AutoMPC: Efficient Multi-Party Computation for Secure and Privacy-Preserving Cooperative Control of Connected Autonomous Vehicles

Tao Li
Department of Computer Science
Purdue University
taoli@purdue.edu

Lei Lin
Goergen Institute of Data Science
Rochester University
lei.lin@rochester.edu

Siyuan Gong
Department of Computer Science
Chang'an University
sgong@chd.edu.cn

Abstract

The advent of connected autonomous vehicles provides opportunities for safer, smoother, and smarter transportation. However, broadcasting information to surrounding vehicles and infrastructures risks security and privacy. Moreover, control decisions relying on such information are vulnerable to malicious attacks. In this paper, we propose a cooperative control strategy incorporating with efficient multi-party computation (MPC). In an effort to perform secure MPC without third-party authentication while reducing latency, we integrate a function secret sharing scheme with a distributed oblivious random access memory. We further design an adaptive proportional-derivative controller to increase resilience toward latency and adversaries. Theoretical foundations and limitations are also discussed.

1 Introduction

Since the first competition of autonomous vehicles hosted by the Defense Advanced Research Projects Agency (DARPA) Grand Challenge in 2005 (Seetharaman, Lakhotia, and Blasch 2006), self-driving vehicle or autonomous vehicle techniques have attracted tremendous attentions from both academia and industry. An autonomous vehicle is equipped with various powerful sensors like camera, radar, LiDAR, GPS, ultrasonic and so on to detect and perceive its surrounding environment. Autonomous vehicles have the potential to change driving behavior and the travel environment, providing opportunities for safer, smoother, and smarter road transportation. However, the development of autonomous vehicles has also raised disputations and skepticism in terms of liability, ethics, cybersecurity, privacy and so on. Especially, the fatal accident in March, 2018 involving an Ubers self-driving car where a pedestrian was killed implies a large room to enhance autonomous vehicle techniques and safety should always be considered with the highest priority in this process (Li et al. 2018a).

On the other hand, connected vehicle techniques are also being deployed to improve the safety and mobility of our transportation system by enhancing situational awareness and traffic state estimation through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure communications, which can enable applications like cooperative collision warning, providing traffic signal status information in real time and so on (Shladover 2018), These applications require low latency and high reliability networking. Hence, efficient, secure, and trustworthy data transmitting is of paramount importance.

More recently, interesting opportunities appear through the utilization of techniques from connected vehicles to autonomous vehicles. The connectivity allows an autonomous to have more detailed knowledge of the environment. The sensing capability of the autonomous vehicle is hence further expanded. A platoon formed by connected and autonomous (CAVs) on the road can increase the capacity, reduce energy consumption and improve safety. It was predicted that the transition from the current human-driven vehicles to a fully CAV traffic environment require a few decades (GSMA 2013), during which the road traffic consist of a mixed traffic flow (see Figure 1). Equipped with multiple sensors and V2V communications, a CAV can track the trajectories of other CAVs in its vicinity, and ideally, all CAVs in communication range. Such CAV trajectory data can be leveraged with advances in computing and machine learning algorithms to potentially predict trajectories of surrounding vehicles, such as acceleration and speed. Based on these predictions, CAVs can react accordingly to avoid or mitigate traffic flow oscillations and accidents.

In reality, V2V communications are unreliable due to factors such as interference, network congestion, and malicious attacks; in the worst case, V2V networks undergo Byzantine failures (Lamport, Shostak, and Pease 1982; Li and Lin 2018), which is the most general and severe failure model, since attackers are fully aware of any information of the entire system. Moreover, current architecutre of vehicular ad-hoc networks (VANETs) communicate in an open-access environment and thereby experience serious issues in security and privacy (Qu et al. 2015). To tackle these, we propose a novel cooperative control strategy, AutoMPC, by leveraging advances in modern cryptography such as multi-party computation (MPC). As V2V communication requires low latency, we further adopt an efficient MPC scheme incorporating with an adaptive proportional-derivative controller and prove its effectiveness through numerical experiments.

The rest of this paper is organized as follows: in Section 2 we introduce necessary background; Section 3 presents the AutoMPC model; future works are discussed in Section 4; we leave the experimental section and more theoretical results in the full paper.

