Faster Private Set Intersection Based on OT Extension

Benny Pinkas, Bar-Ilan University; Thomas Schneider and Michael Zohner, Technische Universität Darmstadt

https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/pinkas

This paper is included in the Proceedings of the 23rd USENIX Security Symposium.
August 20–22, 2014 • San Diego, CA

Open access to the Proceedings of the 23rd USENIX Security Symposium is sponsored by USENIX
Faster Private Set Intersection based on OT Extension

Benny Pinkas  Thomas Schneider  Michael Zohner
Bar-Ilan University, Israel  TU Darmstadt, Germany  TU Darmstadt, Germany

Abstract
Private set intersection (PSI) allows two parties to compute the intersection of their sets without revealing any information about items that are not in the intersection. It is one of the best studied applications of secure computation and many PSI protocols have been proposed. However, the variety of existing PSI protocols makes it difficult to identify the solution that performs best in a respective scenario, especially since they were not all implemented and compared in the same setting.

In this work, we give an overview on existing PSI protocols that are secure against semi-honest adversaries. We take advantage of the most recent efficiency improvements in OT extension to propose significant optimizations to previous PSI protocols and to suggest a new PSI protocol whose runtime is superior to that of existing protocols. We compare the performance of the protocols both theoretically and experimentally, by implementing all protocols on the same platform, and give recommendations on which protocol to use in a particular setting.

1 Introduction
Private set intersection (PSI) allows two parties \( P_1 \) and \( P_2 \) holding sets \( X \) and \( Y \), respectively, to identify the intersection \( X \cap Y \) without revealing any information about elements that are not in the intersection. The basic PSI functionality can be used in applications where two parties want to perform JOIN operations over database tables that they must keep private, e.g., private lists of preferences, properties, or personal records of clients or patients. PSI is used for privacy-preserving computation of functionalities such as relationship path discovery in social networks [37], botnet detection [40], testing of fully-sequenced human genomes [3], proximity testing [43], or cheater detection in online games [10]. Another use case is measurement of the performance of web ad campaigns, by comparing purchases by users who were shown a specific ad to purchases of users who were not shown the ad. This is essentially a variant of PSI where the input of the merchant, or of an agency that operates on its behalf, is the identities of the buyers. It was published that Facebook and Datalogix, a consumer data collection company, perform this type of measurements.\(^1\) (The article indicates that they seem to be using the insecure hash-based solution described in \S1.1, but instead they can use a properly secure PSI protocol while still being reasonably efficient.)

PSI has been a very active research field, and there have been many suggestions for PSI protocols. The large number of proposed protocols makes it non-trivial to perform comprehensive cross-evaluations. This is further complicated by the fact that many protocol designs have not been implemented and evaluated, were analyzed under different assumptions and observations, and were often optimized w.r.t. overall runtime while neglecting other relevant factors such as communication.

In this paper, we give an overview on existing efficient PSI protocols, optimize the recently proposed PSI protocols of [27] and [17], based on garbled circuits and Bloom filters, respectively, and describe a new PSI protocol based on recent results in the area of efficient OT extensions [1, 35]. We compare both the theoretical and empirical performance of all protocols on the same platform and conclude with remarks on the protocols and their suitability for different scenarios.

1.1 Classification of PSI Protocols
A naive solution When confronted with the PSI problem, most novices come up with a solution where both parties apply a cryptographic hash function to their inputs and then compare the resulting hashes. Although this protocol is very efficient, it is insecure if the input domain is not large or does not have high entropy, since one party could easily run a brute force attack that applies the hash function to all items that are likely to be in the input set and compare the results to the received hashes. (When inputs to PSI have a high entropy, a protocol that compares hashes of the inputs can be used [41].)

\(^1\)https://www.eff.org/deeplinks/2012/09/deep-dive-facebook-and-datalogix-whats-actually-getting-shared-and-hows-you-can-opt
PSI is one of the best studied problems in secure computation. Since its introduction, several techniques have been used to realize PSI protocols. While the first PSI protocols were special-purpose solutions based on public-key primitives, other solutions were based on circuit-based generic techniques of secure computation, that are mostly based on symmetric cryptography. A recent development are PSI protocols that are based on oblivious transfer (OT) alone, and combine the efficiency of symmetric cryptographic primitives with special purpose optimizations. Finally, we describe PSI protocols that utilize a third party to achieve even better efficiency.

Public-Key-Based PSI A PSI protocol based on the Diffie-Hellmann (DH) key agreement scheme was presented in [29] (related ideas were presented earlier in [36]). This protocol is based on the commutative properties of the DH function and was used for private preference matching, which allows two parties to verify if their preferences match to some degree.

Freedman et al. [21] introduced PSI protocols secure against semi-honest and malicious adversaries in the standard model (rather than in the random oracle model assumed in the DH-based protocol). This protocol was based on polynomial interpolation, and was extended in [19], which presents protocols with simulation-based security against malicious adversaries, and evaluates the practical efficiency of the proposed hashing schemes. We discuss the proposed hashing schemes in §6. A similar approach that uses oblivious pseudo-random functions to perform PSI was presented in [20]. A protocol that uses polynomial interpolation and differentiation for finding intersections between multi-sets was presented in [34].

Another PSI protocol that uses public-key cryptography (more specifically, blind-RSA operations) and scales linearly in the number of elements was presented in [14] and efficiently implemented and benchmarked in [15].

A PSI protocol based on additively homomorphic encryption was described in [11], but is excluded from this evaluation since it scales quadratically in the number of elements and is hence slower than related solutions.

Circuit-Based PSI Generic secure computation protocols have been subject to huge efficiency improvements in the last decade. They allow the secure evaluation of arbitrary functions, expressed as Arithmetic or Boolean circuits. Several Boolean circuits for PSI were proposed in [27] and evaluated using the Yao’s garbled circuits framework of [28]. The authors showed that their Java implementation scales very well with increasing security parameter and outperforms the blind-RSA protocol of [14] for larger security parameter. We reflect on and present new optimizations for circuit-based PSI in §3.


Third Party-Based PSI Several PSI protocols have been proposed that utilize additional parties, e.g., [4]. In [25], a trusted hardware token is used to evaluate an oblivious pseudo-random function. This approach was extended to multiple untrusted hardware tokens in [18]. Several efficient server-aided protocol for PSI were presented and benchmarked in [32]. For their PSI protocol with a semi-honest server, the authors report a runtime of 1.7 s for server-aided PSI on one million elements using 20 threads between cloud instances in the US east and west coast and 10 MB of communicated data. In comparison, our fastest PSI protocol without a server requires 4.9 s for 216 elements using four threads and sends 78 MB (cf. Tab. 1 and Tab. 8). Note that this comparison is sketchy and is only meant to demonstrate that using a third party can increase performance. In our work we focus on PSI protocols without a third party.

1.2 Our Contributions
We describe in detail the PSI protocols based on generic secure computation and on Bloom filters, and suggest how to improve their performance using carefully analyzed features of OT extension. We then introduce a new OT-based PSI protocol, and perform a detailed experimental comparison of all the PSI protocols that we described. In the following, we detail our contributions.

Optimizations of Existing Protocols We improve the circuit- and Bloom-filter-based PSI protocols using recent optimizations for OT extension [1]. In particular, in §3 we evaluate the circuit-based solution of [27] on a secure evaluation of the GMW protocol, and utilize features of random OT (cf. §2.2) to optimize the performance of multiplexer gates (which form about two thirds of the circuit). In §4.3 we redesign the Bloom filter-based protocol of [17] to benefit from using random OT and to support multi-core environments.

---

2Subsequent work of [15] claimed that the blind-RSA protocol of [14] runs faster than the circuit-based protocol of [27] even for larger security parameter. Their implementation is in C++ instead of Java.
A Novel OT-Based PSI Protocol We present a new PSI protocol that is directly based on OT (§5) and directly benefits from recent improvements in efficient OT extensions [1, 35]. The basic version of the protocol can efficiently compare one element with many elements, but for PSI on $n$ elements it requires $O(n^2 \log n)$ communication. In §6 we use carefully analyzed hashing techniques in order to achieve $O(n \log n)$ communication. The resulting protocol has very low computation complexity since it mostly requires symmetric key operations and has even less communication than some public-key-based PSI protocols.

A Detailed Comparison of PSI Protocols We implement the most promising candidate PSI protocols using state-of-the-art cryptographic techniques and compare their performance on the same platform. As far as we know, this is the first time that such a wide comparison has been made, since previous comparisons were either theoretical, compared implementations on different platforms or programming languages, or used implementations without state-of-the-art optimizations. Our implementations and experiments are described in detail in §7. Certain experimental results were unexpected. We give a partial summary of our results in Tab. 1: the values in parenthesis give the overhead of the original protocols and highlight the gains achieved by our optimizations.

<table>
<thead>
<tr>
<th>PSI Protocol</th>
<th>Runtime (s)</th>
<th>Comm. (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DH ECC [29]</td>
<td>416</td>
<td>24</td>
</tr>
<tr>
<td>Circuit [27]</td>
<td>762 (1,304)</td>
<td>14,040 (23,400)</td>
</tr>
<tr>
<td>Bloom Filter</td>
<td>68 (154)</td>
<td>740 (1,393)</td>
</tr>
<tr>
<td>OT §5+§6</td>
<td>14</td>
<td>78</td>
</tr>
</tbody>
</table>

Table 1: Runtime and transferred data for private set intersection protocols on sets with $2^{18}$ 32-bit elements and 128-bit security with a single thread over Gigabit LAN.

