Multi-Party Computation for Resilient Coordination in Self-Organizing Swarms

Yeghisabet Alaverdyan
Institute for Informatics and
Automation Problems of NAS RA
Yerevan, Armenia
e-mail: ealaverdjan@gmail.com

Suren Poghosyan
Institute for Informatics and
Automation Problems of NAS RA
Yerevan, Armenia
e-mail: surenpoghosyan55@gmail.com

Vahagn Poghosyan
Institute for Informatics and
Automation Problems of NAS RA
Synopsys Armenia CJSC
Yerevan, Armenia
e-mail: povahagn@gmail.com

***Abstract*—Multi-party computation provides a compelling paradigm for secure and privacy-preserving collaboration among distributed entities in ad-hoc networks, and has a growing role in self-organizing systems that autonomously configure and coordinate their components without centralized control. Multi-party computation approaches evolving to meet the architectural and functional demands of self-organizing systems and swarms include techniques such as threshold secret sharing, homomorphic encryption, garbled circuits for pairwise computations, decentralized learning, blockchain, and asynchronous computations designed for dynamically changing topologies. Resilient coordination in self-organizing swarms also suggests embedding mechanisms that enable a decentralized network of highly collaborative peers coordinating actions or decisions, even when some nodes fail, misbehave, or set maliciously. Asynchronous setting of swarms allows messages between peers to be delayed, lost, or arrive out of order. Absence of the global clock and possibility for peers to join or leave the network at any time render these networks dynamic and decentralized without a stable infrastructure or fixed routing. The paper introduces premises for secure asynchronous multi-party computation, also presents a model to ensure explainability and intelligent control of the decisions made during the swarm mission.**

***Keywords*—Multi-party computation, self-organization, asynchronous setting, explainability.**

I. Introduction

In many emerging applications ranging from UAV swarms and mobile sensor networks to ad-hoc cyber-physical systems, distributed peers must make collaborative decisions in real-time without relying on central control or synchronized communication. These environments are inherently dynamic, privacy-sensitive, and pose significant challenges when embedding traditional decision-making models. While multi-party computation (MPC) provides a foundation for privacy-preserving collaboration, its classical forms assume synchronous interaction and lack transparency in how decisions are derived. This black-box nature undermines trust, especially when systems must justify their behavior or adapt to contextual shifts. To address these issues, we propose an asynchronous multi-party computation framework that integrates explainability and intelligent control. Our approach enables peers to jointly compute decisions in a delay-tolerant and privacy-preserving manner, while also understanding the reasoning behind outcomes and autonomously adjusting their behavior based on local context and observed network dynamics. This represents a critical step toward building accountable, resilient, and self-organizing intelligent systems for next-generation ad-hoc environments.

Peers in the UAV swarms act as self-organizing agents with the capability to reason, draw inferences and conclusions, and act based on available evidence. The foundations for building intelligent swarm agents are presented in a series of our publications [1-5]. These include construction of cognitive peers, algorithms for comprehensive information exchange, cloud-based models for self-organization, the development of a multi-user UAV swarm simulation platform, and a tamper-proof solution designed to prevent unauthorized access, interference, or manipulation, thus ensuring the integrity and security of the swarm mission.

Asynchronous multi-party computation (AMPC) enables secure computations across networks where message delivery is not a rare event. For large, distributed systems, AMPC offers efficiency and flexibility compared to synchronous approaches by allowing parties to proceed with computations and actions as soon as they receive stimuli, rather than waiting for a global synchronization.

II. Related Works

Authors in [6] employ Beaver's circuit randomization over shared random multiplication triples, allowing each party to prepare its own multiplication triples. Given enough such shared triples, potentially partially known to the adversary, they developed a method to extract shared triples unknown to the adversary. This allows avoiding communication-intensive protocols and achieves a secure asynchronous multiparty computation. The work [7] presents an AMPC protocol with optimal resilience, involving $n = 3t + 1$ parties and tolerating a computationally bounded static adversary, capable of corrupting up to t parties. In the offline phase, the parties produce encryptions of random multiplication triples using a linearly homomorphic encryption scheme with support for one homomorphic multiplication. Random multiplication triples are used to securely evaluate the multiplication gates in the online phase, using Beaver's

https://doi.org/10.51408/csit2025_01

circuit-randomization technique. Asynchronous Byzantine Agreement (BA) protocols [8] with subquadratic communication complexity tolerate an adaptive adversary who can corrupt $f < \frac{1-\epsilon}{3}$of the parties (for any $\varepsilon > 0$). Depending on the predefined scenario, initial setup by a trusted dealer is optional.

