptography primitives. For example, a secure matrix multiplication can be broken down into several smaller matrix multiplications and an overall summation. In this case, depending on the dimension and structure of the matrices involved, a customized hybrid approach cab yield a better performance.
- We plan to model and quantize the cost of secure outsourcing based on the properties of the platform and data involved in the ML computation. This model would reveal a trade-off between the performance and accuracy of the ML results to the user which can be utilized to tune the secure outsourcing framework for the target performance objectives.
- We shall develop our approach to become secure against malicious adversaries vs. the current attack model which is honest-but-curious. This will make our assumptions stronger about what an adversary can do. In this case, the client is secure against any server-side deviations from the protocol .

Outlook and Broader Impact. Our framework can be universally integrated on the top of state-of-art machine learning and data processing applications on resource-limited users such as mobile phones, tablet, and wearable devices to preserve the privacy of client; the sensitive client information would not revealed to the server while using the cloud power. The user can specify parameters such runtime, power and memory footprint and our framework would generate the most accurate implementation of secure linear algebraic ML application that meets those criteria. Several contemporary ML applications including deep learning, approximate PCA, and various regression/classification can be secured in our framework.

4 Timeline and Management Plan

My plan is to use the grant to fund 1 full-time PhD student (A) and 1 student for half the academic year (B) over 3 years and to partially support my summer research. The schedule for carrying out each of the research projects corresponding to the main 3 thrusts of my proposal is shown in Figure 2. I will be using matching funds from my other grants to supply the materials and test devices as needed.

Project	Y1	Y2	Y3
3.1	A,P	A	
3.2	B	B,P	A,B,P
3.3		A,B	A,B,P

Table 2: Time table of PI's research plan. The symbol "Y" indicates the year. "A" and "B" are my two students at UCSD. Symbol "P" represents PI's summer research.

5 Education Program

My educational goal is to create an environment in which students can actively learn the state-of-the-art concepts, tools, and problem solving methods that empower them for their future roles as engineers and researchers. To achieve this goal, an important step is to identify promising fields that are (or going to be) of high interest and demand in both academia and industry. My long-term educational vision is to teach students a creative and critical way of thinking so that they can address a broad set of other problems in different areas that can benefit from the same concepts that they learn in their courses and through research. All my class notes, slides, seminar videos, readings, resulting codes, reports, articles, data and other educational materials will be publicly available through the NSF-funded Trust-HUB [24].

Part of my educational philosophy is to infuse my students with confidence in themselves; I encourage them to participate in research early in their careers, develop functional hardware and software, write papers, attend conferences, prepare presentations, practice and deliver talks, and acquire teaching skills. This

section details the new opportunities that will be brought by the current research proposal with regard to undergraduate education, graduate education, and women and minority outreach initiatives.

5.1 Undergraduate Education

I believe that research and teaching are reciprocal activities and hence I have always integrated research within my teaching. In all my courses, a fine portion of the course concentrates on motivating examples and homework problems that stem from my research. As a result, students are exposed to real-world and contemporary challenges which make them appreciate the importance of the techniques they learn. Three years ago, I have designed a new senior-level undergraduate course called "Advanced digital design, synthesis, and optimization on FPGA" in Rice University. I have created this course to give students an opportunity to experience the steps necessary for building real systems based on the theoretical concepts that they have learned in DSP, logic design, and communication courses. By the end of the semester, the students develop the necessary skills to build processors suitable for numerically intensive tasks; and they experience a cross layer approach to design which went all the way from application acceleration, to system-level and block-level design of the DSP and encryption algorithms, to DSP optimizations (e.g., pipelining, unfolding, and parallelizing), MATLAB simulations, and to system implementation on FPGA board (including various optimization and verification.) The feedback from the students has been very positive.

To integrate my teaching and research efforts, I will organize a seminar-based course on SFE that includes papers from hardware design and architecture in addition to security, with the goal of exposing students including senior undergraduates and early graduate students to interdisciplinary research. Students will learn the mathematical concepts and techniques for SFE as well as the issues with hardware implementation. I plan to prepare lectures that discuss the ever-increasing applications of SFE techniques and the shortcomings of the current methods. I will also design homework assignments which require students to do a variety of complexity analysis on different SFE protocols. Working on real applications will help them better grasp the challenging concepts of model complexity, adversary models, and cryptographic primitives.

