Laconic Conditional Disclosure of Secrets and Applications

Nico Döttling†, Sanjam Garg‡, Vipul Goyal†, Giulio Malavolta§
†CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
‡University of California Berkeley, Berkeley, USA
§Carnegie Mellon University, Pittsburgh, USA
§Simons Institute for the Theory of Computing, Berkeley, USA

Abstract—In a Conditional Disclosure of Secrets (CDS) a verifier V wants to reveal a message m to a prover P conditioned on the fact that x is an instance of some NP-language L. An honest prover (holding the corresponding witness w) always obtains the message m at the end of the interaction. On the other hand, if x ∈ / L we require that no PPT P∗ can learn the message m. We introduce laconic CDS, a two round CDS protocol with optimal computational cost for the verifier V and optimal communication cost. More specifically, the verifier’s computation and overall communication grows with $poly(|x|, \lambda, \log(T))$, where λ is the security parameter and T is the verification time for checking that $x \in / L$ (given w). We obtain constructions of laconic CDS under standard assumptions, such as CDH or LWE.

Laconic CDS serves as a powerful tool for maliciousifying semi-honest protocols while preserving their computational and communication complexities. To substantiate this claim, we consider the setting of non-interactive secure computation: Alice wants to publish a short digest corresponding to a private large input x on her web page such that (possibly many) Bob, with a private input y, can send a short message to Alice allowing her to learn $C(x, y)$ (where $C$ is a public circuit). The protocol must be reusable in the sense that Bob can engage in arbitrarily many executions on the same digest. In this context we obtain the following new implications.

1) UC Secure Bob-optimized 2PC: We obtain a UC secure protocol where Bob’s computational cost and the communication cost of the protocol grows with $poly(|x|, |y|, \lambda, d)$, where d is the depth of the computed circuit $C$.

2) Malicious Laconic Function Evaluation: Next, we move on to the setting where Alice’s input x is large. For this case, UC secure protocols must have communication cost growing with $|x|$. Thus, with the goal of achieving better efficiency, we consider a weaker notion of malicious security. For this setting, we obtain a protocol for which Bob’s computational cost and the communication cost of the protocol grows with $poly(|y|, \lambda, d)$, where d is the depth of the computed circuit $C$.

Keywords—Cryptography; Secure Computation.

I. INTRODUCTION

Consider the following setting: Alice would like to publish a digest h corresponding to her private data x on her web page. Next, Bob (with a private input y) would like to send a short message to Alice, so that she learns $C(x, y)$ for some public circuit C. As is standard in secure computation, Alice and Bob want to achieve this result while keeping their respective inputs hidden from each other. Analogous to Bob’s message, Charlie or any other party could reuse h provided by Alice on her web page. This non-interactive nature of Alice’s message makes this setting highly desirable and has been extensively studied in cryptography [1]. This primitive is commonly referred to as non-interactive secure computation.

Bob-optimization. Unfortunately, traditional cryptographic techniques for realizing the above task require Bob’s computational complexity to grow with $|C|$ and $|x|$ (in addition to y), which is undesirable in several settings. In particular, since only Alice learns the output of the computation, Bob might find it unfair that he has to perform the computation of $|C|$. In other words, Bob might be happy to see Alice learn the output of the computation, but may not be willing to take on doing the computation himself. For example, consider the case where Alice’s input is her genomic sequence and Bob would like to help Alice learn how likely she is to have cancer while keeping the logic that he is using to make predictions secret.

Making the problem more challenging, computational constraints on Bob imply additional constraints on the sizes of Alice’s digest and Bob’s message, which must now also be small. Constructing such Bob-optimized protocols has been the focus of several recent results such as laconic function evaluation [2] and laconic oblivious transfer [3]. Our setting is inspired by these works. In particular, prior work on laconic function evaluation [2] also considers the problem of non-interactive secure computation, which is computationally optimized for Bob. However, these results are limited to the semi-honest setting and need non-falsifiable assumptions [4], [5], [6], [7], [8] to upgrade security to the malicious setting. This brings us to the following question:
Can we realize maliciously secure Bob-optimized non-interactive secure computation from standard assumptions?

Bob-optimization when Alice has a large input. Next, we consider the more demanding setting, where Alice’s input $x$ itself might be very large. As before, Bob might be happy to see Alice learning the output of the computation, but may find reading $x$ himself prohibitively expensive. This could be especially prohibitive if Bob interacts with multiple users, all playing the role of Alice. For example, the FBI (playing as Alice) could hold a huge database of passenger names on the no-fly list. An airline company (playing as Bob) might want to help the FBI check if any of the passengers on one of its flights is on the list. Here the airline company would prefer to perform computation independent of the FBI’s database. This is a special case of the very important and well-studied problem of private set intersection (PSI) [9]. This brings us to the following question:

Can we realize maliciously secure Bob-optimized non-interactive secure computation when Alice has a large input from standard assumptions?

Reusability of Alice’s Digest. We allow multiple Bob’s to be able to reuse Alice’s digest for multiple computations. In this setting, a corrupt Bob could provide Alice with an ill-formed message and use Alice’s output (that it may learn in some way) to cheat Alice or to learn something about Alice’s input $x$. Thus, we aim for security against a malicious Bob that has access to Alice’s outputs on its prior interactions.

Reverse Delegation. One can view our setting as a reverse delegation scheme. In a delegation scheme, a user outsources its computation to an untrusted server with the goal of learning the output (possibly while even keeping it private). In contrast, our applications allow a user (Bob) to delegate its computation to the untrusted server (Alice) while also letting it learn the output of the computation, and nothing beyond that.

A. Our Results

In this work we introduce the notion of laconic conditional disclosure of secrets (CDS). In a CDS protocol a verifier $V$ wants to reveal a message $m$ to a prover $P$ conditioned on the fact that $x$ is an accepting instance of some NP-language $L$. An honest prover (holding the corresponding witness $w$) always obtains the message $m$ at the end of the interaction. On the other hand if $x \notin L$ we require that no (possibly corrupted) $P^*$ can learn the message $m$. CDS can be seen as the two round analog of witness encryption [10]. The new constraint that we impose is that the interaction has to be laconic in the sense that it should not depend on the size of the parties inputs, and in particular on the size of the witness $w$. Additionally, the verifier computation must be much smaller than recomputing the relation. More specifically, verifier’s computation and overall communication grows with $\text{poly}(|x|, \lambda, \log(T))$, where $\lambda$ is the security parameter and $T$ is the verification time for checking that $x \in L$ (given $w$).

Next, we obtain constructions of laconic CDS in the common reference string model under standard assumptions, such as CDH or (standard) LWE. Laconic CDS serves as a powerful tool for maliciousifying semi-honest protocols while preserving their computational and communication complexities. To demonstrate this power, we show application of laconic CDS to the above-mentioned settings:

1) Bob-optimized 2PC: We obtain a UC secure protocol where Bob’s computational cost and the communication cost of the protocol grows with $\text{poly}(|x|, |y|, \lambda, d)$, where $d$ is the depth of the computed circuit $C$. This protocol achieves UC-security [11] and security is based on the LWE assumption.

2) Malicious Laconic Function Evaluation: Next, we consider the more demanding setting where Alice’s input $x$ is large. For this case, UC secure protocols must have communication cost growing with $|x|$. Thus, with the goal of achieving better efficiency, we consider a weaker notion of malicious secure which we call context security. Context security allows us to rewind parts of the execution while at the same time providing some form of composability and subsumes the standard notion of indistinguishability-based security. For this setting, we obtain a protocol for which Bob’s computational cost and the communication cost of the protocol grows with $\text{poly}(|y|, \lambda, d)$, where $d$ is the depth of the computed circuit $C$. The security of this construction is based on LWE as well. This result can be seen as the malicious variant of the recent work on laconic function evaluation [2].

The above applications demonstrate the power of laconic CDS. We see laconic CDS as a natural primitive and expect it to have other applications. As another example, laconic CDS allows a resource-constrained client to delegate the computation of a large circuit to an untrusted worker and to condition the payment of the worker on the fact that the provided output is the correct one. This does not achieve the notion of verifiable com-
putation in the traditional sense, since the client cannot explicitly check that the output is correct. However in certain scenarios, e.g., mining in cryptocurrencies, one is interested in rewarding under the condition that some computation has been performed. Then miners are free to give the wrong output and not claim the reward. However, there is no clear incentive for that.

B. Technical Overview

To understand and motivate our techniques it is instructive to discuss a few plausible approaches for constructing laconic CDS and highlight the barriers that they encounter. Below we start with such approaches.

Why Known Techniques Fail. If we were to omit the laconic constraint, then CDS admits a very simple two-round protocol based on two-round oblivious transfer (OT) and Yao’s garbled circuits [12]: The prover encodes the binary representation of its witness as the choice bits in several parallel repetitions of the OT. The verifier garbles the circuit that hardcodes the statement \( x \) and the message \( m \) and returns \( m \) if and only if \( R(\cdot, x) = 1 \). Then it sends the garbled circuit together with the second message of the OT on input each pair of input label. The prover can locally recover the labels corresponding to its witness and evaluate the circuit learning nothing beyond its output. It is clear that such a solution satisfies our security requirements but falls short in achieving laconic communication since the full circuit encoding of the NP-relation is exchanged between the two parties. At a first glance this seems to be inherent to garbled-circuit based solutions since secure two-party computation with low communication complexity usually requires more sophisticated tools, such as fully-homomorphic encryption [13].

Another plausible angle to attack the problem is to resort to techniques from the field of succinct arguments [4], [5]. Then the prover could simply augment a succinct proof with a public key and the verifier would then encrypt the message if the proof correctly verifies. Unfortunately known schemes require at least three rounds of interaction (four without assuming a setup) or rely on non-falsifiable assumptions [6], [7], [8]. Constructing succinct arguments from standard assumptions in less than three rounds seems to hit a roadblock: It has been shown [14] that non-interactive succinct arguments cannot be based on falsifiable assumptions, at least in a black-box sense.

Our Solution in a Nutshell. Our starting point is the classical garbled circuit-based solution. A closer look to the source of inefficiency reveals that there are two major challenges to overcome in order to achieve our goal: (1) We need to remove the linear dependency of the OT with respect to the size of the witness and (2) we cannot recompute the full blown NP-relation in the garbled circuit. Our first insight is to bypass the first obstacle using laconic OT [3]. A laconic OT allows one to hash a long database into a small digest, then the sender can compute the second message of an OT where the choice bit is set to be the value at an arbitrary location of the database. The important message here is that the communication complexity is independent of the size of the database (in our case the witness \( w \)). This primitive alone allows us to compress the size of the first message of the CDS. However, laconic OT alone does not buy us anything for the complexity of the second message. Overcoming the second obstacle requires us to borrow techniques from the domain of succinct arguments. The observation here is that checking the validity of an NP-instance does not necessarily require one to recompute the corresponding relation: Probabilistically checkable proofs (PCP) [15] encode a witness into a (longer) string such that the membership of the statement can be probabilistically verified by querying a constant amount of bits. Such verification algorithms are inherently erroneous, but the gap can be made negligibly small via standard amplification techniques.

This tool gives us the right leverage for a candidate laconic CDS construction: A prover can now hash the PCP encoding of its witness via a laconic OT and send the corresponding digest to the verifier. The latter then samples a few random locations and garbles a circuit that takes as input the bits of the PCP encoding at such locations and returns \( m \) if the PCP verifier accepts. Then it sends the garbled circuit in plain and the input labels via the laconic OT. This allows the prover to recover the labels corresponding to the bits of the PCP encoding, evaluate the circuit, and eventually recover the message. This introduces a negligible soundness gap, which does not make a difference in our settings as we rely anyway on computational assumptions. The stretch in the size of the witness is also not a problem since the communication complexity of a laconic OT is independent of the size of the database (in our case the PCP encoding).

While this construction seems to solve all problems at once, a closer look to the building blocks reveals the dependency on a maliciously secure laconic OT. Currently, the only known way to construct laconic OT resilient against active attackers is to compile a semi-honest one with succinct arguments. Due to its compressing nature, bypassing the usage of non-falsifiable
assumptions in laconic CDS might then appear to be out of reach of current techniques. However, we have now reduced the problem of constructing laconic CDS to that of building laconic OT: In this work we show how to construct maliciously secure laconic OT assuming the hardness of CDH or (standard) LWE with polynomial modulo-to-noise ratio. Most of the technical innovations of this work, and the remainder of this section, are devoted to instantiating malicious laconic OT from standard assumptions. Looking ahead, this will allow us to construct laconic CDS, which in turn will be used as the main technical component to build malicious LFE and UC-secure Bob-optimized 2PC. An outline of our results is given in Figure 1.

Towards Malicious Laconic OT. Before we delve into the actual instantiations of malicious laconic OT we further simplify the problem by lowering the efficiency and security requirements for a laconic OT.

Our starting point is a recent work by Döttling, Garg, Hajiabadi, Masny and Wichs [16] which constructs maliciously secure oblivious transfer from search assumptions. The main idea in [16] is to start with a very simple notion of security against malicious receivers and carefully bootstrap this notion to standard simulation based notions. The weakest notion considered in [16] is called elementary OT, and our basic notion of malicious laconic OT extends this notion to the setting of laconic OT. We refer to this primitive as weak malicious laconic OT (when it is clear from the context we drop the term malicious). Jumping ahead, we will then show, building on techniques developed in [16] how to generically upgrade a laconic OT that meets these conditions to a fully efficient and fully secure one. Concretely, we aim for the following guarantees.

1) Weak Functionality: The sender algorithm no longer takes as input two messages $(m_0, m_1)$ to transfer but instead generates two fresh random strings $(k_0, k_1)$ together with the sender output $c$. This can be seen as the analog of key-encapsulation mechanism, where $(k_0, k_1)$ are then used as the session keys to transfer the desired messages.

2) Weak Security: We require that, given the sender message $c$, no efficient polynomial-time algorithm can output both $k_0$ and $k_1$ at the same time. This does not guarantee, for instance, that an attacker cannot output the first half of $k_0$ and the second half of $k_1$. This requirement is in fact identical to the notion of elementary sender security considered in [16].

3) Weak Efficiency: We consider a laconic OT where the only efficiency constraint is that the receiver message is 2-to-1 compressing. That is, we do not impose any bound on the size of the setup string and of the sender message, which are potentially as long as the database.