Analysis of existing AMPCs shows the impracticality of deploying them in large, dynamic, or distributed networks: they lack mechanisms to support dynamic joining or leaving, which is essential in real-world systems like UAV swarms. They may also be fragile against malicious behavior, especially if more than a certain threshold of parties is corrupted. For dynamically reconfigurable swarms, robustness against Byzantine faults, Sybil attacks, or node compromise becomes insufficient. Besides, the computation process in some AMPC implementations is opaque and difficult to trace, verify, or explain. This limits their applicability in regulation-sensitive domains where auditability, explainability, and traceability are critical. As swarm systems increase in complexity, they become more prone to logical inconsistencies or anomalous behaviors. Without robust verification and mechanisms to trace decision pathways, these systems fail to provide justifiable explanations for behavioral shifts, ultimately eroding trust and regulatory compliance.

The challenge with embedding AI is the lack of insight into the processes leading to the model outcomes, as well as to interpret the rationality to perform as intended and assert the flow of information through the network. Authors in [9] outlined a taxonomy for explanation methods: *rule-extraction methods, attribution methods, and intrinsic methods.* Four concepts of explainability are given in [10]: *explain to justify, explain to control; explain to improve, and explain to discover.* The authors preserved the principle of the Five W's (What, Who, When, Why, Where, and How) to cover all aspects related to XAI. In [11], the authors present recent developments in explainability approaches from two different perspectives: ML models that feature some degree of transparency, thereby interpretable to an extent by themselves, and the post-hoc XAI techniques devised to make ML models more interpretable. The authors also develop the concept of Responsible AI, a paradigm that imposes a series of AI principles to be met when implementing in practice, including fairness, transparency, and privacy. Causality between features and the target variable tracing by injecting counterfactual explanations into the prediction model and generating counterfactual instances using adjusted features to reverse the prediction results is presented in [12]. The authors introduced a Counterfactual Explanation Generation method with the Minimal Feature Boundary (MFB), named (CEG MFB). The proposed CEG MFB algorithm consists of two stages: *mining the MFB*, which can reverse the prediction results to restrain the generation range of counterfactual instances, and constructing *a counterfactual generative method* for generating counterfactual instances within the MFB to realize the minimum reversing cost.

In this paper, we outline our proposed asynchronous multi-party computation (AMPC) framework, which integrates several mathematical domains to support secure, explainable, and adaptive decision-making in self-organizing UAV swarms.

III. Mathematical Preliminaries

Mathematical foundations that support an asynchronous multi-party computation framework for resilient coordination in self-organizing swarms with explainability and intelligent control focus on definitely connecting AI/ML, logic, and algebraic structures to the core functions of the system. We propose developing the system based on the following pillars.

- Asynchronous Message Passing
- Threshold logic for algebraic cryptography
- Model approximation
- Quantifying decision influence

For obtaining asynchronous message passing, we adopt proven methods formalized by eventual delivery using a special class of state machines, known as asynchronous labeled transition systems (ALTS). ALTS is commonly used in distributed computing, communication protocols, consensus algorithms, and fault-tolerant solutions.

Our proposed ALTS can be modeled as the following tuple.

$$M = (S, s_0, M, A, \delta), \text{ where}$$

- S is the set of states,

- $s_0 \epsilon S$ is the initial state,

- M is the set of messages,

- A is the set of actions partitioned into
  - o $send(m)$for messages $m \in M$subject to send, and
  - o $recv(m)$for messages $m \in M$subject to receive

- $\delta \subseteq S \times A \times S$ is the transition relation.

Message queue is developed according to the swarm mission performance, based on standard I/O protocol, FIFO, depending on the embedded semantics.

In self-organizing swarms with a strong membership verification and information full exchange, where every process is known to every peer, implementing the algorithm of Birman et al., 1999, is widely recommended. It uses gossip, a.k.a. epidemic dissemination of messages. Messages are delivered to all recipients, even if the sender fails before sending to all. The algorithm is fault-tolerant against crash failures and a number of link failures.

