Improved Private Set Intersection Against Malicious Adversaries

Peter Rindal(✉) and Mike Rosulek

Oregon State University, Corvallis, USA
{rindalp,rosulekm}@eecs.oregonstate.edu

Abstract. Private set intersection (PSI) refers to a special case of secure two-party computation in which the parties each have a set of items and compute the intersection of these sets without revealing any additional information. In this paper we present improvements to practical PSI providing security in the presence of *malicious* adversaries.

Our starting point is the protocol of Dong, Chen & Wen (CCS 2013) that is based on Bloom filters. We identify a bug in their malicious-secure variant and show how to fix it using a cut-and-choose approach that has low overhead while simultaneously avoiding one the main computational bottleneck in their original protocol. We also point out some subtleties that arise when using Bloom filters in malicious-secure cryptographic protocols.

We have implemented our PSI protocols and report on its performance. Our improvements reduce the cost of Dong et al.'s protocol by a factor of $14 - 110\times$ on a single thread. When compared to the previous fastest protocol of De Cristofaro et al., we improve the running time by $8 - 24\times$. For instance, our protocol has an online time of 14 s and an overall time of 2.1 min to securely compute the intersection of two sets of 1 million items each.

1 Introduction

Private set intersection (PSI) is a cryptographic primitive that allows two parties holding sets X and Y, respectively, to learn the intersection $X \cap Y$ while not revealing any additional information about X and Y.

PSI has a wide range of applications: contact discovery [19], secret handshakes [12], measuring advertisement conversion rates, and securely sharing security incident information [22], to name a few.

There has been a great deal of recent progress in efficient PSI protocols that are secure against *semi-honest* adversaries, who are assumed to follow the protocol. The current state of the art has culminated in extremely fast PSI protocols. The fastest one, due to Kolesnikov et al. [16], can securely compute the intersection of two sets, each with 2^{20} items, in less than 4 s.

P. Rindal—Partially supported by NSF awards 1149647, 1617197 and a Google Research Award. The first author is also supported by an ARCS foundation fellowship.

J.-S. Coron and J.B. Nielsen (Eds.): EUROCRYPT 2017, Part I, LNCS 10210, pp. 235–259, 2017.
DOI: 10.1007/978-3-319-56620-7_9

Looking more closely, the most efficient semi-honest protocols are those that are based on **oblivious transfer (OT) extension.** Oblivious transfer is a fundamental cryptographic primitive (see Fig. 1). While in general OT requires expensive public-key computations, the idea of OT extension [3,13] allows the parties to efficiently realize any number of *effective* OTs by using only a small number (e.g., 128) of *base OTs* plus some much more efficient symmetric-key computations. Using OT extension, oblivious transfers become extremely inexpensive in practice. Pinkas et al. [23] compared many paradigms for PSI and found the ones based on OTs are much more efficient than those based on algebraic & public-key techniques.

Our Contributions. In many settings, security against semi-honest adversaries is insufficient. *Our goal in this paper is to translate the recent success in semi-honest PSI to the setting of* ***malicious security.*** Following the discussion above, this means focusing on PSI techniques based on oblivious transfers. Indeed, recent protocols for OT extension against *malicious* adversaries [1,15] are almost as efficient as (only a few percent more expensive than) OT extension for semi-honest adversaries.

Our starting point is the protocol paradigm of Dong et al. [8] (hereafter denoted DCW) that is based on OTs and Bloom filter encodings. We describe their approach in more detail in Sect. 3. In their work they describe one of the few malicious-secure PSI protocols based primarily on OTs rather than algebraic public-key techniques. We present the following improvements and additions to their protocol:

1. Most importantly, we show that their protocol has a subtle security flaw, which allows a malicious sender to induce inconsistent outputs for the receiver. We present a fix for this flaw, using a very lightweight cut-and-choose technique.
2. We present a full simulation-based security proof for the Bloom-filter-based PSI paradigm. In doing so, we identify a subtle but important aspect about using Bloom filters in a protocol meant to provide security in the presence of malicious adversaries. Namely, the simulator must be able to extract all items stored in an adversarially constructed Bloom filter. We argue that this capability is an *inherently* non-standard model assumption, in the sense that it seems to require the Bloom filter hash functions to be modeled as (non-programmable) random oracles. Details are in Sect. 5.1.
3. We implement both the original DCW protocol and our improved version. We find that the major bottleneck in the original DCW protocol is not in the cryptographic operations, but actually in a polynomial interpolation computation. The absence of polynomial interpolation in our new protocol (along with our other improvements) decreases the running time by a factor of over $8 - 75\times$.

1.1 Related Work

As mentioned above, our work builds heavily on the protocol paradigm of Dong et al. [8] that uses Bloom filters and OTs. We discuss this protocol in great detail in Sect. 3. We identify a significant bug in that result, which was independently discovered by Lambæk [17] (along with other problems not relevant to our work).

Several other paradigms for PSI have been proposed. Currently the fastest protocols in the *semi-honest* setting are those in a sequence of works initiated by Pinkas et al. [16,22,23] that rely heavily on oblivious transfers. Adapting these protocols to the malicious setting is highly non-trivial, and we were unsuccessful in doing so. However, Lambæk [17] observes that the protocols can easily be made secure against a malicious *receiver* (but not also against a malicious sender).

Here we list other protocol paradigms that allow for malicious security when possible. The earliest technique for PSI is the elegant Diffie-Hellman-based protocol of [12]. Protocols in this paradigm achieving security against malicious adversaries include the one of De Cristofaro et al. [7]. We provide a performance analysis comparing their protocol to ours.

Freedman et al. [9] describe a PSI paradigm based on oblivious polynomial evaluation, which was extended to the malicious setting in [6].

Huang et al. [11] explored using general-purpose 2PC techniques (e.g., garbled circuits) for PSI. Several improvements to this paradigm were suggested in [22]. Malicious security can be achieved in this paradigm in a generic way, using any cut-and-choose approach, e.g., [18].

Kamara et al. [14] presented PSI protocols that take advantage of a semi-trusted server to achieve extremely high performance. Our work focuses on the more traditional setting with just 2 parties.

2 Preliminaries

We use κ to denote a computational security parameter (e.g., $\kappa = 128$ in our implementations), and λ to denote a statistical security parameter (e.g., $\lambda = 40$ in our implementations). We use $[n]$ to denote the set $\{1, \ldots, n\}$.

2.1 Efficient Oblivious Transfer

Our protocol makes use of 1-out-of-2 oblivious transfer (OT). The ideal functionality is described in Fig. 1. We require a large number of such OTs, secure against malicious adversaries. These can be obtained efficiently via OT extension [3]. The idea is to perform a fixed number (e.g., 128) of "base OTs", and from this correlated randomness derive a large number of effective OTs using only symmetric-key primitives.

The most efficient OT extension protocols providing malicious security are those of [2,15,21], which are based on the semi-honest secure paradigm of [13].

Parameters: ℓ is the length of the OT strings.

- Oninput(m_0,m_1) $\in (\{0,1\}^\ell)^2$ from the sender and $b \in \{0,1\}$ from the receiver, give output m_b to the receiver.

Fig. 1. Ideal functionality for 1-out-of-2 OT

2.2 Private Set Intersection

In Fig. 2 we give the ideal functionality that specifies the goal of private set intersection. We point out several facts of interest. (1) The functionality gives output only to Bob. (2) The functionality allows corrupt parties to provide larger input sets than the honest parties. This reflects that our protocol is unable to strictly enforce the size of an adversary's set to be the same as that of the honest party. We elaborate when discussing the security of the protocol.

We define security of a PSI protocol using the standard paradigm of 2PC. In particular, our protocol is secure in the *universal composability (UC)* framework of Canetti [4]. Security is defined using the real/ideal, simulation-based paradigm that considers two interactions:

- In the **real interaction**, a malicious adversary $\mathcal{A}$ attacks an honest party who is running the protocol π. The honest party's inputs are chosen by an *environment* $\mathcal{Z}$; the honest party also sends its final protocol output to $\mathcal{Z}$. The environment also interacts arbitrarily with the adversary. Our protocols are in a *hybrid* world, in which the protocol participants have access to an ideal random-OT functionality (Fig. 1). We define $\text{REAL}[\pi, \mathcal{Z}, \mathcal{A}]$ to be the (random variable) output of $\mathcal{Z}$ in this interaction.
- In the **ideal interaction**, a malicious adversary $\mathcal{S}$ and an honest party simply interact with the ideal functionality $\mathcal{F}$ (in our case, the ideal PSI protocol of Fig. 2). The honest party simply forwards its input from the environment to $\mathcal{F}$ and its output from $\mathcal{F}$ to the environment. We define $\text{IDEAL}[\mathcal{F}, \mathcal{Z}, \mathcal{S}]$ to be the output of $\mathcal{Z}$ in this interaction.

