Distributed Participation to Threshold Signature Analyzed via Game Theory

Alessandro Buratto
Dept. Inf. Engineering (DEI)
University of Padova
Padova, Italy
alessandro.buratto.1@phd.unipd.it

Sara Ricci, Petr Dzurenda
Dept. Telecommunications (FEEC)
Brno University of Technology
Brno, Czech Republic
{ricci,dzurenda}@vut.cz

Leonardo Badia
Dept. Inf. Engineering (DEI)
University of Padova
Padova, Italy
leonardo.badia@unipd.it

***Abstract*—We investigate the performance of a distributed threshold signature scheme, where at least t out of n signers must participate to authenticate a message. We model this scheme as a participation game, where individual signers choose whether to submit their contribution to the (t, n) signature with a certain probability and incur a cost in doing so. We discuss the resulting Nash equilibria of the game and specifically investigate the symmetric mixed-strategy Nash equilibrium, which corresponds to a stable operating point of distributed decisions made individually by the agents. Finally, we show how tweaking the information revealed to the signers may improve the efficiency of this resulting equilibrium. This study highlights a fundamental trade-off between system-wide efficiency and individual resource consumption. Our proposed mechanism thus provides a practical method for steering a decentralized system towards a more globally efficient outcome without resorting to an impractical and unfair centralized control structure.**

***Index Terms*—Threshold signature; Game theory; Distributed control; Participatory games; Secret sharing.**

I. Introduction

Modern communications and control systems are increasingly shifting towards distributed decision-making mechanisms to cope with the large scale and heterogeneity of interconnected devices [1], [2]. Another strong factor in favor of distributed control is that real-time and latency-critical applications on vast networks of sensors and actuators cannot rely on centralized management, which would become impractical and suffer from the curse of scalability [3].

Thus, in view of a convergence towards the Internet of Everything (IoE), systems are embracing decentralized architectures where local entities autonomously process data and make timely decisions. This poses the challenge of coordination among peers to enable fast response times and efficient resource usage. In particular, in this paper, we focus on the aspects of consensus and trust, which are relevant whenever a generalized agreement is required, at least by a certain subset of nodes, on a specific decision [4]–[6].

For these kinds of scenario, threshold signatures have received interest in recent years due to their ability to support distributed ledger applications such as blockchain [7]. Traditional digital signatures require a single trusted entity to sign, which possibly creates a bottleneck. Threshold signatures address this limitation by allowing any subset of at least t out of n blockchain/computer nodes to produce a valid signature, which is more compact and scalable. They enable decentralized trust, while preserving signature authenticity and robustness, even when some participants are unavailable or uncooperative. However, in realistic decentralized environments, especially in blockchain and similar systems, individual nodes often act autonomously and may incur costs (e.g., computational, communication, or energy-related) to participate in protocols. This introduces the question of whether rational agents will voluntarily participate in signing operations, even when technically capable.

Notably, in 2023, the National Institute of Standards and Technology (NIST) released a draft for its first call for multiparty threshold schemes [8], highlighting the growing standardization efforts and increasing adoption of these schemes. Moreover, threshold signatures have found applicability in blockchain, distributed key management, secure multiparty computation, and consensus protocols [9], [10]. In light of these developments, it becomes essential to understand not only the technical efficiency of threshold signatures but also the strategic behavior of the participating nodes. To our knowledge, this dimension has not been systematically explored in the literature.

In this paper, we investigate how to incentivize participation by individual agents to the threshold signature. We consider a scenario where nodes incur a cost when taking part in the global signature, and therefore, may be reluctant to contribute. However, if nodes rationally consider the successful completion of a signature as a positive reward, they may receive a proper incentive to submit their contribution to the signature. We also propose an improved version of the game, where the assumption of complete information is removed, to improve the efficiency of the allocation. Specifically, we assume that the central collection signature mechanism correctly informs the individual agents of their cost and their total number n, but actually pretends t to be a higher number, to incentivize their participation. We show how this mechanism leads to an improved Nash equilibrium compared with the optimal

This work has been supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, Cascade project SERICS (SEcurity and RIghts in the CyberSpace) PE00000014 PE7 SPOKE 4, CUP D33C22001300002, and by Ministry of the Interior of the Czech Republic under Grant VJ03030014 (Development of International Collaboration in Cryptography and Cybersecurity Research).

allocation, still allowing for a fully distributed approach.