Pitfalls of Known Constructions. A natural question to ask is whether existing constructions of semi-honest laconic OT already satisfies any meaningful notion of security in presence of a corrupted receiver. To exemplify the issues that arise, we briefly recall a simplified version of the hash-encryption construction of [17]: The public parameters consist of a matrix of uniformly sampled group elements

$$crs = \left( \begin{array}{c} g_1^{(0)}, \ldots, g_m^{(0)} \\ g_1^{(1)}, \ldots, g_m^{(1)} \end{array} \right) \leftarrow_s \mathbb{G}^{2 \times m}$$

and the hash of a database $D$ is computed as

$$d = \prod_{i=1}^{m} g_i^{(D[i])}.$$ To generate two keys for a position $L$, one samples two random random integers $(r, s)$, computes the ciphertext $c$ as the concatenation of the matrices

$$\left( \begin{array}{c} g_1^{(0)} \cdot r, \ldots, g_L^{(0)} \cdot r, \ldots, g_m^{(0)} \cdot r \\ g_1^{(1)} \cdot r, \ldots, 1, \ldots, g_m^{(1)} \cdot r \end{array} \right)$$

and

$$\left( \begin{array}{c} g_1^{(0)} \cdot s, \ldots, 1, \ldots, g_m^{(0)} \cdot s \\ g_1^{(1)} \cdot s, \ldots, g_L^{(1)} \cdot s, \ldots, g_m^{(1)} \cdot s \end{array} \right),$$

then sets $k_0 = d^r$ and $k_1 = d^s$. Security stems from the fact that if $D[L] \neq b$, then the receiver has to find a different linear combination of elements that yields the same $d$ in order to compute the corresponding key. This however crucially relies on the fact that the receiver always chooses at least one group element per column of the $crs$. Consider the following attack where $d$ is set to be $d = g_1^{(0)}$. Then the receiver can recover the keys for both $b = \{0, 1\}$, when encrypting with respect to some $L \neq 1$. This is because the element $(g_1^{(0)})^r$ is always given if $L \neq 1$, then $k_0$ and $k_1$ are simply the first element of each matrix. This breaks any meaningful notion of security and forces us to rethink even the most basic building block of the primitive.

Construction from CDH. Our approach diverges from prior works and takes a fresh look at the problem. In our scheme the public parameters consist of a vector of group elements sampled uniformly at random

$$crs = (g_1, \ldots, g_m) \leftarrow \mathbb{G}^m$$
and the hash of a database $D$ is defined as
\[ d = \prod_{i=1}^{m} g_i^{D[i]} . \]
That is the $i$-th element of the vector is included in the product if $D[i] = 1$ and skipped if $D[i] = 0$. The subtle difference with respect to previous approaches lies in the fact that even setting $d = g_1$ gives us a perfectly valid hash, which corresponds to the pre-image $1||0^{m-1}$.

To generate two session keys $(k_0, k_1)$ for a location $L$, the sender samples a random integer $r$ and sets the ciphertext to
\[ c = (g_1^r, \ldots, g_{L-1}^r, g_{L+1}^r, \ldots, g_m^r) , \]
i.e., all powers are given except for $g_L^r$. We now want to define $k_0$ and $k_1$ in such a way that only $k_{D[i]}$ can be recovered using a pre-image $D$ of $d$. To this end we set
\[ k_0 = d^r \quad \text{and} \quad k_1 = d^r / g_L^r . \]
Observe that if $D[L] = 0$, then $c$ contains enough information to recompute
\[ k_0 = d^r = \prod_{i=1}^{m} g_i^{D[i]\cdot r} , \]
since $g_L^r$ would be excluded from the product anyway. On the other hand if $D[L] = 1$, then one can only recompute
\[ k_1 = d^r / g_L^r = \prod_{i=1, i \neq L}^{m} g_i^{D[i]\cdot r} . \]
To get an intuition why the scheme is secure for any (possibly maliciously generated) image $d$, observe that outputting both $k_0$ and $k_1$ also reveals $k_0 / k_1 = g_L^r$, regardless of the value of $d$. However, $g_L^r$ was not given as part of the ciphertext and therefore predicting it, given only $c$ and $crs$, is as hard as solving a random instance of the CDH problem.

**Construction from LWE.** A CDH-based construction is not entirely satisfactory in terms of assumptions since most of the applications of malicious laconic OT (and consequently of laconic CDS) are only known under the hardness of lattice-related problems. If we were to plug in our machinery we would introduce an additional number-theoretic assumption (i.e., CDH), which is not ideal. An additional reason to look into lattice-based schemes is that current cryptanalytic techniques fail even in the quantum settings, whereas there are polynomial-time quantum algorithms to solve discrete logarithm-related problems. For these reasons, we turn our attention to constructing weak malicious laconic OT from the hardness of the LWE problem. The basic idea of our scheme is conceptually simple, but the noisy nature of the LWE problem introduces some complications. The public parameters consist of a single matrix
\[ crs = A = \mathbb{Z}_q^{n \times m} \]
where $m$ is the size of the database and $n$ is a parameter that governs the hardness of the LWE problem. Hashing a database $D \in \{0, 1\}^m$ (parsed as a column vector) is a simple multiplication
\[ AD = d \in \mathbb{Z}_q^n \]
that is, we take a linear combination of the columns of $A$ depending on the bits of $D$. For a given location $L$, the sender algorithm samples a column vector $s \leftarrow \mathbb{Z}_q^n$ and computes a noisy inner product with each column of $A$, except for the $L$-th one. The sender message $c$ consists of the set
\[ \{ s^T a_1 + e_1, \ldots, s^T a_m + e_m \} \setminus \{ s^T a_L + e_L \} \]
where the noise vector is sampled from a discrete Gaussian and has small norm. As before we set the keys in such a way that it is easy to compute one, but
it is hard to compute both. This is done by setting
\[ k_0 = s^T d \text{ and } k_1 = -s^T d + s^T a_L + e_L. \]

It is important to observe that \( k_0 + k_1 = s^T a_L + e_L \),
which is an LWE sample but it is not among those included in \( c \). This suggests that outputting both values of \( k_0 \) and \( k_1 \) is equivalent to predicting an LWE sample and it is going to be our central leverage to show the security of the scheme. However, the more challenging part is how to ensure that the receiver is able to recover \( k_{D[L]} \). In contrast to our previous scheme, the naive strategy fails to recover the key due to the presence of the noise. In fact
\[
\sum_{i=1, i \neq L}^m e_i \cdot D[i] = k_{D[L]} + \sum_{i=1, i \neq L}^m e_i \cdot D[i] = k_{D[L]} + \tilde{e}.
\]

To overcome this issue we exploit the fact that \( \tilde{e} \) is relatively small when compared to \( k_{D[L]} \). We then partition \( \mathbb{Z}_q \) in \( c \)-many intervals and we set the actual session key to be \( k_b \) (as computed above) rounded at the closest multiple of \( q/c \). The key property of this rounding function is that it is resilient to small perturbations, which means that
\[
[k_{D[L]} + \tilde{e}]_c = [k_{D[L]}]_c
\]
with high probability, for a small enough \( \tilde{e} \). This strategy introduces a few issues, among others the fact that the output of the rounding function is not long enough to argue about unpredictability (i.e., it can be randomly guessed with high enough probability). Fortunately, this issue can be easily circumvented with standard amplification techniques.

**Indistinguishability Laconic OT.** As discussed before, our notion of security only guarantees that the adversary cannot output both \( k_0 \) and \( k_1 \) in their entirety but it does not guarantee that there exists a consistent bit \( b \) for which the adversary can always guess \( k_b \) and never \( k_{b \oplus 1} \). For example, it could be possible that for a fixed value of \( d \), the adversary is able to predict \( k_0 \) for half of the support of \( c \) and \( k_1 \) for the complement. To fix this issue, follow the blueprint of [16] and use techniques developed in the context of hardness amplification of puzzles [18]. The key idea of this step is to amplify the success probability of the adversary via parallel repetitions: By setting the new key to be the concatenation of many independent instances, with high probability at least one of elements will belong to the wrong partition of the support of \( c \). Thus with high enough probability, the adversary is forced to simultaneously predict two values \((k_0, k_1)\).

Once this obstacle is surpassed, turning our weak laconic OT into a fully functional one involves rather standard tools: First we turn the search problem into a decision one using Goldreich-Levin hardcore predicate [19]. At this point we can give as input to the sender algorithm any message pair \((m_0, m_1)\) and implement the standard OT functionality by augmenting \( c \) with \( k_0 \oplus m_0 \) and \( k_1 \oplus m_1 \). It is easy to see that at least one of the two messages must be hidden to the eyes of the adversary as the key \( k_{D[L] \oplus 1} \) acts as a one-time pad. At this point, our security definition looks as follows: We define two experiments \((\text{Exp}_0 \text{ and Exp}_1)\) where the adversary is allowed to choose a hash \( d \), two messages \((m_0, m_1)\), and a location \( L \), then the challenger flips a coin \( b \). If \( b = 0 \) then the ciphertext \( c \) is honestly computed via the sender algorithm on input \((L, m_0, m_1)\), otherwise \( m_0 \) for \( \text{Exp}_0 \) is replaced with a uniformly sampled message. The guarantee is that the adversary cannot succeed in both experiments with non-negligible probability.

This gives us a more intuitive security notion but it is still not sufficient for constructing laconic CDS. The reason is that we have no idea whether the adversary is going to be able to succeed in \( \text{Exp}_0 \) or \( \text{Exp}_1 \), for a given value of \( L \). This information is needed by the simulator when using laconic OT in conjunction with garbled circuits: In a reduction against the security of the garbling scheme we need to know in which position we should plug the challenge label, to correctly simulate the view of the adversary. Even worse, determining whether the adversary is successful in \( \text{Exp}_0 \) or \( \text{Exp}_1 \), for all locations \( L \), corresponds to extracting the whole database \( D \)! Recall that the hash \( d \) of a laconic OT is compressing, therefore its pre-image is not even information-theoretically determined, let alone efficiently computable.

**Context-Secure Laconic OT.** The final challenge towards constructing malicious laconic OT boils down to extracting the pre-image of any given (possibly maliciously computed) hash. As discussed before, the hash does not even determine the pre-image in an information theoretic sense, so trivial solutions are not applicable. An additional complication is that the protocol is non-interactive, i.e., the receiver outputs a single message and goes offline. Therefore rewinding the receiver also does not seem to help. Of course one could just assume the existence of an extractor, which would however place our solution within the category of non-falsifiable assumptions.

We address this problem by leveraging the distinguisher-dependent simulation technique recently
developed [20]. We introduce a new security notion called context security to provide a versatile toolkit which allows to deploy distinguisher-dependent simulation in much more complex settings. While on a technical level we use many of the same techniques as [16], context security will allow us to use the distinguisher-dependent simulation technique to its full effect.

We will use distinguisher-dependent simulation in the following way to extract the input of a malicious receiver. A careful look at the indistinguishability-based definition shows that, given black-box access to a malicious receiver, we can determine the bit $D[L]$, by approximating the success probability in $\text{Exp}_0$ and $\text{Exp}_1$: For a given location $L$, the experiment where the adversary is successful must correspond to the value of $D[L]$! Iterating over all locations, we can recover the complete database.

Our main insight is that this technique can be applied to a setting where the overall communication between receiver and sender is too small to information-theoretically specify the input of the receiver. This is in contrast to previous uses of this technique in [20], [16].

Somewhat counterintuitively, we are able to extract the full pre-image of a short hash in polynomial time without resorting to non-falsifiable assumptions. Our new notion of context context security is crafted to precisely characterize the security guarantees we can achieve via distinguisher dependend simulation.

The high level idea of context security is that protocols must remain secure against any context, where a context is defined as a (possibly corrupted) receiver and a distinguisher that takes as input the sender’s message. Security is defined in terms of the existence of an extractor and a simulator: The extractor (with oracle access to the distinguisher) recovers the original input of the receiver and gives enough information to the simulator to simulate the sender message, where the simulator only interacts with the ideal functionality. Additionally, the runtime of the extractor is independent of the computation of the receiver. CDS where the secret is set to $m_1$. That is, the receiver computes the second message of a laconic CDS where the secret is set to $m_2$. A critical aspect in this step which avoids an exponential blowup is that the runtime of the context-extractor is independent of the computation of the receiver.

C. Applications

We now discuss how laconic CDS can be used as a maliciousifier for two-round protocols: A two round protocol consists of a message $m_1$ from the receiver to the sender and a message $m_2$ from the sender to the receiver. At the end of the interaction, the receiver performs some computation to retrieve the output of the protocol. Using laconic CDS we can turn a semi-honest two-round protocol into a malicious one (for a corrupted receiver) by augmenting $m_1$ with the first message of a laconic CDS certifying that $m_1$ is well formed. Then the sender computes the second message of a laconic CDS where the secret is set to $m_2$. That is, the receiver will learn $m_2$ if and only if $m_1$ was well-formed. The new properties that our transformation enables are:

1) The communication complexity of the malicious protocol is identical to that of the semi-honest one.
2) The computational complexity of the sender is unchanged.

This comes particularly useful when the input and the computation of the receiver are particularly burdensome. As an example, a laconic CDS allows us to lift non-interactive secure computation for RAM programs [3] to the malicious settings in a very natural way. Another
interesting scenario is when the above transformation is applied to laconic function evaluation (LFE). In this case we obtain the first maliciously secure Bob-optimized non-interactive secure computation protocol where the communication complexity grows only with the depth of the circuit and with the size of Bob’s input. In other words, the malicious protocol is (asymptotically) as efficient as the underlying semi-honest LFE. We can even lift the security to the UC-settings, however at the cost of the communication growing with the size of the receiver’s input, which is unavoidable.

**Delegating Computation.** A less orthodox usage of a laconic CDS is in the context of non-interactive delegation of computation: A client wants to delegate the computation of a large circuit to an untrusted worker and wants some insurance that the output given by the worker is the correct one. The worker performs the computation and obtains the output $z$, then computes a laconic CDS that certifies that $z$ is indeed the correct output. On input the first message of the laconic CDS and $z$, the client conditions the payment of the worker on the fact that $z$ is computed correctly. This protocol is not verifiable in the traditional sense since the client cannot explicitly check that $z$ is indeed the correct output. However we can envision scenarios where this is not a limitation. As an example, miners of cryptocurrencies often aggregate in pools, where each peer is rewarded basing on the amount of computation it performed. In this case it is not critical to verify that the output is correct but we are mostly interested in the fact that some large circuit has been computed. The miners could of course provide the wrong output and not claim the reward, but it is unclear what would be the incentive to do that.

**II. Definitions**

We denote by $\lambda \in \mathbb{N}$ the security parameter. We say that a function $\text{negl}$ is negligible if it vanishes faster than any polynomial. Given a set $S$, we denote by $s \leftarrow S$ the uniform sampling of an element from $S$. We say that an algorithm is PPT if it can be implemented by a probabilistic Turing machine running in time polynomial in $\lambda$. We introduce two useful inequalities.

**Theorem 1** (Hoeffding Inequality). Let $(X_1, \ldots, X_N)$ be independent and identically distributed random variables in $[0, 1]$ with expectation $E[X]$. Then it holds that

$$ \Pr \left[ \frac{1}{N} \sum_{i=1}^{N} X_i - E[X] > \delta \right] \leq 2e^{-2N\delta^2}. $$

**Lemma 1** (Markov Inequality for Advantages [16]). Let $A(Z)$ and $B(Z)$ be two random variables depending on a random variable $Z$ and potentially additional random choices. Assume that

$$ \left| \Pr_Z[A(Z) = 1] - \Pr_Z[B(Z) = 1] \right| \geq \varepsilon \geq 0. $$

Then

$$ \Pr_Z[|\Pr[A(Z) = 1] - \Pr[B(Z) = 1]| \geq \varepsilon/2] \geq \varepsilon/2. $$

**A. Intractable Problems**

In the following we introduce some hard problems in cryptography that are going to be useful for our work.