We say that a protocol π **UC-securely realizes** functionality $\mathcal{F}$ if: for all PPT adversaries $\mathcal{A}$, there exists a PPT simulator $\mathcal{S}$, such that for all PPT environments $\mathcal{Z}$:

Parameters: σ is the bit-length of the parties' items. n is the size of the honest parties' sets. $n' > n$ is the allowed size of the corrupt party's set.

- On input $Y \subseteq \{0,1\}^\sigma$ from Bob, ensure that $|Y| \leq n$ if Bob is honest, and that $|Y| \leq n'$ if Bob is corrupt. Give output BOB-INPUT to Alice.
- Thereafter, on input $X \subseteq \{0,1\}^\sigma$ from Alice, likewise ensure that $|X| \leq n$ if Alice is honest, and that $|X| \leq n'$ if Alice is corrupt. Give output $X \cap Y$ to Bob.

Fig. 2. Ideal functionality for private set intersection (with one-sided output)

$$\text{REAL}[\pi, \mathcal{Z}, \mathcal{A}] \approx \text{IDEAL}[\mathcal{F}, \mathcal{Z}, \mathcal{S}]$$

where "≈" denotes computational indistinguishability.

Our protocol uses a (non-programmable) random oracle. In Sect. 5.4 we discuss technicalities that arise when modeling such global objects in the UC framework.

2.3 Bloom Filters

A **Bloom filter (BF)** is an N-bit array B associated with k random functions $h_1, \ldots, h_k : \{0,1\}^* \to [N]$. To store an item x in the Bloom filter, one sets $B[h_i(x)] = 1$ for all i. To check the presence of an item x in the Bloom filter, one simply checks whether $B[h_i(x)] = 1$ for all i. Any item stored in the Bloom filter will therefore be detected when queried; however, *false positives* are possible.

3 The DCW Protocol Paradigm

The PSI protocol of Dong et al. [8] (hereafter DCW) is based on representing the parties' input sets as Bloom filters (BFs). We describe the details of their protocol in this section.

If B and B' are BFs for two sets S and S', using the same parameters (including the same random functions), then it is true that $B \wedge B'$ (bit-wise AND) is a BF for $S \cap S'$. However, one cannot construct a PSI protocol simply by computing a bit-wise AND of Bloom filters. The reason is that $B \wedge B'$ leaks more about S and S' than their intersection $S \cap S'$. For example, consider the case where $S \cap S' = \emptyset$. Then the most natural Bloom filter for $S \cap S'$ is an all-zeroes string, and yet $B \wedge B'$ may contain a few 1 s with noticeable probability. The location of these 1 s depends on the items in S and S', and hence cannot be simulated just by knowing that $S \cap S' = \emptyset$.

DCW proposed a variant Bloom filter that they call a **garbled Bloom filter** (GBF). In a GBF G meant to store m-bit strings, each $G[i]$ is itself an m-bit string rather than a single bit. Then an item x is stored in G by ensuring that $x = \bigoplus_i G[h_i(x)]$. That is, the positions indexed by hashing x should store additive secret shares of x. All other positions in G are chosen uniformly.

The **semi-honest** PSI protocol of DCW uses GBFs in the following way. The two parties agree on Bloom filter parameters. Alice prepares a GBF G representing her input set. The receiver Bob prepares a standard BF B representing his input set. For each position i in the Bloom filters, the parties use oblivious transfer so that Bob can learn $G[i]$ (a string) iff $B[i] = 1$. These are exactly the positions of G that Bob needs to probe in order to determine which of his inputs is stored in G. Hence Bob can learn the intersection. DCW prove that this protocol is secure. That is, they show that Bob's view $\{G[i] \mid B[i] = 1\}$ can be simulated given only the intersection of Alice and Bob's sets.

DCW also describe a **malicious-secure** variant of their GBF-based protocol. The main challenge is that nothing in the semi-honest protocol prevents a malicious Bob from learning *all* of Alice's GBF G. This would reveal Alice's

entire input, which can only be simulated in the ideal world by Bob sending the entire universe $\{0,1\}^\sigma$ as input. Since in general the universe is exponentially large, this behavior is unsimulatable and hence constitutes an attack.

To prevent this, DCW propose to use 1-out-of-2 OTs in the following way. Bob can choose to either pick up a position $G[i]$ in Alice's GBF (if Bob has a 1 in $B[i]$) or else learn a value s_i (if Bob has a 0 in $B[i]$). The values s_i are an $N/2$-out-of-N secret sharing of some secret s^* which is used to encrypt all of the $G[i]$ values. Hence, Alice's inputs to the ith OT are $(s_i, \mathsf{Enc}(s^*, G[i]))$, where Enc is a suitable encryption scheme. Intuitively, if Bob tries to obtain too many positions of Alice's GBF (more than half), then he cannot recover the key s^* used to decrypt them.

As long as $N > 2k|Y|$ (where Y is Bob's input set), an honest Bob is guaranteed to have at least half of his BF bits set to zero. Hence, he can reconstruct s^* from the s_i shares, decrypt the $G[i]$ values, and probe these GBF positions to learn the intersection. We describe the protocol formally in Fig. 3.

Parameters: X is Alice's input, Y is Bob's input. N is the required Bloom filter size; We assume the parties have agreed on common BF parameters.

1. Alice chooses a random key $s^* \in \{0,1\}^\kappa$ and generates an $N/2$-out-of-N secret sharing $(s_1, \ldots, s_N)$.
2. Alice generates a GBF G encoding her inputs X. Bob generates a standard BF B encoding his inputs Y.
3. For $i \in [N]$, the parties invoke an instance of 1-out-of-2 OT, where Alice gives inputs $(s_i, c_i = \mathsf{Enc}(s^*, G[i]))$ and Bob uses choice bit $B[i]$.
4. Bob reconstructs s^* from the set of shares $\{s_i \mid B[i] = 0\}$ he obtained in the previous step. Then he uses s^* to decrypt the ciphertexts $\{c_i \mid B[i] = 1\}$, obtaining $\{G[i] \mid B[i] = 1\}$. Finally, he outputs $\{y \in Y \mid y = \bigoplus_i G[h_i(y)]\}$.

Fig. 3. The malicious-secure protocol of DCW [8].

3.1 Insecurity of the DCW Protocol

Unfortunately, the malicious-secure variant of DCW is not secure[1]! We now describe an a attack on their protocol, which was independently & concurrently discovered by Lambæk [17]. A corrupt Alice will generate s_i values that are *not* a valid $N/2$-out-of-N secret sharing. DCW do not specify Bob's behavior when obtaining invalid shares. However, we argue that no matter what Bob's behavior is (e.g., to abort in this case), Alice can violate the security requirement.

As a concrete attack, let Alice honestly generate shares s_i of s^*, but then change the value of s_1 in any way. She otherwise runs the protocol as instructed.

[1] We contacted the authors of [8], who confirmed that our attack violates malicious security.

If the first bit of Bob's Bloom filter is 1, then this deviation from the protocol is invisible to him, and Alice's behavior is indistinguishable from honest behavior. Otherwise, Bob will pick up s_1 which is not a valid share. If Bob aborts in this case, then his abort probability depends on whether his first BF bit is 1. The effect of this attack on Bob's output cannot be simulated in the ideal PSI functionality, so it represents a violation of security.

Even if we modify Bob's behavior to gracefully handle some limited number of invalid shares, there must be some threshold of invalid shares above which Bob (information theoretically) cannot recover the secret s^*. Whether or not Bob recovers s^* therefore depends on *individual bits* of his Bloom filter. And whether we make Bob abort or do something else (like output $\emptyset$) in the case of invalid shares, the result cannot be simulated in the ideal world. Lambæk [17] points out further attacks, in which Alice can cleverly craft shares and encryptions of GBF values to cause her effective input to depend on Bob's inputs (hence violating input independence).

4 Our Protocol

The spirit of DCW's malicious protocol is to restrict the adversary from setting too many 1 s in its Bloom filter, thereby learning too many positions in Alice's GBF. In this section, we show how to achieve the spirit of the DCW protocol using a lightweight cut-and-choose approach.

The high-level idea is to generate slightly more 1-out-of-2 OTs than the number of BF bits needed. Bob is supposed to use a limited number of 1 s for his choice bits. To check this, Alice picks a small random fraction of the OTs and asks Bob to prove that an appropriate number of them used choice bit 0. If Alice uses *random* strings as her choice-bit-0 messages, then Bob can prove his choice bit by simply reporting this string.[2] If Bob cannot prove that he used sufficiently many 0 s as choice bits, then Alice aborts. Otherwise, Alice has high certainty that the unopened OTs contain a limited number of choice bits 1.