The remainder of the paper is structured as follows. Threshold signatures are described in Section II. Our methodology and conceptual framework is discussed in Section III. Our proposed structure of the game-theoretic analysis is presented in Section IV. In Section V, we discuss the resulting symmetric Nash equilibrium and propose a variation, where t is changed to a different value. Section VI presents numerical evaluations. Section VII concludes the paper and outlines future extensions.

II. Preliminaries: Threshold Signatures

Threshold cryptography enables a set of distributed parties to jointly perform cryptographic operations, such as signing and verifying, without reconstructing the underlying secret key. A building primitive in this domain is threshold secret sharing [11], where a secret k is distributed among n parties so that only certain qualified subsets can recover it.

In the widely adopted (t, n)-threshold model, any subset of at least t parties can reconstruct the secret, while any group of fewer than t learns nothing about it. A well-known example is Shamir's scheme [12], which embeds the secret as the constant term of a random polynomial of degree $t - 1$. Each party receives a share corresponding to a unique evaluation point of the polynomial. Reconstruction is based on the uniqueness of low-degree polynomials through t points and can be efficiently achieved via Lagrange interpolation.

On the other hand, secret sharing without threshold allows for arbitrary definitions of qualified subsets. For example, the Ito, Saito and Nishizeki construction [13] supports any monotone access structure, providing fine-grained control over which groups can recover the secret. Such generalizations are particularly useful in advanced applications, such as attribute-based encryption and role-based access control.

Building on these foundations, threshold signature schemes permit n parties to jointly generate a single public key from n private shares of a secret signing key. The system ensures that any subset of at least t parties can collaboratively produce a valid signature, while no coalition of fewer than t parties can forge a signature or recover the secret key.

Algorithm 1 (t, n)**-Threshold Signature**

```
Parties: $P_1, \ldots, P_n$                    ▷ $n$ parties, threshold $t$
1. KeyGen$(t, n)$:
Each $P_i$ runs a distributed protocol to generate:
    A public key $pk$
    A private signing share $sk_i$ of the secret signing key
2. Sign$(m, \{sk_j\}_{j \in \mathcal{J}_t})$:
    Input: message $m$, signing shares from subset $\mathcal{J}_t \subseteq [n]$ with $|\mathcal{J}_t| \geq t$
    Each $P_j \in \mathcal{J}_t$ computes partial signature $\sigma_j$
    $\{\sigma_j\}_{j \in \mathcal{J}_t}$ are aggregated to produce the signature $\sigma$
3. Verify$(m, \sigma, pk)$:
    Input: message $m$, signature $\sigma$, public key $pk$
    Accept or Reject based on signature validity
```

Threshold signatures [14]–[20] combine secret sharing with standard digital signature schemes to enable secure and decentralized signing processes. A sketch of a generic threshold scheme is given in Algorithm 1. In the Internet Computer Protocol (ICP) used in blockchain, threshold cryptography is employed to sign state transitions of smart contracts using a decentralized network of nodes [21]. This design eliminates the need for a single trusted signer and ensures verifiable execution, scalability, and fault tolerance. A quorum of nodes is sufficient to authorize operations, making the system robust against node failures or malicious behavior. Another example is ZetaChain, where Threshold BLS (tBLS) signatures are currently employed to manage cross-chain asset control and message authentication across multiple blockchains [22].

III. Methodology and Conceptual Framework

For the evaluation, we adopt an approach based on *game theory* [23]–[25]. We model the threshold signature as a participation game in which individual signers choose whether to contribute to the (t, n) signature with a certain probability (called a *mixed strategy* in the jargon of game theory) and incur a cost c in doing so. If the number of signers is greater than or equal to t, then the task is successful; otherwise no reward is achieved, but still the signers who decided to participate in the procedure pay the cost c, thus achieving negative utility.