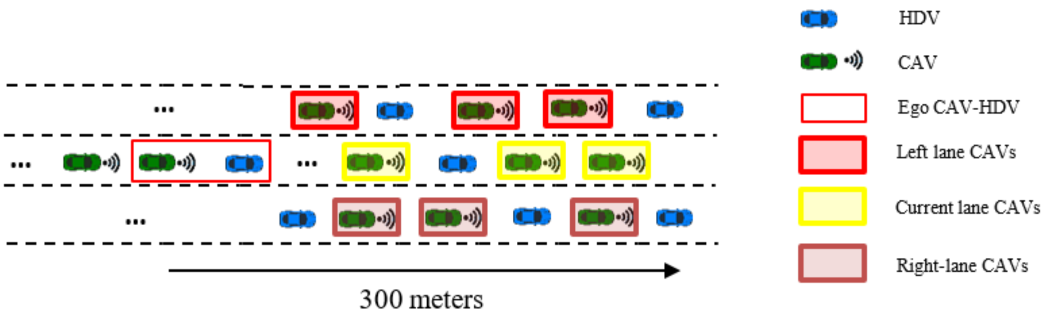

Figure 1: Scenario of a mixed platoon of connected autonomous vehicles (CAVs) and human-driven vehicles (HDVs).

2 Background

We first introduce necessary background in security.

2.1 Secure Multi-Party Computation

To formalize the problem, we suppose a multi-agent system in which each party i has a secret input x_i and a function $f(x_1, x_2, \dots)$ can be jointly evaluated. Secure multi-party computation (MPC) is a mechanism to ensure that each party known the output of the function f while being unaware of others' inputs. Two-party computation (2PC) is a special case of MPC, which was first introduced by (Yao 1982) as a problem that two millionaires (Alice and Bob) wish to know who is richer but don't want to disclose their own wealth. The famous solution is Yao's Garbled Circuits (Yao 1986), which is based on honest-but-curious model or semi-honest security model that curious adversaries and outside observers may learn the secrets by analyzing protocol transcripts.

2.2 Oblivious Random Access Memory

Oblivious random access memory (ORAM) (Goldreich and Ostrovsky 1996) is similar to random access memory (RAM) but translates the sequence of logical access instructions in certain ways so that preserves the observing of physical access patterns from adversaries. An ORAM supports $READ(i)$ and $WRITE(i)$ functions that are able to perform "read" and "write" operations with a private index i. For the case of MPC, we consider a variant of ORAM, distributed oblivious RAM (DORAM) (Lu and Ostrovsky 2013), which generalize ORAM to a scenario that the memory is splited among m parties and has a security property that no party can learn anything of the RAM by observing their own share of the physical memory.

2.3 Secret Sharing

Secret sharing (Shamir 1979) is a method in cryptography that distributes a secret among a group of m parties by dividing the secret into m shares, one for each of m parties, so that none of the individual party has any insight of the secret while all m shares as a group contain full information of the secret. (Franklin and Yung 1992) designed a multi-secret sharing system where multiple points of the polynomial host secrets. (Parakh and Kak 2011) proposed a k-threshold computational secret sharing scheme that divide a secret S into shares of size $\frac{|S|}{K-1}$ for optimal space efficiency.

3 The AutoMPC Model

Inspired by existing works (Gordon et al. 2012; Wang et al. 2014; Doerner and Shelat 2017) and aforementioned techniques, we propose the AutoMPC model, which adopts a function secret sharing (FSS) scheme following the definition in (Boyle, Gilboa, and Ishai 2016) that:

Definition 1. *An m-party function secret sharing scheme is a pair of algorithms (Gen, $Eval$) with the following syntax:*

- *$Gen(1^\lambda, \bar{f})$ is a PPT key generation algorithm, which on input 1^λ (security parameter) and $\bar{f} \in \{0,1\}^*$ (description of a function f) outputs an m-tuple of keys $(k_1, \dots, k_m)$. $\bar{f}$ is assumed to explicitly contains an input length 1^n, group description $\mathbb{G}$, and size parameter $\mathbb{S}$.*
- *$Eval(i, k_i, x)$ is a polynomial-time evaluation algorithm, which on input $i \in [m]$ (party index), k_i (key defining $f_i : \{0,1\}^n \to \mathbb{G}$), and $x \in \{0,1\}^n$ (intput for f_i) outputs a group element $y_i \in \mathbb{G}$ (the value of $f_i(x)$, the i-th share of $f(x)$).*

The setting of FSS ensures correctness and security that each party's key cannot individually reveal any information of f (Boyle, Gilboa, and Ishai 2015). We further adopt a distributed oblivious RAM (Doerner and Shelat 2017) to optimize the computational complexity to $O(n)$ which outperforms current state-of-the-arts such as circuit oblivious RAM (Wang, Chan, and Shi 2015) and square-root oblivious RAM (Zahur et al. 2016).