After this cut-and-choose, Bob can choose a permutation that reorders the unopened OTs into his desired BF. In other words, if $c_1, \ldots, c_N$ are Bob's choice bits in the unopened OTs, Bob sends a random π such that $c_{\pi(1)}, \ldots, c_{\pi(N)}$ are the bits of his desired BF. Then Alice can send her GBF, masked by the choice-bit-1 OT messages permuted in this way.

We discuss the required parameters for the cut-and-choose below. However, we remark that the overhead is minimal. It increases the number of required OTs by only 1–10%.

4.1 Additional Optimizations

Starting from the basic outline just described, we also include several important optimizations. The complete protocol is described formally in Fig. 4.

[2] This *committing* property of an OT choice bit was pointed out by Rivest [24].

Parameters: X is Alice's input, Y is Bob's input. N_{bf} is the required Bloom filter size; k is the number of Bloom filter hash functions; N_{ot} is the number of OTs to generate. H is modeled as a random oracle with output length κ. The choice of these parameters, as well as others $\alpha, p_{\mathsf{chk}}, N_{\mathsf{maxones}}$, is described in Section 5.2.

1. **[setup]** The parties perform a secure coin-tossing subprotocol to choose (seeds for) random Bloom filter hash functions $h_1, \ldots, h_k : \{0,1\}^* \to [N_{\mathsf{bf}}]$.
2. **[random OTs]** Bob chooses a random string $b = b_1 \ldots b_{N_{\mathsf{ot}}}$ with an α fraction of 1s. Parties perform N_{ot} OTs of random messages (of length κ), with Alice choosing random strings $m_{i,0}, m_{i,1}$ in the ith instance. Bob uses choice bit b_i and learns $m_i^* = m_{i,b_i}$.
3. **[cut-and-choose challenge]** Alice chooses a set $C \subseteq [N_{\mathsf{ot}}]$ by choosing each index with independent probability p_{chk}. She sends C to Bob. Bob aborts if $|C| > N_{\mathsf{ot}} - N_{\mathsf{bf}}$.
4. **[cut-and-choose response]** Bob computes the set $R = \{i \in C \mid b_i = 0\}$ and sends R to Alice. To prove that he used choice bit 0 in the OTs indexed by R, Bob computes $r^* = \bigoplus_{i \in R} m_i^*$ and sends it to Alice. Alice aborts if $|C| - |R| > N_{\mathsf{maxones}}$ or if $r^* \neq \bigoplus_{i \in R} m_{i,0}$.
5. **[permute unopened OTs]** Bob generates a Bloom filter BF containing his items Y. He chooses a random injective function $\pi : [N_{\mathsf{bf}}] \to ([N_{\mathsf{ot}}] \setminus C)$ such that $BF[i] = b_{\pi(i)}$, and sends π to Alice.
6. **[randomized GBF]** For each item x in Alice's input set, she computes a summary value
$$K_x = H\left(x \,\middle\|\, \bigoplus_{i \in h_*(x)} m_{\pi(i),1}\right),$$
where $h_*(x) \stackrel{\text{def}}{=} \{h_i(x) : i \in [k]\}$. She sends a random permutation of $K = \{K_x \mid x \in X\}$.
7. **[output]** Bob outputs $\{y \in Y \mid H(y \,\|\, \bigoplus_{i \in h_*(y)} m^*_{\pi(i)}) \in K\}$.

Fig. 4. Malicious-secure PSI protocol based on garbled Bloom filters.

Random GBF. In their treatment of the *semi-honest* DCW protocol, Pinkas et al. [23] suggested an optimization that eliminates the need for Alice to send her entire masked GBF. Suppose the parties use 1-out-of-2 OT of *random* messages (i.e., the sender Alice does not choose the OT messages; instead, they are chosen randomly by the protocol/ideal functionality). In this case, the concrete cost of OT extension is greatly reduced (cf. [1]). Rather than generating a GBF of her inputs, Alice generates an array G where $G[i]$ is the random OT message in the ith OT corresponding to bit 1 (an honest Bob learns $G[i]$ iff the ith bit of his Bloom filter is 1).

Rather than arranging for $\bigoplus_i G[h_i(x)] = x$, as in a garbled BF, the idea is to let the G-values be random and have Alice directly send to Bob a **summary value** $K_x = \bigoplus_i G[h_i(x)]$ for each of her elements x. For each item y in Bob's input set, he can likewise compute K_y since he learned the values of G corre-

sponding to 1 s in his Bloom filter. Bob can check to see whether K_y is in the list of strings sent by Alice. For items x not stored in Bob's Bloom filter, the value K_x is random from his point of view.

Pinkas et al. show that this optimization significantly reduces the cost, since most OT extension protocols require less communication for OT of random messages. In particular, Alice's main communication now depends on the number of items in her set rather than the size of the GBF encoding her set. Although the optimization was suggested for the semi-honest variant of DCW, we point out that it also applies to the malicious variant of DCW and to our cut-and-choose protocol.

In the malicious-secure DCW protocol, the idea is to prevent Bob from seeing GBF entries unless he has enough shares to recover the key s^*. To achieve the same effect with a random-GBF, we let the choice-bit-1 OT messages be random (choice-bit-0 messages still need to be chosen messages: secret shares of s^*). These choice-bit-1 OT messages define a random GBF G for Alice. Then instead of sending a summary value $\bigoplus_i G[h_i(x)]$ for each x, Alice sends $[\bigoplus_i G[h_i(x)]] \oplus F(s^*, x)$, where F is a pseudorandom function. If Bob does not use choice-bit-0 enough, he does not learn s^* and all of these messages from Alice are pseudorandom.

In our protocol, we can let both OT messages be random, which significantly reduces the concrete overhead. The choice-bit-0 messages are used when Bob proves his choice bit in the cut-and-choose step. The choice-bit-1 messages are used as a random GBF G, and Alice sends summary values just as in the semi-honest variant.

We also point out that Pinkas et al. and DCW overlook a subtlety in how the summary values and the GBF should be constructed. Pinkas et al. specify the summary value as $\bigoplus_i G[h_i(x)]$ where h_i are the BF hash functions. Suppose that there is a collision involving two BF hash functions under the same x — that is, $h_i(x) = h_{i'}(x)$. Note that since the range of the BF hash functions is polynomial in size ($[N_{\mathsf{bf}}]$), such a collision is indeed possible with noticeable probability. When such a collision happens, the term $G[h_i(x)] = G[h_{i'}(x)]$ can cancel itself out from the XOR summation and the summary value will not depend on this term. The DCW protocol also has an analogous issue.[3] If the $G[h_i(x)]$ term was the only term unknown to the Bob, then the collision allows him to guess the summary value for an item x that he does not have. We fix this by computing the summary value using an XOR expression that eliminates the problem of colliding terms:

$$\bigoplus_{j \in h_*(x)} G[j], \qquad \text{where } h_*(x) \stackrel{\text{def}}{=} \{h_i(x) : i \in [k]\}.$$

Note that in the event of a collision among BF hash functions, we get $|h_*(x)| < k$.

[3] Additionally, if one strictly follows the DCW pseudocode then correctness may be violated in the event of a collision $h_i(x) = h_{i'}(x)$. If $h_i(x)$ is the first "free" GBF location then $G[h_i(x)]$ gets set to a value and then erroneously overwritten later.

Finally, for technical reasons, it turns out to be convenient in our protocol to define the summary value of x to be $H(x \| \bigoplus_{j \in h_*(x)} G[j])$ where H is a (non-programmable) random oracle.[4]

Hash Only "On Demand." In OT-extension for random messages, the parties compute the protocol outputs by taking a hash of certain values derived from the base OTs. Apart from the base OTs (whose cost is constant), these hashes account for essentially all the cryptographic operations in our protocol. We therefore modify our implementation of OT extension so that these hashes are not performed until the values are needed. In our protocol, only a small number (e.g., 1%) of the choice-bit-0 OT messages are ever used (for the cut-and-choose check), and only about half of the choice-bit-1 OT messages are needed by the sender (only the positions that would be 1 in a BF for the sender's input). Hence, the reduction in cost for the receiver is roughly 50%, and the reduction for the sender is roughly 75%. A similar optimization was also suggested by Pinkas et al. [23], since the choice-bit 0 messages are not used at all in the semi-honest protocol.

Aggregating Proofs-of-Choice-Bits. Finally, we can reduce the communication cost of the cut-and-choose step. Recall that Bob must prove that he used choice bit 0 in a sufficient number of OTs. For the ith OT, Bob can simply send $m_{i,0}$, the random output he received from the ith OT. To prove he used choice bit 0 for an entire *set* I of indices, Bob can simply send the single value $\bigoplus_{i \in I} m_{i,0}$, rather than sending each term individually.