In the initial version of the game, all the above is common knowledge among the players (specifically, the number n of other potential signers and the threshold t to achieve, as well as the cost c that is paid for participation). In such a scenario, a *symmetric Nash equilibrium in mixed strategies*, i.e., a local decision-making mechanism where no individual agent has incentive to deviate from, can be seen as a stable operating point of distributed management. We discuss and compare the efficiency of this equilibrium point compared to a trivially optimal allocation consisting of choosing a participation of exactly t signers. The latter is clearly more efficient, as it is never at risk of having more signers than needed, which increases the cost, nor having fewer than t contributors, which would cause the signature task to fail. While using more than t participants may lead to unnecessary computational and communication overhead, achieving the optimal allocation of exactly t signers requires a centralized scheduler or trusted oracle to pre-select them which is an unrealistic assumption in decentralized environments. This also introduces fairness concerns, as the cost of participation would always fall on the same subset of nodes. In contrast, a symmetric mixed-strategy equilibrium spreads participation probabilistically, promoting fairness and aligning more naturally with distributed, trustless systems.

While minimal participation is optimal in threshold signing, broader participation is beneficial in other settings, such as multiparty computation and distributed consensus, where it enhances robustness and reduces the risk of collusion or failure. Since these systems often rely on the same cryptographic primitives (e.g., secret sharing), our incentive-based analysis remains applicable, offering broader insights for decentralized protocols beyond threshold signatures.

IV. Proposed System Model

Consider a remote contract that can receive the contribution of n possible distributed signers. An immediate possible application of this scenario would be a blockchain wallet, which requires validation through a threshold signature mechanism. However, the same framework would also apply to a broader context of *participatory tasks* that involves remote sensing by multiple sources, federated learning, or distributed control within a cyberphysical system that requires consensus among a certain fraction of nodes [23].

This contract must collect at least t signatures to be valid; otherwise, it remains unexecuted [14], [18], [19]. We consider a fully distributed approach, that is, each signer independently decides whether to sign it or not, without consulting with the others or preliminary sending its decision to a central collection point. We approach this through *game theory*, which imposes that the criterion guiding the decision about whether to sign or not will be the rationality of the agents, i.e., each possible participant will decide to sign the contract if it is convenient to do so. However, this criterion is corroborated by full knowledge of the number of potential signers, as well as having complete information that they are also rational agents [26].

We represent that the individual agents are typically interested in this signature to succeed (otherwise, they would not even be involved in the game in the first place). Thus, we consider that the successful signature gives a reward r to each of the potential signers, regardless of whether they actually participated in the distributed signature or not. Without loss of generality, we can set $r{=}1$, since a different value can be taken simply by rescaling all reward and cost values.

In addition, it is assumed that signing the contract has an individual cost of $c \in (0, 1)$ for each agent, which can be linked to many motivations. These may include computational overhead, as cryptographic operations (e.g., key generation, signing, and verification) can be intensive, especially on constrained devices [10]. There is also a transmission cost related to the exchange of messages to obtain the digital signature, which can be significant in low-bandwidth communications. Furthermore, there is an additional burden imposed by the required availability for the signature task, as active participants must remain responsive during the signing operations, which may not align with their resource allocation [27]. Whatever the reason, claiming a cost for the signature operation is a typical game-theoretic assumption, which, simply put, describes that the distributed agents are lazy and know they can obtain a better benefit whenever the signature task succeeds without the need of their intervention, as they still get the reward without paying any cost. Clearly, this justifies that $c < r$ must hold, otherwise there is insufficient incentive for participation anyway.