We highlight here the conclusions of our results:

- The Diffie-Hellman-based protocol [29], which was the first PSI protocol, is actually the most efficient w.r.t. communication (when implemented using elliptic-curve crypto). Therefore it is suitable for settings with distant parties which have strong computation capabilities but limited connectivity.

- Generic circuit-based protocols [27] are less efficient than the newer, OT-based constructions, but they are more flexible and can easily be adapted for computing variants of the set intersection functionality (e.g., computing whether the size of the intersection exceeds some threshold). Our experiments also support the claim of [27] that circuit-based PSI protocols are faster than the blind-RSA-based PSI protocol of [14] for larger security parameters and given sufficient bandwidth.

- While for larger security parameter previously proposed circuit- and OT-based protocols can be faster than the public-key-based protocols on a Gigabit LAN, the DH-based protocol of [29] outperforms all of them in an Internet network setting. Our new OT-based protocol (§5+§6) is the only protocol that maintains its performance advantage in this setting and even outperforms public-key-based PSI protocols for a mobile network setting.

2 Preliminaries

We give our notation and security definitions in §2.1 and review recent relevant work on oblivious transfer in §2.2.

2.1 Notation and Security Definitions

We denote the parties as $P_1$ and $P_2$, and their respective input sets as $X$ and $Y$ with $|X| = n_1$ and $|Y| = n_2$. When the two input sets are of equal size, we use $n = n_1 = n_2$. We refer to elements from $X$ as $x$ and elements from $Y$ as $y$ and each element has bit-length $\sigma$ (we detail the relation between $n$ and $\sigma$ in the full version [47]).

We write $b[i]$ for the $i$-th element of a list $b$, denote the bitwise-AND between two bit strings $a$ and $b$ of equal length as $a \land b$ and the bitwise-XOR as $a \oplus b$.

We refer to a correlation resistant one-way function as CRF, and to a pseudo-random generator as PRG.

We write $\binom{N}{m}$-OT$_{\ell}^{m}$ for $m$ parallel 1-out-of-$N$ oblivious transfers on $\ell$-bit strings, and write OT$_{\ell}^{m}$ for $\binom{m}{1}$-OT$_{\ell}^{m}$.

Security parameters We denote the symmetric security parameter as $\kappa$, the asymmetric security parameter as $\rho$, the statistical security parameter as $\lambda$, and use the recommended key sizes of the NIST guideline [45], summarized in Tab. 2. We denote the bit size of elliptic curve points with $\varphi$, i.e., $\varphi = 284$ for Koblitz curve K-283 when using point compression.

<table>
<thead>
<tr>
<th>Security</th>
<th>SYM ($\kappa$)</th>
<th>FFC and IFC ($\rho$)</th>
<th>ECC ($\varphi$)</th>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>80-bit</td>
<td>80</td>
<td>1,024</td>
<td>K-163</td>
<td>SHA-1</td>
</tr>
<tr>
<td>128-bit</td>
<td>128</td>
<td>3,072</td>
<td>K-283</td>
<td>SHA-256</td>
</tr>
</tbody>
</table>

Table 2: NIST recommended key sizes for symmetric cryptography (SYM), finite field cryptography (FFC), integer factorization cryptography (IFC), elliptic curve cryptography (ECC) and hash functions.
Adversary definition  The secure computation literature considers two types of adversaries with different strengths: A semi-honest adversary tries to learn as much information as possible from a given protocol execution but is not able to deviate from the protocol steps. The semi-honest adversary model is appropriate for scenarios where software attestation is enforced or where an untrusted third party is able obtain the transcript of the protocol after its execution, either by stealing it or by legally enforcing its disclosure. The stronger, malicious adversary extends the semi-honest adversary by being able to deviate arbitrarily from the protocol steps.

Most protocols for private set intersection, as well as this work, focus on solutions that are secure against semi-honest adversaries. PSI protocols for the malicious setting exist, but they are considerably less efficient than protocols for the semi-honest setting (see, e.g., [13, 16, 19, 21, 26, 31]).

The random oracle model  As most previous works on efficient PSI, we use the random oracle model to achieve more efficient implementations [8]. We provide details and argue about the use of random oracles in the full version [47].

2.2 Oblivious Transfer

Oblivious transfer (OT) is a major building block for secure computation. When executing m invocations of 1-out-of-2 OT on ℓ-bit strings (denoted \( \ell \)-OT\(^m\)), the sender \( S \) holds \( m \) message pairs \( (x_0^i, x_1^i) \) with \( x_0^i, x_1^i \in \{0, 1\}^\ell \), while the receiver \( R \) holds an \( m \)-bit choice vector \( b \). At the end of the protocol, \( R \) receives \( x_{1-b[i]}^i \) but learns nothing about \( x_{1-b[i]}^i \); and \( S \) learns nothing about \( b \). Many OT protocols have been proposed, most notably (for the semi-honest model) the Naor-Pinkas OT [42], which uses public-key operations and has amortized complexity of \( 3m \) public-key operations when performing \( m \) OTs.

OT extension [6, 30] reduces the number of expensive public-key operations for OT\(^m\) to that of only OT\(^3\), and computes the rest of the protocol using more efficient symmetric cryptographic operations which are orders of magnitude faster. The security parameter \( \kappa \) is essentially independent of the number of OTs \( m \), and can be as small as 80 or 128. Thereby, the computational complexity for performing OT is reduced to such an extent, that the network bandwidth becomes the main bottleneck [1].

Recently, the efficiency of OT extension protocols has gained a lot of attention. In [35], an efficient 1-out-of-\( N \) OT extension protocol was shown, that has sub-linear communication in \( \kappa \) for short messages. Another protocol improvement is outlined in [1,35], which decreases the communication from \( R \) to \( S \) by half. Additionally, several works [1,44] improve the efficiency of OT by using an OT variant, called random OT. In random OT, \( (x_0^i, x_1^i) \) are chosen uniformly and randomly within the OT and are output to \( S \), thereby removing the final message from \( S \) to \( R \). Random OT is useful for many applications, and we show how it can reduce the overhead of PSI. We elaborate on these OT extension protocols in the full version [47].

3 Circuit-Based PSI

Unlike special purpose private set intersection protocols, the protocols that we describe in this section are based on a generic secure computation protocol that can be used for computing arbitrary functionalities. State-of-the-art for computing the PSI functionality is the sort-compare-shuffle (SCS) circuit of [27], which has size \( O(n \log n) \) (cf. full version [47] for details.) We discuss these protocols by reflecting on the generic secure computation protocol of Goldreich-Micali-Wigderson (GMW) [23] (§3.1) and outlining major optimizations for evaluating the SCS circuit for PSI using GMW (§3.2).

The usage of generic protocols holds the advantage that the functionality of the protocol can easily be extended, without having to change the protocol or the security of the resulting protocol. For example, it is straightforward to change the protocol to compute the size of the intersection, or a function that outputs 1 if the intersection is greater than some threshold, or compute a summation of values (e.g., revenues) associated with the items that are in the intersection. Computing these variants using other PSI protocols is non-trivial.

3.1 The GMW Protocol

We focus on the GMW protocol [23] for generic secure computation, which was implemented in the semi-honest model for multiple parties in [12], optimized for two parties in [49], and extended to the malicious model in [44].

The GMW protocol represents the function to be computed as a Boolean circuit and uses an XOR-based secret-sharing and OT to evaluate the circuit. A circuit with input bit \( u \) from \( P_1 \) and \( v \) from \( P_2 \) is evaluated as follows. First, \( P_1 \) and \( P_2 \) secret-share their input bit \( u = u_1 \oplus u_2 \) and \( v = v_1 \oplus v_2 \) and \( P_1 \) obtains the shares labeled with \( i \). The parties then evaluate the Boolean circuit gate-by-gate, as detailed next. To evaluate an XOR gate with input wires \( u \) and \( v \) and output wire \( w \), \( P_1 \) locally computes \( w_1 = u_1 \oplus v_1 \) while \( P_2 \) locally computes \( w_2 = u_2 \oplus v_2 \).

Evaluating AND gates using multiplication triples

An AND gate with input wire \( u \) and \( v \) and output wire \( w \)
requires an interaction between both parties using a multiplication triple [5]. A multiplication triple is a set of shares \( \alpha_1, \alpha_2, \beta_1, \beta_2, \gamma, \gamma_2 \in \{0, 1\} \) with \((\alpha_1 \oplus \alpha_2) \wedge (\beta_1 \oplus \beta_2) = \gamma \oplus \gamma_2\). Given a multiplication triple, to evaluate an AND gate implementing \( u \) AND \( v \), the parties compute \( d_1 = \alpha_1 \oplus u \) and \( e_1 = \beta_1 \oplus v \), exchange \( d_1, e_1 \), re-construct \( d = d_1 \oplus d_2 \) and \( e = e_1 \oplus e_2 \), and compute the shares of the gate output wire as \( w_2 = (d \wedge e) \oplus (e \wedge \alpha_2) \oplus (e \wedge \beta_2) \) and \( w_3 = (d \wedge \beta_2) \oplus (e \wedge \alpha_2) \oplus \gamma_2\). These are all extremely efficient operations and therefore the efficiency of the evaluation depends on the efficiency of generating multiplication triples.