Optimization for Programmable Random Oracles. The formal description of our protocol is one that is secure in the *non-programmable* random oracle model. However, the protocol can be significantly optimized by assuming a programmable random oracle. The observation is that Alice's OT input strings are always chosen randomly. Modern OT extension protocols natively give OT of random strings and achieve OT of chosen strings by sending extra correction data (cf. [1]). If the application allows the OT extension protocol itself to determine the sender's strings, then this additional communication can be eliminated. In practice, this reduces communication cost for OTs by a factor of 2.

We can model OT of random strings by modifying the ideal functionality of Fig. 1 to choose m_0, m_1 randomly itself. The OT extension protocol of [21] securely realizes this functionality in the presence of malicious adversaries, in the programmable random oracle model. We point out that even in the semi-honest model it is not known how to efficiently realize OT of strings randomly *chosen by the functionality*, without assuming a programmable random oracle.

[4] In practice H is instantiated with a SHA-family hash function. The XOR expression and x itself are each 128 bits, so both fit in a single SHA block.

5 Security

5.1 BF Extraction

The analysis in DCW argues for malicious security in a property-based manner, but does not use a standard simulation-based notion of security. This turns out to mask a non-trivial subtlety about how one can prove security about Bloom-filter-based protocols.

One important role of a simulator is to extract a corrupt party's input. Consider the case of simulating the effect of a corrupt Bob. In the OT-hybrid model the simulator sees Bob's OT choice bits as well as the permutation π that he sends in 5. Hence, the simulator can easily extract Bob's "effective" Bloom filter. However, the simulator actually needs to extract the receiver's *input set* that corresponds to that Bloom filter, so that it can send the set itself to the ideal functionality.

In short, the simulator must *invert* the Bloom filter. While invertible Bloom filters do exist [10], they require storing a significant amount of data beyond that of a standard Bloom filter. Yet this PSI protocol only allows the simulator to extract the receiver's OT choice bits, which corresponds to a *plain* Bloom filter. Besides that, in our setting we must invert a Bloom filter that may not have been honestly generated.

Our protocol achieves extraction by modeling the Bloom filter hash functions as (non-programmable) random oracles. The simulator must *observe* the adversary's queries to the Bloom filter hash functions.[5] Let Q be the set of queries made by the adversary to any such hash function. This set has polynomial size, so the simulator can probe the extracted Bloom filter to test each $q \in Q$ for membership. The simulator can take the appropriate subset of Q as the adversary's extracted input set. More details are given in the security proof below.

Simulation/extraction of a corrupt Alice is also facilitated by observing her oracle queries. Recall that the *summary value* of x is (supposed to be) $H(x \| \bigoplus_{j \in h_*(x)} m_{\pi(j),1})$. Since H is a non-programmable random oracle, the simulator can obtain candidate x values from her calls to H.

More details about malicious Bloom filter extraction are given in the security proof in Sect. 5.3.

Necessity of Random Oracles. We show that random oracles are necessary, when using plain Bloom filters for a PSI protocol.

Lemma 1. *There is* ***no*** *PSI protocol that simultaneously satisfies the following conditions:*

- *The protocol is UC secure against malicious adversaries in the standard model.*
- *When Bob is corrupted in a semi-honest manner, the view of the simulator can be sampled given only on a Bloom filter representation of Bob's input.*
- *The parameters of the Bloom filter depend only on the number of items in the parties' sets, and in particular not on the bitlength of those items.*

[5] The simulator does not, however, require the ability to *program* the random oracle.

In our protocol, the simulator's indeed gets to see the receiver's OT choice bits, which correspond to a plain Bloom filter encoding of their input set. However, the simulator also gets to observe the receiver's random oracle queries, and hence the statement of the lemma does not apply.

The restriction about the Bloom filter parameters is natural. One important benefit of Bloom filters is that they do not depend on the bit-length of the items being stored.

Proof. Consider an environment that chooses a random set $S \subseteq \{0,1\}^\ell$ of size n, and gives it as input to both parties (ℓ will be chosen later). An adversary corrupts Bob but runs semi-honestly on input S as instructed. The environment outputs 1 if the output of the protocol is S (note that it does not matter if only one party receives output). In this real execution, the environment outputs 1 with overwhelming probability due to the correctness of the protocol.

We will show that if the protocol satisfies all three conditions in the lemma statement, then the environment will output 0 with constant probability in the ideal execution, and hence the protocol will be insecure.

Suppose the simulator for a corrupt Bob sees only a Bloom filter representation of Bob's inputs. Let N be the total length of the Bloom filter representation (the Bloom filter array itself as well as the description of hash functions). Set the length of the input items $\ell > 2N$. Now the simulator's view can be sampled given only N bits of information about S, whereas S contains randomly chosen items of length $\ell > 2N$. The simulator must extract a value S' and send it on behalf of Bob to the ideal functionality. With constant probability this S' will fail to include some item of S (it will likely not include any of them). Then since the honest party gave input S, the output of the functionality will be $S \cap S' \neq S$, and the environment outputs zero.

5.2 Cut-and-Choose Parameters

The protocol mentions various parameters:

N_{ot}: the number of OTs
N_{bf}: the number of Bloom filter bits
k: the number of Bloom filter hash functions
α: the fraction of 1 s among Bob's choice bits
p_{chk}: the fraction of OTs to check
N_{maxones}: the maximum number of 1 choice bits allowed to pass the cut-and-choose.

As before, we let κ denote the computational security parameter and λ denote the statistical security parameter.

We require the parameters to be chosen subject to the following constraints:

- *The cut-and-choose restricts Bob to few 1s.* Let N_1 denote the number of OTs that remain after the cut and choose, in which Bob used choice bit 1. In the security proof we argue that the difficulty of finding an element stored in the

Bloom filter *after the fact* is $(N_1/N)^k$ (i.e., one must find a value which all k random Bloom filter hash functions map to a 1 in the BF).
Let $\mathcal{B}$ denote the "bad event" that no more than N_{maxones} of the checked OTs used choice bit one (so Bob can pass the cut-and-choose), and yet $(N_1/N_{\mathsf{bf}})^k \geq 2^{-\kappa}$. We require $\Pr[\mathcal{B}] \leq 2^{-\lambda}$.
As mentioned above, the spirit of the protocol is to restrict a corrupt receiver from setting too many 1 s in its (plain) Bloom filter. DCW suggest to restrict the receiver to 50% 1s, but do not explore how the fraction of 1 s affects security (except to point out that 100% 1s is problematic). Our analysis pinpoints precisely how the fraction of 1 s affects security.

– *The cut-and-choose leaves enough OTs unopened for the Bloom filter.* That is, when choosing from among N_{ot} items, each with independent p_{chk} probability, the probability that less than N_{bf} remain unchosen is at most $2^{-\lambda}$.
– *The honest Bob has enough one choice bits after the cut and choose.* When inserting n items into the bloom filter, at most nk bits will be set to one. We therefore require that no fewer than this remain after the cut and choose.

Our main technique is to apply the Chernoff bound to the probability that Bob has too many 1 s after the cut and choose. Let $m_h^1 = \alpha N_{\mathsf{ot}}$ (resp. $m_h^0 = (1-\alpha)N_{\mathsf{ot}}$) be the number of 1 s (resp. 0s) Bob is supposed to select in the OT extension. Then in expectation, there should be $m_h^1 p_{\mathsf{chk}}$ ones in the cut and choose open set, where each OT message is opened with independent probability p_{chk}. Let ϕ denote the number of ones in the open set. Then applying the Chernoff bound we obtain,

$$\Pr[\phi \geq (1+\delta)m_h^1 p_{\mathsf{chk}}] \leq e^{-\frac{\delta^2}{2+\delta} m_h^1 p_{\mathsf{chk}}} \leq 2^{-\lambda}$$

where the last step bounds this probability to be negligible in the statistical security parameter λ. Solving for δ results in,

$$\delta \leq \frac{\lambda + \sqrt{\lambda^2 + 8\lambda m_h^1 p_{\mathsf{chk}}}}{2m_h^1 p_{\mathsf{chk}}}.$$

Therefore an honest Bob should have no more than $N_{\mathsf{maxones}} = (1+\delta)m_h^1 p_{\mathsf{chk}}$ 1s revealed in the cut and choose, except with negligible probability. To ensure there are at least nk ones[6] remaining to construct the bloom filter, set $m_h^1 = nk + N_{\mathsf{maxones}}$. Similarly, there must be at least N_{bf} unopened OTs which defines the total number of OTs to be $N_{\mathsf{ot}} = N_{\mathsf{bf}} + (1+\delta^*)N_{\mathsf{ot}} p_{\mathsf{chk}}$ where δ^* is analogous to δ except with respect to the total number of OTs opened in the cut and choose.