5.2 Graduate Education

I will involve 2 doctoral students in the proposed research, who will have the opportunity to study theoretical problems and gain hands-on experience by implementing the proposed projects on real platforms. My lab has demonstrated successful systems-building research in the past, and we anticipate opportunities for hands-on work in several of the directions of the proposed plan, including leakage-resilient processor and developing new methods for scaling up the GC protocol, applying such methods to create novel practical secure stable matching for real-world set sizes and secure outsourcing a ML application with proof-of-concept hardware implementations. Since my research in embedded systems is interdisciplinary and intersects with hardware optimization and security, I attract students from different backgrounds. This creates a diversity of knowledge and opinions and an opportunity for knowledge exchange among different disciplines. I particularly encourage cross-collaborative project groups.

In the spring quarter, I plan to offer a new graduate level course, "Hardware and embedded systems security", which directly involves hardware design. The course covers a wide range of topics pertaining to security of hardware embedded systems, including cryptographic processors, secure memory access, hardware IT protection by monitoring and watermarking FPGA security, physical and side-channel attacks.

6 Broader Impacts of the Proposed Work

Women and Minority Outreach Initiatives. One of the key objectives of my synergistic research and teaching approach has always been to explore and to address the issues related to *retention* and *diversity* of

students in science and engineering (S& E). The retention problems for under-represented minorities and women are much more *acute*. To address the problem, I emphasize on (i) my diverse set of experiences as a female student, mentor and educator; (ii) the invaluable experiences that my former supervisors, mentors, peers, and colleagues share with me; (iii) the wealth of body of literature on the subjects of diversity and retention in the United States [85–87].

As a major step to establish a minority outreach initiative, I founded *E*xCEL a network of women in the ECE Department at Rice University that provides community, mentoring, and cultural enrichment for students [88]. This network also serves to promote career opportunities and cultivate women leadership. In addition, we hope to improve the visibility of women in engineering and to advocate the importance of diversity in ECE. Another major goal of the group is to outreach, which includes inspiring and attracting future generations of underrepresented groups into our field. ExCEL has already established itself as a well-known student association which hosts a number of different educational and outreach seminars annually for undergraduate and graduate audience. I plan to start an ExCEL-like initiative in UCSD where I have recently joined as a full Professor (November 2015).

Roughly half of the students in PI's research group are females, which include 1 post-doc and 3 PhD students. In agreement with their interests and strengths, I am planning to assign at least one of them to work on the GC@Scale project. I will also continue to address the diversity and retention problems among women and minority students by studying the problems' root, taking personal initiatives, organizing motivational seminars, and contributing to different mentoring chapters available at UCSD such as CAMP (California Louis Stokes Alliance for Minority Participation in Science, Engineering and Mathematics), and IDEA (Inclusion, Diversity, Excellence, and Advancement) Engineering Student Center.

Dissemination. I will publish research results and findings in academic conferences and journals. I will continue my tradition of demonstrating research results with prototypes/demo in conferences. The PI strongly believes that by open-source publishing of the code pertaining to the projects' implementation, research becomes much more accessible and will have a higher impact. For example, the source-code of our recent work, TinyGarble [20], is publicly available on GitHub[1]. Open access tools allow researchers in related areas such as secure ML to broaden the spectrum of research resulting from our project. In addition, presentations, survey papers, and tutorials at conferences and summer schools will all be available via the NSF-funded Trust-HUB web portal where Prof. Koushanfar is also a PI [24].

Open Access Through Trust-Hub. The PI will make much of her course material freely available through Trust-HUB [24]. Based on concepts pioneered in open-source computing.

Technology Transfer. The PI has a total of 10 patents and have a history of technology transfer. I will leverage my collaborations with industry leaders to ensure timely technology transfer to industry. My collaborations have already led to joint publications patents and possible product adoption.

