TVA: A multi-party computation system for secure and expressive time series analytics

Muhammad Faisal, Boston University; Jerry Zhang, University of California San Diego; John Liagouris, Vasiliki Kalavri, and Mayank Varia, Boston University

https://www.usenix.org/conference/usenixsecurity23/presentation/faisal
TVA: A multi-party computation system for secure and expressive time series analytics

Muhammad Faisal  
Boston University

Jerry Zhang  
University of California San Diego

John Liagouris  
Boston University

Vasiliki Kalavri  
Boston University

Mayank Varia  
Boston University

Abstract

We present TVA, a multi-party computation (MPC) system for secure analytics on secret-shared time series data. TVA achieves strong security guarantees in the semi-honest and malicious settings, and high expressivity by enabling complex analytics on inputs with unordered and irregular timestamps. TVA is the first system to support arbitrary composition of oblivious window operators, keyed aggregations, and multiple filter predicates, while keeping all data attributes private, including record timestamps and user-defined values in query predicates. At the core of the TVA system lie novel protocols for secure window assignment: (i) a tumbling window protocol that groups records into fixed-length time buckets and (ii) two session window protocols that identify periods of activity followed by periods of inactivity. We also contribute a new protocol for secure division with a public divisor, which may be of independent interest. We evaluate TVA on real LAN and WAN environments and show that it can efficiently compute complex window-based analytics on inputs of $2^{22}$ records with modest use of resources. When compared to the state-of-the-art, TVA achieves up to $5.8 \times$ lower latency in queries with multiple filters and two orders of magnitude better performance in window aggregation.

1 Introduction

Time series analysis is used by organizations to understand the behavior of non-stationary data, monitor the evolution of metrics over time, identify trends, and predict future outcomes [11, 52, 67]. Time series data are ubiquitous in today’s connected world and crucial for applications in IoT, smart cities, mobile health, traffic monitoring, and stock trading [62, 64, 82]. Applications leveraging multi-origin time series data are highly valuable to communities and businesses alike. For example, a smart grid company can monitor energy consumption across clients to improve conservation and reduce peak demand. Medical investigators can assess a drug’s efficacy on patient cohorts by analyzing physiological signals of many individuals over time. Similarly, a smart city infrastructure can leverage location time series to optimize public transport scheduling. While highly valuable, such analyses raise privacy concerns for data holders, who wish to protect their sensitive or proprietary information.

Cryptographically secure collaborative analytics have recently become more accessible and practical thanks to advances in secure multi-party computation (MPC) [61], fully homomorphic encryption [41], and Oblivious RAM [42, 43]. In this work, we focus on the decentralized trust setting where MPC has been successfully used for machine learning [58, 63, 79, 80], relational queries [60, 65, 75], graph analysis [6], aggregate statistics [3, 14, 50], and other operations such as sorting and PSI [8, 59]. Even though existing MPC-based solutions cover a wide range of collaborative use cases, they are not suitable for analytics on time series data.

Time series computations are commonly expressed with advanced time-oriented operators, called windows [4, 52, 71]. Window operators group events into public metrics and data-dependent values. A session window, for instance, identifies periods of “activity” followed by periods of “inactivity” and can be used to compute analytics such as the average glucose level in a patient cohort during their sleep or their exercise.

The challenge of providing efficient and expressive secure collaborative analytics on time series data has not been successfully addressed yet. Existing approaches either sacrifice expressivity to achieve good performance with strong security guarantees [28] or allow information leakage in return for additional functionality [16, 17]. More importantly, prior works do not support secure windowing and assume regular, ordered, and public timestamps [16, 17, 21, 28, 51, 70]. This assumption is problematic for two reasons. First, missing values...
and out-of-order records are common in practice, as time series data are typically produced by distributed and unreliable sources (e.g., sensors). Second, time series analytics are often performed offline for forecasting and pattern mining [67]. In such cases, timestamps must be protected to prevent untrusted parties from inferring the event distribution and learn sensitive information, such as rare incidents or activities of individuals.

In this paper we present TVA (Time-Varying Analytics), a secure and expressive time series analysis system that leverages outsourced MPC. TVA protects data by distributing trust and generalizes the functionality of prior works without compromising security or performance. To mitigate the tension between these two, TVA employs new protocols, cross-layer optimizations, and vectorized primitives that enable it to scale to large datasets with modest use of resources.

1.1 Limitations of existing systems

TVA addresses the following limitations of prior work:

Lack of advanced window functionality. To extract value from time series data, analysts must be able to query the evolution of metrics over time. Such temporal analysis is typically performed with window operators that group events into consecutive time intervals of fixed (tumbling) or custom (session) length. Waldo [28] is optimized for snapshot queries that operate on a single time interval and, as we show in §6.1, it cannot efficiently perform recurring computations. TimeCrypt [16] and Zeph [17] provide limited support for tumbling windows but also leak information to untrusted parties.

By contrast, TVA is the first system to efficiently support both snapshot and arbitrary recurring queries. It offers generic window operators that can efficiently compute aggregates over fixed and custom time intervals, with strong security guarantees through its black-box use of MPC primitives.

No support for complex filters with keyed aggregations. Besides temporal operators, time series analysis typically requires relational transformations, such as filters, sorting, grouping, and aggregations (keyed and global). These operators must be customizable (to support arbitrary predicates) and composable (to express arbitrary analysis tasks). For example, users should be able to define multiple filter conditions along with complex aggregations on time and any other base or derived attributes. Keyed aggregations allow computing functions on logical partitions of the data, e.g., the hourly energy consumption per postcode. Prior work either supports global aggregation only [28] (total consumption for all postcodes) or allows limited additive keyed aggregation by requiring data holders to pre-encode the attribute domain (all possible postcodes) and to periodically transmit values [17, 51].

In contrast, TVA’s aggregation operators can be composed with any operator and can be also chained. For instance, TVA can compute the average energy consumption per postcode over 1-hour windows, which can then be used to compute the maximum average consumption across all windows.

No support for unordered and irregular timestamps. Time series data are commonly produced by distributed sources, such as sensors or wearable devices. As a result, events may be ingested out of order due to network delays and clock skew. Furthermore, sources may transmit data at a fixed frequency (e.g., heart rate every minute) or only when an event occurs (e.g., smoke is detected). State-of-the-art approaches assume in-order and regular timestamps [16, 17, 21, 28, 51, 70], that is, they expect data owners to provide data at fixed time intervals. As a result, data sources must pad the time series with dummy records when events are missing and pre-aggregate events locally when the event generation frequency is higher than the transmission rate. This approach simplifies the problem of providing privacy-preserving time series analytics, since regular and ordered timestamps do not reveal any information (other than the time domain) and can thus be kept public. However, it has two considerable drawbacks. First, when the time series events are irregular, padding can lead to significant communication and computation costs. Second, pre-aggregation comes at loss of data granularity and accuracy. Subsequent queries can only return exact results on time intervals that are multiples of the pre-aggregation bucket size.

On the contrary, TVA does not require the input time series to be regular and ordered by time. Both window and snapshot operators can correctly and efficiently operate on unordered and irregular timestamps, which are protected like all other data attributes. Due to its ability to operate on private time series data, TVA can serve queries on both recent and historical data collected independently by different entities, without revealing the event distribution to computing parties.

1.2 Summary of contributions

Protocols for secure window assignment (§4.1–§4.4). We present the first oblivious algorithms for (global and keyed) tumbling and session window assignment on private time series data. We analyze the complexity of our protocols and prove their correctness and security guarantees.

Our tumbling window protocol relies on a new MPC primitive for secure division with public constants. The state-of-the-art protocols for fast division produce small errors that are acceptable in other use cases (e.g., machine learning applications [63]) but cause incorrect aggregation results in our setting, as records end up in wrong windows with high probability. To address this challenge, we propose error correction protocols for semi-honest and malicious-secure division that can be used to compute tumbling windows with a number of communication rounds independent of the time series size.

For session windows, the plaintext algorithms [4, 71] traverse the time series and update session boundaries while keeping track of the last open session. Although simple, an oblivious implementation of this technique would incur a pro-
efficient implementations of oblivious operators and vectorized MPC primitives that amortize the communication costs of MPC. We also develop a declarative and protocol-agnostic query API that hides the complexity of composition from end users. All experiments we present in this paper use real LAN and WAN deployments. We have implemented the TVA software stack entirely from scratch, and the software is available as open source [34].