A malicious Bob can instead select $m_a^1 \geq m_h^1$ ones in the OT extension. In addition to Bob possibly setting more 1 s in the BF, such a strategy will increase the probability of the cut and choose revealing more than N_{maxones} 1s. A Chernoff bound can then be applied to the probability of seeing a δ' factor fewer 1 s than

[6] nk ones is an upper bound on the number of ones required. A tighter analysis could be obtained if collisions were accounted for.

expected. Bounding this to be negligible in the statistical security parameter λ, we obtain,

$$\Pr[\phi \leq (1-\delta')p_{\mathsf{chk}} m_a^1] \leq e^{-\frac{\delta'^2}{2} p_{\mathsf{chk}} m_a^1} \leq 2^{-\lambda}.$$

Solving for δ' then yields $\delta' \leq \sqrt{\frac{2\lambda}{p_{\mathsf{chk}} m_a^1}}$. By setting N_{maxones} equal to $(1-\delta')p_{\mathsf{chk}} m_a^1$ we can solve for m_a^1 such that the intersection of these two distribution is negligible. Therefore the maximum number of 1 s remaining is $N_1 = (1-p_{\mathsf{chk}})m_a^1 + \sqrt{2\lambda p_{\mathsf{chk}} m_a^1}$.

For a given p_{chk}, n, k, the above analysis allows us to bound the maximum advantage a malicious Bob can have. In particularly, a honest Bob will have at least nk 1 s and enough 0 s to construct the bloom filter while a malicious Bob can set no more than N_1/N_{bf} fraction of bits in the bloom filter to 1. Modeling the bloom filter hash function as random functions, the probability that all k index the boom filter one bits is $(N_1/N_{\mathsf{bf}})^k$. Setting this to be negligible in the computational security parameter κ we can solve for N_{bf} given N_1 and k. The overall cost is therefore $\frac{N_{\mathsf{bf}}}{(1-p_{\mathsf{chk}})}$. By iterating over values of k and p_{chk} we obtain set of parameters shown in Fig. 5.

n	p_{chk}	k	N_{ot}	N_{bf}	α	N_{maxones}
2^8	0.099	94	99,372	88,627	0.274	3,182
2^{12}	0.053	94	1,187,141	1,121,959	0.344	22,958
2^{16}	0.024	91	16,992,857	16,579,297	0.360	150,181
2^{20}	0.010	90	260,252,093	257,635,123	0.366	962,092

Fig. 5. Optimal Bloom filter cut and choose parameters for set size n to achieve statistical security $\lambda = 40$ and computational security $\kappa = 128$. N_{ot} denotes the total number of OTs used. N_{bf} denotes the bit count of the bloom filer. α is the faction of ones which should be generated. N_{maxones} is the maximum number of ones in the cut and choose to pass.

5.3 Security Proof

Theorem 2. *The protocol in Fig. 4 is a UC-secure protocol for PSI in the random-OT-hybrid model, when H and the Bloom filter hash functions are non-programmable random oracles, and the other protocol parameters are chosen as described above.*

Proof. We first discuss the case of a corrupt receiver Bob, which is the more difficult case since we must not only extract Bob's input but simulate the output. The simulator behaves as follows:

> The simulator plays the role of an honest Alice and ideal functionalities in steps 1 through 5, but also extracts all of Bob's choice bits b for the OTs. Let N_1 be the number of OTs with choice bit 1 that remain after the cut and choose. The simulator artificially aborts if Bob succeeds at the cut and choose and yet $(N_1/N_{\mathsf{bf}})^k \geq 2^{-\kappa}$. From the choice of parameters, this event happens with probability only $2^{-\lambda}$.

After receiving Bob's permutation π in step 5, the simulator computes Bob's effective Bloom filter $BF[i] = b_{\pi(i)}$. Let Q be the set of queries made by Bob to *any* of the Bloom filter hash functions (random oracles). The simulator computes $\tilde{Y} = \{q \in Q \mid \forall i : BF[h_i(q)] = 1\}$ as Bob's effective input, and sends $\tilde{Y}$ to the ideal functionality. The simulator receives $Z = X \cap \tilde{Y}$ as output, as well as $|X|$. For $z \in Z$, the simulator generates $K_z = H(z \,\|\, \bigoplus_{j \in h_*(z)} m_{\pi(j),1})$. The simulator sends a random permutation of K_z along with $|X| - |Z|$ random strings to simulate Alice's message in step 6.

To show the soundness of this simulation, we proceed in the following sequence of hybrids:

1. The first hybrid is the real world interaction. Here, an honest Alice also queries the random oracles on her actual inputs $x \in X$. For simplicity later on, assume that Alice queries her random oracle as late as possible (in step 6 only).
2. In the next hybrid, we artifically abort in the event that $(N_1/N_{\mathsf{bf}})^k \geq 2^{-\kappa}$. As described above, our choice of parameters ensures that this abort happens with probability at most $2^{-\lambda}$, so the hybrids are indistinguishable.
   In this hybrid, we also observe Bob's OT choice bits. Then in step 5 of the protocol, we compute Q, BF, and $\tilde{Y}$ as in the simulator description above.
3. We next consider a sequence of hybrids, one for each item x of Alice such that $x \in X \setminus \tilde{Y}$. In each hybrid, we replace the summary value $K_x = H(x \,\|\, \bigoplus_{j \in h_*(x)} m_{\pi(j),1})$ with a uniformly random value.
   There are two cases for $x \in X \setminus \tilde{Y}$:
   - Bob queried some h_i on x before step 5: If this happened but x was not included in $\tilde{Y}$, then x is *not* represented in Bob's effective Bloom filter BF. There must be an i such that Bob did not learn $m_{\pi(h_i(x)),1}$.
   - Bob did *not* query any h_i on x: Then the value of $h_i(x)$ is random for all i. The probability that x is present in BF is the probability that $BF[h_i(x)] = 1$ for all i, which is $(N_1/N_{\mathsf{bf}})^k$ since Bob's effective Bloom filter has N_1 ones. Recall that the interaction is already conditioned on the event that $(N_1/N_{\mathsf{bf}})^k < 2^{-\kappa}$. Hence it is with overwhelming probability that Bob did not learn $m_{\pi(h_i(x)),1}$ for some i.

   In either case, there is an i such that Bob did not learn $m_{\pi(h_i(x)),1}$, so that value is random from Bob's view. Then the corresponding sum $\bigoplus_{j \in h_*(x)} m_{\pi(j),1}$ is uniform in Bob's view.[7] It is only with negligible probability that Bob makes the oracle query $K_x = H(x \,\|\, \bigoplus_{j \in h_*(x)} m_{\pi(j),1})$. Hence K_x is pseudorandom and the hybrids are indistinguishable.

In the final hybrid, the simulation does not need to know X, it only needs to know $X \cap \tilde{Y}$. In particular, the values $\{K_x \mid x \in X \setminus \tilde{Y}\}$ are now being

[7] This is part of the proof that breaks down if we compute a summary value using $\bigoplus_i m_{\pi(h_i(x)),1}$ instead of $\bigoplus_{j \in h_*(x)} m_{\pi(j),1}$. In the first expression, it may be that $h_{i'}(x) = h_i(x)$ for some $i' \neq i$ so that the randomizing term $m_{\pi(h_i(x)),1}$ cancels out in the sum.

simulated as random strings. The interaction therefore describes the behavior of our simulator interacting with corrupt Bob.

Now consider a corrupt Alice. The simulation is as follows:

> The simulator plays the role of an honest Bob and ideal functionalities in steps 1 through 4. As such, the simulator knows Alice's OT messages $m_{i,b}$ for all i, b, and can compute the correct r^* value in step 4. The simulator sends a completely random permutation π in step 5.
> In step 6, the simulator obtains a set K as Alice's protocol message. Recall that each call made to random oracle H has the form $q\|s$. The simulator computes $Q = \{q \mid \exists s : \text{Alice queried } H \text{ on } q\|s\}$. The simulator computes $\tilde{X} = \{q \in Q \mid H(q \,\|\, \bigoplus_{j \in h_*(q)} m_{\pi(j),1}) \in K\}$ and sends $\tilde{X}$ to the ideal functionality as Alice's effective input. Recall Alice receives no output.

It is straight-forward to see that Bob's protocol messages in steps 4 & 5 are distributed independently of his input.

Recall that Bob outputs $\{y \in Y \mid H(y \,\|\, \bigoplus_{j \in h_*(y)} m^*_{\pi(j)}) \in K\}$ in the last step of the protocol. In the ideal world (interacting with our simulator), Bob's output from the functionality is $\tilde{X} \cap Y = \{y \in Y \mid y \in \tilde{X}\}$. We will show that the two conditions are the same except with negligible probability. This will complete the proof.

We consider two cases:

- If $y \in \tilde{X}$, then $H(y \,\|\, \bigoplus_{j \in h_*(y)} m^*_{\pi(j)}) = H(y \,\|\, \bigoplus_{j \in h_*(y)} m_{\pi(j),1}) \in K$ by definition.
- If $y \notin \tilde{X}$, then Alice never queried the oracle $H(y\|\cdot)$ before fixing K, hence $H(y \,\|\, \bigoplus_{j \in h_*(y)} m^*_{\pi(j)})$ is a fresh oracle query, distributed independently of K. The output of this query appears in K with probability $|K|/2^\kappa$.