We assume that all the parameters of the game are common knowledge to all the players. This leads to a game of *complete information* among the players, which individually make the decision of contributing to the signature task or not, knowing all the parameters of the game and that the other signers are also rational. Game theory also dictates that the perspective of the other players and the uncertainty about the others' moves is better represented through a so-called *mixed strategy*, which in the case under exam represents the probability of participation s_i by each player i [26]. In other words, the game results in a vector of n strategies $\mathbf{s} = (s_1, \ldots, s_n)$, where each agent i is the sole to set s_i. The special cases where an agent i decides to always contribute or be inactive are represented with *pure strategies* which are the probabilities $s_i{=}1$ and $s_i{=}0$, respectively. Within this context, we look for possible *Nash equilibria* in mixed strategies, consisting of a distributed choice of the signature probabilities that are strategically stable, i.e., where no agent has an incentive for unilateral deviation. In particular, for fairness reasons, we consider a *symmetric* Mixed Strategy Nash Equilibrium (sMSNE), where each agent decides to sign or not with the same probability s, i.e., $\mathbf{s} = (s, \ldots, s)$ [23]. We notice that other Nash equilibria are immediately found by considering pure strategy $s_i{=}1$ for $i \in \mathcal{A}$ and $s_i{=}0$ for $i \in \mathcal{N} \setminus \mathcal{A}$ where $\mathcal{N} = (1, \ldots, n)$ is the set of all users and $\mathcal{A}$ is the set of *active* users, as long as $|\mathcal{A}| = t$.

The latter *Pure Strategy Nash Equilibria* (PSNE) are clearly advantageous over the sMSNE, as it corresponds to a deterministic activation pattern and therefore completely avoids cases where the signature task does not succeed or an unnecessarily high number of signers participate, thus incurring a cost higher than needed. However, the PSNE would require a centralized decision to determine which agents are active, which goes against the principle of a game-theoretic implementation as a way to distribute management. From a game-theoretic perspective, this also causes a problem of equilibrium selection [28] to determine the exact set $\mathcal{A}$. Moreover, one can also argue that this raises some fairness issues, since the selection of the active participants in the set $\mathcal{A}$ should be cycled among all the players in the set $\mathcal{N}$. While in principle this achieves a better allocation, it also requires some coordination and possibly centralized supervision, which goes against the motivation behind a threshold signature mechanism.

Nevertheless, any PSNE (note that they all achieve identical global performance in terms of total rewards and costs) can be considered as the best solution in terms of network utility maximization. Thus, they are taken as the benchmark to evaluate the efficiency of the sMSNE directly resulting from distributed management [29].

V. Analysis of Strategic Participation

We first discuss some general properties that hold true in the game, which allow to identify the sMSNE. If all users sign with the same probability s, it means that the probability p_k that k users sign follows a binomial distribution.

$$p_k = \binom{n}{k} s^k (1 - s)^{n-k} \tag{1}$$

The signature succeeds with the survival rate of the binomial distribution $P_{\text{succ}} = \sum_{k\geq t} p_k$.

In this framework, we define the following utility function:

$$u_i(s_i) = r - c \cdot s_i \tag{2}$$

with binary reward structure

$$r = \begin{cases} 1 & \text{if signature succeeds} \\ 0 & \text{otherwise} \end{cases} . \tag{3}$$

A Nash equilibrium takes place when no deviation of an individual player gives them a direct gain [25]. However, if the change of participation of a single agent has no direct effect on the resulting success (as is, for example, the case when $k > t$ or $k < t-1$), then it is always convenient for that agent not to contribute to the signature and save the cost. Thus, the only case to consider in the computation for the Nash equilibrium is when the action of a single agent is critical, i.e., it can change the resulting outcome of the threshold signature. In this case, we look for the compensation of the cost for participation with the reward gained when changing from $t-1$ to t participants because of the change. This means that we can formulate

$$c = p_{t-1} \quad \Rightarrow c = \binom{n}{t-1} s^{t-1}(1-s)^{n-t+1} \tag{4}$$

which can be solved via numerical means.