As described in [1], multiplication triples can be generated using two random OTs on one-bit strings as follows: both parties choose \( \alpha \in R \{0, 1\} \) and run two random OTs, where in the first OT \( P_1 \) acts as sender and \( P_2 \) as receiver with choice bit \( \alpha_1 \). From each OT, the sender obtains \( (x_0, x_1) \) and sets \( \beta_1 = x_0 \oplus x_1 \) and the receiver obtains \( x_0' \). To compute valid \( \gamma, \gamma_1 \) values for the triple, note that \((\alpha_1 \oplus \alpha_2) \wedge (\beta_1 \oplus \beta_2) = (\alpha_1 \wedge \beta_1) \oplus (\alpha_1 \wedge \beta_2) \oplus (\alpha_2 \wedge \beta_1) \oplus (\alpha_2 \wedge \beta_2) = \gamma \oplus \gamma_1\). \( P_1 \) locally computes \( \alpha_1 \wedge \beta_1 \). Values \( \alpha_1 \wedge \beta_2 \) and \( \alpha_2 \wedge \beta_1 \) are computed using the output of the random OT as \( \alpha_1 \wedge \beta_2 = x_0' \oplus x_1 \) and \( \alpha_2 \wedge \beta_1 = x_1' \oplus x_0 \). Finally, \( P_1 \) sets \( \gamma_1 = (\alpha_1 \wedge \beta_1) \oplus x_0' \oplus x_1' \) and \( P_2 \) sets \( \gamma = (\alpha_2 \wedge \beta_2) \oplus x_0' \oplus x_1' \). These computations can be done in a preprocessing step before the input is known, are independent of circuit’s structure, and highly parallelizable.

### 3.2 Optimized Circuit-Based PSI

We describe in this section an optimization which greatly reduces the overhead of circuit based PSI for GMW (as is detailed in Tab. 5 in §7, the reduction in the runtime for inputs of size 2\(^{18}\) is about 40%). The optimization is based on a protocol proposed in [39].

Approximately 2/3 of the AND gates in the SCS circuit are due to multiplexers (cf. full version [47] for details). In each multiplexer operation with \( \sigma \)-bit inputs \( x \) and \( y \) and a choice bit \( z \), we compute \( z[j] = s \wedge (x[j] \oplus y[j]) \oplus x[j] \) for each \( 1 \leq j \leq \sigma \) using \( \sigma \) AND gates in total. The evaluation of this multiplication circuit in the GMW protocol requires random OT\(^2\) \( \sigma \), namely 2\(\sigma\) random OTs of single-bit inputs. We observe that the same wire \( s \) is input to multiple AND gates which allows for the following optimization.

Consider an input wire \( u \) that is input to multiple AND gates of the form \( w[1] = (u \text{ AND } v[1]), \ldots, w[\sigma] = (u \text{ AND } v[\sigma])\). Similar to the evaluation of a single AND gate described in §3.1, these gates can be evaluated using a multiplication triple generalized to vectors, which we call a vector multiplication triple.

A vector multiplication triple has the following form: \( \alpha_1, \alpha_2 \in \{0, 1\} ; \beta_1, \beta_2, \gamma_1, \gamma_2 \in \{0, 1\}^\sigma \), where \( P_1 \) holds the shares labeled with \( i \) that satisfy the condition \((\alpha_1 \oplus \alpha_2) \wedge (\beta_1[i] \oplus \beta_2[i]) = \gamma_1[i] \oplus \gamma_2[i]\). To evaluate the AND gates, both parties compute \( d_i = \alpha_i \oplus u_i \) and \( e_i[j] = \beta_1[i] \oplus v_j[i], \) exchange \( d_i, e_i[j] \), set \( d = d_1 \oplus d_2 \), \( e = e_1[j] \oplus e_2[j] \), and \( \gamma[i] = (d \wedge e[i]) \oplus (d \wedge \beta_1[i]) \oplus (e[i] \wedge \alpha_2) \oplus \gamma_2[i]\). The vector multiplication triple can be pre-computed analogously to the regular multiplication triples described in §3.1, but using random OT\(^2\) \( \sigma \), namely only two random OTs applied to \( \sigma \)-bit strings: The parties each choose \( \alpha_1, \alpha_2 \in \mathcal{R} \{0, 1\} \) and perform a random OT\(^2\) \( \sigma \) with \( P_1 \) acting as sender and \( P_2 \) acting as receiver with choice bit \( \alpha_2 \), and a second random OT\(^1\) \( \sigma \) with \( P_2 \) acting as sender and \( P_1 \) acting as receiver with choice bit \( \alpha_1 \). From these random OTs, \( P_1 \) obtains \( \beta_1 \in \{0, 1\}^\sigma = x_0' \oplus x_1' \) and, analogously to the regular multiplication triple generation, a valid \( \gamma \in \{0, 1\}^\sigma \).

### Efficiency

Overall, evaluating \( \sigma \) AND gates with a vector multiplication triple requires to send \( 2\sigma + 2 \) bits (instead of 4\(\sigma\) bits with \( \sigma \) regular multiplication triples). Generating a vector multiplication triple requires 2 random OTs on \( \sigma \)-bit strings (instead of 2\(\sigma\) random OTs with \( \sigma \) regular multiplication triples); as the communication of random OT is independent of the input length, this improves communication by factor \( \sigma \).

In the SCS circuit we have \( 2n \log_2 n + n + 1 \) multiplexers, each of which can be evaluated using a single vector multiplication triple. This reduces the number of random OTs from \( 2\sigma(2n \log_2 n + n + 1) \) to \( 2(2n \log_2 n + n + 1) \).

### Further applications of vector multiplication triples

As a side note, we comment that our vector multiplication triples can be used in every circuit where wires are used as input in two or more AND gates. As such, another beneficial application is multiplication. When computing a multiplication between two \( \sigma \)-bit numbers \( x \) and \( y \) using the school method multiplication circuit [49], each bit \( x_i \) is multiplied with every bit of \( y \): \( \forall 1 \leq i \leq \sigma \forall 1 \leq j \leq \sigma (x_i \wedge y_j) \). Here, using vector multiplication triples allows to reduce the total number of random OTs by a factor two, from \( 4\sigma^2 - 2\sigma \) OTs to \( 2\sigma^2 \).

### 4 Bloom Filter-Based PSI

The recent PSI protocol of [17] uses Bloom Filters (BF) and OT to compute set intersection. We summarize Bloom filters in §4.1 and the PSI protocol of [17] in §4.2. We then present a redesigned optimized version of the protocol in §4.3. This optimization reduces the runtime for inputs of size \( 2^{18} \) by 55% – 60% (cf. §7, Tab. 5).

---

USENIX Association  23rd USENIX Security Symposium  801
4.1 The Bloom Filter

A BF that represents a set of $n$ elements consists of an $m$-bit string $F$ and $k$ independent uniform hash functions $h_1,...,h_k$ with $h_i: \{0,1\}^* \rightarrow [1,m]$, for $1 \leq i \leq k$. Initially, all bits in $F$ are set to zero. An element $x$ is inserted into the BF by setting $F[h_i(x)] = 1$ for all $i$. To query if the BF contains an item $y$, one checks all bits $F[h_i(y)]$. If there is at least one $j$ such that $BF[h_j(y)] = 0$, then $y$ is not in the BF. If, on the other hand, all bits $BF[h_j(y)]$ are set to one, then $y$ is in the BF except for a false positive probability $\varepsilon$. An upper bound on $\varepsilon$ can be computed as $p = 1 - (1 - \frac{1}{m})^kn$. The authors of [17] propose to choose the number of hash functions as $k = \frac{\ln m}{\ln \varepsilon}$ and the size of the BF as $m = kn/\ln 2 \approx 1.44kn$. In their experiments, they set $\varepsilon = 2^{-k}$, resulting in $k = \kappa$ and a filter of size $m \approx 1.44kn$.

4.2 Garbled Bloom Filter-Based PSI

For BF-based PSI, one cannot simply compute the bit-wise AND of the BFs that represent each set, as this leaks information (see [17] for details). Instead, the authors of [17] introduced a variant of the BF, called Garbled Bloom Filter (GBF). Like a BF, a GBF $G$ uses $\kappa$ hash functions $h_1,...,h_\kappa$, but instead of single bits, it holds shares of length $\ell$ at each position $G[i]$, for $1 \leq i \leq m$. These shares are chosen uniformly at random, subject to the constraint that for every element $x$ contained in the filter $G$ it holds that $\bigoplus_{i=1}^{\kappa} G[h_i(x)] = x$.

