Privacy preserving computation allows users to participate in computations while keeping their data private using complex cryptography. An example application is a location server that informs users if friends are nearby but doesn’t learn any information about any user’s locations. The typical privacy preserving computation does not allow information from one computation to be used in another computation, preventing the reuse of already computed results. We created a protocol that allows parties to reuse state and then implemented it in a server-aided, or outsourcing, framework with the three parties. A mobile device, which outsources to the cloud, and one who performs the evaluation of the garbled gates, participating in privacy preserving computation. We created a friend finder application to demonstrate how PartialGC can be used in practice to save the location of friends in a privacy-preserving manner. Each time a user presses the “Set New Location” button, the application updates the user’s location and checks to see whether or not a friend is currently at the user’s location. Using our application, users can determine whether or not there are any friends nearby, while saving their locations in a privacy preserving fashion to prevent a third party server from learning any user’s location.

PartialGC is our system for saving state in a privacy preserving computation. We implemented our technique in a state of the art server-aided system, which allows a mobile phone to outsource part of the computation to the cloud. Without outsourcing, privacy preserving computation is not practical from on mobile device due to the high cost. We also incorporated other recent optimizations into our system.

We compare our results to the previous system using runtime and the amount of bandwidth required by the phone. Not all programs could be created, due to a slow compiler, or executed, due to memory limits, in the previous system leading to the missing result bars in Fig. 3.

PartialGC allows the fastest way to reuse values in the different schemes we tested.

Fig. 4 shows the reduction in total bandwidth used by the phone when it is compared with the previous system. Bandwidth is important due to the high cost of transmitting each byte of information on a mobile phone.

We created a friend finder application to demonstrate how PartialGC can be used in practice to save the location of friends in a privacy-preserving manner. Each time a user presses the “Set New Location” button, the application updates the user’s location and checks to see whether or not a friend is currently at the user’s location. Using our application, users can determine whether or not there are any friends nearby, while saving their locations in a privacy preserving fashion to prevent a third party server from learning any user’s location.

PartialGC is our system for saving state in a privacy preserving computation. We implemented our technique in a state of the art server-aided system, which allows a mobile phone to outsource part of the computation to the cloud. Without outsourcing, privacy preserving computation is not practical from on mobile device due to the high cost. We also incorporated other recent optimizations into our system.

We compare our results to the previous system using runtime and the amount of bandwidth required by the phone. Not all programs could be created, due to a slow compiler, or executed, due to memory limits, in the previous system leading to the missing result bars in Fig. 3.

PartialGC allows the fastest way to reuse values in the different schemes we tested.

Fig. 3 gives results showing PartialGC is the best option when using small incremental parts that combine into a larger program. PartialGC allows the fastest way to reuse values in the different schemes we tested.

PartialGC is our system for saving state in a privacy preserving computation. We implemented our technique in a state of the art server-aided system, which allows a mobile phone to outsource part of the computation to the cloud. Without outsourcing, privacy preserving computation is not practical from on mobile device due to the high cost. We also incorporated other recent optimizations into our system.

We compare our results to the previous system using runtime and the amount of bandwidth required by the phone. Not all programs could be created, due to a slow compiler, or executed, due to memory limits, in the previous system leading to the missing result bars in Fig. 3.

PartialGC allows the fastest way to reuse values in the different schemes we tested.

Fig. 3 gives results showing PartialGC is the best option when using small incremental parts that combine into a larger program. PartialGC allows the fastest way to reuse values in the different schemes we tested.

PartialGC is our system for saving state in a privacy preserving computation. We implemented our technique in a state of the art server-aided system, which allows a mobile phone to outsource part of the computation to the cloud. Without outsourcing, privacy preserving computation is not practical from on mobile device due to the high cost. We also incorporated other recent optimizations into our system.

We compare our results to the previous system using runtime and the amount of bandwidth required by the phone. Not all programs could be created, due to a slow compiler, or executed, due to memory limits, in the previous system leading to the missing result bars in Fig. 3.

PartialGC allows the fastest way to reuse values in the different schemes we tested.