In our construction, we incorporate the Birman algorithm in the state machine implementation.

IV. Premises for Construction

We propose developing a verifiable secret sharing based on non-commutative and non-associative algebraic groups. Conventional Shamir's threshold scheme lacks intrinsic share verification during the reconstruction phase, which exposes the protocol to adversarial injection of forged shares by unauthorized entities. Such attacks can trigger incorrect computations and redundant communication inclusion into the swarm, ultimately leading to increased energy drain and premature battery depletion in resource-constrained devices.

We select n random elements from a quasigroup (Q, * /, \).

$$s_1, s_2, \dots s_n \in Q$$

The three operations of the quasigroup are multiplication ($*$), left division (/), and right division (\), each resulting in different outcomes and having their own inverses. The multiplication operation for a selected quasigroup may be a Latin square.

In our construction, we involve all three operations. Appropriate inverses of the quasigroup. Inverse operations may be outlined as follows.

$$s_{n1} = s_1 \ *^{-1} \ s_2 *^{-1} \dots *^{-1} s_{n-1},$$
$$s_{n2} = s_1 \,/^{-1}\, s_2/^{-1} \dots/^{-1} s_{n-1},$$
$$s_{n3} = s_1 \,\backslash^{-1}\, s_2\backslash^{-1} \dots\backslash^{-1} s_{n-1}.$$

The verification of the shares and the reconstruction of the secret are performed by the chain of computations.

$$s = s_{n1} * \ s_{n1-1} * \ s_{n1-2} * \dots * s_1$$
$$s = s_{n2}/\, s_{n2-1}/\, s_{n2-2}/ \dots/s_1$$
$$s = s_{n2}\backslash\, s_{n2-1} \,\backslash\, s_{n2-2}\backslash \dots\backslash s_1$$

Note that quasigroup computer representation is very efficient due to utilization of solely logical operations: lookup of the quasigroup square matrices.

In our construction, we will approximate

- system dynamics, $s = f(s, u)$, where s is the current state, and u is a control input signal.
- environmental stimuli: e.g., obstacles, noise, signal interference, etc.
- sensor or actuator behavior: e.g., latency, drift.
- control policy to approximate a function that maps state to control: $u = g(x)$.

For the model interpretability and explainability, a Linear model will be selected as a basic predictable solution. For high expressiveness, a suitable neural network will be promoted and tested. Then, a learning model will be constructed accordingly along with the error rate minimization tactics. By deploying a control-theoretic logic along with rule-based agent behavior, the system will govern how a peer:

- accepts or rejects contributions from others (e.g., based on trust scores or behavioral history),
- adjusts computation strategies in response to environmental or network dynamics.
- enables adaptive MPC parameters (thresholds, weights) based on network observations, monitored asynchronously.

Ephemeral identities and token-based authentication (e.g., using blind signatures) will allow peers dynamically join or leave without compromising the swarm computational integrity and network dynamic topology. During the mission performance, peers broadcast signed summaries of:

- why a certain output was accepted?
- which input factors influenced the outcome?

All explanations utilize a Zero-knowledge proof (ZKP) to validate the exchanged information without exposing secrets. To achieve the swarm intelligent control, an eponymous module will be developed to promote:

- trust metrics based on past participation and accuracy rate
- rule-based systems over fuzzy logic for decision tuning, and
- reinforcement signals in terms of feedbacks from environment.

In order to construct a trusty model and to measure how much an individual input, agent, or component influences the final decision or current outputs, we involve a gradient-based influence approach, dy/d_{x_i} to assess how sensitive the output y is to small changes in x_i.

The predefined threshold values controlling the boundaries will detect the outliers pointing to the shift of the system expected behavior. Here, logging of all internal processes will be conducted by recording all appropriate and non-appropriate outcomes. This traceability of the system will reveal, interpret and control the overall system behavior under decisions made by the AI.

To assess the cumulative influence, the following metric of the integrated gradient will be involved (Sundarajan and al, 2017).

$$IG\ (x) \coloneqq (x_i - x_i' \times \int_{\alpha=0}^{1} \frac{dF(x'+\alpha\times(x-x'))}{dx_i})d\alpha.$$

Here, the integral is taken along a straight path from the baseline x' to the instance x parameterized by the parameter α.