To represent a set $X$ using a GBF $G$, all positions of $G$ are initially marked as unoccupied. Each element $x \in X$ is then inserted as follows. First, the insertion algorithm tries to find a hash function $t \in [1...\kappa]$ such that $G[h_t(x)]$ is unoccupied (the probability of not finding such a function is equal to the probability of a false positive, which is negligible due to the choice of parameters). All other unoccupied positions $G[h_j(x)]$ are set to random $\ell$-bit shares. Finally, $G[h_t(x)]$ is set to $G[h_t(x)] = x \oplus (\bigoplus_{j \neq t} G[h_j(x)])$ to obtain a valid sharing of $x$. We emphasize that because existing shares need to be re-used, the generation of the GBF cannot be fully parallelized. (We describe below in §4.3 how the protocol can be modified to enable a parallel execution.)

In the semi-honest secure PSI protocol of [17], $P_1$ generates a $m$-bit GBF $G_X$ from its set $X$ and $P_2$ generates a $m$-bit BF $F_Y$ from its set $Y$. $P_1$ and $P_2$ then perform OT$^\ell$, where for the $i$-th OT $P_1$ acts as a sender with input $(0,G_X[i])$ and $P_2$ acts as a receiver with choice bit $F_Y[i]$. Thereby, $P_2$ obtains an intersection GBF $G_{(X,Y)}$, for which $G_{(X,Y)}[i] = 0$ if $F_Y[i] = 0$ and $G_{(X,Y)}[i] = G_X[i]$ if $F_Y[i] = 1$. $P_2$ can check whether an element $y$ is in the intersection by checking whether $\bigoplus_{i=1}^{\kappa} G_{(X,Y)}[h_i(y)] = y$. (Note that $P_2$ cannot perform this check for any value which is not in its input set, since the probability that it learns all GBF locations associated with that value is equal to the probability of a false positive, which is negligible due to the choice of parameters.) The bit-length of the shares in the GBF can be set to $\ell = \lambda$.

4.3 Random GBF-Based PSI

We introduce an optimization of the GBF-based PSI protocol of [17], which we call the random Garbled Bloom Filter protocol. The core idea is to have parties collaboratively generate a random GBF. This is in contrast to the original protocol where the GBF had to be of a specific structure (i.e., have the XOR of the entries of $x \in X$ be $x$). The modified protocol can be based on random OT extension (in fact, on a version of the protocol which is even more efficient than the original random OT extension). For each position in the filter, each party learns a random value if the corresponding bit in its BF is 1. $P_1$ then sends to $P_2$ the XOR of the GBF values corresponding to each of its inputs, and $P_2$ compares these values to the XOR of the GBF values of its own inputs.

We denote the primitive that enables this solution an oblivious pseudo-random generator (OPRG), which takes as inputs bits $b_1,b_2$ from each party, respectively, generates a random string $s$, and outputs to $P_2$ $s$ if $b_1 = 1$ and nothing otherwise, for $i \in \{0,1\}$. Additionally, we require that the parties remain oblivious to whether the other party obtained $s$. A protocol for computing this functionality is obtained by modifying the existing random OT extension protocol of [1] as follows.

Recall that in random OT extension, $S$ has no input in the i-th OT and outputs two values $(x_0^i,x_1^i)$, while $R$ inputs a choice bit vector $b$ and outputs $x_{b[i]}^i$. Computation of each of these values involves one evaluation of a hash function $H$ (cf. §2.2; the detailed random OT extension protocol is summarized in the full version [47]). The new functionality is obtained by having $S$ ignore the $x_0^i$ output that it receives, and ignore also the $x_1^i$ output if $b_1 = 0$. Similarly, $R$ ignores its output if $b_2 = 0$. The random OT extension protocol thus becomes more efficient, since the parties can ignore parts of the computation.

Our resulting Bloom filter-based protocol works as follows. First, $P_1$ and $P_2$ each generate a BF, $F_X$ and $F_Y$ respectively. They evaluate the OPRG with $P_1$ being the sender and $P_2$ being the receiver, using the bits of $F_X$ and $F_Y$ as inputs, to obtain random BGFs $G_X$ and $G_Y$ with entries in $\{0,1\}^\ell$. For each element $x_j$ in its set $X$, $P_1$ then computes $m_{P_1}[j] = \bigoplus_{i=1}^{\kappa} G_X[h_i(x_j)]$, with $1 \leq j \leq n_1$. Finally, $P_1$ sends all $m_{P_1}$ values in random order to $P_2$, which identifies whether an element $y$ in its set is in the intersection by checking whether a $j$ exists such that $m_{P_2}[j] = \bigoplus_{i=1}^{\kappa} G_Y[h_i(y)]$. 

802 23rd USENIX Security Symposium USENIX Association
**Correctness** For each item in the intersection, \( P_2 \) gets from \( P_1 \) the same XOR value that it computed from its own GBF, and therefore identifies that the item is in the intersection. For any item which is not in the intersection, it holds with overwhelming probability that the XOR value computed by \( P_2 \) is independent of the \( n_1 \) values received from \( P_1 \). The probability of a false positive identification for that value is therefore \( n_1 \cdot 2^{-\ell} \). The probability of a false positive identification for any of the values is \( n_1 n_2 \cdot 2^{-\ell} \). To achieve correctness with probability \( 1 - 2^{-\epsilon} \), we therefore set \( \epsilon = \lambda + \log_2 n_1 + \log_2 n_2 \).

**Security** The security of each party can be easily proved using a simulation argument. \( P_2 \)'s security is obvious, since the only information that \( P_1 \) learns are the random outputs of the random OT protocol, which are independent of \( P_2 \)'s input and can be easily simulated by \( P_1 \). \( P_1 \)'s security is apparent from observing that the information that \( P_2 \) receives from \( P_1 \) is composed of

- The XOR values that \( P_2 \) computed for each item in the intersection.
- The XOR values that \( P_2 \) computed for its \( n_1 - |X \cap Y| \) items that are not in the intersection. These values are independent of \( P_2 \)'s BF unless one of these items is a false-positive identification in the filter, which happens with negligible probability \( \epsilon \).

Therefore, the information received from \( P_1 \) can be easily simulated by \( P_2 \) given its legitimate output, i.e., \( X \cap Y \).

**Efficiency** As shown in Tab. 3, our resulting random GBF-based PSI protocol has less computation and communication complexity than the original GBF protocol in [17]. In terms of communication, in our new protocol, \( P_1 \) has to send the \( n_1 \ell \)-bit vector \( m_{P_1} \) and \( P_2 \) has to send \( m \kappa \) bits in the random OTs. (This is compared to \( 2m \lambda \) bits and \( 2m n \kappa \) bits sent in the original protocol. Later in our experiments in § 7 we show that the communication is reduced by a factor between 1.9 and 3, cf. Tab. 6.)

The computation complexity of our protocol is \( HW(F_{X}) \) hash function evaluations for \( P_1 \) and \( HW(F_{Y}) \) hash function evaluations for \( P_2 \), where \( HW(\cdot) \) denotes the Hamming weight. When the number of hash functions \( k \) and the size of the BF \( m \) are chosen optimally, we can approximate the average Hamming weight in a BF using the probability that a single bit is set to 1, which is \( 1 - (1 - (\frac{1}{2})^m)^{kn} \approx \frac{1}{2} \). Thus, \( HW(F) \approx \frac{n}{2} \).

A main advantage of our protocol is that it allows to parallelize all operations: BFs can be generated in parallel (bits in the BF are changed only from 0 to 1) and, most importantly, the random GBF can also be constructed in parallel, in contrast to the original GBF-based protocol.

<table>
<thead>
<tr>
<th>Optimization</th>
<th>Party</th>
<th># Bits Sent</th>
<th># calls to H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original GBF-based PSI [17]</td>
<td>( P_1 )</td>
<td>( 2m \lambda )</td>
<td>( 2m )</td>
</tr>
<tr>
<td></td>
<td>( P_2 )</td>
<td>( 2m \kappa )</td>
<td>( m )</td>
</tr>
<tr>
<td>Random GBF-based PSI (§4.3)</td>
<td>( P_1 )</td>
<td>( n_1 \ell )</td>
<td>( m/2 )</td>
</tr>
<tr>
<td></td>
<td>( P_2 )</td>
<td>( m \kappa )</td>
<td>( m/2 )</td>
</tr>
</tbody>
</table>

Table 3: Communication and computation complexities for Bloom-filter-based PSI of [17] and our optimization. \((\lambda): \) statistical security parameter, \( \kappa \): symmetric security parameter, \( n_1 \): number of elements of party \( P_1 \), \( m \approx 1.44 \kappa \max(n_1, n_2) \), \( \ell = \lambda + \log_2 n_1 + \log_2 n_2 \).

## 5 Private Set Intersection via OT

We propose a new private set intersection protocol that is based on the most efficient OT extension techniques, in particular the random OT functionality [1, 44] and the efficient 1-out-of-\(N\) OT of [35]. This PSI protocol scales very efficiently with an increasing set size.

We first describe the protocol for a private equality test (PEQT) between two elements \( x \) and \( y \) (§ 5.1) and then describe how to efficiently extend it for comparing \( y \) to a set \( X = \{x_1, \ldots, x_n\} \) (§ 5.2). The resulting protocol can then be simply extended to perform PSI between sets \( X \) and \( Y \) by applying the parallel comparison protocol for each element \( y \in Y \) (§ 5.3). The overhead of the protocol can be greatly improved using hashing (§ 6).