2 TVA in a nutshell

Figure 1 provides an overview of TVA. Data owners are individuals or entities who have agreed to contribute their private data towards a joint analysis (e.g., a medical study, a smart grid monitoring task, etc.), provided that the data remain hidden from untrusted parties. Data analysts are individuals who perform the analysis using TVA. To do so, they access a public catalog of time series metadata (cf. §3) and submit queries to the system. A computing party is a logical entity that may consist of multiple compute nodes (TVA servers). Computing parties are deployed in different trust domains (e.g., competing cloud providers) and can be configured to execute queries either with malicious (default) or semi-honest security, depending on the use case.

TVA operates in the outsourced setting [23], that is, it does not require data owners or analysts to participate in the computation (both can be offline during the analysis). Each data owner interacts with the computing parties independently from others, and only to distribute secret shares of their data.

We emphasize that the security of TVA stems from its data-oblivious execution (so the parties learn nothing beyond the result of the query) and access control (so even the result is only revealed to designated data analysts). In particular, TVA does not protect against inference attacks on the input based on the query results. Combining TVA with differentially private algorithms for time series data (e.g., [37, 38, 55, 77]) remains an exciting possibility for future work.

2.1 Supported workloads

TVA offers a rich set of temporal and time-agnostic operators that can be composed arbitrarily to define complex time series analysis tasks.

Temporal operators. TVA’s temporal operators can be used to express (i) snapshot queries that compute an aggregate over a specific time interval, and (ii) window queries that...
compute an aggregate over multiple time intervals defined by a windowing strategy. Consider a time series dataset collected from a heart rate tracker, a movement sensor, and a glucose monitor. Figure 2 illustrates TVA’s windowing strategies using a digital health use case as an example.

A tumbling window operator (top) divides the time domain into non-overlapping intervals of equal length $\lambda$ so that each input record belongs to exactly one window. For example, the tumbling window can be used to compute "the maximum heart rate per minute across individuals in a cohort".

A session window operator groups records into periods of activity (sessions) followed by periods of inactivity [4]. Session windows have variable and data-dependent length in time units. The gap window (middle) uses a timeout gap $\tau$ as the session delimiter. All records whose time difference is within an interval up to the timeout $\tau$ are grouped together into the same session. The end of a session is detected when the time difference between two consecutive records is greater than $\tau$. A gap-based window could be used to compute an aggregate over “time periods when an individual is moving”.

The threshold window operator (bottom) interprets sessions using a threshold $\theta \in \mathbb{R}$ and a function $q : S \rightarrow \mathbb{R}$, where $S$ is collection of data records. All consecutive records whose value $q(r), r \in S$, is at least equal to the threshold $\theta$ are grouped into the same session. The current session ends when a record with value below $\theta$ is detected. For example, a threshold window can identify “eating periods when the glucose level exceeds a threshold”. As shown in Figure 2, although every input record belongs to exactly one gap window, some records may not belong to any threshold window.

**Time-agnostic operators.** TVA provides a set of time-agnostic operators that can be combined with temporal operators. These include filtering, sorting, grouping, distinct (for duplicate elimination), and all common aggregations, i.e., COUNT, SUM, MIN, MAX, TOP-K, AVG, STDEV, and PERCENTILE. Additionally, TVA supports arbitrary User-defined Functions (UDFs) constructed with its secure primitives. Those include logical and arithmetic operations provided by the protocols ($\land, \lor, \oplus, +, -, \ast$), boolean addition, comparison operators ($\leq, \geq, =, \neq$), and division with public constant.

### 2.2 Putting it all together: the TVA API

TVA exposes a high-level declarative API that lets users combine temporal operators with arbitrary filters, aggregations, and other time-agnostic operators. The API specification is given in the full version of this work [33]. Listing 1 shows an example query that computes a keyed tumbling window on the dataset of Figure 2. To maximize readability, TVA’s API lets users refer to data attributes by name, as shown in the example code snippet. Once the data schema is defined, attribute names can be used as operator arguments. The query first selects records corresponding to patients weighting between 190 and 250 pounds and applies the keyBy operator to partition these records by age group. It then computes the maximum heart rates over 1-hour tumbling windows for each age group. The result is a new time series $hr$ that can be given as input to another query.

```java
// Define the time series data schema
TS ts = get_shares(["TIMESTAMP", "WEIGHT", "AGE_GROUP", "HEART_RATE", "MOVEMENT", "GLUCOSE", "MAX_RATE"]);

// Compute the max hourly heart rate per age group over
// all participants whose weight is within a given range
TS hr = ts.filter("WEIGHT" > 190 AND "WEIGHT" < 250)
    .keyBy("AGE_GROUP")
    .tumbling_window("TIMESTAMP", 3600)
    .aggregate("HEART_RATE", "MAX_RATE", Agg::MAX);
```

Listing 1: An example tumbling window query using the TVA API

Analysts submit queries like the one above to TVA parties for execution and TVA compiles them into a secure MPC program. The query structure is public but the filter predicates and the queried time intervals are secret-shared by the TVA client application (run by the analysts).

### 3 Threat model and security guarantees

TVA protects all data, including timestamps, throughout the entire lifecycle of computations. Overall, TVA protects data privacy using non-colluding computing parties, authenticated network links, and end-to-end oblivious computation. TVA does not reveal any private inputs or intermediate data during the computation and only opens the final query result to the designated analysts. Some metadata about the time series is purposely made public and accessible to the data analysts so they can create their queries; the public metadata include the data schema, the type and number of columns, and the number of input records, as in prior works [16, 17, 28].
Setting. TVA assumes that data owners and analysts have previously agreed on a query to compute. The query structure is known to the computing parties, but predicates are protected with secret sharing. In particular, parties know the type of operators they compute (e.g., the window type or aggregation function) but TVA protects the actual filter values and the session window predicates (gap and threshold). Protecting these parameters ensures that the computing parties do not learn any specific time intervals that are being queried. When a tumbling window operator is used, TVA treats the window length as public. We emphasize that knowledge of the length does not reveal anything about specific time intervals, since the window operator is applied on the entire time series dataset. In the example of Listing 1, TVA parties know that the query involves a filter of the form "WEIGHT > X AND "WEIGHT" < Y followed by keyed window aggregation (MAX) per hour, but they do not learn the filter values 190 and 250.

Protocols. TVA currently provides two replicated secret sharing protocols with $N$ parties: (i) the semi-honest 3-party protocol by Araki et al. [5] ($N = 3$) and the malicious-secure Fantastic Four protocol by Dalskov et al. [26] ($N = 4$). We encode an $\ell$-bit string of secret data $s$ by splitting it into $N$ shares that individually have the uniform distribution over all possible $\ell$-bit strings (for privacy) and collectively suffice to specify $s$ (for correctness). Share generation is cheap and is done locally by the data owners. Each party $P_i$ receives $N - 1$ of the shares; hence, any two parties can reconstruct the secret but any single party cannot. TVA supports both boolean secret sharing $\{0,1\}$ of length-$\ell$ bitstrings and arithmetic secret sharing $\langle x \rangle_\ell$ in the ring mod 2$^\ell$, as well as primitives to convert one format to the other. By convention, we say that party $i$ holds the shares $x_i$ and $x_{i+1}$ for 3-party replicated sharing, or $x_i, x_{i+1}, x_{i+2}$ for 4-party replicated sharing.

Threat model. TVA supports either semi-honest or malicious security in the honest majority setting. When operating with semi-honest security, TVA can withstand adversaries who have three types of capabilities: (i) complete control over the network, (ii) the ability to compromise at most one computing party and passively eavesdrop on its internal state (e.g., memory contents, access patterns, and data sent/received) without altering its execution, and (iii) the ability to collude with one or more data owners to learn inputs into the query, or with the data analyst to learn the output of the query. When operating in the malicious setting, the adversary can additionally force the compromised computing party to actively deviate from the protocol arbitrarily. In this case, TVA provides security up to abort: the honest computing parties will stop and report an error to the analyst.

Security guarantees. TVA offers two types of security guarantees: (i) privacy, meaning that computing parties do not learn anything beyond the public metadata and the information held by any data owners or analysts they are colluding with, and (ii) correctness, meaning that all participants are convinced that the computation output is accurate. TVA inherits both guarantees from the underlying MPC protocols by always operating over secret-shared data using the underlying MPC primitives in a black-box manner, ensuring an oblivious control flow for each operator individually (§4.1-4.4) and jointly (§4.6), and never opening any intermediate results.