We evaluate the performance of our game-theoretic solutions on a system-wide scale. For this reason, we define the global welfare of a solution as the sum of the utilities of all the nodes in the network evaluated with a specific activation strategy

$$W = \sum_{i \in N} u_i(s_i) \, . \tag{5}$$

With this definition, we can compute the amount of inefficiency introduced by a fully distributed solution. This is measured by the *price of anarchy* (PoA), which is a metric commonly adopted in game theory for problems that study the sharing of limited resources, or as in our case, the voluntary participation of signers to achieve a shared common objective [29], [30], and can be formalized as

$$\text{PoA} = \frac{W_{\text{opt}}}{W_{\text{NE}}} \, , \tag{6}$$

where W_{opt} is the global welfare obtained with a centralized optimal solutions, i.e., binary activation masks in our scenario, and W_{NE} is the global welfare of the Nash equilibrium. A value of $PoA \simeq 1$ means that a distributed solution is as efficient as a centralized one at a system-wide level, meaning that it can be adopted without sacrificing efficiency with respect to optimal centralized solutions.

VI. Results and Evaluation

In this section, we report the results of numerical simulations carried out for our model. For each plot, we have fixed $N = 20$ and $r = 1$. We compare the PSNE and sMSNE for two values of the required threshold t. The dotted lines indicate that we are applying the game theory framework to the scenario in which there is complete and true knowledge of the required participation with $t = 10$. Conversely, continuous lines indicate the scenario in which signers are told a higher threshold than the true one which is still kept to $t = 10$, meaning that the signature will still be correctly performed even if less signers than the communicated required threshold decide to participate. As the solution for the pure strategies equilibria are binary activation masks, we plot the average probability of activation and per-signer utility by averaging across all agents in the network.

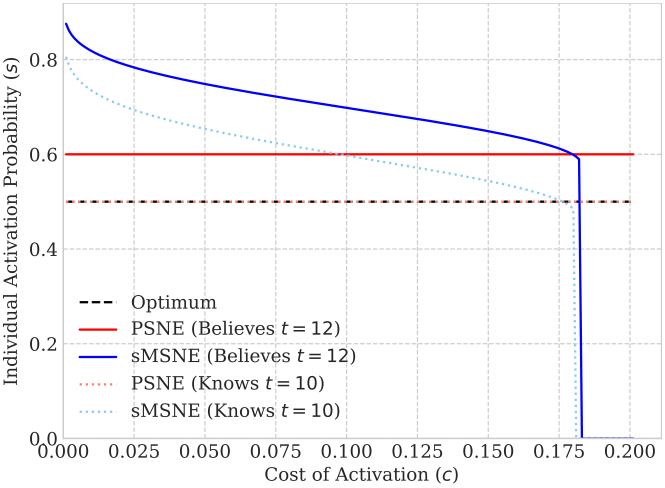

Fig. 1. Individual activation probability for Nash equilibria in pure and mixed strategies for the true value of the required threshold and an artificially raised one. $N = 20$.

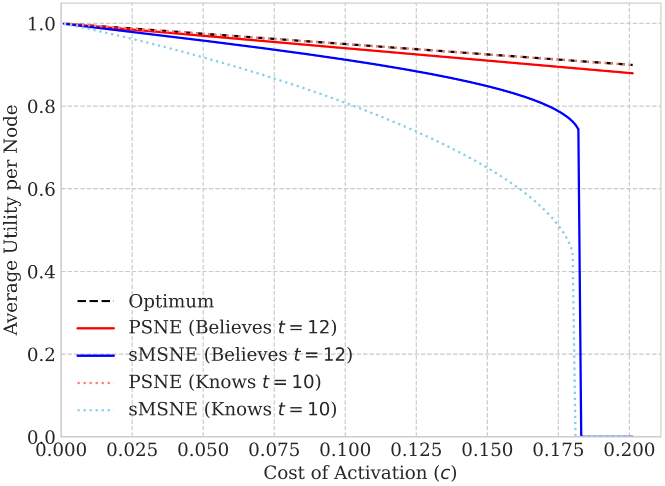

Fig. 2. Average per-signer utility for Nash equilibria in pure and mixed strategies for the true value of the required threshold and an artificially raised one. $N = 20$.