### 5.1 The Basic PEQT Protocol

In the most basic private equality test (PEQT) protocol, \( P_1 \) and \( P_2 \) check whether their \( \sigma \)-bit elements \( x \) and \( y \) are equal by engaging in random \( \binom{\ell}{\ell} \) OTs, where \( P_2 \) uses the bits of \( y \) as its choice vector. From each random OT, \( P_1 \) obtains two uniformly distributed and random \( \ell \)-bit strings \( (s_{0}^{1}, s_{1}^{1}) \), and \( P_2 \) obtains \( s_{y}^{1}[i] \); \( P_1 \) then computes \( m_{P_1} = \bigoplus_{i=1}^{\ell} s_{y}^{1}[i] \) (the XOR of the strings corresponding to the binary representation of \( x \)) and sends it to \( P_2 \). \( P_2 \) compares this value to \( m_{P_2} = \bigoplus_{i=1}^{\ell} s_{y}^{1}[i] \) and decides that \( x = y \) iff \( m_{P_1} = m_{P_2} \).

The basic private equality test can be improved by using a base-\( N \) representation of the inputs and a \( \binom{\ell}{\ell} \) OT in the protocol. Specifically, let \( N = 2^\eta \). \( P_1 \) and \( P_2 \) check whether their \( \sigma \)-bit elements \( x \) and \( y \) are equal by representing them using \( \ell = \sigma / \eta \) letters from an alphabet of size \( N \), and then engaging in random \( \binom{\ell}{\ell} \) OTs.

For this, \( P_2 \) cuts its \( \sigma \)-bit element \( y \) into \( \ell \) blocks \( y[i] \) of bitlength \( \eta \) each: \( y = y[1] | \ldots | y[i] | \ldots | y[\ell] \); similarly, \( P_1 \) interprets \( x = x[1] | \ldots | x[\ell] \). In the \( i \)-th random \( \binom{\ell}{\ell} \) OT, \( P_2 \) inputs \( y[i] \) as choice bits and \( P_1 \) obtains \( N \) random and uniformly distributed \( \ell \)-bit strings \( (s_{0}^{1}, \ldots, s_{N-1}^{1}) \); \( P_2 \) obtains \( s_{y}^{1}[i] \); \( P_1 \) sends \( m_{P_1} = \bigoplus_{i=1}^{\ell} s_{y}^{1}[i] \) to \( P_2 \) who compares it to \( m_{P_2} = \bigoplus_{i=1}^{\ell} s_{y}^{1}[i] \) and decides that \( x = y \) iff \( m_{P_1} = m_{P_2} \).
Correctness  If \( x = y \) then the choices that both parties make for their sums are equal, i.e., \( m_{P_1} = \bigoplus_{t=1}^{\ell} s^t_{x[t]} = \bigoplus_{t=1}^{\ell} s^t_{y[t]} \) and \( m_{P_2} \) successfully identifies equality.  

If \( x \neq y \) then the probability that \( m_{P_1} = m_{P_2} \) is \( 2^{-\ell} \). To see that this is true, assume w.l.o.g. that the inputs differ in their last sub-string, i.e., \( x[T] \neq y[T] \). Equality only holds if the last element received by \( P_2 \), namely \( s^T_{y[T]} \), is equal to \( \bigoplus_{t=1}^{T} s^t_{y[t]} \). The value of \( s^T_{y[T]} \) is independent of the other values, and therefore this equality happens with probability \( 2^{-\ell} \) and thus we can set \( \ell \) to be equal to the statistical security parameter \( \lambda \).

Security  \( P_2 \)'s security is obvious, since the only information that \( P_1 \) learns are the random values chosen in the random OT, which are independent of \( P_2 \)'s input.

As for \( P_1 \)'s security, note that \( P_2 \)'s view in the protocol consists of its \( r \) outputs in the random \( \binom{N}{r} \)-OT protocols, and of the value \( m_{P_1} \) sent by \( P_1 \). If \( x = y \) then \( m_{P_1} \) is equal to the XOR of the first \( r \) values. Otherwise, all \( t+1 \) values are uniformly distributed. In both cases, the view of \( P_2 \) can be easily simulated given the output of the protocol (i.e., knowledge whether \( x = y \)). The protocol is therefore secure according to the common security definitions of secure computation [22].

Efficiency  Since in the \( i \)-th random OT \( P_1 \) needs only the output \( s^i_{x[i]} \) it suffices to evaluate one hash function per random OT. When using the random \( \binom{\ell}{2} \)-OT extension protocol\(^3\) of [1] and \( \ell = \lambda \), the parties perform random \( \text{OT}^\kappa_2 \), send \( \sigma \kappa + \lambda \) bits, and do \( \sigma \) hash function evaluations each. In comparison, when using the random \( \binom{\ell}{1} \)-OT extension protocol of [35], the parties perform only \( \sigma/\eta \) OTs and send \( 2\kappa \) bits per OT; in total, they have to send \( 2\sigma\kappa/\eta + \lambda \) bits and do \( \sigma/\eta \) hash function evaluations each. In the full version [47] we provide an analysis which shows that setting \( \eta = 8 \) results in optimal performance for our PSI protocols.

5.2 Private Set Inclusion Protocol

In a private set inclusion protocol, \( P_1 \) and \( P_2 \) check whether \( y \) equals any of the values in \( X = \{x_1, \ldots, x_n\} \). The set inclusion protocol is similar to the basic PEQT protocol, but in order to perform multiple comparisons in parallel, the OTs are computed over longer strings, essentially transferring (in parallel) a random string for each element in the set \( X \).

In more detail, both parties run a random \( \binom{N}{1} \)-OT\( \text{PEQT}^\kappa_n \), where \( P_2 \) uses the bits of \( y \) as choice bits. Each received string is of length \( n_1 \ell \) bits. That is, in the \( i \)-th random OT, \( P_1 \) obtains \( N \) random strings \( \{s^i_1, \ldots, s^i_{N-1}\} \subset \{0,1\}^{\ell} \), and \( P_2 \) obtains one random string \( s^i_{y[i]} \). The strings are parsed as a list of \( n_1 \) sub-strings of length \( \ell \) bits each. We refer to the \( j \)-th sub-string in these lists as \( s^i_{w[j]} \), for \( 1 \leq j \leq n_1 \) and \( 0 \leq w < N \). Using these sub-strings, \( P_1 \) and \( P_2 \) can then compute the XOR of the strings corresponding to their respective inputs, compare the results and decide on equality, as was described in the basic PEQT protocol in §5.1. In more detail, \( P_1 \) computes \( m_{P_1}[j] = \bigoplus_{t=1}^{\ell} s^i_{w[j]}[t] \) and sends the \( n_1 \ell \)-bit string \( m_{P_1} \) to \( P_2 \). \( P_2 \) decides whether \( y \) matches any of the elements in \( X \) by computing \( m_{P_2} = \bigoplus_{t=1}^{\ell} s^i_{y[t]}[t] \) and checking whether a \( j \) exists with \( m_{P_1}[j] = m_{P_2} \).

Correctness and security follow from the properties of the protocol of §5.1. However, now we require that the value \( m_{P_1} \) and all the \( n_1 \) values \( m_{P_1}[j] \) are distinct, which happens with probability \( n_1 2^{-\ell} \). Thus, to achieve correctness with probability \( 1-2^{-\lambda} \), we must increase the bit-length of the OTs to \( \ell = \lambda + \log_2 n_1 \). Also, note that \( P_2 \) learns the position \( j \) at which the match is found, which can be avoided by randomly permuting the inputs.

Efficiency  The set inclusion protocol that compares \( y \) to many values has the same number of random OTs as the basic comparison protocol comparing \( y \) to a single value, but it requires the transferred strings to be of length \( n_1(\lambda + \log_2 n_1) \) bits instead of \( \lambda \) bits. Note, however, that since we use random OTs there is no need to send these strings in the OT protocol. Instead, all strings corresponding to the same value of the same input bit can be generated from a single seed using a pseudo-random generator. Therefore, the amount of data transferred in the OTs is the same as for the single comparison PEQT protocol.

The only additional data that is sent is the \( n_1(\lambda + \log_2 n_1) \)-bit string \( m_{P_2} \), which \( P_1 \) sends to \( P_2 \). Hence, the total amount of communication is \( 2\sigma\kappa/\eta + n_1(\lambda + \log_2 n_1) \) bits.

In addition, the PRG which is used to generate the output string from the OT must be evaluated multiple times to generate the \( n_1(\lambda + \log_2 n_1) \) bits. Therefore, the set inclusion protocol, which compares \( y \) to \( n_1 \) elements, is less efficient than a single run of the PEQT protocol, but is definitely more efficient than \( n_1 \) invocations of the PEQT protocol.

5.3 The OT-Based PSI Protocol

To obtain the final PSI protocol that computes \( X \cap Y \), \( P_2 \) simply invokes the private set inclusion protocol of §5.2 for each \( y \in Y \). Correctness and security follow from the properties of the private set inclusion protocol.
Efficiency Overall, to compute the intersection between sets $X$ and $Y$ of $\sigma$-bit elements, the protocol requires $n_2 \sigma/\eta$ random $\binom{n_2}{2}$-OTs of $n_1(\lambda + \log_2 n_1)$ bits and additionally $n_1 n_2 (\lambda + \log_2 n_1)$ bits to be sent. Using the random $\binom{n_2}{2}$-OT of [35], the total amount of communication is $2n_2 \sigma k/\eta + n_1 n_2 (\lambda + \log_2 n_1)$ bits. For large $n_1$ and $n_2$, this amount of communication grows too large for an efficient solution. In order to cope with large sets, one can use a hashing scheme, as shown in §6.