Scientific Impact. The GC@Scale proposed thrusts are intended to produce conceptual, theoretical and practical contributions. The goals are: (i) Building a new GC-based hardware emulation framework to realize a general purpose processor for secure computation. The new Garbled processor facilitates rapid prototyping of new privacy-preserving applications and provides designers with high-level, user-friendly interfaces. The processor is leakage-resilience and avoids costly communications by a non-interactive protocol. (ii) Creating challenging application-specific GC matching engines where the underlying algorithms inherently incur a higher than linear complexity. Using secure stable matching as the driver example, the first set of practical methods and tools as well as generalization to a family of standing complex problem will be presented. (iii) Devising new GC-based computing engines for efficient outsourcing of ML applications. Throughout the project we follow an end-to-end design approach that relies on evaluations on real hardware testbeds. The results of GC@Scale directly translate to stronger cryptography and security approaches that

[1] https://github.com/esonghori/TinyGarble

subsequently enable developing new sets of applications not feasible earlier.

Education Impact. My educational initiatives merge paradigm-based and pragmatical teaching methods. My expertise in applied computing and statistical modeling as well as computer security and hardware design allows me to teach courses that merge these topics and enable education of a new generation of researchers and developers that can leverage on and contribute to these fields. I will expose undergraduate students to research literature and actively involve them in research and prepare them for their roles in both industry and academia. I also strongly believe that by publishing the software tools and the source codes pertaining the implementations of the proposed work, my research becomes much more accessible and will have a higher impact.

Broader Impacts of the Proposed Work. GC@Scale will have a significant impact on the practical realization of privacy preserving algorithms through creation of user-friendly general purpose processing solutions for GC, leakage-resilient platforms, as well as scalable application-specific secure methodologies. The fundamental and practicable solutions offered by GC@Scale are of increasing importance in the modern world of data abundance, where complex matching and/or ML algorithms are commonly used as the data analytics engine operating on sensitive data. The applications are far reaching and include privacy-preserving processing of medical, genome, and biometric data, as well as face recognition, voting, auctions, search and cloud-based data analytics. The research program is interdisciplinary and makes synergy not just across the fields of design/design automation (DA) and security but also software/compiler design and ML. The GC@Scale software tools and hardware modules will contribute to a lively and interactive education in security and DA will be relevant to several developers outside academia who develop privacy preserving algorithms and applications. Consistent with PI's strong prior record in research, education and outreach, the GC@Scale plan includes an ambitious educational program that targets both undergraduate/graduate students, and also addresses issues related to outreach to younger generations, women and minorities.

7 Results from Prior NSF Support: Intellectual Merits (IM) and Broader Impact (BI)

CAREER: Coordinated Data-Driven Modeling and Optimization for Wireless Sensor Networks, CNS-0644289 (2007-2013): (IM) PI Koushanfar devised novel data-driven modeling methods, scalable modular structures, and optimization algorithms that comprehensively abstract, capture and operate on traces of deployed wireless sensor networks. (BI) Impact on real deployed wireless networks and publications including [89–93].

Algorithmic Techniques for Post-Silicon Characterization Using Infrared Emissions, CCF-1116858 (2012-2014): (IM) PI Koushanfar (in collaboration with Co–PI Woods and PI Reda from Brown University) performed an algorithmic analysis of infrared emissions from the backside of ICs. (BI) Trojan detection and post-silicon power/thermal characterization were accomplished resulting in publications including [94–97].

CRI:Collaborative Research: CI-ADDO-NEW: Trust-Hub: Design of Trust Benchmarks, Hardware Validation Platforms and a Web-Based Dissemination Portal, CNS-1059416 (2011-2014): (IM) PI Koushanfar (in collaboration with three other PIs in other universities) developed Trust-Hub, a central web-based repository for technical papers, benchmarks, hardware platforms, source codes, tools. (BI) The project accelerated hardware security research and resulted in publications including [22, 94, 95, 98–102]. Trust-Hub is a publicly available web site supporting an interactive forum, which is an active resource for research, education and collaboration in security field.

CI-EN: Trust-Hub: Development of Benchmarks, Metrics, and Validation Platforms for Hardware Security, and a Web-based Dissemination Portal, CNS-1513063 (2015-2018: (IM) This is a continuation of the original Trust-Hub project. (BI) It allows the PIs to further build and develop their community research initiative and continue accelerating research in this important and emerging domain.

References

[1] Andrew C-C Yao, "How to generate and exchange secrets," in *FOCS*. IEEE, 1986, pp. 162–167.

[2] Oded Goldreich, Silvio Micali, and Avi Wigderson, "How to play any mental game or a completeness theorem for protocols with honest majority," in *Symposium on Theory of Computing (STOC'87)*. 1987, pp. 218–229, ACM.