For model approximation, a local surrogate model, Local Interpretable Model-agnostic Explanations (LIME), is applied. Local surrogate model is a classical technique, used to explain individual predictions of a "black-box" machine learning model output in the region of a specific data point.

To explain the entire system black-box model's behavior, global surrogate models will be involved accordingly.

Local surrogate models with interpretability constraint are expressed as follows:

$$explanation(x) = argminL(\check{f}, g, \pi_x) + \Omega(g), g \in G$$

Here,

- x is an instance
- L is the loss function measured by mean square error
- $\check{f}$ is the original model
- g is the model under construction, which may be a linear regression model
- π_x is the proximity measure which outlines the neighborhood around the given instance considered for the explanation.
- $\Omega(g)$ is the measure of the model complexity. With fewer features, this complexity will be kept low.

In practice, LIME optimizes the loss part.

Then, we select a target instance for which we will get the required explanation for its black box prediction. Database sampling with new points will reveal the weights of proximities. Then, the analysis of a weighted interpretable model on the dataset will explain the prediction by interpreting the local model.

In our construction, we embed the following model.

$$\hat{f}(x) = w_0 + \sum_{i=0}^{t-1} w_i x_i \quad (LIME, SHAP)$$

We involve SHAP (Shapley Additive Explanations), which is another efficient machine learning technique for model explainability, widely used in game theory. Here, each feature is assigned a numerical rate value that reveals the feature contribution to a model's prediction for a specific instance across the entire dataset. It addresses the "black-box" problem of complex models by providing both local (per-instance) and global (overall model) insights into how features influence predictions. Meanwhile, feature attribution will incorporate the so-called Shapley values from cooperative game theory.

$$\phi_i(f) = \sum_{S \subseteq N\{i\}} \frac{|S|!\,(n - |S| - 1)!}{n!} [f(S \cup \{i\}) - f(S)]$$

Here,

- n is the number of players
- the sum extends over all subsets S and N not containing player i, including the empty set.

Shapley values provide a "fair share" or "payout" for each feature by reflecting its impact on the deviation of the prediction from the average model output.

Finally, the decision influence will be estimated using quantification of the mutual information, as follows:

$$I(X_i; Y) = H(Y) - H(Y|X_i).$$

Control rules will be modeled as predicate expressions of the form:

$$x \in P\colon if\ Trust(x) > \tau \Rightarrow Include(x).$$

As a representational model of trust for the evaluation of propositional logic terms, probability and fuzziness under uncertainty, proven models given in [12-16] will be evaluated for appropriateness and applied.

The proposed AMPC model will embed the Shortest Vector Problem (SVP) adapted to lattices over algebraic number fields rather than standard Euclidean lattices over Z^n. Lattice-based cryptographic solutions are secure even against quantum attacks. The algebraic lattice will be constructed over the ring of integers R_K of a number field K.

Given a lattice $\mathcal{L} \subset R^n$ generated by a basis $B = \{b_1, \dots, b_n\}$, the SVP asks for a non-zero vector $v \in \mathcal{L}\{0\}$ such that

$$||v|| = \min(||w||),$$
$$w\epsilon\ \mathcal{L}\{0\}.$$

We base our construction on the module SVP (MSVP), which generalizes SVP over modules in R_K.

With a secret lattice embedded in the swarm peers' hardware, multi-party computation will verify the secret attributes and coefficients of the ring of integers R_K.

V. Conclusion

At its core, the proposed framework employs algebraic cryptographic techniques over finite fields to enable privacy-preserving computations without requiring synchronous communication. The system tolerates asynchrony and partial network participation through threshold-based reconstruction and verifiable secret sharing. For explainability, the framework leverages interpretable machine learning techniques, such as local surrogate models and Shapley value analysis, to attribute decision outcomes to individual input contributions in a mathematically principled manner. Adaptive behavior is supported through reinforcement learning, enabling peers to refine their strategies based on local observations and feedback. Modal and temporal logic are used to formalize the reasoning over knowledge states and control flow, while graph-theoretic methods underpin peer discovery, group formation, and secure communication structures. This mathematical foundation ensures the framework's capacity to function securely and intelligibly in complex, distributed, and delay-tolerant environments.