Taking a union bound over $y \in Y$, we have that, except with probability $|K||Y|/2^\kappa$,

$$H(y \,\|\, \bigoplus_{j \in h_*(y)} m^*_{\pi(j)}) \in K \iff y \in \tilde{X}$$

Hence Bob's ideal and real outputs coincide.

Size of the Adversary's Input Set. When Alice is corrupt, the simulator extracts a set $\tilde{X}$. Unless the adversary has found a collision under random oracle H (which is negligibly likely), we have that $|\tilde{X}| \leq |K|$. Thus the protocol enforces a straightforward upper bound on the size of a corrupt Alice's input.

The same is not true for a corrupt Bob. The protocol enforces an upper bound only on the size on Bob's *effective Bloom filter* and a bound on the number of 1 s in that BF. We now translate these bounds to derive a bound on the size of the set extracted by the simulator. Note that the ideal functionality for PSI (Fig. 2) explicitly allows corrupt parties to provide larger input sets than honest parties.

First, observe that only queries made by the adversary before step 5 of the protocol are relevant. Queries made by the adversary *after* do not affect the simulator's extraction. As in the proof, let Q be the set of queries made by Bob

before step 5. Bob is able to construct a BF with at most N_1 ones, and causing the simulator to extract items $\tilde{Y} \subseteq Q$, only if:

$$\left| \bigcup_{y \in \tilde{Y}; i \in [k]} h_i(y) \right| \leq N_1.$$

Then by a union bound over all Bloom filters with N_1 bits set to 1, and all $\tilde{Y} \subseteq Q$ of size $|\tilde{Y}| = n'$, we have:

$$\Pr\begin{bmatrix}\text{simulator extracts}\\ \text{some set of size } n'\end{bmatrix} \leq \binom{|Q|}{n'}\binom{N_{\mathsf{bf}}}{N_1}\left(\frac{N_1}{N_{\mathsf{bf}}}\right)^{kn'}.$$

The security proof already conditions on the event that $(N_1/N_{\mathsf{bf}})^k \leq 2^{-\kappa}$, so we get:

$$\begin{aligned}\Pr\begin{bmatrix}\text{simulator extracts}\\ \text{some set of size } n'\end{bmatrix} &\leq \binom{|Q|}{n'}\binom{N_{\mathsf{bf}}}{N_1}2^{-\kappa n'}\\ &\leq \left(|Q|^{n'}\right)\left(2^{N_{\mathsf{bf}}}\right)2^{-\kappa n'}\end{aligned}$$

To make the probability less than $2^{-\kappa}$ it therefore suffices to have $n' = (\kappa + N_{\mathsf{bf}})/(\kappa - \log|Q|)$.

In our instantiations, we always have $N_{\mathsf{bf}} \leq 3\kappa n$, where n denotes the *intended* size of the parties' sets. Even in the pessimistic case that the adversary makes $|Q| = 2^{\kappa/2}$ queries to the Bloom filter hash functions, we have $n' \approx 6n$. Hence, the adversary is highly unlikely to produce a Bloom filter containing 6 times the intended number of items. We emphasize that this is a very loose bound, but show it just to demonstrate that the simulator indeed extracts from the adversary a modestly sized effective input set.

5.4 Non-Programmable Random Oracles in the UC Model

Our protocol makes significant use of a non-programmable random oracle. In the standard UC framework [4], the random oracle must be treated as *local* to each execution for technical reasons. The UC framework does not deal with global objects like a single random oracle that is used by many protocols/instances. Hence, as currently written, our proof implies security when instantiated with a highly local random oracle.

Canetti et al. [5] proposed a way to model global random oracles in the UC framework (we refer to their model as UC-gRO). One of the main challenges is that (in the plain UC model) the simulator can observe the adversary's oracle queries, but an adversary can ask the environment to query the oracle on its behalf, hidden from the simulator. In the UC model, every functionality and party in the UC model is associated with a *session id* (sid) for the protocol instance in which it participates. The idea behind UC-gRO is as follows:

– There is a functionality gRO that implements an ideal random oracle. Furthermore, this functionality is **global** in the sense that all parties and all functionalities can query it.
– Every oracle query in the system must be prefixed with some sid.
– There is no enforcement that oracle queries are made with the "correct" sid. Rather, if a party queries gRO with a sid that does not match its own, that query is marked as **illegitimate** by gRO.
– A functionality can ask gRO for all of the illegitimate queries made using that functionality's sid.

Our protocol and proof can be modified in the following ways to provide security in the UC-gRO model:

1. In the protocol, all queries to relevant random oracles (Bloom filter functions h_i and outer hash function H) are prefixed with the sid of this instance.
2. The ideal PSI functionality is augmented in a standard way of UC-gRO: When the adversary/simulator gives the functionality a special command `illegitimate`, the functionality requests the list of illegitimate queries from gRO and forwards them to the adversary/simulator.
3. In the proof, whenever the simulator is described as obtaining a list of the adversary's oracle queries, this is done by observing the adversary's queries and also obtaining the illegitimate queries via the new mechanism.

With these modifications, our proof demonstrates security in the UC-gRO model.

6 Performance Evaluation

We implemented our protocol in addition to the protocols of DCW [8] outlined in Sect. 3 and that of DKT [7]. In this section we report on their performance and analyze potential trade offs.

6.1 Implementation and Test Platform

In the offline phase, our protocol consists of performing 128 base OTs using the protocol of [20]. We extend these base OTs to N_{ot} OTs using an optimized implementation of the Keller et al. [15] OT extension protocol. Our implementation uses the programmable-random-oracle optimization for OT of random strings, described in Sect. 4.1. In the multi-threaded case, the OT extension and Base OTs are performed in parallel. Subsequently, the cut and choose seed is published which determines the set of OT messages to be opened. Then one or more threads reports the choice bits used for the corresponding OT and the XOR sum of the messages. The sender validates the reported value and proceeds to the online phase.

The online phase begins with both parties inserting items into a plaintext bloom filter using one or more threads. As described in Sect. 5.1, the BF hash functions should be modeled as (non-programmable) random oracles. We use

SHA1 as a random oracle but then expand it to a suitable length via a fast PRG (AES in counter mode) to obtain:[8]

$$h_1(x)\|h_2(x)\|\cdots\|h_k(x) = \mathsf{PRG}(\mathsf{SHA1}(x)).$$

Hence we use just one (slow) call to SHA to compute all BF hash functions for a single element, which significantly reduces the time for generating Bloom filters. Upon the computing the plaintext bloom filter, the receiver selects a random permutation mapping the random OT choice bits to the desired bloom filter. The permutation is published and the sender responds with the random garbled bloom filter masks which correspond to their inputs. Finally, the receiver performs a plaintext intersection of the masks and outputs the corresponding values.

We evaluated the prototype on a single server with simulated network latency and bandwidth. The server has 2 36-cores Intel(R) Xeon(R) CPU E5-2699 v3 @ 2.30 GHz and 256 GB of RAM (e.i. 36 cores & 128 GB per party). We executed our prototype in two network settings: a LAN configuration with both parties in the same network with 0.2 ms round-trip latency, 1 Gbps; and a WAN configuration with a simulated 95 ms round-trip latency, 60 Mbps. All experiments we performed with a computational security parameter of $\kappa = 128$ and statistical security parameter $\lambda = 40$. The times reported are an average over 10 trials. The variance of the trials was between 0.1%–5.0% in the LAN setting and 0.5%–10% in the WAN setting with a trend of smaller variance as n becomes larger. The CPUs used in the trials had AES-NI instruction set for fast AES computations.

6.2 Parameters

We demonstrate the scalability of our implementation by evaluating a range of set sizes $n \in \{2^8, 2^{12}, 2^{16}, 2^{20}\}$ for strings of length $\sigma = 128$. In all of our tests, we use system parameters specified in Fig. 5. The parameters are computed using the analysis specified in Sect. 5.2. Most importantly they satisfy that except with probability negligible in the computation security parameter κ, a receiver after step 5 of Fig. 4 will not find an x not previously queried which is contained in the garbled bloom filter.

The parameters are additionally optimized to reduce the overall cost of the protocol. In particular, the total number of OTs $N_{\mathsf{ot}} = N_{\mathsf{bf}}/(1 - p_{\mathsf{chk}})$ is minimized. This value is derived by iterating over all the region of $80 \leq k \leq 100$ hash functions and cut-and-choose probabilities $0.001 \leq p_{\mathsf{chk}} \leq 0.1$. For a given value of n, k, p_{chk}, the maximum number of ones N_1 which a possibly malicious receiver can have after the cut and choose is defined as shown in Sect. 5.2. This in turn determines the minimum value of N_{bf} such that $(N_{\mathsf{bf}}/N_1)^{-k} \leq 2^{-\kappa}$ and therefore the overall cost N_{ot}. We note that for κ other than 128, a different range for the number of hash functions should be considered.