[3] Dahlia Malkhi, Noam Nisan, Benny Pinkas, and Yaron Sella, "Fairplay-secure two-party computation system.," in *USENIX Security*. 2004, pp. 287–302, USENIX.

[4] Vladimir Kolesnikov and Thomas Schneider, "Improved garbled circuit: Free XOR gates and applications," in *ICALP'08*. 2008, vol. 5126 of *LNCS*, pp. 486–498, Springer.

[5] Benny Pinkas, Thomas Schneider, Nigel P Smart, and Stephen C Williams, "Secure two-party computation is practical," in *ASIACRYPT*, pp. 250–267. Springer, 2009.

[6] Yan Huang, David Evans, Jonathan Katz, and Lior Malka, "Faster secure two-party computation using garbled circuits," in *USENIX Security'11*. 2011, pp. 539–554, USENIX.

[7] Mihir Bellare, Viet Tung Hoang, Sriram Keelveedhi, and Phillip Rogaway, "Efficient garbling from a fixed-key blockcipher," in *S&P*. 2013, pp. 478–492, IEEE.

[8] Julien Bringer, Hervé Chabanne, and Alain Patey, "Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends," *Signal Processing Magazine, IEEE*, pp. 42–52, 2013.

[9] David Evans, Yan Huang, Jonathan Katz, and Lior Malka, "Efficient privacy-preserving biometric identification," in *NDSS*, 2011.

[10] Mauro Barni, Pierluigi Failla, Vladimir Kolesnikov, Riccardo Lazzeretti, Ahmad-Reza Sadeghi, and Thomas Schneider, "Secure evaluation of private linear branching programs with medical applications," in *ESORICS*, pp. 424–439. Springer, 2009.

[11] Moni Naor, Benny Pinkas, and Reuben Sumner, "Privacy preserving auctions and mechanism design," in *EC*. 1999, pp. 129–139, ACM.

[12] Justin Brickell, Donald E Porter, Vitaly Shmatikov, and Emmett Witchel, "Privacy-preserving remote diagnostics," in *CCS*. ACM, 2007, pp. 498–507.

[13] Somesh Jha, Louis Kruger, and Vitaly Shmatikov, "Towards practical privacy for genomic computation," in *S&P*. 2008, pp. 216–230, IEEE.

[14] M.R. Albrecht, C. Rechberger, T. Schneider, T. Tiessen, and M. Zohner, "Ciphers for MPC and FHE," in *Advances in Cryptology – EUROCRYPT*, 2015, pp. 430–454.

[15] Lior Malka, "Vmcrypt: modular software architecture for scalable secure computation," in *CCS*. 2011, pp. 715–724, ACM.

[16] Wilko Henecka and Thomas Schneider, "Faster secure two-party computation with less memory," in *ASIACCS*. 2013, pp. 437–446, ACM.

[17] Benjamin Kreuter, Abhi Shelat, and Chih-Hao Shen, "Billion-gate secure computation with malicious adversaries.," in *USENIX Security*. 2012, pp. 285–300, USENIX.

[18] Benjamin Kreuter, Abhi Shelat, Benjamin Mood, and Kevin RB Butler, "PCF: A portable circuit format for scalable two-party secure computation.," in *USENIX Security*. 2013, pp. 321–336, USENIX.

[19] Martin Franz, Andreas Holzer, Stefan Katzenbeisser, Christian Schallhart, and Helmut Veith, "Cbmc-gc: An ansi c compiler for secure two-party computations," in *Compiler Construction*. Springer, 2014, pp. 244–249.

[20] Ebrahim M Songhori, Siam U Hussain, Ahmad-Reza Sadeghi, Thomas Schneider, and Farinaz Koushanfar, "Tinygarble: Highly compressed and scalable sequential garbled circuits," in *IEEE S&P'15*. 2015, pp. 411–428, IEEE.

[21] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," in *STOC'87*. 1987, pp. 218–229, ACM.

[22] Daniel Demmler, Ghada Dessouky, Farinaz Koushanfar, Ahmad-Reza Sadeghi, Thomas Schneider, and Shaza Zeitouni, "Automated synthesis of optimized circuits for secure computation," in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2015, pp. 1504–1517.