**Computational Diffie-Hellman.** We recall the search version of the classical computational Diffie-Hellman (CDH) problem [21]. Let $G$ be a (prime-order) group generator that takes as input the security parameter and $1^\lambda$ and outputs $(G, p, g)$, where $G$ is the description of a multiplicative cyclic group, $p$ is the order of the group, and $g$ is a generator of the group.

**Definition 1** (Computational Diffie-Hellman Assumption). We say that $G$ satisfies the CDH assumption (or is CDH-hard) if for any PPT adversary $A$ it holds that

$$ \Pr[A(G, p, g, g^{a_1}, g^{a_2}) = g^{a_1a_2}] = \text{negl}(\lambda) $$

where $(G, p, g) \leftarrow G(1^\lambda)$ and $(a_1, a_2) \leftarrow \mathbb{Z}_p$.

**Learning with Errors.** The learning with errors (LWE) problem was introduced by Regev [22]. In this work we exclusively use the decisional version, since there exists a well known reduction to the search variant of the problem.

**Definition 2** (Learning with Errors Assumption). The LWE$_{n, \bar{n}, q, \chi}$ problem, for $(n, \bar{n}, q) \in \mathbb{N}$ and for a distribution $\chi$ supported over $\mathbb{Z}$, is to distinguish between the distributions $(A, sA + e \mod q)$ and $(A, u)$, where $A \leftarrow \mathbb{Z}_q^\bar{n} \times \mathbb{Z}_q^n$, $s \leftarrow \mathbb{Z}_q^{\bar{n}}$, $e \leftarrow \chi^\bar{n}$, and $u \leftarrow \mathbb{Z}_q^n$. Then, the LWE$_{n, \bar{n}, q, \chi}$ assumption is that the two distributions are computationally indistinguishable.

The assumption is to consider hold for any $\bar{n} = \text{poly}(n, \log(q))$. We denote this problem by LWE$_{n, \bar{n}, q}$. As shown in [22], [23], the LWE$_{n, \bar{n}, q}$ problem with $\chi$ being the discrete Gaussian distribution with parameter $\sigma = \alpha q \geq 2\sqrt{n}$ (i.e. the distribution over $\mathbb{Z}$ where the probability of $x$ is proportional to $e^{-\pi(x/\sigma)^2}$), is at least as hard as approximating the shortest independent vector problem (SIVP) to within a factor of $\gamma = O(n/\alpha)$ worst case dimension $n$ lattices. This is proven using a quantum reduction. Classical reductions (to a slightly different problem) exist as well [24], [25] but with somewhat worse parameters. The best known (classical or quantum) algorithms
for these problems run in time $2^{\tilde{O}(n/\log(\gamma))}$, and in particular they are conjectured to be intractable for $\gamma = \text{poly}(n)$.

A discrete gaussian with parameter $\alpha q$ is $B = \alpha q$ bounded, except with negligible probability. For parameter $\alpha$ the worst-to-average case reduction of [22] gives a worst-case approximation factor of $\tilde{O}(n/\alpha)$ for SIVP. Consequently, in terms of the bound $B$ and the modulus $q$ we get a worst-case approximation factor of $\tilde{O}(nq/B)$ for SIVP.

**B. Laconic Oblivious Transfer**

In the following we introduce laconic oblivious transfer (LOT), the main object of interest of our work [3]. For presentation purposes, we define two variants of LOT with different efficiency and security requirements. Looking ahead, we will show a generic transformation, thereby simplifying the task of designing a LOT scheme to its simplest flavour.

As discussed by Cho et al. [3], we can ignore any security requirement on the receiver side: Although some bits of the database could be leaked, any LOT scheme can be generically upgraded to achieve receiver security through a generic transformation, i.e., by running the LOT under a 2PC protocol. In contrast to our work, Cho et al. [3] also considers the property of updatability for a LOT, which allows one to modify a bit of the database and update the digest in a significantly more efficient way than computing it from scratch. Since it is not relevant for our applications, we omit this property.

**Weak Laconic Oblivious Transfer.** A weak LOT scheme is identical to the standard LOT [3] except that the sender algorithm does not take as input two messages but chooses itself two random keys $(k_0, k_1)$. This can be seen as the analogous to key encapsulation for encryption schemes. The syntax is given below.

**Definition 3** (Weak Laconic Oblivious Transfer). A weak LOT LOT $= (\text{Setup}, \text{Hash}, \text{KGen}, \text{Receive})$ is defined as the following tuple of algorithms.

\begin{align*}
\text{Setup}(1^\lambda) &\to crs : \text{On input the security parameter } 1^\lambda, \text{the generation algorithm returns a common reference string crs.} \\
\text{Hash}(crs, D) &\to (d, \tilde{D}) : \text{On input the common reference string } crs \text{ and a database } D \in \{0, 1\}^*, \text{the hashing algorithm returns a digest } d \text{ and a state } \tilde{D}. \\
\text{KGen}(crs, d, L) &\to (c, k_0, k_1) : \text{On input the common reference string } crs, \text{ a digest } d, \text{ and a location } L \in \mathbb{N}, \text{the key generation algorithm returns a ciphertext } c \text{ and a pair of keys } (k_0, k_1).
\end{align*}

Receive$^D_{\text{crs}, c, L} \to m : \text{On input the common reference string crs, a ciphertext c, and a location } L \in \mathbb{N}, \text{the receiver algorithm (with random access to } \tilde{D}) \text{ returns a key } k.$

The definition of correctness is given in the following.

**Definition 4** (Correctness). A weak LOT LOT $= (\text{Setup}, \text{Hash}, \text{KGen}, \text{Receive})$ is correct if for all $\lambda \in \mathbb{N}$, for all databases $D$ of size polynomial in $\lambda$, and for all memory locations $L \in \{1, \ldots, |D|\}$ it holds that

$$\Pr[k_{D[L]} = \text{Receive}^D_{\text{crs}, c, L}] = 1$$

where

- $\text{crs} \leftarrow \text{Setup}(1^\lambda)$,
- $(d, \tilde{D}) \leftarrow \text{Hash}(\text{crs}, D)$,
- $(c, k_0, k_1) \leftarrow \text{KGen}(\text{crs}, d, L)$,

and the probability is taken over the random coins of Setup and KGen.

We also consider a weaker notion of correctness where the above probability is bounded from below by $1 - 1/\text{poly}(\lambda)$, for some polynomial function poly. We refer to such notion as $(1/\text{poly}(\lambda))$-correctness. A weak LOT is required to satisfy only a rudimental notion of sender security that we define in the following. Loosely speaking, we require that the adversary is not able to predict both keys $(k_0, k_1)$ in their entirety.

**Definition 5** (Weak Sender Security). A weak LOT LOT $= (\text{Setup}, \text{Hash}, \text{KGen}, \text{Receive})$ is weakly sender secure if for all $\lambda \in \mathbb{N}$ and for all PPT adversaries $A = (A_1, A_2)$ there exists a negligible function negl such that

$$\Pr[\text{ExpSendSec}_{\text{LOT}, A}(1^\lambda) = 1] = \text{negl}(\lambda)$$

where the experiment is defined as

**ExpSendSec$_{\text{LOT}, A}(1^\lambda)$** :

- $\text{Compute } \text{crs} \leftarrow \text{Setup}(1^\lambda)$
- $(d, L, \text{st}) \leftarrow A_1(\text{crs})$
- $(c, k_0, k_1) \leftarrow \text{KGen}(\text{crs}, d, L)$
- $(k_0^*, k_1^*) \leftarrow A_2(c, \text{st})$
- $\text{Output } (k_0, k_1) = (k_0^*, k_1^*)$

and the probability is taken over the random coins of Setup, $A_1$, and KGen.

**Efficiency.** For efficiency, it is only required that the size of the digest $d$ is at most half of that of $D$, i.e., the Hash function is 2-to-1 compressing. In particular, there is no bound on the efficiency of the algorithms and on the size of the ciphertext, except for being polynomial in the security parameter. We refer to such notion as
semi-efficiency. Jumping ahead, we will show a generic transformation from any semi-efficient LOT to a full-fledged LOT without additional assumptions.

**Indistinguishable Laconic Oblivious Transfer.** This version of LOT is equivalent to that introduced in [3], except that we upgrade the definition of sender security to the malicious settings. Note that we consider without loss of generality schemes that transfer a single bit (bit-LOT), which can be turned into multi-bit schemes (string-LOT) by simply computing multiple ciphertexts over the same digest. The security is preserved by a standard hybrid argument.

**Definition 6** (Laconic Oblivious Transfer). A LOT LOT = (Setup, Hash, Send, Receive) is defined as the following tuple of algorithms.

\[
\text{Setup}(\lambda) \rightarrow \text{crs} : \text{On input the security parameter } \lambda, \text{the generation algorithm returns a common reference string crs.}
\]

\[
\text{Hash}(\text{crs}, D) \rightarrow (d, \tilde{D}) : \text{On input the common reference string crs and a database } D \in \{0,1\}^*, \text{the hashing algorithm returns a digest } d \text{ and a state } \tilde{D}.
\]

\[
\text{Send}(\text{crs}, d, L, m_0, m_1) \rightarrow c : \text{On input the common reference string crs, a digest } d, \text{ a location } L \in \mathbb{N}, \text{ and a pair of messages } (m_0, m_1) \in \{0,1\}^2, \text{ the sender algorithm returns a ciphertext c.}
\]

\[
\text{Receive}^{\tilde{D}}(\text{crs}, c, L) \rightarrow m : \text{On input the common reference string crs, a ciphertext c, and a database location } L \in \mathbb{N}, \text{ the receiver algorithm (with random access to } \tilde{D}) \text{ returns a message m.}
\]

The definition of correctness is given in the following.

**Definition 7** (Correctness). A LOT LOT = (Setup, Hash, Send, Receive) is correct if for all \( \lambda \in \mathbb{N} \), for all databases \( D \) of size polynomial in \( \lambda \), and for all memory locations \( L \in \{1,\ldots,|D|\} \), and any pair of messages \( (m_0, m_1) \in \{0,1\}^2 \) it holds that

\[
\Pr \left[ m_{D[L]} = \text{Receive}^{\tilde{D}}(\text{crs}, c, L) \right] = 1
\]

where

- \( \text{crs} \leftarrow \text{Setup}(\lambda) \),
- \( (d, \tilde{D}) \leftarrow \text{Hash}(\text{crs}, D) \),
- \( c \leftarrow \text{Send}(\text{crs}, d, L, m_0, m_1) \),

and the probability is taken over the random coins of Setup and Send.

The fact that the digest of a LOT is compressing, makes even defining sender security a non-trivial task. We put forward the following indistinguishability-based definition, which suffices for our purposes.

**Definition 8** (Sender Indistinguishability). A LOT LOT = (Setup, Hash, Send, Receive) is sender secure if for all \( \lambda \in \mathbb{N} \), for all PPT adversaries \( A = (A_1, A_2) \), and for all polynomial functions \( \text{poly}(\lambda) \) there exists a negligible function \( \text{negl} \) such that

\[
\Pr \left[ \varepsilon_0 > \frac{1}{\text{poly}(\lambda)} \text{ and } \varepsilon_1 > \frac{1}{\text{poly}(\lambda)} \right] = \text{negl}(\lambda)
\]

where, for \( \beta \in \{0,1\} \), \( \varepsilon_\beta \) is defined as

\[
\varepsilon_\beta = \frac{\Pr \left[ \text{ExpSendInd}^{(0,\beta)}_{\text{LOT}, A}(1^\lambda) = 1 \right]}{\Pr \left[ \text{ExpSendInd}^{(1,\beta)}_{\text{LOT}, A}(1^\lambda) = 1 \right]}
\]

where the experiment is defined as \( \text{ExpSendInd}^{(b,\beta)}_{\text{LOT}, A}(1^\lambda) : \)

- Compute \( \text{crs} \leftarrow \text{Setup}(1^\lambda) \)
- \((d, L, m_0, m_1, \text{st}) \leftarrow A_1(\text{crs})\)
- If \( b = 0 \) : Set \((r_0, r_1) = (m_0, m_1)\)
- If \( b = 1 \) : Set \( r_B \leftarrow (0,1) \) and \( r_{1-B} = m_{1-B} \)
- \( c \leftarrow \text{Send}(\text{crs}, d, L, r_0, r_1)\)
- \( b^* \leftarrow A_2(c, \text{st})\)
- Output \( b^* \)

and the probabilities are taken over the random coins of Setup, Send, and \( A_1 \).

**Efficiency.** Here it is required that the size of the digest \( d \) is a fixed polynomial in the security parameter. Furthermore, we also impose a bound on the running time of the Hash algorithm of \( |D| \cdot \text{poly}(\log(|D|), \lambda) \) and on the time complexity of Setup, Encode, and Receive of \( \text{poly}(\log(|D|), \lambda) \). These are the same efficiency requirements of Cho et al. [3].

**C. Laconic Conditional Disclosure of Secrets**

Conditional disclosure of secrets (CDS) [26] for a language \( L \) in NP with relation \( R \) is the two-round analog of witness encryption [10]: Given a statement \( x \) and a message \( m \) from the sender, the receiver is able to recover \( m \) if \( x \in L \), whereas \( m \) stays hidden if this is not the case. Furthermore, the witness \( w \) for \( x \) should be kept secret from the eyes of the sender.

**Definition 9** (Conditional Disclosure of Secrets). A CDS scheme CDS = (CDSsetup, CDSreceive, CDSsend, CDSdecode) for an NP-language \( L \) is defined as the following tuple of algorithms.

\[
\text{CDSsetup}(1^\lambda) \rightarrow \text{crs} : \text{On input the security parameter } 1^\lambda, \text{ the generation algorithm returns a common reference string crs.}
\]

\[
\text{CDSreceive}(\text{crs}, x, w) \rightarrow (\text{cds}_1, r) : \text{On input the common reference string crs and a statement-witness pair}
\]
(x, w), the receiver algorithm returns a first message cds₁ and a state r.

CDSSend(crs, x, m, cds₁) → cds₂ : On input the common reference string crs, a statement x, a message m ∈ {0, 1}⁺, a first message cds₁, the sender algorithm returns a second message cds₂.

CDDecode(crs, cds₂, r) → m : On input the common reference string crs, a second message cds₂, and the receiver state r, the decoding algorithm returns a message m.

Correctness requires that the decoding is successful if x ∈ L.