[8] Note that if we model SHA1 as having its queries observable to the simulator, then this property is inherited also when expanding the SHA1 output with a PRG.

6.3 Comparison to Other Protocols

For comparison, we implemented two other protocol paradigms, which we describe here:

DCW Protocol. Our first point of comparison is to the protocol of Dong et al. [8], on which ours is based. The protocol is described in Sect. 3. While their protocol has issues with its security, our goal here is to illustrate that our protocol also has significantly better performance.

In [8], the authors implement only their semi-honest protocol variant, not the malicious one. An aspect of the malicious DCW protocol that is easy to overlook is its reliance on an $N/2$-out-of-N secret sharing scheme. When implementing the protocol, it becomes immediately clear that such a secret-sharing scheme is a major computational bottleneck.

Recall that the sender generates shares from such a secret sharing scheme, and the receiver reconstructs such shares. In this protocol, the required N is the number of bits in the Bloom filter. As a concrete example, for PSI of sets of size 2^{20}, the Bloom filter in the DCW protocol has roughly 2^{28} bits. Using Shamir secret sharing, the sender must evaluate a random polynomial of degree $\sim 2^{27}$ on $\sim 2^{28}$ points. The sender must interpolate such a polynomial on $\sim 2^{27}$ points to recover the secret. Note that the polynomial will be over $GF(2^{128})$, since the protocol secret-shares an (AES) encryption key.

We chose not to develop a full implementation of the malicious DCW protocol. Rather, we fully implemented the [garbled] Bloom filter encoding steps and the OTs. We then **simulated** the secret-sharing and reconstruction steps in the following way. We calculated the number of field multiplications that would be required to evaluate a polynomial of the suitable degree by the Fast Fourier Transform (FFT) method, and simply had each party perform the appropriate number of field multiplications in $GF(2^{128})$. The field was instantiated using the NTL library with all available optimizations enabled. Our simulation significantly underestimates the cost of secret sharing in the DCW protocol, since: (1) it doesn't account for the cost associated with virtual memory accesses when computing on such a large polynomial; and (2) evaluating/interpolating the polynomial via FFT reflects a *best-case scenario*, when the points of evaluation are roots of unity. In the protocol, the receiver Bob in particular does not have full control over which points of the polynomial he will learn.

Despite this optimistic simulation of the secret-sharing step, its cost is substantial, accounting for 97% of the execution time. In particular, when comparing our protocol to the DCW protocol, the main difference in the online phase is the secret sharing reconstruction which accounts for a 113× increase in the online running time for $n = 2^{16}$.

We simulated two variants of the DCW malicious-secure protocol. One variant reflects the DCW protocol as written, using OTs of chosen messages. The other variant includes the "random GBF" optimization inspired by [23] and described in Sect. 4. In this variant, one of the two OT messages is set randomly by the protocol itself, and not chosen by the sender. This reduces the online

communication cost of the OTs by roughly half. However, it surprisingly has a slight negative effect on total time. The reason is that during the online phase Alice has more than enough time to construct and send a plain GBF while Bob performs the more time intensive secret-share reconstruction step. For $n = 2^{16}$, the garbled bloom filter takes less than 5% of the secret share reconstruction time to be sent. When using a randomized GBF, Alice sends summary values to Bob, which he must compare to his own summary values. Note that there is a summary value for each item in a party's set (e.g., 2^{20}), so these comparisons involve lookups in some non-trivial data structure. This extra computational effort is part of the the critical path since the Bob has to do it. In summary, the "random GBF" optimization does reduce the required communication, however it also increases the critical path of the protocol due to the secret-share reconstruction hiding the effects of this communication savings and the small additional overhead of performing n lookups.

DH-Based PSI Protocols. Another paradigm for PSI uses public-key techniques and is based on Diffie-Hellman-type assumptions in cyclic groups. The most relevant protocol in this paradigm that achieves malicious security is that of De Cristofaro et al. [7] which we refer to as DKT. While protocols in this paradigm have extremely low communication complexity, they involve a large number of computationally expensive public-key operations (exponentiations). Another potential advantage of the DKT protocol over schemes based on Bloom filters is that the receiver can be restricted to a set size of exactly n items. This is contrasted with our protocol where the receiver can have a set size of $n' \approx 6n$.

We fully implemented the [7] PSI protocol both in the single and multi threaded setting. In this protocol, the parties perform $5n$ exponentiations and $2n$ related zero knowledge proofs of discrete log equality. Following the suggestions in [7], we instantiate the zero knowledge proofs in the RO model with the Fiat-Shamir transform applied to a sigma protocol. The resulting PSI protocol has in total $12n$ exponentiations along with several other less expensive group operations. The implementation is built on the Miracl elliptic curve library using Curve 25519 achieving 128 bit computational security. The implementation also takes advantage of the Comb method to perform a precomputation to increase the speed of exponentiations (point multiplication). Additionally, all operations are performed in a streaming manner allowing for the greatest amount of work to be performed concurrently by the parties.

6.4 Results

The running time of our implementation is shown in Fig. 7. We make the distinction of reporting the running times for both the total time and online phase when applicable. The offline phase contains all operations which are independent of the input sets. For the bloom filter based protocols the offline phase consists of performing the OT extension and the cut and choose. Out of these operations, the most time-consuming is the OT extension. For instance, with $n = 2^{20}$ we require 260 million OTs which requires 124 s; the cut and choose takes only 3 s.

For the smaller set size of $n = 2^{12}$, the OT extension required 461 ms and the cut and choose completed in 419 ms. The relative increase in the cut and choose running time is primarily due to the need to open a larger portion of the OTs when n is smaller.

The online phase consists of the receiver first computing their bloom filter. For set size $n = 2^{20}$, computing the bloom filter takes 6.4 s. The permutation mapping the receiver's OTs to the bloom filter then computed in less than a second and sent. Upon receiving the permutation, the sender computes their PSI summary values and sends them to the receiver. This process when $n = 2^{20}$ takes roughly 6 s. The receiver then outputs the intersection in less than a second.

As expected, our optimized protocol achieves the fastest running times compared to the other malicious secure constructions. When evaluating our implementation with a set size of $n = 2^8$ on a single thread in the LAN setting, we obtain an online running time of 3 ms and an overall time of 0.2 s. The next fastest is that of DH-based DKT protocol which required 1.7 s, an 8.5× slowdown compared to our protocol. For the larger set size of $n = 2^{12}$, our overall running time is 0.9 s with an online phase of just 40 ms. The DKT protocol is again the next fastest requiring 25× longer resulting in a total running time of 22.6 s. The DCW protocol from which ours is derived incurs more than a 60× overhead. For the largest set size performed of $n = 2^{20}$, our protocol achieves an online phase of 14 s and an overall time of 127 s. The DKT protocol overall running time was more than 95 min, a 47× overhead compared to our running time. The DCW protocol took prohibitively long to run but is expected to take more than 100× longer than our optimized protocol.

When evaluating our protocol in the WAN setting with 95 ms round trip latency our protocol again achieves the fastest running times. For the small set size of $n = 2^8$, the protocol takes an overall running time of 0.95 s with the online phase taking 0.1 s. DKT was the next fastest protocol requiring a total time of 1.7 s, an almost 2× slowdown. Both variants of the DCW protocol experience a more significant slowdown of roughly 4×. When increasing the set size, our protocol experiences an even greater relative speedup. For $n = 2^{16}$, our protocol takes 56 s, with 11 of the seconds consisting of the online phase. Comparatively, DKT takes 393 s resulting in our protocol being more than 7× faster. The DCW protocols are even slower requiring more than 19 min, a 20× slowdown. This is primarily due to the need to perform the expensive secret-sharing operations and send more data.

In addition to faster serial performance, our protocol also benefits from easily being parallelized, unlike much of the DCW online phase. Figure 6 shows the running times of our protocol and that of DKT when parallelized using p threads per party in the LAN setting. With $p = 4$ we obtain a speedup of 2.3× for set size $n = 2^{16}$ and 2× speedup for $n = 2^{20}$. However, the DKT protocol benefits from being trivially parallelizable. As such, they enjoy a nearly one-to-one speedup when more threads are used. This combined with the extremely small communication overhead of the DKT protocol could potentially allow their protocol to outperform ours when the network is quite slow and the parties have many threads available.