6 Hashing Schemes and PSI

Several private set intersection protocols are based on running many invocations of pairwise private equality tests (PEQT). These protocols include [11, 21, 27] or our set inclusion protocol in §5. A straightforward implementation of these protocols requires $n^2$ invocations of PEQT for sets of size $n$, and therefore does not scale well. In [19, 21] it was proposed to use hashing schemes to reduce the number of comparisons that have to be computed. The idea is to have each party use a publicly known random hashing scheme to map its input elements to a set of bins. If an input element is in the intersection, both parties map it to the same bin. Therefore, the protocol can check for intersections only between items that were mapped to the same bin by both parties.

Naïvely, if $n$ items are mapped to $n$ bins then the average number of items in a bin is $O(1)$, checking for an intersection in a bin takes $O(1)$ work, and the total overhead is $O(n)$. However, privacy requires that the parties hide from each other how many of their inputs were mapped to each bin.\(^4\) As a result, we must calculate in advance the number of items that will be mapped to the most populated bin (w.h.p.), and then set all bins to be of that size. (This can be done by storing dummy items in bins which are not fully occupied.) This change hides the bin sizes but also increases the overhead of the protocol, since the number of comparisons per bin now depends on the size of the most populated bin rather than on the actual number of items in the bin. However, while the parties need to pretend externally that all their items are real, they do not need to apply all their internal computations to their dummy items (since they know that these items are not in the intersection). A careful implementation of this observation, which takes into account timing attacks, can further optimize the computation complexity of the underlying protocols.

The work of [19, 21] gave asymptotic values for the bin sizes that are used with this technique, and of the resulting overhead. They left the task of setting appropriate parameters for the hashing schemes to future work. We revisit the hashing schemes that were outlined in [19, 21], namely, simple hashing, balanced allocations, and Cuckoo hashing (§6.1). We evaluate the performance when using hashing schemes for PSI (§6.2), and describe an analysis of the involved parameters (§6.3). We conclude that Cuckoo hashing yields the best performance (for parameters which we find to be most reasonable).

6.1 Hashing Schemes

Simple Hashing In the simplest hashing scheme the hash table consists of $b$ bins $B_{1\ldots b}$. Hashing is done by mapping each input element $e$ to a bin $B_{h(e)}$ using a hash function $h : \{0,1\}^\sigma \mapsto \{1, b\}$ that was chosen uniformly at random and independently of the input elements. An element is always added to the bin to which it is mapped, regardless of whether other elements are already stored in that bin. Estimating the maximum number of elements that are mapped to any bin, denoted $\max_b$, is a non-trivial problem and has been subject to extensive research [24, 38, 48]. When hashing $m$ elements to $b = m$ bins, [24] showed that $\max_b = \min_{\eta m} (1 + o(1))$ w.h.p. In this case, there is a difference between the expected and the maximum number of elements mapped to a bin, which are $1$ and $O(\frac{\log n}{\ln m})$, respectively. When decreasing the number of bins to a value $b$ satisfying $c \cdot b \ln b = m$ for some constant $c$, it was shown in [48] that $\max_b = (d_c - 1 + \alpha) \ln b$, where $d_c$ is the largest solution to $f(x) = 1 + x (\ln c - \ln x + 1) - c = 0$, and $\alpha$ is a parameter for adjusting the conservativeness of the approximation, and should be set to be slightly larger than $1$. In this case the expected and maximum number of elements mapped to a bin are of the same order $O(\ln b) \approx O(\ln m)$. This is preferable for our purposes, since even though privacy requires that we set each bin to be as large as the most populated bin, this size is of the same order as the expected size of a bin when no privacy is needed.

Balanced Allocations The balanced allocations hashing scheme [2] uses two uniformly random hash functions $h_1, h_2 : \{0,1\}^\sigma \mapsto \{1, m\}$. An element $e$ is mapped by checking which of the two bins $B_{h_1(e)}$ and $B_{h_2(e)}$ is less occupied, and mapping the element to that bin. A lookup for an element $q$ is then performed by checking both bins, $B_{h_1(q)}$ and $B_{h_2(q)}$, and comparing the elements in these bins to $q$. The advantage of this scheme, shown in [2], is that when hashing $m$ elements into $b = m$ bins, $\max_b$ is only $\min_{\eta m} \left( 1 + o(1) \right)$, i.e., exponentially smaller than in simple hashing.

\(^4\)Otherwise, and since the hash function is public, some information is leaked about the input. For example, if no items of $P_1$ were mapped to the first bin by the hash function $h$, then $P_2$ learns that $P_1$ has no inputs in the set $h^{-1}(1)$, which covers about $1/n$ of the input range.
Cuckoo Hashing

Similar to balanced allocations hashing, Cuckoo hashing [46] uses two hash functions \( h_1, h_2 : \{0,1\}^\omega \rightarrow [1, b] \) to map elements to \( b = 2(1 + \epsilon)m \) bins. The scheme avoids collisions by relocating elements when a collision is found using the following procedure: An element \( e \) is inserted into a bin \( B_{h_1(e)} \). Any prior contents \( o \) of \( B_{h_1(e)} \) are evicted to a new bin \( B_{h_2(o)} \) using \( h_1 \) to determine the new bin location, where \( h_i(o) \neq h_i(e) \) for \( i \in \{1, 2\} \). The procedure is repeated until no more evictions are necessary, or until a threshold number of relocations has been performed. In the latter case, the last element is put in a special stash \( s \). It was shown that for a stash of size \( s \leq \ln m \), insertion of \( m \) elements fails with probability \( m^{-\epsilon} \) [33]. A lookup in this scheme is very efficient as it only compares \( e \) to the two items in \( B_{h_1(e)} \) and \( B_{h_2(e)} \) and to the \( s \) items in the stash. In exchange for the improved lookup overhead, the size of the hash table is increased to about \( 2m \) bins.

### 6.2 Evaluation of Hashing-Based PSI

We evaluate the asymptotic overhead of applying the OT-based PSI protocol that was introduced in §5.3 while using any of the hashing scheme that we described. Also note that \( P_1 \) can save communication since instead of sending all masks for each bin (including masks for both dummy and real values), it can send only the masks of its real values (in permuted order, so that \( P_2 \) does not know which value is in each bin). \( P_2 \) can then simply check every mask received from \( P_1 \) against every computed mask. However, in this case the bit-length \( \ell \) of the masks has to be increased to \( \ell' = \ell + \log_2 n_1 + \log_2 n_2 \), since \( P_2 \) has to perform a total of \( n_1 n_2 \) comparisons and the overall error probability must be at most \( 2^{-\epsilon'} \). In the following, we address the mask length for checking one item against a set of \( n_1 \) items as \( \ell_1 = \lambda + \log_2 n_1 \) and the mask length for checking a set of \( n_2 \) items against \( n_1 \) items as \( \ell_2 = \lambda + \log_2 n_1 + \log_2 n_2 \).

PSI based on simple hashing

A protocol based on simple hashing allocates the \( n \) inputs of \( P_2 \) to \( b \) bins, such that \( n = O(b \ln b) \) and \( b \) is approximately \( O(n/\ln n) \). Each bin is padded with dummy items to contain the maximum number of items that is expected in a bin, which is \( O(\ln b) = O(\ln n) \). For each bin, the parties need to compute the intersection between sets of \( O(\ln n) \) items. Each item can be represented using \( O(\ln \ln n) \) bits. The protocol requires \( O(\ln n \ln n) \) random OTs for each bin. The total number of OTs is therefore \( O(n \ln \ln n) \). The length of the values transferred in the OTs (the masks) is \( \ell_2 \ln n \) bits.

PSI based on balanced allocations

A major problem occurs when using balanced allocations hashing for PSI: every item can be mapped to one of two bins, and therefore it is unclear with which of \( P_1 \)'s bin should \( P_2 \) compare its own input elements \( e \). Furthermore, the protocol must hide from each party the choice of bins made by the other party to store \( e \), since that choice depends on other input elements and might reveal information about them. The solution to this is to use balanced allocations by \( P_2 \) alone, whereas \( P_1 \) maps each of its input elements to \( \text{two} \) bins using simple hashing with both hash functions \( h_1 \) and \( h_2 \). When using \( b = n \) bins, \( P_2 \) has \( O(\ln \ln n) \) items in each bin, whereas \( P_1 \) has \( O(\ln \ln n) \) items in every bin (actually, it has twice as many items as with simple hashing, since it maps each item twice). The items can be represented using strings of \( O(\ln \ln n) \) bits. The protocol continues as before. \( P_2 \) learns the output, but since \( P_1 \) does not use balanced allocations, \( P_1 \) does not learn \( P_2 \)'s choices in that hashing scheme. The number of OTs is linear in the number of items stored by \( P_2 \) multiplied by the representation length, e.g., \( O(n \cdot (\ln \ln n)^2) \) OTs on \( \ell_2 \ln n / \ln \ln n \) bit strings. This overhead is larger than that of the simple hashing-based scheme.