[23] AJ Paverd, Andrew Martin, and Ian Brown, "Modelling and automatically analysing privacy properties for honest-but-curious adversaries," Tech. Rep., Tech. Rep., 2014.[Online]. Available: https://www. cs. ox. ac. uk/people/andrew. paverd/casper/casper-privacy-report. pdf.

[24] Fermentas Inc, "Trust *HUB*," .

[25] Eric Brier, Christophe Clavier, and Francis Olivier, "Correlation power analysis with a leakage model," in *Cryptographic Hardware and Embedded Systems-CHES 2004*, pp. 16–29. Springer, 2004.

[26] Daniel Genkin, Adi Shamir, and Eran Tromer, "Rsa key extraction via low-bandwidth acoustic cryptanalysis," in *Advances in Cryptology–CRYPTO 2014*, pp. 444–461. Springer, 2014.

[27] Dakshi Agrawal, Bruce Archambeault, Josyula R Rao, and Pankaj Rohatgi, "The em sidechannel (s)," in *Cryptographic Hardware and Embedded Systems-CHES 2002*, pp. 29–45. Springer, 2003.

[28] Shafi Goldwasser, Yael Tauman Kalai, and Guy N Rothblum, "One-time programs," in *Advances in Cryptology – CRYPTO'08*, vol. 5157 of *LNCS*, pp. 39–56. Springer, 2008.

[29] Stefan Dziembowski and Krzysztof Pietrzak, "Leakage-resilient cryptography," in *Foundations of Computer Science, 2008. FOCS'08. IEEE 49th Annual IEEE Symposium on*. IEEE, 2008, pp. 293–302.

[30] Anil K Jain, Arun Ross, and Salil Prabhakar, "An introduction to biometric recognition," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 14, no. 1, pp. 4–20, 2004.

[31] Michael O Rabin, "How to exchange secrets with oblivious transfer.," *IACR Cryptology ePrint Archive*, vol. 2005, pp. 187, 2005.

[32] Oded Goldreich, Silvio Micali, and Avi Wigderson, "How to play any mental game," in *STOC*. 1987, pp. 218–229, ACM.

[33] Assaf Ben-David, Noam Nisan, and Benny Pinkas, "FairplayMP: a system for secure multi-party computation," in *CCS*. 2008, pp. 257–266, ACM.

[34] D. Malkhi, N. Nisan, B. Pinkas, and Y. Sella, "Fairplay – a secure two-party computation system," in *USENIX Security'04*. 2004, pp. 287–302, USENIX.

[35] A. Ben-David, N. Nisan, and B. Pinkas, "FairplayMP: a system for secure multi-party computation," in *ACM CCS'08*. 2008, pp. 257–266, ACM.

[36] W. Henecka, S. Kögl, A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, "TASTY: Tool for Automating Secure Two-partY computations," in *ACM CCS'10*. 2010, pp. 451–462, ACM.

[37] Y. Huang, D. Evans, J. Katz, and L. Malka, "Faster secure two-party computation using garbled circuits," in *USENIX Security'11*. 2011, pp. 539–554, USENIX.

[38] L. Malka, "VMCrypt - modular software architecture for scalable secure computation," in *ACM CCS'11*. 2011, pp. 715–724, ACM.

[39] Benjamin Mood, Lara Letaw, and Kevin Butler, "Memory-efficient garbled circuit generation for mobile devices," in *Financial Cryptography and Data Security*, AngelosD. Keromytis, Ed., vol. 7397 of *Lecture Notes in Computer Science*, pp. 254–268. Springer Berlin Heidelberg, 2012.

[40] B. Kreuter, A. Shelat, and C.-H. Shen, "Billion-gate secure computation with malicious adversaries.," in *USENIX Security'12*. 2012, pp. 285–300, USENIX.

[41] A. Holzer, M. Franz, S. Katzenbeisser, and H. Veith, "Secure two-party computations in ANSI C," in *ACM CCS'12*. 2012, pp. 772–783, ACM.

[42] T. Schneider and M. Zohner, "GMW vs. Yao? Efficient secure two-party computation with low depth circuits," in *FC'13*. 2013, vol. 7859 of *LNCS*, pp. 275–292, Springer.

[43] B. Kreuter, A. Shelat, B. Mood, and K. R. B. Butler, "PCF: A portable circuit format for scalable two-party secure computation.," in *USENIX Security'13*. 2013, pp. 321–336, USENIX.