**Definition 10** (Correctness). A CDS scheme \(\text{CDS} = (\text{CDSSetup}, \text{CDSSend}, \text{CDSReceive}, \text{CDSSend})\) is correct if for all λ ∈ \(\mathbb{N}\), all \((x, w) \in \mathcal{R}\), and any message \(m ∈ \{0, 1\}⁺\) it holds that

\[
\Pr \left[ m = \text{CDSSend}(\text{crs}, \text{cds}, r) \right] = 1
\]

where

- \(\text{crs} \leftarrow \text{CDSSetup}(\lambda)\),
- \((\text{cds}, r) \leftarrow \text{CDSReceive}(\text{crs}, x, w)\),
- \(\text{cds} \leftarrow \text{CDSSend}(\text{crs}, x, m, \text{cds})\),

and the probability is taken over the random coins of CDSSetup, CDSReceive, and CDSSend.

The central requirement for a CDS scheme is that the message is hidden if the given statement is not in the corresponding NP-language.

**Definition 11** (Message Indistinguishability). A CDS scheme \(\text{CDS} = (\text{CDSSetup}, \text{CDSSend}, \text{CDSReceive}, \text{CDSSend})\) is message-indistinguishable if for all λ ∈ \(\mathbb{N}\), for all admissible PPT adversaries \(\mathcal{A} = (A_1, A_2)\), for all \(x \notin \mathcal{L}\) there exists a negligible function \(\text{negl}\) such that

\[
\Pr \left[ \text{ExpMesInd}^{(b)}_{\text{CDS}, \mathcal{A}}(1^\lambda) = 1 \right] = \text{negl}(\lambda)
\]

where the experiment is defined as

\[
\text{ExpMesInd}^{(b)}_{\text{CDS}, \mathcal{A}}(1^\lambda) : \begin{align*}
& \text{Compute crs} \leftarrow \text{CDSSetup}(1^\lambda) \\
& (\text{cds}_1, m_0, m_1, \text{st}) \leftarrow A_1(\text{crs}) \\
& \text{cds}_2 \leftarrow \text{CDSSend}(\text{crs}, x, m_b, \text{cds}_1) \\
& b^* \leftarrow A_2(\text{cds}_2, \text{st}) \\
& \text{Output } b^*
\end{align*}
\]

where \(A\) is admissible if \(m_0\) and \(m_1\) have equal length and the probabilities are taken over the random coins of CDSSetup, CDSSend, and \(\mathcal{A}\).

Finally, we require that no information is leaked to the sender by the message of the receiver.

**Definition 12** (Receiver Simulation). A CDS scheme \((\text{CDSSetup}, \text{CDSSend}, \text{CDSReceive}, \text{CDSSend})\) is receiver simulatable if there exists a PPT simulator \(\text{CDSSim} = (\text{CDSSim}_1, \text{CDSSim}_2)\) such that for all \(\lambda \in \mathbb{N}\), all \((x, w) \in \mathcal{R}\), and all PPT adversaries \(\mathcal{A}\) it holds that

\[
\Pr \left[ \text{ExpRecSim}^{(b)}_{\text{CDS}, \mathcal{A}}(1^\lambda) = 1 \right] = \text{negl}(\lambda)
\]

where the experiment is defined as

\[
\text{ExpRecSim}^{(b)}_{\text{CDS}, \mathcal{A}}(1^\lambda) : \begin{align*}
& \text{If } b = 0 : \text{Compute crs} \leftarrow \text{CDSSetup}(1^\lambda) \\
& \text{CDSSim}_1(\text{crs}, x, w) \\
& \text{If } b = 1 : \text{Compute crs, td} \leftarrow \text{CDSSim}_1(1^\lambda) \\
& \text{CDSSim}_2(\text{crs}, x, w) \\
& b^* \leftarrow A(\text{crs}, \text{cds}_1) \\
& \text{Output } b^*
\end{align*}
\]

Efficiency. The standard requirement for a CDS scheme is to run in time polynomial in the security parameter and, possibly, in the size of the statement and of the witness. We say that a CDS is laconic if the communication complexity is a fixed polynomial \(\text{poly}(\lambda)\) and in particular is independent of the size of \(w\) (up to a poly-logarithmic factor). This notion can be seen as the equivalent of succinct arguments [5], [4] with implicit verification.

### III. CONTEXT SECURITY

In this Section we provide our definition of context security, which is a UC-inspired security notion [11]. The notion is specifically geared towards non-interactive secure computation protocols for which the communication complexity is sublinear in the receiver’s input.

UC security ensures that a protocol is secure in any environment or context. However, the way UC-security is formalized makes it necessary that a straight-line simulator is able to extract the inputs of malicious parties, which immediately implies that the communication complexity scales with the size of the inputs of the parties. An important aspect in (standard) UC-security is that the environment is chosen after the simulator. Specialized-Simulator UC [27] allows the simulator to depend on the environment, but not on its random coins. Context security aims for a compromise, while
salvaging the original motivation of UC, namely that protocols remain secure in any context.

Unlike other works which relax UC security, e.g. [28], [29], the purpose of context security is not to get rid of a trusted setup. Rather, our goal is to obtain meaningful composability guarantees in the malicious setting while allowing for round-optimal protocols with communication complexity that is sublinear in the inputs. This is neither possible with UC/straight-line extraction, nor in the standalone simulation framework: While rewinding does allow to extract large inputs from protocols with small communication, it does not help in the two message setting.

Our definition will only consider the single instance setting, but is crafted in a way that multi instance security can be dealt with via standard hybrid arguments. In this sense, we aim for conceptual simplicity rather than generality. We start by providing the definition of a context.

**Definition 13 (Protocol Context).** We say that a PPT machine $Z = (Z_1, Z_2)$ is a context for two message protocol $\Pi = (\text{Setup}, R_1, S, R_2)$, if it has the following syntactic properties: The first stage $Z_1$ takes as input a common reference string $\text{crs}$ (generated by $\text{Setup}$) and random coins $r_1$ and outputs a receiver message $\text{rec}$ and a state $\text{st}$. The second phase $Z_2$ takes as input the state $\text{st}$ and random coins $r_2$. The second phase is allowed to make queries $y$ to a sender oracle $O(y)$, which are answered by $S(\text{crs}, \text{rec}, y)$ (using fresh randomness from $r_2$). In the end the context outputs a bit $b^\ast$. Define the following experiment.

$\mathcal{Z}(1^\lambda)$:

- Choose random tapes $(r_1, r_2)$
- Compute $\text{crs} \leftarrow \text{Setup}(1^\lambda)$
- $(\text{st}, \text{rec}) \leftarrow Z_1(\text{crs}, r_1)$
- $b^\ast \leftarrow Z_2(\text{crs}, \text{rec}, \text{st}, r_2)$.
- Output $b^\ast$

We now provide our definition of context security.

**Definition 14 (Context Security).** Let $\Pi = (\text{Setup}, R_1, S, R_2)$ be a two-message protocol realizing a two-party functionality $F$. We say that $\Pi$ is context-secure if the following holds for every $\Pi$-context $Z = (Z_1, Z_2)$. We require that there exists a context extractor $\text{Ext}_Z$ and simulators $\text{SimSetup}$ and $\text{Sim}$ such that the following holds for every $\delta > 0$:

1) $\text{SimSetup}$ runs in time polynomial in $\lambda$ (but independent of the run-time of $Z_1$ and $Z_2$) and outputs a common reference string $\text{crs}$ and a trapdoor $\text{td}$.
2) $\text{Ext}_Z$ takes as input $\text{crs}, \text{st}, \text{rec}$, random coins $\text{r}^\ast$ and a parameter $\delta$ and outputs a value $x^\ast$ and an auxiliary string aux. $\text{Ext}_Z$ has overhead $\text{poly}(\lambda, p(\lambda)) \cdot T_2$, where $T_2$ is the overhead of $\mathcal{Z}_2$ and the polynomial is independent of $\mathcal{Z}$, only depending on $\lambda$.
3) $\text{Sim}$ takes as input $\text{td}, \text{rec}, \text{aux}$ and a value $z$ and outputs a sender-message $\text{snd}$. We require The overhead of $\text{Sim}$ to be polynomial in the overhead of $\lambda$, but independent of $Z_1$ and $Z_2$.
4) Define the following experiment.

$\mathcal{E}(1^\lambda, \delta)$:

- Choose random tapes $(r_1, r_2)$
- Compute $(\text{crs}, \text{td}) \leftarrow \text{SimSetup}(1^\lambda)$.
- $(\text{st}, d) \leftarrow Z_1(\text{crs}, r_1)$
- $(x^\ast, \text{aux}) \leftarrow \text{Ext}_Z(\text{crs}, \text{st}, \text{rec}, \text{r}^\ast, \delta)$
- $b^\ast \leftarrow Z_2(\text{crs}, \text{st}, r_2)$, where $O(y) \ computes$ and outputs $\text{Sim}(\text{td}, \text{rec}, \text{aux}, F(x^\ast, y))$.
- Output $b^\ast$

(Security) It holds for every inverse polynomial $\varepsilon = \varepsilon(\lambda)$ that

$$\left| \Pr[\mathcal{Z}(1^\lambda) = 1] - \Pr[\mathcal{E}(1^\lambda, \varepsilon) = 1] \right| < \varepsilon,$$

except for finitely many $\lambda$.

Note specifically that we allow the ideal experiment $\mathcal{E}$ to depend on the distinguishing advantage $\varepsilon$, which looks unusual at first glance. However, it is precisely this dependence which allows us to prove context security for protocols with sublinear communication complexity. Specifically, this dependence will let us use the distinguisher-dependent simulation technique [20] to construct extractors $\text{Ext}_Z$.

The extractor $\text{Ext}_Z$ has a similar syntax as a knowledge extractor [30], however the main difference is we will be able to prove this notion under standard falsifiable assumptions. An important aspect which enables context security to be used in a meaningful way is that $\text{Ext}_Z$ does not get to see $r_2$.

The runtime requirement for $\text{Ext}_Z$ will make this notion compose benignly, unlike knowledge extractors [30]. More specifically, it will be natural and convenient to define experiments iteratively, and this runtime requirement will ensure that runtimes of the experiments do not explode. An important aspect will be that extractors are not run recursively. Extractors will only be used in the first phase of a modified context, but the extractor itself does not use the first phase. That is, in successive uses of the technique the runtime will only grow additively, but not multiplicatively.

We remark that context-security has to be used with care. If a context $(Z_1, Z_2)$ is such that $Z_2$ uses a long-term secret generated by $Z_1$, the extractor also needs to
use this secret when simulating \( \mathbb{Z}_2 \). In particular, this means that in a hybrid proof we cannot make any further modifications to \( \mathbb{Z}_1 \) after extracting the receiver input, as this could invalidate the extracted input. For example, consider a functionality where the sender provides a (long term) signing key for a signature and the receiver obtains a signature on his input. Moreover, assume that the receiver is also given the verification key of the signature (and can therefore check the validity of signatures). Context-security allows us to extract the inputs of the receiver, but in order to do so the extractor needs to know the signing key. This is problematic if we later want to argue about the unforgeability of the signature, where a reduction is not given the signing key but only access to a signing oracle. Yet, by the observation above the context-extractor cannot extract the signing queries without being given the signing key. Note that this issue does not exist in the setting of UC security.

Finally, a very convenient property of context security is that it immediately implies game-based security notions with an efficient experiment. Specifically, phrase a game as a context \( \mathcal{Z} \), apply context security and reason that the advantage in \( \mathcal{E}\mathcal{Z} \) is 0. Via the way we have defined context security this will immediately imply that also in the original experiment \( \mathcal{Z} \) the advantage is negligible.

For instance, for non-interactive secure computation one can consider the following indistinguishability-based security definition. The malicious receiver first obtains a CRS, outputs a receiver message and two randomized functions \( F_0 \) and \( F_1 \) for which it holds that on any input \( x \) the distributions \( F_0(x) \) and \( F_1(x) \) are indistinguishable. The experiment flips a bit \( b \) and provides the adversary with a sender message which allows the receiver to evaluate \( F_b \) on his input. The adversary then has to guess the bit \( b \).

Any context-secure NISC scheme immediately also satisﬁes this notion. We can phrase the experiment, including the adversary as a context \( (\mathcal{Z}_1,\mathcal{Z}_2) \) where \( \mathcal{Z}_1 \) outputs the receiver message (together with a state), and \( \mathcal{Z}_2 \) chooses the random bit \( b \) and computes the sender message via access to a sender oracle. Now, context-security lets us argue that in the experiment \( \mathcal{E}\mathcal{Z} \) the actual bit \( b \) used by the experiment is hidden from the view of the adversary, as the output of the oracle only depends on \( F_b(x) \) (which is indistinguishable from \( F_{1-b}(x) \)) rather than on \( F_b \).

**Some Useful Functionalities.** We deﬁne the functionalities corresponding to the primitives of interest of this work, deﬁned in Section II. Note that all of the functionalities that we consider are single-output, in the sense that only one party learns an output at the end of the execution.

**Laconic Oblivious Transfer:** The ideal functionality \( \mathcal{F}_{\text{LOT}}(D, m_0, m_1, L) \) takes as input a database \( D \), a pair of messages \((m_0, m_1)\) and a location \( L \). It returns \((m_{D[L]}, L)\).

**Laconic Conditional Disclosure of Secrets:** The ideal functionality \( \mathcal{F}_{\text{CDS}}(w, x, m) \) is parametrized by an NP-language \( \mathcal{L} \) with relation \( \mathcal{R} \) and takes as input a statement \( x \), a witness \( w \), and a message \( m \). The functionality returns \( m \) if \( \mathcal{R}(w, x) = 1 \) and \( \perp \) otherwise.

**IV. MALICIOUS LACONIC OBLIVIOUS TRANSFER**

In this section we present our constructions from different cryptographic hard problems. We ﬁrst construct a 2-to-1 compressing weak LOT from the CDH or the LWE assumption, then we show how to generically bootstrap any 2-to-1 compressing weak LOT to a context-secure LOT with arbitrary compression.

**A. From Computational Diffie-Hellman**

We present our scheme for a weak LOT with malicious security assuming the hardness of the CDH problem over a prime-order multiplicative cyclic group \((\mathbb{G}, p, g)\). For conceptual simplicity, we assume that a group element can be represented using \( \lambda \)-many bits, but the scheme can be generalized to arbitrary representations in a natural way. The construction is given in Figure 2.

**Analysis.** We show that our scheme is correct.

**Theorem 2 (Correctness).** Let \((\mathbb{G}, p, g)\) be a prime-order multiplicative cyclic group. Then the construction LOT = (Setup, Hash, Send, Receive) as defined in Figure 2 is correct.

**Proof of Theorem 2:** The proof consists in the observation that

\[
\begin{align*}
    k_{D[L]} = & \left( \frac{d}{g_L} \right)^r = \left( \prod_{i=1}^{2\lambda} g_i \right)^r = \left( \prod_{i=1, i \neq L}^{2\lambda} g_i \right) = 2\lambda \prod_{i=1, i \neq L}^{2\lambda} k_i^{D[i]}
\end{align*}
\]

which is exactly the output of the receiver.

Next we argue about weak sender security.

