STEP-BY-STEP TUTORIAL FOR EASYSMPC

EasySMPC is a simple application to calculate sums over distributed data easily using Secure Multi-Party Computation protocols. The current version of EasySMPC is available at https://github.com/prasser/easy-smpc.

There are two processing modes within the EasySMPC application: (1) *manual mode* and (2) *automated mode*. In the manual mode, the installed email program can be used for manual sending and receiving of pre-generated emails. Here, other methods of communication such as chats could also be employed. In the automated mode, each user configures a mailbox to exchange data automatically. Outside of email communication, no network connection is established between the participants in either mode. Data security is guaranteed in both modes.

EasySMPC is project or study orientated, meaning that the calculation of one or several sums with several parties is always bound to exactly one study. During a study, EasySMPC knows two types of roles: (1) the *creator*, who initiates a study defining its title, participants, variables and processing mode; (2) the *participants*, who initiate their study participation, enter their respective data to the pre-defined variables and, if necessary, their mail box details. Each EasySMPC study has exactly one creator and two or more participants. Which actions to take in each role with each mode is described below in detail.

Remark: This document describes EasySMPC, when used with the Graphical User Interface (GUI). EasySMPC also offers a command-line interface, which is described in the readme documentation of the GitHub repository.

Table of contents

1 Prerequisites 1

2 Creator 2

2.1 Manual mode 2

2.2 Automated mode 15

3 Participant 22

3.1 Manual mode 22

3.2 Automated mode 26

4 Saving, closing and re-opening a study file 30

1 Prerequisites

Installation

To use EasySMPC, please download the software from https://github.com/prasser/easy-smpc/releases. Here, you can choose between installation packages for the operation systems Windows, Linux or MacOS. Moreover, EasySMPC can be downloaded as an executable jar-File. After installation, the user can start the software from the respective entry in the programs library or with the link on the Desktop.

Preparing data

The user needs to provide the data in a format suitable for EasySMPC: The software supports files in the format of Comma Separated Values (CSV) and in Microsoft Excel (".xls" and ".xlsx"). The data needs to be row-oriented (one row for each entry) and must have at least two columns. The last column is regarded as the data value and therefore must always contain numbers only. A single dot a as a decimal separator is allowed but not necessary. In case of exactly two columns, the first column will be regarded as the sole data description. In the case of more than two columns, EasySMPC will concatenate all columns of a row except the last column to a single column and use this as the data description of the data (see Figure 1 for an example).

Figure 1: Original data and its representation in EasySMPC

Choosing a mode

Before starting a new study with EasySMPC, please decide which mode you want to use, the *automated* or the *manual mode*. This decision cannot be changed during the study after it has been defined by the creator. It applies to all participants in the study. If you decide for the *automated mode*, make sure that all participants know the necessary details to connect to their respective mail boxes (see step 3 in chapter 2.2). However, it is always possible to start a new study using another mode.

Clipboard

In *manual mode*, EasySMPC makes use of the *clipboard*, which basically refers the usage of the popular *copy* and *paste* mechanisms (e.g. the key combination of *control + c* and *control + v* on many operating systems). If you are not familiar with these functionalities, please make yourself familiar with them e.g. with the respective Wikipedia article.

2 Creator

2.1 Manual mode

2.1.1 Step 1

To create a new study, first start EasySMPC and click on *Create new study*.

Figure 2: *Start* perspective of EasySMPC

2.1.2 Step 2

Enter the name of the study as well as the name and the e-mail addresses of the participants. The field *automated data exchange* must remain empty for the manual mode. Afterwards click on the button *Load variables and values from file*.

Remark: Red-bordered fields indicate that the content of a field is not correct and needs to be corrected. In this case, the name and value of the first variable needs to be provided.

Figure 3: *Start* perspective of EasySMPC filled out partly

2.1.3 Step 3

Select a Microsoft Excel or CSV file in the now opened file browser. Browse to the folder of your data, select it and click O*pen*.

Figure 4: File browser with EasySMPC

2.1.4 Step 4

The data now appears in the bottom section of EasySMPC. You can click on Save and proceed.