[44] Y. Zhang, A. Steele, and M. Blanton, "PICCO: a general-purpose compiler for private distributed computation," in *ACM CCS'13*. 2013, pp. 813–826, ACM.

[45] E. M. Songhori, S. U. Hussain, A.-R. Sadeghi, T. Schneider, and F. Koushanfar, "TinyGarble: Highly compressed and scalable sequential garbled circuits," in *IEEE S&P'15*. 2015, pp. 411–428, IEEE.

[46] Kimmo Järvinen, Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and Thomas Schneider, "Garbled circuits for leakage-resilience: Hardware implementation and evaluation of one-time programs," in *CHES*, pp. 383–397. Springer, 2010.

[47] Krzysztof Pietrzak, "Provable security for physical cryptography," *the proceedings of WEWORC*, pp. 200–210, 2009.

[48] Samee Zahur, Mike Rosulek, and David Evans, "Two halves make a whole," in *Advances in Cryptology – EUROCRYPT'15*, vol. 9057 of *LNCS*, pp. 220–250. Springer, 2015.

[49] Xiao Shaun Wang, S. Dov Gordon, Allen McIntosh, and Jonathan Katz, "Secure computation of MIPS machine code," Cryptology ePrint Archive, Report 2015/547, 2015, http://eprint.iacr.org/.

[50] Vandana Gunupudi and Stephen R Tate, "Generalized non-interactive oblivious transfer using count-limited objects with applications to secure mobile agents," in *Financial Cryptography and Data Security*, pp. 98–112. Springer, 2008.

[51] Yehuda Lindell and Benny Pinkas, "An efficient protocol for secure two-party computation in the presence of malicious adversaries," in *EUROCRYPT*. Springer, 2007.

[52] Yehuda Lindell and Benny Pinkas, "Secure two-party computation via cut-and-choose oblivious transfer," *Journal of cryptology*, vol. 25, no. 4, pp. 680–722, 2012.

[53] National Residency Matching Program, ," http://www.nrmp.org.

[54] Stable Matching Algorithms, ," http://www.dcs.gla.ac.uk/research/algorithms/stable/.

[55] Atila Abdulkadiroğlu, Parag A Pathak, and Alvin E Roth, "The New York city high school match," *American Economic Review*, pp. 364–367, 2005.

[56] Michael Ostrovsky, "Stability in supply chain networks," *American Economic Review*, vol. 98, no. 3, pp. 897–923, 2008.

[57] David Gale and Marilda Sotomayor, "Ms. machiavelli and the stable matching problem," *American Mathematical Monthly*, pp. 261–268, 1985.

[58] Dan Gusfield and Robert W Irving, *The stable marriage problem: structure and algorithms*, vol. 54, MIT press Cambridge, 1989.

[59] Chung-Piaw Teo, Jay Sethuraman, and Wee-Peng Tan, "Gale-Shapley stable marriage problem revisited: strategic issues and applications," in *Integer Programming and Combinatorial Optimization (IPCO'99)*. 1999, vol. 1610 of *LNCS*, pp. 429–438, Springer.

[60] David Gale and Lloyd S Shapley, "College admissions and the stability of marriage," *American Mathematical Monthly*, pp. 9–15, 1962.

[61] Alvin E Roth, "The economics of matching: Stability and incentives," *Mathematics of operations research*, vol. 7, no. 4, pp. 617–628, 1982.

[62] Chung-Piaw Teo, Jay Sethuraman, and Wee-Peng Tan, "Gale-Shapley stable marriage problem revisited: Strategic issues and applications," *Management Science*, vol. 47, no. 9, pp. 1252–1267, 2001.

[63] Philippe Golle, "A private stable matching algorithm," in *FC'06*. 2006, vol. 4107 of *LNCS*, pp. 65–80, Springer.

[64] Matthew Franklin, Mark Gondree, and Payman Mohassel, "Improved efficiency for private stable matching," in *CT-RSA'07*. 2006, vol. 4377 of *LNCS*, pp. 163–177, Springer.

[65] Matthew Franklin, Mark Gondree, and Payman Mohassel, "Multi-party indirect indexing and applications," in *ASIACRYPT'07*. 2007, vol. 4833 of *LNCS*, pp. 283–297, Springer.