To mitigate the latency trade-offs given by MPCs and increase resilience towards adversaries, we propose an adaptive proportional-derivative (PD) controller based on a two-predecessor-following scheme as shown in Figure 2, in which we assume all CAVs in the platoon to be identical, forming a homogeneous vehicle string. Below is the control command

$$U_i(s) = U_{b,i}(s) + U_{f,i-1}(s) + U_{f,i-2}(s) \qquad (1)$$

which consists of control feedback $U_{b,i}$ from the error E_i and two extra feedforward terms $U_{f,i-1}$ and $U_{f,i-2}$ from

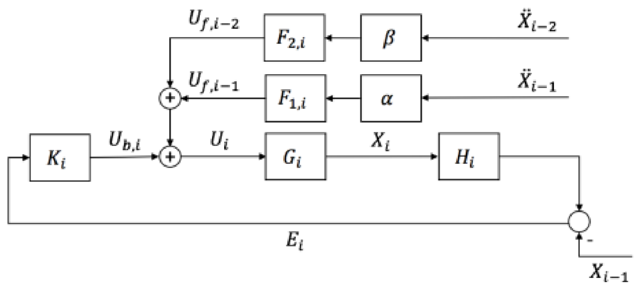

Figure 2: Diagram of the control schematic.

the acceleration rates $\ddot{X}_{i-1}$ and $\ddot{X}_{i-2}$, respectively. X_i is the position output, X_{i-1} is the feedback position information from the immediate predecessor. K_i is the feedback controller which generates a control command to rectify the error. G_i represents the ideal longitudinal vehicle dynamics. H_i denotes spacing policy (e.g., CD and CTH), and $F_{1,i}$ and $F_{2,i}$ are feedforward filters to process the acceleration information from the corresponding predecessor vehicles. α and β are indicators for the success of V2V communications (α and β are equal to 1 for a successful communication between the CAV and the corresponding predecessor vehicles, and 0 otherwise). These terms will be explained in detail later.

4 Discussion and Future Works

The AutoMPC model leverages advances in cryptography to control theory for safer, smoother, and smarter transportation. The contributions lie in several ways: (i) security and privacy are guaranteed via a MPC scheme, without the presence of third-party authentication; (ii) the efficiency of the MPC is achieved by a distributed oblivious RAM and a function secret sharing scheme, and thereby avoids the homomorphic encryption approach which is computationally expensive; and (iii) an adaptive proportional-derivative controller is proposed to increase the resilience toward latency and adversarial attacks. Preliminary experimental results also validate above findings by comparing control performances in speed, spacing, and acceleration rate. Theoretical properties in security and control as well as more experimental results will be discussed in the full paper.

Acknowledgments

The authors thank Jian Wang, Yuntao Guo, Chaojie Wang, and Anye Zhou for insightful discussions and anonymous reviewers for their helpful comments.

References

Angraal, S.; Krumholz, H. M.; and Schulz, W. L. 2017. Blockchain technology: applications in health care. *Circulation: Cardiovascular Quality and Outcomes* 10(9):e003800.

Boyle, E.; Gilboa, N.; and Ishai, Y. 2015. Function secret sharing. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 337–367. Springer.

Boyle, E.; Gilboa, N.; and Ishai, Y. 2016. Function secret sharing: Improvements and extensions. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1292–1303. ACM.

Doerner, J., and Shelat, A. 2017. Scaling oram for secure computation. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 523–535. ACM.

Du, W., and Atallah, M. J. 2001. Secure multi-party computation problems and their applications: a review and open problems. In *Proceedings of the 2001 workshop on New security paradigms*, 13–22. ACM.

Franklin, M., and Yung, M. 1992. Communication complexity of secure computation. In *Proceedings of the twenty-fourth annual ACM symposium on Theory of computing*, 699–710. ACM.

Goldreich, O., and Ostrovsky, R. 1996. Software protection and simulation on oblivious rams. *Journal of the ACM (JACM)* 43(3):431–473.

Gong, S.; Zhou, A.; Wang, J.; Li, T.; and Peeta, S. 2018. Cooperative adaptive cruise control for a platoon of connected and autonomous vehicles considering dynamic information flow topology. In *the 21st IEEE International Conference on Intelligent Transportation Systems*.

Gordon, S. D.; Katz, J.; Kolesnikov, V.; Krell, F.; Malkin, T.; Raykova, M.; and Vahlis, Y. 2012. Secure two-party computation in sublinear (amortized) time. In *Proceedings of the 2012 ACM conference on Computer and communications security*, 513–524. ACM.