To show this claim formally, in this work we perform security analysis in the arithmetic black-box model, as shown in Appendix A. This is a hybrid model in which we presume the existence of a functionality $\mathcal{F}_{\text{ab}}$ that provides perfect correctness and privacy for the following operations: $\mathcal{F}_{\text{ab}}$, input and $\mathcal{F}_{\text{ab}}$, output to share and reconstruct secrets in either arithmetic or boolean representations, $\mathcal{F}_{\text{ab}}$, add and $\mathcal{F}_{\text{ab}}$, mult to compute arithmetic (mod 2$^k$) or multi-bit boolean (mod 2$^k$) operations, and $\mathcal{F}_{\text{ab}}$, A2B and $\mathcal{F}_{\text{ab}}$, B2A to convert between the two representations. In the malicious setting, we also consider a shared input functionality $\mathcal{F}_{\text{ab}.\text{INP}}$ in which two parties provide as input a common secret that they both wish to be shared, and the functionality detects and aborts if there is a discrepancy between the two. For readability, we sometimes use informal notation (e.g., $\langle [a], [b] \rangle = [a/b]$) rather than formal notation (e.g., $\mathcal{F}_{\text{ab}}$, mult(boolean, id$_a$, id$_b$, id$_c$)) in this work.

### 4 Secure time series data analysis in TVA

In this section, we describe TVA’s oblivious operators for secure time series analysis. In §4.1, we describe our division protocol that is the core building block of the tumbling window operator in §4.2. In §4.3 and §4.4, we present two session window operators and, in §4.5, we discuss time-agnostic operators supported by TVA. Finally, in §4.6, we describe TVA’s efficient composition techniques for creating complex time series analysis tasks. Table 1 summarizes the notation.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\langle x \rangle_\ell$</td>
<td>replicated boolean secret share of the length-$\ell$ bitstring $x$</td>
</tr>
<tr>
<td>$\langle [a], [b] \rangle$</td>
<td>replicated arithmetic secret share of $a$ in the ring mod 2$^k$</td>
</tr>
<tr>
<td>$\langle s \rangle_\ell$</td>
<td>non-replicated 2-of-$\ell$ arithmetic secret share of $s$ in the ring mod 2$^\ell$</td>
</tr>
<tr>
<td>$r$</td>
<td>length of a share representation in bits</td>
</tr>
<tr>
<td>$s$</td>
<td>maximum length, in bits, for dividend $x$ in the division protocols</td>
</tr>
<tr>
<td>$t$</td>
<td>bitlength of the public divisor $c$ (in the division protocols) plus one</td>
</tr>
<tr>
<td>$\gamma$</td>
<td>a data record of the form $r = (t, a_1, a_2, \ldots, a_k)$, where $t$ is the record’s timestamp and $r.a_i, 1 \leq i \leq k$, is a data value</td>
</tr>
<tr>
<td>$\delta$</td>
<td>a time series of size $</td>
</tr>
<tr>
<td>$\mathcal{F}_{\text{ab}}$</td>
<td>a window in a time series $X$, i.e., a collection of data records $W \subseteq S$</td>
</tr>
<tr>
<td>$\delta$</td>
<td>length of a tumbling window in time units</td>
</tr>
<tr>
<td>$\gamma$</td>
<td>timeout interval that defines a gap session window</td>
</tr>
<tr>
<td>$\mathcal{F}_{\text{ab}.\text{INP}}$</td>
<td>threshold value that defines a threshold session window</td>
</tr>
<tr>
<td>$\mathcal{F}_{\text{ab}}$, sort operator on key $k$</td>
<td>sort operator on key $k$</td>
</tr>
<tr>
<td>$\mathcal{F}_{\text{ab}}$, group-by operator on key $k$</td>
<td>group-by operator on key $k$ with aggregation function $G$</td>
</tr>
</tbody>
</table>

Table 1: Notation used in the paper
Protocol 1: DIVISION (semi-honest 3PC)

Input: Arithmetic sharing $\langle x \rangle_x$ of a secret $x \in [0, 2^c)$
Public integer $c \in \{1, 2^{c-1}\}$

Output: Quotient $\langle y \rangle_y$ computed as follows.
1. Construct a 2-of-2 sharing $\langle y \rangle_y$ of $y = z$ as follows:
   1.1 Party 1 locally computes $y_1 = \frac{(x_1 + x_2)}{c}$
   1.2 Parties 2, 3 locally compute $y_2 = 2^c - \left\lfloor \frac{(2^c - x_3)}{c} \right\rfloor$
2. Construct 2-of-2 sharing $\langle s \rangle_1$ of $s$ computed as follows:
   2.1 Party 1 locally computes $s_1 = (x_1 + x_2) \mod c$
   2.2 Parties 2, 3 locally compute $s_2 = (2^c - x_3) \mod c$
3. Create replicated sharings $\langle y \rangle_y, \langle s \rangle_1$ as follows:
   3.1 Use $F_{\text{arb}}.\text{input}$ to share $y_1$ and $y_2$ in the ring mod $2^c$
   3.2 Use $F_{\text{arb}}.\text{input}$ to share $s_1$ and $s_2$ in the ring mod $2^c$
   3.3 Locally compute $\langle s \rangle_1 = \langle s_1 \rangle_1 - \langle s_2 \rangle_1$ using $F_{\text{arb}}.\text{add}$
4. Calculate replicated sharing $\langle b \rangle_b$ of the bit $b = (s_1 \leq s_2)$:
   4.1 Use $F_{\text{arb}}.\text{A2B}$ to convert $\langle s \rangle_1$ into boolean shares $\langle x \rangle_x$
   4.2 Set $\langle b \rangle_b$ equal to the most significant bit of $\langle x \rangle_x$
   4.3 Use 1-bit conversion $F_{\text{arb}}.h2A$ on $\langle b \rangle_b$ to compute $\langle b \rangle_b$
5. Locally compute $\langle z \rangle_z = \langle y \rangle_y - \langle b \rangle_b$ using $F_{\text{arb}}.\text{add}$

Protocol 2: DIVISION (malicious 4PC)

Input: Arithmetic sharing $\langle x \rangle_x$ of a secret $x \in [0, 2^c)$
Public integer $c \in \{1, 2^{c-1}\}$

Output: Quotient $\langle y \rangle_y$ computed as follows.
1. Construct a 2-of-2 sharing $\langle y \rangle_y$ of $y = z$ as follows:
   1.1 Parties 1 and 4 compute $y_1 = \frac{(x_1 + x_2)}{c}$
   1.2 Parties 2 and 3 compute $y_2 = 2^c - \left\lfloor \frac{(2^c - x_3 - x_4)}{c} \right\rfloor$
2. Construct 2-of-2 sharing $\langle s \rangle_1$ of $s$ computed as follows:
   2.1 Parties 1 and 4 compute $s_1 = (x_1 + x_2) \mod c$
   2.2 Parties 2 and 3 compute $s_2 = (2^c - x_3 - x_4) \mod c$
3. Perform lines 3-5 of Protocol 1, replacing all instances of $F_{\text{arb}}.\text{input}$ with the Shared Input functionality $F_{\text{arb}}.\text{INP}$

Indexed in ascending order of their timestamps, i.e., $\forall r_i, r_j \in S, r_i \leq r_j \iff i < j \leq |S| \in \mathbb{N}$. We stress that record indices are only used to simplify the presentation and TVA does not assume records to be physically ordered on their timestamps.

TVA window operators are applied to time series and generate new time series. In practice, windowing is performed by appending to each record a new attribute $\omega_t$ that contains a secret-shared window id computed under MPC.

4.1 Integer division by public divisor

TVA assigns records to tumbling windows by discretizing timestamps based on the window length (in time units). Several prior works provide efficient protocols for integer or fixed-point division, but they typically introduce a small rounding error, truncate only by powers of two, or are slow because they provide features that we do not need in our setting like perfect accuracy or private divisors (e.g., [19, 20, 25, 32, 32, 36, 63, 74]).

In this work, we contribute a new secure computation protocol for division-and-truncation, given mixed-mode MPC with replicated secret sharing, that can perform division by any public divisor without a rounding error. For our application to tumbling windows, having some noticeable probability of error means that many data records are being assigned to the wrong window, which could significantly distort the subsequent time series analysis. That said, for improved efficiency we do allow for $\epsilon$ negligible error with probability $2^{-\sigma}$, which is parameterized by a statistical security parameter $\sigma$.