Remark: Loading of data from a file is not necessary. You can also add variables and values manually.

Remark: The study name, the participants' names and e-mail addresses as well as variable names will be shared with **all other** study participants. The data you entered in the *values* field is **secured** and **will not** be shared.

Figure 5: *Start* perspective of EasySMPC filled out completely

2.1.5 Step 5

After clicking on *Save and proceed* a file browser opens to choose a location of your study file generated by EasySMPC. The study file will store all relevant information. EasySMPC allows closing a file, stopping the processing and re-opening at a later point in time (see section *Saving, closing and re-opening a* study file).

Figure 6: Save the project file generated by EasySMPC

2.1.6 Step 6

Now the first *Send* perspective opens. It allows the generation of prepared messages to the other participants. The first line is your own contact data and is displayed for your information only. You can ignore it.

Figure 7: *Send* perspective in EasySMPC in an initial state

2.1.7 Step 7

Click on button *Send e-mail manually* in the second line. Three options appear. Click on *Send e-mail manually.*

Figure 8: *Send* perspective in EasySMPC sending an e-mail manually

2.1.8 Step 8

Your e-mail application (in this case Mozilla Thunderbird) will pop-up with a generated e-mail. You can send the e-mail out without any changes.

Figure 9: Pre-generated e-mail in Mozilla Thunderbird

2.1.9 Step 9

After sending the e-mail with your e-mail program, you can return to EasySMPC. The software will ask you whether the e-mail has been sent correctly. If so, please indicate this with a click on *Ok*.

Remark: After clicking on *Ok*, you can still have the e-mail generated a second time, e.g. when there was a problem receiving the e-mail by one of the participants.

Figure 10: Confirm sending in the *Send* perspective of EasySMPC

2.1.10 Step 10

Now the checkmark in the second line has turned green.

Figure 11: *Send* perspective in EasySMPC after sending the first e-mail.

2.1.11 Step 11

Repeat the sending process for all outstanding participants. Once this is finished and all checkmarks have turned green, you can click on *Proceed*.

Figure 12: Confirm sending in the *Send* perspective of EasySMPC

Remark: You can also click on *Manually send all pending messages* to have e-mails generated for all outstanding participants.

Remark: In some cases the security constraints on the operating system will prevent EasySMPC from starting the e-mail program. In these cases you can select *Copy e-mail text* after clicking on *Send e-mail*. The content of the e-mail is then copied into the clipboard from which you can paste it into an e-mail after opening your e-mail program manually (or any other communication method such as chat programs).

2.1.12 Step 12

EasySMPC displays the next perspective: *Receive*. Here, you need to wait for e-mails sent by the other study participants. Once you received an e-mail by another participant, click on *Manually enter received data*.

Figure 13: The *Receive* perspective of EasySMPC

2.1.13 Step 13

Open your e-mail program, highlight the entire text you received and copy it into the clipboard.

Figure 14: Received e-mail displayed in Mozilla Thunderbird

2.1.14 Step 14

Open EasySMPC again, click into the red-bordered field and click on *Paste*. Proceed by clicking on the now activated *Ok* button.

Figure 15: Copy data into EasySMPC

2.1.15 Step 15

The successful receiving of the message is reflected in the status line as well as by the green checkmark.

Figure 16: The *Receive* perspective of EasySMPC after processing a message

Remark: Since EasySMPC is reading the clipboard continuously, in most cases copying the e-mail to the clipboard as shown in step 13 is sufficient and the steps 12 and 14 are not necessary.

2.1.16 Step 16

Repeat the receiving steps until all checkmarks turn green. Then click on *Receive*.

Figure 17: The *Receive* perspective of EasySMPC after receiving all messages

2.1.17 Step 17

The following *Send* and *Receive* perspectives work exactly as the perspectives described beforehand. Therefore, they are skipped in this tutorial for brevity. We refer to the sources listed in the README documentation of the github repository for a description why two rounds of communications are necessary.