**Theorem 3 (Weak Sender Security).** Let \((\mathbb{G}, p, g)\) be a CDH-hard group. Then the construction LOT = (Setup, Hash, KGen, Receive) as defined in Figure 2 is weakly sender secure.
### Setup(1\(^λ\)):
- Sample \((G,p,g) \leftarrow G(1^λ)\).
- Sample a uniform vector \((g_1, \ldots, g_{2λ}) \leftarrow \mathbb{G}^{2λ}\).
- Return \(crs = (G,p,g,g_1, \ldots, g_{2λ})\).

### Hash\((crs,D)\):
- Parse \(crs\) as \((G,p,g,g_1, \ldots, g_{2λ})\) and \(D \in \{0,1\}^{2λ}\) as a bitstring.
- Compute \(d = \prod_{i=1}^{2λ} g_i[D[i]]\).
- Set \(\tilde{D} = (D,d)\) and return \((d,\tilde{D})\).

### KGen\((crs,d,L)\):
- Parse \(crs\) as \((G,p,g,g_1, \ldots, g_{2λ})\) and \(d \in \mathbb{G}\).
- Sample a uniform \(r \leftarrow \mathbb{Z}_p\).
- Compute the vector \(c = (g_1^r, \ldots, g_{2λ}^r)\).
- Set \(k_0 = d^r\) and \(k_1 = (d/g_L)^r\).
- Return \((c,k_0,k_1)\).

### Receive\(\tilde{D}(crs,c,L)\):
- Parse \(\tilde{D} = (D,d)\) and return \((h_1, \ldots, h_{2λ})\).
- Return \(\prod_{i=1,i\neq L}^{2λ} k_{D[i]}^i\).

---

**Figure 2:** CDH-Based Weak LOT.

### Proof of Theorem 3:
The theorem is shown with a reduction to the CDH assumption. Assume towards contradiction that there exists a PPT adversary \(\mathcal{A} = (\mathcal{A}_1,\mathcal{A}_2)\) such that

\[
\Pr[\text{ExpSendSec}(\text{LOT},\mathcal{A})(1^λ) = 1] = \frac{1}{\text{poly}(\lambda)}
\]

for some polynomial function \(\text{poly}\). On input a CDH challenge \((G,p,g,g^{a_1},g^{a_2})\), the reduction samples a uniform vector \((x_1, \ldots, x_{2λ}) \leftarrow \mathbb{Z}_p^{2λ}\) and an index \(\tilde{L} \leftarrow \{1, \ldots, 2λ\}\). Then it sets

\[
\text{crs} = (G,p,g,g^{x_1}, \ldots, g^{x_{2λ}}, g^{a_1}, g^{x_{2λ+1}}, \ldots, g^{x_{2λ}})
\]

and runs \((d,L,\text{st}) \leftarrow \mathcal{A}_1(\text{crs})\). If \(L \neq \tilde{L}\) the reduction aborts, else it sets

\[
c = (g^{ax_1}, \ldots, g^{ax_{2λ}}, g^{a_1x_{2λ+1}}, \ldots, g^{a_2x_{2λ}}).
\]

Then it runs \((k_0,k_1) \leftarrow \mathcal{A}_2(c,\text{st})\) and returns \(k_0/k_1\). The reduction runs in polynomial time and the inputs given to the adversary are identically distributed as those in the original game. Note that if \(L = \tilde{L}\) and the adversary correctly guesses both \(k_0\) and \(k_1\), then we have that

\[
k_0/k_1 = \frac{d^{a_2}}{d^{a_2} \cdot g_L^{a_2}} = g_L^{a_2} = g^{a_1a_2}.
\]

Since this happens with probability at least \(\frac{1}{\text{poly}(\lambda) \cdot 2λ}\), it contradicts the CDH assumption.

### B. From Learning with Errors

In the following we present our weak LOT scheme assuming the hardness of the LWE problem. Our scheme is shown in Figure 3.

**Rounding.** Let \(q = c \cdot p\) be an integer modulus. Define the rounding function \([\cdot]_c : \mathbb{Z}_q \rightarrow \mathbb{Z}_c\) as

\[
[x]_c = [\bar{x} \cdot c/q] \mod c
\]

where \(\bar{x} \in \mathbb{Z}\) is an arbitrary residue-class representative of \(x \in \mathbb{Z}_q\). We are going to use the following lemma about the rounding function, implicitly proven in [31].

**Lemma 2.** Let \(q = c \cdot p\) be an integer modulus. Let \(x \leftarrow \mathbb{Z}_q\) be distributed uniformly at random. Then it holds for all \(v \in \{-B, \ldots, B\}\) that \([x + v]_c = [x]_c\), except with probability \((2B + 1) \cdot c/q\) over the random choice of \(x\).

**Proof of Lemma 2:** Note that there are exactly \(c\) multiples of \(p = q/c\) in \(\mathbb{Z}_q\). Thus, the probability that a uniform \(x \in \mathbb{Z}_q\) lands \(B\)-close from the nearest multiple of \(q/c\) is exactly \((2B + 1) \cdot c/q\).

Another property of the rounding function is that it partitions the domain \(\mathbb{Z}_q\) in \(c\)-many well defined intervals of size exactly \(q/c = p\). More concretely, the \(i\)-th interval is \([p \cdot (i - 1), p \cdot i - 1]\). This fact is going to be useful for our analysis.

**Analysis.** Our scheme is parametrized by the following variables:
Setup$(\lambda) :$
- For all $i \in \{1, \ldots, \lambda\}$: Sample $A^{(i)} \leftarrow \mathbb{Z}_q^{n \times m}$.
- Return $crs = (A^{(1)}, \ldots, A^{(\lambda)})$.

Hash$(crs, D) :$
- Parse $crs$ as $(A^{(1)}, \ldots, A^{(\lambda)})$ and $D \in \{0, 1\}^m$ as a column vector.
- For all $i \in \{1, \ldots, \lambda\}$: Compute $d^{(i)} = A^{(i)} D$.
- Set $d = (d^{(1)}, \ldots, d^{(\lambda)})$, $\bar{D} = (D, d)$, and return $(d, \bar{D})$.

KGen$(crs, d, L) :$
- Parse $crs$ as $(A^{(1)}, \ldots, A^{(\lambda)})$ and $d$ as $(d^{(1)}, \ldots, d^{(\lambda)})$.
- Sample $s \leftarrow \mathbb{Z}_q^m$ and parse it as a column vector.
- For all $i \in \{1, \ldots, \lambda\}$:
  - Parse $(\mathbf{a}_1^{(i)}, \ldots, \mathbf{a}_m^{(i)})$ as the columns of $A^{(i)}$.
  - Sample $(e_1^{(i)}, \ldots, e_m^{(i)}) \leftarrow \chi^m$.
  - For all $j \in \{1, \ldots, m\} \setminus \{L\}$: Compute $b_j^{(i)} = s^T \mathbf{a}_j^{(i)} + e_j^{(i)}$.
  - Set $b^{(i)}$ to be the row vector $(b_1^{(i)}, \ldots, b_{m-1}^{(i)})$.
- Sample $(t_0^{(i)}, t_1^{(i)}) \leftarrow \mathbb{Z}_q^2$.
- Set $k_0^{(i)} = \left[ s^T d^{(i)} + t_0^{(i)} \right]_c$ and $k_1^{(i)} = \left[ -s^T d^{(i)} + s^T a_L^{(i)} + e^{(i)} + t_1^{(i)} \right]_c$.
- Set $c = ((b^{(1)}, t_0^{(1)}, t_1^{(1)}), \ldots, (b^{(\lambda)}, t_0^{(\lambda)}, t_1^{(\lambda)}))$.
- Set $k_0 = k_0^{(1)} \| \ldots \| k_0^{(\lambda)}$ and $k_1 = k_1^{(1)} \| \ldots \| k_1^{(\lambda)}$.
- Return $(c, k_0, k_1)$.

Receive$^D(crs, c, L) :$
- Parse $c$ as $((b^{(1)}, t_0^{(1)}, t_1^{(1)}), \ldots, (b^{(\lambda)}, t_0^{(\lambda)}, t_1^{(\lambda)}))$ and $\bar{D} = D \setminus D[L]$ as a column vector.
- For all $i \in \{1, \ldots, \lambda\}$: Compute $k^{(i)} = \left[ -(1)^D[L] \cdot b^{(i)} \bar{D} + t^{(i)} \right]_c$.
- Return $k = k^{(1)} \| \ldots \| k^{(\lambda)}$.

Figure 3: LWE-Based Weak LOT.

- $m$: The size of the database $D \in \{0, 1\}^m$.
- $n$: The dimension of the LWE problem.
- $q$: The modulus of the LWE problem. For ease of the analysis we are going to assume that $q$ is of the form $c \cdot p$, for some constant $c$ and an arbitrary integer $p$.
- $B$: The bound on the absolute value of the noise, i.e., $e \in \{-B, \ldots, B\}$.
- $c$: A constant that parametrizes the function $[\cdot]_c$, which is used in our construction.

In the analysis we set constraints on the parameters on demand. In the end of the section we are going to show that such a set of constraints forms a satisfiable system of relations and that the resulting LWE$_{n,q,x}$ problem is still in the regime of parameters for which it is conjectured to be hard.

Note that setting $m \geq 2 \cdot \lceil \log(q) \rceil \cdot n \cdot \lambda$ makes the first message 2-to-1 compressing. We now argue about the (weak) correctness of our scheme.

**Theorem 4 (Correctness).** The construction LOT = (Setup, Hash, KGen, Receive) as defined in Figure 3 is $(1/\lambda^2)$-correct.

**Proof of Theorem 4:** For all $i \in \{1, \ldots, \lambda\}$, we expand the product

$$b^{(i)} \bar{D} = \sum_{j \neq L} D[j] \cdot b_j^{(i)}$$

by linearity. Applying the equality above for all $i \in \{1, \ldots, \lambda\}$.
\{1, \ldots, \lambda\} \text{ we obtain}
\begin{align*}
k^{(i)} &= \left[ -1 \right]^{[D_L]} \cdot b^{(i)} \bar{D} + t^{(i)} \left[ D_L \right]
&= \left[ -1 \right]^{[D_L]} \cdot \left( s^T d^{(i)} - D_L \cdot s^T a^L_{k^*} \right) + \\
&\quad \left[ -1 \right]^{[D_L]} \sum_{j \neq L} D[j] \cdot e_j^{(i)} + t^{(i)} \left[ D_L \right]
&= \left[ -1 \right]^{[D_L]} \cdot s^T d^{(i)} + D_L \cdot s^T a^L_{k^*} + \\
&\quad \left[ -1 \right]^{[D_L]} \sum_{j=1}^m D[j] \cdot e_j^{(i)} + t^{(i)} \left[ D_L \right]
&= \left[ -1 \right]^{[D_L]} \cdot s^T d^{(i)} + \\
&\quad \left[ -1 \right]^{[D_L]} \sum_{j=1}^m \left[ D_L \right] \cdot e_j^{(i)} + t^{(i)} \left[ D_L \right]
&= k^{(i)} \left[ D_L \right]
\end{align*}
except with probability

\begin{align*}
\frac{2mb + 1}{q}
\end{align*}

Setting \( \log(q) \geq 3 \log(\lambda) + \log(2mbc + c) \) then we have that the above equality holds for all \( i \in \{1, \ldots, \lambda\} \) except with probability at most \( 1/\lambda^3 \). Taking a union bound over the \( \lambda \)-many parallel repetitions gives us the desired inequality.

We now argue that our construction satisfies weak sender security.

**Theorem 5 (Weak Sender Security).** If the LWE\(_{n,q,x}\) assumption holds, then the construction LOT = (Setup, Hash, KGen, Receive) as defined in Figure 3 is weakly sender secure.

**Proof of Theorem 5:** We show the claim with a reduction against the LWE\(_{n,q,x}\) problem. Assume towards contradiction that there exists a PPT adversary \( \mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2) \) such that

\[
\Pr [\text{ExpSendSec}_{\text{LOT}, \mathcal{A}}(\lambda) = 1] = \frac{1}{\text{poly}(\lambda)}.
\]

Then we construct a reduction (\( \mathcal{R} \)) that solves LWE\(_{n,q,x}\) as follows. The reduction is given a challenge (A, u) where A \( \in \mathbb{Z}_{q}^{n \times m \cdot \lambda} \) and u \( \in \mathbb{Z}_{q}^{n \cdot \lambda} \) and parses A as the horizontal concatenation of \( \lambda \)-many \( \mathbb{Z}_{q}^{n \times m} \) matrices (\( A^{(i)}, \ldots, A^{(\lambda)} \)). The adversary \( \mathcal{A}_1 \) is invoked on input \( c_{rs} = (A^{(i)}, \ldots, A^{(\lambda)}) \) and returns a tuple \( (d, L, s) \). For each \( i \in \{1, \ldots, \lambda\} \), the reduction sets the vector \( b^{(i)} \) to \( (u_{(i-1)m+1}, \ldots, u_{(i-1)m+m}) \) except that it omits the element \( u_{(i-1)m+L} \). Then samples \( (t^{(i)}_0, t^{(i)}_1) \) \( \leftarrow \mathcal{Z}_{q}^{2} \) uniformly at random. The reduction returns to the adversary \( \mathcal{A}_2 \) the ciphertext

\[
c = (b^{(1)}, t^{(1)}_0, t^{(1)}_1, \ldots, b^{(\lambda)}, t^{(\lambda)}_0, t^{(\lambda)}_1)
\]
along with the state s. The adversary outputs a pair \( (k_0, k_1) \) that is parsed by the reduction as the concatenation of two \( \lambda \)-long vectors in \( \mathbb{Z}_{q}^L \) \( k_0 = k^{(1)}_0 \cdots k^{(\lambda)}_0 \) and \( k_1 = k^{(1)}_1 \cdots k^{(\lambda)}_1 \). For all \( i \in \{1, \ldots, \lambda\} \), define \( R^{(i)}_0 \) as the interval of all elements \( y_0 \in \mathbb{Z}_{q} \) such that \( y_0 \in R^{(i)}_0 \) and \( y_1 \in R^{(i)}_1 \) such that \( y_0 + y_1 = z \). The reduction checks whether \( u_{(i-1)m+L} + t^{(i)}_0 + t^{(i)}_1 \in R^{(i)} \) and returns 1 if this is the case for all \( i \in \{1, \ldots, \lambda\} \). Else it returns 0.

Note that all steps are efficiently computable: In particular, for all \( k^{(i)}_0 \in \mathbb{Z}_{q} \) the corresponding interval \( R^{(i)}_b \) consists of \([p \cdot k^{(i)}_b, p \cdot (k^{(i)}_b + 1) - 1]\) and consequently also \( R^{(i)} \) is trivial to compute. We analyze the probability that the reduction outputs 1 for two separate cases.