For simplicity, we show the TVA division algorithms in Protocols 1 and 2 in the case that the secret dividend $x$ and public divisor $c$ are unsigned (positive) integers. This suffices for our application, in which the dividends $x$ are timestamps and the window lengths $c$ are a positive number of time units. It is straightforward to extend our protocols to support signed fixed-point numbers, as long as the absolute value of the divisor is at least 1 (otherwise there is a risk of overflow).

For semi-honest 3-party MPC, our starting point is the probabilistic truncation protocol of Mohassel and Rindal [63], which can perform probabilistic truncation with only one round of communication. Their technique roughly corresponds to step 1 of Protocol 1. Starting from a dividend that is at most $\ell_t$ bits long ($x < 2^{\ell_t}$) and public divisor $c < 2^{\ell_t-1}$, step 1 computes a non-replicated 2-of-2 arithmetic sharing $\langle y \rangle_y$, which we later convert to a replicated secret sharing in step 3. The value $y$ is close to the correct quotient $z = \left\lfloor \frac{x}{c} \right\rfloor$, but $y$ has two possible sources of error: an off-by-one rounding error occurs with probability $\approx 1/2$ (namely, when the fractional part of $\frac{x_s}{c}$ is greater than the fractional part of $\frac{x_{s+1}}{c}$), and a large error occurs with negligible probability (when $x_3 < x$).

In lines 2-5 of Protocol 1, we compute the rounding error within MPC itself so we can eliminate it. In step 2, we calculate the fractional parts $s_1$ and $s_2$ that were the source of the potential off-by-one error. Then, we use mixed-mode operations to calculate the error bit $b$ based on whether $s_1 < s_2$. We calculate this inequality by computing $s = s_1 - s_2$ mod $2^c$, where $\ell_c = |c| + 1$, and converting to boolean shares in order to isolate the most significant bit of $\langle s \rangle_1$ and set it equal to $\langle b \rangle_b$.

Protocol 1 makes only black-box use of mixed-mode MPC operations. This leads to a simple extension of our division algorithm to the malicious 4-party MPC setting, as shown in Protocol 2 where we achieve malicious security through redundancy. Specifically, we ensure that two parties perform each calculation; then, using the Shared Input (INP) protocol within Dalskov et al. [26], the honest parties can detect any discrepancy between them. Modularity also simplifies both the security analysis and the resulting implementation within TVA. In the full version [33], we prove that Protocols 1-2 are private and correct with probability $1 - 2^{-\sigma}$, where $\sigma = \ell - \ell_c$.

Protocols 1-2 require $\log(\ell_c) + 3$ communication rounds and $2\ell_c + 2\log(\ell) + 1$ total bits of communication (plus some small additive overhead in the 4-party case to send the hashes in the protocol of Dalskov et al. [26]). Concretely, line
3 requires one communication round to distribute shares, line 4 requires \( \log(\ell_c) + 1 \) rounds to perform the arithmetic-to-boolean conversion using a Parallel Prefix Adder (PPA) [48] plus one round for the subsequent bit-to-arithmetic conversion, and the remaining lines do not require any communication. See the full version of this work [33] for a longer comparison of this division protocol with closely related works.

### 4.2 Tumbling window

We can now describe TVA’s tumbling window operator. Let \( S \) be a time series, \( \lambda \in \mathbb{N}^+ \) a window length (in time units), and \( G \) an aggregation function on data records.

**Definition 1 (Tumbling Window Operator)** Given a window length \( \lambda \) and an aggregation function \( G \), TVA’s tumbling window operator \( T \) defines a new time series as follows:

\[
T_G(S, \lambda) = \{(k, G(W_k)) \mid W_k = \{r_i \in S \mid \lambda \cdot k \leq r_i.t < \lambda \cdot (k + 1), k \in \mathbb{N}\}
\]

The new time series defined by the tumbling window operator contains records of the form \( r = (t, G(W_k)) \), where \( t = k \) is the timestamp of the new record, \( W_k \) is the \( k \)-th tumbling window, i.e., the collection of records that fall into the time interval \( \lambda \cdot k \leq r_i.t < \lambda \cdot (k + 1) \), and \( G(W_k) \) is the result of the aggregation function on \( W_k \).

The secure tumbling window operator works as follows. First, parties iterate over the records’ shares in the time series \( S \) and compute the discretized timestamps \( \frac{t}{\ell} \) by executing the secure division protocol (Protocols 1 and 2). All these divisions are independent of each other and are performed in bulk, i.e., they can all be completed in \( \lceil \log(\ell_c) \rceil + 3 \) total rounds. The output of each division amounts to the tumbling window id \( w_{i.d} \) of the respective record and is appended to the record as a new attribute\(^1\). In the next step, parties apply the aggregation function \( G \) to the collection of records in each window. To do so, they group records by their window ids using TVA’s group-by operator \( \gamma \) that is based on the protocol by Jönsson et al. [54] (cf. §4.5-4.6). The output of the operator is a new time series \( S' = \gamma^G_{w_{i.d}}(S) \) with one record per window containing the result of the aggregation \( G \).

### 4.3 Gap-based session window

Computing sessions under MPC is challenging, as windows can be of variable length that depends on the data. Let \( S \) be a time series and \( \ell \in \mathbb{N}^+ \) a timeout (in time units). Let also \( \delta : \mathbb{N} \rightarrow \mathbb{R}_+ \cup \{\infty\} \) be a function that computes the time difference between consecutive records in \( S \) as shown below:

\[
\delta(i) = \begin{cases} r_i.t - r_{i-1}.t, & 1 \leq i < |S| \\ \infty, & \text{otherwise} \end{cases}
\]

\(^1\)If the record timestamp is not needed in a subsequent step of the analysis, TVA can simply overwrite it with \( w_{i.d} \) instead of appending a new attribute.

---

**Protocol 3: SESSIONIZATION**

**Input**: A time series \( S = \{r_0, r_1, \ldots, r_{|S|-1}\} \)

**Result**: The updated time series with all sessions marked

1. **SESSIONSTART(S)**: //First phase
2. Let \( \delta = 1 \); //Distance between records in \( S \)
3. **while** \( |S| - d \) **steps are independent**
   **do**
   **for** \( i = 0 \); \( i < |S| - d \); \( i++ \) **do**
   4. Parties locally compute bit \( b[\delta] \) for \( b = (r_{i+d}.w_{i+d} < 0) \)
   5. Parties locally compute mask \([m]_\ell = \text{expand}([b]_1, \ell)\)
   6. Parties compute the window id of \( r_{i+d} \) as follows:
      \[r_{i+d}.w_{i+d} = \omega([m]_\ell \land [r_i.t]_\ell) \land [w_{i.d}]_\ell\]
4. **end**
5. \( d \leftarrow d + 2\)

**Protocol 4: SESSIONSTART (GAP)**

**Input**: A time series \( S = \{r_0, r_1, \ldots, r_{|S|-1}\} \), a timeout \( \ell \)

**Param.**: Function \( \delta \) (Eq. 1), timestamp length \( \ell \) (in bits)

1. \( s_{\ell}(S) \): //Sort records by timestamp (ASC)
2. Let \( \epsilon = 1 \) be an invalid timestamp; //Negative number
3. **for** \( i = 0 \); \( i < |S| \); \( i++ \) **do**
   4. Parties compute bit \( b[\delta] \) for \( b = (r_i.t < \epsilon) \)
   5. Parties locally compute mask \([m]_\ell = \text{expand}([b]_1, \ell)\)
   6. Parties compute the window id of \( r_i \) as follows:
      \[r_i.w_{i.d} = \omega([m]_\ell \land [r_i.t]_\ell) \land [w_{i.d}]_\ell\]
4. **end**

**Definition 2 (Gap Window Operator)** Given \( \delta \) and an aggregation function \( G \), TVA’s gap window operator \( \Gamma \) defines a new time series as follows:

\[
\Gamma_G(S, \delta, \tau) = \{(r_i.t, G(W_i)) \mid W_i = \{r_i \mid 0 \leq s \leq i \leq e < |S|, \delta(s) > \tau, \delta(e + 1) > \tau, \forall r_j \in S : \delta(j) > \tau, s < j \leq e\}
\]