[66] R. Tibshirani, "Regression shrinkage and selection via the lasso," *J. Royal Statist. Soc B*, vol. 58, no. 1, pp. 267–288, 1996.

[67] M. Figueiredo, R. Nowak, and S. Wright, "Gradient projections for sparse reconstruction: Application to compressed sensing and other inverse problems," vol. 1, no. 4, pp. 586–597, 2007.

[68] Michael C. Ferris and Todd S. Munson, "Interior-point methods for massive support vector machines," *SIAM J. on Optimization*, pp. 783–804, 2002.

[69] Azalia Mirhoseini, Eva Dyer, Ebrahim Songhori, Richard Baraniuk, Farinaz Koushanfar, et al., "Rankmap: A platform-aware framework for distributed learning from dense datasets," *arXiv preprint arXiv:1503.08169*, 2015.

[70] Azalia Mirhoseini, Ebrahim M. Songhori, Bita Darvish Rouhani, and Farinaz Koushanfar, "Flexible transformations for learning big data," in *Proceedings of the 2015 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems*. ACM, 2015, pp. 453–454.

[71] B.D. Rouhani, E.M. Songhori, A. Mirhoseini, and F. Koushanfar, "Ssketch: An automated framework for streaming sketch-based analysis of big data on fpga," in *Field-Programmable Custom Computing Machines (FCCM), 2015 IEEE 23rd Annual International Symposium on*, May 2015, pp. 187–194.

[72] Mikhail J Atallah and Keith B Frikken, "Securely outsourcing linear algebra computations," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*. ACM, 2010, pp. 48–59.

[73] Kehuan Zhang, Xiaoyong Zhou, Yangyi Chen, XiaoFeng Wang, and Yaoping Ruan, "Sedic: privacy-aware data intensive computing on hybrid clouds," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 515–526.

[74] Sumit Bajaj and Radu Sion, "Trusteddb: A trusted hardware-based database with privacy and data confidentiality," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 26, no. 3, pp. 752–765, 2014.

[75] Thore Graepel, Kristin Lauter, and Michael Naehrig, "Ml confidential: Machine learning on encrypted data," in *Information Security and Cryptology–ICISC 2012*, pp. 1–21. Springer, 2013.

[76] Valeria Nikolaenko, Udi Weinsberg, Sotiris Ioannidis, Marc Joye, Dan Boneh, and Nina Taft, "Privacy-preserving ridge regression on hundreds of millions of records," in *Security and Privacy (SP), 2013 IEEE Symposium on*. IEEE, 2013, pp. 334–348.

[77] Raphael Bost, Raluca Ada Popa, Stephen Tu, and Shafi Goldwasser, "Machine learning classification over encrypted data," in *22nd Annual Network and Distributed System Security Symposium, NDSS 2015, San Diego, California, USA, February 8-11, 2014*, 2015.

[78] Yangyi Chen, Bo Peng, XiaoFeng Wang, and Haixu Tang, "Large-scale privacy-preserving mapping of human genomic sequences on hybrid clouds.," in *NDSS*, 2012.

[79] Kartik Nayak, Xiao Shaun Wang, Stratis Ioannidis, Udi Weinsberg, Nina Taft, and Elaine Shi, "*GraphSC*: Parallel secure computation made easy," in *IEEE Symposium on Security and Privacy (S & P)*, 2015.

[80] Cynthia Dwork, "Differential privacy," in *Encyclopedia of Cryptography and Security*, pp. 338–340. Springer, 2011.

[81] Shafi Goldwasser, Silvio Micali, and Charles Rackoff, "The knowledge complexity of interactive proof-systems," in *Proceedings of the seventeenth annual ACM symposium on Theory of computing*. ACM, 1985, pp. 291–304.

[82] M. Sudan, "Probabilistically checkable proofs," *Commun. ACM*, vol. 52, no. 3, pp. 7684, 2009.

[83] Shafi Goldwasser, Yael Tauman Kalai, and Guy N Rothblum, "Delegating computation: interactive proofs for muggles," in *Proceedings of the fortieth annual ACM symposium on Theory of computing*. ACM, 2008, pp. 113–122.