Uniform Samples: In this case it is enough to observe that all elements \( u_L, \ldots, u_{\lambda-1 \cdot m+L} \) are uniform in \( \mathbb{Z}_{q}^L \) and completely independent from the view of the adversary. Therefore, for all \( i \in \{1, \ldots, \lambda\} \), the probability that \( u_{(i-1)m+L} + t^{(i)}_0 + t^{(i)}_1 \in R^{(i)} \) is at most

\[
\frac{|R^{(i)}|}{q} = \frac{|R^{(i)}_0| + |R^{(i)}_1|}{q} = \frac{2q}{q} \cdot \frac{1}{q} = \frac{2}{c}
\]

Setting \( c = 4 \) we obtain that the probability that the reduction outputs 1 is at most \( 1/2^\lambda \).

LWE Samples: Note that in this case the input given to the adversary are identically distributed as an honest run of the protocol where the keys are (implicitly) set to

\[
k^{(i)}_0 = [s^T d^{(i)} + t^{(i)}_0]_c
\]
and

\[
k^{(i)}_1 = [-s^T d^{(i)} + u_{(i-1)m+L} + t^{(i)}_1]_c
\]
where \(d^{(i)}\) is part of the digest \(d\) given by the adversary. Let \(\text{guess}\) be the event that the adversary correctly guesses both \(k_0\) and \(k_1\). Then, by the law of total probability we have

\[
\Pr[1 \leftarrow R] = \Pr[1 \leftarrow R|\text{guess}] \Pr[\text{guess}] + \Pr[1 \leftarrow R|\neg \text{guess}] \Pr[\neg \text{guess}]
\]

\[
\geq \Pr[1 \leftarrow R|\text{guess}] \Pr[\text{guess}]
\]

\[
= \Pr[1 \leftarrow R|\text{guess}] \frac{1}{\text{poly}(\lambda)}
\]

by initial hypothesis. Conditioned on the fact that the adversary correctly guesses both \(k_0\) and \(k_1\), then for all \(i \in \{1, \ldots, \lambda\}\) we have that

\[
s^T d^{(i)} + t^{(i)}_0 \in R_0^{(i)}
\]

and

\[
-s^T d^{(i)} + u_{(i-1)m+L} + t^{(i)}_1 \in R_1^{(i)}
\]

definition, and consequently

\[
s^T d^{(i)} + t^{(i)}_0 - s^T d^{(i)} + u_{(i-1)m+L} + t^{(i)}_1 = u_{(i-1)m+L} + t^{(i)}_1 + t^{(i)}_0 \in R^{(i)}.
\]

Thus the reduction outputs 1 with probability 1. It follows that \(\Pr[1 \leftarrow R] \geq 1/\text{poly}(\lambda)\).

The two bounds above show that the probability that the reduction outputs 1 differs by a non-negligible amount depending on whether \((A, u)\) is an LWE sample or not. This contradicts the LWE\(_{n,q,x}\) assumption and concludes our proof.

**Parameters.** The above analysis fixes the following set of constraints:

- \(m \geq 2 \cdot \lceil \log(q) \rceil \cdot n \cdot \lambda\)
- \(\log(q) \geq 3 \log(\lambda) + \log(2mBc + c)\)
- \(c = 4\)

Ignoring the constants, the constraint \(O(\log(q)) \geq O(\log(\lambda) + \log(m) + \log(B))\) introduces a gap polynomial in \(\lambda\) in the modulo-to-ratio, since \(m\) is polynomially bounded. Note that the circular dependency of the first two constraints is always satisfied for a large enough \(q\). The parameter \(n\) is free and can be set to the regime for which LWE\(_{n,q,x}\) is conjectured to be hard.

**C. Upgrading Laconic Oblivious Transfer**

We first upgrade the security and then the efficiency of a LOT, through generic transformations.

**From Weak Sender Security to Sender Indistinguishability.** We show how to generically upgrade any weak LOT into a LOT with sender indistinguishability. The compiler, shown in Figure 4, heavily relies on the tools introduced by Döttling et al. [16]: We first ensure that the adversary is not able to produce some digest \(d\) that allows him to predict \(k_0\) for some values of \(c\) and \(k_1\) for the others. This is done by amplifying the success probability of the adversary up to the point where it is no longer possible to be successful consistently on two different choices for the receiver’s bit. Then we turn the search problem into a decision one, using the standard Goldreich-Levin hard-core predicate [19]. Here the function \(\text{GLEnc}(k; t)\) is defined as \(\sum_{i=1}^{\lambda} k_i \cdot t_i\), computed over \(\mathbb{F}_2\).

The following theorem establishes our claim. The analysis is imported by the work of Döttling et al. [16] and is given in the full version.

**Theorem 6 (Weak to Full Sender Security).** Let LOT = (Setup, Hash, KGen, Receive) be a weak LOT. Then LOT = (Setup, Hash, KGen, Receive) as defined in Figure 4 is a standard LOT.

**From Indistinguishability Security to Context Security.** We now show that any LOT with indistinguishability security also suffices context security. To establish this, we will use distinguisher-dependent simulation. Technically, the theorem uses the same ideas of Theorem 6.3 in [16] and some paragraphs are verbatim from [16].

**Theorem 7 (Ind. to Context Security).** Assume that LOT = (Setup, Hash, Send, Receive) satisfies indistinguishability security. Then it also satisfies context security.

**Proof of Theorem 7:** We prove the theorem via several lemmas. In order to do so, we will first provide constructions of the relevant algorithms. Fix a PPT-context \(Z = (Z_1, Z_2)\) for LOT. We start by defining a hybrid sender algorithm as follows:

\(S_i((crs,d,(x_1^*, \ldots, x_i^*)), L, m_0, m_1)\):

- If \(L > i\) output \(\text{Send}(crs,d,L,m_0,m_1)\)
- Otherwise, set \(m_i^{x_i^*} = m_{x_i^*}^{x_i^*}\) and \(m_j^{x_j^*} = 0\)
- compute and output \(\text{Send}(crs,d,L,m_0,m_1)\)

We introduce the following notation. For an efficiently sampleable random variable \(T \in \{0,1\}\) we use the shorthand “Compute an approximation \(\bar{\mu}\) of \(E[T]\) with error \(\delta\)” to denote the following algorithm which computes a sample average:

- Set \(N = \lceil \lambda/\delta^2 \rceil\)
- For \(j \in \{1, \ldots, N\}\) sample \(t_j \leftarrow T\)
- Output \(\bar{\mu} \leftarrow \frac{1}{N} \sum_{j=1}^{N} t_j\)

We also define the following bit-extraction algorithm, which extracts an approximation of the \(i\)-th bit of the receiver’s input.
\text{Setup}(1^\lambda) : \text{Return Setup}(1^\lambda).
\text{Hash}(\text{crs}, D) : \text{Return Hash}(\text{crs}, D).
\text{Send}(\text{crs}, d, L, m_0, m_1) :
\begin{itemize}
\item For all \( i \in \{1, \ldots, \lambda\} \): Sample \((c(i), k_0(i), k_1(i)) \leftarrow \text{KGen}(\text{crs}, d, L)\).
\item Set \( \tilde{c} = (c(1), \ldots, c(\lambda)) \), \( K_0 = (k_0(1), \ldots, k_0(\lambda)) \), and \( K_1 = (k_1(1), \ldots, k_1(\lambda)) \).
\item Sample two random strings \((t_0, t_1) \leftarrow \{0, 1\}^{K_0[|+|K_1]}\).
\item For all \( b \in \{0, 1\} \): Compute \( C_b = \text{GLEnc}(K_b, t_b) \oplus m_b \).
\item Return \( c = (\tilde{c}, C_0, C_1, t_0, t_1) \).
\end{itemize}
\text{Receive}^D(\text{crs}, c, L) :
\begin{itemize}
\item Parse \( c \) as \((\tilde{c}, C_0, C_1, t_0, t_1)\).
\item For all \( i \in \{1, \ldots, \lambda\} \): Compute \( k(i) \leftarrow \text{Receive}^D(\text{crs}, c(i), L)\).
\item Set \( K = (k(1), \ldots, k(\lambda)) \).
\item Return \( \text{GLEnc}(K; t_{D[L]}) \oplus \tilde{c} \).
\end{itemize}

\text{Figure 4: From Weak to Full Sender Security.}

\text{Extract}_i(\text{crs}, st, d, r_1, (x^*_1, \ldots, x^*_{i-1}), \varepsilon') :
\begin{itemize}
\item Compute an approximation \( \bar{\mu} \) of \( E[Z_2^{\tilde{S}_i(\text{crs}, d, (x^*_1, \ldots, x^*_{i-1}), \cdot, \cdot)}(\text{crs}, st)] \) with error \( \varepsilon' / 4 \).
\item Compute an approximation \( \bar{\mu}_0 \) of \( E[Z_2^{\delta_i(\text{crs}, d, (x^*_1, \ldots, x^*_{i-1}, 0), \cdot, \cdot)}(\text{crs}, st)] \) with error \( \varepsilon' / 4 \).
\item Compute an approximation \( \bar{\mu}_1 \) of \( E[Z_2^{\delta_i(\text{crs}, d, (x^*_1, \ldots, x^*_{i-1}), \cdot, \cdot)}(\text{crs}, st)] \) with error \( \varepsilon' / 4 \).
\item Set \( \delta_{i, 0} \leftarrow |\bar{\mu}_{i, 0} - \bar{\mu}_i| \).
\item Set \( \delta_{i, 1} \leftarrow |\bar{\mu}_{i, 1} - \bar{\mu}_i| \).
\item If \( \delta_{i, 0} > \varepsilon' \) and \( \delta_{i, 1} > \varepsilon' \) abort and output \( \bot \).
\item Else if \( \delta_{i, 1} > 2\varepsilon' \) output \( x^*_i \leftarrow 0 \).
\item Otherwise output \( x^*_i \leftarrow 1 \).
\end{itemize}

We now define the context extractor \( \text{Ext}_Z \) and the simulator \( \text{Sim} \). The setup-simulator \( \text{SimSetup} \) is identical to the Setup algorithm, thus we do not specify it.

\text{Ext}_Z(\text{crs}, st, d, r^*, \varepsilon) :
\begin{itemize}
\item For \( j \in \{1, \ldots, i\} \) : Compute \( x^*_j \leftarrow \text{Extract}_j(\text{crs}, st, d, (x^*_1, \ldots, x^*_{j-1}), \varepsilon') \).
\item Output \( x^* \leftarrow (x^*_1, \ldots, x^*_n) \).
\end{itemize}

\text{Sim}(\text{crs}, d, x^*, z = (L, m)) :
\begin{itemize}
\item Set \( m_{x^*_z} = m \) and \( m_{1-x^*_z} = 0 \).
\item Compute and output \( \text{Send}(\text{crs}, d, L, m_0, m_1) \).
\end{itemize}

Finally, we set choose \( \varepsilon'(\varepsilon) = \varepsilon / n \). This choice of \( \varepsilon' \) will become meaningful in a moment. Assume towards contradiction that there exists an inverse polynomial \( \varepsilon \) such that it holds for infinitely many \( \lambda \) that
\[
|\Pr[Z(1^\lambda) = 1] - \Pr[\varepsilon Z(1^\lambda, \varepsilon') = 1]| > \varepsilon,
\]
where \( \varepsilon' = \varepsilon / n \). Consider the following sequence of hybrid experiments.

Hybrid \( \mathcal{H}_0 \) : This experiment is real context \( Z(1^\lambda) \).
For \( i \in \{1, \ldots, n\} \) define the following hybrids.

\text{Hybrid} \( \mathcal{H}_i \) :
\begin{itemize}
\item Choose random tapes \( r_1, r_2 \).
\item Compute \( \text{crs} \leftarrow \text{Setup}(1^\lambda) \).
\item Compute \( (\text{st}, d, \text{aux}) \leftarrow Z_1(\text{crs}, r_1) \).
\item For \( j \in \{1, \ldots, i\} \) : Compute \( x^*_j \leftarrow \text{Extract}_j(\text{crs}, st, d, (x^*_1, \ldots, x^*_{j-1}), \varepsilon') \).
\item Output \( b^* \leftarrow Z_0(\cdot, \cdot)(\text{st}, r_2) \), where the oracle \( \mathcal{O}_i(L, m_0, m_1) \) returns \( S_i(\text{crs}, d, (x^*_1, \ldots, x^*_i), L, m_0, m_1) \).
\end{itemize}

Notice that it holds that \( \mathcal{H}_n \) is identically distributed to \( \varepsilon Z(1^\lambda, \varepsilon') \). Consequently, it holds by the averaging principle that there must exist an index \( i^* \in \{1, \ldots, b\} \) such that
\[
\Pr[\mathcal{H}_{i^*} = 1] - \Pr[\mathcal{H}_{i^*-1} = 1] > \varepsilon / n.
\]

We now construct an adversary against the indistinguishability security of LOT. The algorithm \( \text{Extract}_{i^*}(\text{crs}, st, d, (x^*_1, \ldots, x^*_{i^*-1}), \varepsilon') \) computes approximations \( \delta_{i^*, 0} \) and \( \delta_{i^*, 1} \) of the advantages
\[
\begin{align*}
\delta_{i^*, 0} &= \Pr[Z_2^{S_i(\text{crs}, d, L, m_0, m_1)}(\text{crs}, st) = 1] - \Pr[Z_2^{S_{i^*-1}(\text{crs}, d, L, m_0, m_1)}(\text{crs}, st) = 1], \\
\delta_{i^*, 1} &= \Pr[Z_2^{S_i(\text{crs}, d, L, m_0, m_1)}(\text{crs}, st) = 1] - \Pr[Z_2^{S_{i^*-1}(\text{crs}, d, L, m_0, m_1)}(\text{crs}, st) = 1].
\end{align*}
\]

698
We first establish that the approximations $\tilde{\delta}_{i^*,0}$ and $\tilde{\delta}_{i^*,1}$ are close to $\delta_{i^*,0}$ and $\delta_{i^*,1}$ respectively, except with negligible probability over the coins used to compute the approximations. We establish this by a routine application of the Hoeffding bound.

Lemma 3. Fix crs, st, d and $(x_1^*, \ldots, x_{i^*-1}^*)$. Then it holds that

$$|\tilde{\delta}_{i^*,0} - \delta_{i^*,0}| \leq \varepsilon'$$

$$|\tilde{\delta}_{i^*,1} - \delta_{i^*,1}| \leq \varepsilon'$$

except with probability $2^{-\lambda}$ over the choice of $r_{Extract,i^*}$.