Fig. 1 shows the per-signer activation probability. As expected, increasing the participation threshold that the signers believe to satisfy increases the participation rate of the signers and also increases the cost that they are willing to sustain in order to satisfy the more stringent requirements. The vertical drops indicate exactly this threshold on the cost value. For

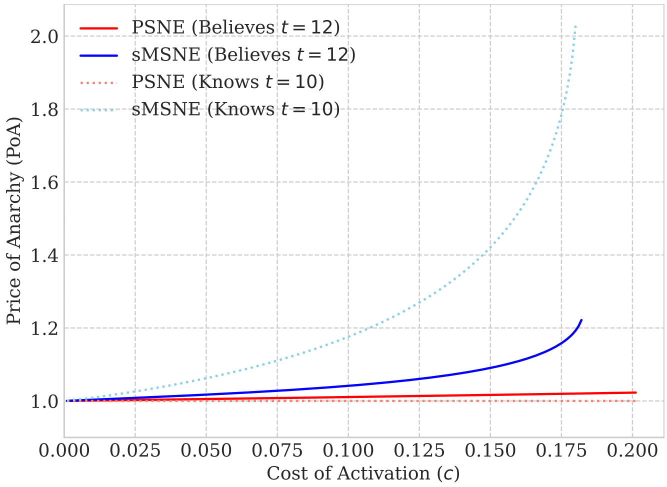

Fig. 3. Price of Anarchy for Nash equilibria in pure and mixed strategies for the true value of the required threshold and an artificially raised one. $N = 20$.

costs greater than this value, the sMSNE collapses into a pure strategy equilibrium with all the signers not participating, thus guaranteeing the failure of the signature.

Fig. 2 displays the average utility the signers obtain as formulated in (2). It is immediately evident that artificially increasing the participation of the signers has a positive effect to the utility achieved by the signers in mixed strategies. This is because in this case the task is much more likely to succeed even though the cost component of the utility is much higher, as can be noticed in Fig. 1 where the belief of $t = 12$ has the effect of boosting signers participation thus increasing the number of agents that will incur the activation cost. Another interesting remark is that, while for sMSNE the utility increases by setting a higher t, this cannot be said for PSNE, as a centralized activation of more than the exact number of required signers is just wasting resources.

Fig. 3 shows the PoA as computed in (6) for the considered distributed solutions. While it is again evident that requiring more participation using pure strategies results in a waste of resources, communicating a t higher than necessary for the sMSNE increases their efficiency by a large margin with higher cost values. This result suggests that forcing more collaboration in the network greately improves the efficiency of the system with the only expense of more resource consumption by the single signers. Thus, a tradeoff between system-wide efficiency and single-signer resource consumption appears. Requiring higher collaboration than necessary forces more signers to employ their resources, improving the odds of successful tasks, while only asking for the correct amount of signers to collaborate has only a local advantage for the signers that can allow themselves to activate more sporadically, thus compromising the efficiency for the whole system.

VII. Conclusions

In this paper, we have addressed the challenge of ensuring robust participation in distributed threshold signature schemes, which is a critical component for coordination and agreement in decentralized systems. Recognizing that individual agents may be disincentivized from contributing due to associated costs, we adopted a game-theoretic framework to model this scenario. We analyzed the behavior of rational signers as a participation game, identifying a stable, distributed operating point in the form of a symmetric mixed-strategy Nash Equilibrium.

Our analysis revealed that while this fully distributed equilibrium allows for autonomous decision-making, it suffers from inherent inefficiency when compared to a centrally-managed pure-strategy equilibrium where exactly the required number of signers participate. This inefficiency, captured by the Price of Anarchy, arises from the risk of failed signature attempts due to underparticipation or wasted resources from overparticipation.

The central contribution of this work is the introduction and evaluation of a simple yet effective mechanism to enhance the efficiency of the distributed system. By having the central authority communicate an artificially inflated participation threshold we can effectively incentivize signers to increase their participation probability thus raising the probability of a successful task. This, in turn, boosts the average utility per signer and substantially improves the Price of Anarchy, especially in high-cost scenarios where agents are otherwise more reluctant to contribute.