2.1.18 Step 18

After finishing sending and receiving the second time, the *Result* perspective shows the sums for each variable (each sum is calculated with the data of all participants). This perspective will be the same for all participants. Click on *Export data* to export the data as a CSV or Microsoft Excel file.

Figure 18: The *Result* perspective of EasySMPC

2.2 Automated mode

2.2.1 Step 1

To create a new study, first start EasySMPC and click on *Create new study*.

Figure 19: *Start* perspective of EasySMPC

2.2.2 Step 2

Enter the name of the study and click on *Add* to add a new e-mail address for the automated mode.

Remark: You do not need to add an e-mail address if you did this before. In these cases just select your e-mail address from the dropdown field left to the button *Add.* Later on you will be asked for your password only.

Remark: Red-bordered fields indicate that the content of a field is not correct and needs to be corrected. In the example below, the e-mail address as well as the name (and value) of the first variable needs to be provided.

Figure 20: *Start* perspective of EasySMPC filled out partly

2.2.3 Step 3

The simple e-mail configuration dialog appears. Enter the e-mail address, your password and the names and ports of the receiving (IMAP) and sending (SMTP) server (if you do not know this data please ask your administrator). After entering the data you can click on *Proceed*. The connection will be automatically checked. If the check is successful, the dialog will close automatically. If the check is not successful, a warning message will appear and you can alter your configuration in the e-mail dialog. You will not be able to store the connection if the check is not successful.

Remark: You can also add your e-mail address only and click on *Determine configuration automatically*. If successful all data but the password will be entered automatically. The automatic configuration detection does not work for all e-mail addresses.

Remark: You can also switch to the advanced e-mail configuration dialog. The dialog offers the following additional configuration options:

- The definition of a separate e-mail address for sending. The e-mail address which will be shared with the other participants will always be the receiving one.
- The definition of user names for the e-mail boxes differing from the e-mail address (e.g. the user name is *name* and not *name@domain.org*)
- The authentication mechanisms supported by the e-mail boxes. For details, please refer to the property *mail.imap.auth.mechanisms* in the Jakarta e-mail documentation.

Figure 21: The simple e-mail configuration dialog

2.2.4 Step 4

Now enter the remaining participants and the data. Please refer to step 2-4 and the following steps in the in chapter 2.1, since they are identical. After entering the information please click on *Save and Proceed* and save the file as described in step 5 in chapter 2.1.

Figure 22: *Start* perspective of EasySMPC filled out completely

2.2.5 Step 5

EasySMPC now sends the necessary e-mails for starting a study to the other participants. You do not have to do anything. After sending, EasySMPC will proceed automatically to the next perspective.

Remark: In case of errors while sending the e-mail, a message will appear asking you to alter your e-mail configuration. You can re-send all e-mails at once automatically by clicking on the button *Automatically send all pending messages*. Moreover, you can send out the messages manually as described in the steps 7-9 in chapter 2.1. You will only be able to proceed once all e-mails have been successfully sent.

Figure 23: Automatic sending in the *Send* perspective

2.2.6 Step 6

Now EasySMPC checks your e-mail box for messages sent by other participants which can be seen by the status bar in the upper right corner. The status bar also indicates the receiving of a message. Once all necessary messages have been received, EasySMPC will automatically proceed to the next perspective.

Remark: In case of errors during receiving, an error message occurs and the status bar changes accordingly. You can restart your connection to the e-mail server by clicking on *Create connection to e-mail box*.

Figure 24: Automatic receiving in the *Receive* perspective

2.2.7 Step 6

The following *Send* and *Receive* perspectives work exactly as the perspectives previously described in this chapter. Therefore, they are skipped in this tutorial for brevity. We refer to the sources listed in the README documentation of the github repository for a description why two rounds of communications are necessary.

2.2.8 Step 7

After finishing sending and receiving for the second time, the *Result* perspective shows the sums for each variable (each sum is calculated with the data of all participants). This perspective will be the same for all participants. Click on *Export data* to export the data as a CSV or Microsoft Excel file.