Proof of Lemma 3: The random variable $\tilde{\mu}_{i^*}$ is the average of $N = \lceil \lambda/\varepsilon'^2 \rceil$ samples of

$$Y = Z_{2}^{S_{i^*-1}(crs,d,(x_1^*, \ldots, x_{i^*-1}^*))}(crs, st).$$

Analogously, for $b \in \{0, 1\}$ the random variables $\tilde{\mu}_{i^*,b}$ is the average of $N = \lceil \lambda/\varepsilon'^2 \rceil$ samples of

$$Y_b = Z_{2}^{S_{i^*}(crs,d,(x_1^*, \ldots, x_{i^*-1}^*,b))}(crs, st).$$

We can thus write

$$\delta_{i^*,b} = |E[Y_b] - E[Y]|.$$

Consequently, it holds by the Hoeffding inequality (Theorem 1) that

$$\Pr[|\tilde{\mu}_{i^*} - E[Y]| > \varepsilon'/2] \leq 2e^{-2N(\varepsilon'/2)^2} \leq 2e^{-\lambda}$$

and for $b \in \{0, 1\}$

$$\Pr[|\tilde{\mu}_{i^*,b} - E[Y_b]| > \varepsilon'/2] \leq 2e^{-2N(\varepsilon'/2)^2} \leq 2e^{-\lambda}.$$

Given that

$$|\tilde{\mu}_{i^*} - E[Y]| \leq \varepsilon'/2$$

$$|\tilde{\mu}_{i^*,0} - E[Y_0]| \leq \varepsilon'/2$$

$$|\tilde{\mu}_{i^*,1} - E[Y_1]| \leq \varepsilon'/2$$

and using that

$$\tilde{\delta}_{i^*,0} = |\tilde{\mu}_{i^*,0} - \tilde{\mu}_{i^*}|$$

$$\tilde{\delta}_{i^*,1} = |\tilde{\mu}_{i^*,1} - \tilde{\mu}_{i^*}|$$

we get that

$$|\tilde{\delta}_{i^*,0} - \delta_{i^*,0}| \leq \varepsilon'$$

and

$$|\tilde{\delta}_{i^*,1} - \delta_{i^*,1}| \leq \varepsilon'.$$

Consequently, it holds by a union-bound that

$$\Pr\left[|\tilde{\delta}_{i^*,0} - \delta_{i^*,0}| > \varepsilon' \text{ or } |\tilde{\delta}_{i^*,1} - \delta_{i^*,1}| > \varepsilon'\right] \leq 6e^{-\lambda} \leq 2^{-\lambda}$$

which concludes the proof.

Lemma 4. Assume that

$$|\Pr[\mathcal{H}_i = 1] - \Pr[\mathcal{H}_{i^* - 1} = 1]| \geq \varepsilon'$$

for an $i^* \in \{1, \ldots, n\}$. Then there exists a PPT adversary $B$ which breaks the indistinguishability sender security of LOT.

Proof of Lemma 4: First note that $\mathcal{H}_{i^* - 1}$ and $\mathcal{H}_{i^*}$ are identical until $x_{i^*} \leftarrow Extract_i(crs, st, d, (x_1^*, \ldots, x_{i^*-1}^*), \varepsilon')$ is computed in $\mathcal{H}_{i^*}$. We therefore first rephrase $\mathcal{H}_{i^* - 1}$ and $\mathcal{H}_{i^*}$.

Towards this goal, define an alternate first stage $Z_{1}'(crs, r_1)$ by

- Compute $(st, d) \leftarrow Z_1'(crs, r_1)$
- For $j \in \{1, \ldots, i^* - 1\}$: Compute $x_j^* \leftarrow Extract_j(crs, st, d, (x_1^*, \ldots, x_{i^*-1}^*), \varepsilon')$
- Output $(st, d, aux, (x_1^*, \ldots, x_{i^*}^*))$

We can now rephrase $\mathcal{H}_{i^* - 1}$ and $\mathcal{H}_{i^*}$ by cutting of the common prefix.

Hybrid $\mathcal{H}_{i^*}'(crs, st, d, aux, (x_1^*, \ldots, x_{i^*-1}^*))$:

- Compute $(st, d, aux, (x_1^*, \ldots, x_{i^*-1}^*)) \leftarrow Z_{1}'(crs, r_1)$
- Compute $b^* \leftarrow Z_2^{S_{i^*}(crs,d,(x_1^*, \ldots, x_{i^*-1}^*),\ldots)}(st, r_2)$

Hybrid $\mathcal{H}_{i^*}'(crs, st, d, aux, (x_1^*, \ldots, x_{i^*-1}^*))$:

- Compute $(st, d, aux, (x_1^*, \ldots, x_{i^*-1}^*)) \leftarrow Z_{1}'(crs, r_1)$
- Compute $x_{i^*}^* \leftarrow Extract_{i^*}(crs, st, d, (x_1^*, \ldots, x_{i^*-1}^*), \varepsilon')$
- Compute $b^* \leftarrow Z_2^{S_{i^*}(crs,d,(x_1^*, \ldots, x_{i^*-1}^*),\ldots)}(st, r_2)$

Further, fix $crs, st, d, (x_1^*, \ldots, x_{i^*-1}^*)$ and the random tape $r_2$ used for $Extract_{i^*}$ and collect them in a variable $z$. Note that the parameters in inp also determine $x_{i^*}^*$. We now define three events gap(inp), approx(inp) and good(inp) which only depend on inp.

1) gap(inp) holds, if and only if

$$|\Pr[\mathcal{H}'_i(inp) = 1] - \Pr[\mathcal{H}'_{i^* - 1}(inp) = 1]| > 4\varepsilon',$$

where the random coins are over the random coins $r_2$ of $Z_2$ and the random choices made by the oracles $S_{i^* - 1}$ and $S_{i^*}$.

2) Let $\delta_{i^*,0}$ and $\delta_{i^*,1}$ be the approximated values computed during the execution of $Extract_{i^*}(crs, st, d, (x_1^*, \ldots, x_{i^*-1}^*), \varepsilon')$. approx(inp) holds, if and only if

$$|\delta_{i^*,0} - \delta_{i^*,0}| \leq \varepsilon'$$

$$|\delta_{i^*,1} - \delta_{i^*,1}| \leq \varepsilon'.$$
3) good(inp) holds if and only if
\[
\delta_{i^*} > \varepsilon',
\delta_{i^*} > \varepsilon'.
\]
We first elaborate on the events in more detail. The event gap(inp) characterizes that for the same choice of inp, the hybrids \( H_{i^*}(\text{inp}) \) and \( H_{i^* - 1}(\text{inp}) \) have distance at least \( 4\varepsilon' \). Notice that the extracted prefix \( (\bar{x}_1, \ldots, \bar{x}_{i^* - 1}) \) is identical in both experiments \( H_{i^*}(\text{inp}) \) and \( H_{i^* - 1}(\text{inp}) \). Consequently, gap(inp) immediately implies that none of the \( x_{i^* - 1} \) was set to \( \perp \), as this would imply that the two experiments are identically distributed.

The event approx(inp) ensures that the approximations \( \delta_{i^*} \) and \( \delta_{i^* - 1} \) are sufficiently close to the true advantages. Finally, the event good(inp) ensures that inp is such that we will be able to mount a successful attack against indistinguishability sender security of LOT. Our first goal will be to show that the event good(inp) holds with reasonably high probability over the choice of inp. Once this is established, we will construct an adversary \( B \) against the indistinguishability sender security of LOT. Observe that by Lemma 3 it holds that
\[
\Pr_{\text{inp}}[-\text{approx}(\text{inp})] \leq 2^{-\lambda}. \tag{1}
\]
Since
\[
|\Pr_{\text{inp}}[H_{i^*}(\text{inp}) = 1] - \Pr_{\text{inp}}[H_{i^* - 1}(\text{inp}) = 1]| = |\Pr_{\text{inp}}[H_{i^*} = 1] - \Pr_{\text{inp}}[H_{i^* - 1} = 1]| \geq 8 \cdot \varepsilon',
\]
it holds by the Markov inequality for advantages (Lemma 1) that
\[
\Pr_{\text{inp}}[\text{gap}(\text{inp})] = \Pr_{\text{inp}} \left[ \left| \Pr_{\text{inp}}[H_{i^*}(\text{inp}) = 1] - \Pr_{\text{inp}}[H_{i^* - 1}(\text{inp}) = 1] \right| > 4\varepsilon' \right] \geq 4\varepsilon'. \tag{2}
\]
We now show that if gap(inp) holds, then it must either good(inp) or not approx(inp). We will establish this by showing that good(inp) and approx(inp) imply gap(inp). Thus, fix inp \( = (crs, st, d, (x_1^*, \ldots, x_{i^* - 1}^*), r_i^*) \) with good(inp) and approx(inp). From good(inp) it follows that there is a \( \beta \in \{0, 1\} \) such that
\[
\frac{\Pr_{\text{inp}}[Z_2^{S_{i^*}(crs, d, (x_1^*, \ldots, x_{i^* - 1}^*, \beta)) \cdot (crs, st) = 1] - \Pr_{\text{inp}}[Z_2^{S_{i^* - 1}(crs, d, (x_1^*, \ldots, x_{i^* - 1}^*), \beta)) \cdot (crs, st) = 1]} \leq \varepsilon'.
\]
We are now going to show that under this condition Extract\(_{i^*}(crs, st, d, (x_1^*, \ldots, x_{i^* - 1}^*), \varepsilon') \) will be able to identify the correct \( x_{i^*} \). Observe that since it holds that approx(inp), we get that
\[
\delta_{i^*, \beta} \leq \delta_{i^*, \beta} + \varepsilon' \leq 2\varepsilon'.
\]
Consequently, Extract\(_{i^*}(crs, st, d, (x_1^*, \ldots, x_{i^* - 1}^*), \varepsilon') \) will not output \( \perp \). We distinguish two cases.

Case 1: In this case it holds that
\[
\delta_{i^*, 1} \leq 4\varepsilon'.
\]
It follows immediately that
\[
\delta_{i^*, x_{i^*}} \leq 4\varepsilon',
\]
regardless which \( x_{i^*} \in \{0, 1\} \) is chosen.

Case 2: In this case it holds that
\[
\delta_{i^*, 1} > 4\varepsilon'.
\]
Again since it holds that approx(inp), we get that
\[
\delta_{i^*, 1} - \varepsilon' \geq 3\varepsilon' > 2\varepsilon'.
\]
Consequently, Extract\(_{i^*}(crs, st, d, (x_1^*, \ldots, x_{i^* - 1}^*), \varepsilon') \) will set \( x_{i^*} \leftarrow \beta \) and again we can conclude
\[
\delta_{i^*, x_{i^*}} \leq 4\varepsilon'.
\]
Furthermore, observe that, since Extract\(_{i^*}(crs, st, d, (x_1^*, \ldots, x_{i^* - 1}^*), \varepsilon') \) will not output \( \perp \), the output of \( H_{i^*}(\text{inp}) \) is distributed according to \( Z_2^{S_{i^*}(crs, d, (x_1^*, \ldots, x_{i^* - 1}^*), \beta)) (st, r_2) \). We also know that \( H_{i^* - 1}(\text{inp}) \) is distributed according to \( Z_2^{S_{i^* - 1}(crs, d, (x_1^*, \ldots, x_{i^* - 1}^*), \beta)) (st, r_2) \). This implies that
\[
\Pr_{\text{inp}}[H_{i^*}(\text{inp}) = 1] - \Pr_{\text{inp}}[H_{i^* - 1}(\text{inp}) = 1] = \frac{\Pr_{\text{inp}}[Z_2^{S_{i^*}(crs, d, (x_1^*, \ldots, x_{i^* - 1}^*), \beta)) \cdot (crs, st) = 1] - \Pr_{\text{inp}}[Z_2^{S_{i^* - 1}(crs, d, (x_1^*, \ldots, x_{i^* - 1}^*), \beta)) \cdot (crs, st) = 1]} \leq 4\varepsilon',
\]
which in turn implies that \( -\text{gap}(\text{inp}) \). Thus, we have established that
\[
\text{gap}(\text{inp}) \Rightarrow \text{good}(\text{inp}) \text{ or } -\text{approx}(\text{inp}). \tag{3}
\]
From (2), (3) and (1) we obtain that
\[
4\varepsilon' \leq \Pr[\text{gap}(\text{inp})] \leq \Pr[\text{good}(\text{inp}) \text{ or } -\text{approx}(\text{inp})] \leq \Pr[\text{good}(\text{inp})] + \Pr[-\text{approx}(\text{inp})] \leq \Pr[\text{good}(\text{inp})] + 2^{-\lambda},
\]
where the third inequality follows by the union-bound. This implies that
\[
\Pr[\text{good}(\text{inp})] \geq 4\varepsilon' - 2^{-\lambda} > \varepsilon'.
\]
We are now ready to construct an adversary $B$ against the indistinguishability sender privacy of LOT. The adversary $B = (B_1, B_2)$ is given as follows. In abuse of notation, we assume that $B$ is stateful, i.e. the second stage $B_2$ remembers all variables of the first stage $B_1$. 

$B_1(crs; r_1)$:

- Compute $(st, d) \leftarrow Z_1^t(crs, r_1)$
- For $j \in \{1, \ldots, i^* - 1\}$: Compute $x_j^t \leftarrow \text{Extract}_j(crs, st, d, (x_1^t, \ldots, x_{j-1}^t), \varepsilon')$
- Output $(d, i^*)$

$B_2^{O(\cdot)}(st, r_2)$:

- Compute and output $b^* \leftarrow Z_2^{S_{i^*}}(\cdot, \cdot, \cdot)$, where the oracle $S_{i^*}(L, m_0, m_1)$ is implemented as follows:
  - If $L > i^*$ output $\text{Send}(crs, d, L, m_0, m_1)$
  - If $L < i^*$, set $m_{x_1} = m_{x_2} = 0$ and $m_{1} = 0$
  - output $\text{Send}(crs, d, L, m_1, m_1')$
  - If $L = i^*$ query and output $O(m_0, m_1)$

Fix $crs$ and $r_1$. We distinguish 3 cases.

**Case 1**: The oracle $O(m_0, m_1)$ computes the function $\text{Send}(crs, d, i^*, m_0, m_1)$. It follows by inspection that in this case the output of $B$ is distributed according to $\mathbb{Z}_2^{S_{i^*}}(crs, d, (x_1^t, \ldots, x_{i^*-1}^t), \cdot, \cdot, \cdot, \cdot, \cdot)(crs, st)$.

**Case 2**: The oracle $O(m_0, m_1)$ computes the function $\text{Send}(crs, d, i^*, m_0, 0)$. It follows by inspection that in this case the output of $B$ is distributed according to $\mathbb{Z}_2^{S_{i^*}}(crs, d, (x_1^t, \ldots, x_{i^*-1}^t, 0), \cdot, \cdot, \cdot, \cdot, \cdot)(crs, st)$.

**Case 3**: The oracle $O(m_0, m_1)$ computes the function $\text{Send}(crs, d, i^*, m_0, 1)$. It follows by inspection that in this case the output of $B$ is distributed according to $\mathbb{Z}_2^{S_{i^*}}(crs, d, (x_1^t, \ldots, x_{i^*-1}^t, 1), \cdot, \cdot, \cdot, \cdot, \cdot)(crs, st)$.