This study highlights a fundamental trade-off between system-wide efficiency and individual resource consumption. Forcing higher participation increases costs for the signers, but it greatly improves the collective benefit by making the distributed operation more reliable and efficient. Our proposed mechanism thus provides a practical method for steering a decentralized system towards a more globally efficient outcome without resorting to an impractical and unfair centralized control structure.

The analysis presented in this paper can be extended with multiple coexisting signature tasks, which might involve further consideration about coordination through game theory [25]. Moreover, incorporating other aspects such as asymmetry of the participants introducing personalized costs and rewards may be interesting for applications ranging from blockchain to federated learning. Furthermore, an important direction for future research lies in optimizing the choice of the parameters t and n, accounting for the presence of malicious or inactive signers. By explicitly modeling the probability of signer failure or adversarial behavior, one can derive more robust thresholds that maximize system reliability while minimizing resource expenditure.

Finally, the insights gained from this analysis are not limited to threshold signature schemes alone. The proposed game-theoretic framework and incentive mechanism can be generalized to other decentralized coordination tasks that rely on partial participation, such as multiparty computation, consensus protocols, or federated learning.

References

[1] J. Wang, Z. Yan, H. Wang, T. Li, and W. Pedrycz, “A survey on trust models in heterogeneous networks,” *IEEE Commun. Surv. Tut.*, vol. 24, no. 4, pp. 2127–2162, 2022.

[2] Q. Zhu, S. W. Loke, R. Trujillo-Rasua, F. Jiang, and Y. Xiang, “Applications of distributed ledger technologies to the Internet of things: A survey,” *ACM Comput. Surv. (CSUR)*, vol. 52, no. 6, pp. 1–34, 2019.

[3] A. Buratto and L. Badia, “Massive opportunistic sensing with limited collaboration for age of information,” in *Proc. IEEE Wirel. Commun. Netw. Conf. (WCNC)*, 2024.

[4] I. Murenin, E. Doynikova, and I. Kotenko, “Towards security decision support for large-scale heterogeneous distributed information systems,” in *Proc. Int. Conf. Sec. Inf. Netw. (SIN)*, vol. 1, 2021, pp. 1–8.

[5] S. Ricci, P. Dzurenda, J. Hajny, and L. Malina, “Privacy-enhancing group signcryption scheme,” *IEEE Access*, vol. 9, pp. 136 529–136 551, 2021.

[6] R. Rani, S. Kumar, and U. Dohare, “Trust evaluation for light weight security in sensor enabled Internet of things: Game theory oriented approach,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8421–8432, 2019.

[7] Y. Wang, B. Li, J. Wu, G. Liu, Y. Li, and Z. Mao, “An efficient multi-party signature for securing blockchain wallet,” *Peer-to-Peer Netw. Appl.*, vol. 18, no. 3, pp. 1–20, 2025.

[8] L. Brandao and R. Peralta, “NIST First Call for Multi-Party Threshold Schemes,” https://doi.org/10.6028/NIST.IR.8214C.ipd, 2023.

[9] F. Liu, Z. Zheng, Z. Gong, K. Tian, Y. Zhang, Z. Hu, J. Li, and Q. Xu, “A survey on lattice-based digital signature,” *Cybersecurity*, vol. 7, no. 1, p. 7, 2024.

[10] B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, and M. Peng, “When Internet of things meets blockchain: Challenges in distributed consensus,” *IEEE Netw.*, vol. 33, no. 6, pp. 133–139, 2019.

[11] A. Beimel, “Secret-sharing schemes: a survey,” in *Int. Conf. Coding Crypt.* Springer, 2011, pp. 11–46.

[12] A. Shamir, “How to share a secret,” *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[13] M. Ito, A. Saito, and T. Nishizeki, “Secret sharing scheme realizing general access structure,” *Electron. Commun. Jpn.*, vol. 72, no. 9, pp. 56–64, 1989.