Acknowledgment

The research was supported by the Science Committee of the Republic of Armenia within the framework of the research projects 24DP-1B016 and 21AG-1B052.

References

[1] Y. Alaverdyan, "Multi Agent Machinery in Construction of Cognitive Systems", *Journal of Neuro Quantology*, vol. 20, Issue 8, pp. 2445--2452, 2022.

[2] S. Poghosyan, Y. Alaverdyan, V. Poghosyan, A. Lazyan, D. Hayrapetyan, Yu. Shoukourian, "Algorithms for operating self-organizing swarms of UAVs implementing full exchange of information", *AIP Conference Proceedings*, 2757, 070003, 2023.

[3] S. Poghosyan, V. Poghosyan, S. Abrahamyan, A. Lazyan, H. Astsatryan, Y. Alaverdyan, K. Eguiazarian, "Cloud-Based Mathematical Models for Self-organizing Swarms of UAVs: Design and Analysis", *Drone Systems and Applications*, vol. 99, pp. 1--17, 2024.

[4] V. Poghosyan, S. Poghosyan, A. Lazyan, A. Atashyan, D. Hayrapetyan, Y. Alaverdyan, H. Astsatryan, "Self-Organizing Multi-User UAV Swarm Simulation Platform", *Programming and Computer Software*, vol. 49, pp. S7--S15, 2024.

[5] S. Poghosyan, V. Poghosyan and Y. Alaverdyan, "Tamper-proof hardware solution and algorithms for UAV swarms operating in hostile environments", *CSIT Conference 2023*, Yerevan, Armenia, pp. 45--47, 2023.

[6] A. Choudhury, M. Hirt and A. Patra, "Asynchronous multiparty computation with linear communication complexity", *Proceedings of the 27th International Symposium on Distributed Computing*, vol. 8205, DISC 2013, pp. 388--402, Berlin, Heidelberg, Springer-Verlag, 2013.

[7] A. Choudhury and A. Patra, "Optimally resilient asynchronous MPC with linear communication complexity", *Proceedings of the 2015 International Conference on Distributed Computing and Networking, ICDCN '15*, New York, USA, 2015, Article no. 5, pp.1--10, 2015.

[8] E. Blum, J. Katz, C-D. Liu-Zhang and J. Loss. "Asynchronous byzantine agreement with subquadratic communication, *Rafael Pass and Krzysztof Pietrzak, editors, TCC Part I*, vol. 12550 of LNCS, Springer, Heidelberg, pp. 353—380, November 2020.

[9] G. Ras, M. van Gerven and P. Haselager, "Explanation methods in deep learning: Users, values, concerns and challenges," *Explainable and Interpretable Models in Computer Vision and Machine Learning*, Springer, pp. 19--36, 2018.

[10] A. Adadi and M. Berrada, "Peeking inside the black-box: A survey on explainable artificial intelligence (xai)", *IEEE Access*, vol. 6, pp. 52138--52160, 2018.

[11] A. B. Arrieta, N. D´ıaz-Rodr´ıguez, J. Del Ser, A. Bennetot, S. Tabik, A. Barbado, S. Garc´ıa, S. Gil-Lopez, D. Molina, R. Benjamins et al., "Explainable artificial intelligence (xai): Concepts, taxonomies, opportunities and challenges toward responsible AI", *Information Fusion*, vol. 58, pp. 82--115, 2020.

[12] R. Moraffah, M. Karami, R. Guo, A. Raglin and H. Liu, "Causal interpretability for machine learning-problems, methods and evaluation", *ACM SIGKDD Explorations Newsletter*, vol. 22, no. 1, pp. 18--33, 2020.

[13] D.W. Manchala, "E-Commerce Trust Metrics and Models", *IEEE Internet Computing*, March-April, pp. 36-44. 2000.

[14] J. Tian, Ch., X. He, R. Tian, "A Trust Model Based on The Multinomial Subjective logic for P2P Network", *International J. communications, Network and Systems*, vol. 2, pp. 546-554, 2009.

[15] N. Nilsson, "Probabilistic Logic", *Artificial Intelligence*, vol. 28, pp. 71--87, 1986.

[16] W. Teacy, et al. "Trust and reputation in the context of inaccurate information sources", *Aut. Agentsand Multi-Agent Systems*, vol. 12, no. 2, pp. 183--198, 2006.