Setting	Protocol	Set size n							
		2^8		2^{12}		2^{16}		2^{20}	
		Total	Online	Total	Online	Total	Online	Total	Online
LAN	*DCW (Fig. 3)	3.0	(1.4)	58.5	(27.8)	1,134	(532)	-	
	*DCW + RGBF	2.9	(1.4)	58.4	(27.6)	1,145	(542)	-	
	DKT	1.7		22.6		358		3,050	
	Ours (Fig 4)	**0.2**	(0.003)	**0.9**	(0.04)	**9.7**	(0.7)	**127**	(14)
WAN	*DCW (Fig. 3)	4.2	(1.8)	61.3	(28.8)	1,185	(532)	-	
	*DCW + RGBF	4.0	(1.6)	60.6	(28.6)	1,189	(530)	-	
	DKT	1.7		23.1		393		5,721	
	Ours (Fig 4)	**0.95**	(0.1)	**4.6**	(0.8)	**56**	(11)	**935**	(175)

Fig. 6. Total running time in seconds for the DKT and our protocol when 4, 16, and 64 threads per party are used. The evaluations were performed in the LAN setting with a 0.2 ms round trip time.

Threads	Protocol	Set size n			
		2^8	2^{12}	2^{16}	2^{20}
4	DKT	0.79	6.75	98.1	1,558
	Ours (Fig 4)	0.17	0.63	4.3	66
16	DKT	0.36	2.56	31.0	461
	Ours (Fig 4)	0.17	0.46	3.8	51
64	DKT	0.17	1.30	20.1	309
	Ours (Fig 4)	0.17	0.30	2.3	37

Fig. 7. Total time in seconds, with online time in parentheses, for PSI of two sets of size n with elements of 128 bits. The LAN (resp. WAN) setting has 0.2 ms (resp. 95 ms) round trip time latency. As noted in Sect. 6.3, when the protocol is marked with an asterisk, we report an optimistic underestimate of the running time. Missing times (-) took >5 h.

In Fig. 8 we report the empirical and asymptotic communication costs of the protocols. Out of the bloom filter based protocols, ours consumes significantly less bandwidth. For $n = 2^8$, only 1.9 MB communication was required with most

	set size n				asymptotic	
	2^8	2^{12}	2^{16}	2^{20}	Offline	Online
DCW (Fig. 3)	3.2	50.7	810	-	$2n\kappa^2$	$4nk^2$
DCW + RGBF	2.4	33.9	541	-	$2n\kappa^2$	$2n\kappa^2 + n\kappa$
DKT	0.05	0.8	14	213	0	$6n\phi + 6\phi + n\kappa$
Ours (Fig 4)	1.9	23	324	4,970	$2n\kappa^2$	$2n\kappa \log_2(2n\kappa) + n\kappa$

Fig. 8. The empirical and asymptotic communication cost for sets of size n reported in megabytes, and bits respectively. $\phi = 283$ is the size of the elliptic curve elements. Missing entries had prohibitively long running times and are estimated to be greater than 8,500 MB.

of that cost in the offline phase. Then computing the intersection for $n = 2^{16}$, our protocol uses 324 MB of communication, approximately 5 KB per item. The largest amount of communication occurs during the OT extension and involves the sending of a roughly $2n\kappa^2$-bit matrix. The cut and choose contributes minimally to the communication and consists of np_{chk} choice bits and the xor of the corresponding OT messages. In the online phase, the sending of the permutation consisting of $N_{\mathsf{bf}} \log_2(N_{\mathsf{ot}}) \approx 2n\kappa \log(2n\kappa)$ bits that dominates the communication.

References

1. Asharov, G., Lindell, Y., Schneider, T., Zohner, M.: More efficient oblivious transfer and extensions for faster secure computation. In: Sadeghi et al. [25], pp. 535–548
2. Asharov, G., Lindell, Y., Schneider, T., Zohner, M.: More efficient oblivious transfer extensions with security for malicious adversaries. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 673–701. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46800-5_26
3. Beaver, D.: Correlated pseudorandomness and the complexity of private computations. In: 28th ACM STOC, pp. 479–488. ACM Press, May 1996
4. Canetti, R.: Universally composable security: a new paradigm for cryptographic protocols. In: 42nd FOCS, pp. 136–145. IEEE Computer Society Press, October 2001
5. Canetti, R., Jain, A., Scafuro, A.: Practical UC security with a global random oracle. In: Ahn, G.-J., Yung, M., Li, N. (eds.) ACM CCS 14, pp. 597–608. ACM Press, New York (2014)
6. Dachman-Soled, D., Malkin, T., Raykova, M., Yung, M.: Efficient robust private set intersection. In: Abdalla, M., Pointcheval, D., Fouque, P.-A., Vergnaud, D. (eds.) ACNS 2009. LNCS, vol. 5536, pp. 125–142. Springer, Heidelberg (2009). doi:10.1007/978-3-642-01957-9_8
7. De Cristofaro, E., Kim, J., Tsudik, G.: Linear-complexity private set intersection protocols secure in malicious model. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 213–231. Springer, Heidelberg (2010). doi:10.1007/978-3-642-17373-8_13
8. Dong, C., Chen, L., Wen, Z.: When private set intersection meets big data: an efficient and scalable protocol. In: Sadeghi et al. [25], pp. 789–800
9. Freedman, M.J., Nissim, K., Pinkas, B.: Efficient private matching and set intersection. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 1–19. Springer, Heidelberg (2004). doi:10.1007/978-3-540-24676-3_1
10. Goodrich, M.T., Mitzenmacher, M.: Invertible bloom lookup tables. In: 49th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2011, Allerton Park & Retreat Center, Monticello, IL, USA, 28–30 September 2011, pp. 792–799. IEEE (2011)
11. Huang, Y., Evans, D., Katz, J.: Private set intersection: are garbled circuits better than custom protocols? In: NDSS 2012. The Internet Society, Feburary 2012
12. Huberman, B.A., Franklin, M.K., Hogg, T.: Enhancing privacy and trust in electronic communities. In: EC, pp. 78–86 (1999)
13. Ishai, Y., Kilian, J., Nissim, K., Petrank, E.: Extending oblivious transfers efficiently. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 145–161. Springer, Heidelberg (2003). doi:10.1007/978-3-540-45146-4_9

14. Kamara, S., Mohassel, P., Raykova, M., Sadeghian, S.: Scaling private set intersection to billion-element sets. In: Christin, N., Safavi-Naini, R. (eds.) FC 2014. LNCS, vol. 8437, pp. 195–215. Springer, Heidelberg (2014). doi:10.1007/978-3-662-45472-5_13
15. Keller, M., Orsini, E., Scholl, P.: Actively secure OT extension with optimal overhead. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 724–741. Springer, Heidelberg (2015). doi:10.1007/978-3-662-47989-6_35
16. Kolesnikov, V., Kumaresan, R., Rosulek, M., Trieu, N.: Efficient batched oblivious PRF with applications to private set intersection. In: Weippl, E.R., Katzenbeisser, S., Kruegel, C., Myers, A.C., Halevi, S. (eds.) ACM CCS 16, pp. 818–829. ACM Press, New York (2016)
17. Lambæk, M.: Breaking and fixing private set intersection protocols. Master's thesis, Aarhus University (2016). https://eprint.iacr.org/2016/665
18. Lindell, Y.: Fast cut-and-choose based protocols for malicious and covert adversaries. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8043, pp. 1–17. Springer, Heidelberg (2013). doi:10.1007/978-3-642-40084-1_1
19. Marlinspike, M.: The difficulty of private contact discovery (2014). Blog post https://whispersystems.org/blog/contact-discovery
20. Naor, M., Pinkas, B.: Efficient oblivious transfer protocols. In: Kosaraju, S.R. (ed.) 12th SODA, pp. 448–457. ACM-SIAM, New York (2001)
21. Orrù, M., Orsini, E., Scholl, P.: Actively secure 1-out-of-N OT extension with application to private set intersection. In: Handschuh, H. (ed.) CT-RSA 2017. LNCS, vol. 10159, pp. 381–396. Springer, Cham (2017). doi:10.1007/978-3-319-52153-4_22
22. Pinkas, B., Schneider, T., Segev, G., Zohner, M.: Phasing: private set intersection using permutation-based hashing. In: Jung, J., Holz, T. (eds.) 24th USENIX Security Symposium, USENIX Security 15, pp. 515–530. USENIX Association, Berkeley (2015)
23. Pinkas, B., Schneider, T., Zohner, M.: Faster private set intersection based on OT extension. In: Fu, K., Jung, J. (eds.) 23rd USENIX Security Symposium, USENIX Security 14, pp. 797–812. USENIX Association, Berkeley (2014)
24. Rivest, R.L.: Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer (1999, unpublished manuscript). http://people.csail.mit.edu/rivest/Rivest-commitment.pdf
25. Sadeghi, A.-R., Gligor, V.D., Yung, M. (eds.): ACM CCS 13. ACM Press, New York (2013)