[14] I. Damgård and M. Koprowski, “Practical threshold RSA signatures without a trusted dealer,” in *Int. Conf. Th. Appl. Crypt. Techn.* Springer, 2001, pp. 152–165.

[15] V. Shoup, “Practical threshold signatures,” in *Int. Conf. Th. Appl. Cryptol. Techn.* Springer, 2000, pp. 207–220.

[16] B. Cogliati, Y. Dodis, J. Katz, J. Lee, J. Steinberger, A. Thiruvengadam, and Z. Zhang, “Provable security of (tweakable) block ciphers based on substitution-permutation networks,” in *Proc. Ann. Int. Cryptol. Conf.* Springer, 2018, pp. 722–753.

[17] R. Gennaro and S. Goldfeder, “Fast multiparty threshold ECDSA with fast trustless setup,” in *Proc. ACM SIGSAC Conf. Comp. Commun. Sec.*, 2018, pp. 1179–1194.

[18] S. Ricci, P. Dzurenda, R. Casanova-Marqués, and P. Cika, “Threshold signature for privacy-preserving blockchain,” in *Proc. Int. Conf. Business Process Manag.*, 2022, pp. 100–115.

[19] C. Komlo and I. Goldberg, “Frost: flexible round-optimized schnorr threshold signatures,” in *Proc. Int. Conf. Sel. Areas Crypt.* Springer, 2020, pp. 34–65.

[20] S. Garg, A. Jain, P. Mukherjee, R. Sinha, M. Wang, and Y. Zhang, “hints: Threshold signatures with silent setup,” in *Proc. IEEE Symp. Secur. Privacy (SP)*, 2024, pp. 3034–3052.

[21] O. Tkachenko, “Threshold signatures,” https://internetcomputer.org/docs/references/t-sigs-how-it-works, 2025, last updated: May 28, 2025; Accessed: August 7, 2025.

[22] ZetaChain, “Threshold BLS signature for decentralized asset control,” https://www.zetachain.com/blog/threshold-bls-signature-for-decentralized-asset-control, Apr. 2025, accessed: 2025-08-07.

[23] A. Buratto, A. Mora, A. Bujari, and L. Badia, “Game theoretic analysis of AoI efficiency for participatory and federated data ecosystems,” in *Proc. IEEE Int. Conf. Commun. Wkshps (ICC Workshops)*, 2023, pp. 1301–1306.

[24] K. Saurav and R. Vaze, “Game of ages in a distributed network,” *IEEE J. Sel. Areas Commun.*, vol. 39, no. 5, pp. 1240–1249, May 2021.

[25] L. Badia, A. Zanella, and M. Zorzi, “A game of ages for slotted ALOHA with capture,” *IEEE Trans. Mob. Comput.*, vol. 23, no. 5, pp. 4878–4889, 2024.

[26] A. Buratto, A. Munari, and L. Badia, “Strategic backoff of slotted ALOHA for minimal age of information,” *IEEE Commun. Lett.*, vol. 29, no. 1, pp. 155–159, 2025.

[27] L. Badia, S. Merlin, A. Zanella, and M. Zorzi, “Pricing VoWLAN services through a micro-economic framework,” *IEEE Wireless Commun.*, vol. 13, no. 1, pp. 6–13, 2006.

[28] E. Đokanović, A. Munari, and L. Badia, “Harsanyi’s equilibrium selection for distributed sources minimizing age of information,” in *Proc. IEEE Mediterr. Commun. Comp. Netw. Conf. (MedComNet)*, 2024.

[29] M. Favero, C. Schiavo, A. Buratto, and L. Badia, “Price of anarchy for green digital twin enabled logistics,” in *Proc. IEEE Symp. Comp. Commun. (ISCC)*, 2025.

[30] D. Paccagnan, R. Chandan, and J. R. Marden, “Utility Design for Distributed Resource Allocation—Part I: Characterizing and Optimizing the Exact Price of Anarchy,” *IEEE Trans. Automat. Contr.*, vol. 65, no. 11, pp. 4616–4631, 2019.