[84] A. Mirhoseini and F. Koushanfar, "Enabling privacy preserving computing at scale by modular signal processing," *In Proceedings of Allerton Conference on Communication, Control, and Computing*, 2015.

[85] Andrea H. Tapia and Lynette Kvasny, "Recruitment is never enough: Retention of women and minorities in the it workplace," in *Proceedings of the 2004 SIGMIS Conference on Computer Personnel Research: Careers, Culture, and Ethics in a Networked Environment*. 2004, pp. 84–91, ACM.

[86] Alan Seidman, "Minority student retention: Resources for practitioners," *New Directions for Institutional Research*, vol. 2005, no. 125, pp. 7–24, 2005.

[87] Tracy L. Lewis, Wanda J. Smith, France Bélanger, and K. Vernard Harrington, "Are technical and soft skills required?: The use of structural equation modeling to examine factors leading to retention in the cs major," in *Proceedings of the Fourth International Workshop on Computing Education Research*. 2008, pp. 91–100, ACM.

[88] "Women excel network at rice university," .

[89] Yousra Alkabani, Farinaz Koushanfar, Negar Kiyavash, and Miodrag Potkonjak, "Trusted integrated circuits: A nondestructive hidden characteristics extraction approach," in *Information Hiding*. Springer, 2008, pp. 102–117.

[90] Yousra Alkabani and Farinaz Koushanfar, "Consistency-based characterization for ic trojan detection," in *Proceedings of the 2009 International Conference on Computer-Aided Design*. ACM, 2009, pp. 123–127.

[91] Farinaz Koushanfar, Ahmad-Reza Sadeghi, and Hervé Seudie, "Eda for secure and dependable cybercars: challenges and opportunities," in *Proceedings of the 49th Annual Design Automation Conference*. ACM, 2012, pp. 220–228.

[92] Mohammad Tehranipoor and Farinaz Koushanfar, "A survey of hardware trojan taxonomy and detection," 2009.

[93] Azalia Mirhoseini, Miodrag Potkonjak, and Farinaz Koushanfar, "Coding-based energy minimization for phase change memory," in *Proceedings of the 49th Annual Design Automation Conference*. ACM, 2012, pp. 68–76.

[94] Farinaz Koushanfar, Saverio Fazzari, Carl McCants, William Bryson, Matthew Sale, Peilin Song, and Miodrag Potkonjak, "Can eda combat the rise of electronic counterfeiting?," in *Proceedings of the 49th Annual Design Automation Conference*, 2012, pp. 133–138.

[95] Sheng Wei, Kai Li, Farinaz Koushanfar, and Miodrag Potkonjak, "Hardware trojan horse benchmark via optimal creation and placement of malicious circuitry," in *Proceedings of the 49th Annual Design Automation Conference*. ACM, 2012, pp. 90–95.

[96] Sheng Wei, Kai Li, Farinaz Koushanfar, and Miodrag Potkonjak, "Provably complete hardware trojan detection using test point insertion," in *Computer-Aided Design (ICCAD), 2012 IEEE/ACM International Conference on*. IEEE, 2012, pp. 569–576.

[97] Sheng Wei, Ani Nahapetian, Michael Nelson, Farinaz Koushanfar, and Miodrag Potkonjak, "Gate characterization using singular value decomposition: Foundations and applications," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 2, pp. 765–773, 2012.

[98] Farinaz Koushanfar, "Provably secure active ic metering techniques for piracy avoidance and digital rights management," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 1, pp. 51–63, 2012.

[99] Negar Kiyavash, Farinaz Koushanfar, Todd P Coleman, and Mavis Rodrigues, "A timing channel spyware for the csma/ca protocol," *Information Forensics and Security, IEEE Transactions on*, vol. 8, no. 3, pp. 477–487, 2013.

[100] D. Shahrjerdi, J. Rajendran, S. Garg, F. Koushanfar, and R. Karri, "Shielding and securing integrated circuits with sensors," in *IEEE/ACM International Conference on Computer-Aided Design, ICCAD*, 2014, pp. 170–174.

[101] M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1283–1295, 2014.

[102] E.M. Songhori, S.U. Hussain, A-R. Sadeghi, T. Schneider, and F. Koushanfar, "TinyGarble: Highly compressed and scalable sequential garbled circuits," in *IEEE Symposium on Security and Privacy (S&P)*, 2015, pp. 411–428.