GSMA. 2013. Gsma: Every new car connected by 2025 as embedded mobile technology drives growth of connected car market.

IEEE. 2012. News releases.

International, S. 2014. Automated driving: levels of driving automation are defined in new sae international standard j3016.

Lamport, L.; Shostak, R.; and Pease, M. 1982. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)* 4(3):382–401.

Li, T., and Lin, L. 2018. Byzantine-tolerant v2x communication system. In *2018 INFORMS Annual Meeting Phoenix*.

Li, T.; Choi, M.; Guo, Y.; and Lin, L. 2018a. Opinion mining at scale: A case study of the first self-driving car fatality. In *2018 IEEE International Conference on Big Data*.

Li, T.; Kaewtip, K.; Feng, J.; and Lin, L. 2018b. IVAS: Facilitating safe and comfortable driving with intelligent vehicle audio systems. In *2018 IEEE International Conference on Big Data*.

Li, T. 2018. Modeling uncertainty in vehicle trajectory prediction in a mixed connected and autonomous vehicle environment using deep learning and kernel density estimation. In *the Fourth Annual Symposium on Transportation Informatics*.

Lin, L., and Li, W. 2018. A compressive sensing approach for connected vehicle data capture and recovery and its impact on travel time estimation. *arXiv preprint arXiv:1806.10046*.

Lin, L.; Wang, Q.; Huang, S.; and Sadek, A. W. 2014. Online prediction of border crossing traffic using an enhanced spinning network method. *Transportation Research Part C: Emerging Technologies* 43:158–173.

Lin, L.; Wang, Q.; and Sadek, A. W. 2015. A novel variable selection method based on frequent pattern tree for real-time traffic accident risk prediction. *Transportation Research Part C: Emerging Technologies* 55:444–459.

Lin, L.; Wang, Q.; and Sadek, A. W. 2016. A combined m5p tree and hazard-based duration model for predicting urban freeway traffic accident durations. *Accident Analysis & Prevention* 91:114–126.

Lin, L. 2018. Efficient collection of connected vehicle data based on compressive sensing. *arXiv preprint arXiv:1806.02388*.

Lu, S., and Ostrovsky, R. 2013. Distributed oblivious ram for secure two-party computation. In *Theory of Cryptography*. Springer. 377–396.

Parakh, A., and Kak, S. 2011. Space efficient secret sharing for implicit data security. *Information Sciences* 181(2):335–341.

Qu, F.; Wu, Z.; Wang, F.-Y.; and Cho, W. 2015. A security and privacy review of vanets. *IEEE Transactions on Intelligent Transportation Systems* 16(6):2985–2996.

Seetharaman, G.; Lakhotia, A.; and Blasch, E. P. 2006. Unmanned vehicles come of age: The darpa grand challenge. *Computer* 39(12).

Shamir, A. 1979. How to share a secret. *Communications of the ACM* 22(11):612–613.

Shladover, S. E. 2018. Connected and automated vehicle systems: Introduction and overview. *Journal of Intelligent Transportation Systems* 22(3):190–200.

Tapscott, D., and Tapscott, A. 2016. The impact of the blockchain goes beyond financial services. *Harvard Business Review* 10.

Wang, X. S.; Huang, Y.; Chan, T. H.; Shelat, A.; and Shi, E. 2014. Scoram: oblivious ram for secure computation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 191–202. ACM.

Wang, C.; Gong, S.; Zhou, A.; Li, T.; and Peeta, S. 2019a. Cooperative adaptive cruise control for connected autonomous vehicles by factoring communication-related constraints. In *the 23rd International Symposium on Transportation and Traffic Theory*.

Wang, J.; Peeta, S.; Lu, L.; and Li, T. 2019b. Multiclass information flow propagation control under vehicle-to-vehicle communication environments. *Transportation Research Part B: Methodological*.

Wang, X.; Chan, H.; and Shi, E. 2015. Circuit oram: On tightness of the goldreich-ostrovsky lower bound. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 850–861. ACM.

Yao, A. C. 1982. Protocols for secure computations. In *Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on*, 160–164. IEEE.

Yao, A. C.-C. 1986. How to generate and exchange secrets. In *Foundations of Computer Science, 1986., 27th Annual Symposium on*, 162–167. IEEE.

Zahur, S.; Wang, X.; Raykova, M.; Gascón, A.; Doerner, J.; Evans, D.; and Katz, J. 2016. Revisiting square-root oram: efficient random access in multi-party computation. In *Security and Privacy (SP), 2016 IEEE Symposium on*, 218–234. IEEE.