Records in the new time series have the form \( r = (t, G(W_i)) \), where \( W_i \) is a gap session window, \( t = r_i.t \) is the earliest timestamp in \( W_i \), and \( G(W_i) \) is the result of the aggregation function \( G \) on \( W_i \). The most expensive condition in the gap session window operator is the last one: \( \forall r_j \in S : \delta(j) > \tau, s < j \leq e \). This condition requires identifying pairs of records \( r_i \) and \( r_e \) with no in-between records \( (r_c \text{ included}) \) that belong to a different session. Given a time series \( S \) sorted by timestamp, the straightforward approach to evaluate this condition is to scan \( S \) and keep track of the current session by applying function \( \delta \) to each pair of adjacent records. This approach, however, incurs prohibitive communication overhead, as it requires communication rounds linear to the number of records in \( S \). Instead, we propose an efficient two-phase SESSIONIZATION protocol (Protocol 3) that can
correctly identify all session windows in $S$ with a logarithmic number of rounds. We discuss the phases of the protocol next:

**Phase 1: Mark the beginning of each session.** In this phase, parties identify the beginning of each gap session window as shown in Protocol 4. To do so, they first order records on their timestamp using TVA’s oblivious sort operator (this step can be omitted if records arrive in order). Next, they compare adjacent records by applying function $\delta$ (Eq. 1) using a PPA. Given a timeout $\tau$, a new session is marked at $r_i$ iff $\delta(i) > \tau$; the result of this inequality is saved as a bit $b$. Next, we expand the single bit $b$ into a mask $m$ of length $\ell$, such that every bit of $m$ is equal to $b$. Parties set the window id of each record using an oblivious multiplexer of the form $m \land x \oplus \overline{m} \land y$, where $m$ is a mask, and $\overline{m}$ is its boolean complement. Hence, if a record $r_i$ marks the start of a new window, parties set $w_{id} = r_i$; otherwise, they use an invalid timestamp $\epsilon$ (e.g., a negative constant like $-1$) to denote that this record is currently unassigned. All steps of the for-loop in the first phase of the protocol do not depend on each other and incur a number of rounds that is independent of the time series size. That is, executing steps 3–7 in $\text{SESSIONSTART}(\text{GAP})$ requires $2\lceil \log(\ell + 1) \rceil + 1$ rounds in total, where $\ell$ is the length of the timestamp representation in bits (fixed).

**Phase 2: Assign records to sessions.** In the second phase of TVA’s $\text{SESSIONIZATION}$ (steps 2–10 in Protocol 3), parties assign the remaining records to their corresponding session in $\lceil \log|S| \rceil$ rounds. This is done by replacing the negative $w_{id}$ of each unassigned record with the non-negative $w_{id}$ of the nearest preceding record. Records in $S$ are guaranteed to be in order after the first phase, therefore, the earliest record in each session always precedes the remaining unassigned records. Our protocol leverages this ordering to reduce interaction during window assignment as follows. In the first iteration, parties examine adjacent records at distance $d = 1$ starting from the first record in $S$. If $r_{i+d}, w_{id} < 0$ (unassigned), it is overwritten by $r_i$, otherwise it is left as is. This is done using an oblivious multiplexer and a mask $m$ that is generated locally, as in the first phase. Step 5 is local because $b$ corresponds to the sign of $r_{i+d}, w_{id}$, i.e., its most significant bit. At the end of each iteration, parties double the distance $d$ of the previous step and repeat the same process. All for-loop iterations in the second phase of the protocol are independent one another, i.e., executing steps 4–8 in $\text{SESSIONIZATION}$ requires a single round (due to multiplexing), for any time series $S$. The overall control flow has a butterfly-like structure that has been used for multi-set operations [10] (e.g., to compute cardinality) and element compaction [44]. In TVA, we leverage this technique to perform sessionization and, as we show in §4.6, efficient composition with window aggregation for a wide range of functions. We prove the correctness and privacy of our protocol in the full version of this work [33].

When sessionization terminates, parties can use TVA’s group-by operator to apply the aggregation function $G$ to each window. As the number of records grows, TVA’s operator $\Gamma$ takes $O(\log^2|S|)$ rounds and $O(|S|\log^2|S|)$ communication if records arrive out of order, since TVA relies on bitonic sort (§4.5). For ordered timestamps, the asymptotic costs are $O(\log|S|)$ and $O(|S|\log |S|)$ respectively.

### 4.4 Threshold-based session window

TVA’s threshold window operator works similarly to gap session window. Let $g : S \rightarrow \mathbb{R}$ be a function on data records in a time series $S$. In its simplest form, $g$ is a function that returns a record’s attribute but, in general, it can be any function constructed using TVA’s primitives. Let $h : \mathbb{N} \rightarrow \mathbb{R} \cup \{-\infty\}$ be the function:

$$h(i) = \begin{cases} \theta(r_i), & 0 \leq i < |S| \\ -\infty, & \text{otherwise} \end{cases}$$

**(Definition 3 (Threshold Window Operator))** Given $h$ and an aggregation function $G$, TVA’s threshold window operator $\Theta$ defines a new time series as follows:

$$\Theta_{G,h}(S, \theta) = \{(r_s, \theta, G(W_s)) | W_s = \{r_i \}, 0 \leq s \leq i \leq e < |S|, h(s) \geq \theta, h(s-1) < \theta,$$

$$h(e) \geq \theta, h(e+1) < \theta, s \leq j < e \}$$

The boundaries of a threshold window $W_s$ are defined by a pair of records $r_s$ and $r_e$ that satisfy all conditions above. TVA identifies threshold windows using the same oblivious control flow from Protocol 3. The main difference with respect to gap session windows lies in the first phase of sessionization that is described in Protocol 5. In this case, parties identify the beginning of each threshold window by applying function $h$ (Eq. 2) to each record in $S$. A session starts at $r_i$ iff $h(i) \geq \theta$ and
h(i - 1) < θ. To keep track of records that do not belong to any threshold window, parties store the result of the comparison h(i) ≥ θ in a new single-bit attribute aθ that is appended to record rj. This bit is used in an oblivious multiplexer to mark the beginning of each session and is reused in the second phase of the protocol, as we describe later. Executing steps 3-11 in SESSIONSTART (THRESHOLD) requires Rq + log(ℓ + 1) rounds, where Rq is the number of rounds required to apply q to a single record (independent of |S|). In the common case where q(r) = r.aθ, 1 ≤ i ≤ k, we have Rq = 0.

During the second phase, parties execute steps 2-10 in Protocol 3 with a minor change in step 5 that is now replaced by the operation \[ [b]_1 = [[r_{i+d}.wd] \land [r_{i+d}.aθ]_1. \]
For threshold windows, b is a composite bit that denotes whether record r_{i+d} belongs to a threshold window (r_{i+d}.aθ = 1) and is currently unassigned (r_{i+d}.wd = 0). Computing b requires a single round between parties since both r_{i+d}.aθ and r_{i+d}.wd have been computed in the previous phase. As a result, steps 4-8 in SESSIONIZATION require two rounds in total for threshold windows (one more compared to gap session windows).

The final aggregation step and the overall asymptotic costs in terms of rounds and bandwidth for threshold windows are the same with gap windows, as given in §4.3. We prove the correctness and privacy of our protocol in the full version [33].

4.5 Other TVA operators

In addition to windows, TVA provides a rich set of oblivious operators for secure time series analysis, namely, snapshot, filter, sorting, grouping, and distinct (for duplicate elimination). TVA’s snapshot operator H has the same semantics as in prior work, that is, it applies an aggregation function G to a collection of records whose timestamps fall into a user-defined time interval I. More formally:

\[ H_G(S, I) = G(W) \mid W = \{r_j\}, r_j \in S, r_j \in I \] (3)

Filters are logical predicates constructed with TVA’s secure primitives (+, -, ×, ∨, ∧, ∨, ∧, ≤, ≥, =, ≠) and may also include arithmetical operations, e.g., Watt × Unit_Price ≥ $30. TVA’s equality, inequality, and parallel prefix adder [48] require O(log ℓ) rounds and O(ℓ log ℓ) communication, where ℓ is the length of the secret-shared operands in bits.

TVA’s sort operator s_tk(S) is based on a sorting network that requires O(log^2 |S|) rounds and O(|S| log^2 |S|) communication w.r.t the number of records. We choose a sorting network because it is easily parallelizable and works well with duplicate values, however, there exist oblivious sorting algorithms with lower asymptotic costs (e.g., [7, 8, 22, 47]). Combining these techniques with TVA’s protocols is an intriguing opportunity for future work.