PSI based on Cuckoo hashing

Designing PSI based on Cuckoo hashing encounters the same privacy problem as when using balanced allocations hashing, and therefore the same solution is used. \( P_2 \) uses Cuckoo hashing whereas \( P_1 \) maps each of its elements using simple hashing with each of the two hash functions. \( P_2 \) maps a single item to each of the \( 2n \) bins, whereas \( P_1 \)'s \( n \) elements contain \( O(\ln \ln n) \) items in addition. \( P_2 \) has a stash of size \( s = \ln n \) items. Each of these elements must be compared with \( P_1 \)'s \( n \) elements. An item in a bin can again be represented using \( O(\ln \ln n) \) bits, whereas an item in the stash can be represented using \( O(\ln n) \) bits. Furthermore, when checking items in the stash, we check one item against \( n_1 \), allowing us to reduce the bit-size of the masks in the OTs to \( \ell_1 \) instead of \( \ell_2 \). The protocol therefore performs \( O(n \ln \ln n) \) OTs on inputs of length \( O(\ell_2 \ln n) \) bits (for the items in the bins), and in addition \( O((\ln n)^2) \) OTs of inputs of length \( O(\ell_1 \ln n) \) (for the items in the stash, which are each compared to all items of \( P_1 \)'s input). Overall, the protocol has the same asymptotic overhead as the protocol that uses simple hashing.

### 6.3 Maximum Bin Size and Overhead

When using hashing schemes for private set intersection, the number of bins \( b \) and the corresponding maximum bin size \( m_{\text{max}} \) must be set to values that balance efficiency and security. If \( m_{\text{max}} \) is chosen too small, the probability of a party failing to perform the mapping, denoted \( P_{\text{fail}} \), increases. As a result, the output might be inaccurate."
Table 4: Number of OTs and communication for the different hashing-based protocols. The total communication given in the last column is calculated for $\ell_1 = \lambda + \log_2 n$, $\ell_2 = \lambda + 2 \log_2 n$, $\kappa = 128$, $\lambda = 40$, $\epsilon = 0.2$, $s = 4$. The first value in this column is for $t = \sigma = 32$\(^{(2)}\)-OTs per element and the second value is for $t = 32/8$\(^{(2)}\)-OTs, $N = 2^8$. It is composed of the total number of OTs in the 2\textsuperscript{nd} column times the communication per OT plus the communication from $P_1$ to $P_2$ in the 3\textsuperscript{rd} column.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Total # OTs</th>
<th>Comm. [bits] $P_1$ to $P_2$</th>
<th>Comm. [MB] total, $n = 2^n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>No hashing</td>
<td>$nt$</td>
<td>$n^2t_1$</td>
<td>458.880 / 458.784</td>
</tr>
<tr>
<td>Simple Hashing</td>
<td>$3.7nt$</td>
<td>$nt_2$</td>
<td>476 / 121</td>
</tr>
<tr>
<td>Balanced Alloc.</td>
<td>$2.9nt(\ln n)$</td>
<td>$2nt_2$</td>
<td>1,298 / 595</td>
</tr>
<tr>
<td>Cuckoo Hashing</td>
<td>$(2(1+\epsilon)n + s)t$</td>
<td>$nt_2 + 2nt_2$</td>
<td>319 / 89</td>
</tr>
</tbody>
</table>

7 Experimental Evaluation

In the following we experimentally evaluate the PSI protocols described before. We describe our benchmarking environment in §7.1 and then detail the comparison between the protocols in §7.2. Tab. 5 compares the single-threaded runtimes of all protocols over Gigabit LAN, Tab. 6 compares the communication complexities, and Tab. 7 compares the single-threaded runtimes on different networks. In the tables we highlight the protocol with lowest runtime and communication for each type.

7.1 Benchmarking Environment

We ran our experiments on two Intel Core2Quad desktop PCs without AES-NI extension with 4 GB RAM, connected via Gigabit LAN. In each experiment, $P_1$ and $P_2$ held the same number of input elements $n$ and were not allowed to perform any pre-computation. We set $n$ as in [17], i.e., $n \in \{2^{10}, 2^{12}, 2^{14}, 2^{16}, 2^{18}\}$, but omitted $n = 2^{20}$, since many implementations exceeded the available main memory. We use $\sigma = 32$ as the bit length of the elements.\(^6\) We use a statistical security parameter $\lambda = 40$ and a symmetric security parameter $\kappa \in \{80, 128\}$ (other security parameters are chosen according to Tab. 2). For our set-inclusion protocol we set $\eta = 8$, i.e., use 1-out-of-$2^8$ OT extensions.

In our tables, the asymptotic performance is given for the party with the majority of the workload, and are divided to public-key operations (asym) and symmetric cryptographic operations (sym).

Implementations

The implementation of the blind-RSA-based [14] and garbled Bloom-Filter [17] protocols were taken from the authors, but we used a hashable to compute the last step in the blind-RSA protocol that finds the intersection (the original implemen-

\(^6\)For protocols whose complexity depends on $\sigma$, elements from a large domain can be hashed to short representations; cf. full version [47] for details.
tion used pairwise comparisons with quadratic runtime overhead. We implemented a state-of-the-art Yao’s garbled circuits protocol (using garbled-row-reduction, point-and-permute, free-XOR, and pipelining, cf. [28]) by building on the C++ implementation of [12] and using the fixed-key garbling scheme of [7]. For Yao’s garbled circuits protocol, we evaluated a size-optimized version of the sort-compare-shuffle circuit (comparison circuits of size and depth $\sigma$) while for GMW we evaluated a depth-optimized version (comparison circuits of size $3\sigma$ and depth $\log_2 \sigma$) for $\sigma$-bit input values [49].

We implemented FFC (finite field cryptography) and IFC (integer factorization cryptography) using the GMP library (v. 5.1.2), ECC using the Miracl library (v. 5.6.1), symmetric cryptographic primitives using OpenSSL (v. 1.0.1e), and used the OT extension implementation of [1] which requires about 3 symmetric cryptographic operations per OT for the asymptotic performance analysis.

We argue that we provide a fair comparison, since all protocols are implemented in the same programming language (C/C++), run on the same hardware, and use the same underlying libraries for cryptographic operations.

For each protocol we measured the time from starting the program until the client outputs the intersecting elements. All runtimes are averaged over 10 executions.

### 7.2 Performance Comparison

We divide the performance comparison into three categories, depending on whether the protocol is based on public-key operations, circuits, or OT. Afterwards, we provide experiments for different networks and give a comparison between the best protocols in each category.

#### Public-Key-Based PSI

For the public-key-based PSI protocols, we observe that the DH-based protocol of [29] outperforms the RSA-based protocol of [14] when using finite field cryptography (FFC). Similarly to [1], we also obtain the somewhat surprising result that for 80-bit security elliptic curve cryptography (ECC) using the Miracl library is slower than FFC using the GMP library. For larger security parameters, however, ECC becomes more efficient and outperforms FFC by a factor of 3 for 128-bit security for the DH-based protocol. (The reason for this phenomenon might be better implementation optimizations in the GMP library.) The advantage of the ECC-based protocol is its communication complexity, which is lowest among all PSI protocols, cf. Tab. 6. Note that a major advantage of these protocols is their simplicity, which makes them comparably easy to implement.

---

### Circuit-Based PSI

Here we tested Yao- and GMW-based implementations, as well as an implementation of our optimized vector multiplication-triple-based GMW protocol (§3.2). Following is a summary of the results:

- Both the computation complexity and the communication complexity of the circuit-based PSI protocols are the highest among all protocols that we tested.
- The basic GMW protocol has the highest overall runtime and communication complexity.
- Our vector multiplication triple optimization reduces the runtime and communication of GMW by approximately 40%. For security parameter $\kappa = 80$, this implementation is slightly faster than Yao’s protocol, but it is slightly slower for $\kappa = 128$. Communication-wise, the vector multiplication triple GMW is more efficient than Yao’s protocol.
- The runtime of Yao’s protocol hardly increases with the security parameter, since we use AES-128 for both versions. Note, however, that our implementation of Yao’s protocol exceeded the main memory when processing $2^{18}$ elements.
- Our Yao implementation does not use the AES-NI hardware support. Using AES-NI is likely to improve the runtime of the Yao implementation.

We give a more detailed performance comparison for GMW and Yao’s protocol in the full version [47].

### OT-Based PSI

The random garbled Bloom filter protocol of §4.3 improves the original garbled Bloom filter protocol of [17] by more than a factor of two in runtime and by factor of 2-3 in communication.

We also implemented our protocol of §5, where we used Cuckoo hashing with parameters $\varepsilon = 0.2$ and $s = 4$, cf. §6. This protocol had the best runtime, and was about 5 times faster than the random garbled Bloom filter protocol for $\kappa = 128$. In terms of communication, our set inclusion protocol uses less than 20% of the communication of the random garbled Bloom filter protocol for $\kappa = 80$ and less than 10% communication for $\kappa = 128$.