We conclude that the advantage of the adversary (fixing the bit $b$) is equal to

$$\Pr[\mathbb{Z}_2^{S_{i^*}}(crs, d, (x_1^t, \ldots, x_{i^*-1}^t, b), \cdot, \cdot, \cdot, \cdot, \cdot)(crs, st) = 1] - \Pr[\mathbb{Z}_2^{S_{i^*}}(crs, d, (x_1^t, \ldots, x_{i^*-1}^t), \cdot, \cdot, \cdot, \cdot, \cdot)(crs, st) = 1].$$

This implies that for both $b \in \{0, 1\}$ the advantage of the adversary is

$$\Pr_{crs, r_1, t, t'}[\text{good}(crs, r_A, t, \text{Extract})] > \varepsilon',$$

which contradicts the indistinguishability sender privacy of LOT.

**Weak to Full Efficiency.** The following construction shows that it suffices to consider LOT schemes with 2-to-1 compressing Hash and algorithms Send and Receive with polynomial running times in the size of the database. A similar statement already appeared in the work of Cho et al. [3], however their analysis crucially relies on the semi-honest settings and does not directly extend to malicious security. In the following we recall a simplified version of the transformation from [3]. We assume without loss of generality that the database has $2^d \cdot \lambda$ locations, which can be indexed with strings of the form $b_1 \ldots b_0 \parallel t$ where the bits $b_i$ define the root-to-leaf path and the string $t$ define the position of the leaf. For ease of exposition we overload the notation for the sender algorithm and we write $\text{Send}(crs, d, K)$ as $\text{Send}(crs, d, 1, (K_0, K_1)) \ldots || \text{Send}(crs, d, 2\lambda, (K_0^{2\lambda}, K_1^{2\lambda}))$ where $K$ consists of $2\lambda$ pairs of $\lambda$-bit strings. The same shortcut is used for the receiver algorithm.

The construction (given in Figure 7) consists of a chaining of garbled circuits that allows the receiver to traverse the tree downwards via the selected path. Since the sender only knows the root of the tree, the generation of subsequent Send algorithms is deferred by garbling the circuit $C_{\text{trav}}$ (Figure 6). Once the leaf is reached, the choice of the message can be constrained on the desired bit via the circuit $C_{\text{read}}$ (Figure 5).

The following theorem shows that considering a LOT with 2-to-1 compression factor suffices.

**Theorem 8 (Weak to Full Efficiency).** Let LOT = $(\text{Setup}, \text{Hash}, \text{Send}, \text{Receive})$ be a LOT with 2-to-1 compression. Then LOT = $(\text{Setup}, \text{Hash}, \text{Send}, \text{Receive})$ as defined in Figure 7 is LOT with arbitrary compression.

**Proof of Theorem 8:** We start with the high-level overview. Our strategy is to associate every node in the Merkle tree with two hybrids. In this sequence of hybrids we start in the root node traverse the tree in such a way that it is ensure that once we reach a node

**Figure 5:** Circuit $C_{\text{leaf}}[m_0, m_1]$.

**Figure 6:** Circuit $C_{\text{trav}}[crs, b, K, r]$. Hardwired Values: $(t, m_0, m_1)$.

Input: $(N_0^d || N_0^1, \ldots, N_{d-1}^d || N_{d-1}^1, N^d)$.

- Return $m_{N^t}[t]$.
H₁(δ) : This is the real experiment. Specifically,
  • crs ← Setup(1^λ)
  • (st, d) ← Z₁(cr)
  • Compute and output \( b^* \leftarrow Z_2^{O(0)}(st) \)
    where the oracle \( O(0)(L, m_0, m_1) \) implements Send\( crs, d, L, m_0, m_1 \)

Hybrid H₀(δ) : In this experiment we will extract \( d_{v_1} \) as a LOT hash (i.e., 2-to-1). First we rephrase \( H_0 \) as a context \( (Z_1^{(1)}, Z_2^{(1)}) \) for LOT. We will set \( Z_1^{(1)} = Z_1 \) but interpret \( d = d_{v_1} \) as a hash value for LOT. Moreover, we interpret \( Z_2^{O(0)}(st) \) as a single machine \( Z_2^{(1)} \), except for calls by \( O(0) \) to Send\( (crs, d, \cdot) \), which will be implemented by oracle calls. Consequently, \( Z_2^{O(0)}(st) \) and \( Z_2^{(1)} \) compute identical functions. Context security of LOT yields an extractor \( Ext_2^{(1)} \) and a simulator \( Sim \), which we will use in the construction of \( H_1 \). We can now define \( H_1 \) as follows.
  • crs ← Setup(1^λ)
  • (st, d) ← Z₁(cr)
  • Let \( ν_1, l \) be the left child node of the root node \( ν_1 \) and \( ν_{1, r} \) be the right child node of the root node \( ν_1 \).
    • \( (d_{v_1,l} \parallel d_{v_1,r}, \text{aux}_1) \leftarrow Ext_2^{(1)}(crs, st, d_{v_1,l}, δ) \)
  • Compute and output \( b^* \leftarrow Z_2^{O(0)}(st) \) where \( O(1) \) is identical to \( O(0) \), except that we replace calls to Send\( (crs, d_{v_1,l}, K) \) for any \( K \) by calls to Sim\( (crs, d, \text{aux}_{root}, K_{d_{v_1,l}, d_{v_1,r}}) \).

Define the following hybrids \( i \in \{1, \ldots, 2^d - 1\} \).

Hybrid H₂₁(δ) : \( O(2^i) \) is identical to \( O(2^i - 1) \), except for the following changes. For a given index \( L \) let \( ν_1^1, \ldots, ν'_d \) be the root-to-leaf path for \( L \), where \( ν_1^1 \) is the root node and \( ν'_d \) a leaf node. If \( ν_i = ν'_d \) (i.e., \( ν_i \) is the leaf-node in the path for index \( L \)), we replace the instruction \( (C_d, K^d) \leftarrow Garble(1^λ, C_{\text{leaf}}[t, m_0, m_1]) \) by \( (C_d, K^d) \leftarrow \text{GCSim}(1^λ, m_{D[t]}) \).

Otherwise, at node \( ν_i = ν'_j \) for some \( j \) we
replace the instruction \((\tilde{C}_i, K^j) \leftarrow \text{Garble}(1^\lambda, C_{\text{trav}}(crs, b_j, K^{j+1}, r_j))\) by \((\tilde{C}_{\text{trav}}, K^j_{\nu,i, ||\nu, r}) \leftarrow \text{GCSim}(1^\lambda, \text{Send}(crs, N_{b_j}, K;r))\).

**Hybrid \(H_{2i+1}(\delta)\):** In this experiment we will extract \(d_{\nu,i}\) as a LOT hash (i.e. 2-to-1). First we rephrase \(H_{2i}\) as a context for LOT. That is, we define a context \(Z_2^{(i)}\) which outputs a state \(st'\) comprising of a state \(st\) and all LOT hash preimages extracted so far. It also outputs the hash \(d_{\nu,i}\) at node \(\nu_i\).

Moreover, we interpret \(Z_2^{(2i+1)}(\cdot)\) as a single machine \(Z_2\), except for calls by \(O^{(2i)}\) to \(\text{Send}(crs, d_{\nu,i}, \cdot)\), which will be implemented by oracle calls. Consequently, \(Z_2^{(2i+1)}(\cdot)\) and \(Z_2^{(i)\text{Send}(crs, d_{\nu,i}, \cdot)}\) compute identical functions. Context security of LOT yields an extractor \(\text{Ext}_{\nu}^{(i)}\) and a simulator \(\text{Sim}\), which we will use in the construction of \(H_{2i+1}\). We can now define \(H_{2i+1}\) as follows.

- \(crs \leftarrow \text{Setup}(1^\lambda)\)
- \((st, d) \leftarrow Z_1(crss)\)
- For \(j \in \{0, \ldots, \ell\}\):
  - Let \(\nu_{j,l}\) be the left child of node \(\nu_j\) and \(\nu_{j,r}\) be the right child of node \(\nu_j\).
  - \((d_{\nu_{j,l}}, d_{\nu_{j,r}}, aux_j) \leftarrow \text{Ext}_\nu^{(i)}(crs, (st, (d_{\nu_k}, d_{\nu_k, i}, d_{\nu_k, r}, aux_k)_{k \leq j}), d_{\nu_j}, \delta)\)
  - Compute and output \(b^* \leftarrow Z_2^{(2i+1)}(st, \cdot)\), where \(O^{(2i+1)}\) is identical to \(O^{(2i)}\), except that we replace calls to \(\text{Send}(crs, d_{\nu,i}, K)\) for any \(K\) by calls to \(\text{Sim}(crs, d, aux_i, K_{d_{\nu,i}, ||\nu_{a,r}})\).

In the last hybrid \(H_{2(2i+1)}(\delta)\), the oracle \(O^{2i+1}\) does not make any calls to \(\text{Send}\), but only calls to \(\text{Sim}\). We can therefore now define the extractor \(\text{Ext}_\nu\) and the simulator \(\tilde{\text{Sim}}\).

\(\text{Ext}_\nu(crss, st, d, \delta)\):
- For \(j \in \{0, \ldots, \ell\}\):
  - Let \(\nu_{j,l}\) be the left child of node \(\nu_j\) and \(\nu_{j,r}\) be the right child of node \(\nu_j\).
  - \((d_{\nu_{j,l}}, d_{\nu_{j,r}}, aux_j) \leftarrow \text{Ext}_\nu^{(i)}(crs, (st, (d_{\nu_k}, d_{\nu_k, i}, d_{\nu_k, r}, aux_k)_{k \leq j}), d_{\nu_j}, \delta)\)
  - Set \(D = (D_1, \ldots, D_{2i})\)
  - Set \(aux = (aux_j)_{j}\)
  - Output \((D, aux)\)

\(\tilde{\text{Sim}}(crs, d, aux, (L, z))\):
- Let \(\nu'_1, \ldots, \nu'_d\) be the root-to-leaf path corresponding to \(L\)
- Compute \((\tilde{C}_d, K^d_{d_{\nu^d}, \nu}) \leftarrow \text{GCSim}(1^\lambda, m_{D[\ell]}\))
- For \(j \in \{d - 1, \ldots, 1\}\):
  - Let \(\nu_{j,l}\) be the left child of node \(\nu'_j\) and \(\nu_{j,r}\) be the right child of node \(\nu'_j\).
  - Compute \((\tilde{C}_{\text{trav}}, K^j_{\nu,i, ||\nu, r}) \leftarrow \text{GCSim}(1^\lambda, \text{Sim}(crs, d, aux_k, K^j_{\nu_{i,l}, ||\nu_{a,r}}))\)
  - Compute \(e \leftarrow \text{Sim}(crs, d, aux_k, K^j_{d_{\nu_{i,l}, ||\nu_{a,r}}})\)

As there are \(2\ell + 1\) hybrid steps, we set \(\delta = \epsilon/(2\ell + 1)\). Now assume towards contradiction that there exists an inverse polynomial \(\varepsilon\) such that it holds for infinitely many \(1^\lambda\) that

\[
\left| \Pr[Z^{(crs)} = 1] - \Pr[\mathcal{E}Z^{(crs, \varepsilon/(2\ell + 1))}] \right| > \varepsilon.
\]

As \(\mathcal{H}_0(\varepsilon/(2\ell + 1))\) is identical to \(Z^{(crs)}\) and \(\mathcal{H}_{2\ell+1}(\varepsilon/(2\ell + 1))\) is identical to \(\mathcal{E}Z^{(crs, \varepsilon/(2\ell + 1))}\), by the averaging principle there exists an \(k \in \{1, \ldots, 2\ell + 1\}\) such that

\[
\left| \Pr[\mathcal{H}_k(\varepsilon/(2\ell + 1)) = 1] - \Pr[\mathcal{H}_{k-1}(\varepsilon/(2\ell + 1))] \right| > \varepsilon/(2\ell + 1),
\]

We now show that this leads to a contradiction for every \(k \in \{1, \ldots, 2\ell + 1\}\).

**Case \(k = 1\):** In this case we show that this leads to a contradiction against the context-security of LOT. For hybrid \(H_1\) we constructed an LOT context \(Z_1 = (Z_1^{(1)}, Z_2^{(1)})\) which produces an output that is identically distributed to \(\mathcal{H}_0\). \(H_1\) is constructed in a way such that its output is identically distributed to that of \(\mathcal{E}Z\). Consequently, it holds that

\[
\left| \Pr[Z^{(1)}_1 = 1] - \Pr[\mathcal{E}Z^{(1)}(\varepsilon/(2\ell + 1))] \right| = \left| \Pr[\mathcal{H}_1(\varepsilon/(2\ell + 1)) = 1] - \Pr[\mathcal{H}_0(\varepsilon/(2\ell + 1))] \right| > \varepsilon/(2\ell + 1),
\]

which contradicts the context-security of LOT.

**Case \(k = 2i\):** For this case we get a contradiction via a routine application of simulation security of the garbling scheme. In more detail, in hybrid \(H_{2i-1}\) there is only one set of input labels at node \(\nu_i\) which \(Z_2\) can obtain. Consequently, we can apply security of the garbling scheme in a hybrid fashion, i.e. once for each call to the oracle and the contradiction follows.

**Case \(k = 2i + 1\):** In this case we show that this leads to a contradiction against the context-security of LOT. We proceed as in the case \(k = 1\). More specifically, to define hybrid \(H_{2i+1}\) we have rephrased \(H_{2i}\) as a context \(Z^{(i)}_1 = (Z^{(i)}_1, Z^{(i)}_2)\) for LOT. By the way we have constructed \(H_{2i+1}\) it holds that the output of \(H_{2i+1}\) is identically distributed to \(\mathcal{E}Z^{(i)}\). Consequently, it holds
that

\[
| \Pr[Z_1^{(i)} = 1] - \Pr[\mathcal{E}Z^{(i)}(\varepsilon/(2\ell + 1)) = 1] = \\
| \Pr[H_2(I)(\varepsilon/(2\ell + 1)) = 1] - \Pr[H_{2i-1}(\varepsilon/(2\ell + 1))] > \\
\varepsilon/(2\ell + 1),
\]

which contradicts the context-security of LOT. This concludes the proof.

Acknowledgment

The second author is supported in part from DARPA/ARL SAFESWITCH Award W911NF15C0210, AFOSR Award FA9550-15-1-0274, AFOSR Award FA9550-19-1-0200, AFOSR YIP Award, NSF CNS Award 1936826, DARPA and SPAWAR under contract N66001-15-C-4065, a Hellman Award and research grants by the Okawa Foundation, Visa Inc., and Center for Long-Term Cybersecurity (CLTC, UC Berkeley). The views expressed are those of the author and do not reflect the official policy or position of the funding agencies.

The third author is supported in part by a gift from Ripple, a gift from DoS Networks, a grant from DARPA/ARL SAFEWARE Award N66001-15-C-4065, a Hellman Award and research grants by the Okawa Foundation, Visa Inc., and Center for Long-Term Cybersecurity (CLTC, UC Berkeley). The views expressed are those of the author and do not reflect the official policy or position of the funding agencies.

The third author is supported in part by a gift from Northrop Grumman, a Cylab seed funding award, and a JP Morgan Faculty Fellowship.

Part of the work was done when the fourth author was at Carnegie Mellon University.

References