The group-by operator \( γ(G)^{\delta}(S) \) uses the protocol by Jónsson et al. [54] and consists of two phases: a sorting phase where the input records are sorted on the grouping key(s), and an odd-even aggregation phase that applies the aggregation function G to each group with O(log|S|) rounds and O(|S| log|S|) communication in total. Distinct is a special case of grouping.

4.6 Operator composition

In this section, we describe all non-trivial cases of operator composition in TVA. We stress that the details of the composition process are completely hidden from TVA users by the high-level query API.

Composing filter and snapshot predicates. TVA does not pose any restriction to the number of filter predicates a user can specify. Predicates can be combined via logical AND and OR operators; for example, Weight < 140 lb OR (Weight > 150 lb AND Height ≤ 6 ft) is a valid composite filter. Each individual filter predicate \( φ \) appends a (secret-shared) single-bit attribute a\( φ \) to each record it is applied to. Predicate composition requires ANDing or ORing (under MPC) these attributes according to the abstract syntax tree (AST) of the composite filter. To reduce interaction between parties, TVA composes independent predicates in a binary tree of operations. This way, composing a series of \( m \) result bits of the form a\( φ_1 \land a_{\phi_2} \land \cdots \land a_{\phi_m} \) can be done with \( \log m \) rounds in total. In the end, each record has only one attribute a\( φ \land a_{\phi_2} \land \cdots \land a_{\phi_m} \) that denotes whether the record “passes” the composite filter or not.

In case a filter is followed by a snapshot operator, the condition \( r_j \in I \) from Eq. 3 is treated as one more filter on timestamps (with its own a\( φ \) attribute) and is composed with the rest of the filter predicates as described above.

Composing session window with aggregation. The strawman approach to compute the final aggregation on session windows is to first execute the SESSIONIZATION protocol (Protocol 3) and then use TVA’s group-by operator \( γ(G)^{\delta}(S) \) to apply the aggregation function G to each window. Although correct, this two-step approach requires \( 2 \times \) more operations and communication rounds compared to sessionization alone. In TVA we employ a more efficient composition technique that eliminates this overhead.

Recall that TVA’s group-by operator is based on the oblivious control flow by Jónsson et al. [54, Algorithm 6]. This algorithm compares records at distance d = |S| / 2 and, at each step of the iteration, reduces the distance to half of that in the previous step. Sessionization, however, only works if we access the time series S in the opposite way, i.e., when we start comparing adjacent records (at distance d = 1) and double the distance at each iteration. Interestingly, the oblivious aggregation by Jónsson et al. can be modified to work similarly, enabling us to perform the sessionization and group-by protocols within a single oblivious control flow. This approach saves O(log|S|) rounds and O(|S| log|S|) communication in total and requires minor protocol modifications. Specifically, we only need to add the following operation at the end of each
for-loop in Protocol 3 (right after line 7):

\[
\langle r_i, a_y \rangle_1 = \langle b \rangle_1 \cdot G(\langle r_i, a_y \rangle_1, \langle r_{i+1}, a_y \rangle_1) + (1 - \langle b \rangle_1) \cdot \langle r_i, a_y \rangle_1
\]  

Eq. 4 updates (in place) the value of the aggregated attribute \(a_y\) of the \(i\)-th record. To do so, parties apply the aggregation function \(G\) to the pair of records \((r_i, r_{i+1})\) and use arithmetic shares of the bit \(b\) (already computed in Protocol 3) to perform the oblivious multiplexing of the form \(b \cdot x + (1 - b) \cdot y\). Arithmetic shares of \(b\) are constructed on the fly using the single-bit conversion protocol from Mohassel and Rindal [63] (semi-honest security) or Dalskov et al. [26] (malicious security). This conversion requires one round between parties.

The composition technique we described works with any function \(G\) that is commutative and associative. This holds for all common aggregations, including \(\text{SUM}, \text{COUNT}, \text{MIN}, \text{MAX}^2\), \(\text{AVG}\), and \(\text{STDEV}\) (for the last two we must maintain the nominators and denominators separately).

**Composing keyBy with session window.** When a keyBy operator precedes a session window, the key \(k\) used in keyBy must be taken into account in the first phase of SESSIONIZATION. In this case, records are ordered on the pair \((k, t)\), instead of their timestamp \(t\) only, and the start of each session is marked when the default condition holds or the \(i\)-th record in the time series \(S\) has a different key value from the previous one, i.e., \(r_i.k \neq r_{i-1}.k, 0 \leq i < |S|\) (true for \(i = 0\)). This requires evaluating an extra equality predicate in step 4 of Protocol 4 and step 8 of Protocol 5.

**Composing multiple operators with aggregation.** The final aggregation is always computed with TVA's group-by operator but the actual grouping keys depend on the operators in the query. Recall that all operators besides keyBy append a secret-shared attribute to the records they apply to: filter and snapshot append an attribute \(a_y\) whereas window operators append an attribute \(w_{id}\). Whenever such an attribute exists in the input of the aggregation, TVA uses it along with the key \(k\) of the keyBy operator (if any) to construct a composite key for grouping. The more complex case is when the query contains a filter, a keyBy, and a window operator followed by an aggregation \(G\). In this case, TVA applies the operator \(G^2_{a_y, k, w_{id}}(S)\) that returns one aggregated value for each group of records with the same composite key \((a_y, k, w_{id})\).

### 5 Implementation

We have developed TVA from scratch in C++. We use MPI [2] for inter-party communication and libsodium [1] for random number generation. TVA supports shares of size \(2^\ell\), where \(\ell\) can be configured by the users. The default length for attributes is \(\ell = 32\) and for timestamps is \(\ell = 64\).

TVA’s architecture consists of three layers: (i) a runtime that is responsible for resource management and communication, (ii) a protocol layer that contains vectorized implementations of semi-honest and malicious-secure primitives \((+, \cdot, -, \oplus, \land, \lor, \neg, /)\), and (iii) a library of oblivious temporal and time-agnostic operators. The TVA runtime is carefully implemented to load balance computation in the asymmetric malicious protocol and to trade off computation for communication depending on the available resources. For example, the INP protocol (cf. §4.1) requires a party to send a vector of shares, another party to send the vector’s hash, and a third party to verify the hash. Hashing is used to reduce bandwidth consumption at the cost of increasing local computation. In low-latency environments, however, it is sometimes better if both parties send shares instead of hashing.

Computing parties can be deployed on premises or across multiple clouds. Analysts submit queries through a client application that exposes TVA’s high-level API and runs a lightweight module for generating and shipping shares.

### 6 Evaluation

Our experimental evaluation is structured into three parts:

**Comparison with state-of-the-art.** In §6.1, we present a performance comparison with Waldo [28], the only publicly available time series database with strong security guarantees. For multi-predicate queries, TVA provides up to \(5.8 \times\) lower latency compared to Waldo in the malicious setting and \(2 \times\) lower latency in the semi-honest setting. For window queries, TVA is up to two orders of magnitude faster than Waldo, which becomes competitive only when the ratio of the window length over the whole time domain is relatively small.

**Performance in real-world applications.** In §6.2, we use three real use cases to evaluate TVA’s performance in LAN and WAN with varying input sizes. We use queries that combine tumbling and session windows with filters and keyed aggregations. Our results demonstrate that TVA offers excellent performance for both continuous and historical analysis: it can successfully compute online queries with rigid time constraints and evaluate complex analytics on millions of input rows with modest use of resources.

**Microbenchmarks and cloud costs.** In the long version of the paper [33], we dive deeper into TVA’s performance and evaluate the scalability of window assignment protocols, the overhead of malicious security, the benefits of parallelization, and its cost. We show that TVA’s primitives scale effectively as the input size grows and that primitives under the malicious protocol are only \(2 \times\) slower compared to the semi-honest. At the same time, increasing the number of compute threads reduces latency by up to \(7 \times\). Finally, our results verify TVA’s ability to amortize I/O with message batching. Comparing the performance achieved in LAN with that of a WAN de-
deployment with $200-250\times$ higher RTT, latency is only $4.6\times$ higher on a time series with $2^{22}$ records.