The main difference between the set inclusion protocol and the random garbled Bloom filter protocol is the dependency of the performance on the symmetric security parameter $\kappa$. In the random garbled Bloom filter protocol, the number of OTs is independent of the bit-length $\sigma$ but scales linearly with $\kappa$. On the other hand, the number of OTs for the set inclusion protocol is independent of $\kappa$ but linear in $\sigma$. As a result, the runtime of the Bloom filter protocol (but not the set inclusion protocol) is greatly affected when $\kappa$ is increased.
Table 5: Runtimes in seconds for PSI protocols with one thread over Gigabit LAN ($\sigma = 32$: bit size of set elements, asym: public-key operations, sym: symmetric cryptographic operations).

<table>
<thead>
<tr>
<th>Type</th>
<th>Symm. Security Parameter $\lambda$</th>
<th>80-bit</th>
<th>128-bit</th>
<th>Asymptotic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Size $n$</td>
<td>$2^{10}$</td>
<td>$2^{12}$</td>
<td>$2^{15}$</td>
<td>$2^{18}$</td>
</tr>
<tr>
<td>Public-Key</td>
<td>DH-based FFC [29]</td>
<td>0.4</td>
<td>1.6</td>
<td>6.2</td>
</tr>
<tr>
<td></td>
<td>DH-based ECC [29]</td>
<td>0.7</td>
<td>2.8</td>
<td>11.0</td>
</tr>
<tr>
<td></td>
<td>RSA-based [14]</td>
<td>0.5</td>
<td>2.0</td>
<td>7.9</td>
</tr>
<tr>
<td>Circuit [27]</td>
<td>Yao [7, 28]</td>
<td>1.2</td>
<td>5.7</td>
<td>27.7</td>
</tr>
<tr>
<td></td>
<td>GMW [1]</td>
<td>1.9</td>
<td>8.6</td>
<td>35.2</td>
</tr>
<tr>
<td></td>
<td>Vector-MT GMW [3,2]</td>
<td>1.2</td>
<td>5.1</td>
<td>21.2</td>
</tr>
<tr>
<td>OT</td>
<td>Garbled Bloom Filter [17]</td>
<td>0.3</td>
<td>0.9</td>
<td>3.9</td>
</tr>
<tr>
<td></td>
<td>Random Garbled Bloom Filter [4,3]</td>
<td>0.15</td>
<td>0.5</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td>Set Inclusion $| x |$ + Hashing $| x |$</td>
<td>0.13</td>
<td>0.2</td>
<td>0.8</td>
</tr>
</tbody>
</table>

Table 6: Communication complexity in MB for PSI protocols. ($\sigma = 32$: bit size of set elements, $\kappa, \lambda, \rho, \varphi$ as defined in §2.1). Numbers are computed from the asymptotic complexity given in the last column.

<table>
<thead>
<tr>
<th>Type</th>
<th>Symm. Security Parameter $\kappa$</th>
<th>80-bit</th>
<th>128-bit</th>
<th>Asymptotic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Size $n$</td>
<td>$2^{10}$</td>
<td>$2^{12}$</td>
<td>$2^{15}$</td>
<td>$2^{18}$</td>
</tr>
<tr>
<td>Public-Key</td>
<td>DH-based FFC [29]</td>
<td>0.4</td>
<td>1.5</td>
<td>6.0</td>
</tr>
<tr>
<td></td>
<td>DH-based ECC [29]</td>
<td>0.2</td>
<td>1.0</td>
<td>3.8</td>
</tr>
<tr>
<td></td>
<td>RSA-based [14]</td>
<td>0.3</td>
<td>1.1</td>
<td>4.3</td>
</tr>
<tr>
<td>Circuit [27]</td>
<td>Yao [7, 28]</td>
<td>2.8</td>
<td>15.0</td>
<td>63.0</td>
</tr>
<tr>
<td></td>
<td>GMW [1]</td>
<td>3.1</td>
<td>15.0</td>
<td>70.0</td>
</tr>
<tr>
<td></td>
<td>Vector-MT GMW [3,2]</td>
<td>1.8</td>
<td>9.0</td>
<td>42.0</td>
</tr>
<tr>
<td>OT</td>
<td>Garbled Bloom Filter [17]</td>
<td>3.4</td>
<td>15.5</td>
<td>54.0</td>
</tr>
<tr>
<td></td>
<td>Random ORF [4,3]</td>
<td>1.1</td>
<td>4.5</td>
<td>18.1</td>
</tr>
<tr>
<td></td>
<td>Set Inclusion $| x |$ + Hashing $| x |$</td>
<td>0.2</td>
<td>0.8</td>
<td>3.3</td>
</tr>
</tbody>
</table>

Experiments for Different Networks For each protocol type (public-key-based, circuit-based, and OT-based), we benchmark the best performing PSI protocol in different network scenarios: Gigabit LAN, 802.11g WiFi, intra-country WAN, inter-country WAN, and mobile Internet (HSDPA) and depict our results in Tab. 7. We characterize each network scenario by its bandwidth and latency. By latency we mean one-way latency, i.e., the time from source to sink, and we used the same bandwidth for up- and downlink. We simulated these network types using the Linux command `tc` and ran the protocols on $n = 2^{10}$ elements for $\kappa = 128$ and with one thread.

The only protocol that is nearly unaffected by the change in network environment and for which the network has not become the bottleneck is the DH-based ECC protocol. In this protocol computation is the bottleneck which can be improved by using multiple threads.

For the other protocols we observe how the main bottleneck transitions from computation to communication:

For Yao’s protocol this transition happens very early, already when changing from Gigabit LAN to WiFi (factor 6 in runtime). Our vector-MT GMW protocol and our random garbled Bloom filter protocol suffer less drastically from the decreased bandwidth (factor 2.3 in runtime). However, from the WiFi connection on, the performance of all three protocols decreases approximately linear in the bandwidth. Note that, although our vector-MT GMW protocol has only 66% of the communication complexity of Yao’s protocol, it is more than two times faster in slower networks. This can be explained by the direction of the communication. In Yao’s protocol, the large garbled circuit is sent in one direction, whereas the communication in GMW can be evenly distributed in both directions s.t. it uses both up- and downlink.

For our set inclusion protocol, the network saturation happens when using intra-country WAN. From this point on, the performance also decreases linearly with the bandwidth. Still, this protocol is the fastest of all protocols in all network settings.

Experiments with Multiple Threads Tab. 8 shows the runtimes with four threads. Of special interest is the last column, which shows the ratio between the runtimes with four threads and a single thread for $n = 2^{18}$ elements and security parameter $\kappa = 128$. The DH-based protocol, which is very simple and easily parallelizable, achieves almost the optimal speedup of 4x as computation is the performance bottleneck. The GMW protocol achieves only a speedup of about 2x, possibly due to the gate-by-gate evaluation of the circuit resulting in multiple rounds of communication as the bottleneck. The OT-based protocols achieve a very good speedup of about 3x.

---

8The performance advantage of using fixed-key AES garbling instead of SHA-1/SHA-256 already diminished in the WiFi setting.
Table 7: Runtimes in seconds for PSI protocols with one thread in different network scenarios for \( n = 2^{16} \) elements, \( \sigma = 32 \): bit size of elements, and \( \kappa = 128 \)-bit security (cf. Tab. 2); online time for Vector-MT GMW in ().

Table 8: Runtimes in seconds for PSI protocols with four threads and \( \sigma = 32 \); speedup for \( n = 2^{18} \) and \( \kappa = 128 \).

Comparison From the results we observe that OT-based protocols have the lowest runtime on a fast network. The public-key-based protocols require costly public-key operations, which scale very poorly with increasing security parameter, but need less communication than the OT- or circuit-based protocols. The circuit-based protocols have a smaller runtime than the public-key-based protocols using FFC or RSA for \( \kappa = 128 \), but by far the highest communication complexity.

Our set inclusion protocol achieves both the most efficient runtime and a very low communication overhead. Compared to the second fastest protocol, namely our optimized random garbled Bloom-filter protocol, the set inclusion protocol is at least 5 times faster and uses 10 times less communication (for 128 bit security). Moreover, this protocol has the second best communication overhead, requiring only 3 times the communication of the DH-ECC-based protocol of [29], but running faster in all network environments that we tested.

We stress that the choice of the preferable PSI protocol depends on the application scenario. For instance,

- If communication is the bottleneck and computation is vast, then the DH-based PSI protocol using ECC is the most favorable. That protocol is also the simplest protocol to implement.

- The circuit-based protocols are unique in that they are based on generic secure computation techniques and can therefore be easily modified to compute more complex variants of PSI.

- While our set inclusion protocol performs very efficiently for \( \sigma = 32 \), it would require twice the runtime for \( \sigma = 64 \), while the random garbled Bloom filter protocol would have approximately the same runtime (which would still be greater).

Acknowledgements We thank the anonymous reviewers of USENIX Security 2014 for their helpful comments on our paper. This work was supported by the European Union’s 7th Framework Program (FP7/2007-2013) under grant agreement n. 609611 (PRACTICE), by the German Federal Ministry of Education and Research (BMBF) within EC SPRIDE, by the Hessian LOEWE excellence initiative within CASED, and by a grant from the Israel Ministry of Science and Technology (grant 3-9094).

References