Figure 25: The *Result* perspective of EasySMPC

3 Participant

3.1 Manual mode

3.1.1 Step 1

The first step as a participant in manual mode is to receive an e-mail by the creator (see step 3 an example). Once you received the e-mail, you can start EasySMPC and click on *Participate in study*.

Figure 26: *Start* perspective of EasySMPC

3.1.2 Step 2

A dialog to enter the initial data you received will appear.

Figure 27: Dialog to enter initially received data into EasySMPC

3.1.3 Step 3

Open your e-mail program, highlight the entire text you received and copy it into the clipboard.

Figure 28: Initially received e-mail displayed in Mozilla Thunderbird

3.1.4 Step 4

Open EasySMPC again, click into the red-bordered field and click on *Paste*. Proceed by clicking on the now activated *Ok* button.

Figure 29: Copy initial data into EasySMPC

3.1.5 Step 5

Now the *Start* perspective appears showing all participants, e-mail addresses and variables. You cannot change this data. The sole thing you are entitled to enter are your values for the different variables. These values are **secured** and **will not** be shared. You can either enter your values manually or load your data from a file (see steps 2 and 3 in section *Manual mode* of the creator). EasySMPC will try to match the variable name in your provided file with the one displayed in EasySMPC and enter the specified data automatically. After entering your values, you can proceed by clicking on *Save and proceed*.

Figure 30: The *Start* perspective of EasySMPC for a participant after loading data

3.1.6 Step 6

From here on please refer to step 7 and following in chapter 2.1, since they are identical to the steps of the participant.

3.2 Automated mode

3.2.1 Step 1

The first step as a participant in manual mode is to receive an e-mail by the creator (step 3 below in chapter 3.2.3 provides an example). Once you received the e-mail, you can start EasySMPC and click on *Participate in study*.

Figure 31: *Start* perspective of EasySMPC

3.2.2 Step 2

A dialog to enter the initial data you received will appear.

Figure 32: Dialog to enter initially received data into EasySMPC

3.2.3 Step 3

Open your e-mail program, highlight the entire text you received and copy it into the clipboard.

Figure 33: Initially received e-mail displayed in Mozilla Thunderbird

3.2.4 Step 4

Open EasySMPC again, click into the red-bordered field and click on *Paste*. Proceed by clicking on the now activated *Ok* button.

Figure 34: Copy initial data into EasySMPC

3.2.5 Step 5

The study name, the participants' names and e-mail addresses as well as variable names are displayed. As a participant you cannot change the content of these fields. Please enter your data either manually or load it from a file as described in steps 2-3 in chapter 2.1. If you load data from a file, EasySMPC will try to match the loaded data with the variables names. Data from a file without a match will be ignored. Moreover, either choose your existing e-mail address or add one as described in step 3 in chapter 2.1.

Remark: Your e-mail addressed must be configured as the same one appearing next to your name in the *Participants* part of the screen.

Remark: The data you entered in the *values* field is **secured** and **will not** be shared.

Figure 35: The *Start* perspective of EasySMPC for a participant

3.2.6 Step 6

From here on please refer to step 5 and forth following in chapter 2.2, since they are identical to the steps of the participant.

4 Saving, closing and re-opening a study file

EasySMPC supports to save the current state to the study file to proceed at a later point in time for all *Send* and *Receive* perspectives. The steps necessary are described below.

4.1.1 Step 1

While working with an EasySMPC study, click on *Action* and then on *Save study interim state.* The study is saved to the project file.

Figure 36: Saving the current state of an open study

4.1.2 Step 2

Now click on *Action* and *Exit* or the red *X* in the upper right corner. The subsequent dialog can be confirmed with *Yes.*

Figure 37 Confirm closing EasySMPC

4.1.3 Step 3

To reload the file, click on *Load study* after starting EasySMPC.

Figure 38: Start loading a study in EasySMPC

4.1.4 Step 4

Select the study file in the now opened file browser and click O*pen*.

Figure 39: Dialog to select the study file

4.1.5 Step 5

Now you can proceed working with EasySMPC.

Figure 40: EasSMPC opened the study in the recent state