### 6.1 Comparison with Waldo

#### 6.1.1 Differences between Waldo and TVA

We highlight a few important differences between the two systems that need to be considered when evaluating the performance results. First, WaldoTable requires data owners to pre-encode attributes into a $N \times 2^l$ table of one-hot vectors, where $N$ is the number of input records. In TVA, data owners only perform secret sharing (arithmetic or boolean, depending on the target query). Second, WaldoTree queries operate on public timestamps and return partial aggregates to the client, who is responsible for computing the global aggregation in the clear. On the other hand, TVA’s parties compute on private timestamps and return the final aggregation result to the client. Neither the pre-processing (index creation) nor the post-processing time of Waldo are included in the results of §6.1.2. Finally, both systems operate in the honest-majority setting: for semi-honest security, they rely on the same protocol [5] but, for malicious security, TVA uses a more efficient 4-party protocol [26] that requires three honest parties as opposed to Waldo’s 3-party protocol that requires two honest parties.

#### 6.1.2 Performance results

TVA can comfortably operate on machines with modest resources and supports large feature sizes (as we show later), however, for the sake of the comparison in this section we use the experimental setting of the Waldo paper [28, §VII]. In particular, we deploy parties on r5n.16xlarge instances (64 vCPUs and 512GB RAM), we use 8-bit attributes for both systems, and we set the network RTT to $20\text{ms}$. We note that we were unable to reproduce some of the published Waldo performance results. In our comparison below, we use the result reported in the Waldo paper when it is better than the one we measured in our own experiments.

Since Waldo is primarily optimized for snapshot queries, we devise the following two experimental scenarios to perform a meaningful comparison. First, we execute a Waldo-style multi-predicate snapshot query in TVA and compare its performance with the respective WaldoTable query. Second, we express a TVA-style tumbling window query in Waldo by executing multiple concurrent snapshot queries on consecutive time intervals on WaldoTree. All experiments of this section use sorted time series, as Waldo does not support out-of-order records.

**Comparison with WaldoTable.** For this experiment we set the number of input records to $2^{20}$ and run composite filters with equality and range predicates. Each filter contains 8 predicates of the same type and has the form $p_1 \land p_2 \land \cdots \land p_8$. Table 2 shows the results. We see that TVA’s performance exceeds that of the specialized WaldoTable data structure. This is not surprising, as WaldoTable’s computation and communication costs are linear in the input size and the round trips are linear in the number of predicates [28] (§VII-C). TVA can perform equality (resp. inequality) with three (resp. four) rounds and requires another three for the composition of the final result. Further performance benefits come from TVA’s ability to effectively parallelize the computation and amortize network I/O with its vectorized primitives. In the semi-honest case, TVA provides $1.94\times$ and $1.04\times$ lower latency than Waldo, for equality and range queries respectively. When operating with malicious security, the performance difference is more significant. TVA computes the equality query $5.8\times$ and the range query $3.08\times$ faster than Waldo.

**Comparison with WaldoTree.** In time series analytics, the window length can vary significantly depending on the use case. For example, monitoring applications compute fine-grained windows in the order of seconds, forecasting applications operate on intervals of minutes or hours, while anomaly detection involves comparing results over windows of different lengths [40]. To cover these diverse requirements, in this experiment we use a time series with $2^{20}$ measurements recorded every second ($\sim 12$ days of data in total). TVA needs 20 bits to encode the whole time domain, that is, the security parameter is $\sigma = 44$. We run tumbling window queries that compute a global aggregate per window and measure latency for both systems.

Figure 3 shows TVA’s speedup over Waldo for window lengths ranging from 5s to 24h (top x-axis). The bottom axis

<table>
<thead>
<tr>
<th>Query latency (s)</th>
<th>Equality</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>WALDO</td>
<td>Malicious</td>
<td>Semi-honest</td>
</tr>
<tr>
<td>WALDO</td>
<td>11.94</td>
<td>1.7</td>
</tr>
<tr>
<td>TVA</td>
<td>2.056</td>
<td>0.876</td>
</tr>
</tbody>
</table>

Table 2: Performance evaluation of WaldoTable and TVA queries with 8 predicates on a time series dataset with $2^{20}$ records.

---

Figure 3: Speedup of TVA’s tumbling window aggregation over WaldoTree on a time series dataset with $2^{20}$ records. The bottom x-axis shows the number of windows in the time series, which is equal to the number of searches Waldo performs for the respective query. Waldo achieves low latency for coarse-grained windows but its performance degrades significantly for fine-grained windows.
shows the number of searches that Waldo needs to perform on the aggregation tree to compute the corresponding window. TVA’s query latency is 6.8s (semi-honest) and 12.5s (malicious) irrespective of the window length. Recall that TVA’s tumbling window cost does not depend on the window length $\lambda$ (§4.2) but Waldo needs to perform $\frac{T_{\text{max}}-T_{\text{min}}}{\lambda}$ searches, where $T_{\text{min}}$ and $T_{\text{max}}$ are the minimum and maximum record timestamps in the dataset. We see that TVA is orders of magnitude faster than Waldo for small windows, as Waldo’s performance depends on the number of searches it performs in the underlying aggregation tree. When the ratio of the window length over the time domain becomes small, Waldo achieves better latency, as it performs fewer searches and the benefit of pre-aggregation pays off. Finally, we emphasize that the TVA’s speedup over Waldo is significantly higher if we include initialization time. While TVA’s parties simply receive secret shares, Waldo servers need to construct the tree index. In our experiments, this initialization step took over 1000s. If this overhead is considered, Waldo’s latency cannot match that of TVA, even for coarse windows.

### 6.2 Performance on real-world applications

**Evaluation setup.** In the remainder of the experimental evaluation we use two cloud deployments with smaller machines than before: (i) LAN uses one EC2 r5.8xlarge instance per party in the us-east-2 region of AWS, and (ii) WAN distributes parties across different geographical regions. For the semi-honest protocol, parties run in us-east-2 (Ohio), us-east-1 (Virginia), and us-west-1 (California). For the malicious protocol, we use the same three regions plus us-west-2 for the fourth party (Oregon). All VMs have 16 physical cores, 256GB RAM, and run Ubuntu 20.04.4, C++14, g++ 9.4.0, and MPICH 3.3.2. The RTT between west and east regions is 40-50ms and the bandwidth is limited at 5 Gbps. In all experiments we use the default configuration with 32-bit attributes and 64-bit timestamps. Reported measurements are averaged over at least three runs and plotted in log-scale, unless otherwise specified. In all experiments of this section, timestamps require up to 22 bits (which are sufficient to encode 10s measurements over the course of one year). That is, TVA’s security parameter is $\sigma = 42$ or greater.

#### 6.2.1 Application scenarios

In this set of experiments, we use three complex window queries that process time series from different application domains. We provide the queries written in TVA’s API in the full version of this work [33]. We use these real-world applications to evaluate TVA’s ability to support efficient time series queries in both online and historical analysis scenarios. In the first case, we demonstrate that TVA can comfortably compute query results under rigid time constraints. In the second scenario, we show that TVA can also support large-scale offline analytics on millions of input records.

**Monitoring energy consumption.** Privacy-preserving time series analysis can enable various smart grid applications, such as monitoring grid conditions to improve energy conservation and reduce peak demand [51, 72]. For this use case, we use a time series dataset that consists of energy consumption measurements across clients connected in a smart grid. The query computes the total energy consumption of the grid over tumbling windows.

**Mobile health analytics.** We developed the second use-case together with collaborators from our institution’s medical school. The input time series corresponds to measurements collected by wearable devices in a cohort of patients with diabetes. The measurements include glucose values and insulin dose events, among other attributes, and are used by the investigators to assess the effects of insulin doses across patients in the cohort. The analysis requires counting the number of insulin doses during each patient’s eating period, which is identified by a threshold in the glucose value. We express this query using a threshold session window operator.

**Job scheduling optimization.** The third application considers a cloud provider who wishes to optimize resource provisioning without compromising their clients’ privacy. To this end, the provider needs to process telemetry time series data from multiple clients without gaining access to raw execution logs that may contain proprietary information. We use a time series that follows the schema of real-world monitoring traces collected from Google clusters [73]. The provider is interested in analyzing the length of job phases (sessions) assigned to the various machine types and use this information to decide when to transfer long-running client workloads to larger machines or co-locate client workloads with short job sessions. We implement this application by first applying a filter to retain schedule events and then using a keyed gap session window to identify job sessions per machine type. The respective query performs a final aggregation to compute the session length and returns the maximum session per machine type.

#### 6.2.2 Online analysis scenario with time constraints

For a system to guarantee online operation, it needs to produce query results at a rate higher than that of data ingestion. For the energy use case, we consider sensors that generate measurements every 10s and a monitoring dashboard that needs to
We emphasize that, both in this and the previous experiment, with malicious security, TVA can update the energy grid TVA exceeds the requirements of real-world applications. Additionally, approaches, but also supports irregular timestamps and out-of-order records. This is in contrast to many prior techniques that either assume ordered timestamps (e.g., [28]) or operate in the “synchronous” setting where the aggregator receives data every k time units (e.g., [21,66,70]). Recently, Zheng et al. [81] proposed a technique to compute similarity queries on time series snapshots. We leave such operations as future work.

**FSS-based approaches.** Function secret sharing [12,13] is a cryptographic technique that allows creating shares of a function as opposed to creating shares of a value in MPC. Approaches using FSS, including distributed point functions, incur lower communication compared to MPC-based techniques. Waldo [28], DuraSift [35], and Vizard [18] use FSS to securely evaluate range and equality predicates by splitting shares of the predicate to untrusted non-colluding parties. Splinter [76] uses FSS to evaluate private SQL queries on public data, whereas Dittmer et al. [29] employ FSS for efficient streaming PSI. Expressing TVA’s complex window operations using FSS is still an open problem and an interesting direction for future work.

**ORAM-based approaches.** Oblivious RAM [42,43] allows for hiding access patterns in arbitrary programs but its generality comes at a high cost. Distributed ORAM constructions by Bunn et al. [15] and Doerner et al. [30] achieve better performance by leveraging FSS. TVA hides access patterns via oblivious operators that we specifically design for time series analytics.

### 6.2.3 Historical analysis scenario

For the historical analytics scenario, we measure query latency as the time series size increases. Figure 4 shows the results. We emphasize that, both in this and the previous experiment, timestamps are not considered to be ordered and the reported times include sorting under MPC. TVA comfortably scales to millions of records and computes all queries within a few minutes. For $2^{20}$ records, the Energy query takes 1 min in LAN and 9 min in WAN, while the mHealth and Scheduling queries have similar performance and take $\sim 2.4$ min in LAN and 20 min in WAN. The mHealth and Scheduling queries are both based on sessionization but the latter is more complex, including filter and keyBy operators. The overhead of these additional operators is negligible thanks to TVA’s efficient composition protocols. The cost of using a malicious protocol is small, resulting in a $2^\times$ slowdown.

### 7 Related work

Here we discuss closely related works and provide more details in the full version of the paper [33].

**Privacy-preserving time series analysis.** Although there is a large amount of work in privacy-preserving time series analysis, none of the existing approaches supports secure windowing. Despite their particular differences with respect to threat models and security guarantees, the vast majority of efforts focus on global aggregations or snapshot queries with (optional) filters and aggregation [21,27,28,46,49,51,53,66,68–70,78]. TimeCrypt [16] and Zeph [17] have built-in support for tumbling windows, but they reveal information to the untrusted server and can only operate on public timestamps. Zeph also supports limited (additive) per-group aggregation within time windows but requires data holders to pre-encode the grouping key domain (e.g., all possible zipcodes).

TVA extends the functionality of prior works without compromising security or performance. TVA introduces expressive recurring window operators (§4.2–4.4) and allows for efficient composition of window and snapshot operators with custom grouping, filters, and aggregation (§4.6). In addition, TVA hides queried time intervals, as in state-of-the-art approaches, but also supports irregular timestamps and out-of-order records. This is in contrast to many prior techniques that either assume ordered timestamps (e.g., [28]) or operate in the “synchronous” setting where the aggregator receives data every k time units (e.g., [21,66,70]). Recently, Zheng et al. [81] proposed a technique to compute similarity queries on time series snapshots. We leave such operations as future work.
Acknowledgments

The authors thank the anonymous reviewers and shepherd for their valuable feedback. We also thank Dr. Nicole Spartano and Dr. Lisa Quintiliani for helping us develop the mobile health application, and Ian Saucy for his help with the WAN deployments. This work has been supported by the National Science Foundation under Grants No. 1915763 and 2209194, the DARPA SIEVE program under Agreement No. HR00112020021, a Red Hat Collaboratory grant (No. 2022-01-RH02), a Hariri Institute Focused Research Project Award, and a gift from Robert Bosch GmbH.

References


We do make a few modifications to our functionality $\mathcal{F}_{\text{abb}}$ as compared to the ABB model of Escudero et al. First, our functionality considers a single addition operation at a time rather than providing support for more complicated linear combinations directly; this is purely a modeling decision and has no impact on the capabilities of the functionality. Second, we support addition and multiplication over arithmetic rings of different sizes; support for multiple moduli provides a small efficiency benefit in Protocols 1-2 but is not required and may be omitted. Third, we add support for the shared input (INP) and bit-to-arithmetic (b2A) functionalities. Additionally, we follow the convention that the method name itself implicitly in all other protocols). Second, we can abstract away the underlying implementations of these MPC operations when specifying TVA’s protocols (as shown formally in Protocols 1 and 2, and implicitly in all other protocols). Second, we can write generic proofs (in the full version of this work [33]) that all of the protocols within TVA are secure when provided with any instantiation of the ABB functionality. Several prior works use the ABB model to prove the security of higher-level protocols that make black-box use of MPC primitive operations (e.g., [31, 32, 36, 45, 57, 74]).

In this work, we require a functionality that supports mixed-mode operations: both arithmetic and boolean computation as well as conversions between them. For this reason, our starting point is the functionality provided by Escudero et al. [32, Figure 1]. Our functionality $\mathcal{F}_{\text{abb}}$ in Figure 5 is similar to Escudero et al. [32, Figure 1]. In particular, we emphasize that the “add” and “mult” functionalities in Figure 5 support both arithmetic and boolean operations—that is, they also support the operations of boolean XOR and boolean AND. Additionally, we follow the convention that the method name itself is also the first input to the functionality; as a consequence, we use the notations $\mathcal{F}_{\text{abb}}(\text{input}(\cdot))$ and $\mathcal{F}_{\text{abb}}(\text{output}(\cdot))$ interchangeably.

We make a few modifications to our functionality $\mathcal{F}_{\text{abb}}$:
A2B, which is instantiated in the 3-party variant of TVA using a parallel prefix adder as described in Mohassel and Rindal [63, §5.3], and we extend their technique to the 4-party setting in Appendix B.

It is straightforward to see that the works of Araki et al. [5] and Dalskov et al. [26] provide most of the protocols that collectively instantiate our $\mathcal{F}_{\text{abb}}$. Concretely, they provide specific ideal functionalities for each method within Figure 5 (e.g., multiplication is described in [5, Functionality 3.3] and [26, Protocol 4]), and then provide simulation-secure instantiations of each method. Furthermore, revealing the output to one party does not reveal any information about other secrets, due to the use of fresh randomness to re-randomize shares after every interactive operation. There are two caveats, however. First, only Dalskov et al. [26] provides an instantiation of the shared input method INP. As a result, we only use INP within the 4-party variant of TVA (e.g., we use it in Protocol 2 but not Protocol 1). Second, we adopt the arithmetic-to-boolean conversion protocols from Mohassel and Rindal [63, §5.3] (in the 3-party setting) and Appendix B (in the 4-party setting).

B 4-party arithmetic to boolean conversion

In Protocol 6, we provide a new mixed-mode protocol for arithmetic to boolean conversion. Its main advantage is to reduce the number of communication rounds required: our protocol uses 1 boolean adder rather than 3 of them. Additionally, our protocol is amenable to use within our 4-party secure division protocol, in which case the “shares merging” step below can be removed since the INP sharing is already performed within Protocol 2.

**Protocol 6: A2B CONVERSION (Malicious 4PC)**

| Input | An arithmetic secret-shared integer $\langle x \rangle_\ell$ |
| Output | A boolean secret-shared integer $\langle [x] \rangle_\ell$ |
| //Shares Merging | |
| 1 | Parties 1, 4 locally compute $x'_1 = x_1 + x_2$ |
| 2 | Party 2, 3 locally compute $x'_2 = x_3 + x_4$ |
| //Shares redistribution | |
| 3 | Let $\langle a \rangle_\ell = \text{INP}(x'_1, 1, 4)$ |
| 4 | Let $\langle b \rangle_\ell = \text{INP}(x'_2, 2, 3)$ |
| 5 | Output $\langle [x] \rangle_\ell = \langle [a] \rangle_\ell + \langle [b] \rangle_\ell$ |

Figure 5: Arithmetic black-box functionality $\mathcal{F}_{\text{abb}}$ that supports mixed-mode operations and conversions. Based upon Escudero et al. [32, Figure 1], with a few modifications described in Appendix A.